Blockbit

Resource Center

Documentation

Blockbit NGFW - Administrator's Guide

Index

NGFW - CHANGELOGS

To see the list containing the Changelogs from all previous versions, click here.

Release Notes 2.4.1

21/11/2023

Several features have been implemented in the release of Blockbit NGFW 2.4.1:

- **Implemented DNS Content Filtering support.**
- **The Cluster's operation in HA has been optimized.**
- **The option to remove DHCP leases has been implemented.**
- **The Firewall settings received performance optimization options (tunning).**
- **The Web Filter settings received performance optimization options (tunning).**
- **Implemented WiFi support and network interface configuration screen.**
- **The IPSec VPN now supports Multi-Factor Authentication (MFA).**
- **DH groups 31 and 32 were implemented in the IPSec VPN - Remote Access encryption.**

The following table lists the improvements and Correctiones done in the release of the Blockbit NGFW 2.4.1:

Code	Description
8000	Correction done in the Web Filter error logs.
19901	Correction done in the analysis of Samples in the Sandbox.
24158	Correction done in Threat Protection Quarantine service.
25158	Correction done in the SD-WAN service not to remove packets tags.
26040	Correction done in Firewall Segfault errors.
26920	Correction done on IPS profiles in Port Forwarding rules which were blocking connections.
27317	Correction done on the SNMP service working with the NFS storage.
29310	Correction done in the source interface field in Port Forwarding.
30693	Correction done in the access to the Virtual Office via Captive Portal.
30897	Correction done in the Captive Portal service after restoring a snapshot.
31156	Correction done in the display of Virtual Office profiles.
31404	Correction done when logging in without a profile match in the authentication portal.
31408	Correction done when displaying visitor logs in the authentication portal even when disabled.
31441	Correction done in the NGVPN HUB settings after restoring a backup.
31450	Correction done in the communication with the NGVPN's API.
31506	Correction done in the Radius sync with AD for Captive Portal authentication.
31650	Correction done in the packages' update during the NGVPN's upgrade process.
31816	Correction done in the Captive Portal logout when the user is configured in several rules.
31833	Correction done in the display of interfaces used in the Cluster's configuration.
33309	Correction done in the editing of nodes. UDP protocol was not being automatically checked.
33354	Correction done on the deletion of network interfaces.
33913	Correction done in the identification of IPv6 address objects.
33915	Correction done on the use of IPv4 objects without usage identification.
33917	Correction done in the High Availability service timing.
33918	Correction done in the DHCP Relay service to enter IPv6 servers through interface editing.
33933	Correction done in the database synchronization so that there is no replication of the MAC Address of the interfaces.
34126	Correction done in the object selection on the "Servers" field in DHCPv6 Relay.

34182	Correction done in the "rewizard" command.
34319	Correction done in the convergence of Backup to Master in the Cluster.
34361	Correction done to an English screen text.
34393	Correction done when uploading Port Forwarding rules.
34413	Correction done in the DHCPv6 service to configure more than one DHCP server.
34452	The display of encryption options in the site-to-site IPSec VPN has been corrected.
34457	Correction done in the wizard in browsers with languages other than those approved.
34659	Correction done in the Cluster audit, which was not displaying information on the "interfaces" field.
34811	Correction done in the selection of interfaces already in use for a new DHCP Relay configuration.
34839	Correction done on the screen refresh option after saving and applying settings in HA.
35226	Correction done when accessing the NGFW settings, while using a VDOM user.
35280	Correction done to the Cluster logs when disabling the service.
35294	Correction done on the Cluster synchronism failure.
35477	Correction done in the routine of the HA synchrony service.
35646	Correction done to add the eth apply in the HA service.
35743	Correction done when saving DHCP Server settings.
35813	Improvement done in the Web Filter which had a high memory consumption.
35846	Correction done in the backup machine's permitions to save and change not allowed options.
35943	Correction done to the DNS Content Filter redirection rules.
35985	The DNS Content Filter service has been optimized.
36011	Correction done in the tooltip search in the DNS Content Filter.
36068	Correction done in the database service's log file.
36080	Correction done in the authentication service to generate an apply when adding a new LDAP server.
36095	Correction done in the high CPU consumption by the DNS Content Filter service.
36119	Correction done on the Cluster's convergence after the primary device's crash.
36140	Correction done in the Cluster. Machines awaiting each other's status uppon convergence.
36231	Correction done in the DNS Content service to upload rules after the "fwreload" command.
36256	Correction done to a segfault in the Firewall service.
36322	Correction done when creating local users from AD and LDAP servers.
36368	Correction done in the synchrony of the backup device in the Cluster.
36405	Correction done in the presentation of the restore snapshot field, straight on the Wizard.
36448	Correction done in the DNS Content Filter profile name addition.
36506	Correction done on the backup server, which was uploading the wrong mask.
36508	Correction done in the DNS Server service.
36509	Correction done in the NGVPN packets' traffic.
36569	Correction done in the replication of the Cluster's network interfaces.
36849	Correction done in the antimalware service.
36851	Improvement done in the HA service when configuring the VIP interface.
36853	Correction done in the HA synchrony service.
36891	Correction done to problems in the co Cluster network.

37187	Correction done in the use of CA LOCAL after using an imported certificate.
37660	Correction done in the ping command using the Alias interface.
38206	Correction done on the creation process of an NGVPN profile.
38469	Correction done on the closing of Firewall processes.
38755	Correction done when generating CSV reports in logsessions.
38757	Correction done in the multiplication of eth records configured as input in the DNAT rule.
38758	Correction done in the option that blocks the editing of the Port Forwarding rules.
38789	Correction done in the filtering of the "debug-update -d" command.
38818	Correction done to the SMB, NFS and SSH storage lock settings.
38884	Correction done in the system not respecting disabled categories.
38899	Correction done on the profile creation and deletion processes in DNS Content Filter.
38906	Correction done when saving a new profile in DNS Content Filter.
39004	The TUN interface removal process has been optimized.
39057 **40616**	Improvement done in the DNS Content Filter audit logs.
39137	Correction done to the administrator profile permissions after update.
39236	Correction done in the DNS Content Filter profile using virtual interfaces.
39242	Correction done to the "debug-smtp-proxy" command via CLI.
39249	Improvement done in the visualization of user permissions to execute commands in the terminal via SSH Proxy.
39251	Correction done to the "ssh-proxy-sessions" command via CLI.
39296	Correction done in the PDF and CSV reports to match selected time period.
39502	Correction done in the DNS Content Filter rules after service disabling.
39609 **39629**	Correction done in the Port Forwarding rule editing.
39624	Improvement done in the saving of Port Forwarding settings.
39625	Correction done in the HA Cluster service execution when the secondary device is off.
39665	Correction done in the authenticated user session limit.
39715	A Security correction was done on the system settings' database.
39817	Improvement done on the fields' display in Port Forwarding.
40181	Correction done to static routes after HA Cluster convergence.
40274	Improvement done in the session timeout on the Captive Portal.
40558	Correction done in the Firewall ARP tables.
40749	Improvement done in the DNS Content Filter Rule after reboot.
40793	Improvement done in the Disk Log Partition.
41225	Correction done in the installation package during system update.
41446	Correction done to the NGFW ACL table synchronization.
41457	Correction done to the Cluster HA file synchronization.
41492	Improvements done to the mandatory field in the SSL Portal settings.
41753	Correction done on the MFA settings sync on HA Cluster devices.
41824	Improvement done in the NGVPN virtual interface presentation.

41857	Improvement done in the DHCP Relay service for VLAN interfaces.
41928	Correction done in the "Quarantine" window presentation and "Timeout" button in the IPS service configuration.
42321	Improvement done in the "debug-update" command logs.
42457	Improvement done to sync CA, user and service certificates on HA Cluster devices.
43649	Correction done in the access to blocked system configuration pages in the HA Cluster device.
44015	Correction done in the DNS Content Filter profile deletion.
44044	Correction done in the Zone Protection rule creation for NGVPN service after update.
44257	Correction done in the device license editing on the HA Cluster.
44276	Correction done in the PFS Group field in the IPSec VPN service settings.
44703	Correction done in the duplicate profiles and LDAP servers.
44851	Improvement done in the Support for IPv4 and IPv6 Protocols in DHCP Server Settings.
44872	Correction done on the listing of local and remote Windows AD users.
45385	Correction done in the duplicate IPs in DHCP + Auth Radius service table.
45616	Improvement done in the user field in NGVPN HUB configuration.
46414	Correction done on the services execution after remote CA import.
46486	Correction done in the IPSec VPN form to disallow the use of double quotes in the Shared Key field.
46531	Improvement done in the (MFA) Multi-Factor Authentication.
46757	Improvement in the HA Cluster process startup with the service disabled.
46817	Correction done on the creation of new NGVPN HUBs.
46918	Correction done in the IPSec VPN service startup.
47270	Correction done to access the system configuration menus.
47608	Improvement and optimization done in the PPPoE link processes.
47938	Correction done in the application of the TUN interface configuration on HA Cluster devices.
48040	Correction done in the CSV reports of authentication and VPN logs.
48457	Correction done in the TUN interface status after HA Cluster sync.
49148	Correction done in the data presentation on Dashboard widgets.
49234	Correction done in the Port Forwarding rule application using PPPoE links.
50242	Correction done to the addition of network interfaces in system route configuration.

Previous Versions:

Blockbit NGFW version 2.4.0

Blockbit NGFW version 2.3.0

Blockbit NGFW version 2.2.2

Blockbit NGFW version 2.2.1

Blockbit NGFW version 2.2.0

Blockbit NGFW version 2.1.1

Blockbit NGFW version 2.1.0

Blockbit NGFW version 2.0.13

Blockbit NGFW version 2.0.12

Blockbit NGFW version 2.0.11

Blockbit NGFW version 2.0.10

Return

Blockbit NGFW Version 2.4.2

Release notes

24/09/2024

To ensure a safer and more efficient operation, version 2.4.2 of Blockbit NGFW includes various bug fixes, providing a superior experience for our customers. We are constantly monitoring and improving our systems to meet market needs.

Below is a list of the main elements that have been fixed in version 2.4.2 of Blockbit NGFW, focusing on enhancing security, performance, and functionality:

Authentication and Permissions

- Fixed permission image for rules and authentication (61119)
- Fixed authentication settings (61133)
- Fixed DNAT policy authentication (59944)
- Fixed user authentication (60075)

Services and Features

- Fixed authentication service after cluster convergence (63789)
- Fixed cluster service (63597, 39625)
- Fixed high availability service (58171)
- Fixed SD-WAN service (48281)
- Fixed Virtual Office (48473)

Configurations and Interfaces

- Fixed local user creation (44872)
- Fixed threat protection configuration (43441)
- Fixed encryption menu settings (60467)
- Fixed network mask validation (47622)

Logs and Monitoring

- Fixed logging system (40793, 63598)
- Fixed Log Session report generation (56363, 56520)

Protocols and Connections

- Fixed DHCP issues (44063, 34808)
- Fixed IPSEC VPN (46918, 62871)
- Fixed DNS Content Filter (39236, 36441)
- Fixed cluster trigger (43649)

Performance Issues

- Fixed refresh error causing excessive CPU consumption (39793)
- Fixed error leading to high resource usage (33991)
- Fixed memory usage issues (36816)

Backup and Replication

- Fixed centralized backup (42016)
- Fixed MTU parameter replication on backup server (60133)
- Fixed certificate replication issues (43436)

User Interface and Experience

- Fixed NGFW home screen after first synchronization (38497)
- Fixed messages in the graphical interface (38941)
- Fixed navigation in unsupported languages (34457)

Blockbit NGFW version 2.4.1

Release Notes

21/11/2023

Several features have been implemented in the release of Blockbit NGFW 2.4.1:

- **Implemented DNS Content Filtering support.**
- **The Cluster's operation in HA has been optimized.**
- **The option to remove DHCP leases has been implemented.**
- **The Firewall settings received performance optimization options (tunning).**
- **The Web Filter settings received performance optimization options (tunning).**
- **Implemented Wi-Fi support and network interface configuration screen.**
- **The IPSec VPN now supports Multi-Factor Authentication (MFA).**
- **DH groups 31 and 32 were implemented in the IPSec VPN - Remote Access encryption.**

The following table lists the improvements and Correctiones done in the release of the Blockbit NGFW 2.4.1:

Code	Description
8000	Correction done in the Web Filter error logs.
19901	Correction done in the analysis of Samples in the Sandbox.
24158	Correction done in Threat Protection Quarantine service.
25158	Correction done in the SD-WAN service not to remove packets tags.
26040	Correction done in Firewall Segfault errors.
26920	Correction done on IPS profiles in Port Forwarding rules which were blocking connections.
27317	Correction done on the SNMP service working with the NFS storage.
29310	Correction done in the source interface field in Port Forwarding.
30693	Correction done in the access to the Virtual Office via Captive Portal.
30897	Correction done in the Captive Portal service after restoring a snapshot.
31156	Correction done in the display of Virtual Office profiles.
31404	Correction done when logging in without a profile match in the authentication portal.
31408	Correction done when displaying visitor logs in the authentication portal even when disabled.
31441	Correction done in the NGVPN HUB settings after restoring a backup.
31450	Correction done in the communication with the NGVPN's API.
31506	Correction done in the Radius sync with AD for Captive Portal authentication.
31650	Correction done in the packages' update during the NGVPN's upgrade process.
31816	Correction done in the Captive Portal logout when the user is configured in several rules.
31833	Correction done in the display of interfaces used in the Cluster's configuration.
33309	Correction done in the editing of nodes. UDP protocol was not being automatically checked.
33354	Correction done on the deletion of network interfaces.
33913	Correction done in the identification of IPv6 address objects.
33915	Correction done on the use of IPv4 objects without usage identification.
33917	Correction done in the High Availability service timing.
33918	Correction done in the DHCP Relay service to enter IPv6 servers through interface editing.
33933	Correction done in the database synchronization so that there is no replication of the MAC Address of the interfaces.
34126	Correction done in the object selection on the "Servers" field in DHCPv6 Relay.

34182	Correction done in the "rewizard" command.
34319	Correction done in the convergence of Backup to Master in the Cluster.
34361	Correction done to an English screen text.
34393	Correction done when uploading Port Forwarding rules.
34413	Correction done in the DHCPv6 service to configure more than one DHCP server.
34452	The display of encryption options in the site-to-site IPSec VPN has been corrected.
34457	Correction done in the wizard in browsers with languages other than those approved.
34659	Correction done in the Cluster audit, which was not displaying information on the "interfaces" field.
34811	Correction done in the selection of interfaces already in use for a new DHCP Relay configuration.
34839	Correction done on the screen refresh option after saving and applying settings in HA.
35226	Correction done when accessing the NGFW settings, while using a VDOM user.
35280	Correction done to the Cluster logs when disabling the service.
35294	Correction done on the Cluster synchronism failure.
35477	Correction done in the routine of the HA synchrony service.
35646	Correction done to add the eth apply in the HA service.
35743	Correction done when saving DHCP Server settings.
35813	Improvement done in the Web Filter which had a high memory consumption.
35846	Correction done in the backup machine's permitions to save and change not allowed options.
35943	Correction done to the DNS Content Filter redirection rules.
35985	The DNS Content Filter service has been optimized.
36011	Correction done in the tooltip search in the DNS Content Filter.
36068	Correction done in the database service's log file.
36080	Correction done in the authentication service to generate an apply when adding a new LDAP server.
36095	Correction done in the high CPU consumption by the DNS Content Filter service.
36119	Correction done on the Cluster's convergence after the primary device's crash.
36140	Correction done in the Cluster. Machines awaiting each other's status uppon convergence.
36231	Correction done in the DNS Content service to upload rules after the "fwreload" command.
36256	Correction done to a segfault in the Firewall service.
36322	Correction done when creating local users from AD and LDAP servers.
36368	Correction done in the synchrony of the backup device in the Cluster.
36405	Correction done in the presentation of the restore snapshot field, straight on the Wizard.
36448	Correction done in the DNS Content Filter profile name addition.
36506	Correction done on the backup server, which was uploading the wrong mask.
36508	Correction done in the DNS Server service.
36509	Correction done in the NGVPN packets' traffic.
36569	Correction done in the replication of the Cluster's network interfaces.
36849	Correction done in the antimalware service.
36851	Improvement done in the HA service when configuring the VIP interface.
36853	Correction done in the HA synchrony service.
36891	Correction done to problems in the co Cluster network.

37187	Correction done in the use of CA LOCAL after using an imported certificate.
37660	Correction done in the ping command using the Alias interface.
38206	Correction done on the creation process of an NGVPN profile.
38469	Correction done on the closing of Firewall processes.
38755	Correction done when generating CSV reports in logsessions.
38757	Correction done in the multiplication of eth records configured as input in the DNAT rule.
38758	Correction done in the option that blocks the editing of the Port Forwarding rules.
38789	Correction done in the filtering of the "debug-update -d" command.
38818	Correction done to the SMB, NFS and SSH storage lock settings.
38884	Correction done in the system not respecting disabled categories.
38899	Correction done on the profile creation and deletion processes in DNS Content Filter.
38906	Correction done when saving a new profile in DNS Content Filter.
39004	The TUN interface removal process has been optimized.
39057 **40616**	Improvement done in the DNS Content Filter audit logs.
39137	Correction done to the administrator profile permissions after update.
39236	Correction done in the DNS Content Filter profile using virtual interfaces.
39242	Correction done to the "debug-smtp-proxy" command via CLI.
39249	Improvement done in the visualization of user permissions to execute commands in the terminal via SSH Proxy.
39251	Correction done to the "ssh-proxy-sessions" command via CLI.
39296	Correction done in the PDF and CSV reports to match selected time period.
39502	Correction done in the DNS Content Filter rules after service disabling.
39609 **39629**	Correction done in the Port Forwarding rule editing.
39624	Improvement done in the saving of Port Forwarding settings.
39625	Correction done in the HA Cluster service execution when the secondary device is off.
39665	Correction done in the authenticated user session limit.
39715	A Security correction was done on the system settings' database.
39817	Improvement done on the fields' display in Port Forwarding.
40181	Correction done to static routes after HA Cluster convergence.
40274	Improvement done in the session timeout on the Captive Portal.
40558	Correction done in the Firewall ARP tables.
40749	Improvement done in the DNS Content Filter Rule after reboot.
40793	Improvement done in the Disk Log Partition.
41225	Correction done in the installation package during system update.
41446	Correction done to the NGFW ACL table synchronization.
41457	Correction done to the Cluster HA file synchronization.
41492	Improvements done to the mandatory field in the SSL Portal settings.
41753	Correction done on the MFA settings sync on HA Cluster devices.
41824	Improvement done in the NGVPN virtual interface presentation.

41857	Improvement done in the DHCP Relay service for VLAN interfaces.
41928	Correction done in the "Quarantine" window presentation and "Timeout" button in the IPS service configuration.
42321	Improvement done in the "debug-update" command logs.
42457	Improvement done to sync CA, user and service certificates on HA Cluster devices.
43649	Correction done in the access to blocked system configuration pages in the HA Cluster device.
44015	Correction done in the DNS Content Filter profile deletion.
44044	Correction done in the Zone Protection rule creation for NGVPN service after update.
44257	Correction done in the device license editing on the HA Cluster.
44276	Correction done in the PFS Group field in the IPSec VPN service settings.
44703	Correction done in the duplicate profiles and LDAP servers.
44851	Improvement done in the Support for IPv4 and IPv6 Protocols in DHCP Server Settings.
44872	Correction done on the listing of local and remote Windows AD users.
45385	Correction done in the duplicate IPs in DHCP + Auth Radius service table.
45616	Improvement done in the user field in NGVPN HUB configuration.
46414	Correction done on the services execution after remote CA import.
46486	Correction done in the IPSec VPN form to disallow the use of double quotes in the Shared Key field.
46531	Improvement done in the (MFA) Multi-Factor Authentication.
46757	Improvement in the HA Cluster process startup with the service disabled.
46817	Correction done on the creation of new NGVPN HUBs.
46918	Correction done in the IPSec VPN service startup.
47270	Correction done to access the system configuration menus.
47608	Improvement and optimization done in the PPPoE link processes.
47938	Correction done in the application of the TUN interface configuration on HA Cluster devices.
48040	Correction done in the CSV reports of authentication and VPN logs.
48457	Correction done in the TUN interface status after HA Cluster sync.
49148	Correction done in the data presentation on Dashboard widgets.
49234	Correction done in the Port Forwarding rule application using PPPoE links.
50242	Correction done to the addition of network interfaces in system route configuration.

Blockbit NGFW version 2.4.0

Release Notes

27/02/2023

Several features have been implemented in the release of Blockbit NGFW 2.4.0:

- **Support to DNAT (Many-to Many) has been implemented in Port Forwarding.**
- **The monitoring of logs has been implemented in CGNAT > Live Sessions.**
- **Support to CGNAT (Carrier Grade Network Address Translator) has been implemented.**
- **Support for 2 more servers in the LDAP and Windows AD authentication for fail safe has been implemented.**
- **The Hotfix and Patch feature has been implemented.**
- **A widget that displays the CPU's temperature in physical appliances has been implemented.**
- **Improvement done in the Upgrade/Update process with H.A enabled.**
- **Commands for the restart/reboot of the NGFW/Services/Network interfaces have been implemented.**
- **Support to Web adm access via HTTP has been implemented.**
- **Implemented support to Snapshot restore without wizard.**
- **The option to send reports generated by the analyzer via e-mail has been implemented.**
- **Local and AD (Windows Active Directory) authentication have been implemented in the NG VPN Client.**
- **Log and report of browsing time on domains/websites.**
- **MFA with Google Authentication integration**
- **New Next Generation VPN service implemented**
- **New version of Captive Portal.**
- **Implemented functionality for Proxy SSH.**
- **Support for DHCP Relay IPv6 implemented.**

The following table lists the improvements and fixes done in the release of the Blockbit NGFW 2.4.0:

Code	Description
1357	Correction done in the browsing via NAT with a PPPoE link.
1366	Improvement done in the Provisioning Service.
1384	Improvement done in policies using Geolocation blockage.
4303	Correction done to the display of the Gateway column using IPv6.
4681	Correction done when mapping the IPv6 addresses in NAT 64 and 46.
4686	Correction done in the Firewall logs using IPv6 connections.
4871	Correction done in the generation of the Apply option when editing an object related to an IPv6 Policy.
5021	Correction done in the session timeout in simultaneous sessions in port 9803.
5100	Correction done in the displayed message after editing a network interface.
5114	Correction done in the Port Forwarding rule after PPPoE link down.
5115	Correction done in the ratemask default value.
5116	Correction done when opening CSV files in Excel.
8955	Correction done in the secondary device which enabled LAG interfaces' IPs when syncing.
9927	Correction done in the toogle function of the main menu, now being displayed correctly in smaller resolutions.
10920	Correction done in DSL interfaces' settings.
13676	Improvement done in the creation and configuration of parameters in the Database, by the Wizard.
13691	Correction done in the displayed message in Max Connections, in Services > Firewall > General Settings.
13765	Correction made in Antimalware services.
14229	SSH vulnerability properly eliminated.
14306	Correction done in the "WMI Authentication" field text. Settings > Authentication > Servers > Windows > WMI Authentication
14375	AV disabled in Threat Protection profiles.

14716	Correction done when reseting a password via Captive Portal.
14824	Improvement done in the display of Web Filter, SSL, Proxy, SD-WAN and IPv4 Policies debug logs.
15056	Correction done in the SSL Inspection when using a dictionary object.
15671	Correction done in the DHCP Server services with IPv6.
15811	Correction done in the licensing process in case the server is down.
18267	Correction done when generating Analyzer reports in PDF.
18285	Improvement done in the imported Policies's apply from a Policy package.
18830	Correction done when displaying specific dates' logs, in Monitor > Security Events > Query Editor > Date.
18894	Correction made when loading Port Forwarding rules.
19080	Improvement in the editing of VPN tunnels.
19666	Changes in the ARP Reply response
19699	Improvement done in the password recovery process in the Captive Portal.
19802	Correction done in the 'speedtest' command.
19884	Correction done in the antimalware.scanner using Sandbox.
20715	Correction done in the false positives of SD-WAN when applying settings.
20730	Correction done in Web Filter Top Categories' search box in the NGFW.
20963	Improvement done in the WMI authentication.
21760	Correction done in the session timeout while clients are browsing.
22036	Improvement done so the LOAD doesn't get to high.
22074	Correction done in the License Server.
23016	Correction done in DNS service.
23430	Correction done in Services > DHCP > Relay.
23503	Correction done in the warning notice displayed on the in IPv4 Policy screen, in the Advanced tab.
23646	Improvement done in the applyes execution.
23959	The Blockbit Unified Threat Manager (UTM) has been renamed to Blockbit Next Generation Firewall (NGFW).
23981	Correction done in the Profile Portal settings in the Captive Portal.
24141	Correction done in the Reports' scheduling, in Monitor.
24238	Improvement done in the forwarding between stations with IPv6.
24706	Correction done in the user certificate download.
24724	Improvement done in the browser validation using Authentication certificates.
24741	Correction done in the Captive Portal authentication using created user + domain.
25098	Correction done when removing network interfaces.
25147	Correction done to the Captive Portal access through a different configured interface in the NGFW.
25148	Correction done in the API page.
25158	Correction done in the SD-WAN service.
25455	Correction done in the Captive Portal to create a VPN SSL - Portal profile.
25457	Correction done to the Captive Portal's access page.
25533	Correction done in the H.A. settings.
26164	Security correction done when disabling TLSv1.0 e 1.1 on port 9803
26972	Correction done in the functioning of the Quarantine's database, in Services > ATP > Quarantine.

27074	Correction done to the VPN IPSec debug commands, and in the informations displayed in Live Sessions.
27837	Improvement done in the option of remotely logging out another NGFW's session.
28283	Improvement done in registration of new users allowing now, the usage of dots (.)
28362	Correction done to the Captive Portal access after rebooting or updating to another version.
28571	Correction done to not loose access after Wizard.
28585	Correction done in the bandwidth indicators after new settings.
28596	Correction done when showing doubled number os sessions.
28657	Correction done in the Proxy HTTP apply.
28660	Correction done in the passwor reset on Captive Portal.
29052	Correction done when accessing Captive Portal through Mozilla Firefox browser.
29087	Correction done when creating hubs using the same name in the VPN NG.
29149	Correction done on IPs redirection in Port Forwarding.
29310	Correction done em interface de origem vazia em Port Forwarding after update.
29452	Correction done on Captive Portal when using a domain which is not the default.
29611	Correction done in the unavailability of API service on NG VPN.
29614	Correction done in the NG VPN Server service.
29715	Improvement in the password service usage on NG VPN Server.
30071	Correction done in the 'Allow Table' table.
30097	Improvement done in the Captive Portal login.
30115	Correction done in the DHCP Relay service.
30212	Correction done when enabling and setting up the Proxy service.
30693	Correction done in the Virtual Offive access via Captive Portal.
30873	Correction done in the Port Forwarding table.
30897	Correction done in the Captive Portal access after a snapshot *restore*.
30947	Correction done in the NG VPN authentication.
30965	Correction done in the Application Control base after version upgrade.
31156	Correction done in the Virtual Office profile display.
31403	Correction done when setting up the TCP MSS in policies.
31404	Correction done in logins without 'match' in the Authentication Portal.
31408	Correction done when displaying the visitor record in the Authentication Portal even when desabled.
31441	Correction done in the settings of HUB in the NG VPN after backup *restore*.
31450	Correction done in the communication with the API of NG VPN.
31816	Correction done when login out on Captive Portal when the user is set up in several policies.
32411	Improvement done in the Authetication service monitor.
33756	Correction done in the CSV reports.
33913	Correction done in the indication of usage of IPv6 address objects.
33918	Correction done in the DHCP Relay, allowing the IPv6 usage.
34126	Correction done in the DHCPv6 Relay field, not allowing object duplicity.
34413	Correction done in the DHCPv6 service to set up multiple servers.

Blockbit NGFW version 2.3.0

Release Notes

31/10/2022

Several features have been implemented in the Blockbit NGFW 2.3.0:

- **The ATP Sandbox functionality has been implemented.**
- **The Virtual Domains (VDOM) functionality has been implemented.**
- **The dynamic objects functionality has been implemented in Addresses, Services and Dictionaries.**
- **Support to the batch importation of CSVs, in Static Addresses has been implemented in the DHCP Settings.**
- **SSH Access to CLI via Telnet has been implemented.**
- **The commands for activating and deactivating IPSec VPN Tunnels have been created.**
- **The monitoring of SDWAN links by IPv6 has been implemented.**
- **Support to packet duplication has been implemented in both SDWAN and Advanced Routing modules.**
- **The Blockbit IPSec VPN to CISCO integration via XAuth Authentication has been added.**
- **Suport to the import of Root Certificates to the Proxy's SSL Inspection module has been implemented.**
- **The recurrent reports feature has been implemented.**
- **A new function has been implemented to check and validate Firewall Policies.**
- **The support to data packets capture (PCAP) by IPS signature has been implemented.**
- **Support to creation, editing and import of signatures to the IPS has been implemented.**
- **Support for the VPN IPSec with Google cloud VPN has been implemented.**
- **The sending of license expiring notifications has been implemented.**
- **Web Filter monitoring, enabling the obtention of information on the flow of users has been implemented.**
- **Support to Root Certificates by profile, for the Web Filter's SSL Inspection module.**
- **Support to Heartbeat #3 has been implemented on High Availability.**
- **The minute insertion field in Sync Interval, H.A, has been standardized.**
- **The parameters of the Failover VPN configuration have been detailed.**
- **The max timeout field has been realocated in the Firewall settings.**
- **The Next Generation VPN has been released.**
- **The creation of NGVPN Hubs via configuration forms has been implemented.**
- **AD and Local authentication have been implemented in the NGVPN server.**

The following table lists the improvements and fixes done in the Blockbit NGFW 2.3.0:

Code	Description
UTM-293	Improvement done in the Captive Portal's authentication.
UTM-3277	Improvement done in the classification of IPv4 and IPv6 policies in the system's audit screen.
UTM-3740	The possibility of filtering logs by networks has been implemented in "Security Events". Ex: Use the expression 172.25.0.% (it filters the 172.25.0.0-172.25.0.255 range).
UTM-4169	Improvement done in the naming of "Time" and "Content" objects.
UTM-4175	Improvement done in the Failover service of the VPN IPSec.
UTM-4190	Improvement done in the redirectiong after drop/return of the PPPoE link.
T1-1431	Improvement done in the ETH settings when creating a Device, in the Provisioning tab.
T1-1584	Correction done in the system that sends access reports via e-mail.
T1-1812	Improvement done in the appliances' licencing (license and UUID).
T1-2150	Correction done in the IPv4 and IPv6 policies' editing/creation and deletion.
T1-2350	Correction done in the UTM main screen's display adjust button.
T2-115	Improvement done in the cluster's activation with the Firewall working.
T2-1090	The import of static addresses in batches (CSV) in the DHCP's window.
T2-1605	Improvement done in the checksum verification in TUN interfaces.
T2-2061	Improvement done in the characters insertion in Captive Portal, Social Login.

T2-2147	Improvement done in the authentication service.
T2-2149	Improvement done in the memory allocation and reading of the Firewall, Monitor and Anti-malware services.
T3-282	Improvement done in the SDWAN profiles' configuration.
T3-362	Improvement done in the creation of Intrusion Prevention Profiles with the PCAP option.
T3-565	Correction done in the Node connection service.
T3-579	Improvement done in the signature search filters in Intrusion Prevention – PCAP and in the fields in Device.
T3-619	Improvement done in the data saving of SSL Profiles, in Proxy > SSL Inspection > Create Profile.
T4-15	Improvement done in the VPN tunnels' settings.
T4-89	Improvement done in the Live virtual networks' stability in Live Sessions, via virtual tunnels.
T4-140	Improvement done in the application of IPv4 Policies in the communication between local and remote networks.
T4-272	Improvement done in the importation of models of CSV files when importing static Ips lists, in Services > DHCP > Static IP options > Import > Download model.
T4-457	Improvement done in the saving of Heartbeat settings.
T4-462	Improvement done in the VDOM's icon.
T4-514	Improvement done in the version displayed in IPv4 and IPv6 Policies.
T4-657	Improvement done in the rules deletion of the firewall, when closing a session.
SUS-8	Improvement done in the Provisioning service.
SUS-18	Improvement done in the display of users that have been imported with CSV lists.
SUS-62	Correction done in the Web Filter's layout when moving profiles.
SUS-66	Improvement done in the timetable display in the Security Events' forms.
SUS-73	Improvement done in the approval presentation display of batch ZTP.
SUS-87	Improvement done in the system's backup restoration.
SUS-115	Improvement done in the settings saving in Zone Protection's Device Templates.
SUS-129	Improvement done in the Threat Protection reports display in Dashboard, Events.
SUS-298	Improvement done in the application of Policy blocks by Geolocation.
SUS-307	The "Blacklist" and "Whitelist" field namings were changed to "Denied Addresses" e "Allowed Addresses" respectively, in Intrusion Prevention.
SUS-319	Correction done in the version displayed after upgrade.
SUS-327	Correction done in the message displayed when changing the synchronization mode in System > Authentication > Synchronism.
SUS-330	Correction done in the connection to the PHP Bank.
5161	Improvement done in the users sessions display from headquarters to branches.
5219	Improvement done in the Policies deploy using App Control, IPS, ATP, Web Filter and SSL Inspection profiles.
5221	Improvement done in the functioning of Zone Protection clonned rules.
8510	Improvement done in the CSV reports generation, in Monitor > Reports.
8669	Improvement done in the IPv4 Policies' permissions.
10009	Improvement done in the creation of Policy packages.
10116	Improvement done in the functioning of Firewall with active clusters.
10137	Improvement done in the functioning of the IPS Filter.
10275	Correction done in the script of Policy packages deploy.
10907	Improvement done in the application of IPv4 Policy packages to packets from remote networks.
11208	Correction done in the cloning of Policies.

11948	Correction done in the time insertion field in renewal time in Services > DHCP > Server.
11655	Improvement done in the IPSec VPN's Failover.
12583	Correction done in the Firewall options display.
12610	Improvement done in the apply of ATP update script.
12785	Improvement done in the "File Prefix" field naming in Services > Intrusion Prevention > Create Profile > Settings.
12852	Improvement done in the information displayed in the Threat Protection's Audit Logs.
13573	Correction done in the password exchange/recovery via portal.
13711	Correction done in the Sandbox's process of samples analysis.
14229	A vulnerability of medium level has been eliminated from the SSH.
14575	Improvement done in the functioning of the instalation Wizard.
14605 **14794**	Improvement done in the administrator's settings of the Sandbox.
14649	Correction done in the display of the Traffic Monitor option in VDOM.
14650	Improvement done in the Event Logs generation in VDOM.
14823	Improvement done int he verification of links downloaded to the Sandbox.
14899	Improvement done in the display of Device Templates already configured in the provisioning list.
14900	Improvement done in the deploy of Policy Packages.
15138	Improvement done in the editing of IPv4 rules after the NGFW's upgrade.
15671	Improvement done in the functioning of the IPv6's DHCP server.
18225	Improvement done in the clone function of Device Templates.
18285	Improvement done in the application of policies that have been imported from a Policy Package.
18286	Improvement done in the access to UTMs bound in Device's inventory via Monitor.
18830	Improvement done in the generation of Logs in Security Events, in Monitor > Security Events > Query Editor > Date.
19884	Improvement done in the Antimalware service of the SandBox.
19901	Correction done in the samples analysis done by the SandBox.
19929	Improvement done in the use of TCP MSS in NAT Policies.

Blockbit UTM version 2.2.2

Release Notes

02/08/2022

- **WMI SSO integration to multiple Active Directory has been implemented.**
- **Support to the batch importation of CSVs, in Static Addresses has been implemented in the DHCP Settings.**
- **DNAT rules can now be created while the key is disabled.**

The following table lists the improvements and fixes done in the release of the Blockbit UTM 2.2.2:

Code	Description
T1-82	Improvement done in the ordination of the Application Control's base.
T1-232	Improvement done in the editing of interfaces with registered Policies.
T1-235	Improvement done in the SSL Inspection.
T1-271	Improvement done in the IPSec VPN's tunnel stablishment.
T1-287	Correction done in the license key reaplication.
T1-292	Improvement done in the update settings via proxy server.
T1-462	An update has been done in the Open SSL.
T1-464	An update has been done in the Proxy SSL.
T1-660	Support to TLS 1.3 protocol inspection has been included, in SSL Inspection.
T1-767 **T1-777**	Improvement done in the functioning of the RADIUS authentication service.
T1-869	Improvement done in the VPN IPSec Site to Site's communication, with Firewall rules.
T1-915	The IPSec VPN has been updated.
T1-932	Correction done in the Query Filters' filters, in Security Events.
T1-1055	Improvement done in the VPN Monitor (VPN SSL) service's settings.
T1-1056	Correction done in the VPN Monitor (Segfault).
T1-1127	Improvement done in the creation od DNAT rules with enabled key, in Services > Firewall > Port Forwarding > Create DNAT rule.
T1-1147	Improvement done in the SDWAN's Load Balance profile.
T1-1161	Improvement done in the ETH network interfaces' setup, after provisioning.
T1-1193	Correction done in the App filter in Application Control.
T1-1221	Improvement done in the upgrade scripts.
T1-1265	Improvement done in the ETH interfaces setup, with active DNAT rules.
T1-1277	Correction done in the information contained in the settings file in VPN IPSec.
T1-1295	Improvement done in the physical interface's settings.
T1-1320	Improvement done in the sending of e-mails by the License.
T1-1326	Improvement done in the Full Mesh IPSec VPN's routes.
T1-1364	Improvement done in the IPSec VPN's settings screen
T1-1410	Improvement done in the CSV reports creation.
T1-1423	Improvement done in the CSV and PDF Reports storing, in Monitor.
T1-1463	Improvement done in the interfaces settings with policies using SNAT.
T1-1530	Improvement done in the creation of network interfaces with IPv4 Policies.

T1-1884	Correction done in the use of language displayed in the UTM’s interface.
T1-1959	Improvement done in the application of the VPN IPSec Site to Site version IKEv1’s settings.
T1-2076	Improvement done in the Strongswan’s Policies.
T1-2351	Correction done in the REDIS' connection in the Firewall, Reporter and VPN Monitor services.
T1-2440	Correction done in the access to HTTPS sites with SSL Inspection and block to non-categorized sites activated.
T2-150	Improvement done in the DNAT rules.
T2-287	The Proxy HTTP service has been updated.
T2-316	Improvement done in the creation of network tunnel interfaces.
T2-597	Improvement done in the users registration in Policy packages.
T2-810	Improvement done in the cache service’s memory allocation.
T2-820	Improvement done in the synchrony between master and slave, in High Availability.
T2-916	Improvement done in the characters insertion in the “Login” and “Name” fields when creating a user.
T2-964	Improvement done in the loading of files required for the cache to work in full capacity.
T2-1004	Improvement done in the network interface’s stability.
T2-1040	Improvement done in the Log rotate’s functioning.
T2-1198	The fwreload command has been normalized in the UTM’s script.
T2-1209	Improvement done in the Virtual Office’s redirecting with the Firewall active.
T2-1292	Correction done in the Auth-portal’s redirecting.
T2-1372	Correction done in the characters insertion field in the name field, in Settings > Certificates > Services.
T2-1398	Improvement done in the UTM’s interface after the Windows Server setup.
T2-1767	Improvement done in the creation of DNAT rules with enabled key.
T2-1907 **T3-291**	Improvement done in the Update scripts’ applies.
T2-2136	Correction done in the Malware release for download, in Monitor > Malware Quarantine.
T3-326	Improvement done in the network sync time in the High Availability.
T4-55	Correction done in the time displayed in the CSV reports, in monitor > Reports.
SUS-7	Improvement done in the deletion process of SSL Inspection profiles.
SUS-100 **5307**	Improvement done in the network interfaces display after provisioning.
SUS-395	Correction done in the IPv4 Policies, Zone Protection and Port Forwarding authentication.
1697	Improvement done in Port Forwarding, Zone Protection and IPv4 Policies.
5248	Improvement done in the Firewall settings application.
12611	Improvement done in the application of Web Filter, Políticas and Firewall settings.
14149	Improvement done in the behavior of DNAT rules in Port Forwarding.
14759	Improvement done in the VPN IPSec's compatibility with QAT.
14824	Correction done in the "debug-webfilter's" Logs.
15056	Improvement done in the application of Objects' rules with active Web Filter and SSL Inspection profiles.

Blockbit UTM version 2.2.1

Release Notes

30/05/2022

Several features have been implemented in the release of Blockbit UTM 2.2.1:

- Improvement done in the DHCP + RADIUS compatibility.
- Improvement done in the VPN IPSEC Site to Site general settings.
- Improvement done in the SSL VPN settings application in Web Portal.
- Improvement done in the communication between two Networks via site-to-site VPN in the same subnet.
- Cluster monitoring via CLI and SNMP has been implemented.

The following table lists the improvements and fixes done in the release of the Blockbit UTM 2.2.1:

Code	Description
T1-86	Correction done in the VPN user up time display.
T1-283	Correction done in the naming of the “Allowed” and “Blocked” fields, in Firewall > Port Forwarding.
T1-284	Improvement done in the license validation.
T1-637	Improvement done in the creation of policies’ deploy.
T1-667	Improvement done in the editing of information in RADIUS domain.
T1-715	Improvement done in the RADIUS’ DHCP IP attribution.
T1-828	Correction done in the time displayed in the IPSEC VPN’s reports.
T1-1057	Improvement done in the deploy of Device Templates between a UTM and a GSM.
T1-1118	Improvement done in the DNAT Port Forwarding’s stability when virtual interfaces are created.
T1-1120	Improvement done in the daily licensing validation via Keepalive.
T1-1131	Improvement done in the update settings.
T1-1221	Improvement done in the update script.
T1-1295	Improvement done in the physical interface’s settings.
T2-106	Correction done in the backup system with High Availability on.
T2-110	Improvement done in the Synchrony between UTMs in cluster with different hardware.
T2-316	Correction done in the creation of TUN interfaces for GRE tunnels.
T2-597	Correction done in the edition of users in NAT Policies.
T2-612	Correction done in the explicit Proxy functioning.
T2-648	Improvement done in the Network interface’s settings.
T2-742	Correction done in the Logs’ management by the REDIS.
T2-743 **T2-745**	Optimization done in the CPU consumption by Firewall and explicit Proxy.
T2-883	Improvement done in the functioning of SD-WAN Policies and Profiles.
T2-938	Improvement done in the Dynamic Remote Host of the IPSEC VPN.
T2-992	Optimization done in the reply time of consults in the WMI service.
T2-1372	Correction done in the name field in Imported Service Certificate.

Blockbit UTM version 2.2.0

Release Notes

22/09/2021

Several features have been implemented in the release of Blockbit UTM 2.2.0:

- **RADIUS authentication system via DHCP has been implemented.**
- **Support to Syslog via TLS has been implemented.**
- **A denied access screen in case of user without permission to login in the identity provider server has been created.**
- **Whitelist for access to management interface has been implemented in Access Control.**
- **Support to *IEEE 802.1Q standard* VLAN has been implemented.**
- **Support to the Spanish language has been implemented.**
- **SSO authentication solution for multiple UTMs has been implemented.**
- **"debug-provisioning" command that shows the ZTP log has been implemented.**
- **Optimization has been done in the logs processing and traffic summarization.**
- **A function for displaying the build through the "keepalive" has been implemented in the license.**
- **License data detailing has been implemented in the "show-license" command.**
- **A sheet by Zone and Geolocation has been implemented in Port Forwarding.**
- **Single Sign On (SSO) authentication method via WMI has been implemented.**
- **WMI debug log has been implemented.**

The following table lists the improvements and fixes done in the release of the Blockbit UTM 2.2.0:

Code	Description
T1-9	Improvement done in the server domain authentication.
T1-66	Improvement done in the CSV reports generation.
T1-158	Improvement done in the value selection in the Web cache setup, in Web filter.
T1-188	Improvement done in the users' authentication in policies > Firewall.
T1-202	Improvement done in the Applications routing through the SDWAN.
T1-203	Improvement done in the SDWAN's Load balance.
T1-204 **T2-350**	Improvement done in the Port Forwarding connections display in Live Sessions.
T1-211	Improvement done in the validation of the VPN SSL fields.
T1-212	Improvement done in the validation of the VPN IPSEC fields.
T1-213	Improvement done in the RADIUS server settings fields, in Settings > Authentication > Servers > RADIUS.
T1-259	Correction done in the Web filter's policies authentication, in Services > Web Cache > Hierarchy.
T1-270	Correction done in the message display when creating Device Templates.
T1-282	Improvement done in the HTTPD service activation.
T1-292	Improvement done in the update validation through the Proxy server.
T1-355	Correction done in the message displayed when displaying the Traffic Monitor, in Firewall > Zone Protection > Policy editing.
T1-364	Improvement done in the DNAT Policies loading.
T1-366	Improvement done in the rule setup and port redirecting.
T1-381	Improvement done in the Zone Protection Logs in the Security Events window.
T1-393	Improvement done in the Firewall Policies application in Port Forwarding connections.
T1-419	Improvement done in the automatic selection of the Traffic Monitor and Traffic Logging options.
T1-420	Correction done in the maximum number of packets in the DoS rule.

T1-424	Correction done in the DNAT rule application in secondary links.
T1-439	Improvement done in the validation of the setup fields of the SSL VPN.
T1-443	Improvement done in the validation of the setup fields of the SSL VPN.
T1-449	Improvement done in the Port Forwarding connections display in Live Sessions.
T1-453	Improvement done in the message displayed when editing a policy in Zone Protection.
T1-524 **T2-418**	Improvement done in the displayed connection information in Live Sessions.
T1-526	Implemented a limit to the maximum number of connections by appliance in Firewall.
T1-535	Improvement done in the Network Interfaces setup.
T1-554	Improvement done in the VPN IPSEC's authentication.
T1-564	Improvement done in the loading of the Web filter.
T1-577	Improvement done in the update script.
T1-581	Improvement done in the VPN IPSEC's web browsing.
T1-598 **T1-731** **T1-742**	Improvement done in the QoS rules application in NAT rules.
T1-621	Improvement done in the creation of Zone Protection rules through Device Templates.
T1-715	Correction done in the IP generation via the Radius' DHCP.
T1-727	Correction done in the Analyser's Logs display.
T1-746	Improvement done in the IPV6 policy packages forwarding in the Firewall.
T1-749	Correction done in the LAG and Bridge interfaces.
T1-763	Improvement done in the Application Control enabling.
T1-767	Improvement done in the Ips attribution and working of the DHCP + RADIUS service.
T1-769	Improvement done in the User's validation in Dynamic DDS, in Services > DDNS.
T1-773	Improvement done in the version display in the console.
T1-828	Correction done in the connection time display in the in the VPN IPSEC's reports.
T1-842	Correction done in the version display in IPV4/IPV6 Policies.
T1-999	Improvement done in the policy rules export from the GSM to the UTM.
T1-1016	Improvement done in the ETH settings editing.
T1-1037	Improvement done in the application of IPv4 policies in remote networks packets.
T2-64	Improvement done in the standard definition of the number of Workers, in Application Control.
T2-132	Improvement done in the Firewall TACACS+ authentication.
T2-135	Improvement done in the HOST files update.
T2-139	Improvement done in the application of SSL tunnel web access settings, in Services > SSL VPN > Portal.
T2-141	Improvement done in the topology edition, in ADVPN settings.
T2-164	Improvement done in the Secure SDWAN rules application.
T2-199	Improvement done in the Security Events and Analyzer's Logs display.
T2-211	Improvement done in the SSL Tunnel compatibility with other applications.
T2-242	Improvements were done in a general way on the security applications, such as Nexus and Apache.
T2-257	Improvement done in the SDWAN's band limit.
T2-258	Improvement done in the control of infected files, in Services > ATP > Quarantine.

T2-262	Melhorias feitas nos seguintes sistemas de segurança: IMAP overflow, Stone Trip allow system, jQuery version update, HTTP TRACE /TRACK methods, CSRF, Filtro de autorização de autores para exibição de informações.
T2-355	Improvement done in the Proxy's Hash limit.
T2-387	Improvement done in the communication between two UTMs.
T1-391	Improvement done in the Policy Templates setup and IPV4 and IPV6 Policies.
T2-399	Improvement done in the Workers setup in Application Control.
T2-403	Improvement done in the origin and destination IPs display in the creation of policies in Port Forwarding.
T2-407	Improvement done in the setup of TCP ports with service objects.
T2-411	Improvement done in the OMNE authentication service.
T2-415	General improvements done in the UTM’s Security Protocols.
T2-552	Improvement done in the IPSEC VPN’s setup.
T2-578	Correction done in the activation of the Ipsec VPN’s tunnel.
T2-588	Improvement done in the Interface edition in “Dynamic IP” mode.
T2-597	Improvement done in the users’ registration in Firewall.
T2-755	Improvement done in the manual update system.
UTM-471	Improvement done in the ip6tables forwarding in IPV6 Policies.
UTM-3453	Improvement done in the Reslave’s setup.
UTM-3760	Improvement done in the Licence application.
UTM-3775	Improvement done in the import of Logs from the VPN Analyzer from previous versions of the UTM.

Blockbit UTM version 2.1.1

Release Notes

23/08/2021

Several features have been implemented in the release of Blockbit UTM 2.1.1:

- Added option to clone *Port Forwarding* and *Zone Protection* Policies.
- Added object search bar in *Port Forwarding* and *Zone Protection*.
- Implemented option to disable the Traffic Monitor by *Port Forwarding*, *Zone Protection*, *IPv4 and IPv6 Policies*.
- Implemented the edition of the search fields of IPS profiles imported from a GSM.
- Implemented option to limit the number of Packets by second in *Port Forwarding* and *IPv4 and IPv6 Policies*.
- Added information description column in *Zone Protection*.
- Added multiple workers (processes) selection option by *Application Control* and *SSL Inspection* profile.

The following table lists the improvements and fixes done in the release of the Blockbit UTM 2.1.1:

Code	Description
UTM-359	Correction done in the block rules in Zone Protection.
UTM-396	Correction done in the Threat Block System.
UTM-494	Improvement done in the percentage of used disk displayed, in System Notifications.
UTM-543	Correction done in the access portal settings.
UTM-919	Correction done in the HTTPS Proxy access liberation with explicit Proxy.
UTM-1290	Change done in the field naming in Hosts > DDNS Services.
UTM-1656	Correction done in the ATP in cases of full disk.
UTM-1658	Correction done in the POP3 Proxy in cases of full disk.
UTM-1659	Correction done in Proxy ATP in cases of full disk.
UTM-1749	Correction done in the activity notifications in Threat Protection.
UTM-1786	Correction done in the update notifications system.
UTM-1954 **UTM-1873**	Correction done in the system's Backup restore.
UTM-1957	Improvements done in the information display in Live sessions regarding VPN SSL Site to Site.
UTM-2222	Improvement done in the intuitivity of the support information in Settings > authentication > Portal.
UTM-2248	Implemented the export of Logs in Backup, in System > Backup.
UTM-2348	Improvement done in the system's notification management.
UTM-2350	Improvement done in the synchrony of two UTMs through High Availability.
UTM-2521	Implementation of an update button in system update > Backups > Device backup.
UTM-2613	Correction done in the Network settings > Traffic Shaping belonging to the LAN and DMZ zones.

UTM-2670	Correction done in the Uptime display.
UTM-2671	Improvement done in the character insertion in the Description field in Static Routes.
UTM-2681	Improvement done in the Log sending via Syslog.
UTM-2755	Correction done in the removal of a UTM from the GSM, now also deleting objects, profiles and policies.
UTM-2766	Improvement done in the Firewall's reply to changes in the Settings window in System > Logging.
UTM-2768	Correction done in the displayed message in case of the insertion of invalid character in the Wizard's setup.
UTM-2772	Correction done in the VPN display in audit Logs.
UTM-2837	Improvement done in the security notification system.
UTM-2905	Improvement done in the displayed information in the Audit Logs of the Webfilter profile.
UTM-2906	Correction done in the display of enabled items in the inclusion of IPV4 Policies.
UTM-2933	Correction done in the time displayed in the Analyser's history.
UTM-2937	Correction done in the IPS' Logs.
UTM-2947	Improvement done in the maximum number of connections in more robust models of the Blockbit appliances.
UTM-2952	Correction done in the Web Proxy's cache.
UTM-2964	Correction done in the application of IPV4, SSL inspection and Web filter.
UTM-2967	Improvement done in the application of Network Backup configurations.
UTM-2978	Correction done in the HA synchrony in Heartbeat interfaces.
UTM-2980	Correction done in the Webfilter's Log generation.
UTM-2991	Correction done in the Debug-web's traffic.
UTM-2996	Correction done in the information displayed in the system's Log audit.
UTM-3004	Correction done in the IPS block Logs.
UTM-3010	Correction done in the user authentication when updating the notification options.
UTM-3013	Correction done in the Webfilter's message display.
UTM-3025	Improvements done in the IPS profile management, as well as in the Logs generated after the modification of White or Blacklists.
UTM-3034	Adjustment done in the synchrony with LDAP Linux sever.
UTM-3037	Correction done in the navigation in IPS.
UTM-3038	Improvement done in the management of files in quarantine.
UTM-3052	Improvement done in the version's feature compatibility with BB-30-F.

UTM-3065	Improvement done in Threat Protection.
UTM-3066	Correction done in the definition of Workers in SSL Proxy.
UTM-3067	Improvement done in the RSSO validation when configuring RADIUS servers.
UTM-3093	Adjustments done in the VPN IPsec Logs generation.
UTM-3095	Correction done in the display of messages in SSL Proxy.
UTM-3097	Correction done in the communication of policies between Firewall and Proxy.
UTM-3115	Correction done in the groups of Users' synchrony.
UTM-3132	Correction done in the display order of objects in groups of Users.
UTM-3133	Correction done in the application of Port Forwarding rules.
UTM-3144	Correction done in the server authentication.
UTM-3145	Improvement done in the Webfilter in Analyser.
UTM-3146	Correction done in the destination field in Live session > Web.
UTM-3162	Adjustments done in the saving of band control settings for ETH4.
UTM-3178	Correction done in the rule changing in Firewall > Port Forwarding.
UTM-3180	Adjustments done in the functioning of Policies in case of the exclusion of Interfaces.
UTM-3183	Correction done in the VPN SSL files saving.
UTM-3202	Correction done in the access to the database.
UTM-3206	Adjustments made in the Logtype filter in Monitor > Security Events.
UTM-3220	Correction done in the graphics displayed in the Analyser's Log.
UTM-3221	Adjustments done in the OSPF setting in Tunnel type interfaces.
UTM-3233	Adjustments done in the DoS Protection options in the Firewall's global settings.
UTM-3254	Improvement done in the update and upgrade automatic system.
UTM-3256	Change done in the timezones in VPN Logs in Security Events.
UTM-3277	Correction done in the displayed name of IPV4 Policies.
UTM-3278	Correction done in the profile names displayed in Port Forwarding rules
UTM-3344	Correction done in the application select filter for receiving notifications.
UTM-3351	Correction in the Range register in Port Forwarding.
UTM-3352	Improvement done in the Common Name Webfilter in cases of conflict with SSL Proxy.
UTM-3354	Correction done in the Speedtest command used for data transfer speed tests.
UTM-3355	Correction done in the Web filter's policies authentication, in Services > Web Cache > Hierarchy.
UTM-3381	Correction done in the Firewall backup restoration.
UTM-3382	Improvement done in the implementation of Firewall Policies.
UTM-3383	Correction done in the Log's days limit.
UTM-3385	Improvement done in the Netflow's module.
UTM-3394 **UTM-3407**	Correction done in the tag colors in IPV6/IPV4 settings.
UTM-3395	Correction done in the options marking when creating/editing policies in Firewall.

UTM-3396	Adjustments done in the Burst Rate in the creation of IPV6/IPV4 Policies.
UTM-3405	Adjustment done on the display of preset option in Policies, Traffic Monitor/Firewall.
UTM-3406	Improvement done in the default options in the creation of a new Policy in Traffic Monitor > Firewall.
UTM-3441	Adjustments done in the profile editing and the menu in Threat Protection.
UTM-3442	Correction done in the reporter apply and Log generation.
UTM-3454	Adjustments done in the displayed message in Services > Web filter profile creation.
UTM-3464	Improvement done in the performance of an environment configured as Master in Settings > System > High Availability.
UTM-3475	Improvement done in the authentication service in the portal.
UTM-3476	Correction done in the error message displayed in Proxy configuration.
UTM-3481	Correction done in the signature enabling in Intrusion Prevention System.
UTM-3487	Improvement done in the detailing of IPV6 Audit Logs.
UTM-3491	Improvement done in the Policies and Objects detailing in Audit Logs.
UTM-3511	Correction done in the time exhibition in CSV Reports.
UTM-3517	Correction done in the interface selection in Port Forwarding.
UTM-3532	Correction done in the parameter’s display in the Top Policies field in Dashboard.
UTM-3533	Improvement done in the customization of categories (Blocked/Allowed) in Webfilter Profiles.
UTM-3551	Improvement done in the editing of interfaces in SD-WAN profiles.
UTM-3561	Improvement done in the profile editing in Services > Application Control.
UTM-3576	Correction done in the message displayed when deleting SSL Inspection profiles.
UTM-3611	Improvement done in the setup of installation files.
UTM-3632	Improvement done in the base generation and reading of IPS signatures.

Blockbit UTM version 2.1.0

Release Notes

25/03/2021

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.1.0:

- Implementation of ECMP routing protocol support;
- Implementation of support for native encapsulation of MPLS networks;
- Addition of controls for optimization and retransmission of TCP flows;
- Improvements in Web Filter, Categories and Web Applications policies are considered for policy matching, making the product much more flexible and adhering to the needs of network environments.

In addition, the following CLI commands have been implemented:

- Creation of the “ssh-client” command, which allows access to the cluster's slave node, through the command line;
- Creation of the “set-ethernet-channels” command to define the number of channels per network card.

The following table lists the improvements made in the release of Blockbit UTM:

Code	Description
UTM-830	Correction in the creation of DNAT port redirection
UTM-913	Correction applied to DHCP link delivery
UTM-940	Correction applied to permission to change password in user profiles
UTM-1887	Improvement in the performance of the display of sessions in live sessions and in the debug-firewall command
UTM-2047	Fixed receiving Zero Touch Provisioning settings
UTM-2124	Correction in the Microsoft Active Directory user synchronization process
UTM-2212	Correction applied to changes made to single objects in use
UTM-2233	Correction in the display of the interfaces of the equipment identified in the netflow
UTM-2261	Correction applies when editing objects in the IPv4 Policies window
UTM-2264	Fixed display of remote VPN users report
UTM-2268	Renaming the "debug-appcontrol" command to: "debug-dpi", used to analyze the logs on the command line of the Application Control functionality
UTM-2357	Correction in the display of information sent by e-mail notifications
UTM-2488	Improved validation of the duplicate DNAT creation process
UTM-2517	Correction in the display of groups when editing policies
UTM-2528	Improved performance of the AntiMalware Service
UTM-2536	Corrections to Application Control features

UTM-2563	Correction applied to the snapshot restore tool
UTM-2577	Fixed character validation in Webfilter forms
UTM-2581	Correction applied when editing objects assigned to groups
UTM-2596	Correction applied when creating rules in the SD-WAN configuration
UTM-2602	Correction in the application of Webfilter policies with dictionary object
UTM-2622	Correction applied to IP retention in NAT policies
UTM-2623	Fixed email authentication on the portal and IPsec VPN
UTM-2624	Improved performance of proxy services
UTM-2628	Improved layout of the port forwarding screen
UTM-2634	Improvement in the limit of registered ports in the proxy
UTM-2642	Improvement in the performance of the apply of changes in SSL profiles
UTM-2667	Correction in the display of debug logs in Analyzer
UTM-2687	Firewall apply fixes when removing policies
UTM-2701	Fixes in removing IPSEC RAS VPN settings when disabling it
UTM-2707	Fixes in the deployment service startup
UTM-2709	Corrections applied to IP reservation in DHCP ranges
UTM-2712	Correction in the process of unlinking the UTM from a GSM
UTM-2715	Correction applied to the replication of authentication sessions on secondary servers in H.A.
UTM-2870 **UTM-2871** **UTM-2875**	General improvements in UTM custom branding to enable use as a whitelabel
UTM-2718	Correction in the creation of objects in Security Policies
UTM-2775	Correction in the display of SNMP information
UTM-2845	Correction applied in removing IPs from interfaces in use
UTM-2852	Correction in the display of policies in SSL Inspection
UTM-2908	Correction applied when removing connections in Live Sessions

UTM-2909	Correction applied to the blocking of already established connections
UTM-2912	Correction in Webfilter with Explicit Proxy and Captive Portal
UTM-2920	Improvements in the performance of SSL Inspection policies
UTM-2930	Improved performance of the policy addition and removal process
UTM-2931	Correction in the virtual interfaces of the secondary H.A. server
UTM-2932	Correction in the application of changes in Application Control
UTM-2940	Improved Reporter service performance

Blockbit UTM version 2.0.13

Release Notes

02/08/2022

Updates and improvements presented in the BLOCKBIT UTM Version 2.0.13:

Code	Description
T1-232	Improvement done in the editing of interfaces with registered Policies.
T1-235	Improvement done in the SSL Inspection.
T1-287	Correction done in the license key reaplication.
T1-292	Improvement done in the update settings via proxy server.
T1-777	Improvement done in the functioning of the RADIUS authentication service.
T1-869	Improvement done in the VPN IPSec Site to Site's communication, with Firewall rules.
T1-932	Correction done in the Query Filters' filters, in Security Events.
T1-1147	Improvement done in the SDWAN's Load Balance profile.
T1-1221	Improvement done in the upgrade scripts.
T1-1277	Melhoria feita na aplicação de configurações ao desabilitar um túnel de VPN IPSec.
T1-1364	Correction done in the information contained in the settings file in VPN IPSec.
T1-1410	Improvement done in the CSV reports creation.
T1-1423	Improvement done in the CSV and PDF Reports storing, in Monitor.
T1-1530	Improvement done in the creation of network interfaces with IPv4 Policies.
T2-150	Improvement done in the DNAT rules.
T2-597	Improvement done in the users registration in Policy packages.
T2-601	Improvement done in the remote access VPN.
T2-810	Improvement done in the REDIS service's memory allocation.
T2-820	Improvement done in the synchrony between master and slave, in High Availability.
T2-916	Improvement done in the characters insertion in the "Login" and "Name" fields when creating a user.
T2-964	Improvement done in the loading of files required for the REDIS to work in full capacity.
T2-1004	Improvement done in the network interface's stability.
T2-1198	The fwreload command has been stabilized in the UTM's script.
SUS-395	Correction done in the IPv4 Policies, Zone Protection and Port Forwarding authentication.

Blockbit UTM version 2.0.12

Release Notes

30/05/2022

Updates and improvements presented in the BLOCKBIT UTM Version 2.0.12:

Code	Description
T1-283	Correction done in the naming of the “Allowed” and “Blocked” fields, in Firewall > Port Forwarding.
T1-284	Improvement done in the license validation.
T1-667	Improvement done in the RADIUS domain editing.
T1-828	Correction done in the time displayed in the IPSEC VPN’s reports.
T1-871	Correction done in the information displayed in the Logger’s settings.
T1-1041	A command for updating the Logger has been implemented.
T1-1057	Improvement done in the deploy of Device Templates between a UTM and a GSM.
T1-1118	Improvement done in the DNAT Port Forwarding’s stability when virtual interfaces are created.
T1-1131	Improvement done in the Root configuration.
T1-1221	Improvement done in the update script.
T1-1276	Correction done in the display of SD-WAN profiles.
T1-1280	Correction done in the VPN site to site’s Analyzer.
T2-597	Correction done in the edition of users in NAT Policies.
T2-600	Improvement done in the IP assignment in the Bridge interface.
T2-612	Correction done in the explicit Proxy functioning.
T2-742	Improvement done in the Logs management of the REDIS.
T2-938	Improvement done in the Dynamic Remote Host of the IPSEC VPN.

Blockbit UTM version 2.0.11

Release Notes

24/08/2021

Improvements presented in the BLOCKBIT UTM Version 2.0.11:

- **Application Control base's priority has been reordered.**
- **Implemented command for using the Debug-provisioning.**
- **Implemented function to display the licence's validity along with the information that can be obtained through the show license command.**
- **Added an option to set the system's language to Spanish.**

Updates presented in the BLOCKBIT UTM Version 2.0.11:

Code	Description
T1-9	Correction done in the server authentication and setup.
T1-66	Optimization has been done in the database Logs generation.
T1-87	Improvement done in the creation of Zone Protection rules through the Device Template
T1-158	Improvement done in the Web filter’s general settings.
T1-188	Improvement done in the Policy filter in Security Services.
T1-202	Improvement done in the Applications routing through the SDWAN.
T1-203	Improvement done in the SDWAN’s Load balance.
T1-204 **T1-206** **T1-449**	Improvement done in the Port Forwarding connections display in Live Sessions.
T1-213	Improvement done in the RADIUS server settings fields, in Settings > Authentication > Servers > RADIUS.
T1-270	Correction done in the message display when creating Device Templates.
T1-282	Improvement done in the HTTPD service activation.
T1-292	Improvement done in the update validation through the Proxy server.
T1-364	Improvement done in the DNAT Policies loading.
T1-366	Improvement done in the rule setup and port redirecting.
T1-381	Improvement done in the Zone Protection Logs in the Security Events window.
T1-393	Improvement done in the Firewall Policies application in Port Forwarding connections.
T1-424	Correction done in the DNAT rule application in secondary links.

T1-439 **T1-443**	Improvement done in the validation of the VPN SSL fields.
T1-526	Improvement done in the maximum number of connections, now standardized according to the maximum capacity of the Appliance's model, in Services > Firewall > General Settings.
T1-531	Correction done in the network interface display, in Settings > Network > Interfaces.
T1-554	Improvement done in the VPN IPSEC's authentication.
T1-564	Improvement done in the Web filter's loading.
T1-581	Improvement done in the VPN IPSEC's web browsing.
T1-598 **T1-731** **T1-742**	Improvement done in the QoS rules application in NAT rules.
T1-727	Improvement done in the analyzer's Logs display.
T1-746	Improvement done in the IPV6 policy packages forwarding in the Firewall.
T1-749	Improvement done in the Lag and Bridge interfaces display in the graphic interface.
T1-763	Improvement done in the Application Control enabling.
T1-769	Improvement done in the User's validation in Dynamic DDS, in Services > DDNS.
T1-828	Correction done in the connection time display in the in the VPN IPSEC's reports.
T2-67	Improvement done in the authentication service and Web filter policies.
T2-132	Improvement done in the Firewall TACACS+ authentication.
T2-135	Improvement done in the HOST files update.
T2-141	Improvement done in the topology edition, in ADVPN settings.
T2-164	Improvement done in the Secure SDWAN rules application.
T2-211	Improvement done in the SSL Tunnel compatibility with other applications.
T2-242	Improvements were done in a general way on the security applications, such as Nexus and Apache.
T2-257	Improvement done in the SDWAN's band limit.
T2-258	Improvement done in the control of infected files, in Services > ATP > Quarantine.
T2-262	Improvements done in the following security systems: IMAP overflow, Stone Trip allow system, jQuery version update, HTTP TRACE/TRACK methods, CSRF, Author authorization filter for information display.

T2-381	Improvement done in the sending of installed version by the Keepalive to the licences server.
T2-407	Improvement done in the setup of TCP ports with service objects.
T2-415	General improvements done in the UTM’s Security Protocols.
T2-552	Improvement done in the creation and setup of the VPN IPSEC.
T2-588	Improvement done in the Interface edition in “Dynamic IP” mode.
T2-597	Improvement done in the Users’ registration in NAT policies.
UTM-3681	Improvement done in the Users creation in the IPSET.

Blockbit UTM version 2.0.10

Release Notes

23/08/2021

Updates and improvements presented in the BLOCKBIT UTM Version 2.0.10.

Code	Description
UTM-329	Improvement done in the editing of RADIUS servers.
UTM-359	Improvement done in the ICMP block and liberation rules.
UTM-543	Improvement done in the service in the 9803 port in Firewall > Zone Protection.
UTM-1556	Improvement done in the display of policies in the Port Forwarding Logs.
UTM-1657	Improvement done in the full disk notification, in Settings > System > Notifications.
UTM-1749	Improvement done in the threat notifications via e-mail and SMTP.
UTM-2222	Improvement done in the displayed information in Allowed Domains and Allowed Groups, in Settings > Authentication > Portal.
UTM-2348	Improvement done in the display of new system's notifications.
UTM-2670	Improvement done in the uptime display of the server, in Settings > Network.
UTM-2671	Correction done in the validation of the description field, in Settings > Network > Static Routing.
UTM-2768	Improvement done in the Wizard's settings message.
UTM-2952	Improvement done in the Proxy's Log messages.
UTM-2980	Improvement done in the Firewall and Web filter's Logs register.
UTM-2991	Correction done in the Web filter's traffic debug.
UTM-3004 **UTM-3025**	Improvement done in the audit Logs in the IPS profiles.
UTM-3064	Improvement done in the search parameters, in Security Events.
UTM-3067	Improvement done in the RADIUS serves authentication via RSSO.
UTM-3132	Correction done in the sequencing of group users in Authentication Services.
UTM-3145	Improvement done in the drill draws of the Web filter's Logs.
UTM-3146	Correction done in the destination field, in Live Sessions > Web.
UTM-3162	Correction done in the band controls for the network interfaces, in Settings > Network > Band Control.
UTM-3163	Improvement done in the searched items display in the Analyzer.
UTM-3202	Correction in the return message in the execution of the rewizard command.
UTM-3206	Improvement done in the filter by Logtype, in Monitor > Security Events.
UTM-3207 **UTM-3577**	Improvement done in the block of IPv4 policies, in Application Control.
UTM-3217	Correction done in the top profiles' information, in > Analyzer > Web filter.
UTM-3220	Correction done in the information displayed in the Logs, in Analyzer.
UTM-3221	Improvement done in the Routing settings.
UTM-3254	Improvement done in the automatic updates system.
UTM-3262	Improvement in the interface security administration, deactivating support to the TLS 1.0 and 1.1.

UTM-3277	Improvement done in the classification of Ipv4 and Ipv6 policies in the system's audit screen.
UTM-3344	Improvement done in the Applications selection, in Settings > System > Notifications.
UTM-3385	Correction done in the removal of Netflow's module.
UTM-3449	Improvement done in the certificate naming fields.
UTM-3454	Improvement done in the nomenclature in portuguese of "tittle", in Services > Web filter.
UTM-3475	Optimization done in the user authentication process when logging in the UTM Portal.
UTM-3511	Improvement done in the Timezone display after the generation of reports, in Monitor > Reports.
UTM-3532	Correction done in the information displayed in Top Policies, one of the Dashboard's Widgets.
UTM-3533	Improvement done in the customization of categories of the Web filter's profiles.
UTM-3545	Improvement done in the Secure SDWAN.
UTM-3551	Improvement done in the handling/control of interfaces in the SD-WAN profiles.
UTM-3556	Improvement done in the authentication settings.
UTM-3558	Correction done in Administration Services.
UTM-3559	Correction done in the displayed information in Monitor > System Status.
UTM-3561	Correction done in the profile pagination, in Services > Application Control, after the base's update.
UTM-3568	Improvement done in the virtual interface's option.
UTM-3572	Improvement done in the Port Forwarding service in Security Services.
UTM-3576	Improvement done in the profile exclusion/deletion, in Services > Proxy > SSL Inspection.
UTM-3611	Improvement done in the system update.
UTM-3617	Improvement done in the creation of objects, in services.
UTM-3626	Improvement done in the setup of static routing.
UTM-3648	Improvement done in the VPN IPsec Site to Site.
UTM-3659	Improvement done in the application database in Application Control.
UTM-3672 **UTM-3673**	Improvement done in the validation of the VPN IPsec fields.

Blockbit UTM version 2.0.9

Release Notes

17/05/2021

The following table lists the improvements made in the release of Blockbit UTM 2.0.9.

Code	Description
UTM-396	Improvement done in the threat blocking policy system.
UTM-919	Improvement done in the HTTPS access systems.
UTM-1272	Correction done in the IP insertion field in Manager Address.
UTM-1290	Improvement done in the Host fields of the DDNS service.
UTM-1412	Adjustment done in the Speedtest command.
UTM-1656	Correction done in the disk space detection for the Antimalware.
UTM-1873	Improvement done in the authentication of the system's backup and restore.
UTM-1954	Correction done in the data base initialization when restoring backup.
UTM-1957	Improvements done in the ID display in Live Sessions.
UTM-2248	Correction done in the Log export list in backups done by the UTM.
UTM-2350	Correction done in the VPN Logs.
UTM-2521	Inclusion of a refresh button in the device backup screen.
UTM-2613	Correction done in the Network>Traffic Shaping setup in LAN and DMZ zone interfaces.
UTM-2681	Correction done in the sending of Logs via Syslog by the UTM.
UTM-2755	Correction done in the removal of objects in a Device untying from a GSM.
UTM-2766	Improvement done in the system's performance when applying changes in the Settings window.
UTM-2772	Correction done on the message displayed in VPNSSL changes.
UTM-2837	Correction done in the sending of security notifications by e-mail.
UTM-2881	Correction done in the application of Templates to UTM Devices.
UTM-2905 **UTM-2906**	Improvement done in the Web Filter audit Log and IPv4 Policies.
UTM-2933	Improvement done in the time display in Threat Protection reports.
UTM-2937	Improvement done in the IPS Logs.
UTM-2947	Improvement done in the maximum number of connections according to the hardware model.
UTM-2964	Improvement done in the application of IPv4 Policies with Web Filter with: "Deny" actions.
UTM-2967	Improvement done in the Network Setup application in backup environment.
UTM-2978	Correction done in the synchrony of Heartbeat interfaces.
UTM-2996	Improvement done in the audit Logs, implementing the Log with the Applies' time.
UTM-3010	Correction done in the user authentication system in cases of change in the notifications' system.
UTM-3013	Improvement done in the generation of Logs in the Webfilter.
UTM-3034	Improvement done in the user synchronization with LDAP Linux server.
UTM-3037	Correction done in the navigation on the quarantine pages of the IPS module.

UTM-3038 **UTM-3065**	Improvement done in the Malware Protection system.
UTM-3052	Improvement done in the Update system.
UTM-3093	Correction done in the generation of the IPSEC VPN's Logs.
UTM-3095	Improvement done in the display of messages by the SSL Proxy.
UTM-3097	Improvement done in the Policies between Firewall and Proxies in great network traffics.
UTM-3115 **UTM-3144**	Improvement done in the user authentication in the LDAP server.
UTM-3133	Correction done in the Port Forwarding (DNAT) loading.
UTM-3139	Correction done in the Logs' filters in Security Events.
UTM-3178	Improvement done in the application of Port Forwarding rerouting rules.
UTM-3180	Improvement done in the exclusion of Network interfaces with Port Forwarding Policies associated.
UTM-3183	Correction done in the VPN SSL Site to Site setup.
UTM-3194	Improvement done in the editing of IPS Profiles search fields.
UTM-3221	Correction in the saving of OSPF parameters with tunnel interfaces.
UTM-3233	Correction in the maximum limit of packets per second in the DoS Protection options in Firewall.
UTM-3256	Correction made in the VPN Logs when configured in different Timezones.
UTM-3278	Correction done in the naming of SSL Inspection Profiles in cases of inclusion of Firewall rules for Port Forwarding.
UTM-3351	Correction in the Range register in Port Forwarding.
UTM-3352	Improvement done in the Common Name Webfilter in cases of conflict with SSL Proxy.
UTM-3354	Correction done in the Speedtest command used for data transfer speed tests.
UTM-3355	Correction done in the Hierarchy Cache of the Web Filter.
UTM-3381	Correction done in the Firewall backup restoration.
UTM-3382	Improvement done in the implementation of Firewall Policies.
UTM-3383	Correction done in the Log's days limit.
UTM-3476	Correction done on the message displayed when configuring the Proxy server in the System window: Updates.
UTM-3512	Correction done in the use of cloned MAC in virtual Interfaces.
UTM-3517	Correction done in the application of Port Forwarding rule in different interfaces.
UTM-3529	Correction done in the disk maintenance display.
UTM-3575	Update done in the Log service.

Blockbit UTM version 2.0.8

Release Notes

30/03/2021

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.8:

- Implementation of commands to enable and disable session monitoring and logging;
- Implementation of a command to display the current temperature detected by the appliance's sensors;
- Implementation of a command to migrate the logs from the old Firewall structure to the new version.

The following table lists the improvements made in the release of Blockbit UTM

Code	Description
UTM-390	Grammar correction in the Web Filtering lock screen
UTM-1786	Correction applied to sync notifications with GSM
UTM-2348	Fixed clearing notifications button on UTM
UTM-2582	Correction in the legend of the SD-WAN profile monitoring graph
UTM-2602	Correction in the application of Webfilter policies with dictionary object
UTM-2634	Improvement in the limit of registered ports in the proxy
UTM-2641	Correction applied to the display of the Dashboard logs
UTM-2681	Correction in the service responsible for sending logs
UTM-2738	Correction applied to IPS log inspection
UTM-2744	Correction in the IP address list of the IPS quarantine
UTM-2763	Correction in data synchronization of Traffic Monitor and Dashboard
UTM-2768	Correction applied to the message displayed in the UTM Wizard
UTM-2775	Correction in the display of SNMP information
UTM-2780	Performance improvements for Live Sessions and Traffic Monitor
UTM-2809	Correction in the mapping of dictionary objects applied in SSL profile
UTM-2826	Correction applied in the display of the graphs of the reports in PDF
UTM-2827	Fixed IPS logs integrated with SSL Proxy
UTM-2831	Improved information displayed by the debug-sync command
UTM-2841	Correction applied to the disable-snmp command
UTM-2843	Correction applied to SMTP and POP3 proxy routing rules
UTM-2863	Corrected authentication of expired users in Captive Portal
UTM-2867	Improved SSL proxy performance
UTM-2888	Improvement in the performance of the rules, enabling implementation in more than 127 interfaces
UTM-2893	Fixed storage size display on Storage NFS
UTM-2903	Correction in the display of results when selecting File Listers in the Web Filter
UTM-2909	Correction in the blocking of already established connections
UTM-2912	Correction in Webfilter with Explicit Proxy and Captive Portal
UTM-2913	Performance improvements in Live Sessions

UTM-2914	Correction applied when creating NFS arrays
UTM-2917	Correction in the initialization of the SD-WAN service
UTM-2920	Improvements in the performance of SSL Inspection policies
UTM-2923	Correction in the restoration of snapshots when the UTM is accessed by GSM
UTM-2924	Correction applied in the execution of weekly backups
UTM-2928	Correction in CLI display after system upgrade
UTM-2930	Improved performance of the policy addition and removal process
UTM-2931	Correction in the virtual interfaces of the secondary H.A. server
UTM-2932	Correction in the application of changes in Application Control
UTM-2933	Correction applied to the threat protection history in the Analyzer
UTM-2934	Correction applied to the VPN service when making changes to the DNS
UTM-2935	Improvements applied to the “upgrade-blockbit” CLI command
UTM-2940	Improved Reporter service performance
UTM-2942	Fix kernel update in H.A. environments
UTM-2945	Correction applied to the display of the User Behavior report of the Analyzer
UTM-2948	Correction when restarting SSL Inspection profiles
UTM-2951	Fixes in the display of connections established in Firewall Live Sessions
UTM-2955	Improved display of memory usage information on the Dashboard
UTM-2966	Correction of the space limit of the antimalware quarantine
UTM-2968	Correction in the display of VPN data in Live Sessions
UTM-2971	Fixes applied to Analyzer Drill-Down
UTM-2974	Correction to the Portscan rule
UTM-2976	Correction allowing the creation of DNAT rules of the same function, but with different conditions
UTM-2977	Correction applied to the scale of the limit fields in the DoS protection
UTM-2979	Improved performance of Firewall Daemons
UTM-2985	Correction applied to the Remote Users graph in the VPN report
UTM-2986	Traffic correction in web policy
UTM-2987 **UTM-2990**	Correction in the application in SSL Inspection profiles
UTM-2993	Correction in the display of some information in the Port Forward rules
UTM-2994	Correction in the display of authenticated users in Security Events
UTM-2995	Correction in the display of VPN connections in Security Events
UTM-2997	Improved performance of the authentication service
UTM-2998	Correction applied to the Common Name when a Web Filter block is made
UTM-2999	Correction in the generation of reports in CSV of the log session
UTM-3000	Correction in the display of the bandwidth consumption values in the Web Filter report
UTM-3003	Improvements in creating authentication rules to prevent re-entry to the domain
UTM-3009	Fixed redirection of Analyzer filters
UTM-3014	Improved performance of Captive Portal authentication
UTM-3015	Correction in the display of IP objects in the Port Forwarding form

UTM-3018	Correction applied to the maximum number of connections to the database
UTM-3020	Improvements applied to CLI upgrade-blockbit and upgrade-kernel commands, blocking if secondary H.A. device is active
UTM-3025	Fixes applied to IPS audit logs
UTM-3026	Correction applied to the IPS module when moving Whitelist or Blacklist IP addresses
UTM-3027	Improvement applied to the limits of ARP tables
UTM-3028	Correction applied to Firewall logs
UTM-3029	Correction in the installation wizard service to avoid running Zero-touch provisioning
UTM-3031	Improvement in the amount of results displayed in searches in Security Events
UTM-3036	Correction in the release of navigation in Captive Portal with Explicit Proxy
UTM-3040	Correction applied when removing SSL Inspection profiles
UTM-3041	Improved collection of firewall connection source information
UTM-3042	Improved Live Sessions performance
UTM-3045	Correction in the display of Policy ID in Audit Logging
UTM-3047	Performance improvements in the log database
UTM-3049	Correction applied to the VLAN sub-interfaces of the secondary cluster in H.A. environments
UTM-3060	Correction applied to changing custom categories in Web Filter
UTM-3063	Fixed file redirection to ATP in Web Filter
UTM-3069	Correction in the checking of disable-logsessions by Live Sessions
UTM-3070	Fixes applied to IPS in Firewall mode
UTM-3073	Correction in the ARP table and in the identification of the firewall Zones
UTM-3074	Improved performance of the application of the Web Filter settings
UTM-3075	Correction applied to the Primary Cluster in H.A. environments
UTM-3077	Correction of access records in Security Events reports
UTM-3092	Correction applied when creating NAT policies for DNS servers
UTM-3099	Improvement in the update script, now it automatically restarts the firewall to consolidate the settings
UTM-3106	Correction in pagination in Security Events
UTM-3112	Correction in the classification of sites for SSL Inspection
UTM-3121	Fix applied to Threat Protection malware blocks
UTM-3122	Correction in the display of policies in the Dashboard
UTM-3123	Correction in the timing of the information displayed in Traffic Monitor, Live Sessions and SNMP
UTM-3125	Correction in the display of Malware information in the Top Threats graph in User Behavior
UTM-3127	Corrections to Logtype records in Security Events
UTM-3128	Fixes in RX/TX monitoring in SNMP
UTM-3130	Corrections to information request in Live Sessions
UTM-3135	Fixes applied in the execution of the rotate log
UTM-3139	Fixes applied in Query Editores
UTM-3140	Corrections in the display of users in the Top profiles chart in Web Filter Analyzer
UTM-3141	Fixes applied to the database after running the log rotate
UTM-3142	Corrections on Top Threats query in User Behavior
UTM-3143	Correction in the display of the user selection menu in User Behavior

UTM-3145	Fixed display of items in analyzer and security events
UTM-3148	Correction in the performance of the editing window of user groups in the Authentication settings
UTM-3150	Correction applied to time information logged into the VPN
UTM-3152	Correction in the detailing of the VPN in the Analyzer
UTM-3153	Correction in the browsability of SSL Inspection profiles
UTM-3155	Correction in CLI command “reset-logs”
UTM-3156	Correction applied to logs by Session ID
UTM-3157	Improved layout of the user group edit window in Authentication
UTM-3158	Correction applied when exporting CSV reports and creating Analyzer reports
UTM-3179	Correction applied to messages displayed when performing the rewizard

Blockbit UTM version 2.0.7

Release Notes

14/12/2020

- Revision of the layout in Port Forwarding, in addition to the design and usability having been improved, the performance was improved bringing agility to this screen

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.7:

Code	Description
UTM-913	Corrections applied to DHCP link delivery
UTM-2124	Correction in the process of synchronizing users with LDAP and Microsoft Active Directory Servers
UTM-2642	Correction applied to the checking SSL profile policies check
UTM-2701	Correction in the IPSEC RAS VPN settings removal when disabling it
UTM-2709	Corrections applied to IP reservation in DHCP ranges
UTM-2845	Correction in removing IPs used in SNAT policy

Blockbit UTM version 2.0.6

Release Notes

04/11/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.6:

Code	Description
UTM-830	Corrections in the creation of redirection with port range (TCP or UDP)
UTM-940	Fixed password reset in user profiles
UTM-1887	Addition of parameter in the “debug-firewall” command to display logs in real time
UTM-1902	Fixes applied to policies that go up when restoring snapshot
UTM-2047	Correction applied when receiving Zero Touch Provisioning settings
UTM-2124	Correction in AD user timing
UTM-2212	Correction applied to the option to edit single IP address objects
UTM-2261	Corrections applied in editing the ranges of IPv4 policies
UTM-2264	Improved VPN reporting for remote users
UTM-2268	Correction applied to the Application Control service name
UTM-2357	Correction in the display of the name and ID of the ports in the notifications sent by e-mail
UTM-2488	Correction in the validation of the Port Forward form in the creation of DNATs
UTM-2517	Correction in the display of edited policy groups
UTM-2528	Improved performance of the Antimalware service
UTM-2563	Correction applied to the size allowed for snapshot upload
UTM-2577	Improved validation of the Hostname field in Webfilter
UTM-2581	Correction in the application of edited IP objects or dictionary
UTM-2596	Correction in the configuration of SD-WAN service rules
UTM-2602	Correction in the application of Webfilter policies that use dictionary objects
UTM-2622	Improved IP block validation in NAT policies
UTM-2623	Fixed email authentication over IPSec VPN
UTM-2624	Improved performance of proxy access
UTM-2628	Improved layout of Port Forwarding to facilitate display of ports
UTM-2667	Improved the layout of Intrusion Prevention to display data from IPS debug logs
UTM-2687	Fixed the creation of removed policies apply
UTM-2707	Correction in the execution of the deploy service after connection with GSM
UTM-2712	Correction applied in the service of removing the link between UTM and GSM

Blockbit UTM version 2.0.5

Release Notes

04/09/2020

- Using the GSM Template Deploy, it is now possible to make the UTM brand customization (favicon, logo, wallpaper and colors);
- Support for EAP authentication implemented in the IPSEC RAS VPN service;
- Added an exclusive tab for creating access and session control policies in the authentication service, allowing:
    - Authentication controls: Allow or block access to the condition-based authentication service;
    - Session controls: Set user session parameters.
- Logging of events based on the action applied by authentication policies;
- Detection of active sessions outside the hours configured in authentication policies, automatically logging users out;
- Added CSV *authentication log* export option;
- *Failback in the SD-WAN service* adjustment was implemented, defining how long the system should wait before enabling routing to an interface that had failed;
- The SD-WAN now monitors the network card, marking the affected link as down and switching to the best link if it detects which card is off.

In addition, the Blockbit Client, the improved and updated version of the Blockbit Agent, was released, check out the news:

- Import of connection profile automatically at the time of installation;
- Improvements in connection flow, the VPN application establishes the connection at the public address and establishes Firewall authentication at the virtual address;
- Configuration of secondary Remote Gateway addresses;
- Support for static routes configured on the Client;
- Keepalive support, which discontinues dependence on the UTM notification service;
- It allows to establish an IPsec VPN connection using the authentication method with Simple Login (Login and Password) or Simple Login with Digital Certificate;
- Export of VPN connection logs in text file for troubleshooting;
- Option to activate the VPN split tunneling feature, allowing directing of part of the traffic through the VPN while other applications maintain access on the Internet.

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.5:

Codes	Description
UTM-1719	Correction in limiting the search for users for inclusion in a group
UTM-2141	Correction in handling errors in the configuration of VPN tunnels
UTM-2143	Correction in the presentation of the Explicit proxy authentication Pop-up
UTM-2144	Correction in reconnecting proxy service sockets
UTM-2148	Improved system performance when saving reports
UTM-2154	Corrections when changing users of a group in Web Filter
UTM-2158	Corrections applied to digital certificate files after licensing
UTM-2161	Correction applied to the VPN SSL Server database
UTM-2163	Correction in the captive portal authentication service
UTM-2202	Correction applied in the treatment of administrator users with @domain login
UTM-2214	Correction in the inspection of WEB policies with SD-WAN
UTM-2215	Fix applied to malware scanning in Threat Protection
UTM-2220	Correction applied to policy display orders
UTM-2258	Correction in the validation of users in explicit proxy
UTM-2275	Correction in Safe Search performance

Blockbit UTM version 2.0.4

Release Notes

22/06/2020

- Implementation of support for 3G/4G/LTE network connectivity in the system of some appliances. For more information, check this page.
- Integration of the Netflow service in the system logging settings. For more information, check this page.

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.4:

Codes	Description
UTM-464	Correction in the ordering of interfaces in LAG mode.
UTM-832	Correction in the layout of the SD-WAN monitor window.
UTM-855	Correction in the activation of captive portal accounts using social login.
UTM-960	Correction in the limitation of network interfaces of the system.
UTM-1086	Correction applied to TUN interfaces in network services.
UTM-1772	Correction in the ordering of the interfaces in the system OVAs.
UTM-1804	Improvements in the performance of the firewall service.
UTM-1823	Correction applied to the display of infected domains in Threat Protection in Analyzer.
UTM-1828	Correction applied to the performance of the Firewall modules.
UTM-1899	Correction in the priority in which the GSM rules are being applied.
UTM-1900	Improvement to the performance of the authentication server.
UTM-1908	Improvement to the Antivirus performance.
UTM-1911	Improvement to the memory consumption of the firewall.
UTM-1916	Integration with Netflow service in the system logging settings
UTM-1955	Improvement to the SSL Inspection performance.
UTM-1984	Implementation of support for 3G/4G/LTE network connectivity in the system of some appliances.
UTM-2016	Correction in the CSV export in Log Sessions reports.
UTM-2039	Correction in the display of VPN Monitor information.
UTM-2058	Correction applied to the RDP service through the Portal.

Blockbit UTM version 2.0.3

Release Notes

18/05/2019

- New SSL VPN active connections monitor;
- New IPSEC VPN active connections monitor;
- New SSL VPN connection logs viewer;
- New IPSEC VPN connection log viewer;
- Exporter for SSL VPN logs to CSV;
- Exporter for IPSEC VPN logs to CSV;
- Exporter for VPN Traffic reports to PDF;
- New VPN Traffic report (daily and monthly):
    - Total traffic sent and received per connection;
    - Total time per connection;
    - Total hourly active users;
    - Top Site-to-Site connections (by traffic);
    - Top remote access users (by traffic);
- New command to monitor SSL VPN connections.

 VPNs will be restarted in the bugfix application.

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.11:

Codes	Description
UTM-761	Correction in the display of the SSL VPN module.
UTM-813	Correction applied to NFS storage.
UTM-923	Improvement in the process of establishing SSL VPN tunnels.
UTM-1324	Correction of the SSL VPN service status.
UTM-1678	Correction applied to the search field in policies.
UTM-1756	Correction in the display of VPNs in Live Sessions.
UTM-1767	Correction in the ordering of fiber optic interfaces in the installation process.
UTM-1816	Correction in the display of IPs in the IPSec Live Session window.
UTM-1820	Improved VPN authentication: It is now possible to authenticate using email.
UTM-1821	Correction applied to the Failover configuration in IPsec VPN.
UTM-1890	Improved download speed for PPPOE links.
UTM-1892	Correction applied to the settings transferred in the import process.
UTM-1894	Correction in the use of times objects in policies.
UTM-1907	Correction in the automatic use of firewall parameters when restarting the system.

Blockbit UTM version 2.0.2

Release Notes

14/04/2019

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 2.0.2:

Code	Description
UTM-849	Improvements to the SNMP MIB that monitors network interface description.
UTM-957	Correction applied to the versions that are possible to perform restoration from UTM 1.5.8
UTM-1063	Correction in the Wizard form in the H.A. Slave with LAG interface
UTM-1087	Correction applied when editing VLAN interfaces
UTM-1763	Correction in the display of the notification of joining the Domain.
UTM-1764	Correction in creating DNAT rules.
UTM-1769	Correction applied to the form for creating the user certificate through the interface 98.
UTM-1780	Correction applied when saving the scheduled report in CSV format.
UTM-1790	Correction when importing Zone Protection objects.
UTM-1791	Correction to the display of groups when creating and editing policies
UTM-1798	Correction on the user session control in Captive Portal
UTM-1799	Correction in the NAT rules import.
UTM-1824	Policy panel optimization when loading more than 10 simultaneous policies.

Blockbit UTM version 2.0

Release Notes

New package inspection flow:

- Firewall service with full data flow inspection by policy: SSL Inspection, Intrusion Prevention, Threat Protection, Application Control, Web Filter**;**
- Port Forwarding service with full data flow inspection by policy: SSL Inspection, Intrusion Prevention, Threat Blocking;
- Zone Protection service with inspection of data flow integration by policy: Intrusion Prevention, Threat Blocking;
- Independent Explicit Proxy Service;
- Policy loading module optimization;
- Optimization in the policy localization module;
- Optimization in the traffic routing module by SD-WAN.

New log summarization and processing service:

- Session logs correlated by unique session id: Firewall, Web Filter, Application Control, Intrusion Prevention, Threat Protection;
- Optimization in the event summarization process for generating Top Hits and Reports.

Management of multiple independent inspection sensors:

- Multiple SSL Inspection sensors;
- Multiple Threat Protection sensors;
- Multiple Intrusion Prevention sensors;
- Multiple Application Control sensors;
- Multiple Web Filter

New centralized dashboard for policy management based on inspection profiles;

New centralized panel for viewing session logs;

New centralized panel for exporting and scheduling reports in multiple formats: HTML, PDF, CSV;

New centralized panel for real-time system monitoring:

- System Monitor;
- Service Monitor;
- Security Monitor;
- Connection Monitor;
- Traffic Monitor.

Firewall service improvements:

- Geolocation access controls (Origin and Destination).

Web Filter service improvements:

- Access controls on unclassified sites;
- Custom category management.

Improvements in the Intrusion Prevention service:

- Blocking quarantined addresses in real time.

Threat Protection service improvements:

- Policy analysis of malware for protocols: HTTP, SMTP, POP3.

SD-WAN service improvements:

- Application-based traffic routing by policy;
- Policy-encrypted traffic routing for protocols: HTTP, SMTP, POP3.

Backup & Restore service improvements:

- Tool for selective export and import of configurations.

Blockbit UTM version 1.5.17

Release Notes

24/08/2021

Improvements presented in the release of the Blockbit 1.5.17:

Code	Description
T2-22	Improvement done in the VPN traffic through VOIP.
T2-24	Correction done in the VPN tunnels reload.
T2-242	Improvements were done in a general way on the security applications, such as Nexus and Apache.
T2-248	Improvement done in the master and slave server communication through the Heartbeat interface.
T1-249 **T1-296**	Improvement done in the Log cleaning process of the SDWAN.
T2-250	Improvement done in the antimalware update system.

Blockbit UTM version 1.5.16

Release Notes

28/06/2021

Improvements done in the release of the Blockbit 1.5.16:

Code	Description
UTM-723	Improvement done in Policies with authentication via GSM Deploy.
UTM-2350	Improvement done in the VPN Monitor Service after UTM HA Synchronization.
UTM-2978	Improvement done in the HA synchrony through Heartbeat Interfaces.
UTM-3093	Improvement done in the IPsec Logs generation.
UTM-3197	Improvement done in static routes after the system’s update.

Blockbit UTM version 1.5.15

Release Notes

14/12/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.15:

Code	Description
UTM-628	Correction applied to the download of files allowed in the Malware quarantine
UTM-695	Correction in the information display in Administrator - Audit Logs
UTM-831	Correction in editing address objects belonging to a group
UTM-913	Correction applied to DHCP link delivery
UTM-920	Improvements in the functionality of the DHCP registration form
UTM-2124	Correction in the AD user synchronization process

Blockbit UTM version 1.5.14

Release Notes

04/11/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.14:

Code	Description
UTM-830	Corrections in the creation of redirection with port range (TCP or UDP)
UTM-2124	Correction in AD user timing
UTM-2707	Correction in the execution of the deploy service after connection with GSM

Blockbit UTM version 1.5.13

Release Notes

04/09/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.13:

Code	Description
UTM-1719	Correction in limiting the search for users for inclusion in a group
UTM-2147	Improved limit of open files by VPN Monitor
UTM-2149	Correction applied to user \ domain authentication on VPN
UTM-2183	Correction in the display of information of users logged in the VPN Monitor
UTM-2279	Correction in DNAT access authorization
UTM-2342	Correction applied when creating rules from GSM 1.2 to UTM 1.5

Blockbit UTM version 1.5.12

Release Notes

22/06/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.12:

Code	Description
UTM-464	Correction in the ordering of interfaces in LAG mode.
UTM-521	Correction in the bandwidth control of Network Services.
UTM-642	Correction for the year displayed on the login panel.
UTM-832	Correction in the layout of the SD-WAN monitor window.
UTM-854	Improved proxy availability.
UTM-855	Correction in the activation of captive portal accounts using social login.
UTM-856	Correction in DHCP static address registration.
UTM-912	Improvements applied to the layout of the licensing panel.
UTM-960	Correction in the limitation of network interfaces of the system.
UTM-1086	Correction applied to TUN interfaces in network services.
UTM-1140	Correction in the services used in the snapshot restore.
UTM-1772	Correction in the ordering of the interfaces in the system OVAs.
UTM-2026	Improved the layout of the VPN Monitor screen.
UTM-2039	Correction in the display of VPN Monitor information.

Blockbit UTM version 1.5.11

Release Notes

18/05/2019

- New SSL VPN active connections monitor;
- New IPSEC VPN active connections monitor;
- New SSL VPN connection logs viewer;
- New IPSEC VPN connection log viewer;
- Exporter for SSL VPN logs to CSV;
- Exporter for IPSEC VPN logs to CSV;
- Exporter for VPN Traffic reports to PDF;
- New VPN Traffic report (daily and monthly):
    - Total traffic sent and received per connection;
    - Total time per connection;
    - Total hourly active users;
    - Top Site-to-Site connections (by traffic);
    - Top remote access users (by traffic);
- New command to monitor SSL VPN connections.

 VPNs will be restarted in the bugfix application.

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit UTM 1.5.11:

Codes	Description
UTM-761	Correction in the display of the SSL VPN module.
UTM-813	Correction applied to NFS storage.
UTM-923	Improvement in the process of establishing SSL VPN tunnels.
UTM-947	Correction applied when editing VLAN interfaces.
UTM-1324	Correction of the SSL VPN service status.
UTM-1816	Correction in the display of IPs in the IPSec Live Session window.
UTM-1820	Improved VPN authentication: It is now possible to authenticate using email.
UTM-1890	Improved download speed for PPPOE links.

Blockbit UTM version 1.5.10

New Feature:

Implementation of an SNMP MIB for monitoring the network interface description.

Code	Description
UTM-859	Improved stability of the proxy service on servers with many interfaces.
UTM-957	Correction applied when restoring snapshots
UTM-1063	Correction applied to the High Availability service with LAG interface.
UTM-1087	Correction applied when editing the VLAN interface ID
UTM-1280	Correction when enabling and disabling policies on links configured in the SDWAN profile.
UTM-1584	Correction in the log sending service

Blockbit UTM version 1.5.9

New Features

The network interface management system allows adding and removing addresses of the same device, it can be applied to the following types of device:

- Physical;
- Virtual;
- VLAN;
- LAG.

The backup interface now has a selective exporter of settings for imports in UTM 2.0, allowing the export of:

- Services (Selection by services, Objects, Dynamic routing and SNMP "CLI");
- IPVA or IPV6 Policies (Profiles / Policies);
- System.

Support for integration with GSM 2.0.

Blockbit UTM version 1.5.8

New Features:

SD-WAN:

Correction on the conversion of addresses by Mac address on SD-WAN;

Support to 4 digits on the Latency and Jitter configurations on SD-WAN;

Improvement on the use of SD-WAN with dynamic links (DHCP and PPPoE);

Other features:

Improvement on log rotation, preventing the disk from getting full and interrupting services;

Improvement on the control of Youtube Channels;

Improvement in PPoE connections in case of operator failure.

The following table exhibits the improvements made in the release of BLOCKBIT UTM

Code	Description
UTM-487	Correction on the service certificate import.
UTM-720	Correction on the Proxy source and destination conditions.
UTM-721	Correction applied to the personal information fields duplication in the captive portal.
UTM-762	Correction applied on the PSK file creation process.
UTM-765	Correction applied to VPN SSL service status information.
UTM-768	Correction on VPN communication using NAT-T.
UTM-771	Correction applied to the upgrade-kernel command in H.A environment.
UTM-775	Correction on the SD-WAN configuration with AD-VPN in link with dynamic IP.
UTM-776	Correction on the operation of NAT by mac address in SD-WAN.
UTM-778	Correction on the control policies applied on the access of Youtube channels.
UTM-786	Improvement on SD-WAN latency and jitter forms, now the fields support 4 digits.
UTM-787	Correction on the operation of objects used in NAT policy.
UTM-788	Correction applied on the AD-VPN Full-Mesh TUN interface configurations.
UTM-789	Correction on the DNAT after executing fwreload command.
UTM-827	Correction on the communication between LANs in SD-WAN environment.
UTM-835	Improvement on the reconnection of DSL interfaces with PPPoE authentication.
UTM-843	Improvement on optimization and performance of cache records.
UTM-846	Correction on the storage of old logs.
UTM-847	Added debug-ppp command, responsible for performing PPPoE service monitoring.
UTM-848	Improvement on the data partitioning and system logs rotate.
UTM-909	Correction in AD user and group synchronism through proxy.
UTM-924	Correction applied to QoS settings.
UTM-929	Correction to the daylight saving time on server clock.

Blockbit UTM version 1.5.7

New Features:

CLI Commands for disk resizing – With the **parted**, **partprobe**, and **resize2fs** commands, it's possible to extend disk size from the console;

SNMP Remote Product Monitoring Improvements – New MIBs implemented to collect information about BLOCKBIT equipment on an automated basis.

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.7

Code	Description
UTM-125	Correction applied on the display of users and IPs on the Dashboard.
UTM-453	Correction on the display of URLs in event window.
UTM-474	Correction applied to the ordering of network interfaces.
UTM-526	Correction on the filter icon in dashboard IPv6 events.
UTM-527	Correction applied to the display of policy names in dashboard.
UTM-537	Correction in antimalware monthly report creation.
UTM-596	Correction on the Security Alerts widget policy filter.
UTM-612	Correction applied to DPI report.
UTM-613	Correction in creating Intrusion Prevention reports in pdf format.
UTM-674	Correction on IPSEC tunnel display in the Monitor window when establishing a VPN.
UTM-675	Correction applied when creating tunnel type interfaces in AWS.
UTM-679	Corrected directory access on port 9803.
UTM-685	Correction applied to the Kernel (see the guide "how to upgrade-kernel" available in the resource center).
UTM-688	Correction on HTTPS access with explicit proxy.
UTM-691	Correction applied to the database.
UTM-693	Correction on the display of remote access VPN connections in IPSEC connection monitor.

Blockbit UTM version 1.5.5

New Features:

Support the use of Web Proxy for licensing and updates, providing greater flexibility in the implementation of the product;

Improvements to remote product monitoring by SNMP:

- Monitoring of DHCP and DHCP6 leases;
- Monitoring of network summarized traffic throughput;
- Monitoring of connected users;
- Monitoring of established connections.

DPI module with support for IPv6 addresses;

Improvements to the Whitelist and Blacklist of the DPI module;

Implementation of Smart Bypass (bypass version 3) support in the DPI module;

CLI commands for Bypass management, being possible to enable, disable and monitor the status of the bypass board;

Improvements in administration and product control during upgrade and update;

Improvements in summarization, dashboards, and reporting of the DPI service;

DPI now supports MPLS for Ethernet protocol;

Optimization of the security policy loading process.

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.5

Code	Description
UTM-122	Improvement on the return of the H.A. primary server.
UTM-140	Correction applied to the “configure-syslog” CLI command.
UTM-158	Correction applied to the notifications display and interface description in SD-WAN.
UTM-159	Correction applied to the nomenclature of the backup options.
UTM-288	Correction in editing personal information on the authentication portal.
UTM-289	Correction applied to the login in the authentication portal using email.
UTM-295	Correction applied to blocking subscription groups in the DPI Service.
UTM-301	Correction applied in the Threat Protection report.
UTM-302	Improvement on the DPI Services settings.
UTM-308	Improvement on the default values of SD-WAN performance indicators.
UTM-330	Correction applied to SD-WAN IP markup.
UTM-352	Correction applied in the text fields on Certificates, in the Authorities tab.
UTM-353	Correction applied to the upgrade in the service certificates.
UTM-354	Correction on RAS site-to-site IPSEC VPN connections IKEv1.
UTM-370	Corrections to the selection, filters and actions of the DPI Services window.
UTM-371	Correction applied to the enable and disable function on the Firewall Service.
UTM-386	Correction applied to the search system in Dictionaries.
UTM-394	Correction to the default value of the number of attempts to reconnect the IPSEC VPN in the event of a fall.
UTM-398	Correction in firewall summarization processes.
UTM-403	Correction in manual conversion of H.A.
UTM-412	Correction in the IP of the interface used during DNAT editing.
UTM-415	Correction to the IPSEC Monitor Disconnect Button.
UTM-419	Correction applied to the Logger service notifications.

UTM-420	Improvements to the IPSEC VPN Service, providing more flexibility in integrating with other market solutions.
UTM-422	Correction applied to the editing, activating and deactivating of the LAG interface.
UTM-423	Optimization in cluster convergence time.
UTM-427	Correction applied in the WEB browsing control without SSL inspection in policies.
UTM-428	Correction applied to the UTM log storage.
UTM-429	Correction applied to the session logoff.
UTM-430	Correction in the management and cleaning of the logs.
UTM-432	Correction in the application of SD-WAN functions.
UTM-438	Correction in WEB server application on OVAs wizard.
UTM-439	Correction in the UTM WEB Proxy.
UTM-440	Correction applied to the notifications that are displayed when authentication is performed on the UTM.
UTM-443	Correction in the display of the update-system command in the CLI.
UTM-444	Correction in SNAT rules.
UTM-448	Correction to the DPI Service initialization.
UTM-449	Correction in DPI Service preprocessors.
UTM-450 UTM-451 UTM-491	Improvements to changes in DPI service rules.
UTM-454	Correction in IPSec VPN event display.
UTM-455	Correction on Whitelist and Blacklist of DPI in transparent mode.
UTM-456	Correction applied to the HTTP port on Proxy.
UTM-457	Correction applied to the DPI configurations.
UTM-461	Correction applied to the SD-WAN process interruption.
UTM-462	Improvement SD-WAN performance.
UTM-463	Improved Global Management performance.
UTM-465	Correction in Cluster Slave synchronization.
UTM-467	Improvement on the execution time of the fwreload command on the CLI.
UTM-485	Correction applied in the reactivation of the Master cluster in H.A.
UTM-486	Correction applied to the cluster convergence in H.A.
UTM-493	Correction applied in the loading of UTM settings after backup restore.
UTM-510	Correction in Dynamic Selection application on the SD-WAN.
UTM-511	Correction on activation of services during the reactivation of the Master cluster in H.A.
UTM-513	Correction in SD-WAN activation when changing the order of interfaces.
UTM-514	Correction in the DHCP-Relay service.
UTM-518	Correction in activating the DPI Service signature block.
UTM-525	Correction on the temporary IPv4 policies.
UTM-529	Correction in the UTM authentication service.
UTM-530	Grammar Correction in System Administration.
UTM-532	Correction in the SD-WAN.
UTM-533	Correction in the WebFilter Service.
UTM-535	Correction applied in BLOCKBIT OS memory share.
UTM-536	Correction applied to the gsm-deployer service.

UTM-538 UTM-544	Correction in IP and DPI Service settings during migration from UTM 1.5.4 to 1.5.5.
UTM-540	Correction on the pre-enabling services after the update.
UTM-545	Correction applied to the creation of UTM service certificates.
UTM-547	Correction in the application of policies and configurations of device template via GSM in UTM 1.5.5.
UTM-552	Correction in the profile exclusion on the DPI Services.
UTM-554	Correction in sending the addresses to the DPI Service quarantine.
UTM-557	Improvement on the snapshot restoration.
UTM-559	Improvement to the notification and e-mail about UTM update status.
UTM-566	Improvement access to SSH and Web interface.
UTM-567	Correction applied to the system user notification service to improve UTM performance.
UTM-580	Correction applied in DPI service memory usage limitation.
UTM-581	Correction in the selection of objects used by Port Forwarding.
UTM-531 UTM-601 UTM-614	Correction applied to the upgrade.
UTM-615	Correction in deactivating and activating the DPI sensors.
UTM-616	Correction on SD-WAN activation after UTM restart.

Blockbit UTM version 1.5.4

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.4

Code	Description
UTM-14	Correction applied to the documentation in the SSO packet.
UTM-16	Correction applied to the DHCP Relay service.
UTM-20	Correction applied to Web Server CPU consumption.
UTM-98	Correction applied on the creation of static addresses on the DHCP interface.
UTM-99	Correction applied in rewizard execution.
UTM-100	Correction applied to the storage of database connections.
UTM-107	Correction applied when adding users to groups.
UTM-119	Correction applied when editing and saving SSL VPN settings.
UTM-123	Removal of unnecessary Multilink logs.
UTM-126	Correction in the WebProxy rules with SNI.
UTM-149	Correction applied in the domain ingress of the secondary H.A. server.
UTM-151	Correction applied in Site-to-site VPN communication.
UTM-154	Correction applied in the download of files through web filter with antimalware.
UTM-157	Correction applied to firewall logs of connections that pass through Web Proxy.
UTM-165	Correction applied to the visualization of values on BLOCKBIT UTM band control.
UTM-280	Correction applied to the renewal time configured on the DHCP.
UTM-283	Correction applied in the access connections of the internal system services.
UTM-287	Correction applied in the VPN redundancy with BGP dynamic routing.
UTM-290	Correction applied on the static host edit in DHCP.
UTM-294	Correction applied in the user search in the system authentication tab.
UTM-307	Correction applied to IP assignment in RAS IPSEC VPN.
UTM-315	Correction applied to the graphic interface of the network window.
UTM-317	Correction in the sorting of profiles in SD-WAN.
UTM-318	Correction applied on the DHCP SERVER service.
UTM-319	Correction applied on the Flood control logs.
UTM-322	Correction applied in editing Tunnel interfaces.
UTM-328	Correction applied in Site-to-site VPN navigation with compression enabled.
UTM-333	Correction in certificate validation on RAS VPN connection.
UTM-350	Correction in the retention of global IP reputation and geolocation settings while upgrading to version 1.5.
UTM-351	Correction applied in the H.A. authentication.
UTM-356	Correction applied in the package installation during upgrade to version 1.5.
UTM-368	Correction applied in the packet transmission during IPSEC VPN and GRE tunnel server traffic.

Blockbit UTM version 1.5.3

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.3

Code	Description
UTM-136	Correction applied on the web browsing logs.
UTM-137	Correction applied on MAC address objects.
UTM-147	Correction applied on the synchronism of group members.
UTM-150	Correction applied to Samba LDAP server authentication via captive portal.
UTM-156	Correction applied to the update of WEB policy members in the proxy.

Blockbit UTM version 1.5.2

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.2

Code	Description
UTM-5	New feature: TACACS + support for administration users.
UTM-6	New feature: TACACS + support for firewall users.
UTM-9	New feature: Multilink with Loadbalance supports new session persistence mode.
UTM-25	Correction applied to Samba LDAP server authentication.
UTM-26	Correction on sending firewall logs to remote syslog.
UTM-28	Correction on reading period/date objects by proxy.
UTM-84	New feature: CLI command to display the license number.
UTM-85	New feature: CLI command to display the version number.
UTM-86	New feature: CLI command to execute the product registration.
UTM-128	Correction applied on the background exportation of CSV reports.
UTM-129	Correction applied on the removal of MAC objects from the filtering rules.

Blockbit UTM version 1.5.1

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.5.1

- **Improvements in the Dashboard**
- **Improvements in the Event Viewer**
- **Improvements in the Policy Panel**
- **Security policies with option to disable logs**
- **Security policies with option to reject**
- **Tool to simulate traffic and locate policy**
- **Tool to detect conflicting policies**
- **Disk maintenance tool**
- **Multilink with support for multiple configuration profiles**
- **Multilink with LoadBalance and Spillover support**
- **Multilink with latency-based performance monitoring support**
- **Multilink with performance-based dynamic link balancing support**
- **LDAP integration for administration service**
- **Multiple packet inspection sensors with integrated services (IPS / ATP / APP)**
- **Deep packet inspection with support for Whitelist, Blacklist and Quarantine**
- **New VPN and Authentication Reports**

Blockbit UTM version 1.4.6

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.4.6

Code	Description
UTM-25	Correction applied to Samba LDAP server authentication.
UTM-26	Correction on sending the firewall logs to remote syslog.
UTM-27	Correction on policies that use objects with IP groups.
UTM-28	Correction on reading period/date objects by proxy.
UTM-29	New feature: HTTP / HTTPS option for same port in proxy, use accepted only in explicit mode.
UTM-84	New feature: CLI command to display the license number.
UTM-85	New feature: CLI command to display the version number.
UTM-86	New feature: CLI command to execute the product registration.
UTM-117	Correction on session synchronism and removal of the temporary script on the H.A.
UTM-140	Correction on the CLI command for syslog configuration.

Blockbit UTM version 1.4.3

The following table exhibits the improvements made* in the release of BLOCKBIT UTM version 1.4.3

Code	Description
BB-3060	Correction applied to the “LDAP” authentication system that wasn’t validating without domain information.
BB-12172	Correction applied to “WEB” policies in “HTTP” services different from those of standard ports, configured in the “Proxy” module.
BB-12224	Improvements made in the summarization of reports of the module “IPS”.
BB-12230	Correction applied to “Live Sessions” “Monitor” for established connections.
BB-12238*	Improvements made to a comprehensive inspection of packages, integrating ATP with IPS in the same sensor.
BB-12242 BB-12243	Improvements made in BLOCKBIT GSM’s integration API, with support for “Group” synchronisms.
BB-12320	Correction applied to changes in the portal settings, in the service responsible for the WEB interface.
BB-12322	Correction applied to the summarized “IPS” module that wasn’t generating reports correctly.
BB-12046	Correction applied to APP configurations of the “ATP” module when enabling integration with IPS.
BB-12324	Correction applied to the exhibition of blocked data in the “ATP” Report.
BB-12330	Correction applied to “IPS” initialization when enabled blocked type signatures.
BB-12338	Correction applied to changes of the value of the field “Gateway” in the general network settings.
BB-12342	Correction applied to the translation of the screen “Multiple Threat Edition” to English.
BB-12349	Correction applied to the summarization of the module “IPS”, which was looping.
BB-12353	Correction applied to the scanner’s SSL files from the “Antimalware” module.
BB-12393	Change applied to the default system security policies for a new default action of the rule.
BB-12396	Correction applied to the command “upgrade-blockbit”.
BB-12401	Correction applied to the SSO agent installed on the Windows Server 2016 version.
BB-12402	Improvements made to the process of securing the communication between the interface and the operating system.
BB-12403	Correction applied to restore when storage was configured via “SSH”.

*Firewall system will be reloaded, restarting all active connections.

Blockbit UTM version 1.4.0

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.4.0

IPv6 Support – Address Objects Added support for registration of IPv6 type address objects.
IPv6 Support – SSH and WEB Management Added access to the WEB and CLI management interface with IPv6 support.
IPv6 Support – Static addressing Added registration of physical type interface with IPv6 Support.
IPv6 Support – Dynamic addressing Added Registration of Dynamic type interface wit IPv6 Support.
IPv6 Support – Virtual Addressing Added Registration of virtual type interface with IPv6 Support.
IPv6 Support – NAT 66 Added NAT 66 over IPv6 Support.
IPv6 Support – NAT 64 Added NAT 64 over IPv6 Support.
IPv6 Support – NAT 46 Added NAT 46 over IPv6 Support.
IPv6 Support – DHCPv6 Added DHCP with IPv6 Support.
IPv6 Support – ICMPv6 Added ICMP protocol with IPv6 Support.
IPv6 Support – IGMPv3 Added IGMPv3 protocol with IPv6 Support.
IPv6 Support – Dynamic ports for FTP/ H323/SIP protocols Added IPv6 support for FTP/H323/SIP protocols.
IPv6 Support – Static Routing Added Static routing registration with IPv6 Support.
IPv6 Support – Dynamic routing (OSPFv3/RIP/BGP) Added Dynamic routing registration with IPv6 Support.
IPv6 Support – Multicast Routing (PIM-SM) Added Multicast routing (PIM-SM) registration with IPv6 Support.
IPv6 Support – Router Advertisement Added Router advertisement feature for IPv6.
IPv6 Support – Packet routing and filtering Added IPv6 support for routing and packet filtering.
IPv6 Support – Content Filter Added IPv6 support for the content filter.
IPv6 Support – QoS & Traffic Shapping Added IPv6 support for QoS & traffic shapping.
IPv6 Support – TCP MSS Added IPv6 Support for TCP MSS.
VPN SSL Site-to-Site Added Site-to-site SSL VPN feature.
VPN SSL Remote Access Added VPN SSL Remote Access feature.
VPN SSL Clientless Access Added VPN SSL Clientless Access feature.
VPN IPsec RAS Integrated with DHCP server Added VPN IPsec RAS integrated with DHCP server with IPv6 Support.

VPN IPsec RAS Integrated with RADIUS server Added VPN IPsec RAS integrated with RADIUS server to provide authentication.
VPN IPsec RAS access control by user group Added VPN IPsec RAS access control by group or user.
IPsec Compression Support VPN IPsec compression support.
Support for simultaneous tunnels per user (uniqueids) VPN IPsec RAS support for simultaneous tunnels per user.
IPv6 Support – Site-to-Site IPv6 over IPv6 VPN IPv6 Support at VPN site-to-site IPv6 over IPv6.
IPv6 Support – Site-to-Site IPv4 over IPv6 VPN IPv6 Support at VPN site-to-site IPv4 over IPv6.
IPv6 Support – Site-to-Site IPv6 over IPv4 VPN IPv6 Support at VPN site-to-site IPv6 over IPv4.
Jumbo Frames Support Added Jumbo frames support
Tunnel type interface Added Tunnel interface support.
Bridge type interface Added Bridge interface support.
PCAP packets Capture Added Monitor to capture network traffic through WEB interface with possibility of download in PCAP format.
SMTP and SMTPS proxy with antivirus scan support Added SMTP Proxy and SMTPS features with antimalware analysis support.
Proxy POP3 and POP3S with antivirus scan support Added Proxy POP3 and POP3S with antimalware analysis support.
FTP Proxy with antivirus scan support Added FTP Proxy feature with antimalware analysis support.
Invalid certificate verification Added Feature that validates invalid certificates by policy.
IP Reputation Filters by Policy Added Feature that allows definition “IP Reputation” filters by policy.
Geolocation Filters by Policy Added Feature that allows definition of “Geolocation” filters by policy.
Security protection filters by Policy Added Feature that allows definition of security protection filters by policy.
Transparent and passive IPS sensor Added Support for IPS feature for analysis in transparent and passive mode.
TCP Flood, UDP Flood and IP Spoofing protections Added Firewall feature for protections (TCP Flood, UDP Flood and IP Spoofing).
Social Captive Portal Added Users Portal Feature that allows authentication via social captive (Facebook, Google and Twitter).
Captive Portal Customization Added User portal customization feature.
Lock Page Customization Added “Web Filter” blocking page customization feature.
2FA per digital certificate Added Digital certificate Two-factor authentication.
Verification of valid certificates through revocation lists Added Revocation list of certificates for validation of certificates.
User Alert Notification Service Added Alert notification feature for the user.

Firewall and VPN authentication agent Added Firewall, SSL VPN and IPsec VPN Authentication Agents.
Management of Certification Authorities Added new resource to manage Certification Authorities.
Logical object grouping Added support for logical objects grouping, to create rules;
Integration with GSM Analyzer Added new feature for integration with BLOCKBIT GSM.
Monitor for System events and alerts via Syslog and SNMP Monitor of system events and alerts implemented, sent via syslog and SNMP.
Backup Storage via SSH Added feature for backup storage via SSH protocol added.
Feature Select Added feature that allows the administrator to enable or disable system services.
Centralized update management Added feature that allows the administrator to update every UTM connected to Manager.

Blockbit UTM version 1.3.11

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.3.11

Code	Description
BB-3500	Correction applied to the interface with security validations.
BB-3774	Correction applied to the “PROXY” service when SSL Inspection is enabled for government sites.
BB-3822	Correction applied to the “TIMELINE” Report, which did not display the data correctly.
BB-11301	Correction applied to the field “Description” of the policy, which did not display data when the report was generated from the policy description.
BB-11576	Correction applied to the SSO agent when installed on Windows server 2016.
BB-11951	Correction applied to the “SIP” module when automatically loaded.
BB-11979	Correction applied to the Monitor “Antimalware Quarantine”, which did not display all quarantine data.
BB-12040	Correction applied to the pagination at the “Active Directory” query for “Windows” and “LDAP” synchronizations.
BB-12046	Correction applied to the pagination at the “Active Directory” query for “Windows” and “LDAP” synchronizations.
BB-12068	Correction applied to the details of the view by application in the “TIMELINE” report.
BB-12139	Correction applied to validation of the authentication sessions on the SSO agent.
BB-12144	Correction applied in the process of activating the Master server as active in the service H.A.
BB-12148	Correction applied to the OS in the process of capture, filtering and analysis of packets.
BB-12373	Correction applied in the initialization process of the “Antimalware” service.
BB-12374	Correction applied to the “DNAT” registration form, whose response was “Invalid Field”.
BB-12375	Correction applied to the “IPS/ATP” module, which failed after system reboot.

Blockbit UTM version 1.3.10

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.3.10

Code	Description
BB-11230	Correction applied on the monitor “Live Sessions”, to filter by destination IP.
BB-11368	Correction applied on the monitor “Live Sessions”, to filter by any given policy.
BB-11874	New command added on CLI console “upgrade-blockbit” for version update.
BB-11981	Correction applied on the “Antimalware” feature, that was unstable.

Blockbit UTM version 1.3.9

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.3.9

Code	Description
BB-4243	Correction applied to destination IP filter performed on “Live Sessions” monitor.
BB-11012	Correction applied on the “ATP” “Report” view, in the cases no no threat was detected.
BB-11014	Correction applied on the “ATP” “Report” view for locked applications.
BB-11347	Correction applied on the “Antimalware” “Report” view and data displayed on quarantine.
BB-11378	Correction applied to access to “Captive Portal” via Android “OS”.
BB-11379	Correction applied in the operating system logs rotation.
BB-11465	Enhancements applied to the “ATP” application base.
BB-11487	Correction applied to the download of a Certificate Authority (C.A.) through user portal.
BB-11507	Correction applied on the user portal to remove files blocked by Antimalware.
BB-11508	Correction applied on “Multilink” service when a virtual network card is set up.
BB-11522	Correction applied to firewall reports maintenance.
BB-11527	Correction applied to set the “Multilink” service up on a H.A. environment.

Blockbit UTM version 1.3.8

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.3.8

Code	Description
BB-4264	Correction applied on model BB5, to synchronize data in H.A. environment.
BB-11278	Correction applied on controls by traffic or time quota in “WEB” policy.
BB-11303	Correction applied on IPS signatures base.
BB-11329	Improvements applied in the process of report storage, detailing when redirected to an external syslog server.

Blockbit UTM version 1.3.7

The following table exhibits the improvements made in the release of BLOCKBIT UTM version 1.3.7

Code	Description
BB-3716	Correction applied to the Command Line Interface – CLI console's "tcptrack" command.
BB-3961	Correction applied to the dictionary object search in field the "SSL Comon Name" during registration of a policy.
BB-4008	Correction applied to Web Filter log summarization, optimizing the use of the resource.
BB-4121	Correction applied to the Command Line Interface – CLI console's commands "debug-auth" and "debug-dhcp".
BB-4286	Correction applied on "(DNAT) Redirects" to edit a rule, preventing that the field "Source" is removed during saving.
BB-10882	Correction applied to remote certificates service. During importation, access to the "Captive Portal" page and "Web Filter" block screen was compromised.
BB-10927	Enhancements applied to the "Antimalware" service, to optimize the use of hardware resources.
BB-10953	Correction applied to the "Multilink" service. The registration of the object with test addresses was configured with FQDN (Fully Qualified Domain Name) addresses.
BB-10990	Correction applied on the access control settings for "Google Domains" at "Web Filter", when restricting access by users.
BB-11006	Correction applied to the report filling process of the ATP service.
BB-11143	Correction applied to the update process "IPS" and "ATP" bases when the license expired.
BB-11155	Correction applied to enable new "IPS" signatures. It was not loading correctly when applied on the system.
BB-11226	Correction applied to the WEB policies validation – control by Content-type.

NGFW - VIRTUAL APPLIANCE

Versions

VMware

KVM/Proxmox

Citrix/XenServer

VMware		
Appliance	**Version**	**CHECKSUM**
BBX40	NGFW 2.4.2	3b151a25f41e835b6535e66608a37bdd
	NGFW 2.4.1	2785cf3fa1e0d17b89f79914111af024
	NGFW 2.4.0	d37BBa3ec7c3c7802bdc51baeebf551b
	NGFW 2.3.0	4d73c4f471005878d0fb3ccf14e5ba39
	NGFW 2.2.2	2aa7a7024c08dddb3d1b5490363957f9
	NGFW 2.2.1	1bced8745eede68583a973e89adbe61a
	NGFW 2.2.0	70725d801822d4a29c2fe65bf122d3a3
	NGFW 2.1.1	0bc6c89736429f682c0c794c2c093c35
	NGFW 2.1.0	406012a0e8445a2a4d1e142e1c76f56d
	NGFW 2.0.13	326f3ff9938ff7f627b0ae5c9e9c388d
	NGFW 2.0.12	a6b718a73d44c1c9cd83aa9bfb803840
	NGFW 2.0.11	fb2f9ff0fd24fa032a7d124c88aa4833
	NGFW 2.0.10	76d47e411676c28082e47e88e35363ba
	NGFW 2.0.9	1d600deb4a7a536b99d05ad1ae49cbff
	NGFW 2.0.8	eb0acf9a6eb3acf73dba491f543c73cd
	NGFW 2.0.7	5a54316fb11530119f0871082c6f3c8d
	NGFW 2.0.6	f72f7474505ab38352df6e920a4e053d
	NGFW 2.0.5	2419939d9783ce0a8e8c877f61814dc6
	NGFW 2.0.4	d824e7525050a71912b0f19440231f72
	NGFW 2.0.3	546151a46d98c490493c1c017d43bc49
	NGFW 2.0.2	4d9bd44057d0b33a382bfd82fce5a229
	NGFW 2.0	75e6c64d51a010269ff587532cfeeb25
	NGFW 1.5.17	0adce898103664aad208cecb0d1727c3
	NGFW 1.5.15	25f9b29d21f9ba9689d346bd5028fd7c
	NGFW 1.5.14	a0995b5c3ee3548591aecd4bf487be3f
	NGFW 1.5.13	be359490b89d67e2ddfb74286353bfe9
	NGFW 1.5.12	0b1e4afd7894009ee2404356ed64f03b
	NGFW 1.5.11	1543b9a687ced2b13a31c7d662926694
	NGFW 1.5.7	d9ce7041c8f3897f4815bc119cddd981
	NGFW 1.5	2e8a08e623bda41a6349012d5247a5b4
	NGFW 1.4	99f77158b5a579778de5c553e60b38de

BB 5	NGFW 2.4.2	b7ffbfac2919a150be2b87fe454e5653
	NGFW 2.4.0	da0ddea0941eab48BB6855d69ec79103
	NGFW 2.3.0	e810116ef37ca309c114285c673a4604
	NGFW 2.2.2	659cec01a16f658ac4d0d27b4f9dd5d3
	NGFW 2.2.1	0b117ffb4fe96b38ad53f5b4b32349dd
	NGFW 2.2.0	643ea152a391fe0b6433c3ac79d55917
	NGFW 2.1.1	0190da8f7a2e8d1f53c74d88362e1546
	NGFW 2.1.0	4c01108d9291ae196f22b7e39a69d085
	NGFW 2.0.12	23f6c8504303fd407558914ea02d457d
	NGFW 2.0.11	d8490b30e050533db86609e8df090a4c
	NGFW 2.0.10	58ad4929a4f35f65510b39f8f016f483
	NGFW 2.0.9	3a50fcb739f1e2866a253762b7b09ed2
	NGFW 2.0.8	8b2d743fab7e4ffe74e7533c0932492d
	NGFW 2.0.7	997e9329245cb69dbd868b272f5c031e
	NGFW 2.0.6	BBe7e942927849 65bc46a72021ffe71f
	NGFW 2.0.5	0719bd1c7197f60880c348b6ff7e9964
	NGFW 2.0.4	5a43f36e8259af5241f7f19d9f529f3a
	NGFW 2.0.3	66c5613e084f246d334554783f97c761
	NGFW 2.0.2	6d793653c0d6c7a7ec9cb02873727fdb
	NGFW 2.0	18d489ee17a0d86d3531b5111001ca79
	NGFW 1.5.17	ca9377525891a3cdc1ecc2f875aafb7e
	NGFW 1.5.15	e95ce74baccf8b68007853cff9cb8b23
	NGFW 1.5.14	329c831adb046484898e465152c79a24
	NGFW 1.5.13	ece77885398efe9cc4524073e0e6ad8e
	NGFW 1.5.12	e272292172db3ee683d7160d06c88bee
	NGFW 1.5.11	94a3637305322ab3610b05129b0af001
	NGFW 1.5.7	a49394047c69c59e597c23ba0e85a855
	NGFW 1.5	35be07809cdBB9c1bde1eb6e99515da4
	NGFW 1.4	f9dda5076ae1424dd75857bf46BBbf61
	NGFW 1.3	6849c014efe8d572c47f229bc66123db
BBX80	NGFW 2.4.2	bd0caa7073e8c681ef594e46a98e4f3d
	NGFW 2.4.1	33ac636a149c4e58bb98e3dfdc1f94e3
	NGFW 2.4.0	db4f3b20628529739929aab7552e08e1
	NGFW 2.3.0	734b654fab2fe952ffd4b73124717936
	NGFW 2.2.2	83eab8e4780de5a2f042d827768ad46d
	NGFW 2.2.1	0def5d8208751440c3d2ac87eeba4173
	NGFW 2.2.0	b811a30b96bacc1c83abc05aaaecebc5
	NGFW 2.1.1	580889b6d5da646d67f9077e28168bc4
	NGFW 2.1.0	07dac6b8cf3ca0c4c18817f0d7a6c7a0
	NGFW 2.0.13	75c976223e5e976a989b776ab4fe78fd

	NGFW 2.0.12	097806e6a5f0a87f7fc952d3a6ebad20
	NGFW 2.0.11	c7a876b16faf73de4c508dbd0035aab3
	NGFW 2.0.10	1e620ff771aa394e280332aae7793cf4
	NGFW 2.0.9	19f509a5b6c13291aca4f365BB908056
	NGFW 2.0.8	840aef68228c48e1d742e862f4a649a3
	NGFW 2.0.7	b7e8ee9f2d1dd2c7311eb108259734d8
	NGFW 2.0.6	3b3a5d9ea5802b086ab226b83bfef7e4
	NGFW 2.0.5	3622e3b4b2672f824b0308b7eb13debc
	NGFW 2.0.4	92e9cd4fecd3670b34bc360d51ace6bc
	NGFW 2.0.3	a124031999afe1b00d7645f21e0f56ef
	NGFW 2.0.2	b8c1ec0e236ad7e2b8e658acf8bad331
	NGFW 2.0	6ecd5edd735045904fef20c6e2cfff9c
	NGFW 1.5.17	0b4b4af4b7c90e6427BB1404cfb8a3eb
	NGFW 1.5.15	3BBde3a3d3ced228793d730ace81acf4
	NGFW 1.5.14	ddbc7a36f064f3fb40f2d392ecb4d1c3
	NGFW 1.5.13	6ef0ad51739c7cf0632494392ac040f2
	NGFW 1.5.12	74927c2452643eb1895645b965c62f36
	NGFW 1.5.11	6b4d532d442d4a52b1614ba0e61459c1
	NGFW 1.5.7	5d619a3fe4ba06c7b75b96BB382c7955
	NGFW 1.5	1414874ffa35f43cBB27a36ddf71936e
	NGFW 1.4	1a8f59b1655b74039f941952221333ad
	NGFW 1.3	d498f8b4eb8b6a08fa273e34dff89046
BBX100	NGFW 2.4.2	ef259f7853349b02f08c9613ddae20f5
	NGFW 2.4.1	3934e887742175d937172f905880a8f7
	NGFW 2.4.0	29c65d57ff26addca246abfdeBB23650
	NGFW 2.3.0	f63fb08195756f173540c34917e1d65d
	NGFW 2.2.2	173a9491e7dcb4b8c4e2c2d2c26c2dbf
	NGFW 2.2.1	72bae5e63717e73bd48cb555d0872e75
	NGFW 2.2.0	1b35223374cf93d8217e7d74a1dbfc1c
	NGFW 2.1.1	228db3317296aa17f8fbad6473ab81ef
	NGFW 2.1.0	79e8769307132c854b29cb0a4d3cbf1b
	NGFW 2.0.13	43fbd2f4fc838bcda8a1791db20dda7f
	NGFW 2.0.12	1f43095c97c037fab32f854ec74c87b9
	NGFW 2.0.11	b02612aaec8ee44e0b8e4e13e8d09773
	NGFW 2.0.10	9433e8c9190ab2a697f00920b33cd51e
	NGFW 2.0.9	399acae962b312879639102785001502
	NGFW 2.0.8	8c92dd9eda540BBcad7bf8f109969bcc
	NGFW 2.0.7	430ff1cdd371679c2a3f43f915d2778d
	NGFW 2.0.6	f9ea12a5d0e6599eb9b63eece82954b3

BBX200	NGFW 2.4.2	4ff58b62aab87a081dd645cfc203ccdf
	NGFW 2.4.1	1a11d578d68557ee18701f2ee08ef182
	NGFW 2.4.0	b4c0a4a93f719be66ec529508e8346d6
	NGFW 2.3.0	f4bd5940e4092840854de68d4a577fd9
	NGFW 2.2.2	fe993fd42a45ba17ff9bac6d0a1415f9
	NGFW 2.2.1	c3cd94fb13762be958c0caba42cf0dca
	NGFW 2.2.0	c110dc04974237f66d43ffe1e8fbe6cd
	NGFW 2.1.1	b491869f12cBB96157bf34d860d3da61
	NGFW 2.1.0	18e08b7fc7881c24c54e80e54c5f860e
	NGFW 2.0.13	96ea2d806c20446db675cafd99BBe49b
	NGFW 2.0.12	1954eac8dada55149b27be6b060af2ad
	NGFW 2.0.11	609dd155a9f802062bceae4e59973a32
	NGFW 2.0.10	8b1b49b9c8cdc3588a5d2b4466506500
	NGFW 2.0.9	07c9e5d1c9676eda094df2a08ff55d1c
	NGFW 2.0.8	4eed9198b5f68a57d8c6798858f64124
	NGFW 2.0.7	0f393eef351cd742e43b7525460bfe9d
	NGFW 2.0.6	e357f28db03bd58674f918411c051fe8
	NGFW 2.0.5	ce5a6dd5d00757b5f6a11930fdccb7e4
	NGFW 2.0.4	7c8f17c47c25d7c38c3653ef006e0dd2
	NGFW 2.0.3	0b16d4b396b52a067536f0615483f134
	NGFW 2.0.2	c2cfb7ec5e7f3de05a2825145da7e3cb
	NGFW 2.0	d329d4622b22046547d107BBb5249a8b
	NGFW 1.5.17	ab65645edd1d298867860689915df27f
	NGFW 1.5.15	5226e12b772bcacfe34bd079ead7d8d5
	NGFW 1.5.14	860c78e2c8bab714ca16183e4471a521
	NGFW 1.5.13	9d8cad1e43c04e3e657cded3c1e4fc55
	NGFW 1.5.12	3a379c24867e8c9a6e7acf473a433f1e
	NGFW 1.5.11	227410bffeab4d16ee6fa0e5e3dc4e1e
	NGFW 1.5.7	2d949f773dc393220e5b68792f190512
	NGFW 1.5	214705e33cf7ff85d08a805ef88187ed
	NGFW 1.4	69bafd8e8f5722f0a913ea2d378d2e4b
	NGFW 1.3	bda52a78ba23a3a847b96ed884fd1dc0
	NGFW 2.4.2	23dcbbc6e8eb9a65f4e403578e229077
	NGFW 2.4.1	4a182c94eea5bc214075bfbe36e0d2d0
	NGFW 2.4.0	774b54be1baa5c42cc0544327e34fb26
	NGFW 2.3.0	479dd2d1b0e138df19480bc2503c8f48
	NGFW 2.2.2	`a4b35d839abb9dd151a35f2d62ebe1fe`
	NGFW 2.2.1	9167de6efa4a1a89751b716b4c4f5f73
	NGFW 2.2.0	e61120b7fe57879f734ca1858985e159

BBX700	NGFW 2.1.1	03d1a4e05b592f3ae5cc5b992f032530
	NGFW 2.1.0	bda5dc7df7c0cf0affc4e34e6d66b6ee
	NGFW 2.0.13	c0f204b382b80cf727b4e156e4b7071c
	NGFW 2.0.12	cc39a543e260efa24927e350a4031ead
	NGFW 2.0.11	d4d3f52501b54f280fdfc8ae6ce9079a
	NGFW 2.0.10	770282650013BB69762994d937248244
	NGFW 2.0.9	a4819c5c871b6730eb7954d391e72c3d
	NGFW 2.0.8	fe44ee4725de9797ab30b2d8d2d38761
	NGFW 2.0.7	37da39d9f49f27b138ac7a7a307f5058
	NGFW 2.0.6	7df3fc6ffaef62299b7a4bc1577e159c
	NGFW 2.0.5	fba8e0ac7e0f648f6a134c3835d6870d
	NGFW 2.0.4	c5641d540161b23d463830a282270a84
	NGFW 2.0.3	51b61aa663879c8dff5919375c83f4f9
	NGFW 2.0.2	0b726c6eb18b9b9b14b429767894bdb1
	NGFW 2.0	9bd258c16d8ed0f2353b5a5fdc6d184c
	NGFW 1.5.17	c58c1bc603d5107dfa0391c6014312BB
	NGFW 1.5.15	e5cfe0cb6ed49373f0387b134f783f4c
	NGFW 1.5.14	57cb382ff1fd51c1fa92adee2542a82f
	NGFW 1.5.13	a227BB367e3cf4850fcd8141fa32f180
	NGFW 1.5.12	506746ed7065e31ece3e999bd1908934
	NGFW 1.5.11	ac9660b3eb586db90adcd5986e48cfc5
	NGFW 1.5.7	deabeee59499015042da7a2620926120
	NGFW 1.5	1883cde424225bf4b92f9a183f8e6606
	NGFW 1.4	f359856448963d81162bf1a0dec5ee49
	NGFW 1.3	05f11c9a3e07d20ff4482f6359886d5c
BBX1500	NGFW 2.4.2	7854dd1cb19b7818a69bd0c4ab65a757
	NGFW 2.4.1	021089199ab89ed6325c4f4a371ac969
	NGFW 2.4.0	438d2688d53afe981fbd2ef4b467fdf6
	NGFW 2.3.0	d0bfaf36034b1817e3416b58beBB0379
	NGFW 2.2.2	2bf985eb684d6b364f8a4fbd6e0e9d2e
	NGFW 2.2.1	f7219d763c0b8ce143852a659fac7738
	NGFW 2.2.0	2cb50367af1cfcde1008e836042c4a76
	NGFW 2.1.1	c3fc1BB0e82868223338d1187d4320b3
	NGFW 2.1.0	d8ee6eb5429785a40df4d7663a41f42b
	NGFW 2.0.13	59f1414a1890f127b69f21112ceaf4ed
	NGFW 2.0.12	5c06cff914b99564e08818e9b1451afd
	NGFW 2.0.11	ddc952BBe21ac1a16d8cff767bdcabf3
	NGFW 2.0.10	6f21649aa26e59e274ec6aefa56bc673
	NGFW 2.0.9	3b499e496c99f97b3bfa90fd08d4e60f
	NGFW 2.0.8	62f76452a3dcb3ecfd3d07d5c0cde14f

	NGFW 2.0.7	2abc8012f4e900e538dd94b361d29325
	NGFW 2.0.6	3d5d94b48fe744e3ed3167fc1db4163fb
	NGFW 2.0.5	31e3e6c57aecf6de76d22bf9d903085f
	NGFW 2.0.4	3b336812acaf8f1f44919eafdf354087
BBX3000	NGFW 2.4.2	93ceb8e55db2279343d127e442a14781
	NGFW 2.4.1	85aa45fd1c628aa47aeee4bbb5565560
	NGFW 2.4.0	700720e79345e7ef71263bc32a27e3cc
	NGFW 2.3.0	3382c6758507fd8916085b1edbaefbc9
	NGFW 2.2.2	215f3412f6b00ef707f7f1cfcc613eb2
	NGFW 2.2.1	14437856dc2e1dabf683268665a6a1fc
	NGFW 2.2.0	abd305fd0732f0b8df9daf5c4a0c1aac
	NGFW 2.1.1	593596188c0456643e0cecd3befaa5e4
	NGFW 2.1.0	9fba8df691dcbdfadd90f221ecfcad80
	NGFW 2.0.13	886533895bc8e4654eb8434e730d5c2e
	NGFW 2.0.12	b6ed4f357968405eca15f91661410816
	NGFW 2.0.11	e2d4be61d95c3490472c5d3bc0b7637d
	NGFW 2.0.10	ed409e5840fc482b38f089ced13423df
	NGFW 2.0.9	bab1935216d205848668f6b47a95ae36
	NGFW 2.0.8	f2475dda39b77b60cfc296c52c5500aa
	NGFW 2.0.7	4a32cff81d368a45a92bf2b8603f9be1
	NGFW 2.0.6	aca26dc7102b5b13c0c4893464c46e3e
	NGFW 2.0.5	f5c476f7bd1d2e010183173d696f8909
	NGFW 2.0.4	b801bc064d135570cd91151721173ae7
	NGFW 2.0.3	3d23675646eaa9b6034affd9372b75f5
	NGFW 2.0.2	0ee1df62ae1b85395c3816740aff8fca
	NGFW 2.0	e97198877ad3eced6cc470d9004d5f3e
	NGFW 1.5.17	17a6e2939dcd0b331deb1f5bd4c00283
	NGFW 1.5.15	9c110b43eef6d18b6d152080d96452a3
	NGFW 1.5.14	c0333aeb76fec8d8d220bd09527f4113
	NGFW 1.5.13	a990d5bff1aaeee3bda8338b0ff38384
	NGFW 1.5.12	ae5c8adc42c0e92390839c8162358697
	NGFW 1.5.11	4536d140d04d9a1830e080d51d6ccBB5
	NGFW 1.5.7	08c1ec3a9cd55bd9cab50def21c4d7a6
	NGFW 1.5	2482a46686258ad3064ff7d3eeb15cf2
	NGFW 1.4	01dcf00e70bfc95a23d023d455e28be4
	NGFW 1.3	fb5621cb1051c4625f5a10f2d8315936
	NGFW 2.4.2	2e67f0469b8fd37084c8f292de88cd18
	NGFW 2.4.1	0a42f17026cb5de346fa552ad8abee6d
	NGFW 2.4.0	63d9aaac60b98f76fce1c575dd65f065

BBX3600 **BBX4200** **BBX5000**	NGFW 2.3.0	b317002c77e9fd6f7eb6ebc0071c1ad8
	NGFW 2.2.2	4c992ae38ba9dcd1305b5b4454332430
	NGFW 2.2.1	d379ea84d5d1e346671b23ca0603870e
	NGFW 2.2.0	a523c9e3eBB265273a6eb0f528a717da
	NGFW 2.1.1	35129ebf3245b885dc3ca18795cBB197
	NGFW 2.1.0	39a060ef77d15afa5a7b52eb85bc771c
	NGFW 2.0.13	3f80097fb5714b2ccc4a2172e48b23c9
	NGFW 2.0.12	1eb331662791d431b84ecf3a8d1afc72
	NGFW 2.0.11	38436a4dcd73186b8fa934779c684575
	NGFW 2.0.10	ccf8c75edc1b3a5b75c899fe8ebcde3d
	NGFW 2.0.9	2bcda21e3ca963a3ee2d03c8bcc9f98c
	NGFW 2.0.8	45c6ae7ecc02e841f378d17114d50dce
	NGFW 2.0.7	854f6538f52e157d247930e8c54dfbea
	NGFW 2.0.6	2a4f177c62769f9dd831250c0836e111
	NGFW 2.0.5	855c885a3f54e97a67ef0f565062424c
	NGFW 2.0.4	21afba1dd50d8f22768f0f0986e82669

Topo da Página

KVM/Proxmox		
Appliance	**Version**	**CHECKSUM**
BBX80	NGFW 2.4.2	63416091c2be1e630be5f71ed1a5c6a6
	NGFW 2.4.1	a2102d85a9548cbda69af863c5129b37
	NGFW 2.4.0	46c23da075e04cd01d06e967024a5427
	NGFW 2.2.2	`9199cef6dfb5c04d114915f96d07e28c`
	NGFW 2.2.1	69da2a5cc0cf1d92ce1e3204b5388275
	NGFW 2.2.0	168c5041702f39f44BBc11188245a13f
	NGFW 2.1.1	27d34b2aa4969f72183853839e7f1033
	NGFW 2.0.13	d93fd541e368cd9d47fa474ddc20ca93
	NGFW 2.0.12	a81a50381bd35aea8d87e1d092d8e5ea
	NGFW 2.0.11	ae088f07eeba8b40e1b0cfeb5ed05a46

Topo da página

Citrix/XenServer		
Appliance	**Version**	**CHECKSUM**
BBX40	NGFW 2.4.2	0ef297ea72befef99bc8419f881bb712
	NGFW 2.4.1	2785cf3fa1e0d17b89f79914111af024
	NGFW 2.4.0	d37BBa3ec7c3c7802bdc51baeebf551b
	NGFW 2.3.0	4d73c4f471005878d0fb3ccf14e5ba39
	NGFW 2.2.2	1bced8745eede68583a973e89adbe61a
	NGFW 2.2.1	71160d3374dfb1e50aefb846be949f8a

	NGFW 2.2.0	70725d801822d4a29c2fe65bf122d3a3
	NGFW 2.1.1	0bc6c89736429f682c0c794c2c093c35
BB 5	NGFW 2.4.2	b7ffbfac2919a150be2b87fe454e5653
	NGFW 2.4.0	da0ddea0941eab48BB6855d69ec79103
	NGFW 2.3.0	e810116ef37ca309c114285c673a4604
	NGFW 2.2.2	659cec01a16f658ac4d0d27b4f9dd5d3
	NGFW 2.2.1	0b117ffb4fe96b38ad53f5b4b32349dd
	NGFW 2.2.0	643ea152a391fe0b6433c3ac79d55917
	NGFW 2.1.1	0190da8f7a2e8d1f53c74d88362e1546
BBX80	NGFW 2.4.2	bd0caa7073e8c681ef594e46a98e4f3d
	NGFW 2.4.1	33ac636a149c4e58bb98e3dfdc1f94e3
	NGFW 2.4.0	db4f3b20628529739929aab7552e08e1
	NGFW 2.3.0	734b654fab2fe952ffd4b73124717936
	NGFW 2.2.2	83eab8e4780de5a2f042d827768ad46d
	NGFW 2.2.1	0def5d8208751440c3d2ac87eeba4173
	NGFW 2.2.0	b811a30b96bacc1c83abc05aaaecebc5
	NGFW 2.1.1	580889b6d5da646d67f9077e28168bc4
BBX100	NGFW 2.4.2	ef259f7853349b02f08c9613ddae20f5
	NGFW 2.4.1	3934e887742175d937172f905880a8f7
	NGFW 2.4.0	29c65d57ff26addca246abfdeBB23650
	NGFW 2.3.0	f63fb08195756f173540c34917e1d65d
	NGFW 2.2.2	173a9491e7dcb4b8c4e2c2d2c26c2dbf
	NGFW 2.2.1	72bae5e63717e73bd48cb555d0872e75
	NGFW 2.2.0	1b35223374cf93d8217e7d74a1dbfc1c
	NGFW 2.1.1	228db3317296aa17f8fbad6473ab81ef
BBX200	NGFW 2.4.2	4ff58b62aab87a081dd645cfc203ccdf
	NGFW 2.4.1	1a11d578d68557ee18701f2ee08ef182
	NGFW 2.4.0	b4c0a4a93f719be66ec529508e8346d6
	NGFW 2.3.0	f4bd5940e4092840854de68d4a577fd9
	NGFW 2.2.2	fe993fd42a45ba17ff9bac6d0a1415f9
	NGFW 2.2.1	c3cd94fb13762be958c0caba42cf0dca
	NGFW 2.2.0	c110dc04974237f66d43ffe1e8fbe6cd
	NGFW 2.1.1	b491869f12cBB96157bf34d860d3da61
	NGFW 2.4.2	23dcbbc6e8eb9a65f4e403578e229077
	NGFW 2.4.1	4a182c94eea5bc214075bfbe36e0d2d0
	NGFW 2.4.0	774b54be1baa5c42cc0544327e34fb26

BBX700	NGFW 2.3.0	479dd2d1b0e138df19480bc2503c8f48
	NGFW 2.2.2	a4b35d839abb9dd151a35f2d62ebe1fe
	NGFW 2.2.1	9167de6efa4a1a89751b716b4c4f5f73
	NGFW 2.2.0	e61120b7fe57879f734ca1858985e159
	NGFW 2.1.1	03d1a4e05b592f3ae5cc5b992f032530
BBX1500	NGFW 2.4.2	7854dd1cb19b7818a69bd0c4ab65a757
	NGFW 2.4.1	021089199ab89ed6325c4f4a371ac969
	NGFW 2.4.0	438d2688d53afe981fbd2ef4b467fdf6
	NGFW 2.3.0	d0bfaf36034b1817e3416b58beBB0379
	NGFW 2.2.2	2bf985eb684d6b364f8a4fbd6e0e9d2e
	NGFW 2.2.1	f7219d763c0b8ce143852a659fac7738
	NGFW 2.2.0	2cb50367af1cfcde1008e836042c4a76
	NGFW 2.1.1	c3fc1BB0e82868223338d1187d4320b3
BBX3000	NGFW 2.4.2	93ceb8e55db2279343d127e442a14781
	NGFW 2.4.1	85aa45fd1c628aa47aeee4bbb5565560
	NGFW 2.4.0	700720e79345e7ef71263bc32a27e3cc
	NGFW 2.3.0	3382c6758507fd8916085b1edbaefbc9
	NGFW 2.2.2	215f3412f6b00ef707f7f1cfcc613eb2
	NGFW 2.2.1	14437856dc2e1dabf683268665a6a1fc
	NGFW 2.2.0	abd305fd0732f0b8df9daf5c4a0c1aac
	NGFW 2.1.1	593596188c0456643e0cecd3befaa5e4
BBX3600 **BBX4200** **BBX5000**	NGFW 2.4.2	2e67f0469b8fd37084c8f292de88cd18
	NGFW 2.4.1	0a42f17026cb5de346fa552ad8abee6d
	NGFW 2.4.0	63d9aaac60b98f76fce1c575dd65f065
	NGFW 2.3.0	b317002c77e9fd6f7eb6ebc0071c1ad8
	NGFW 2.2.2	4c992ae38ba9dcd1305b5b4454332430
	NGFW 2.2.1	d379ea84d5d1e346671b23ca0603870e
	NGFW 2.2.0	a523c9e3eBB265273a6eb0f528a717da
	NGFW 2.1.1	35129ebf3245b885dc3ca18795cBB197

Back to top

NGFW - INSTALLATION FILES

Version	CHECKSUM
NGFW 2.4.2	9ea9cd62681097bf2833d5e897ec98fa
NGFW 2.4.1	65b7c5217ed2fa1f1561dfc16f426a84
NGFW 2.4.0	348f8c89444981ca177603876bfdcde1
NGFW 2.3.0	1e7e82dd2b94bbe1fd1320d0c84d25a5
NGFW 2.2.2	383bc12bf8b1176b38f00ea69a63bc8a
NGFW 2.2.1	306bcaee1309d176c31c50441055170c
NGFW 2.2.0	24d7af6a12540354a25548f451f8eedb
NGFW 2.1.1	61f305e41d987ee48d99f76182a63147
NGFW 2.1.0 (Series F)	7ce03715bcc473c9d11852708612c0ed
NGFW 2.1.0	7c29491589f55000c173d2c624d85e38
NGFW 2.0.13	b02e2bfe5a39d2f45229ff8969daf5ef
NGFW 2.0.12	f7cf0ae926176c67f54d939fb5f0e6ba
NGFW 2.0.11	63f77b1172239ddd6edfee4d3dd6e38f
NGFW 2.0.10	309d8b5439b5934e1151b342305d9068
NGFW 2.0.9	61f1a36cc949a4988c5de751e60a450b
NGFW 2.0.8	39f267997aa53755454e5351e2339342
NGFW 2.0.7	9d73bd33f9d7f08b2d4d6988d9943397
NGFW 2.0.6	ca1a1b6632cedfcd47087636521385cc
NGFW 2.0.5	a9e2539d3ce50029607212ca5105cea5
NGFW 2.0.4	e96ec3babedc247a2a2c03864c1b98f0
NGFW 2.0.3	25245ad625c2f3ef70f6aa978a9ecda3
NGFW 2.0.2	730fd0f42886bf16f327b8b05127f7ea
NGFW 2.0	2fef31146a4022f44567be2ff43401a2
NGFW 1.5.17	b0f72a7d0dc186e609efa340ec878ede
NGFW 1.5.15	b39cb1a133b667bc6c552f6de31fcf5d
NGFW 1.5.14	b426a09d417a7526aee86c98031094e9
NGFW 1.5.13	fb85f1641ebe03dfbb90f78d05616243
NGFW 1.5.12	1f70c3fb3bad08e4ab934cb2e97374e2
NGFW 1.5.11	751f73aa839726ae3c0eb0e7f2ef69aa
NGFW 1.5.7	cd12bc78354e5a2277d58b1216bae425
NGFW 1.5.6	149e8536c41aa42821b7b28c086832e6
NGFW 1.5.5	7732b0b8d4623561df44111a8bdcda95
NGFW 1.5.4	c039834711d84b04a67cb001c65b634d
NGFW 1.4	5ce19cc158bd7d635110327e851aecf0
NGFW 1.3	2922c115de3d9482c0bd4382c1953c4e

How to Upgrade in Blockbit NGFW

The upgrade of Blockbit NGFW is an important process to ensure that your security environment is updated with the latest features and improvements. Below are the steps for a safe and efficient upgrade.

Key Steps:

1. **Choose an Appropriate Maintenance Window:** Perform the upgrade outside of production hours, preferably during a maintenance window, to minimize impacts on operations.
2. **Have a Recovery Plan:** Ensure you have a recovery plan in case of any unforeseen issues:
    - Physical access to the appliance or virtual machine;
    - Firmware on a USB drive or OVA image.
3. **Perform a Complete Backup:** In addition to generating a snapshot, we recommend creating a complete backup of the system on an external device.
4. **Execute the Upgrade:** Start the upgrade process following the instructions from the management interface or CLI.
5. **System Reboot:** After completing the upgrade, it is crucial to reboot the system to ensure the new features are fully applied and functioning correctly.
6. **Post-Upgrade Validation:** After the upgrade, validate all critical functionalities, such as firewall policies, VPN, and SSL inspection.
7. **Create a New Snapshot:** Once you confirm that everything is functioning correctly in the new version, create a new snapshot to ensure an updated restoration point. For more information, please refer to this page.

Requirements:

This procedure is validated for Blockbit NGFW version 2.X.

Access to the console will be necessary for this procedure.

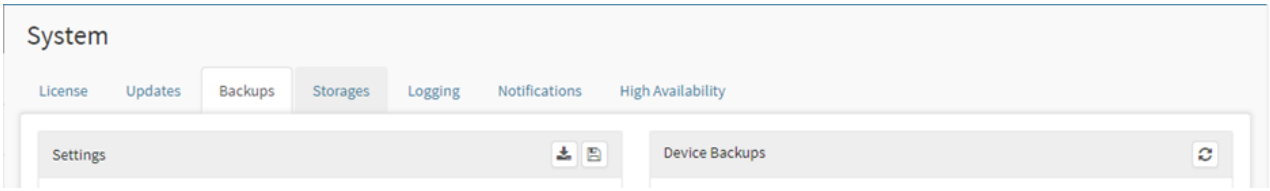
Content:

How to Upgrade Blockbit NGFW- Generate a system backup

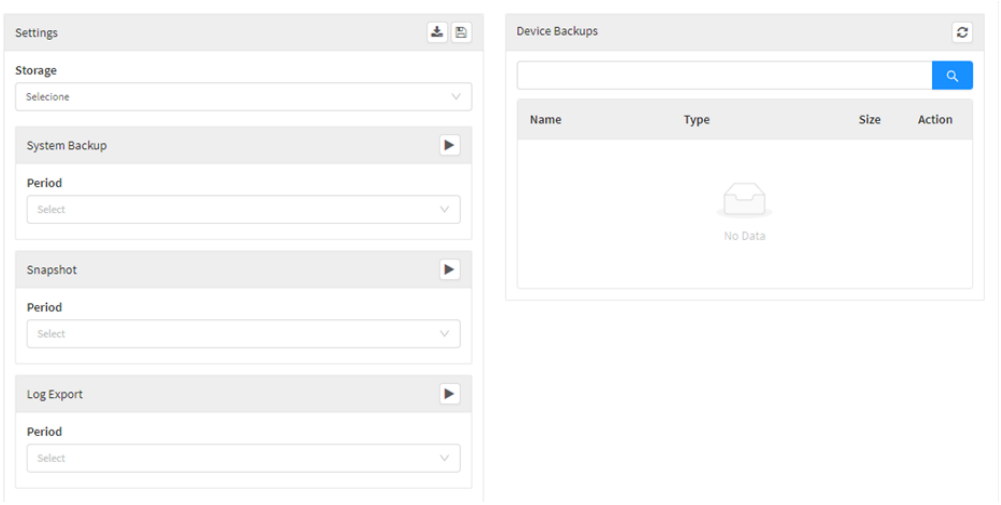
Before configuring the backup service, you will need to configure the Storage service.

To access backup management, click on "Backups".

To find a device, use the research bar and click on refresh [ ].



This screen will appear:

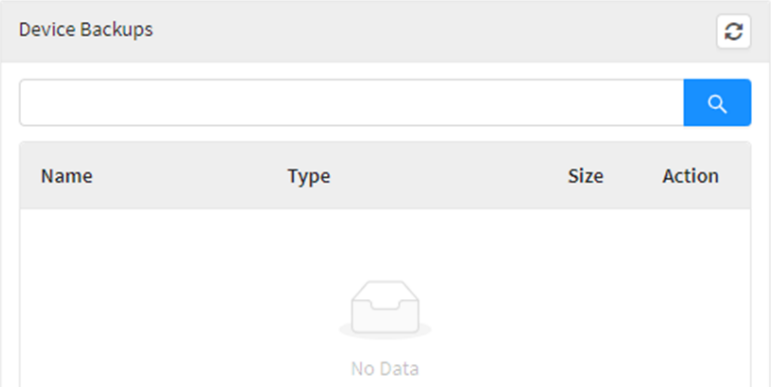


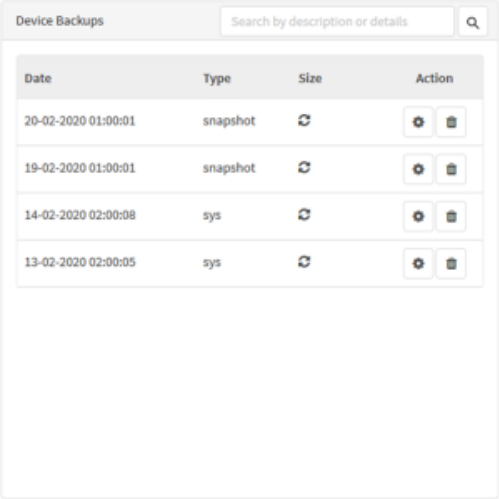
This screen has the following panels:

- Settings;
- Device Backups.

How to Upgrade Blockbit NGFW- Generate a system backup - Device backups

In this area, the system returns the list of backup files available in the selected storage configured in the settings panel.





- **Date:** date and time of the backup system;
- **Type:** type of backup;
- **Size:** size of the backup. The size is displayed after clicking the button [ ];
- **Action:** includes two action buttons:
  - **Restore [ ]:** to restore the backup;
  - **Delete [ ]:** to delete the backup from storage.

All backups are saved in "encrypted" mode. The algorithm used depends on the integrity key generated by the "Configuration Wizard" during the original installation of the backup/restore encryption and decryption system.

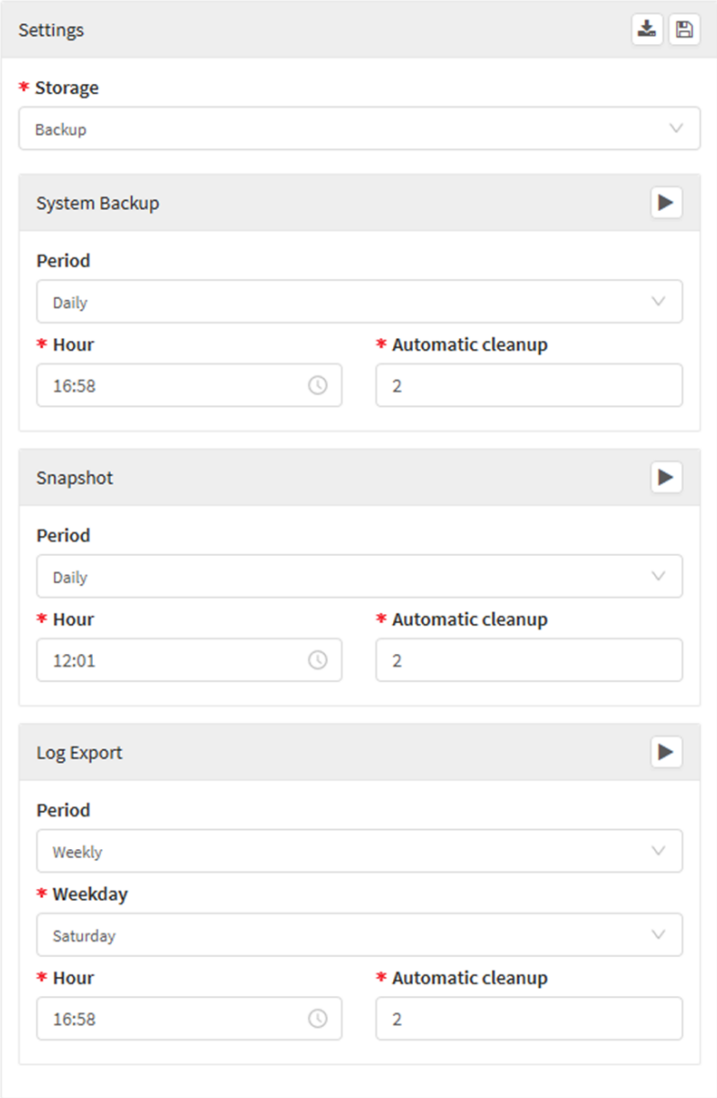
To restore a backup, the same integrity key from the previous installation is required, which can be found in **Settings - Administration - Sessions > Integrity**.

All backups are saved in "encrypted" mode. The algorithm used depends on the integrity key generated by the "Configuration Wizard" during the original installation of the backup/restore encryption and decryption system.

To restore a backup, click on the icon [ ] and confirm.

How to Upgrade no Blockbit NGFW- Generate a system backup - Settings

In this panel, you configure the backup service and define the storage location. The system allows you to perform system backups, snapshot backups, and log exports.



Settings

- **Storage:** Defines the location where backups will be stored. E.g., Backup;

System Backup

- **Period:** Defines how often the system backup will be performed:
  - **Daily:** daily;
  - **Weekly:** weekly.
- **Hour:** Defines the time when the backup will be performed. E.g., 12:01;
- **Automatic Cleanup:** Defines the number of backups to be stored in the storage. E.g., 2.

Snapshot

- **Period:** Defines how often the snapshot backup will be performed:
  - **Daily:** daily;
  - **Weekly:** weekly.
- **Hour:** Defines the time when the backup will be performed. E.g., 12:01;
- **Automatic Cleanup:** Defines the number of snapshot backups to be stored in the storage. E.g., 2.

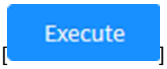
Log Export

- **Period:** Defines how often the log export will be performed:
  - **Daily:** daily;
  - **Weekly:** weekly.
- **Hour:** Defines the time when the backup will be performed. E.g., 12:01;
- **Automatic Cleanup:** Defines the number of log backups to be stored in the storage. E.g., 2.

Configure the **SYSTEM BACKUP** option in a **Remote Storage** or **USB drive**.

To create a backup immediately, click the button [].

The following message will be displayed:

Click on [] to create the backup.

The backup is generated in encrypted mode. To restore it, the same integrity key from the previous installation is required, found in **Settings - Administration - Sessions > Integrity**.

How to Upgrade Blockbit NGFW - System update

Always make a COMPLETE BACKUP of the latest system version and reports, and save it in a secure location before any update or upgrade.

Before updating, follow these steps:

1. Access the CLI and run the command **[update-system]**.
2. The Blockbit NGFW should be on the latest version and build.
3. Install the update package for NGFW 2.4.2 on the Hotfixes page.
4. Install HF 92. Run the command **[update-system]** again.

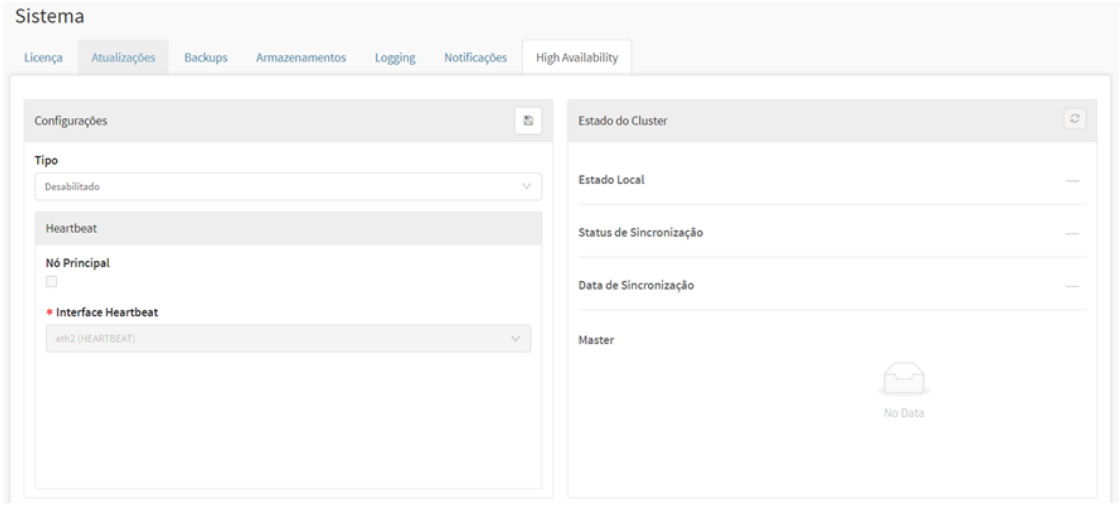
To confirm the update, use the command:

`[show-version]`

Click here to check the update in a cluster environment.

How to Upgrade Blockbit NGFW- System update - Update in a cluster environment

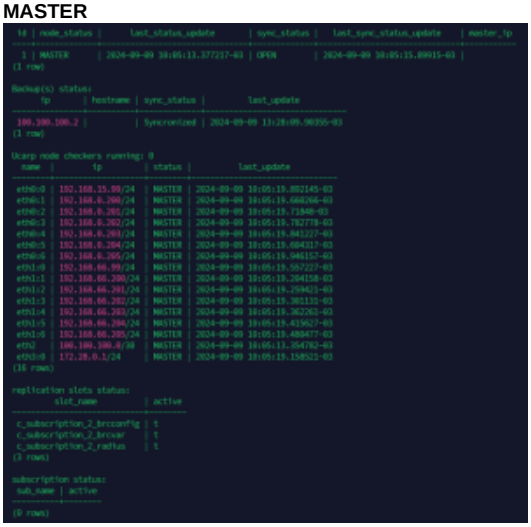
To ensure the availability of the environment, follow the steps below in sequence:



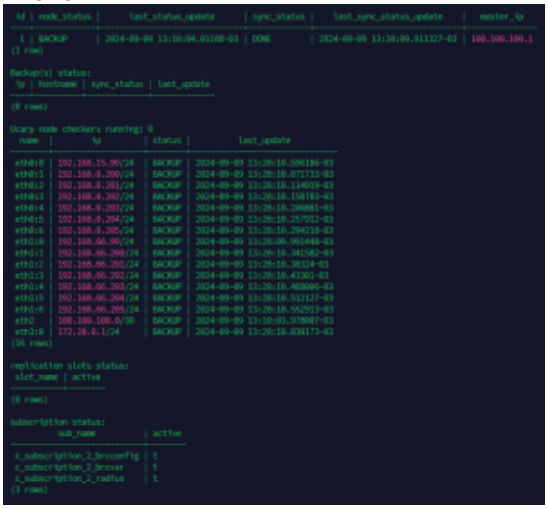
1. Disable the cluster on both Nodes (Master and Backup);
2. Perform the Upgrade (all previous steps);
3. Confirm that both nodes are on the same build (`show-version`);
4. Activate the cluster on the Master Node;
5. Monitor the Logs to ensure the Cluster is active: `[debug-cluster -t -s first_line]` and `[debug-cluster -w]`;
6. Activate the cluster on the Backup node;
7. Monitor the Logs to check if synchronization occurred: `[debug-cluster -t -s first_line]` and `[debug-cluster -w]`.

The expected result is:

MASTER



BACKUP


id | node_status | last_status_update | sync_status | last_sync_status_update | master_ip
1 | BACKUP | 2024-09-09 13:16:04.01188-03 | DONE | 2024-09-09 13:28:09.911327-03 | 180.106.160.1
(1 row)
Backup(s) status:
ip | hostname | sync_status | last_update
(0 rows)
Usarp node checkers running: 0
rname | ip | status | last_update
eth0:0 | 192.168.15.99/24 | BACKUP | 2024-09-09 13:28:10.596186-03
eth0:1 | 192.168.0.200/24 | BACKUP | 2024-09-09 13:28:10.071733-03
eth0:2 | 192.168.0.201/24 | BACKUP | 2024-09-09 13:28:10.134039-03
eth0:3 | 192.168.0.202/24 | BACKUP | 2024-09-09 13:28:16.158783-03
eth0:4 | 192.168.0.203/24 | BACKUP | 2024-09-09 13:28:10.206681-03
eth0:5 | 192.168.0.204/24 | BACKUP | 2024-09-09 13:28:10.257922-03
eth0:6 | 192.168.0.205/24 | BACKUP | 2024-09-09 13:28:10.294218-03
eth1:0 | 192.168.66.99/24 | BACKUP | 2024-09-09 13:28:00.901448-03
eth1:1 | 192.168.66.200/24 | BACKUP | 2024-09-09 13:28:10.341582-03
eth1:2 | 192.168.66.201/24 | BACKUP | 2024-09-09 13:28:10.38314-03
eth1:3 | 192.168.66.202/24 | BACKUP | 2024-09-09 13:28:10.43302-03
eth1:4 | 192.168.66.203/24 | BACKUP | 2024-09-09 13:28:10.468006-03
eth1:5 | 192.168.66.204/24 | BACKUP | 2024-09-09 13:28:10.512127-03
eth1:6 | 192.168.66.205/24 | BACKUP | 2024-09-09 13:28:10.552913-03
eth2 | 100.100.100.0/30 | BACKUP | 2024-09-09 13:10:03.578607-03
eth3:0 | 172.28.0.1/24 | BACKUP | 2024-09-09 13:28:10.630173-03
(16 rows)
replication slots status:
slot_name | active
(0 rows)
subscription status:
sub_name | active
c_subscription_2_bresconfig | t
c_subscription_2_brcver | t
c_subscription_2_radius | t
(3 rows)

How to Upgrade in Blockbit NGFW- Console access

The Blockbit NGFW offers the Command Line Interface (CLI), which allows you to execute administrative and troubleshooting commands for the main services of the system.

Only execute this step after creating a snapshot.

To perform the configuration, an SSH client and console are required. The minimum recommended applications are:

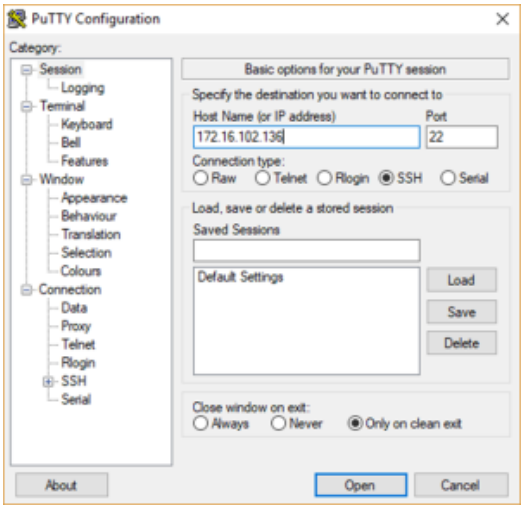
- PUTTY;
- CygWin;
- Mobaxterm.

Make sure the access device has an SSH client installed.

Here, "PUTTY" was used.

Access the SSH console and fill in the fields:

- **Host Name (or IP Address):** Enter the IP address of the Blockbit NGFW. E.g., 172.16.102.136.



Click the “Open” button.

The console will be displayed, prompting for a username and password;

In "login as:", type the username "admin" and press "Enter".

The image below shows the commands for the main services of the system.

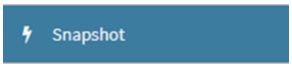
```
admin  >help
arp               enable-ospf  lscpu                   show-license
arping            enable-pim   lsusb                   show-sessions
configure-bgp     enable-rip   mkfs                    show-uuid
configure-ospf    enable-root  more                    show-version
configure-ospf6   enable-sip   mtr                     show-vpn-conn
configure-pim     enable-snmp  netads                  show-vpn-info
configure-rip     ethtool      netstat                 shutdown
configure-rip6    exit         nslookup                speedtest
configure-syslog  fdisk        ntpdate                 sync-users
conntrack         free         passwd                  sysctl
date              fsck         ping                    tcpdump
debug-auth        fwrecovery   reboot                  tcptop
debug-dhcp        fwreload     reset                   tcptrack
debug-events      grep         reset-admin-blocks      telnet
debug-firewall    help         reset-admin-password    tracepath
debug-ha          history      reset-admin-sessions    traceroute
debug-sync        host         reset-logs              update-license
debug-threats     hostname     reset-stats             update-system
debug-vpn         ifconfig     rewizard                uptime
debug-web         ifstat       route                   vmstat
dig               iostat       sar                     vtysh
disable-bgp       iotest       service-disable         watch-cpu
disable-ospf      ip           service-enable          watch-io
disable-pim       ipcalc       service-start           watch-mem
disable-rip       iplist       service-status          watch-srv
disable-sip       iptraf       service-stop            wc
disable-snmp      ldapsearch   set-irqbalance-dynamic  whois
enable-bgp        less         set-irqbalance-static
```

For more information, refer to Blockbit Interface – CLI.

Now, turn off the secondary interface and update the system.

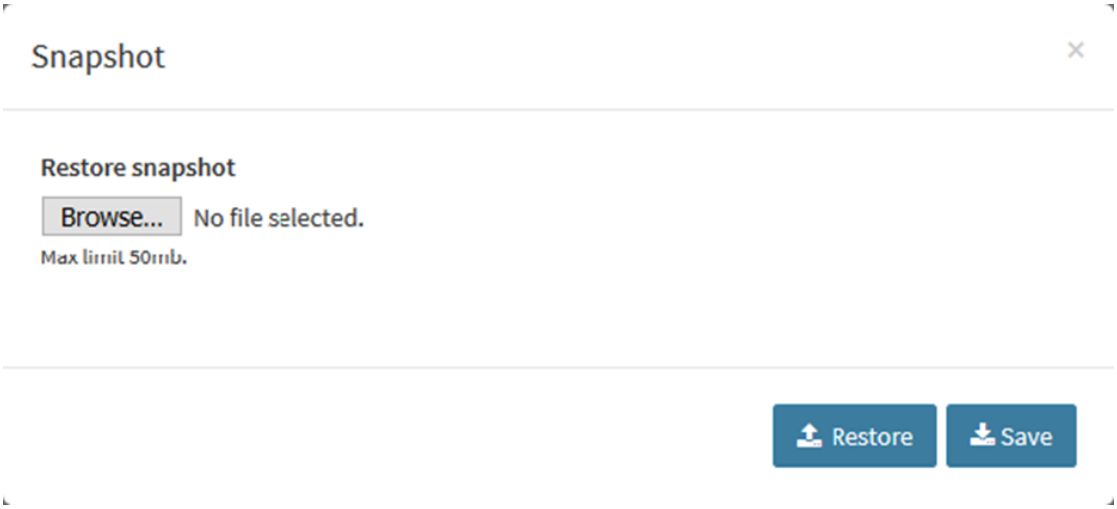
How to Upgrade no Blockbit NGFW- Generate a Snapshot

After you login in the interface, click on the button Snapshot at the upper left menu.



Snapshot

This screen will appear:



Snapshot

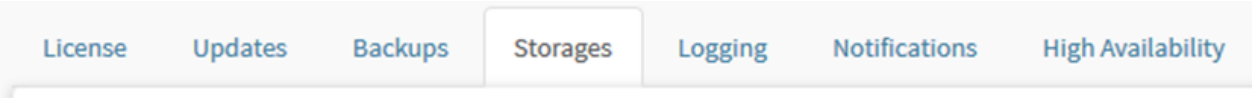
Click on the [] button to generate *snapshot*.

This *snapshot* is essential to guarantee your data stability and integrity. Keep in a safe place.

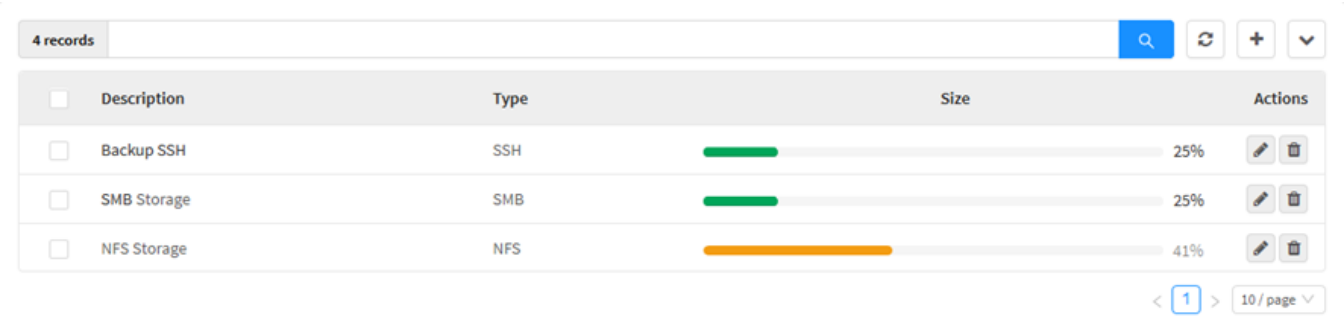
How to Upgrade Blockbit NGFW- Generate a system backup - System - Storages

Storage is the device or system used to permanently store data, making it an essential component in computer systems and networks.

In Blockbit NGFW, it is used for storing backups. To access it, click on the "Storages" tab:



Ao abrir, você terá acesso aos arquivos de backup:



When opened, you will have access to the backup files:

The following types of storage are supported:

- SMB;
- NFS;
- SSH;
- Disc.

Here is an example of a file on a USB drive, a physical data storage device. Devices of type (USB-HDD; USB-SSD) are supported. This model of “Storage” is provided by the system for “Backup/Restore” applications.

To identify a "Disk" type device, click on [ ].

“Disk” type devices must be formatted according to the EXT4 file system.

To format the disk, access the Blockbit NGFW console.

To log in to the terminal, use the username admin and the custom password.

1. To list the new disk, use the command:
2.
```
fdisk -l
```

```
admin > fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes, 625142448 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000b93f6

Dispositivo Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     1026047      512000   83  Linux
/dev/sda2         1026048   625141759   312057856   8e  Linux LVM

Disk /dev/mapper/root: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/swap: 4177 MB, 4177526784 bytes, 8159232 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/data: 293.9 GB, 293890686976 bytes, 574005248 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 8000 MB, 8000110592 bytes, 15625216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin  >
```

2. Before formatting the disk, it may be necessary to partition it.

To do this, execute the command:

`fdisk /dev/sdb`

```
admin  >fdisk /dev/sdb


Welcome to fdisk (util-linux 2.23.2).



Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help):
```

Type “**m**” to list the command options of the “**fdisk**” utility for disk partitioning.

```
Command (m for help): m
Command action
   a   toggle a bootable flag
```

```
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   g   create a new empty GPT partition table
   G   create an IRIX (SGI) partition table
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)


Command (m for help):
```

To delete the current partition, use “**d – delete a partition**”

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted


Command (m for help):
```

To add a partition, use

`n – add new partition`

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-31299583, default 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-31299583, default 31299583):
```

```
Using default value 31299583
Partition 1 of type Linux and of size 14.9 GiB is set


Command (m for help):
```

To save the new partition table to disk:

`w – write table to disk and exit`

```
Command (m for help): w
The partition table has been altered!


Calling ioctl() to re-read partition table.
Syncing disks.
```

To format the identified disk that is already partitioned, type:

mkfs -t ext4 /dev/sdb1

```
admin  >mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3912192 blocks
195609 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208


Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Once connected to the server and formatted to the EXT4 standard, the device will be ready.

   To list it, click on [] and the device will automatically be available for selection.

   After saving, access the **command queue** [] to apply the changes. For more information, refer to NGFW - Command Queue.

Blockbit NGFW - How to: Import and Export the NGFW 1.5 to the 2.0

Thank you for choosing Blockbit.

In this document we will discuss how to perform the export and import processes from the NGFW 1.5 to the 2.0.

After reading and applying the steps in this tutorial you will be able to export your Blockbit NGFW data to the most updated version with ease and security.

 Taking into account the criticality of the exported settings, it is recommended that the export procedure be carried out locally and that the import be made on the same network in order to ensure that the administrator has access to the device in case something unexpected occurs.

This guide consists of the following themes:

Import and Export 1.5 to 2.0 - Export Requirements

Before exporting Blockbit NGFW version 1.5 it is recommended to make sure that the system is up to date. You can perform an update in two ways:

- Through the CLI;
- Using the WEB interface.

In addition, we ALWAYS recommend that a system SNAPSHOT of the latest version be performed before any update or upgrade procedure is performed and that the generated file be saved in a safe place.

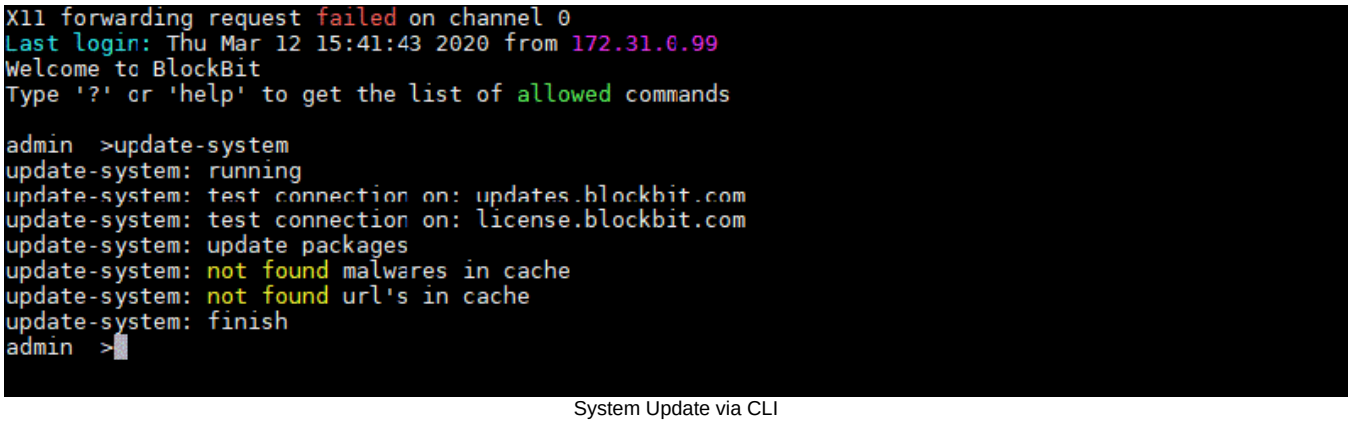
 For more in-depth information regarding all the procedures mentioned in this how to consult the Blockbit NGFW manual.

Below we will briefly demonstrate how to perform each of these procedures, starting with the update via CLI.

Import and Export 1.5 to 2.0 - Update - CLI

Having access to the console, make an SSH connection, when the system asks for a user and password, enter the registered credentials to access the system.

Run the **[*update-system*]** command, as shown in the image below:



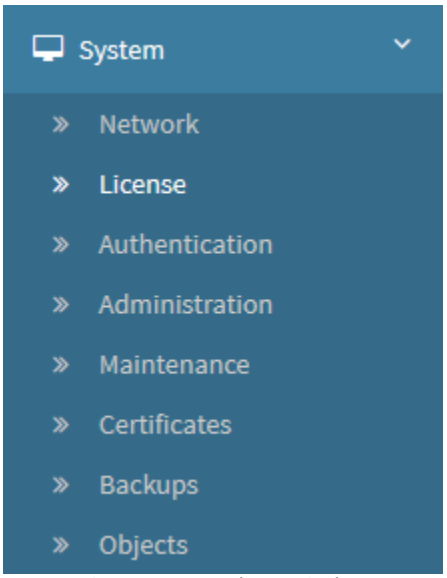
System Update via CLI

After performing the update, confirm the version using the **[show-version]** command, make sure that the version is BLOCKBIT NGFW 1.5.9 build 20031200 or higher.

After performing the steps previously mentioned, the update via CLI will have been successful. Next we will analyze how to update the NGFW through the *WEB interface*.

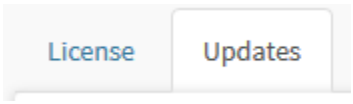
Import and Export 1.5 to 2.0 - Update - WEB Interface

Having access to the interface, enter the System option and select the License option.



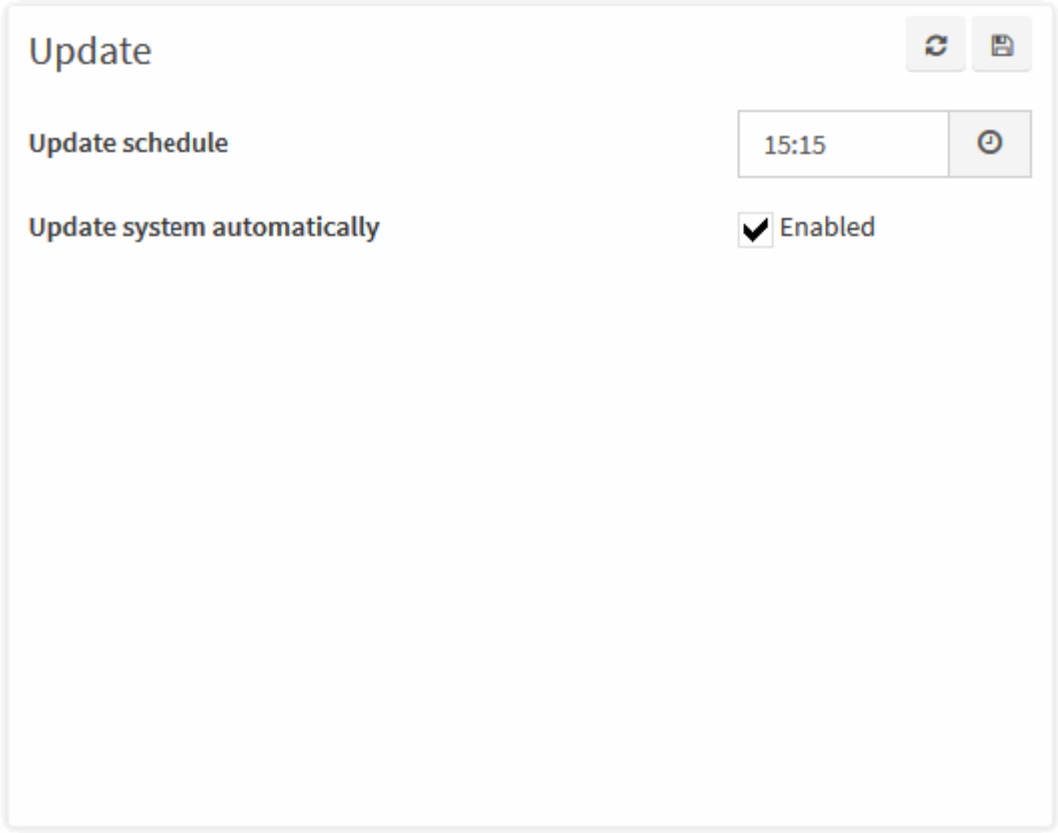
System Menu - License Option

Select the Updates tab, as shown by the image below:



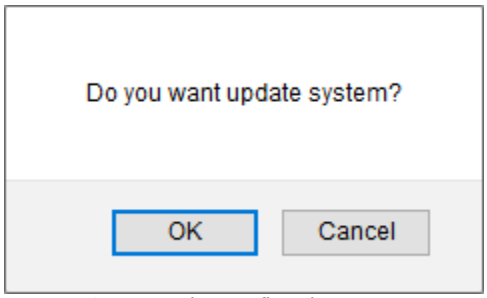
License - Updates

Access the Update panel, as shown below:

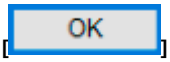
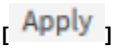


License - *Updates* - Panel

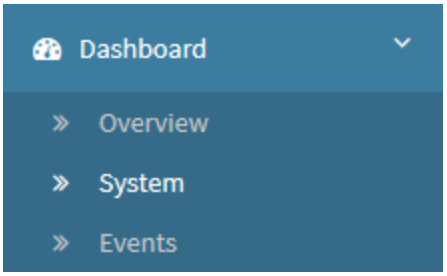
To perform the update, click on the **[**  **]**, the following window will be displayed:



System update confirmation screen

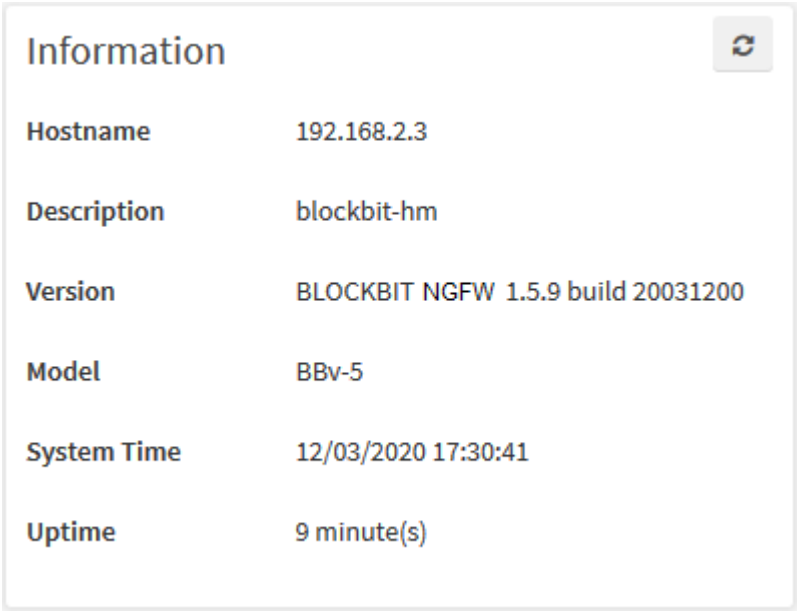
Click on the **[**  **] button**. In the command line **[**  **]** click on **[**  **]** to perform the update.

After performing the update, enter the Dashboard option and select the System option.



Dashboard Menu - System Option

Access the Information panel, as shown below:



System - Information

In the “version” field, make sure that the version is BLOCKBIT NGFW 1.5.9 build 20031200 or higher.

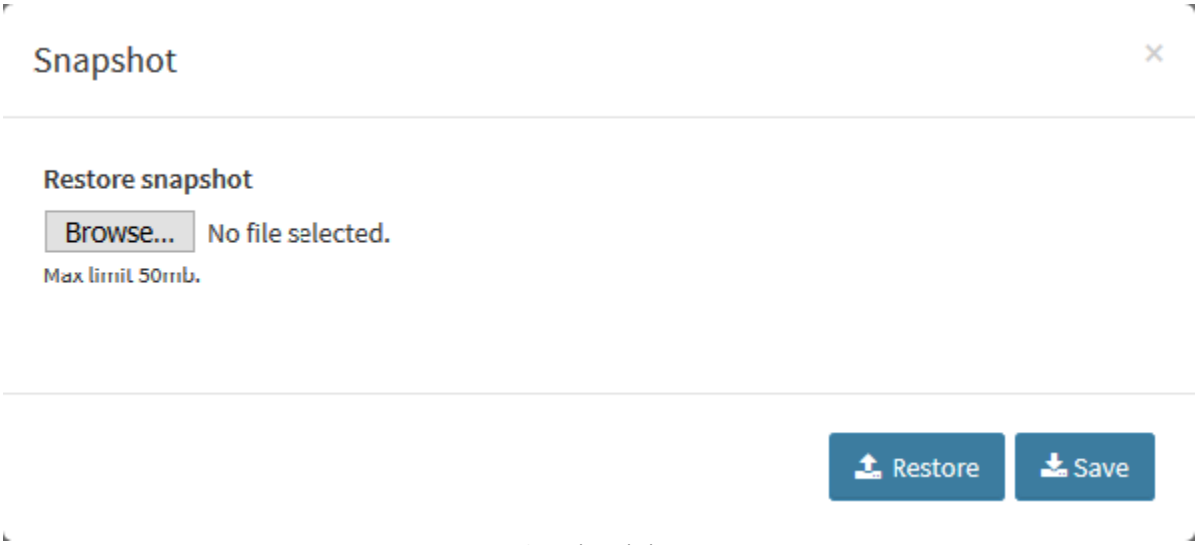
After performing the steps previously mentioned, the update via the WEB interface will have been successfully performed. Next we will analyze how to create a *Snapshot*.

Import and Export 1.5 to 2.0 - How to generate a Snapshot

Having access to the interface, click on the Snapshot option.

Snapshot option

The following window will appear:



Snapshot window

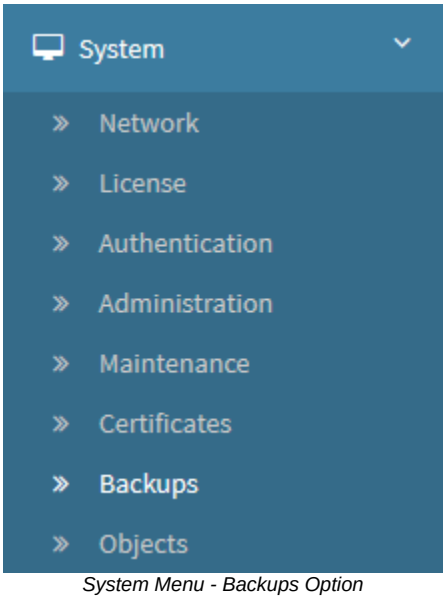
Click on the [

] button to generate a snapshot. Keep the file in a safe place.

After performing the steps previously mentioned, the snapshot will have been successfully generated. Next, we will analyze how to perform the export itself.

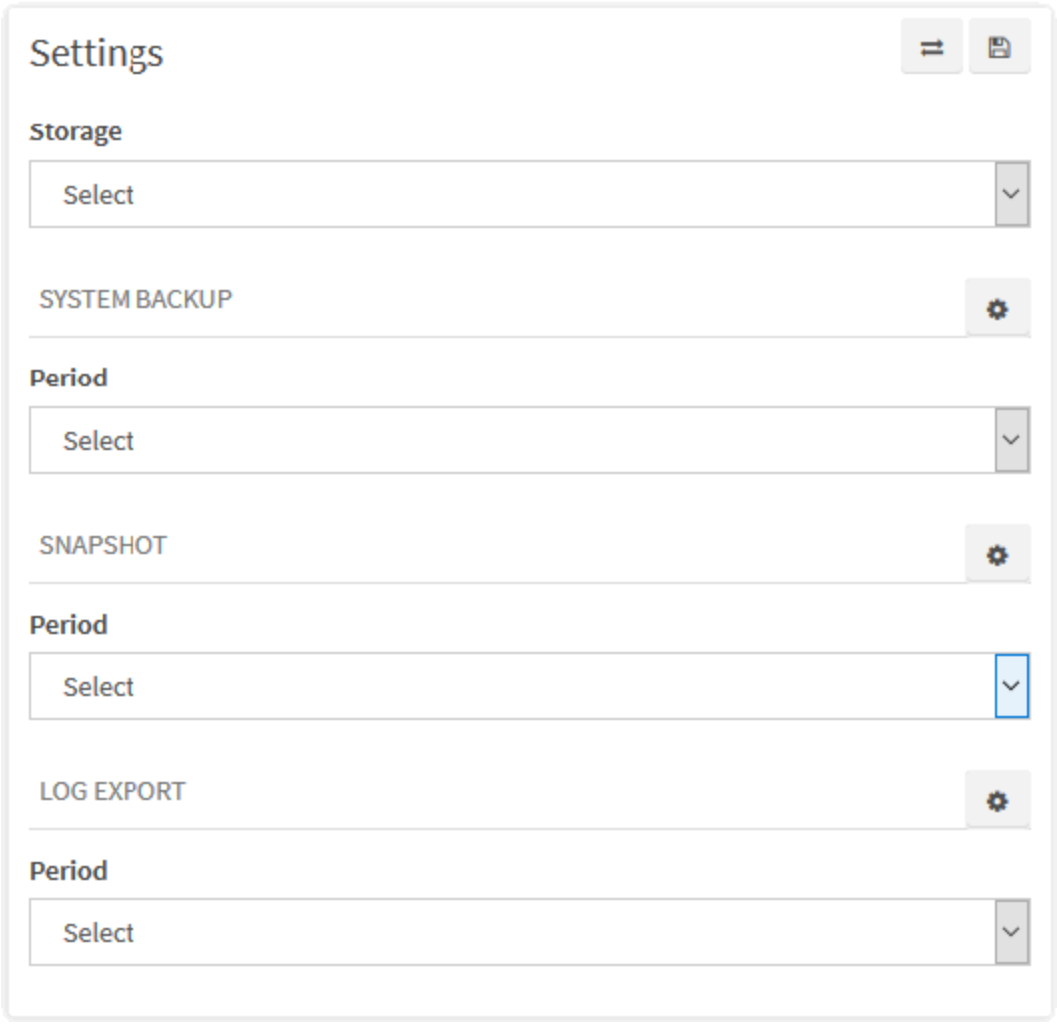
Import and Export 1.5 to 2.0 - Export

First, make sure that the logged in user has **super user** permissions. To perform the export, enter the System option and select the Backups option.



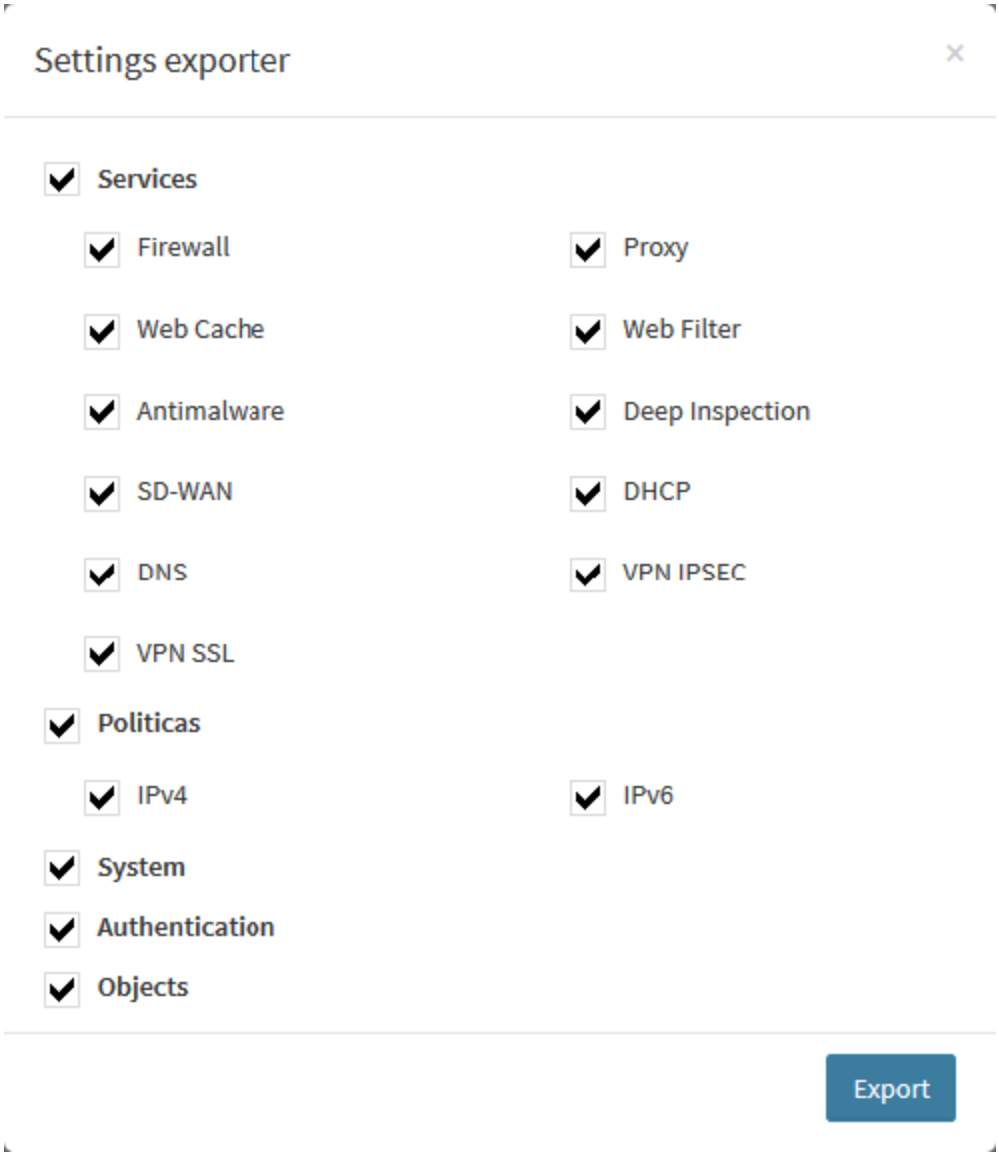
System Menu - Backups Option

The Backups tab will automatically be selected, access the Settings panel:



Backups - Settings

When you click on **[** **]**, the “Settings exporter” window will appear, select the items that want to export, as shown below:

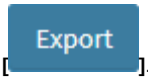


Settings Exporter

As shown in the image above, it is recommended that all items are exported.

Note that the following data will NOT be imported:

- Network settings (Settings tab);
- Personal information (in System, option Authentication, in the Portal tab);
- GSM settings;
- Notification Settings;
- Dynamic routing settings;
- Deep Inspection settings;
- Antimalware settings;
- Empty IPv6 configurations;
- Session management with the NGFW default values;
- Backup and Storage Settings;
- Scheduled or automatic update settings;
- H.A. settings;
- IPSEC VPN Failover Settings;
- IPS settings.

To start exporting, click on [

].

The system will generate a “JSON” extension file. Disable the browser pop-up blocker if it blocks the download.

ATTENTION: The “JSON” extension file contains sensitive sensitive information. It is the administrator's responsibility to ensure the protection and non-distribution of this file, in order to maintain confidentiality and ensure the confidentiality of this data.

When downloading the file, be sure to save it in a safe place.

The file will contain the password of the administrator users, it is highly recommended to change the password. The file also contains the passwords of local authentication users, but they will be required to register a new one when they log in for the first time.

Passwords are encrypted in a hash format.

After performing the steps previously mentioned, the export will have been successful. Next, we will analyze the necessary requirements to perform an import.

Import and Export 1.5 to 2.0 - Import Requirements

Before importing to Blockbit NGFW version 2.0, it is recommended to make sure of the following points:

The system must have undergone a new installation and be licensed;

- Must be in factory settings;
- Import user must have “super user” permission.

 For more in-depth information regarding all the procedures mentioned in this how to consult the Blockbit NGFW manual.

Next we will analyze how to perform the installation, before demonstrating how to perform the import itself.

Import and Export 1.5 to 2.0 - Installation of UTM

In this chapter we will deal with the installation of Blockbit NGFW, it can be installed in two types of Appliances: Hardware and Virtual, which are compatible with the following solutions: VMware, XenServer, KVM and ProxMox.

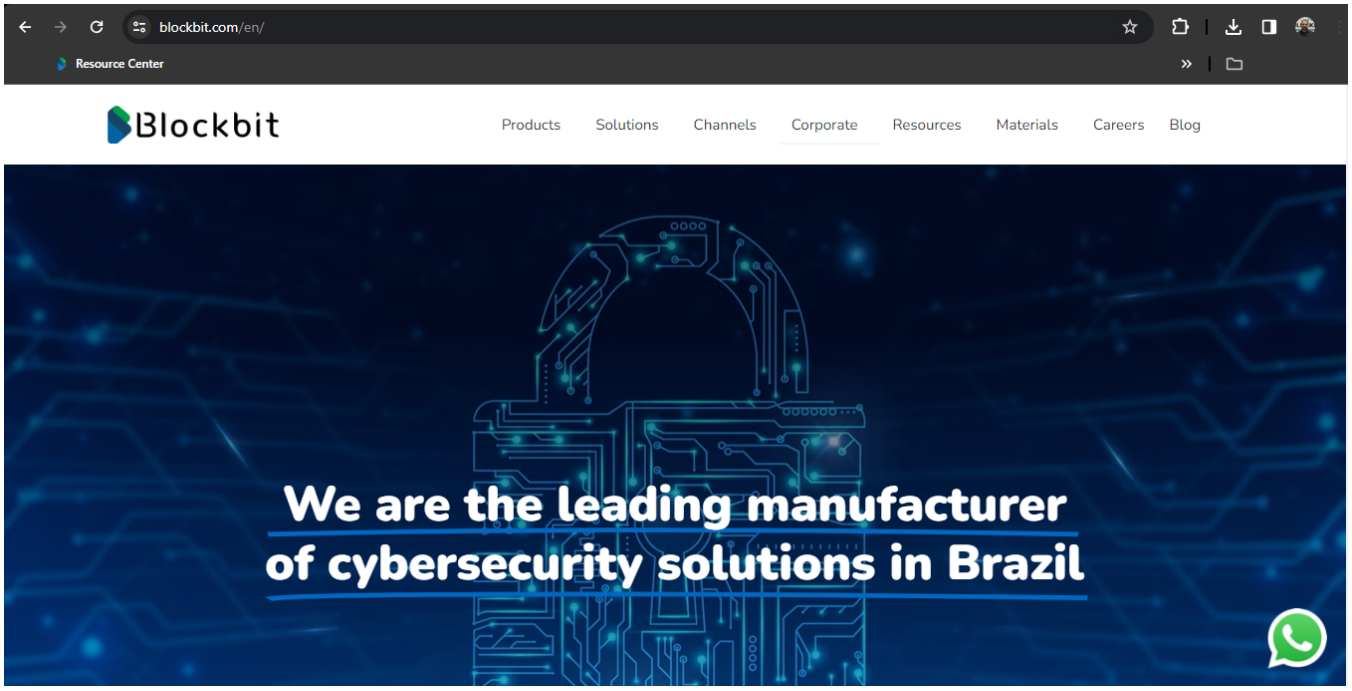
- Download installation files;
  - OVA Download;
  - IMG Download.
- Recording the installation image on flash drive;
- Appliance Installation;
- Importing the Virtual Machine;
- First Access.

Below, we will exemplify how to download installation files.

Import and Export 1.5 to 2.0 - Download installation files

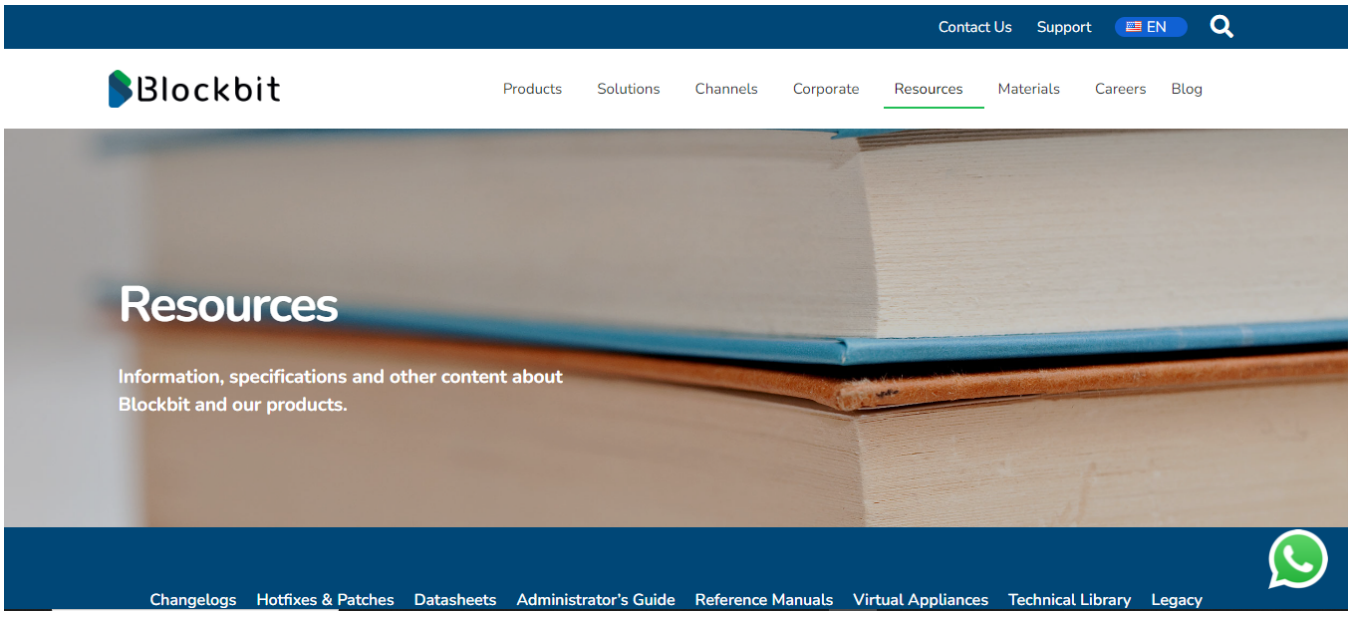
To perform the import, it is essential to download the Open Virtual Appliance (OVA) or Installation File (IMG) from Blockbit NGFW, for this, follow the steps below:

Access Blockbit website (www.blockbit.com):



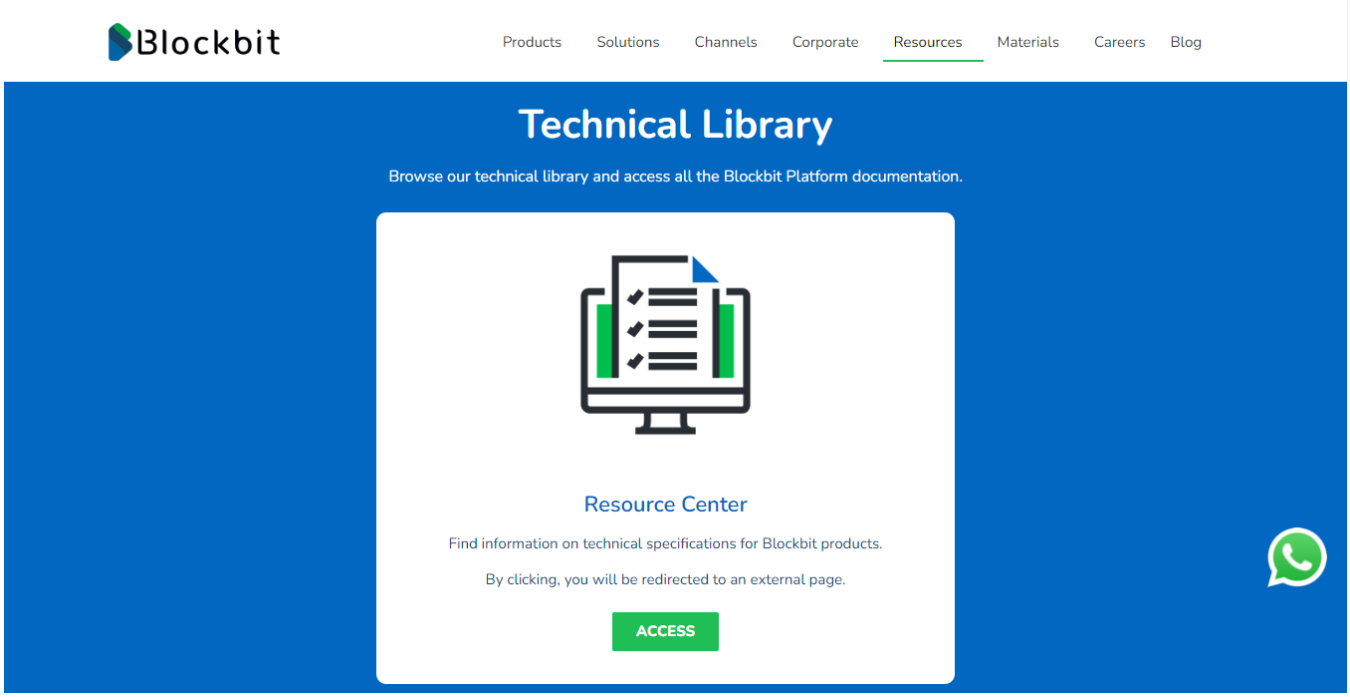
Blockbit Homepage

Click on the **Resources** option and the screen below will appear:



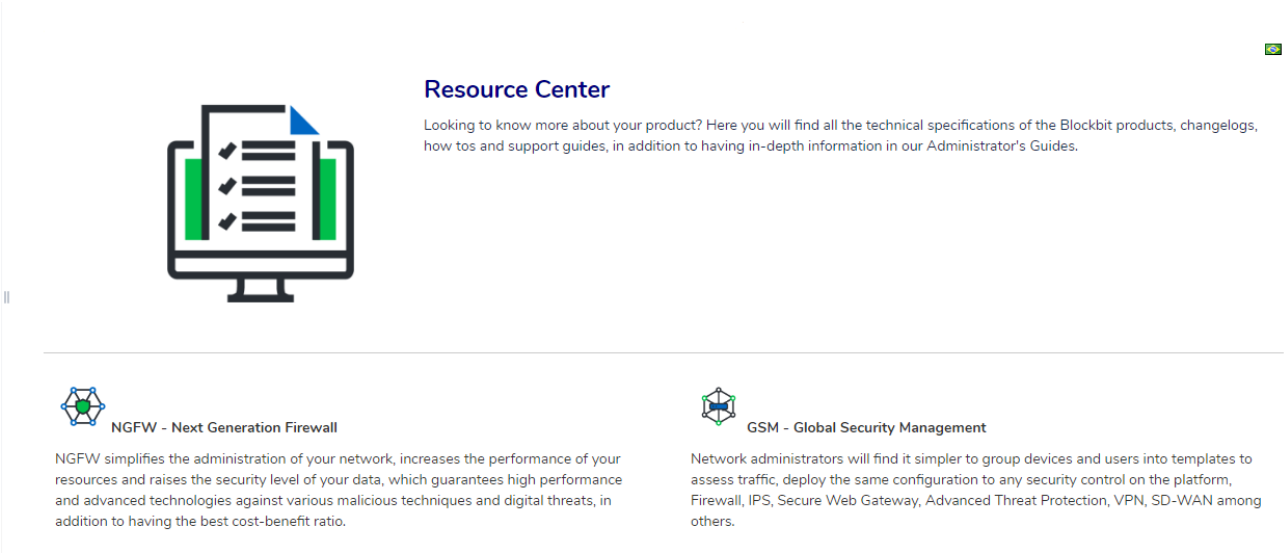
Resource Center page

Scroll down to the technical library, until you the screen below is displayed:



Resource Center homepage

Click on the "Access" button and you'll be redirected to the **NGFW - Next Generation Firewall** main resource center page, as shown below:

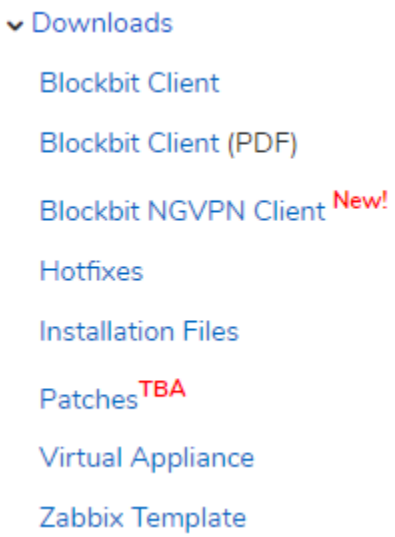


Next generation Firewall Resource Center

Overview of the documents available:

Documentation main page

Click on **Downloads** to expand it and have access to the other options, as shown on the following image:



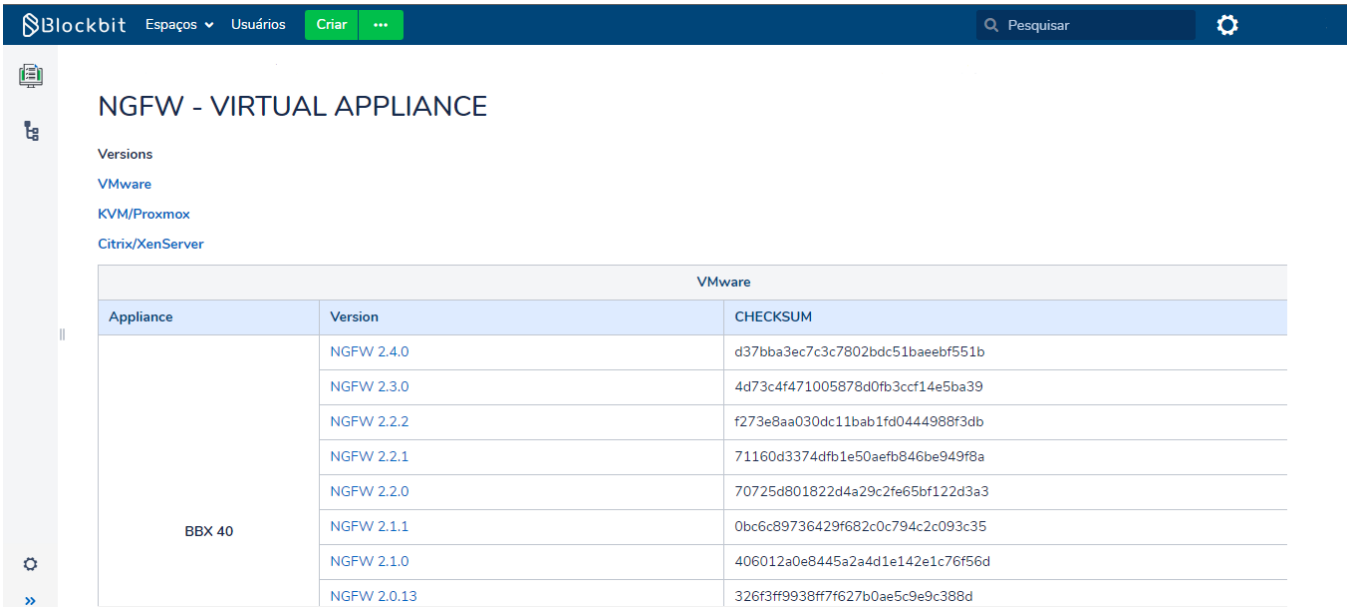
Expanded Downloads

Below we will analyze each option:

- OVA Download;
- IMG Download.

Import and Export 1.5 to 2.0 - OVA Download

Select the **Virtual Appliance** option and the following page will be displayed, where it's possible to select the version of the OVA you want to download then click on the link of the version:

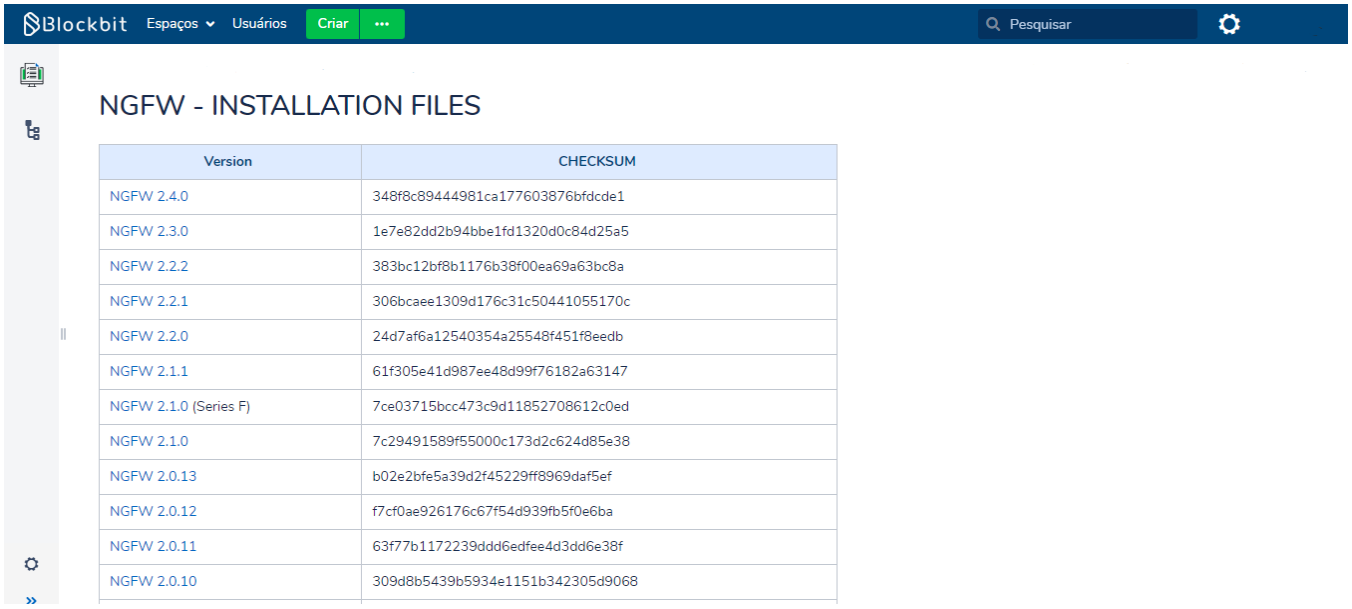


Virtual Appliances page

This concludes the OVA download, then you will need to import the virtual machines.

Import and Export 1.5 to 2.0 - IMG Download

Select the **Installation Files** option and the following page will be displayed. Finally, just select the version of the IMG you want to download and click on the link of the version, as shown:



Virtual Appliances page

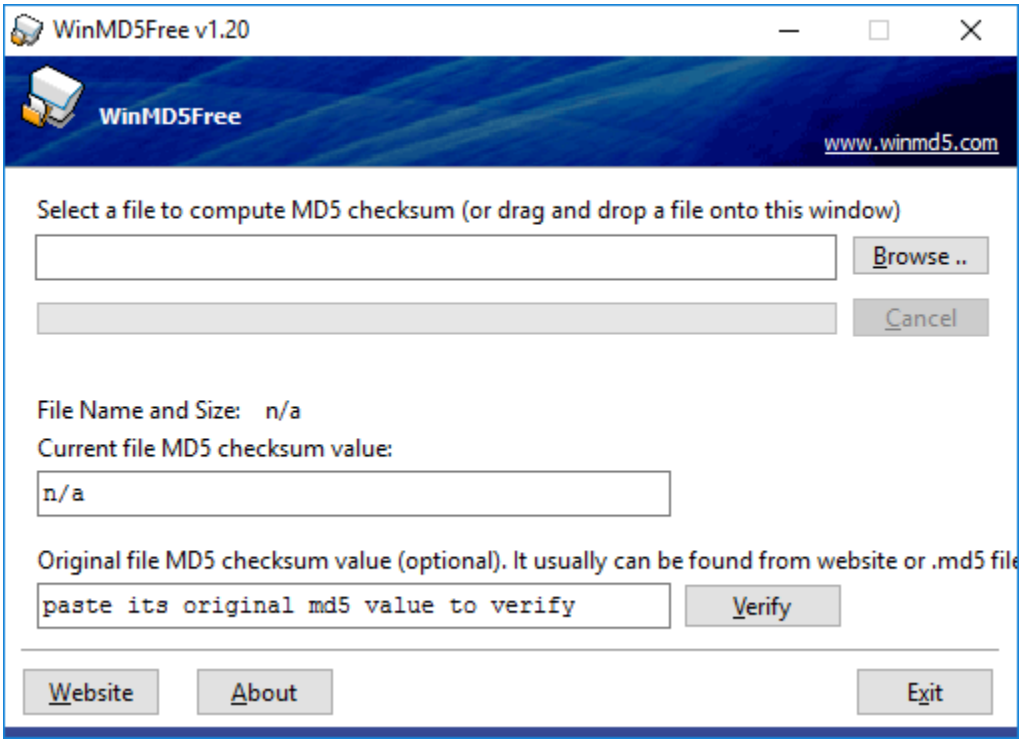
This concludes the IMG download, then you will need to import the virtual machines.

Import and Export 1.5 to 2.0 - Recording the installation image on a flash drive

On the Blockbit website download the corresponding installation image.
The images must be downloaded and saved to a folder on the computer. Check the MD5 SUM of the files to ensure they are not corrupted. The application to perform MD5 SUM on Microsoft Windows is WinMD5Free (http://www.winmd5.com/), to perform this verification follow the steps below:

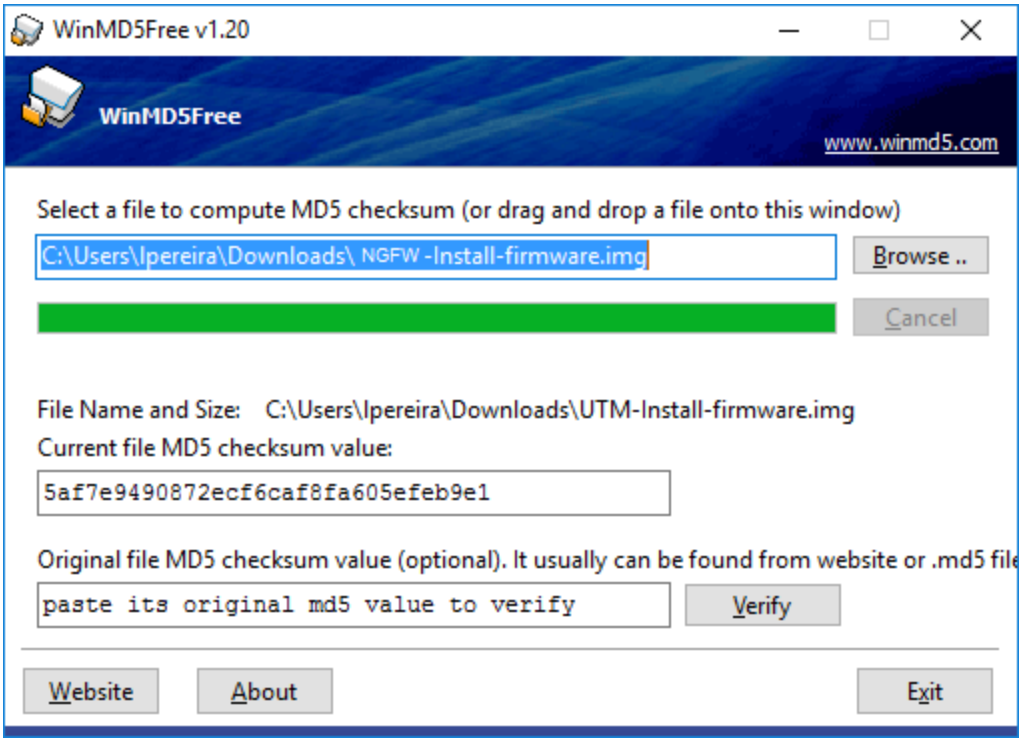
Checking files

1. Open the application, the following screen will be displayed:



WinMD5

2. Select the image file and wait for the calculation:



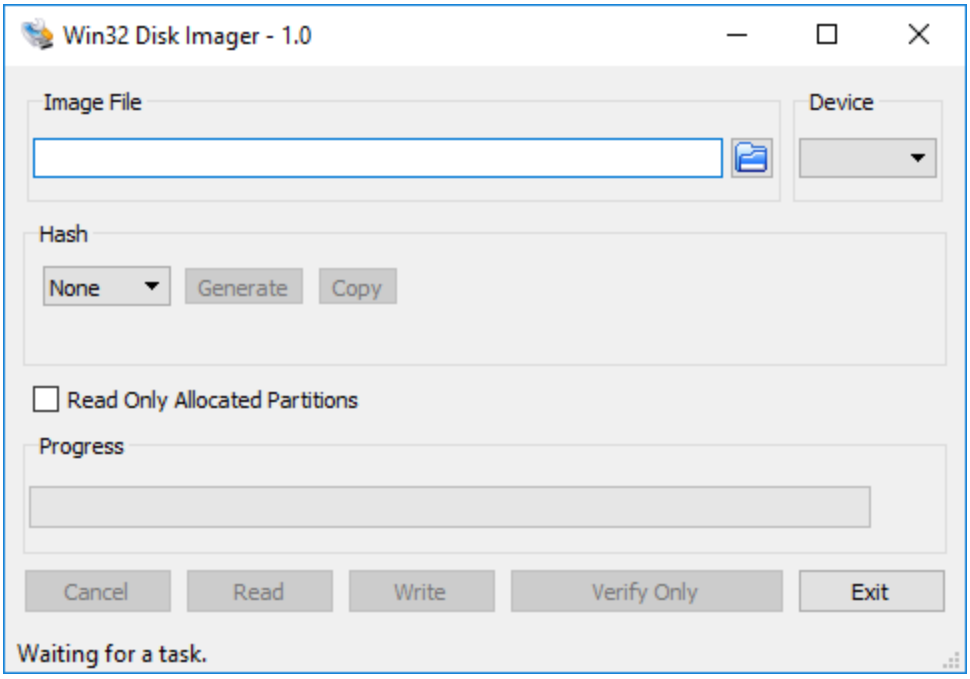
MD5 Check

3. Compare the values obtained from the two images in WinMD5 with the respective values saved in the section.

Recording the images

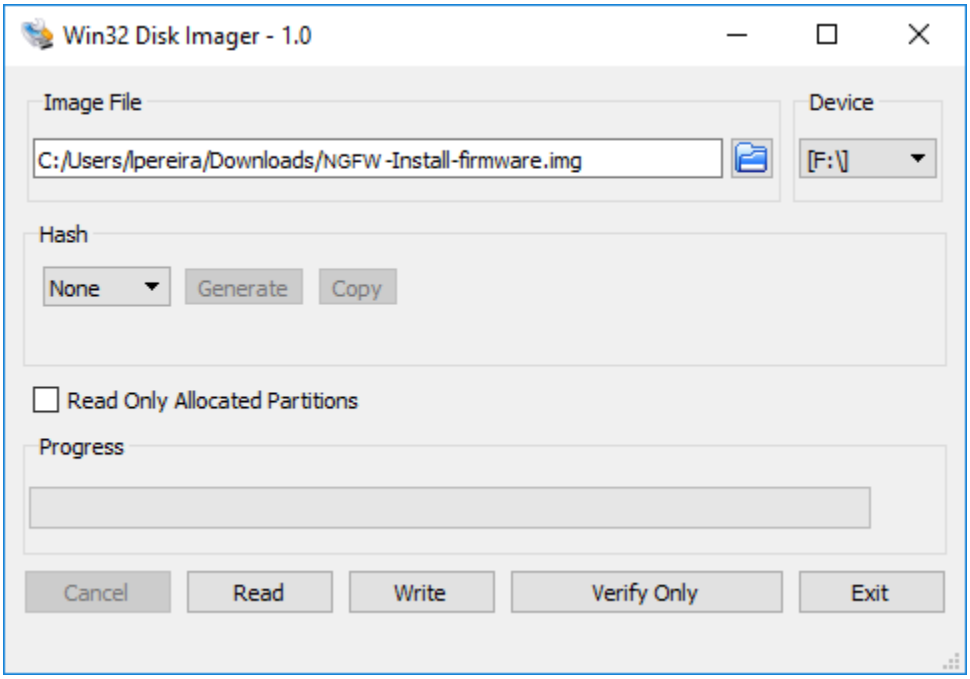
To save the images, you need the Win32 Disk Imager application that can be downloaded by clicking on this link: https://sourceforge.net/projects/win32diskimager/files/Archive/.

1. Insert a pendrive, at least 8 GB;
2. Open the application, the following screen will be displayed:



Win Disk Image

3. Click on the "folder" image and select the appropriate image to be saved to the USB sticks. Ex.: NGFW-Install-firmware.img;



Recording the image

4. Select the Device corresponding to the USB stick that you want to record the image;

5. To save the image click on "Write" and wait for the image to be saved on the USB stick;

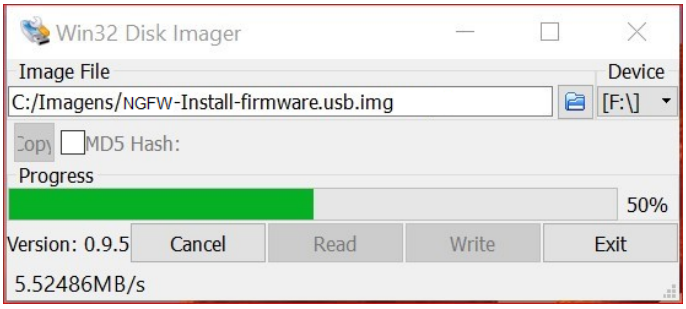
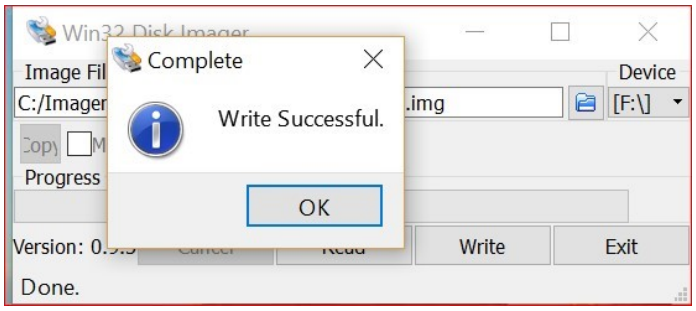


Image recording process

6. After the recording confirmation message appears, the flash drive will be ready for use;



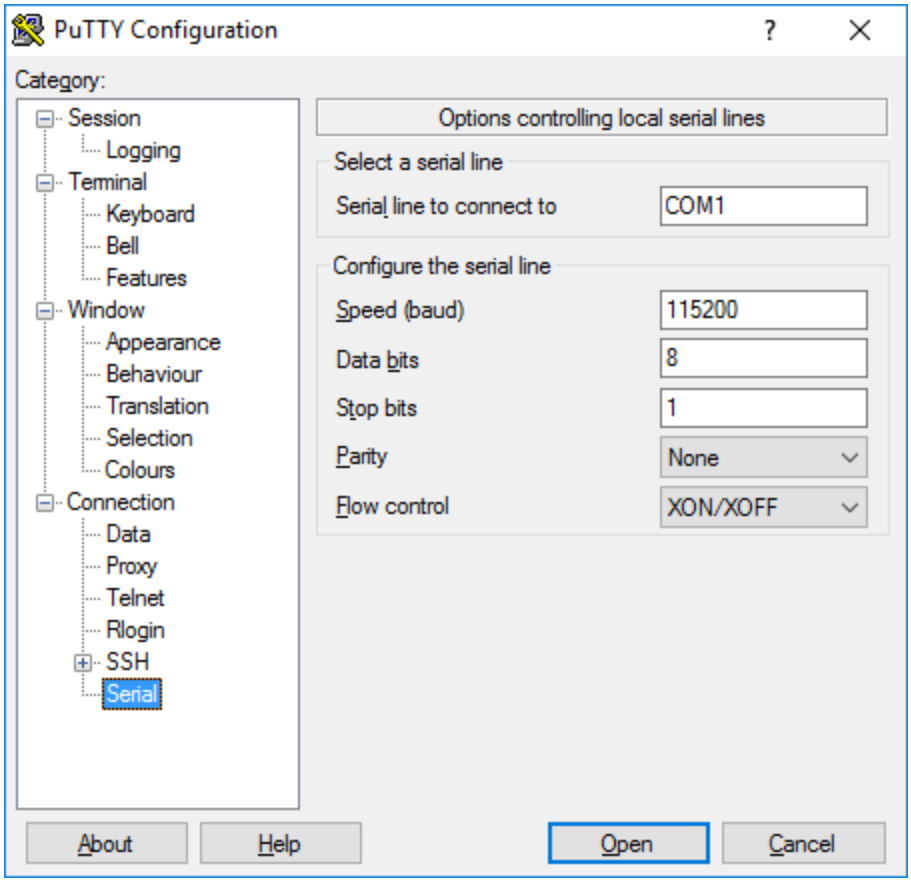
Completing image recording

Console Access - Putty

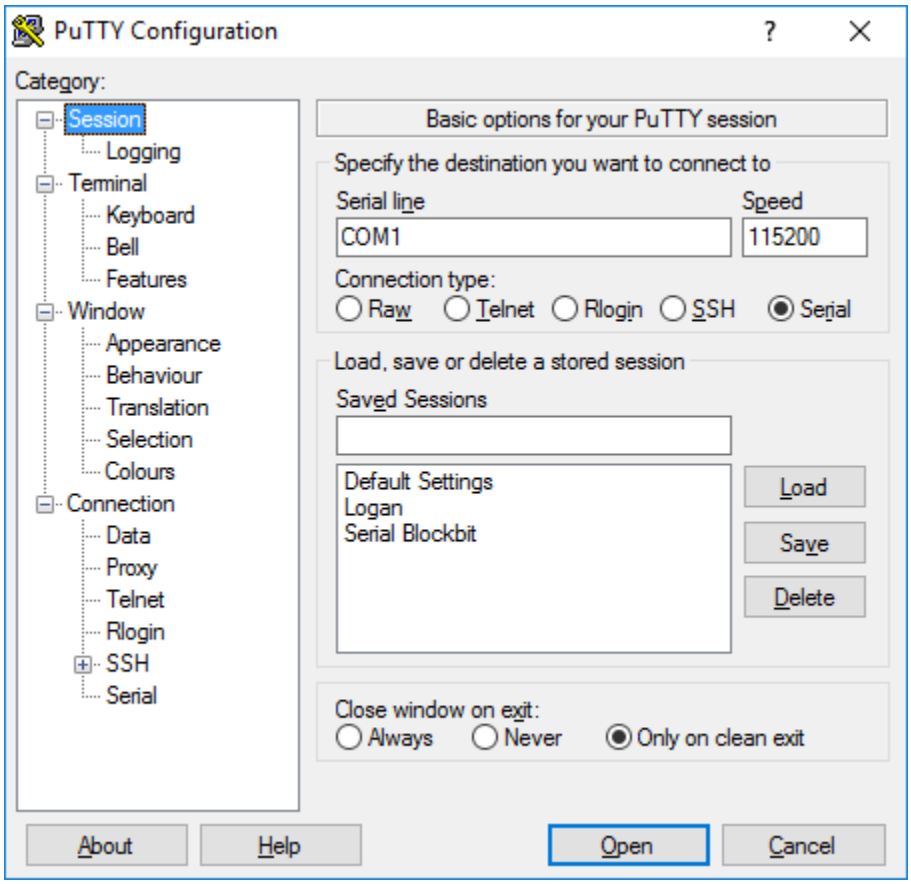
Before starting the following procedures, the Putty application must be available on the machine where the connection to the Equipment will be made. Putty is free and open source terminal emulation software.

Now configure the terminal emulator with the following parameters:

- Port: COM1 (a porta pode variar, verifique seu gerenciador de dispositivos do *Windows*);
- Standard transmission rate: 115200;
- Standard data bits: 8;
- Standard stop bits: 1;
- Standard parity: None.



Putty Settings



Putty Connect

Next, we will analyze how to perform the physical installation of the Appliances.

Import and Export 1.5 to 2.0 - Appliance Installation

In this chapter we will detail the physical installation of the Appliance.

The installation process is different depending on the technical peculiarities of the BIOS of each model.

- BB 2;
- BB 5/10/50/100/500/1000;
- BB 10000.

Below we will detail the particularities of the installation of each model.

Import and Export 1.5 to 2.0 - Installation of BB2

To perform the installation it will be necessary to access the BIOS, in order to make some settings on the appliance, the importance of which is to enable access to the pendrive recorded with the installation image.

In this appliance model, the BIOS does not appear on the console, so connect a monitor to the VGA port to access the BIOS*;*

Connect the monitor to the VGA port

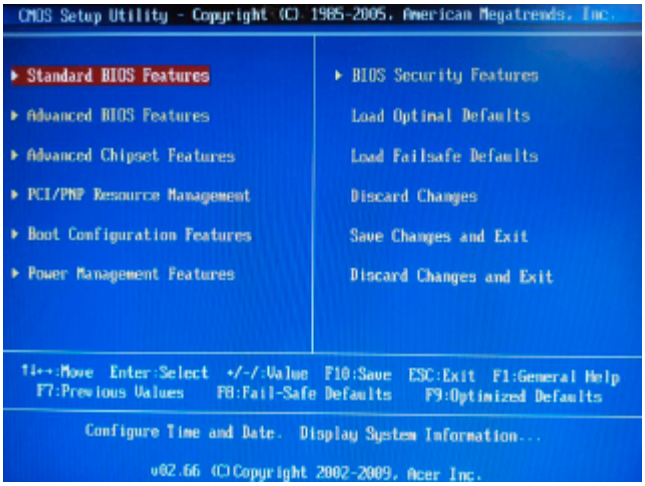
ATTENTION: Before turning on the appliance, connect a keyboard to one of the USB ports in order to access the BIOS.

Here is the step by step how to install via USB stick:

1. Connect the installation stick to the USB port on the appliance;

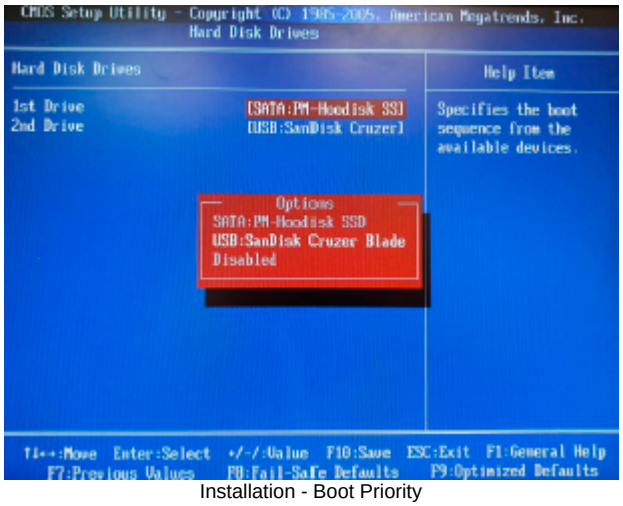
Installation pendrive

2. Plug the power cord into an electrical outlet and **press the “del” key** repeatedly until the BIOS is displayed on the monitor;



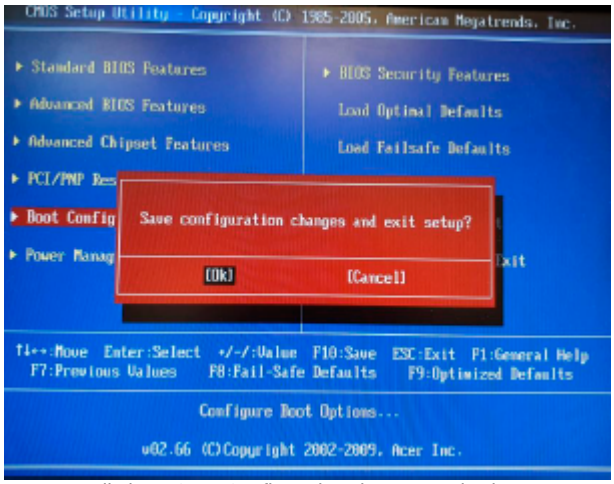
Installation - BIOS initial screen

3. Go to "Hard Disk Drives" and make the pendrive a boot priority;



Installation - Boot Priority

4. Press “F10”, when the message appears asking to exit and save, select **[OK]**;



Installation - *Save Configuration changes and exit setup*

5. The first phase of the installation should start automatically, just wait until the appliance turns itself off. When all LEDs have gone out, remove the flash drive and turn the appliance on again;

Installation phase 1

6. The second phase will also start automatically, wait until the installation is complete.

Installation phase 2

This concludes the BB 2 model installation process, then see the settings that must be made at the first access.

Import and Export 1.5 to 2.0 - Installation of BB 5/10/50/100 /500/1000

To perform the installation it will be necessary to access the BIOS, in order to make some settings on the appliance, the importance of which is to enable access to the pendrive recorded with the installation image.

In these appliance models, the BIOS does not appear on the console, so connect a monitor to the VGA port to access the BIOS;

Connect the monitor to the VGA port

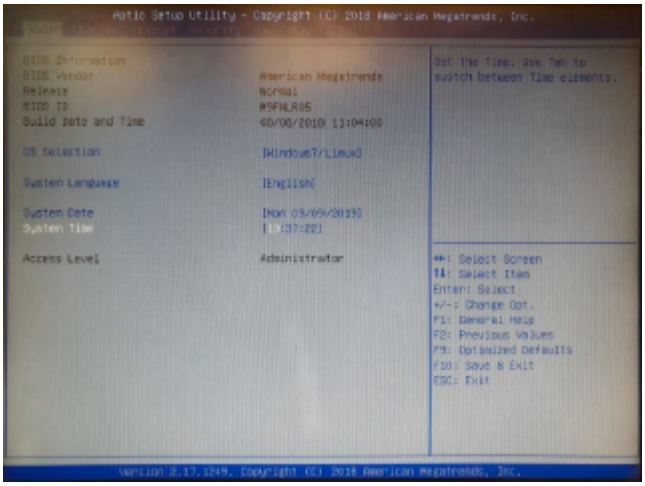
ATTENTION: Before turning on the appliance, connect a keyboard to one of the USB ports in order to access the BIOS.

Here is the step by step how to install via USB stick:

1. Connect the installation stick to the USB port of the appliance;

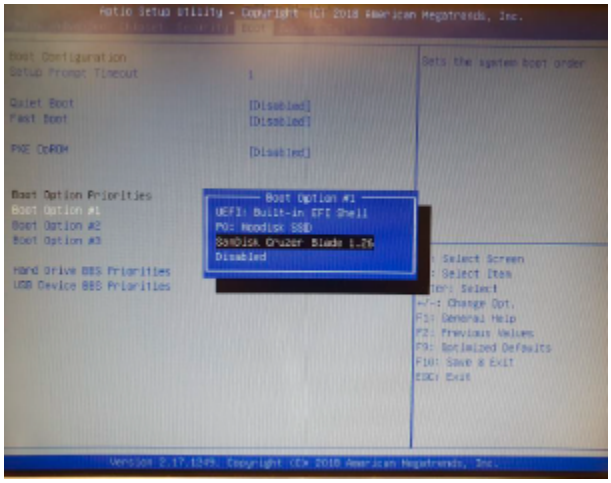
Installation pendrive

2. Plug the power cord into an electrical outlet and **press the “del” key** repeatedly until the BIOS is displayed on the monitor;



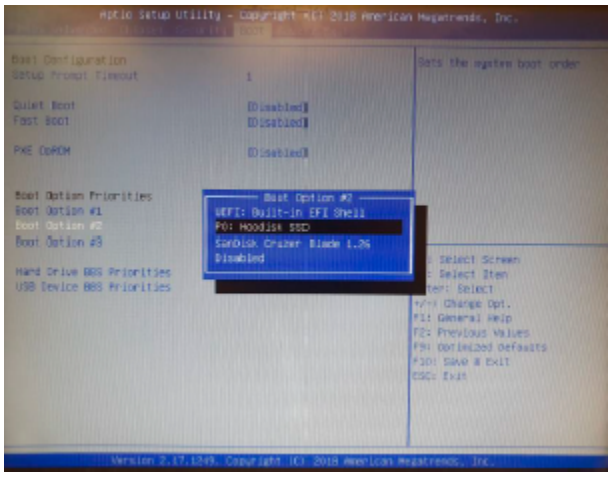
Installation - BIOS initial screen

3. Access the "Boot" tab, select "Boot Option # 1" and change to the installation pendrive, as shown in the image below;

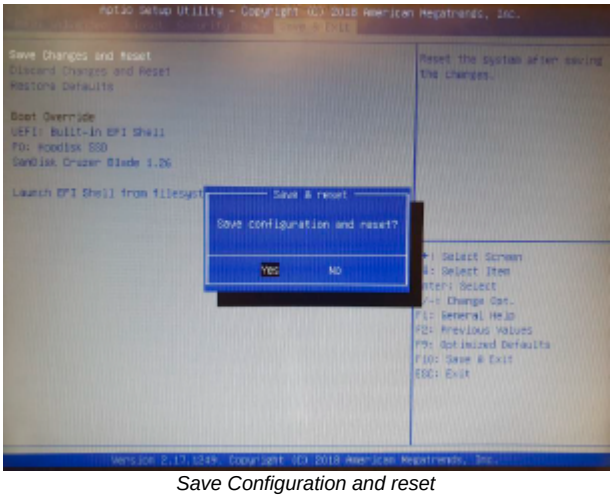


Installation - Boot Option # 1

4. In addition, select “Boot Option # 2” and change to “P0: Hoodisk SSD”;



5. In the “Save & Exit” tab, select the option “Save Changes and Reset”, when the message asking to exit and save appears, select **[Yes]**;

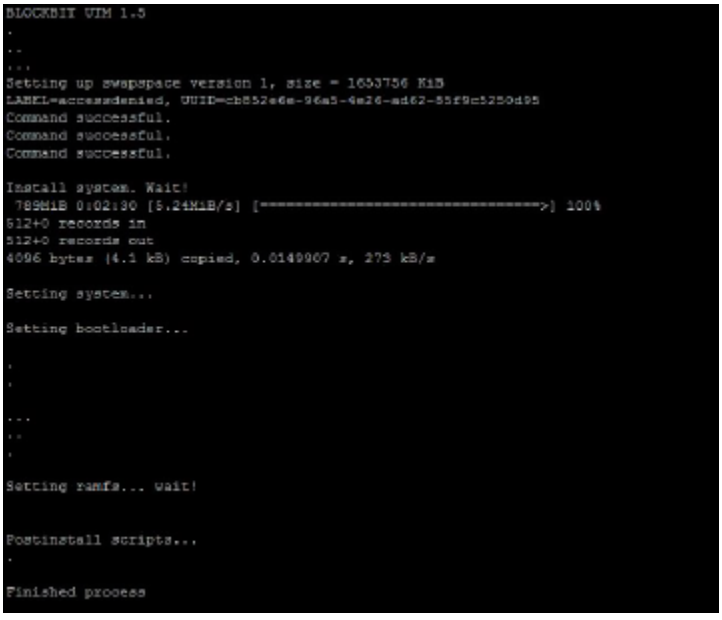


Save Configuration and reset

6. The first phase of the installation should start automatically, just wait until the appliance turns itself off. When all LEDs have gone out, remove the flash drive and turn the appliance on again;

Installation phase 1

7. The second phase will also start automatically, wait until the installation is complete.



This concludes the process of installing these appliance models, then see the settings that must be made on first access.

Import and Export 1.5 to 2.0 - Installation of BB 10000 and legacies

To perform the installation it will be necessary to access the BIOS, in order to make some settings on the appliance, the importance of which is to enable access to the pendrive recorded with the installation image.

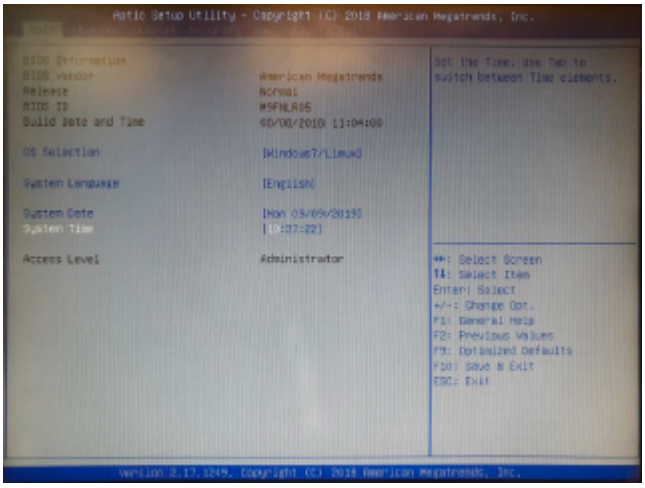
On the BB 10000 model, the BIOS is displayed on the console, so there is no need to use a monitor and keyboard.

Here is the step by step how to install via USB stick:

1. Connect the installation stick to the USB port on the appliance;

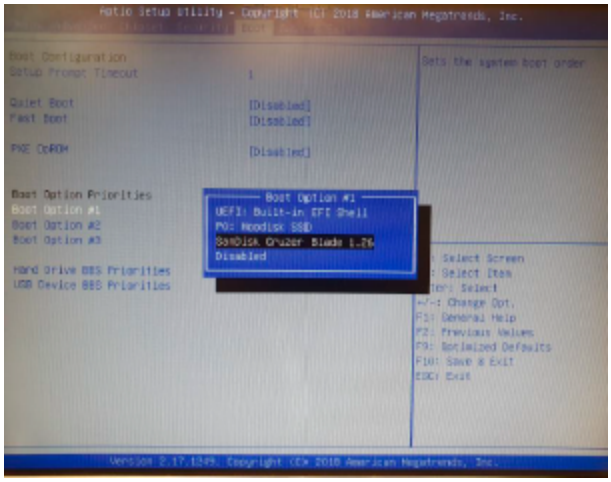
Installation USB

2. Plug the power cord into an electrical outlet and **press the “del” key** repeatedly until the BIOS is displayed on the monitor;



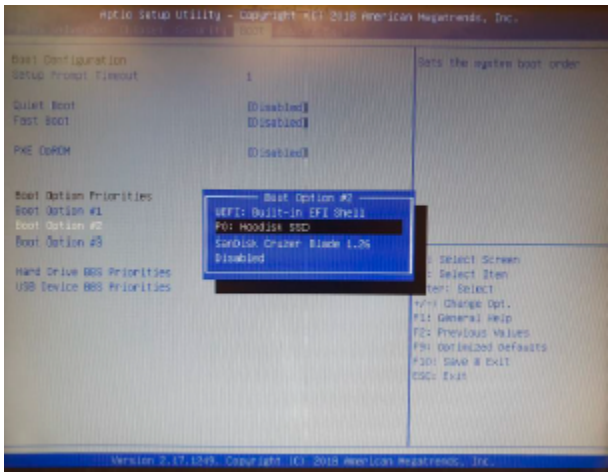
Installation - BIOS initial screen

3. Access the "Boot" tab, select "Boot Option # 1" and change to the installation pendrive, as shown in the image below;



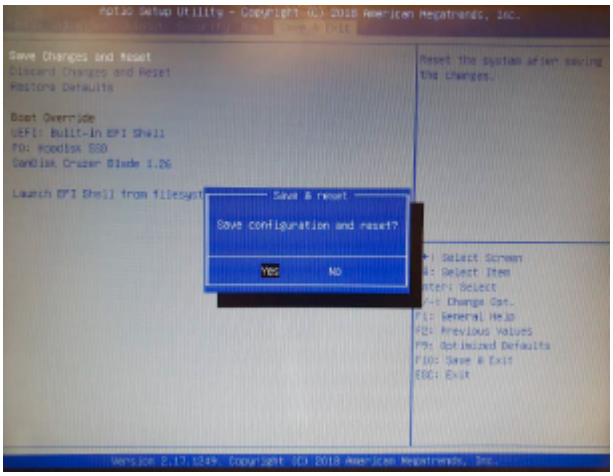
Installation - Boot Option # 1

4. Also, select “Boot Option # 2” and change to “P0: Hoodisk SSD”;



Installation - Boot Option # 2

5. In the “Save & Exit” tab, select the option “Save Changes and Reset”, when the message asking to exit and save appears, select **[Yes]**;

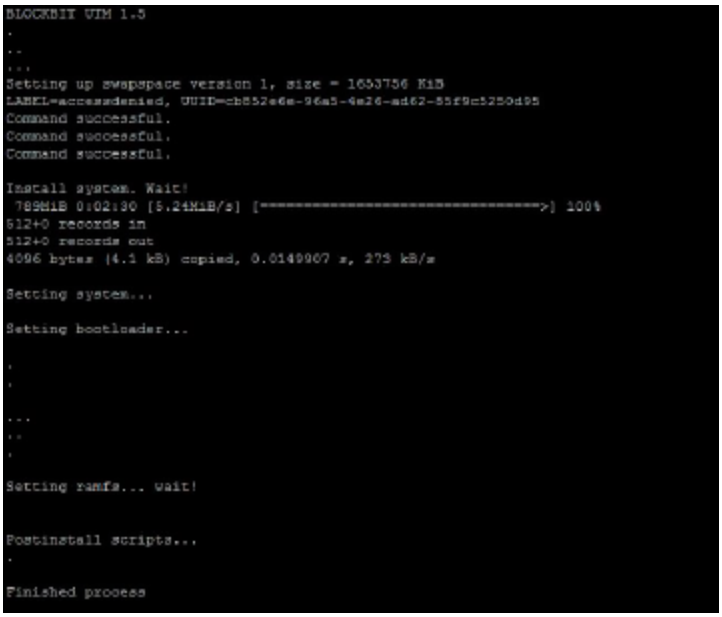


Save Configuration and reset

6. The first phase of the installation should start automatically, just wait until the appliance turns itself off. When all the LEDs have gone out, remove the flash drive and turn the appliance on again;

Installation phase 1

7. The second phase will also start automatically, wait until the installation is complete.



Installation phase 2

This concludes the installation process of the model BB 10000, then consult the settings that must be made at the first access.

Import and Export 1.5 to 2.0 - Importing the Virtual Machine

Initially, it is important to consider the minimum characteristics of the Virtual Appliance, as shown in the table below:

Table - Minimum characteristics of the Virtual Appliance

Model	Memory	Disk	CPU	Interfaces
BBv-2	2 GB	32 GB	2	4
BBv-5	4 GB	32 GB	4	4
BBv-10	4 GB	32 GB	4	4
BBv-100	8 GB	120 GB	4	8
BBv-1000	16 GB	240 GB	8	9, with a limit of up to 26
BBv-10000	32 GB	480 GB	32	9, with a limit of up to 26

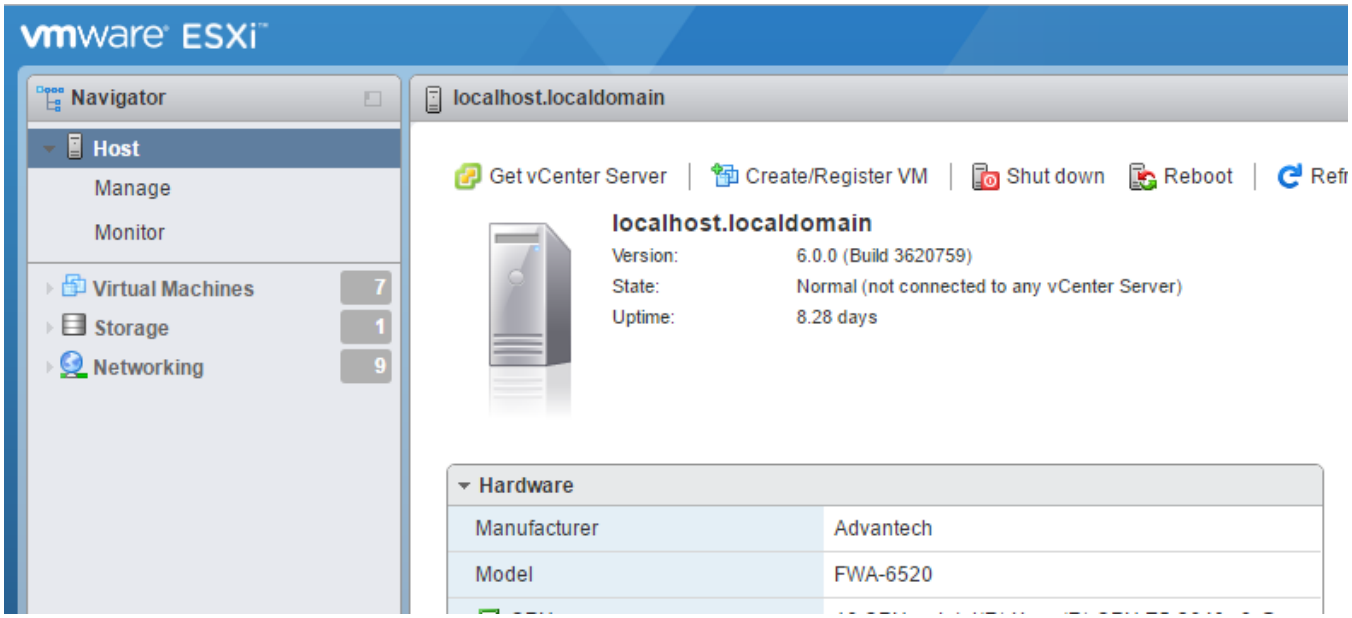
To import, download the Open Virtual Appliance (OVA) from Blockbit NGFW, for more information see the chapter *Download* OVAs.

1. Using your preferred web browser, access the VMware ESXi management console on the VMware Host Client;
2. Fill in the fields with the following information:

- ***User name*:** User registered in VMware;
- ***Password*:** User password;
- Click on the **"Log in"** button.

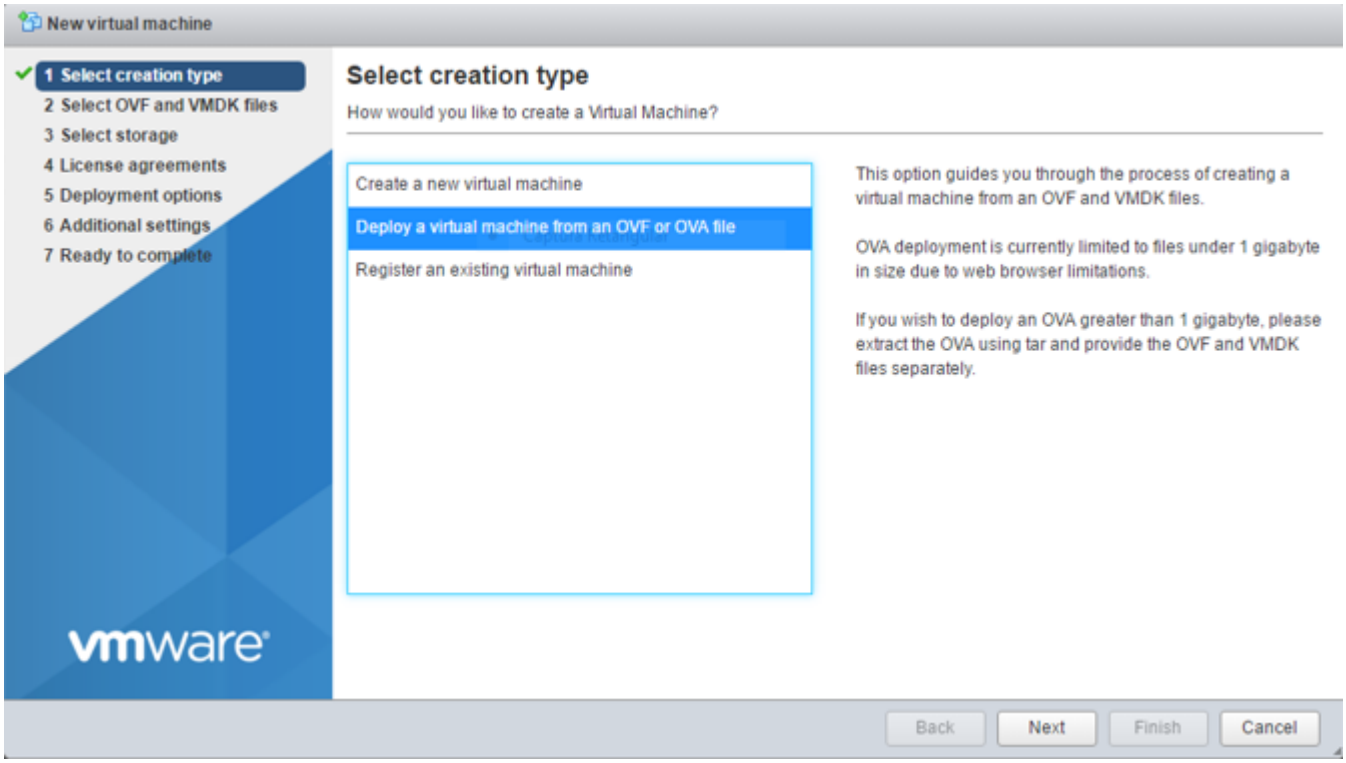
Login VMware

3. Click on "Create/Register VM";



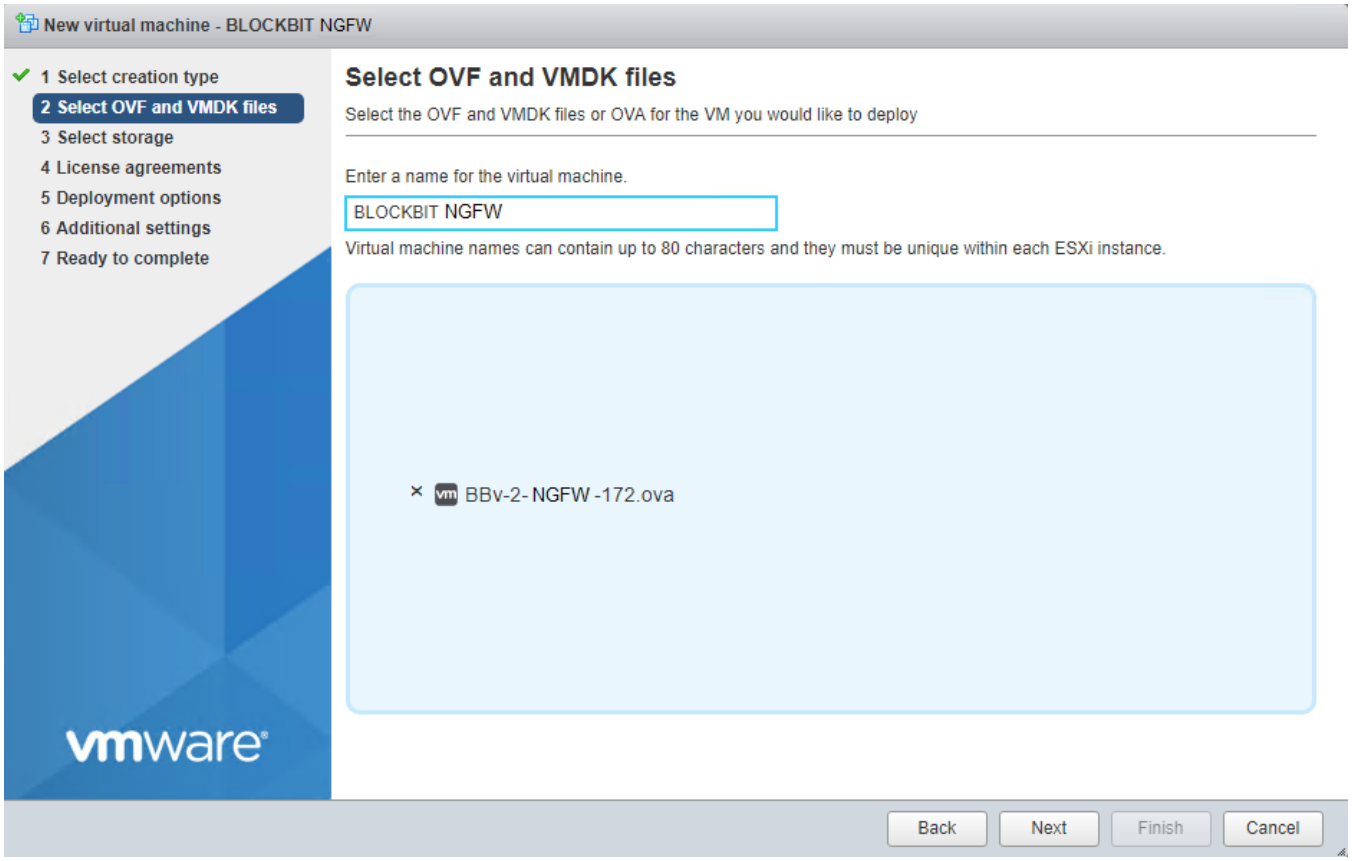
Console VMware

4. Select the option “Deploy a virtual machine from an OVF or OVA file”;



Select creation type

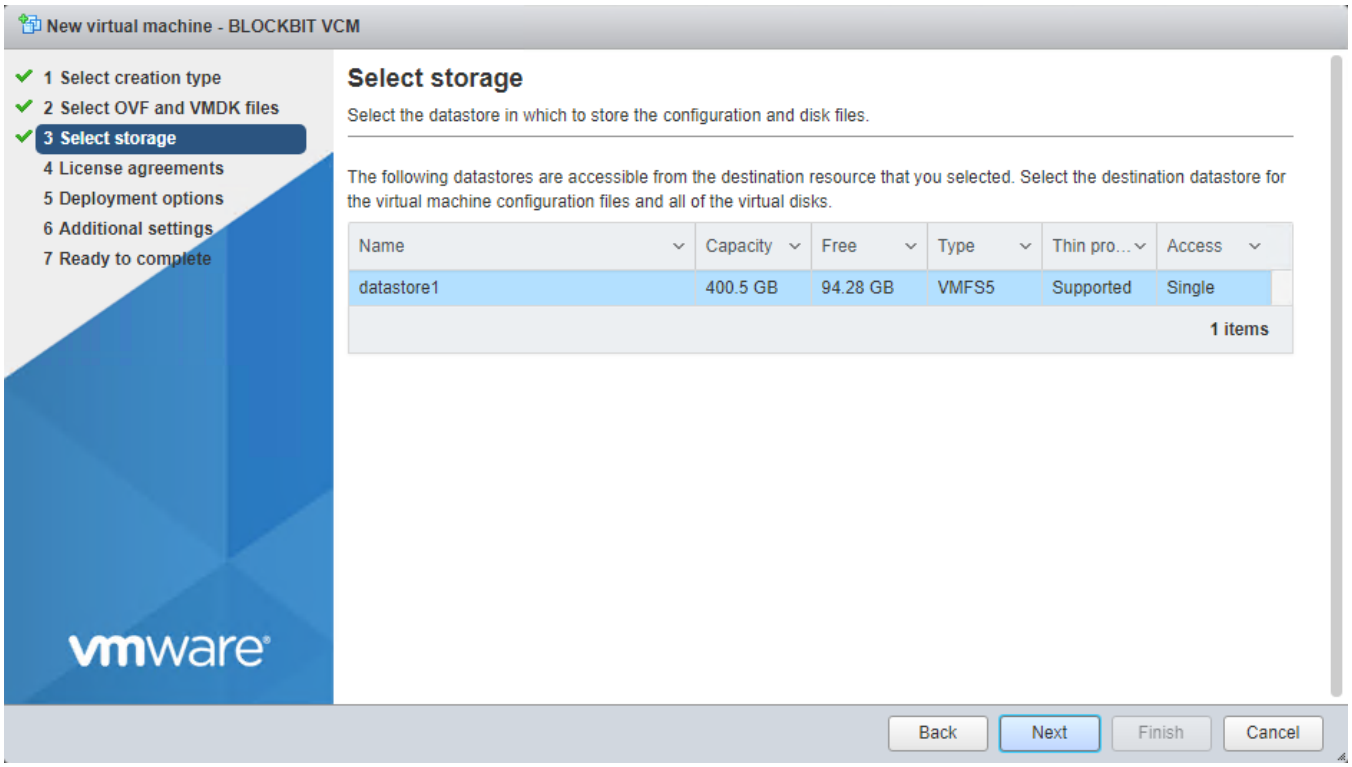
- Click the “Next” button.
- Select the image of the Blockbit NGFW that was downloaded from the Blockbit website and enter the name of the machine in the field “Enter a name for the virtual machine”. Ex .: Blockbit NGFW;



Select OVF and VMDK files

- Click the “Next” button;

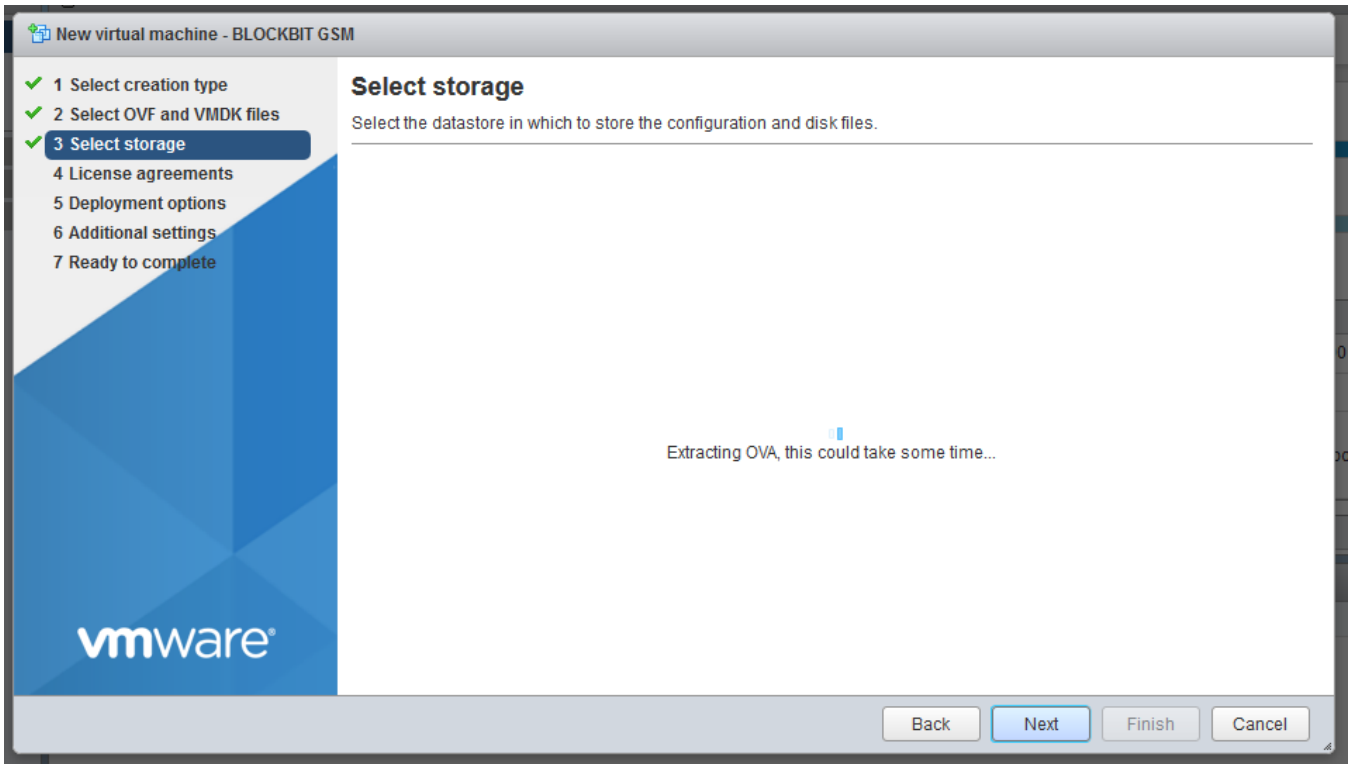
5. Select the desired storage. Ex .: datastore1;



Select Storage

- Click the “Next” button;

6. Wait for the OVA to upload. While uploading, the following message will appear: “Extracting OVA, this could take some time ...”. Wait for the completion of this process, which should occur automatically;

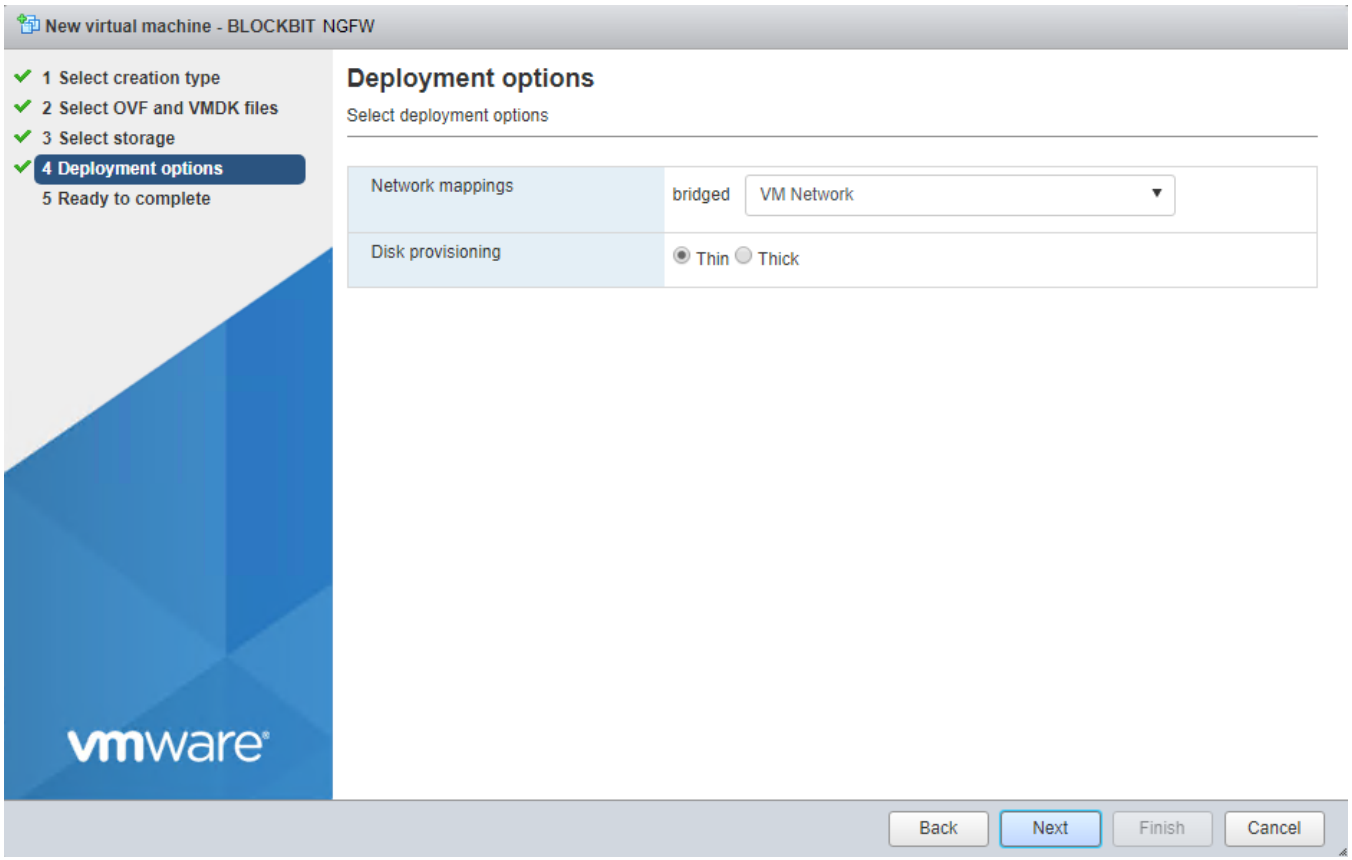


Select Storage – "Extracting OVA, this could take some time..."

7. Configure virtual machine settings:

- ***Network mappings*:** Set the network mode appropriate for your environment. Ex.: Mode bridged;
- ***Disk provisioning*:** Set the option to your preference. A brief description of the options follows:
    - **Disk *Thick*:** They are disks fully allocated in the datastore, that is, if you create a Thick disk with 20GB, it will occupy 20GB of your datastore;
    - **Disk *Thin*:** It is a type of disk that allocates only the space that is written by the virtual machine's operating system. For example, if you create a 20GB disk for a VM, initially it will occupy only a few KB/MB in the datastore, however, the moment you start recording data on it through the operating system, its size can reach the limit of 20GB.

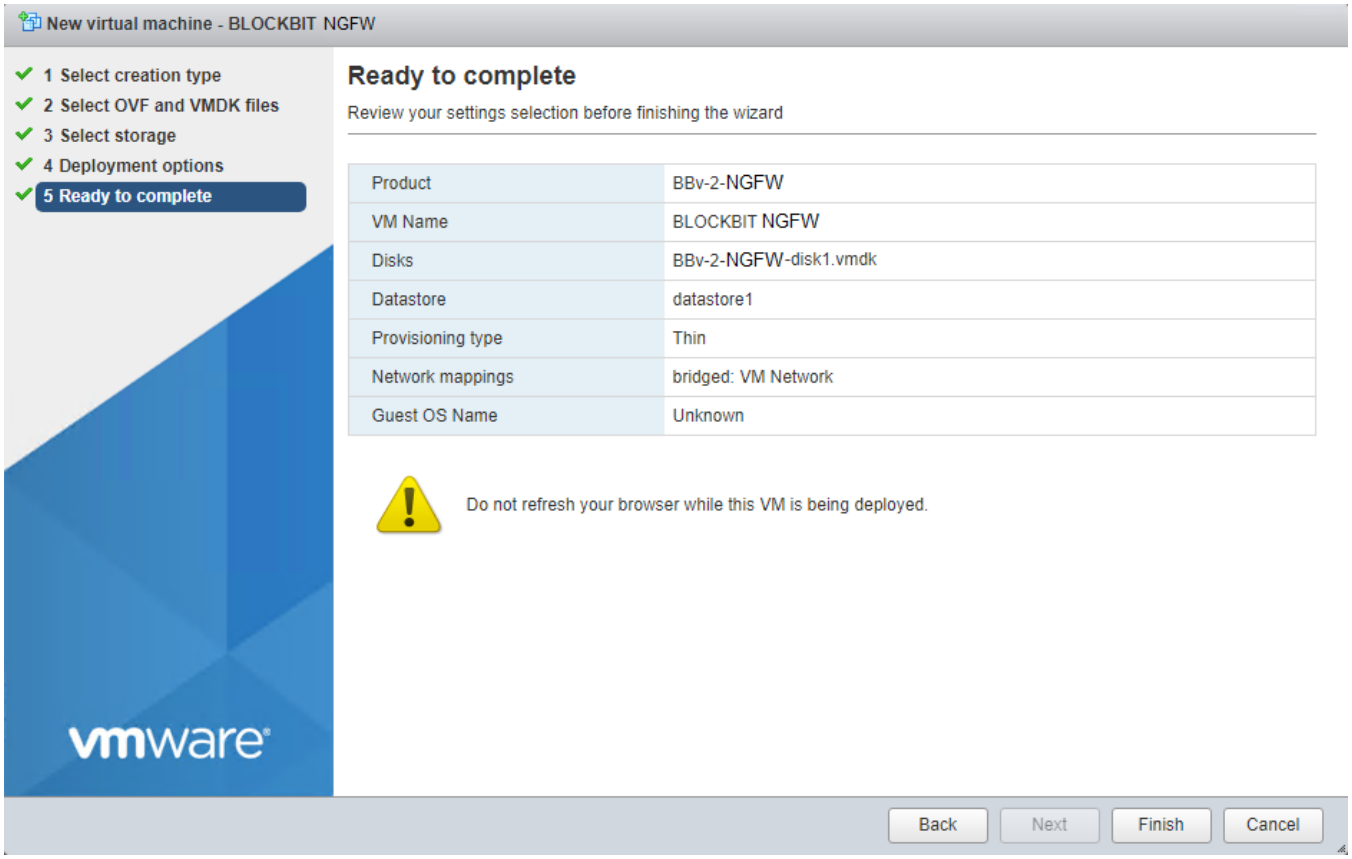
For more information, see the VMware manual. In this example, the configuration "Disk provisioning - Disk Thin" will be used.



Deployment options

- Click the "Next" button.

8. Review the configured settings before finalizing upload;



Ready to complete

- Click the "Finish" button.

The import is complete, just click on the “Power on” button to start the virtual machine and proceed to install Blockbit NGFW.

Next, see the settings that must be made at the first access.

Import and Export 1.5 to 2.0 - First Access

The initiation process presented below is the same for both Hardware Appliances and Virtual Appliances.
There is no need to perform any steps, just wait until the login screen is released, as shown by the image below:

Login screen – Blockbit NGFW

You will now need to configure the IP. To do so, perform the following steps:

1. ***Localhost login*:** Log in through the CLI console;
2. After performing the Authentication in the CLI console, fill in the following fields:

- ***Login*:** admin
- ***Pass*:** admin

It is highly recommended to change the default password for the "admin" console user. To change the default password, it is necessary to create a secure password. This password must contain at least 8 characters with upper and lower case letters, numbers and special characters.

To change the password, type the command below:

```
Enter the passwd command and type "Enter".
Enter the current password and type "Enter".
Enter the new password and confirm it.
```

After performing this procedure the password will have been successfully changed.

3. Change the IP address of the Blockbit NGFW;

The default IP address for Blockbit Network Security is 192.168.1.1. This IP is used on the eth1 port. In this guide we will use the IP address 172.16.102.136 as an example. If you want to change, follow the steps below:

Configuration details:

***IP*:** 172.16.102.136
***Mask*:** 255.255.255.0
Default Gateway: 172.16.102.1

If you need to check your appliance's UUID, enter the command [show-uuid].

In old versions of the NGFW, the management interface was eth0, as of NGFW 2.0 this interface is used for *Zero Touch Provisioning*, for more information, check the GSM manual. With this in mind:

Eth0 is the main interface, it is a dynamic WAN interface, used for internet access and device provisioning.

Eth1 is the management interface with the default IP for NGFW configuration, it will be configured below.

Enter the commands:

```
Ifconfig eth1 172.16.102.136/24, and type "Enter".
route add default gw 172.16.102.1, and type "Enter".
```

After performing this procedure, the IP address will have been changed.
With the command below it is also possible to edit the IP address of the Blockbit NGFW:

```
Enter the command blockbit> changeip.
Type "Enter".
```

Then see how to configure the exception in the browser of your choice in order to facilitate access.

Import and Export 1.5 to 2.0 - Exception Configuration

This section will introduce how to configure an exception in web browsers: Google Chrome and Mozilla Firefox.
When performing the first access to the Blockbit NGFW Web Interface, it is normal for browsers to issue a security alert reporting a certificate error**.** This is because the browser does not recognize any certifying authority that validates access to this page as reliable. Therefore, it is necessary to configure the exception in the web browser.
To configure the exception, follow the steps:

1. Connect to your internet browser and access the address: https://172.16.102.136:98. If you have changed the IP address, use the changed IP;

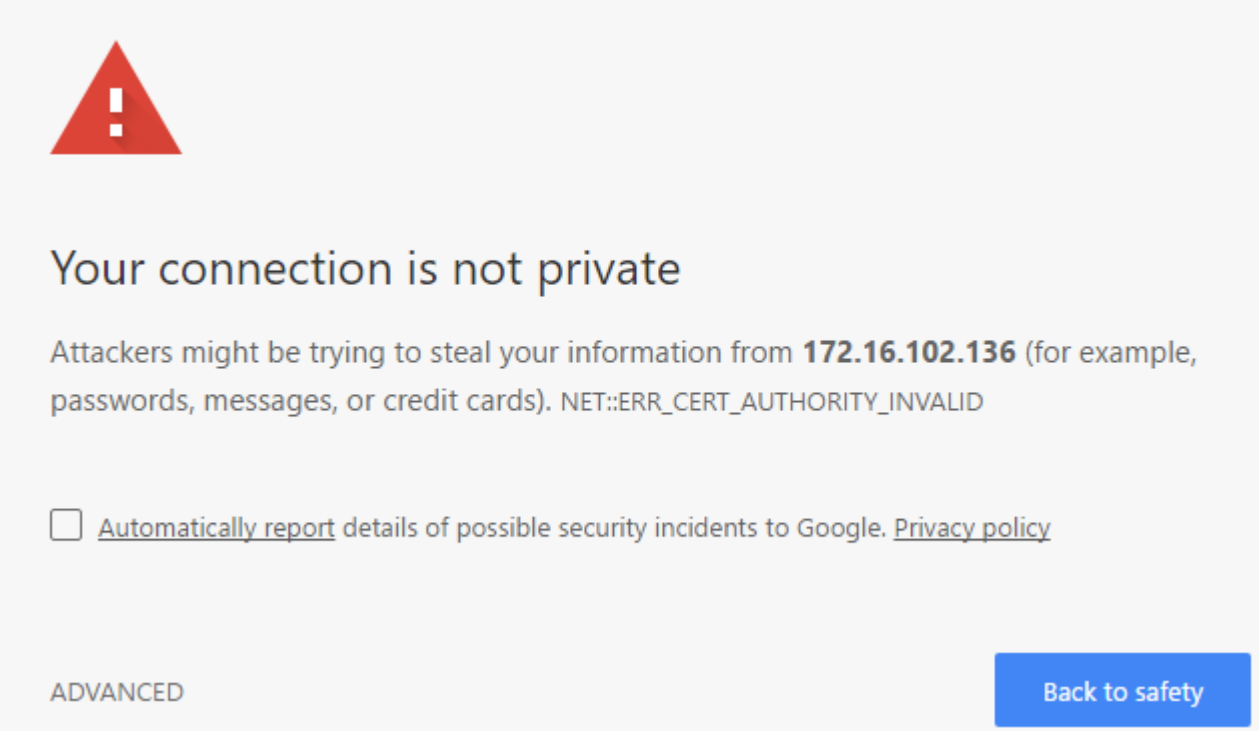
If the browser issues a **SECURITY ALERT**, follow the recommendations below.

Each browser has a procedure to release the connection as trusted. Follow the directions on how to proceed.

Setting exception in Google Chrome

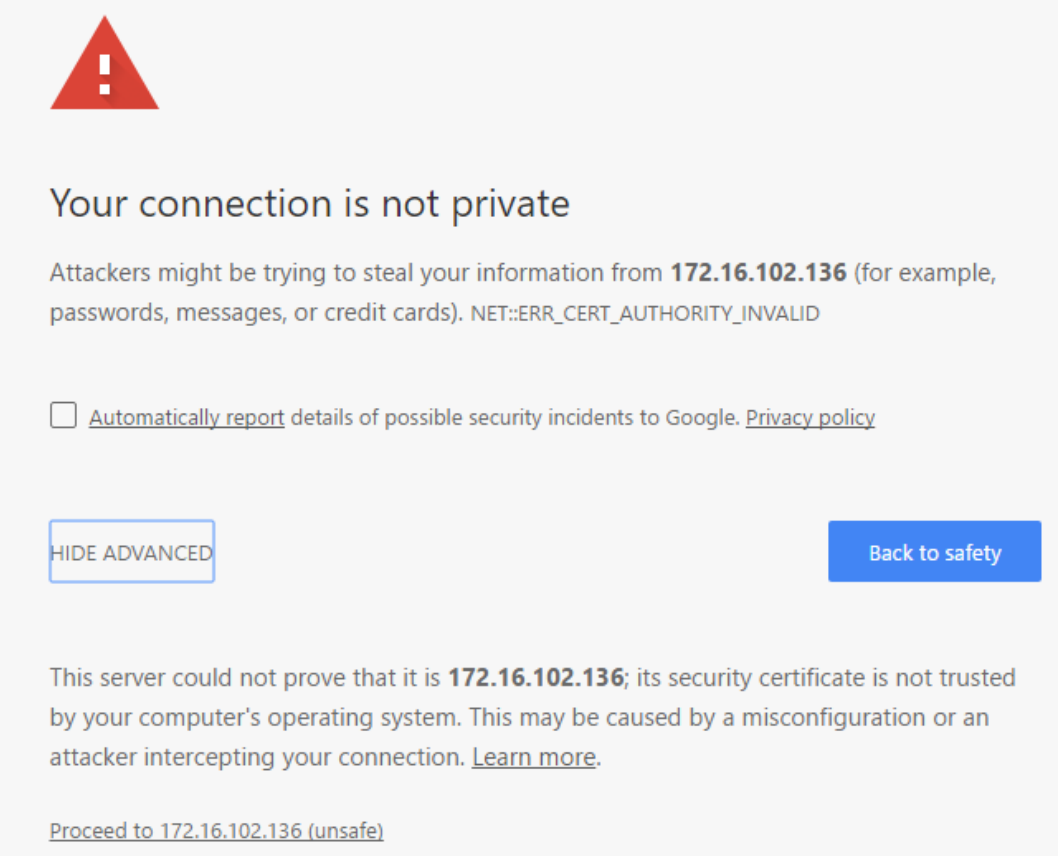
To configure the exception in Google Chrome, follow these steps:

1. Click the "Advanced" button;



Chrome exception - "Advanced" button

2. Click on the "Proceed to 172.16.102.136 (unsafe)" link to accept this page as trusted;



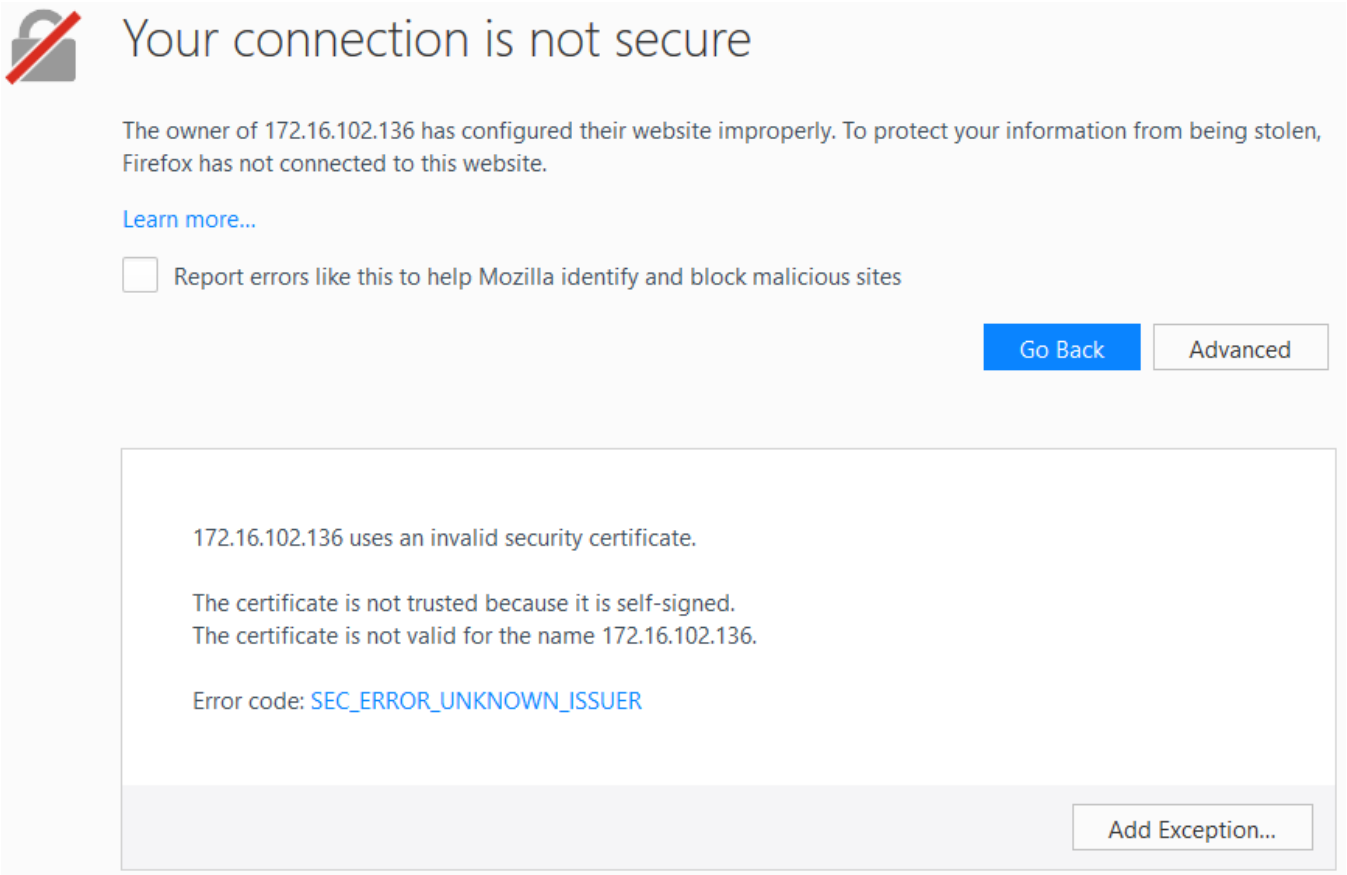
Chrome exception - "Proceed to 172.16.102.136 (unsafe)"

Exception setting in Google Chrome was successful.

Setting exception in Mozilla Firefox

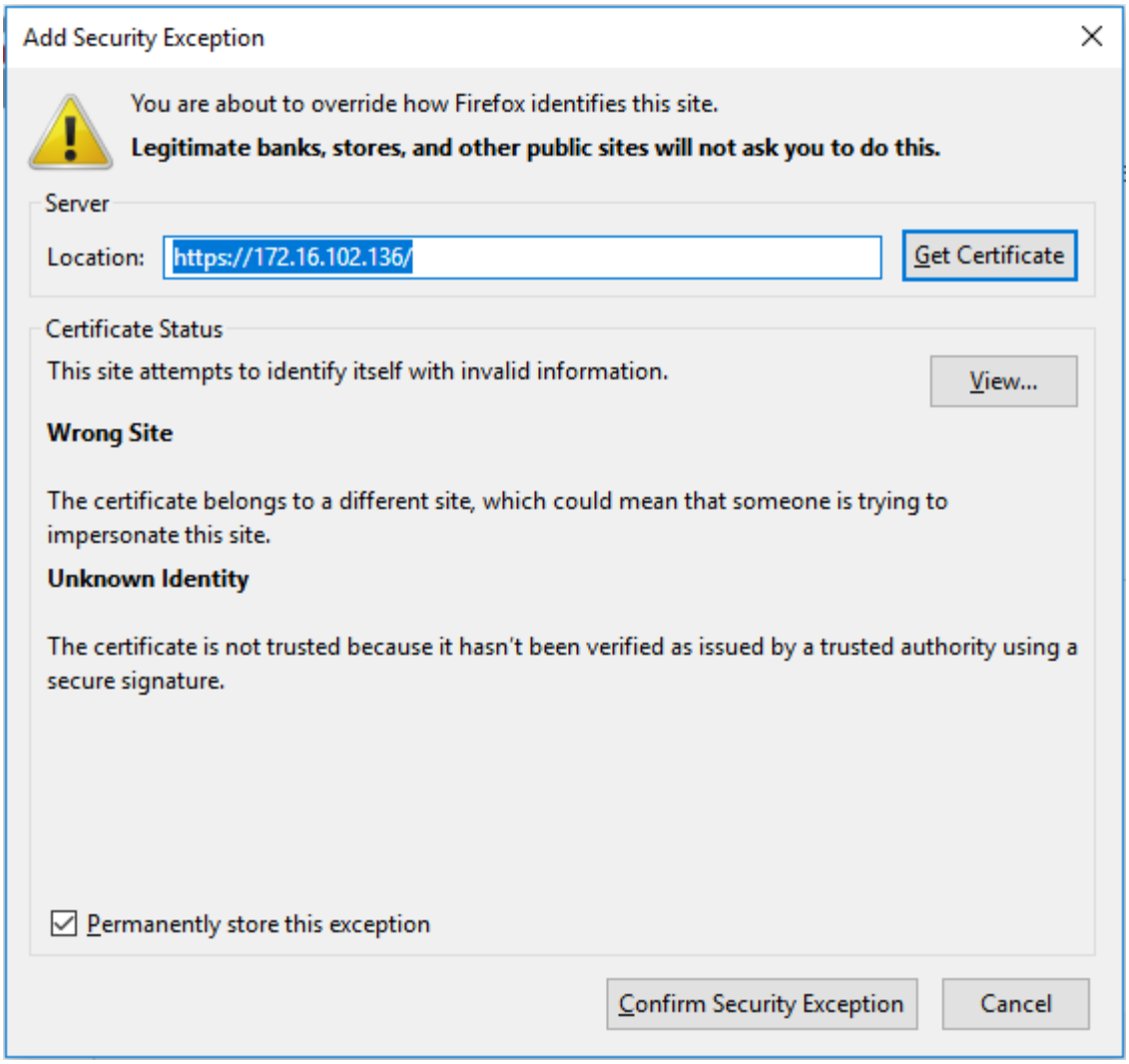
To configure the exception in Mozilla Firefox follow these steps:

1. Click the "Advanced" button;
2. Click the "Add Exception ..." button;



Mozilla Firefox exception - Your connection is not secure

3. Click on the "Confirm Security Exception" button.



Exceção *Mozilla Firefox – Confirm Security Exception*

Exception configuration in Mozilla Firefox was successfully performed.

Next we will detail the installation wizard.

Import and Export 1.5 to 2.0 - Installation Wizard

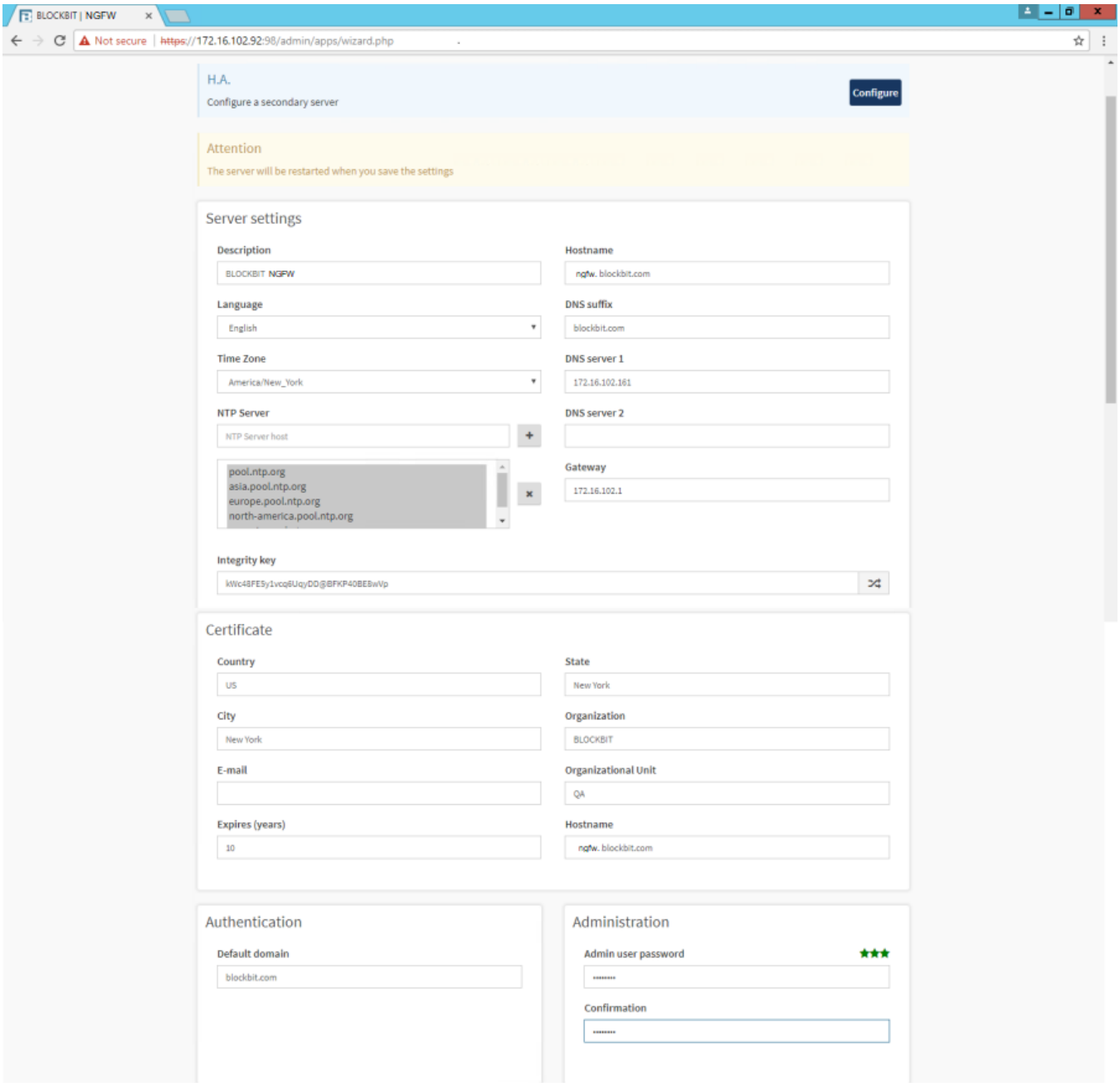
This section will introduce how to configure the Blockbit NGFW Installation Wizard.

The installation process and the correct completion of all fields required by the form will be presented below.

Installing the Blockbit NGFW

To install Blockbit NGFW, follow these steps:

1. Connect to your internet browser and access the address: https://172.16.102.136:98. If you have changed the IP address, use the changed IP:



Installation Wizard

2. Enter the following data in the "Server settings" frame, for the initial network settings of the Blockbit NGFW:

- ***Description*:** Field to describe the server name. Ex.: Blockbit NGFW;
- ***Language*:** Select the default language. Ex.: *English*;
- ***Time Zone*:** Select the time zone your business is in. Ex.: *America*/*New York*;
- ***NTP Server*:** Set the clock synchronization server. Ex.: pool.ntp.org;
- ***Hostname*:** It can be anyone as long as it complies with FQDN - Fully Qualified Domain Name. Ex.: utm.blockbit.com;
- ***DNS suffix*:** Network domain. Ex.: blockbit.com;
- ***DNS server* 1:** Set the network or internet DNS server. Ex.: 176.16.102.161;
- ***DNS server 2*:** Set the secondary DNS for your network or the internet;
- ***Gateway*:** Set the default network route. Ex.: 176.16.102.1;
- ***Integrity key*:** System integrity key, used in the backup file encryption process. This field is automatically generated.

3. Enter the following data in the "Certificate" frame, this information will be used to create the SSL certificate in the administration console of Blockbit NGFW:

- ***Country*:** Set the country. Ex.: *US*;
- ***State*:** Set the state. Ex.: *New York*;
- ***City*:** Define the city. Ex.: *New York*;
- ***Organization*:** Set your company name. Ex.:Blockbit;
- ***E-mail*:** Set the administrator email. Ex.: admin@blockbit.com;
- ***Organizational Unit*:** Define the department. Ex.: QA;
- ***Expires* (*years*):** Set the certificate validity time. Ex.: 10 years;
- ***Hostname*:** Set the FQDN for the certificate. Ex.: utm.blockbit.com.

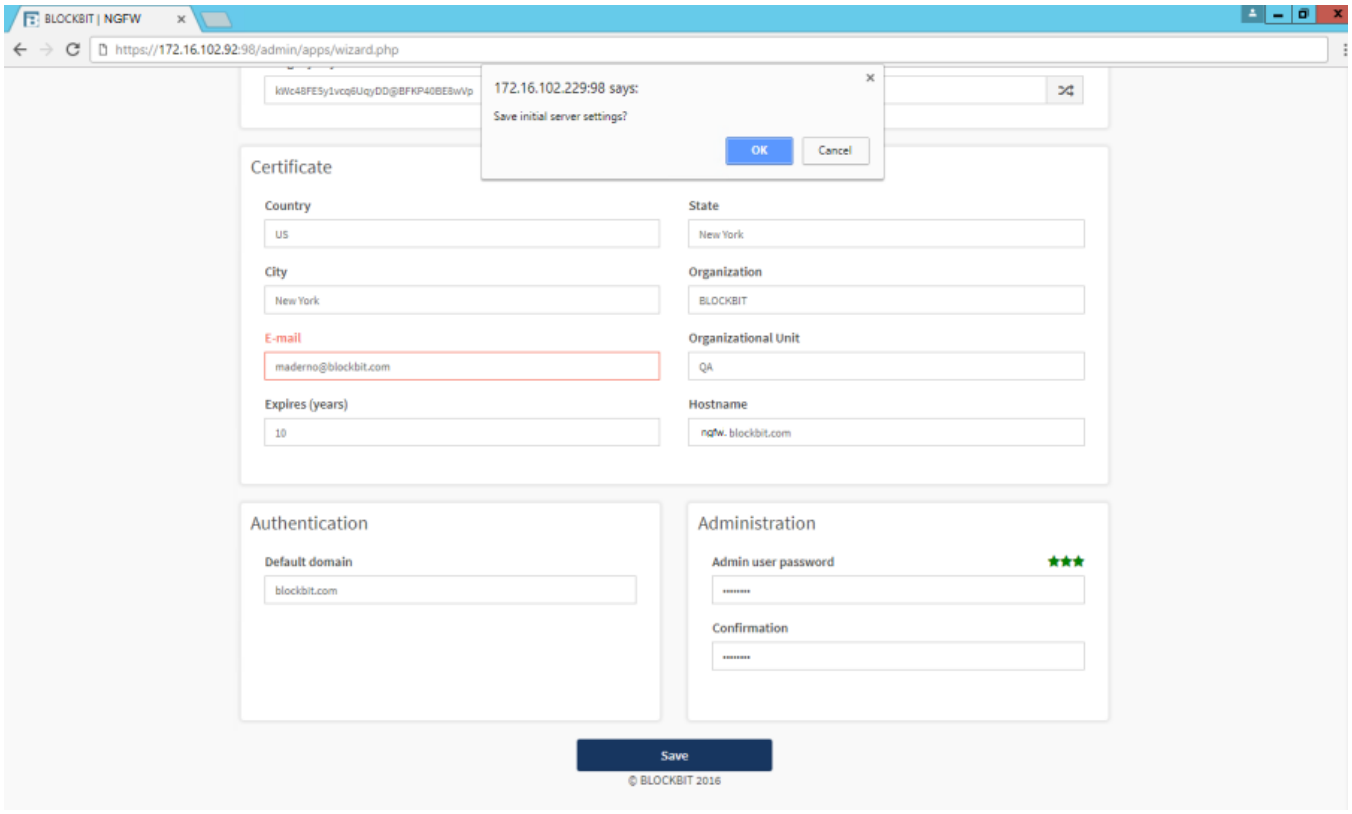
4. Enter the following data in the "Authentication" frame, define the default local domain for authentication of Blockbit NGFW users.

- ***Default domain***: Set the default authentication domain. Ex.: blockbit.com.

5. Enter the following data in the "Administration" frame, the password for the "admin" user of the Blockbit NGFW administration console:

- ***Admin user password***: Enter a password of at least eight characters. The password must contain uppercase, lowercase letters and special characters. Ex.: q1W@e3R$;
- ***Confirmation Save***: Confirm the password entered above.

6. Click the "Save" button. The screen below will be displayed asking for confirmation, when clicking "ok" the system will apply the settings and will be restarted.



Installation Wizard - Form

- Click the "OK" button. The system will apply the settings and be rebooted.

After completing these steps, the Installation Wizard will have been successfully completed.
Wait for initialization, the browser will AUTO-REFRESH the address of access to the WEB interface and return to the login interface.

Blockbit NGFW - Login screen

We will continue accessing the web interface.

Import and Export 1.5 to 2.0 - Accessing Web interface

Use one of the recommended browsers.

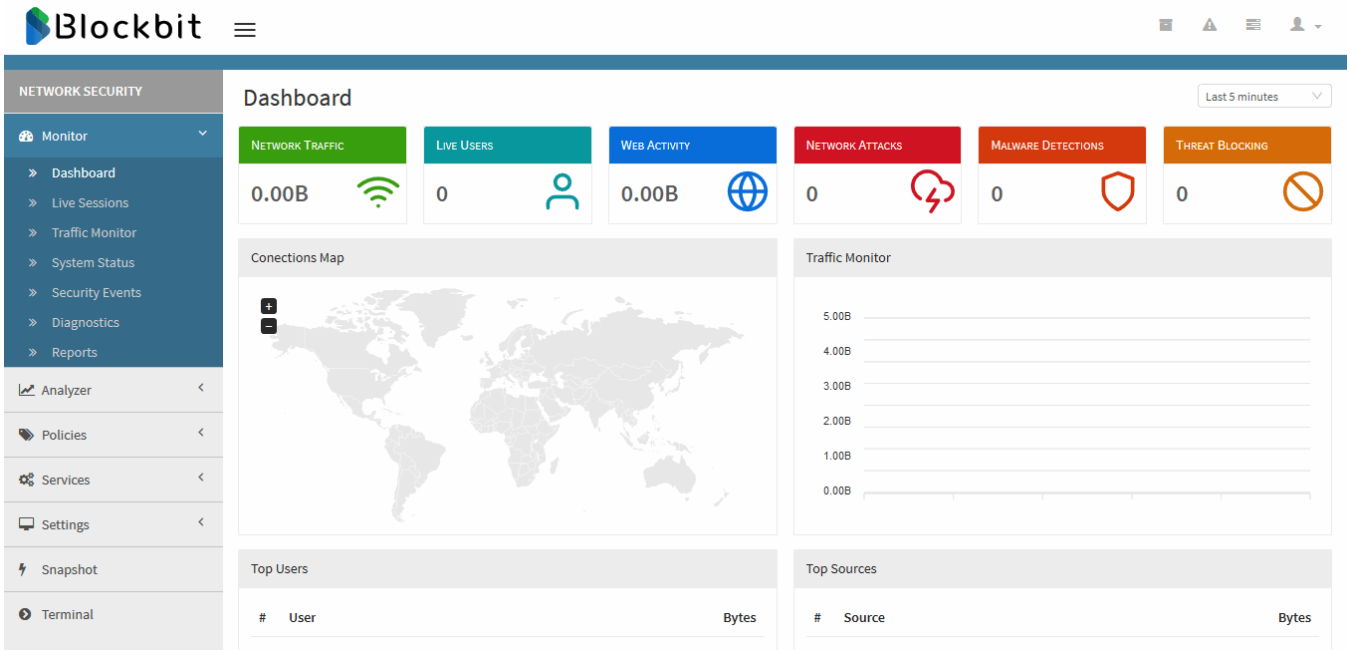
1. Connect to the internet and access the address: https://172.16.102.136:98. If you have changed the IP address, use the changed IP;
2. Access using the following data:

- ***User*:** The registered user's login, moreover, if the email has been registered, it is possible to use it to login. Ex.: admin;
- ***Password*:** Registered password;
- ***English*:** The desired language is defined to access the Web Interface. The language can be English or Portuguese. Ex.: *English*.

Login Screen - Blockbit NGFW

- Click the **[** Login **]** button to access the Web Interface.

The main screen of the Blockbit NGFW will be displayed: The Dashboard.



Blockbit NGFW main screen - Dashboards

Finally, we'll demonstrate how to license.

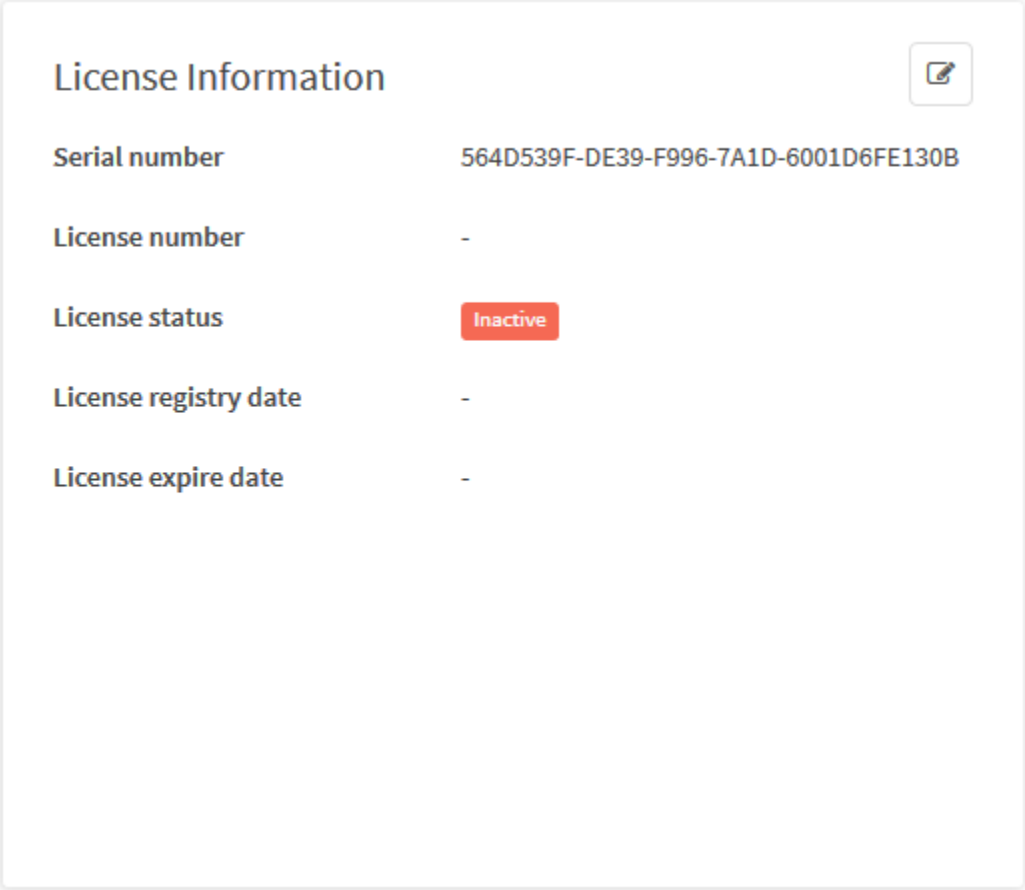
Import and Export 1.5 to 2.0 - Licensing

To use the features of the Blockbit NGFW it is necessary to license your installation, to do so, follow these steps:

In order to license Blockbit Network Security, it is necessary to be connected to the internet and with access to Port 443 without a proxy to the following addresses:
https://license.blockbit.com
https://update.blockbit.com

To apply or renew the activation license it is necessary to provide the UUID - Universal Unique Indicator of your Blockbit NGFW.

1. To view the UUID of your device, access the Settings menu, on the System tab:



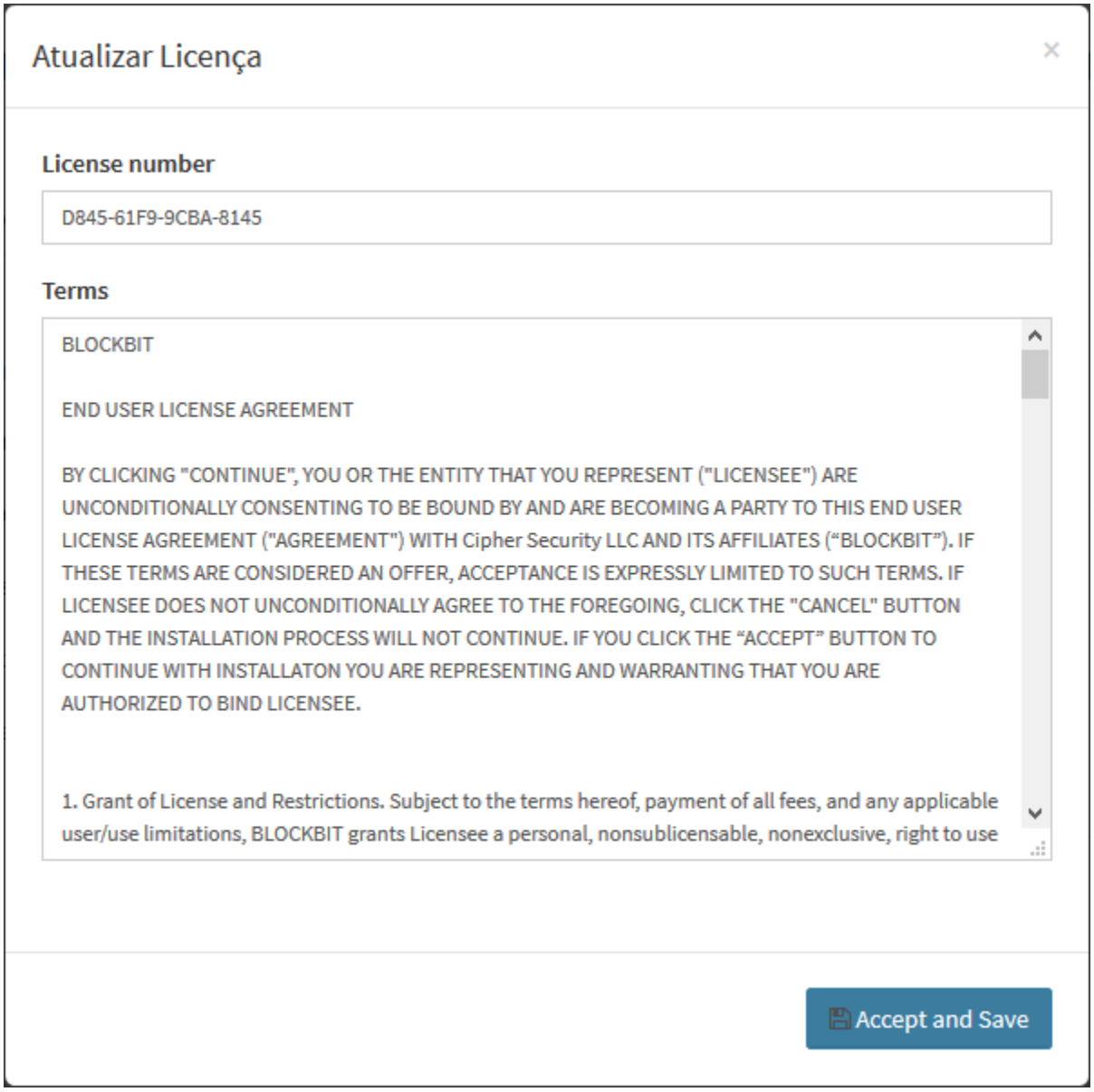
Dashboard – System

- The License Information widget will inform the Serial Number (or UUID): Ex.: 564D539F-DE39-F996-7A1D-6001D6FE130B.

You can also find out the UUID using the "show-uuid" command on the console. For more information check this page: [show-uuid].

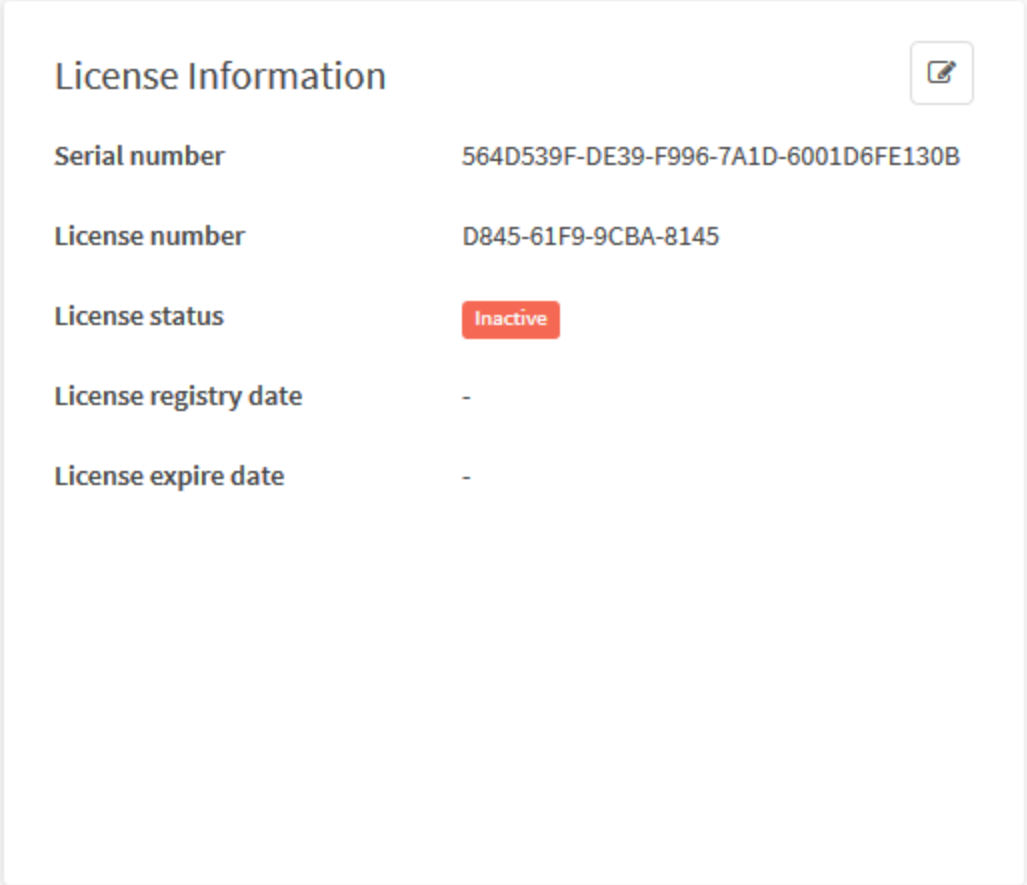
- Copy the UUID and forward it to your service channel, so that your license number is provided;
- You will receive the license number code from your service channel. Ex.: D845-61F9-9CBA-8145.

2. Click on [ ], the screen below will be displayed:



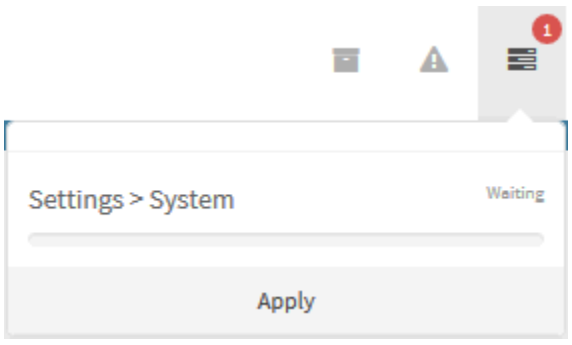
Update License

- ***Serial Number*:** Enter the license number in this field. Ex.: D845-61F9-9CBA-8145;
- After that click on the ***[*** Accept and Save ***]*** button, the screen below will be displayed.



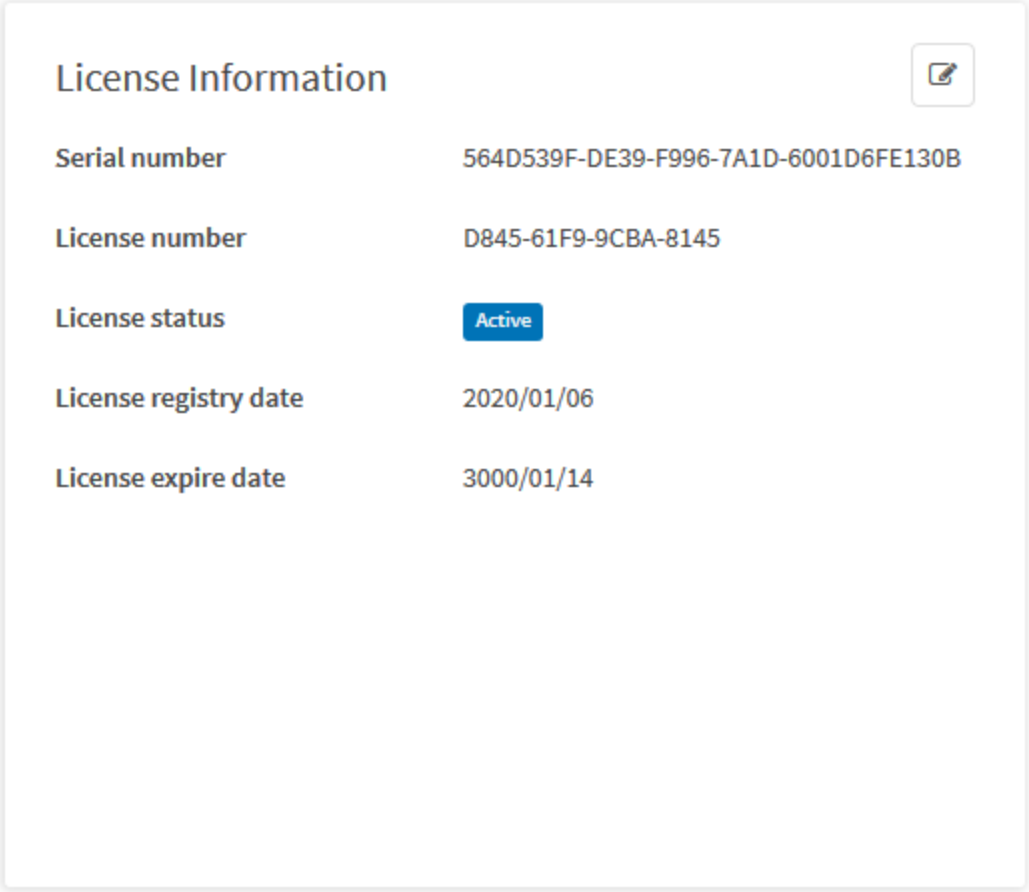
Update License - Inactive

After saving the license, the request will be sent to a command queue where it can be applied on the system. To access the command queue, click **[ ]** . The screen below shows the command queue waiting to be executed;



Apply queue

- After clicking ***[Apply]***, wait for the system to apply the settings for product licensing. As shown below:



Update License - Active

This concludes the product licensing.

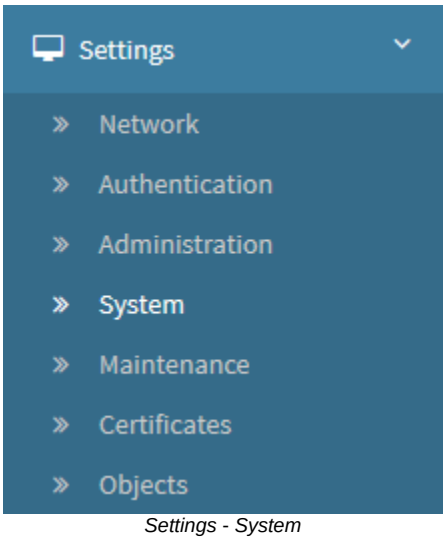
In the next chapter we will deal with the Import process.

Import and Export 1.5 to 2.0 - Import

Firstly, it is important to note that the import procedure can only be executed once, in case of any unforeseen circumstances, it will be necessary to execute the command **[rewizard]** and reinstall the system before executing the import once again..

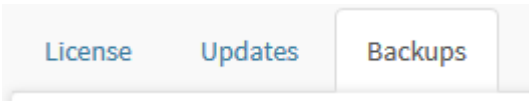
For more in-depth information about how the **[rewizard]** command works or how to reinstall the system, see the Blockbit NGFW manual.

As previously mentioned, first make sure that the logged in user has **super user** permissions. To perform the export, enter the Settings option and select the System option.



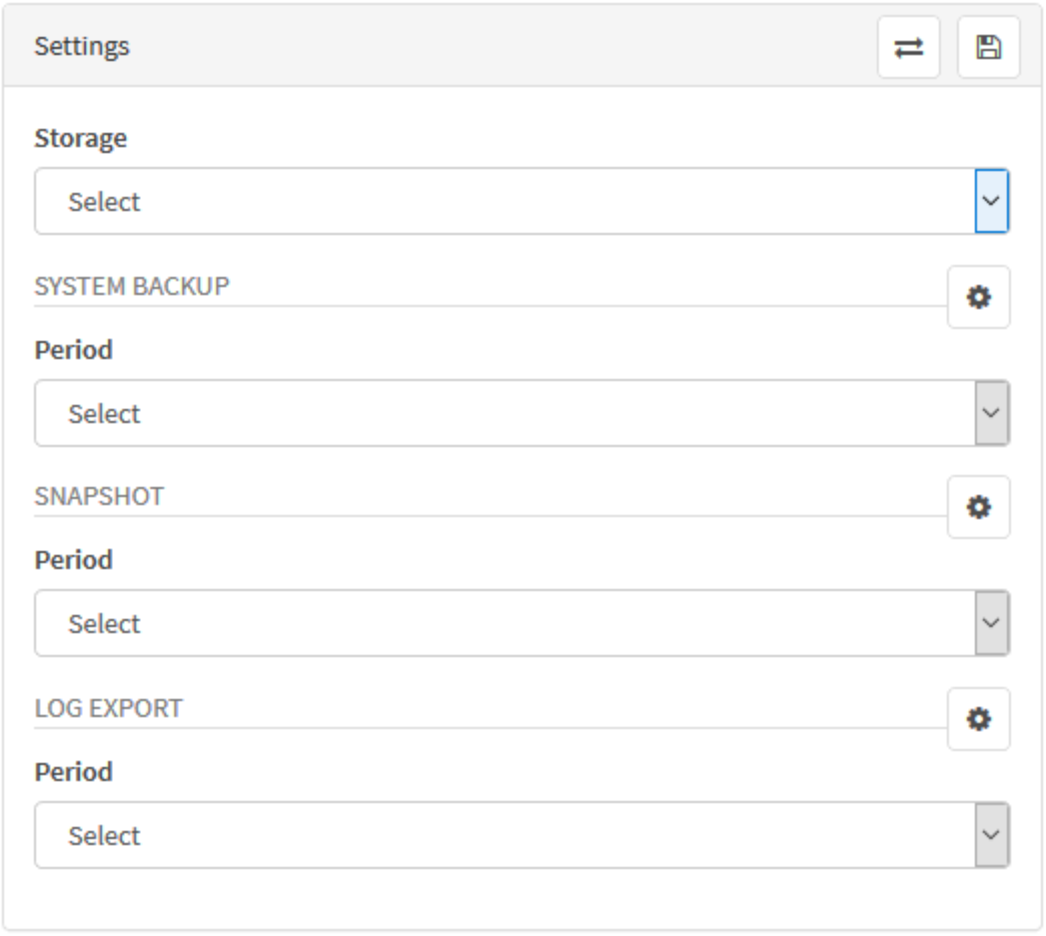
Settings - System

Click on the Backups tab:



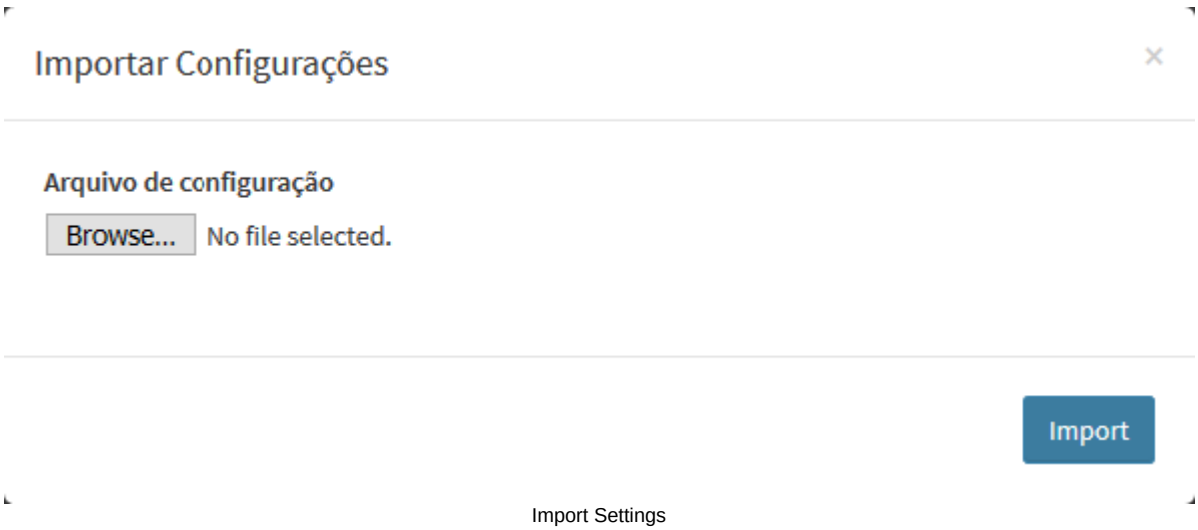
System - Backups

Access the Settings panel:



Backups - Settings

When you click [ ], the “Import Settings” window will appear, as shown below:



Import Settings

Click the [Browse...] button and select the “JSON” extension file that was created during the export process.

⚠ Policies with Web Filter settings will be imported, but will be disabled. This is due to the differences in the functioning of these configurations and the new functionalities of the NGFW 2.0, therefore, a reconfiguration is necessary..

In addition, thanks to changes in the system architecture, the Deep Inspection and Antimalware settings will NOT be imported. It is necessary to configure them in the NGFW 2.0.

For more details see the manual.

Finally, click **[Import]** to start the import process.

Note that the following data will NOT be imported:

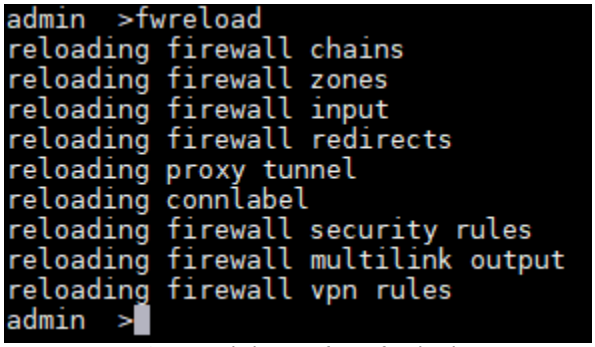
- Network settings (Settings tab);
- Personal information (in System, Authentication option, in the Portal tab);
- GSM settings;
- Notification Settings;
- Dynamic routing settings;
- Deep Inspection settings;
- Antimalware Settings;
- Empty IPv6 settings;
- Session Management with default NGFW values;
- Backup and Storage Settings;
- Scheduled or automatic update settings;
- H.A settings;
- IPSEC VPN Failover Settings;
- IPS settings.

Import time varies according to the characteristics of each environment.

If using an H.A. environment, the user must update the Master, then the Slave and configure the environment as H.A. after performing the previous steps.

At the end of the import, you will be redirected to the Login screen. Just login again to use the system normally.

If something unexpected occurs with the import, it is recommended to reload all firewall configurations, Blockbit NGFW has a reload system in its CLI interface, being an alternative to make the settings effective, to do so, execute the command **[fwreload]**, as demonstrated by image below:



Command Line Interface - fwreload

ATTENTION: When executing this command, all accesses will be interrupted shortly.

For more in-depth information regarding the operation of the **[fwreload]** command, refer to the Blockbit UTM manual.

This concludes the objectives of this How to, for more in-depth information on how to configure or operate the NGFW 2.0, see the administrator's guide.

Blockbit

it's easy to be secure

www.blockbit.com

Blockbit NGFW - How to Upgrade Kernel

In this document we will cover the process of downloading and running the installer of the kernel update on Blockbit NGFW.

After reading and applying the steps in this tutorial you will be able to update your Blockbit NGFW kernel easily and safely.

Requirements

It is important to perform the step-by-step mentioned in this guide, since the kernel update will not be performed automatically by NGFW.

In addition, we ALWAYS recommend that a system SNAPSHOT of the latest version be performed before any update or upgrade procedure is performed and that the generated file be saved in a safe place. For more information on how to generate a snapshot, see this page.

This procedure is approved in Blockbit NGFW version 2.1.

In this guide, it will be necessary to execute a command to update the kernel manually through the CLI, for that, it will be necessary to have console access.

For more information on how to execute a console access or how to update your product, refer to the Blockbit NGFW manual.

Content

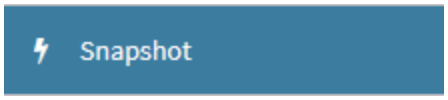
In this how to the following topics will be covered:

- How to generate a Snapshot;
- Console Access;
- System Update;
- Performing the kernel update;
- System Reboot;
- Updating the kernel in a clustered environment.

IInitially we will analyze how to create a Snapshot.

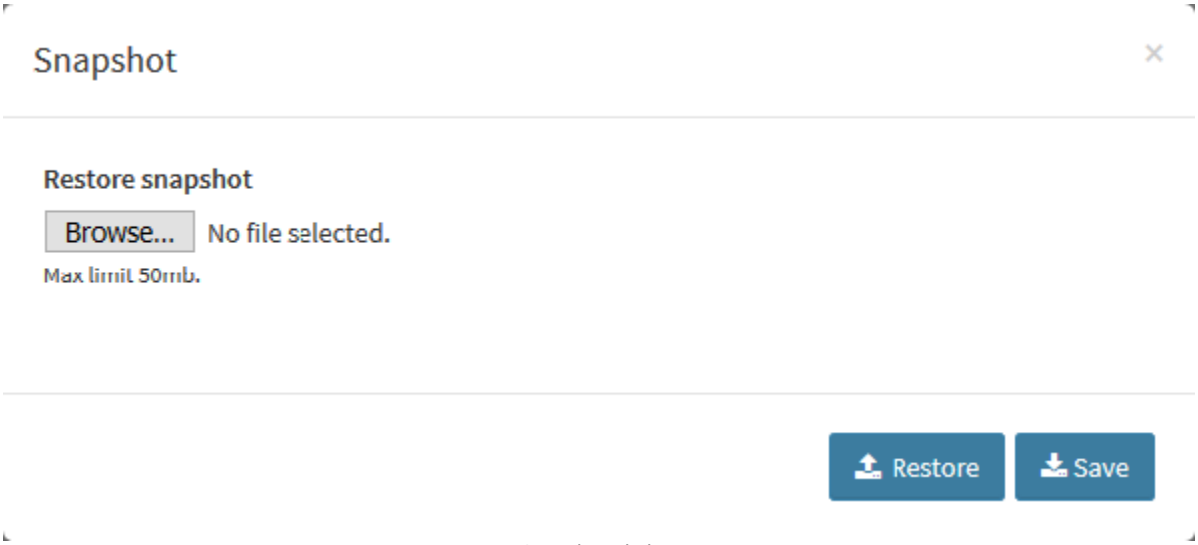
Blockbit UTM - How to Upgrade Kernel - How to create a Snapshot

Initially, log in to the interface, locate the Snapshot button in the side menu on the left of the screen and click on it.



Snapshot option

The following window will appear:



Snapshot window

Click the [] button to take a snapshot. Keep the file in a safe place.

WARNING: The execution of this snapshot is essential to guarantee the integrity of your data. After taking the snapshot, store it in a safe place.

After performing the steps previously mentioned, the snapshot will have been successfully generated.

Next, we'll look at how to access the console.

Blockbit UTM - How to Upgrade Kernel - Console Access

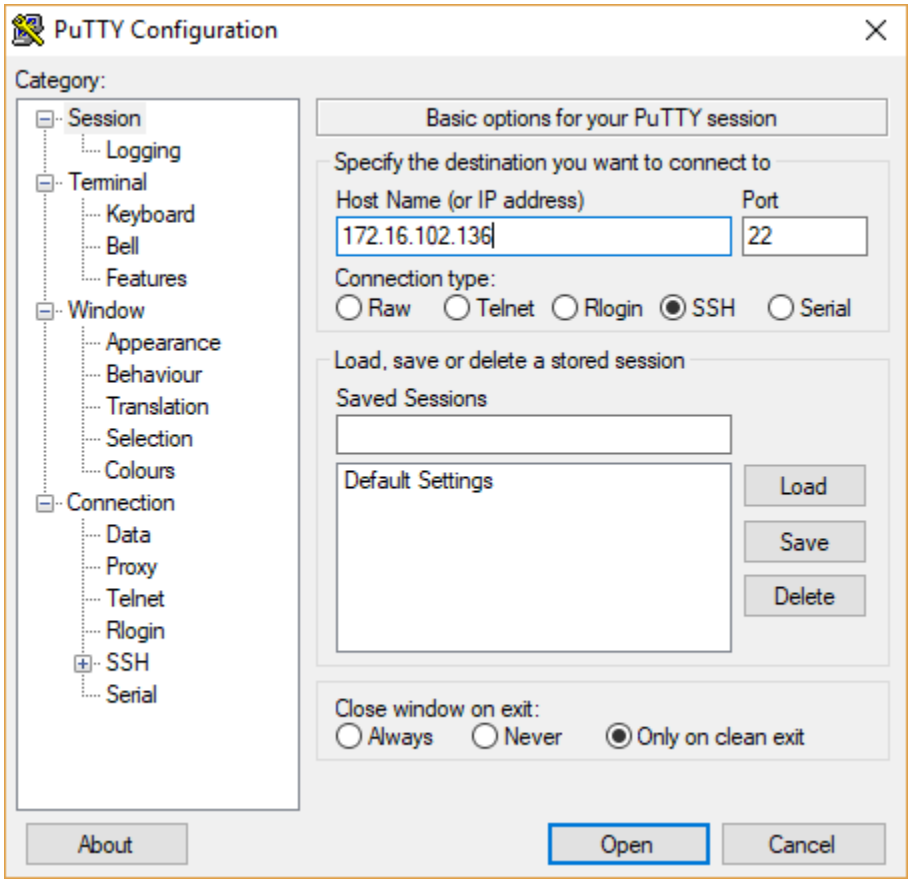
Blockbit NGFW provides a Command Line Interface (CLI) console feature, which allows the administrator to execute administrative and troubleshooting commands for the main system services. To perform the configuration you need an SSH client and Console. The minimum recommended applications are:

- *PUTTY*;
- *CygWin*;
- *Mobaxterm*.

Next we will present step by step how to access the Blockbit NGFW CLI console:

1. Check that the access device has a recommended SSH client already installed. In this case, we will exemplify the process using the “PUTTY” application;
2. Access the SSH console and fill in the fields:

- ***Host Name* (or *IP Address*):** Enter the Blockbit NGFW IP address. Ex.: 172.16.102.136;



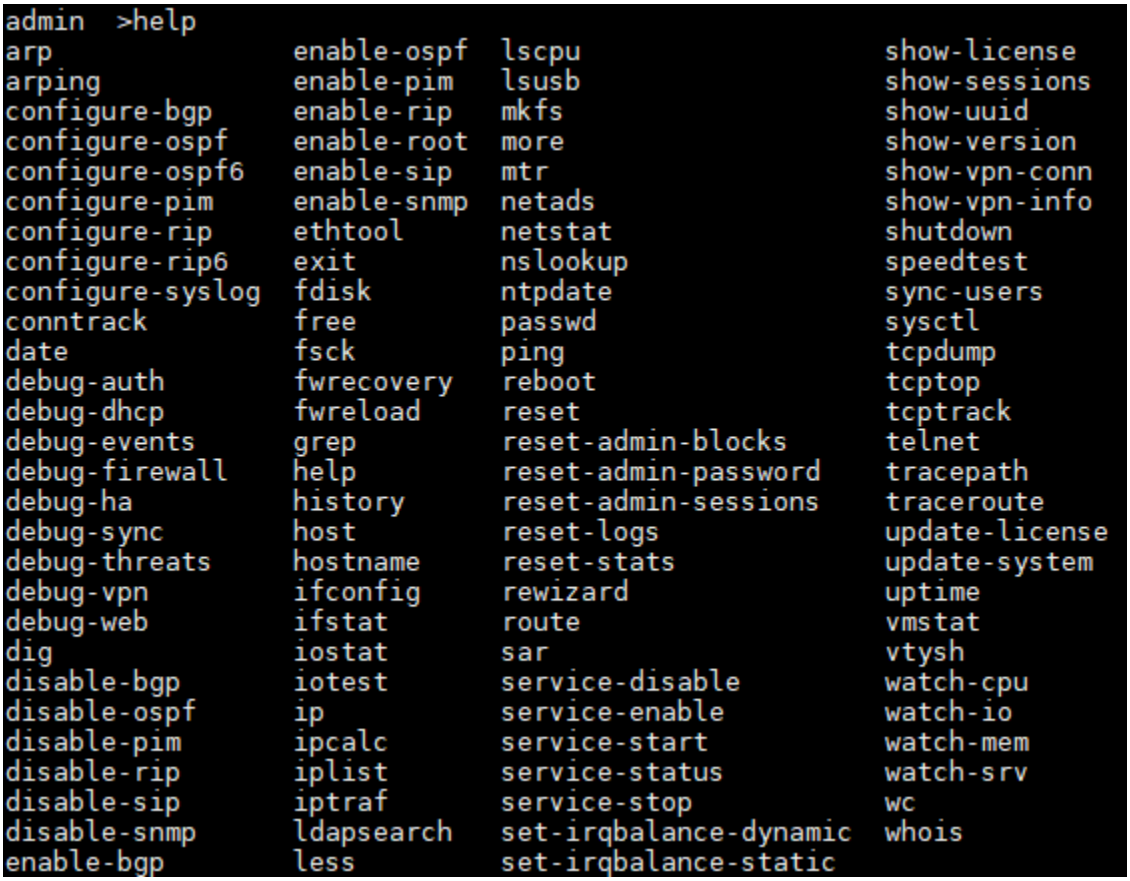
PuTTY Configuration

- Click on the “Open” button.

3. The console will appear, asking for a user and password;

```
In "login as:" type the user "admin" and press "Enter".
```

The image below shows the commands of the main system services.



Blockbit NGFW – *Command Line Interface*

For more information on how to access via the console, see this page of the Blockbit NGFW manual.

As a snapshot of the system settings has already been taken (if you have not already done this, see this page) the next step will be to turn off the secondary interface and update the system.

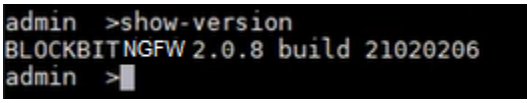
Blockbit UTM - How to Upgrade Kernel - System Update

Before updating the kernel, it will be necessary to purchase the packages related to NGFW 2.0.8, to do so, access the Primary Cluster console and enter the command **[update-system]**:

WARNING: We ALWAYS recommend that a FULL BACKUP of the latest system version and reports be made before any update or upgrade procedure is performed and that the files are saved in a safe place.

Command Line Interface – update-system

To confirm that the system has been updated, use the **[show-version]** command.



Command Line Interface – show-version

After installing the update previously mentioned, we will now update your NGFW kernel.

Blockbit UTM - How to Upgrade Kernel - Performing the Kernel Update

Access the Primary Cluster console to enter the system, in this step we will upgrade the system to the most current version, this step will also install the Kernel.

WARNING: It is worth emphasizing again that it is recommended to ALWAYS do a FULL BACKUP of the latest version of the system and reports before executing any update or upgrade procedure and that the files are saved in a safe place..

WARNING: At the end of the execution of this command, it will be necessary to restart your NGFW.

To avoid interruptions due to a network outage, it is suggested that the upgrade process be done directly through the appliance's console.

In the CLI of the Primary Cluster execute the command **[upgrade-blockbit]** as shown below.

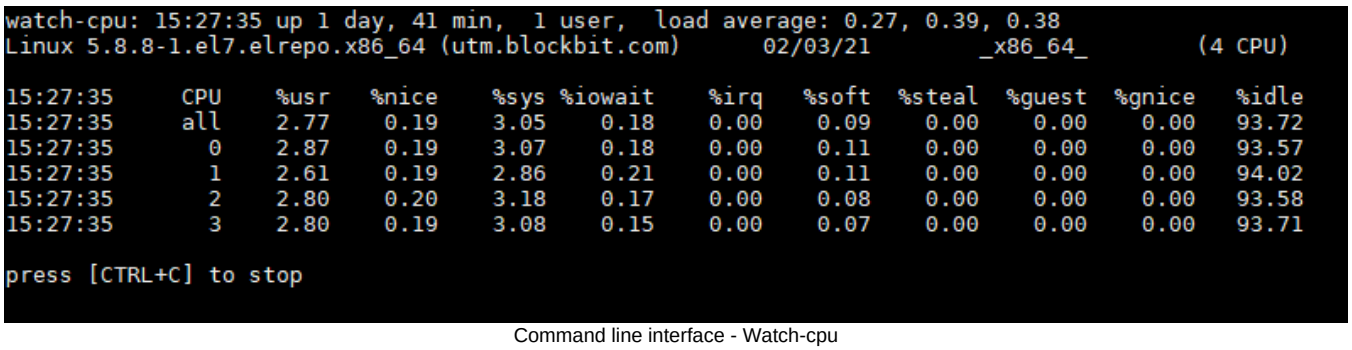
```
admin  >upgrade-blockbit
Are you sure do you want upgrade version 2.0 to 2.1 (restart system is required)? [y/N]y
Have you export all reports? [y/N]y
Have you made a full system backup? [y/N]y

Testing connection to update server:
Connection succeeded

will restart when the upgrade is complete
Upgrading...

- No SSL mode enabled
- Downloading packages
Checking for license...
Checking for available upgrade...
Downloading kernel upgrade...
######################################################################## 100.0%
Kernel upgrade downloaded
Kernel upgrade downloaded. Installing...
Checking environment...
Preparing environment...
Environment ok.
Testing installer integrity...
Installer integrity ok.
Unpacking installer...
Installer unpacked.
Running installer...
Finding instalation disk...
Mounting instalation disk
Installing new kernel files. It will take a while...
Installing new initramfs...
Setting new kernel as bootable...
Cleaning up old entries...
New kernel installed!
Kernel upgraded from 3.10.0-957.10.1 to 5.8.8-1
A reboot is required.
```

Command Line Interface – upgrade-blockbit

When the installation is finished, the update of the Kernel will have already been done successfully, however as the command itself displays on the screen, it will be necessary to restart the system.

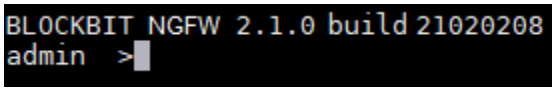
After the machine boots again, check that the kernel has been upgraded to version 5.8 and the system has been upgraded to version 2.1;

To check the kernel version, run the command **[watch-cpu]**:



Command line interface - Watch-cpu

To check the system version, run the **[show-version]** command:

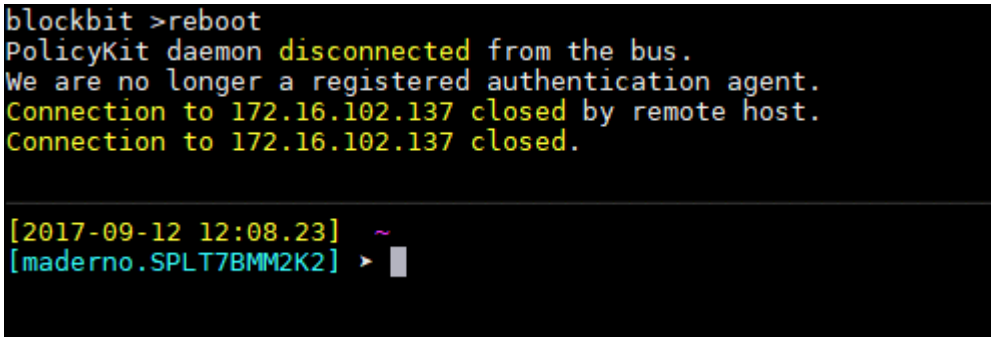


Command Line Interface – show-version

When the installation is finished, the update of the Kernel will have already been done successfully, however as the command itself displays on the screen, it will be necessary to restart the system.

Blockbit UTM - How to Upgrade Kernel - Resetting the UTM

Finally, to complete the upgrade, run the **[reboot]** command to reboot the system.



Command Line Interface – reboot

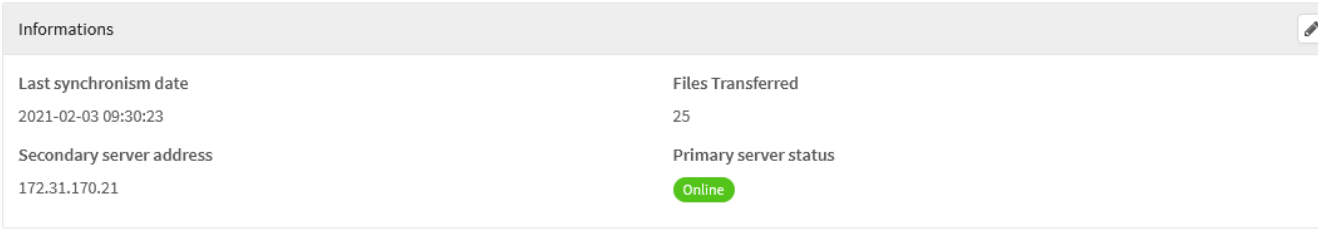
After the system reboots, the kernel update will have been successfully completed and Blockbit NGFW will be ready for normal use.

In the following we will delve into how to safely upgrade the Kernel in an H.A. environment.

Blockbit UTM - How to Upgrade Kernel - Kernel update in an H.A. environment

In order to guarantee the availability of the environment, it is advisable to carry out the entire update process mentioned in the previous chapters, in a specific order. To do this, follow the steps below in the following order:

1. Wait for synchronization time with secondary device or force it. To know the time of the last synchronism, consult the Last synchronism date field in the Information panel as shown below:



High Availability - Information

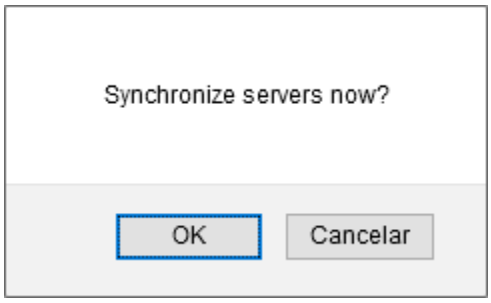
For more information on High Availability, see this *page*.

To force the synchronism, access the Secondary Cluster and locate the Information panel at the bottom of the page, following an image showing this panel:

Seconday server Settings - Information

For more information on configuring High Availability on the secondary device, see this *page*.

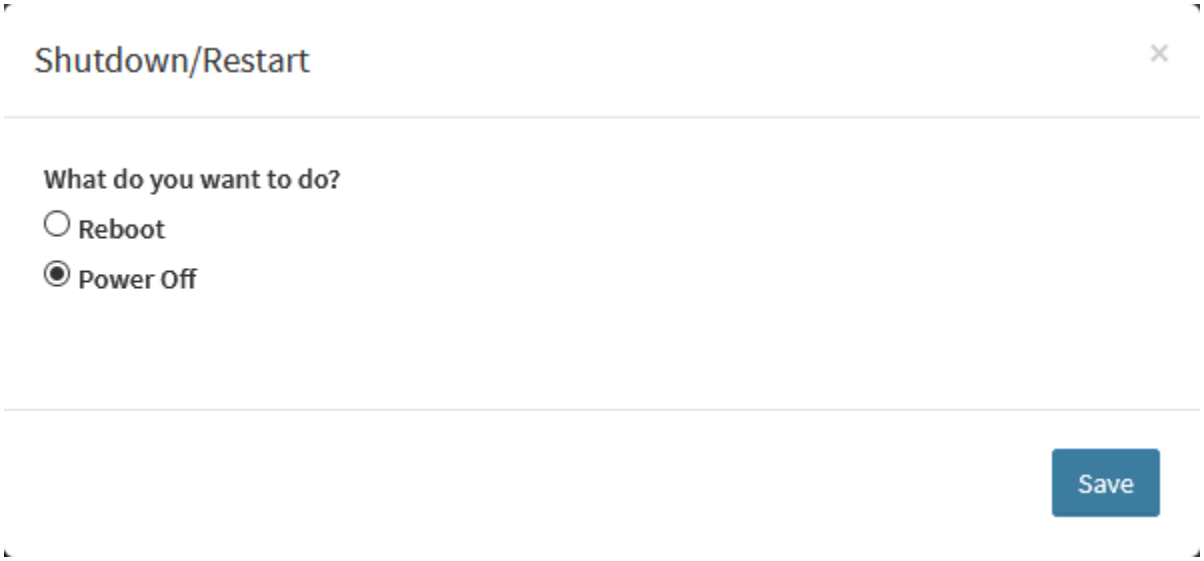
Click the **[ ]** button to force the synchronization with the Primary Server, the following window will be displayed:



Secondary server Settings - Synchronize servers now

Click **[** OK **]** to start the operation.

As mentioned earlier, confirm in the Information panel, when the synchronization was done in the "Last Synchronism" option, if the operation was completed, turn off the Secondary Cluster. To turn it off, just click the **[ ]** button located at the top of the screen, the following window will be displayed:

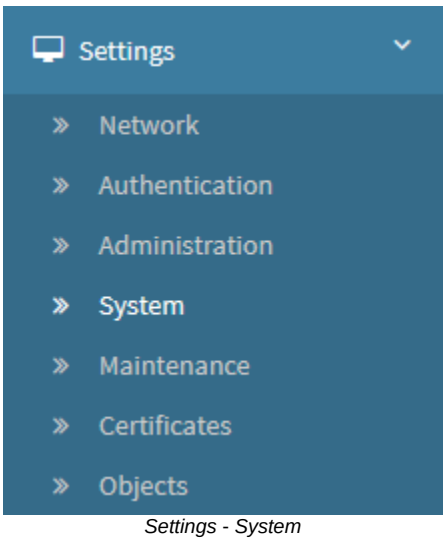


Secondary server Settings - Shutdown/Restart

Make sure that the ***Power Off*** option is selected and click the **[ ]** button.

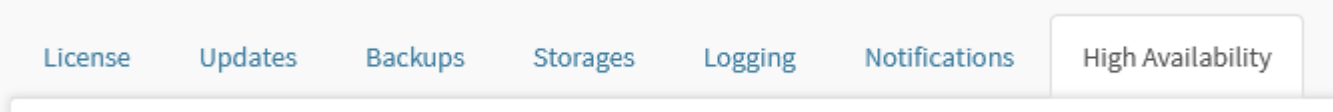
The secondary Cluster will be used as your redundancy system and therefore, it should be used as a backup.

2. In the primary device interface, go to Settings and click on the System menu:



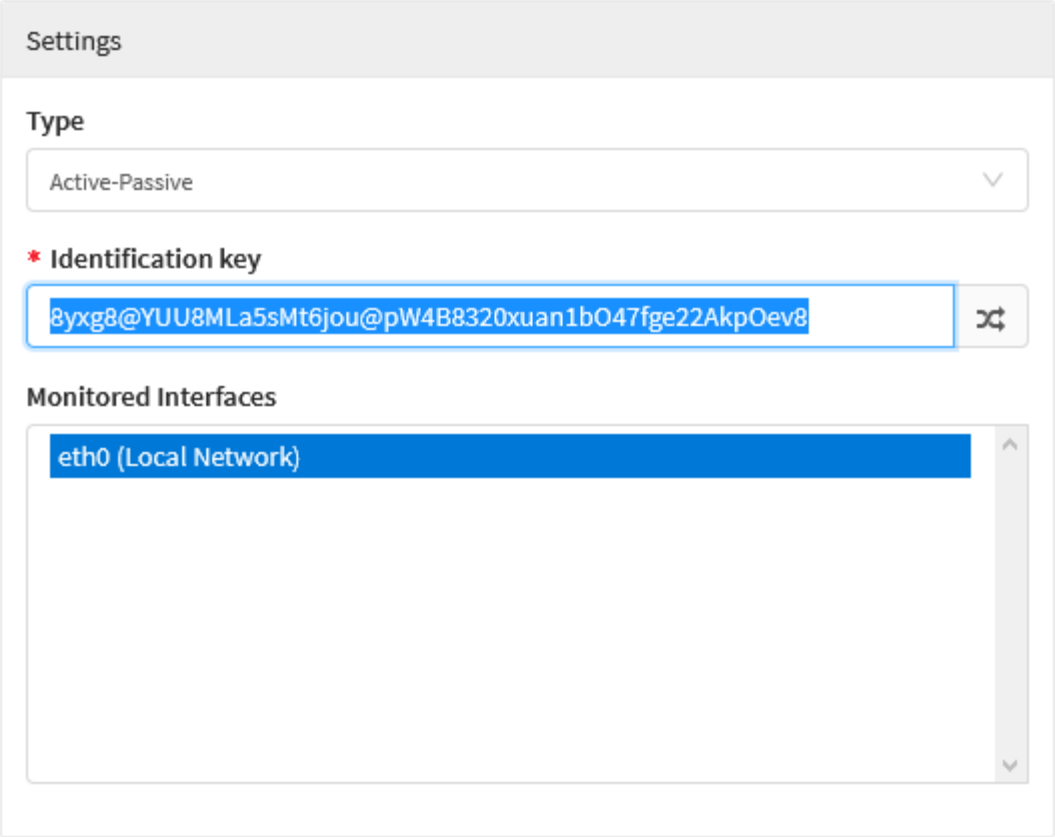
Settings - System

Access the High Availability tab:



System - High Availability

Copy the H.A. Identification Key:



High Availability - Painel *Settings*

WARNING: Keep the Identification Key in a safe place, you will need it later.

3. Access the CLI interface of the primary device and execute the command ***[update-system]*** to update the system and acquire the packages related to NGFW 2.0:

Command Line Interface – update-system

To confirm that the system has been updated, use the command **[show-version]**.

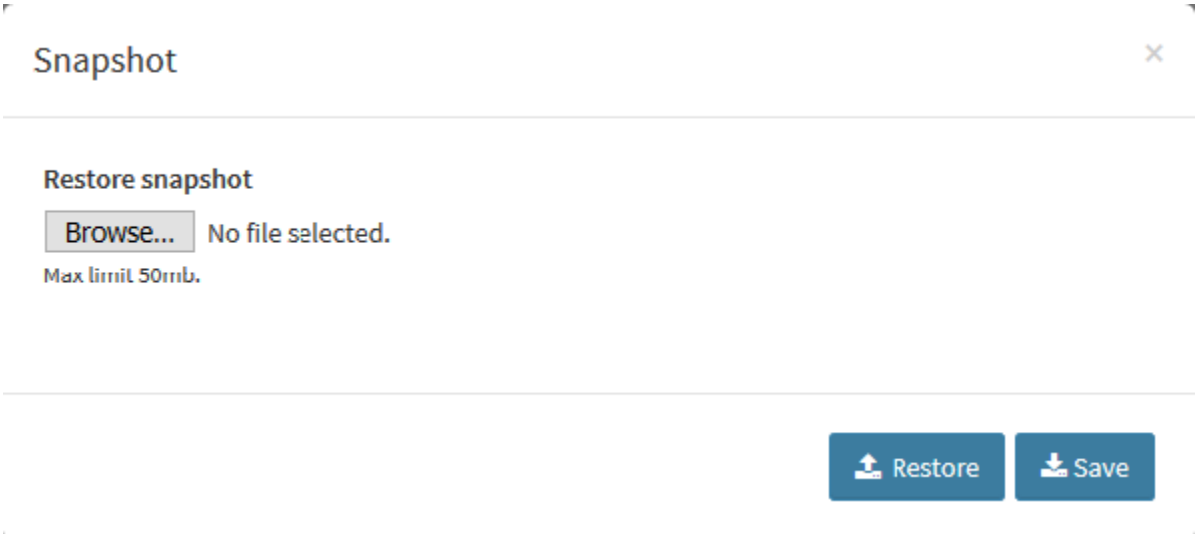
Command Line Interface – show-version

4. After upgrading to build 2.0.8, log in to the Primary Cluster interface, locate the Snapshot button in the side menu on the left of the screen and click on it.

WARNING: The execution of this snapshot is essential to guarantee the integrity of your data. After taking the snapshot, store it in a safe place.

Snapshot option

After clicking on the button, the following window will be displayed:



Snapshot window

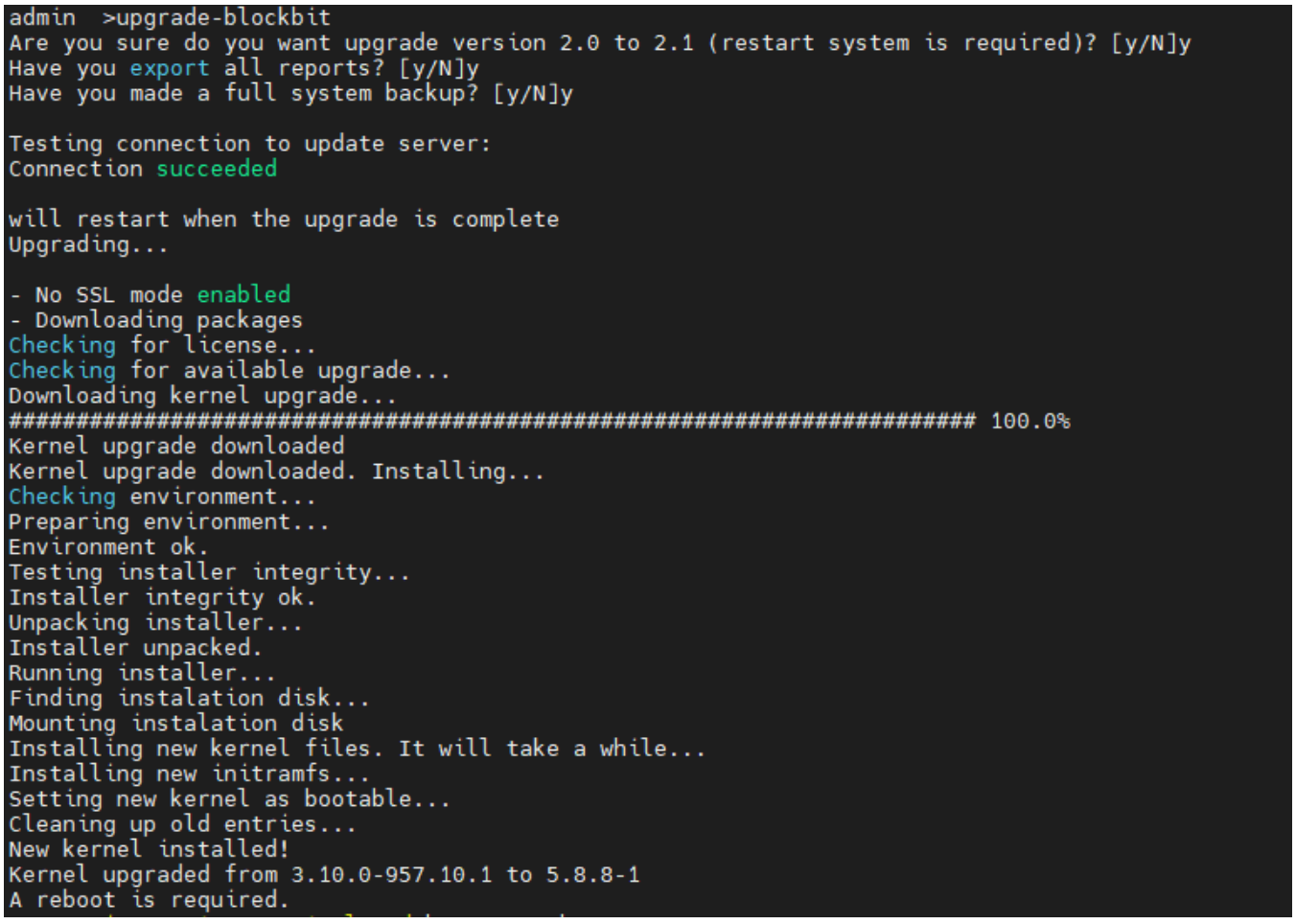
Click the [Save] button to take a snapshot. Store the file in a safe place

After performing the steps previously mentioned, the snapshot will have been successfully generated.

5. Access the Primary Cluster console to enter the system, in this step we will execute the command “upgrade-blockbit”, to update the kernel version.

WARNING: At the end of the execution of this command, it will be necessary to restart your NGFW.

In the CLI of the Primary Cluster execute the command **[upgrade-blockbit]** as shown below.



Command Line Interface – upgrade-blockbit

This procedure will take a few minutes and will reset the device.

When the installation is finished, the kernel update will have already been carried out successfully, however just as the command itself displays on the screen, it will be necessary to restart the system.

6. After the machine boots again, to verify that the kernel has been upgraded to version 5.8 and the system has been upgraded to version 2.1, perform the procedures below:

To check the kernel version, run the command ***[watch-cpu]***:

```
watch-cpu: 15:27:35 up 1 day, 41 min,  1 user,  load average: 0.27, 0.39, 0.38
Linux 5.8.8-1.el7.elrepo.x86_64 (utm.blockbit.com)      02/03/21        _x86_64_        (4 CPU)

15:27:35     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
15:27:35     all    2.77    0.19    3.05    0.18    0.00    0.09    0.00    0.00    0.00   93.72
15:27:35       0    2.87    0.19    3.07    0.18    0.00    0.11    0.00    0.00    0.00   93.57
15:27:35       1    2.61    0.19    2.86    0.21    0.00    0.11    0.00    0.00    0.00   94.02
15:27:35       2    2.80    0.20    3.18    0.17    0.00    0.08    0.00    0.00    0.00   93.58
15:27:35       3    2.80    0.19    3.08    0.15    0.00    0.07    0.00    0.00    0.00   93.71

press [CTRL+C] to stop
```

Command line interface - Watch-cpu

To check the system version, run the ***[show-version]*** command:

```
BLOCKBIT NGFW 2.1.0 build 21020208
admin  >
```

Command Line Interface – show-version

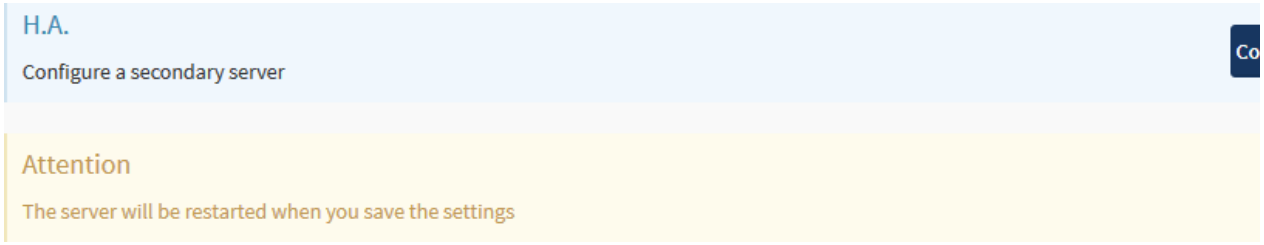
If the system is operating normally with functional services, policies, routing and web browsing, turn off the primary device. To shut down the primary device just use the **[shutdown]** command on your CLI:

```
admin  >shutdown
```

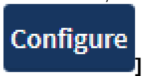
Command Line Interface – shutdown

After the primary device has been successfully turned off, reconnect the secondary device and after system initialization, access the web interface and follow the steps as appropriate:

- If the interface presented is the login one, immediately follow the next step, click this link to access it. Otherwise, if it is the cluster configuration interface, as shown below:



Seconday server Settings - Cluster configuration interface

In this case, the device is not enabled to activate automatically, so it will be necessary to activate it manually, to do so, locate and click the **[** 

] button at the top right of the screen, when the secondary device configuration settings appear, locate the Information panel at the bottom of the screen, as shown below:

For more information, see this page.

Seconday server Settings - Information

To activate the device, make sure that the *H.A. Identification Key* is in the correct field and click the **[** 

] button;

This procedure will take a few minutes and will reset the device.

- Update your system to receive the latest version 2.0 packages. to do so, access the Secondary Cluster console and enter the command **[update-system]**:

Command Line Interface – update-system

- After activating the system, access the CLI interface and execute the “upgrade-blockbit” command, to update the kernel version.

WARNING: At the end of the execution of this command, it will be necessary to restart your NGFW.

In the CLI of the Primary Cluster execute the command **[upgrade-blockbit]** as shown below.

```
admin  >upgrade-blockbit
Are you sure do you want upgrade version 2.0 to 2.1 (restart system is required)? [y/N]y
Have you export all reports? [y/N]y
Have you made a full system backup? [y/N]y

Testing connection to update server:
Connection succeeded

will restart when the upgrade is complete
Upgrading...

- No SSL mode enabled
- Downloading packages
Checking for license...
Checking for available upgrade...
Downloading kernel upgrade...
######################################################################## 100.0%
Kernel upgrade downloaded
Kernel upgrade downloaded. Installing...
Checking environment...
Preparing environment...
Environment ok.
Testing installer integrity...
Installer integrity ok.
Unpacking installer...
Installer unpacked.
Running installer...
Finding instalation disk...
Mounting instalation disk
Installing new kernel files. It will take a while...
Installing new initramfs...
Setting new kernel as bootable...
Cleaning up old entries...
New kernel installed!
Kernel upgraded from 3.10.0-957.10.1 to 5.8.8-1
A reboot is required.
```

Command Line Interface – upgrade-blockbit

 This procedure will take a few minutes and will reset the device.

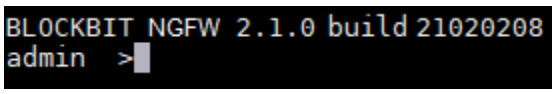
When the installation is finished, the kernel update will have already been carried out successfully, however just as the command itself displays on the screen, it will be necessary to restart the system.

7. After the machine boots again, check that the kernel has been updated to version 5.8 and the system has been updated to version 2.1 have been updated;

To check the kernel version, run the command **[*watch-cpu*]**:

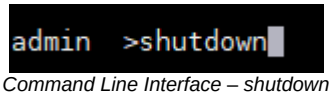
```
watch-cpu: 15:27:35 up 1 day, 41 min,  1 user,  load average: 0.27, 0.39, 0.38
Linux 5.8.8-1.el7.elrepo.x86_64 (utm.blockbit.com)      02/03/21        _x86_64_        (4 CPU)

15:27:35     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
15:27:35     all    2.77    0.19    3.05    0.18    0.00    0.09    0.00    0.00    0.00   93.72
15:27:35       0    2.87    0.19    3.07    0.18    0.00    0.11    0.00    0.00    0.00   93.57
15:27:35       1    2.61    0.19    2.86    0.21    0.00    0.11    0.00    0.00    0.00   94.02
15:27:35       2    2.80    0.20    3.18    0.17    0.00    0.08    0.00    0.00    0.00   93.58
15:27:35       3    2.80    0.19    3.08    0.15    0.00    0.07    0.00    0.00    0.00   93.71

press [CTRL+C] to stop
```

To check the system version, run the **[show-version]** command:



Command Line Interface – show-version

If the system is operating normally with functional services, policies, routing and web browsing, turn off the primary device. To disconnect the secondary device, just use the **[shutdown]** command in your CLI:



Command Line Interface – shutdown

8. Finally, simply reconnect the primary device again to complete the Kernel update in an H.A. environment.

WARNING: If the device loses connection during the Kernel upgrade process, or if there is another type of failure, run the **[upgrade-blockbit]** command.

This concludes the installation of the Kernel, for more in-depth information regarding the system features, access the Blockbit NGFW administrator's guide.

Blockbit

it's easy to be secure

www.blockbit.com

Blockbit Client

Blockbit Client is a client / server application integrated with Windows that serves as much in user authentication for the “Firewall” service as for other remote connection resources such as: “IPSEC VPN” or “SSL VPN”.

It is the enhanced version of the Blockbit Agent and has numerous new features to facilitate access to VPNs, including:

- Configuration of multiple connection profiles;
- Import and export of these profiles to facilitate possible future implementations;
- Exporting connection profile logs;
- And much more, check out all the news on this page.

To download **Blockbit Client, click here.**

To download **Blockbit NGVPN Client, Click here.**

The Blockbit Client is approved for MS-Windows 7+ Superior versions.

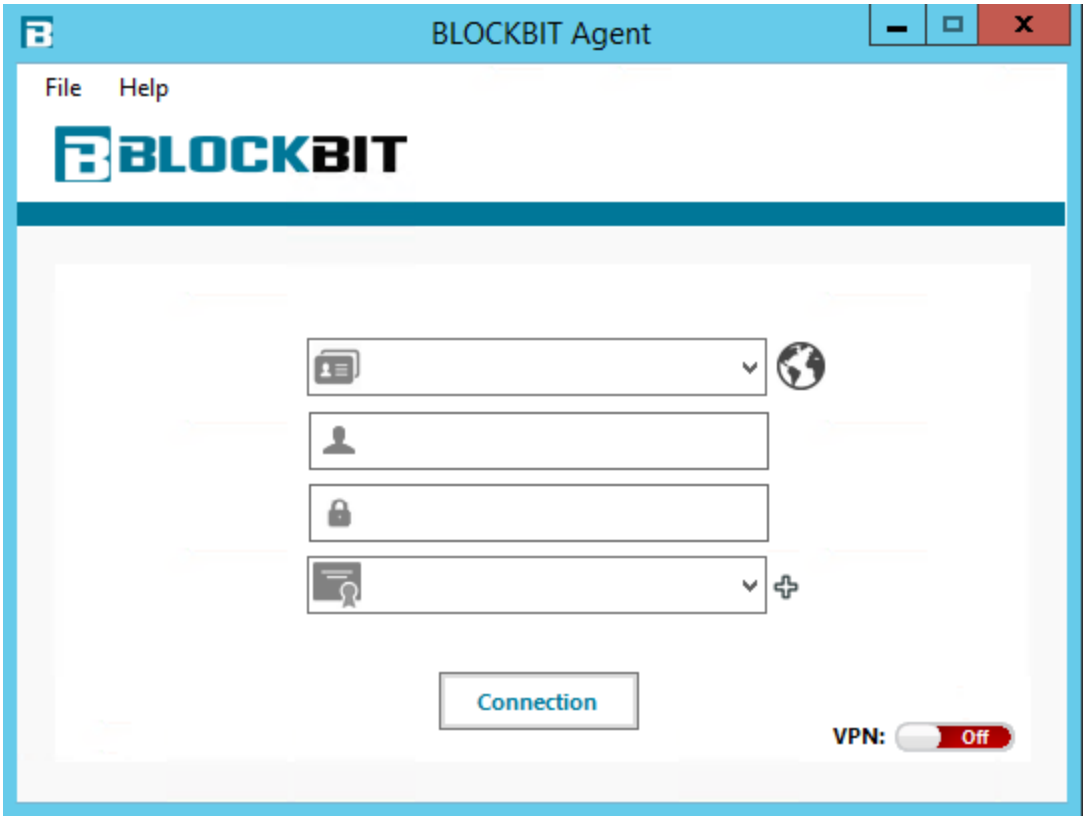
In this session we'll review the following topics:

- Comparison of previous versions;
- Minimum requirements, environment check, download and installation of the *Blockbit Client;*
- Blockbit Client configuration;
- How to make a connection using Blockbit Client;
- How to access the Blockbit Client logs in the Windows event viewer.

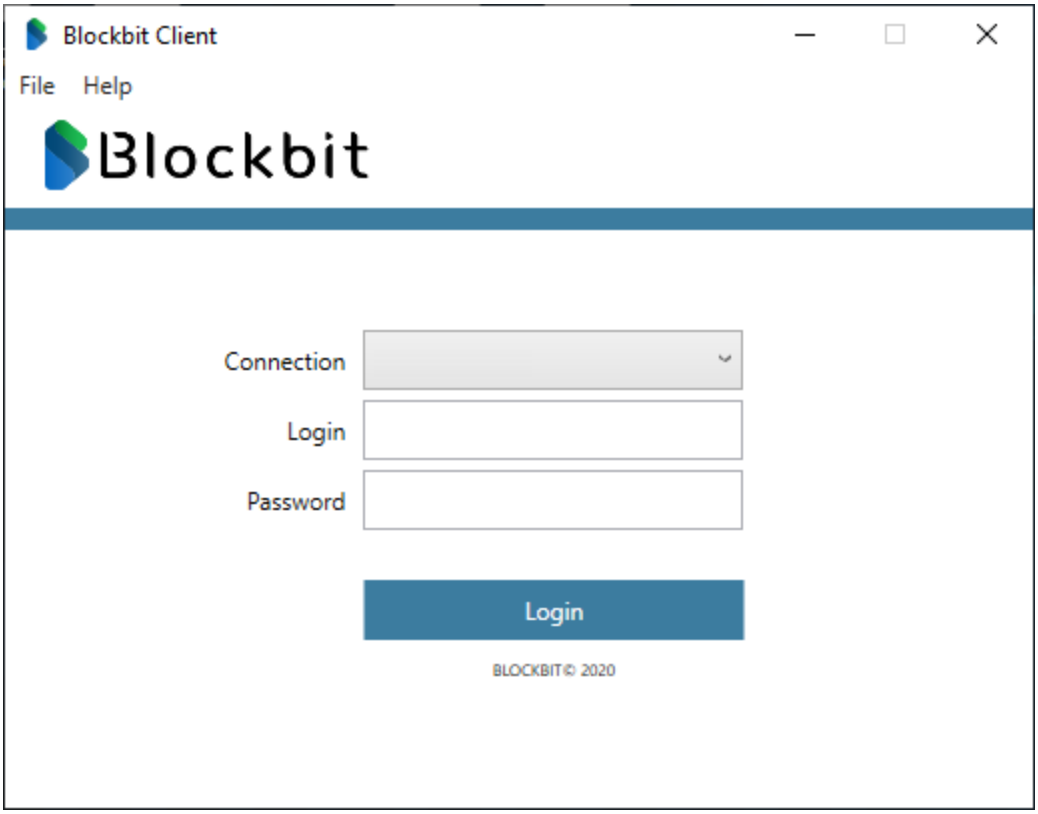
To download the Blockbit Client access the authentication portal (through the IP address or hostname of your NGFW through port 9803) and click on **[**  **]**. For more information, see this page.

Comparison of previous versions

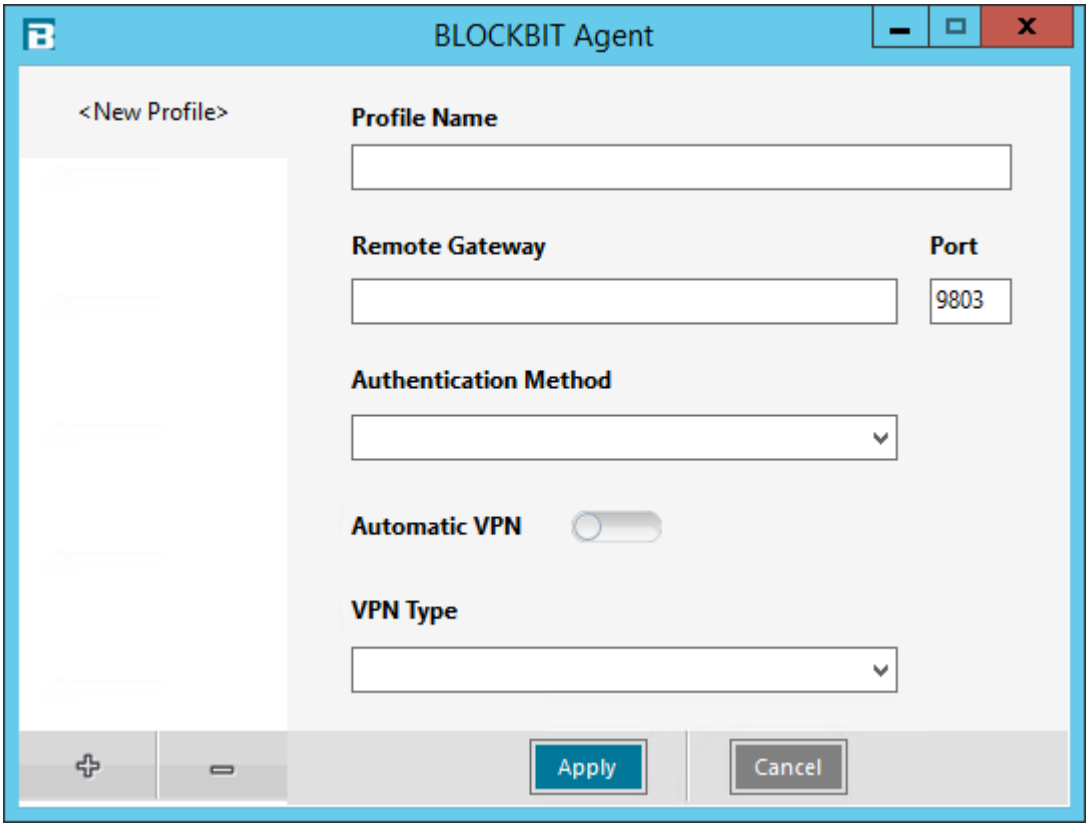
Blockbit Client is the improved version of the old Blockbit Agent, it has several improvements that have considerably improved its functionality. Below is a sequence of comparative screenshots between the two versions to show the new features.



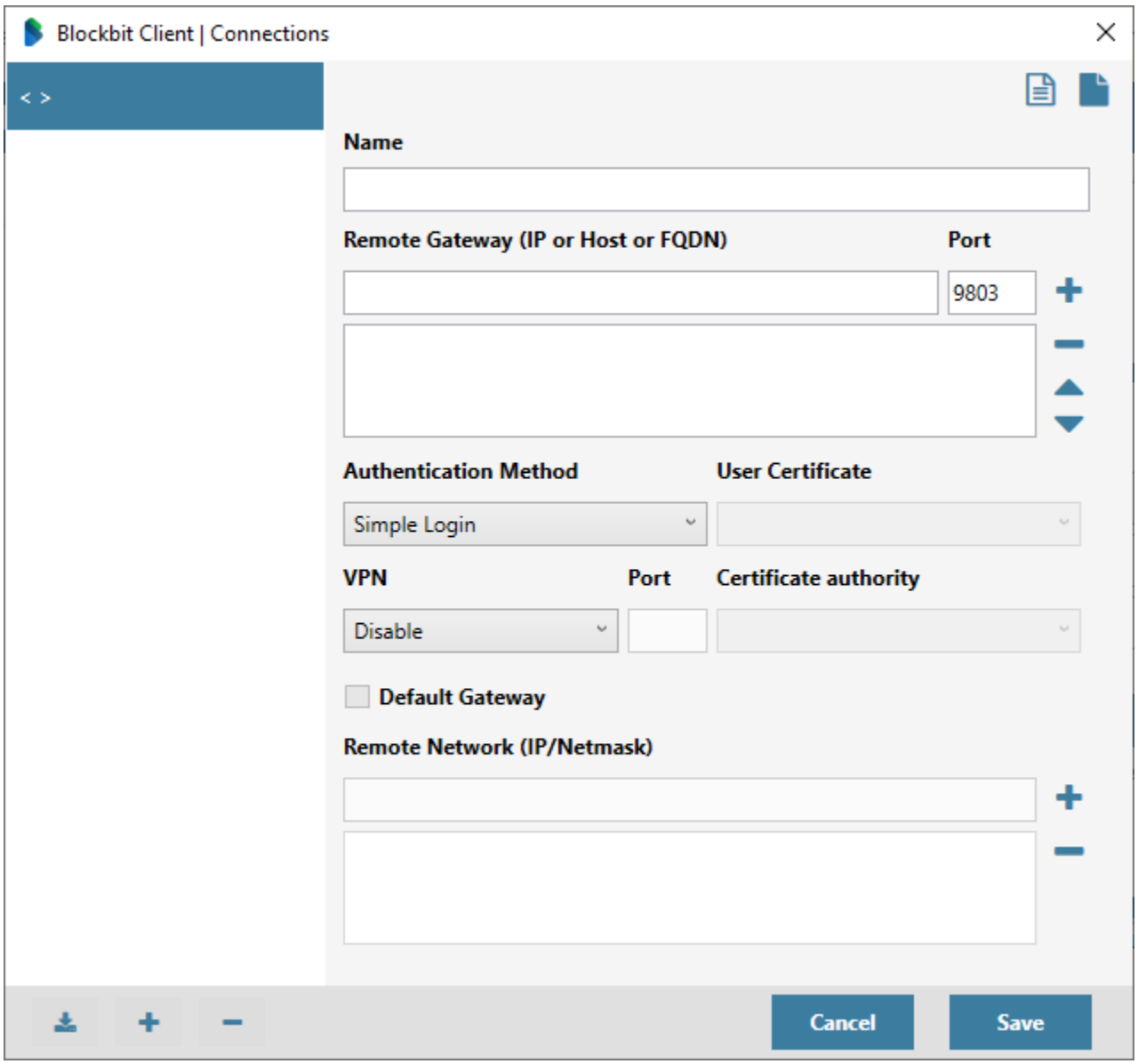
Blockbit Agent - Main screen



Blockbit Client - Main screen



Blockbit Agent - *New Profile*



Blockbit Client- *New Profile*

In this session we will list the news and features that were developed in this version:

- This version makes it possible to import a connection profile automatically at the time of installation (which allows the Network Administrator to distribute the pre-configured installer to users);
- There were improvements in the connection flow, in this version, the VPN application to establish the VPN connection at the public address and establish the Firewall authentication at the virtual address (VPN);
- The Blockbit Client now makes it possible to configure secondary Remote Gateway addresses, improving the availability of the service (the VPN connection service (IPSEC or SSL) tries to connect at the secondary address if it is unable to establish the connection via the Primary);
- Supports static routes configured on the Client;
- The menus have been restructured and the design has been improved (updated icon, logo and layout);
- The Blockbit Client authentication service has support for keepalive, which discontinues dependence on the NGFW notification service;
- Firewall authentication and VPN connection service notification messages have been revised and improved;
- The option to disable VPN before or after connecting to a profile has been removed;
- The management of importing certificates has been removed, in this version importing digital certificates is done directly by the native Windows tool;
- Internationalization support, the Blockbit Client adopts the language used in the installation (English and Portuguese);
- Performance improvement when trying to connect to an Unreachable Gateway;
- TAP interface drive and application is now signed with an Authenticode digital certificate issued by Blockbit;
- Blockbit Client now allows you to establish an IPSEC VPN connection using the authentication method "Simple Login (Login and Password)" and "Simple Login with Digital Certificate";
- In case of troubleshooting, Blockbit Client now makes it possible to export VPN connection logs in text file, displaying information:
    - Firewall Authentication Events;
    - IPSEC VPN events;

    - SSL VPN events.
- The Blockbit Client has the option to activate the VPN split tunneling feature, allowing the user to direct part of their device's traffic through the VPN while other applications maintain direct access to the Internet.

For more information on how to download and install the Blockbit Client, visit this page.

Blockbit Client installation

In this session we will present a step by step from the download to the completion of the installation of the Blockbit Client.

- *Minimum requirements*;
- *Checking the Environment for Installing the Blockbit Client*;
- *Download Process*;
- *Installation Guide;*
- *SSL VPN configuration.*

Minimum requirements

Make sure internet communication is active, licensing processes, system updates and databases require internet connection.

Minimum installation requirements:

- .NET Framework versão 4.6;
- MS-Windows 7+ Superiores.

The Client is approved only for MS-Windows 7+ Superior versions.

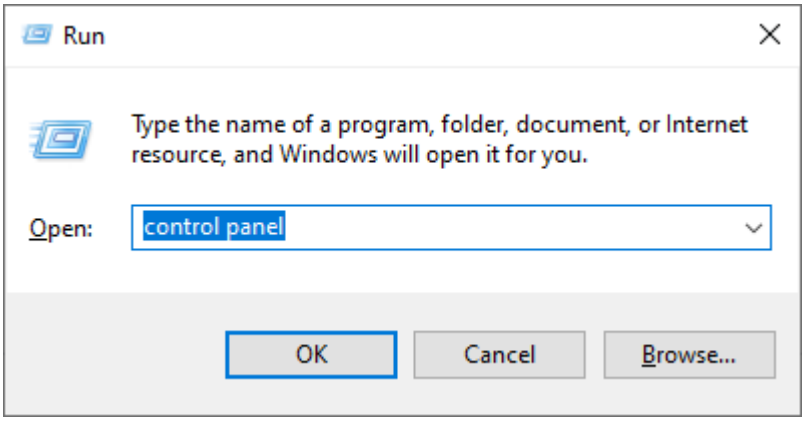
Next, we will confirm that the environment is ready to install the Blockbit Client.

Checking the Environment for Installing the Blockbit Client

For the operation of the Blockbit Client and integration with the Windows event and notification service, the system requires the installation and enabling of the **.NET Framework version 4.6** application on Windows workstations.

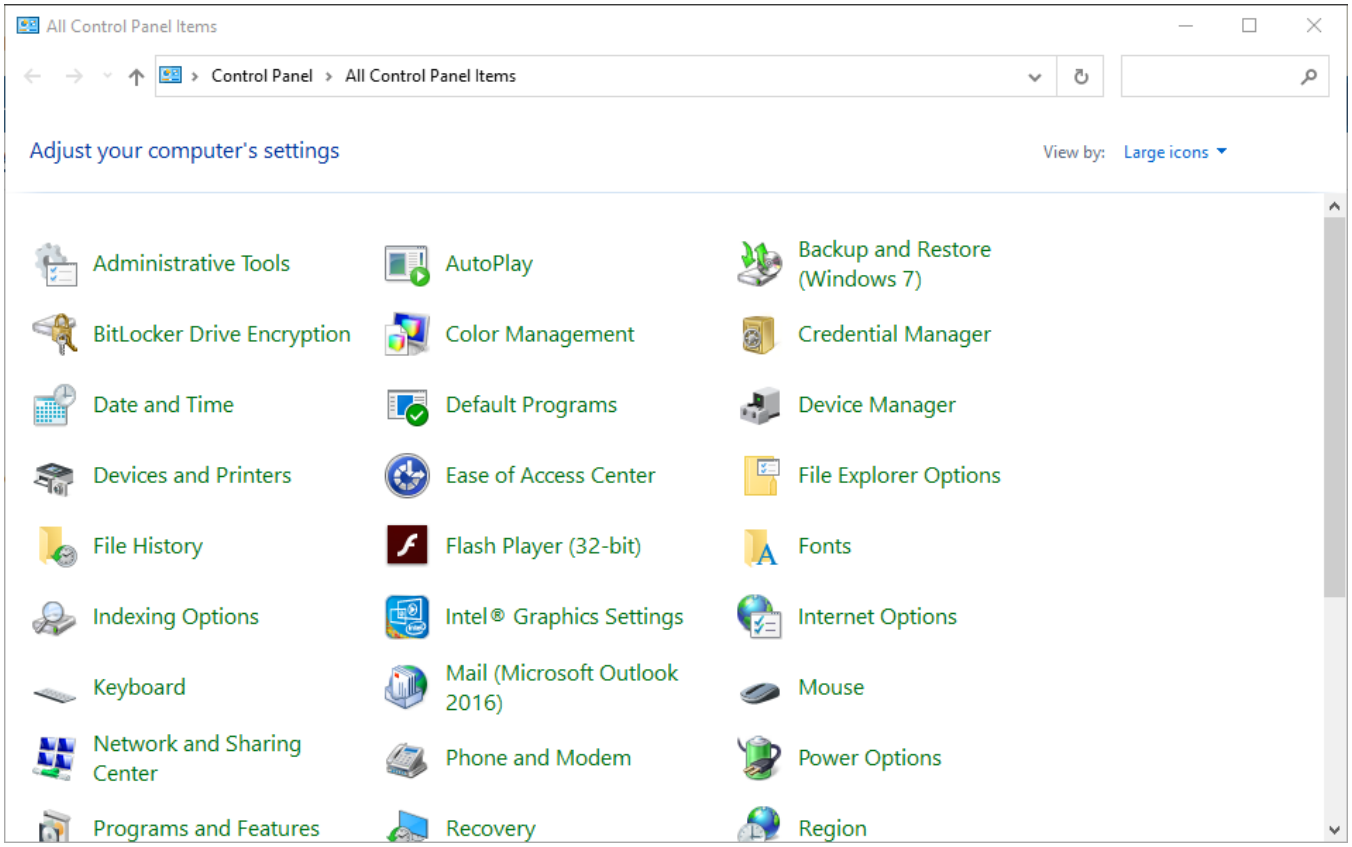
To install the **.NET version 4.6** application, follow the steps below:

Type the command **Windows + R**, or select "Run" in your Start Menu, the window below will appear, in its text field, type "control panel".



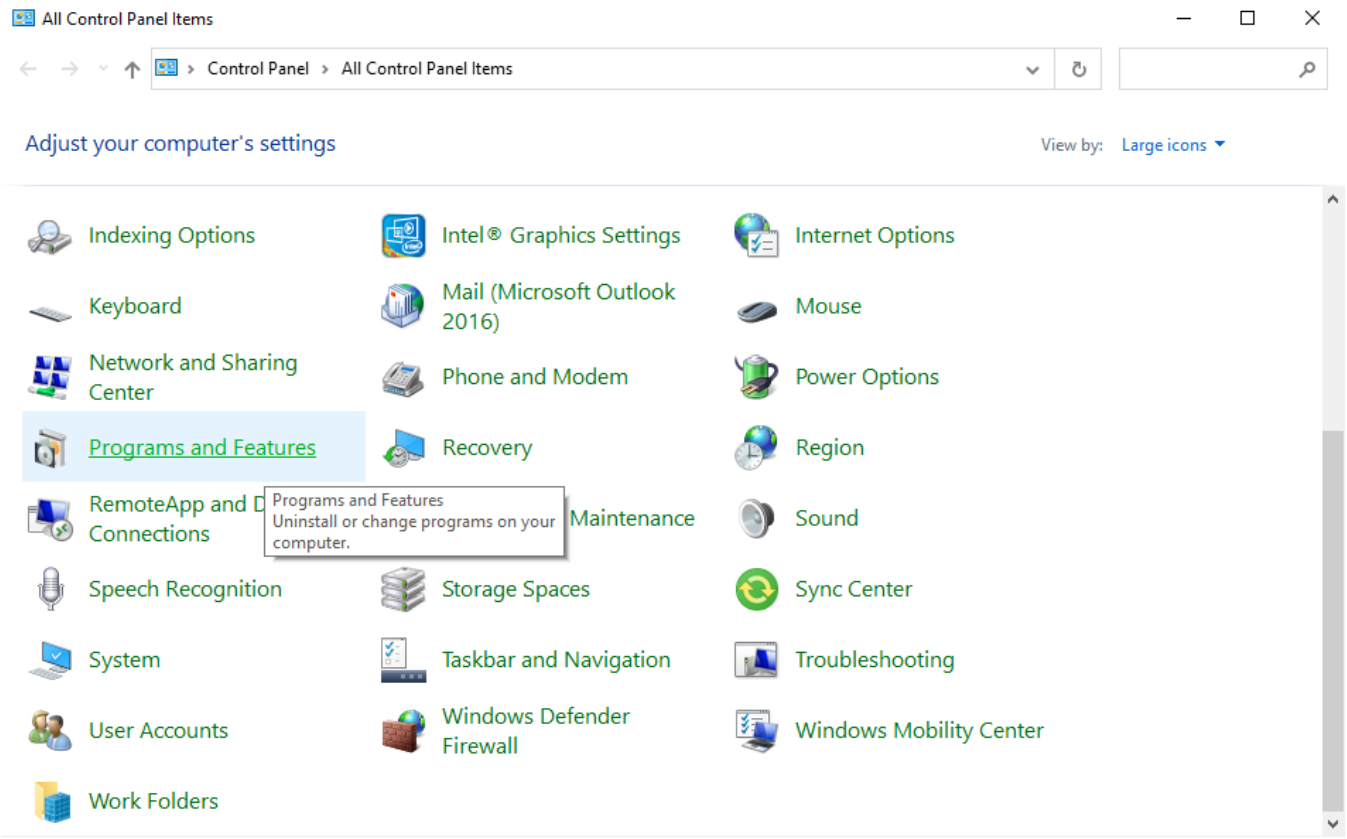
Run - control panel

The control panel will be displayed, as shown below:



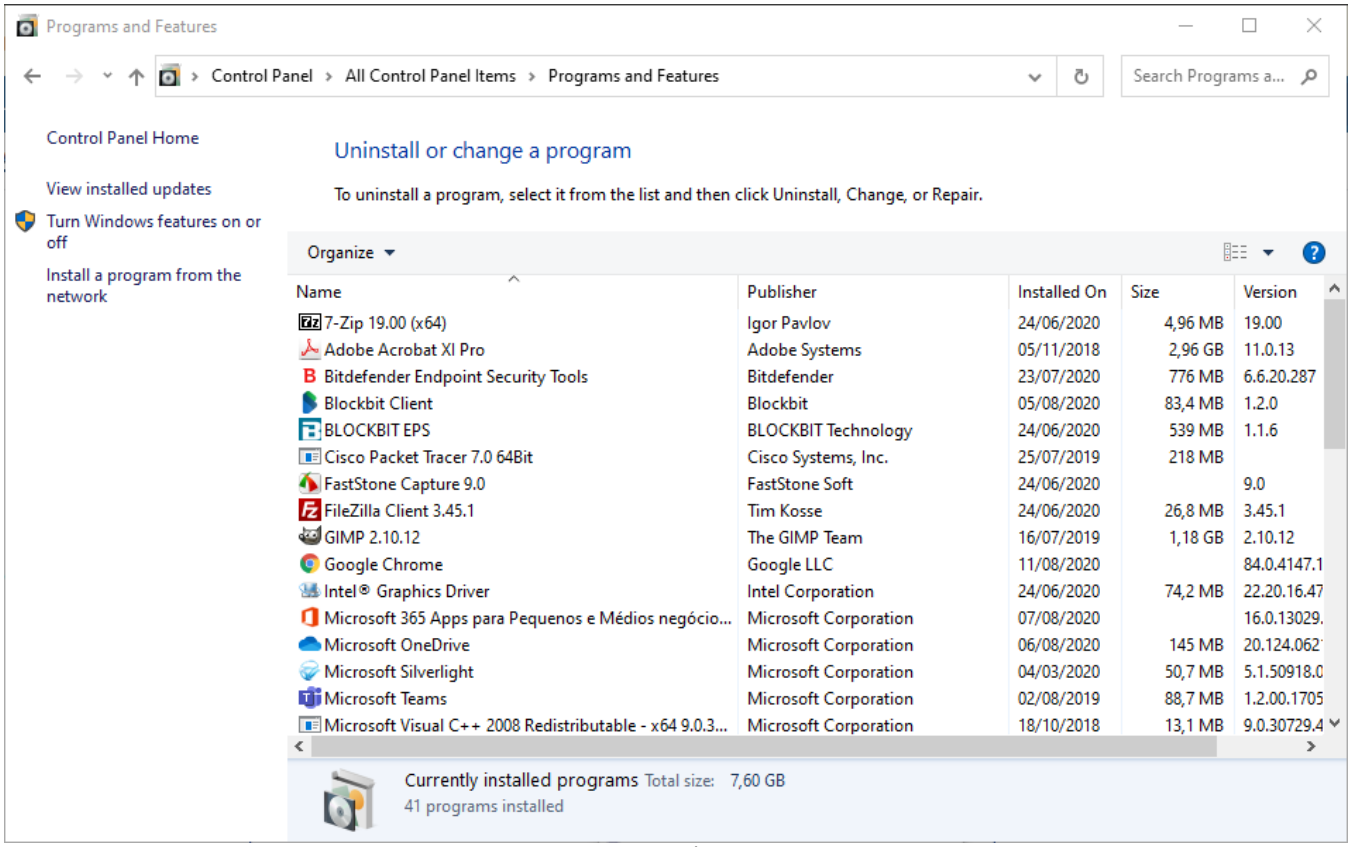
Control Panel

Select the **[Windows Programs and Features]** option:



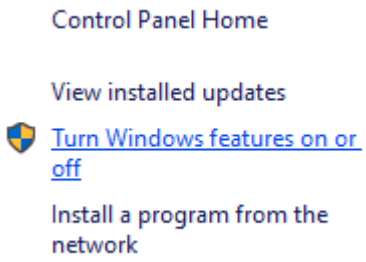
Control Panel - Programs and Features

The window below will appear:



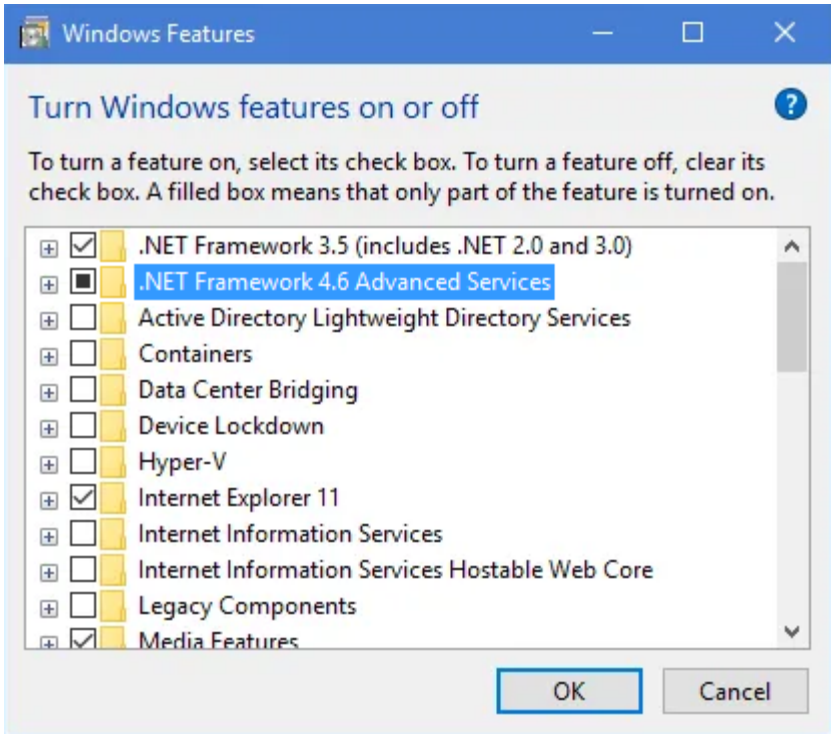
Programs and Features

Select the **[Enable/Disable Windows features]** option located in the menu on the left:



Programs and Features - Turn Windows features on or off

The window below will appear:



Windows Features

To install the .Net Framework 4.6, just select it in this window, press [OK] and follow the installer's instructions.

Below we will download the Blockbit Client.

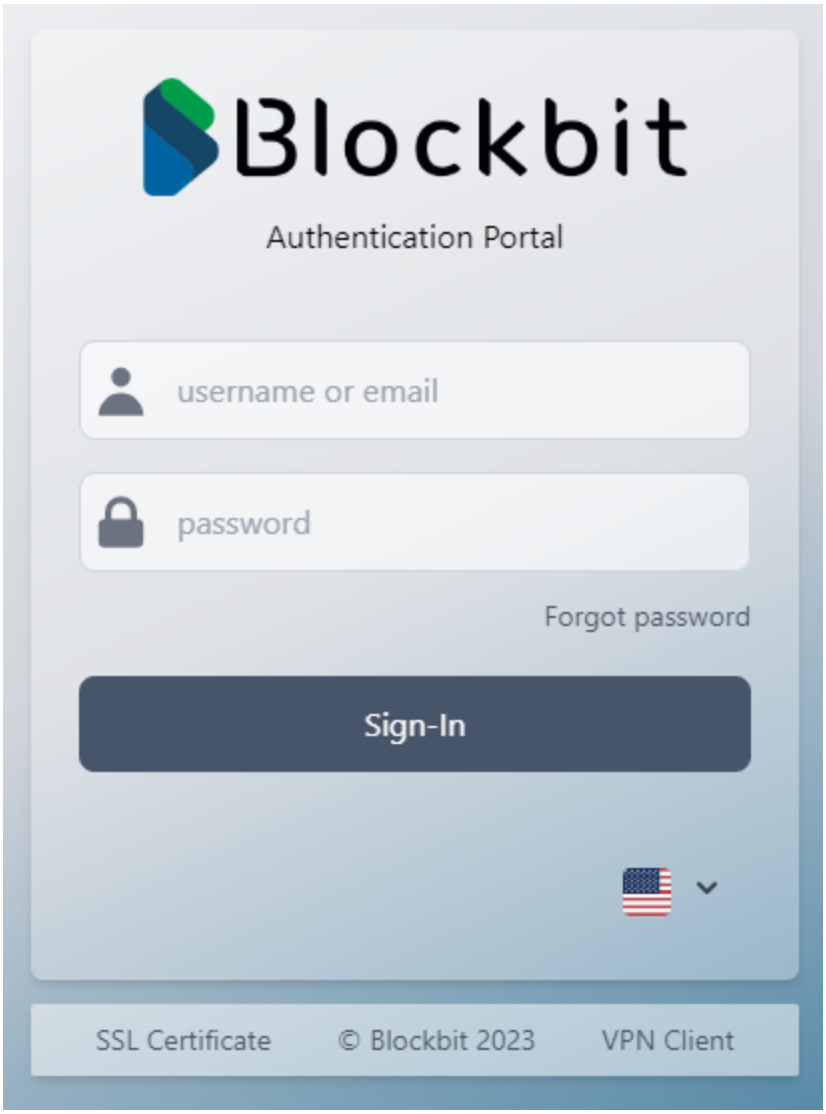
Processo de *Download*

The download link for the Blockbit Client is available from the authentication portal.

To access the authentication portal, access a browser and enter the same address that was configured to access your NGFW, but use port 9803, for example:

https://utm.blockbit.com:9803.

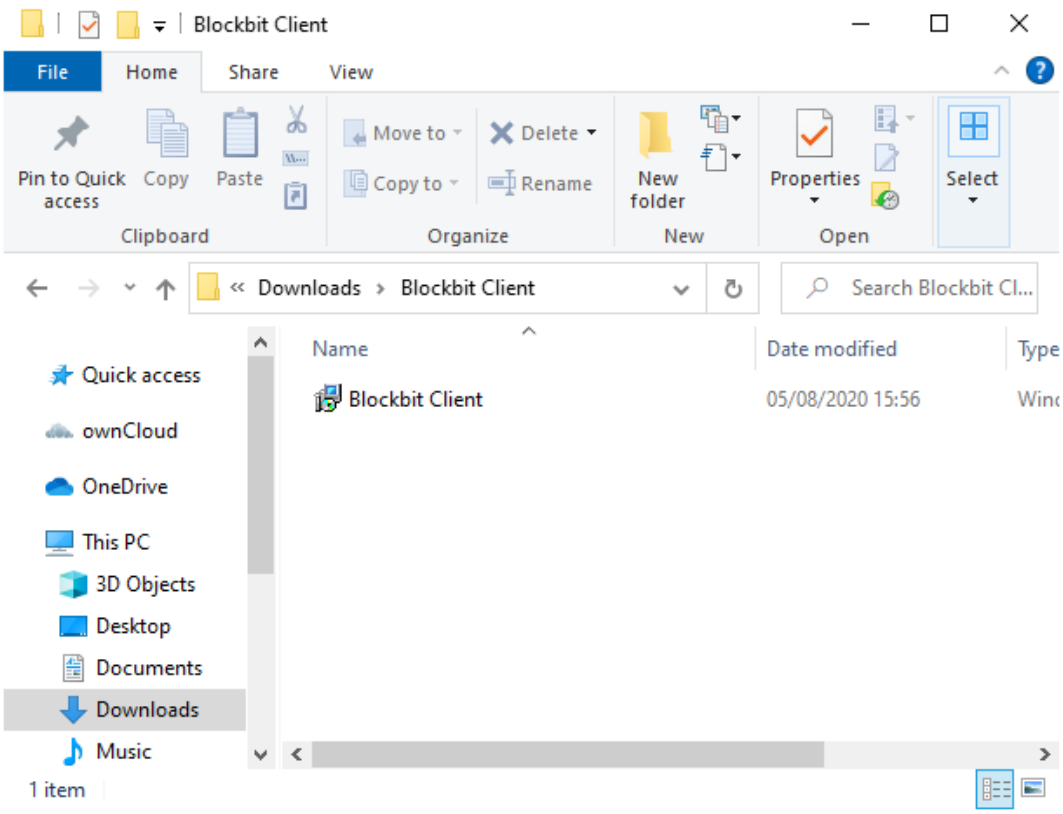
The screen below will be displayed:



User's Portal Authentication

On the bottom right, we have a **LINK** to Download the **Windows Authentication Client**. Click **[**  **]** to download the **[Blockbit_Client.msi]** agent.

The installer is a "msi - Microsoft Windows installer" file, just run the file with 2 (double) clicks and proceed with the standard installation.

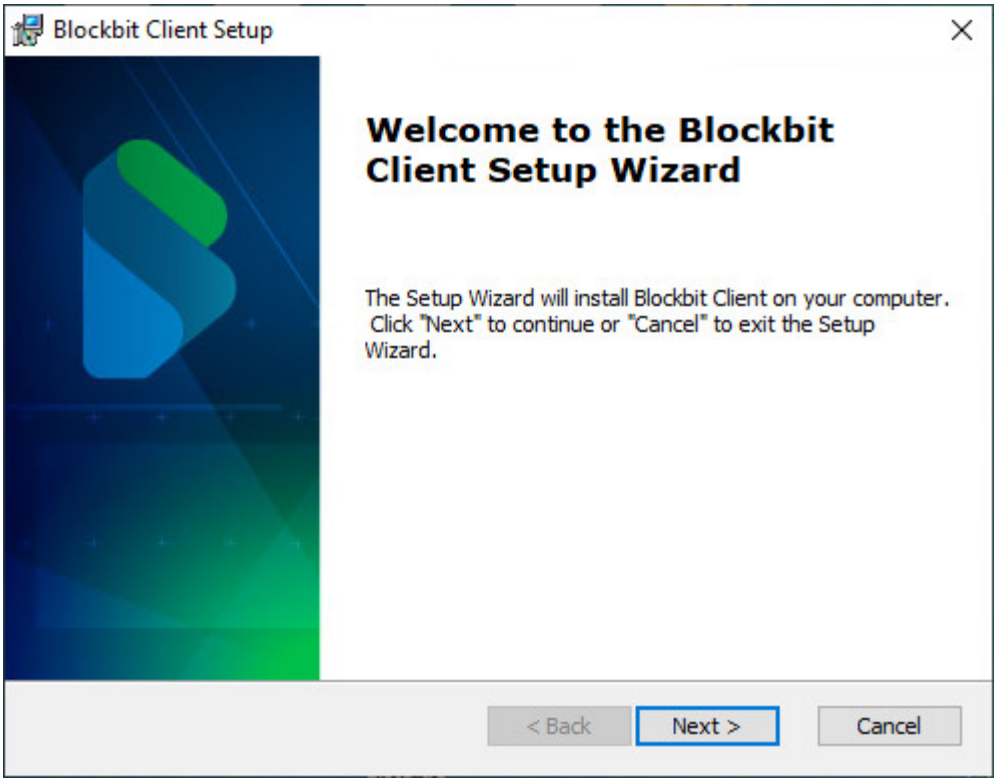


Save the Blockbit Client

Next, we'll review the Blockbit Client installation process.

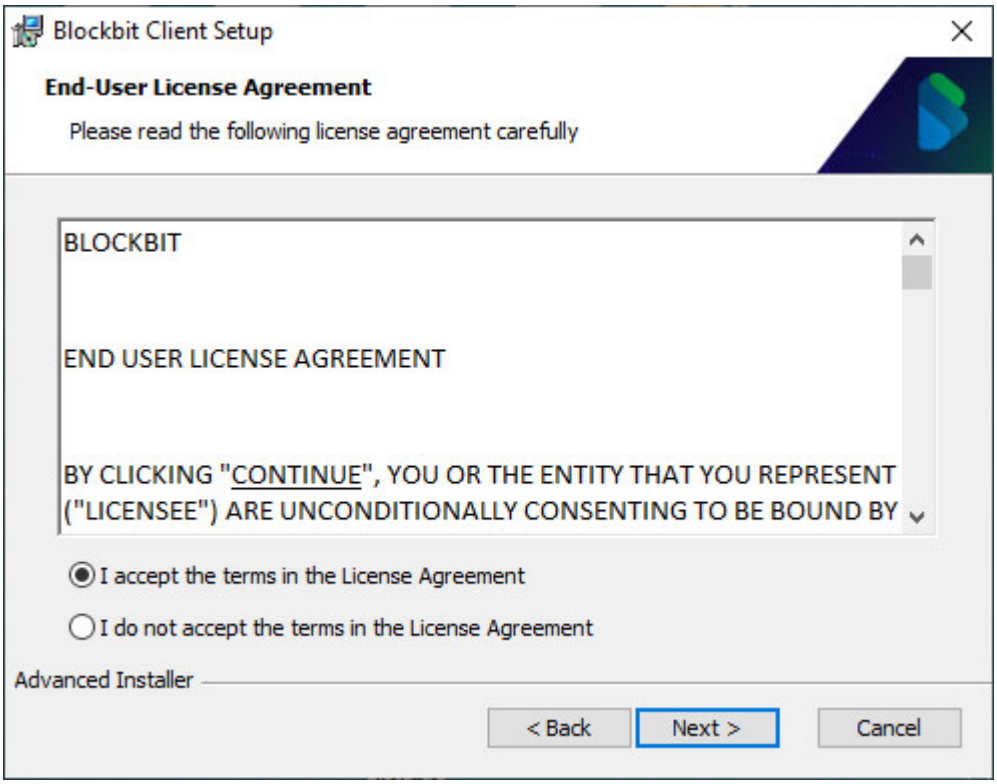
Installation Guide

After double-clicking on the Blockbit Client installer, the following screen will be displayed:



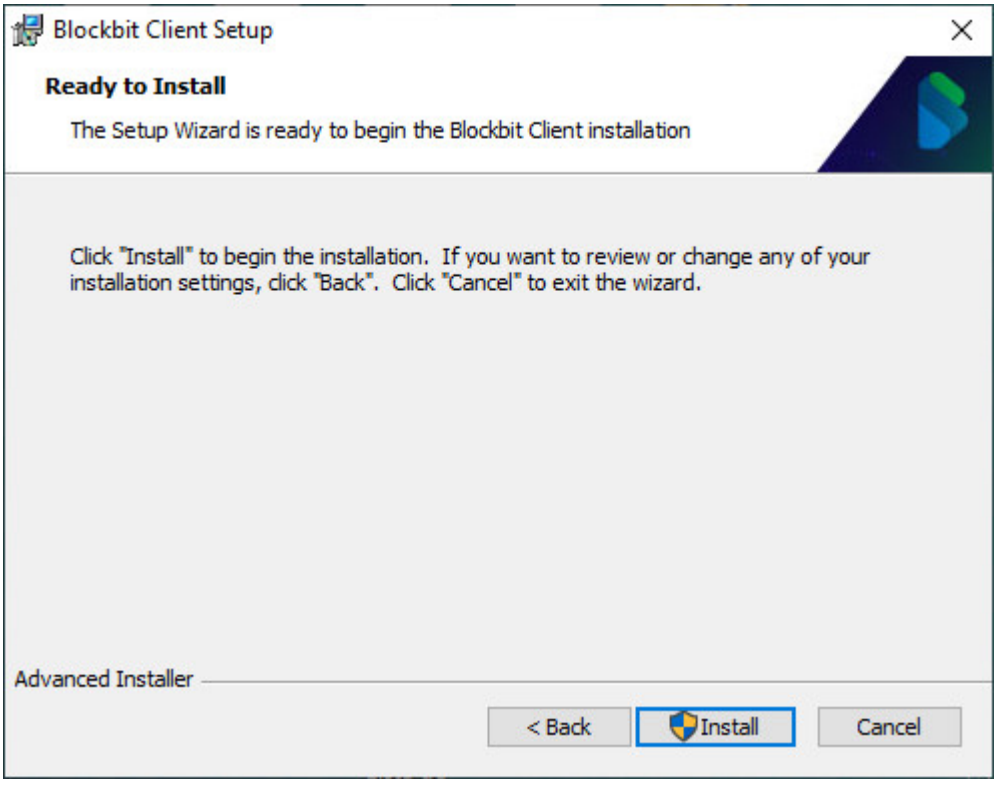
Welcome to the InstallShield Wizard for Blockbit Agent

Click [Next >] to proceed.



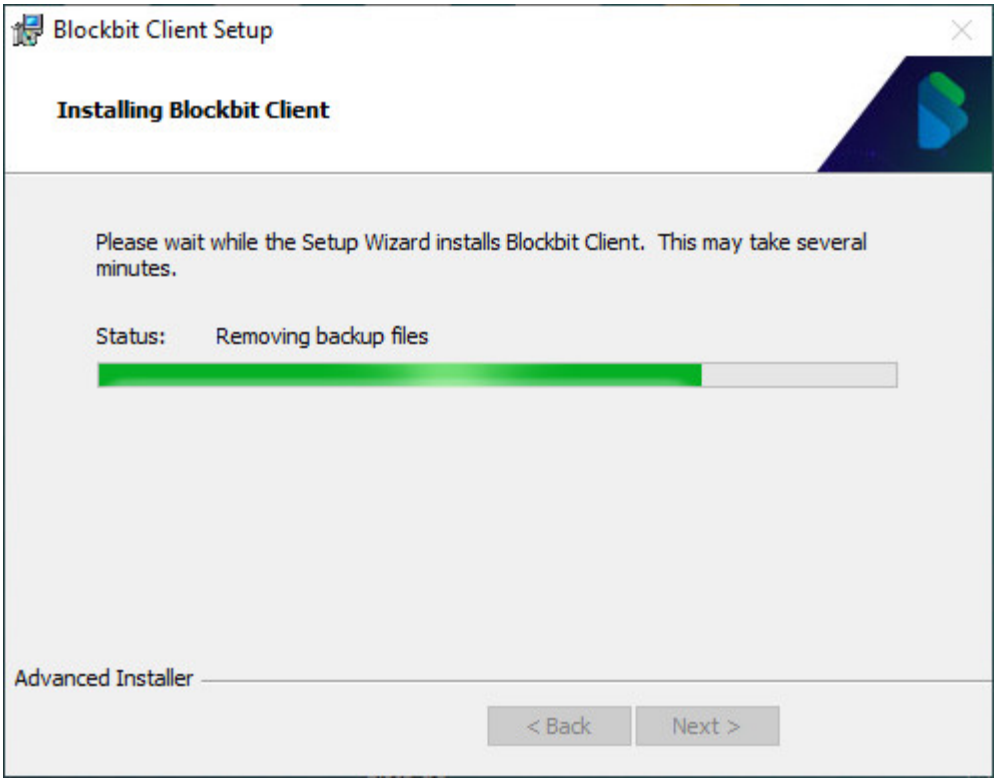
End-User License Agreement

Make sure that [◉] **I accept the terms in this license agreement** is selected and press [Next >].



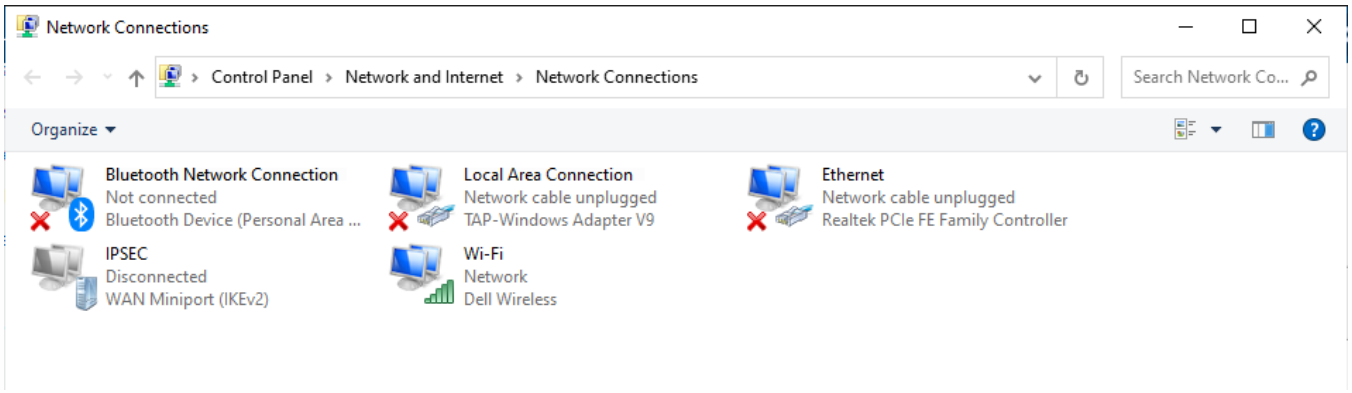
Ready to Install

Click the [Install] button to start the installation and wait.



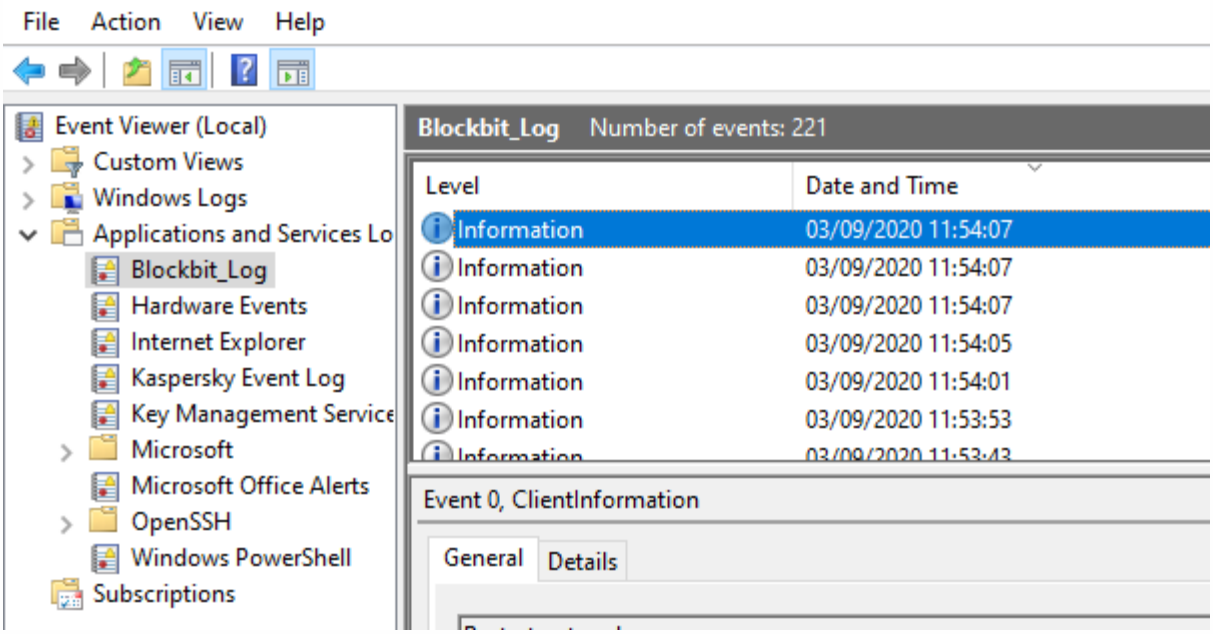
Files in Use

During installation, a service called "Blockbit Service" and a TAP network driver are registered and started, this interface is disabled in the background while not in use, being automatically activated the moment a connection is made. You can view it in the network connections window, as shown below:



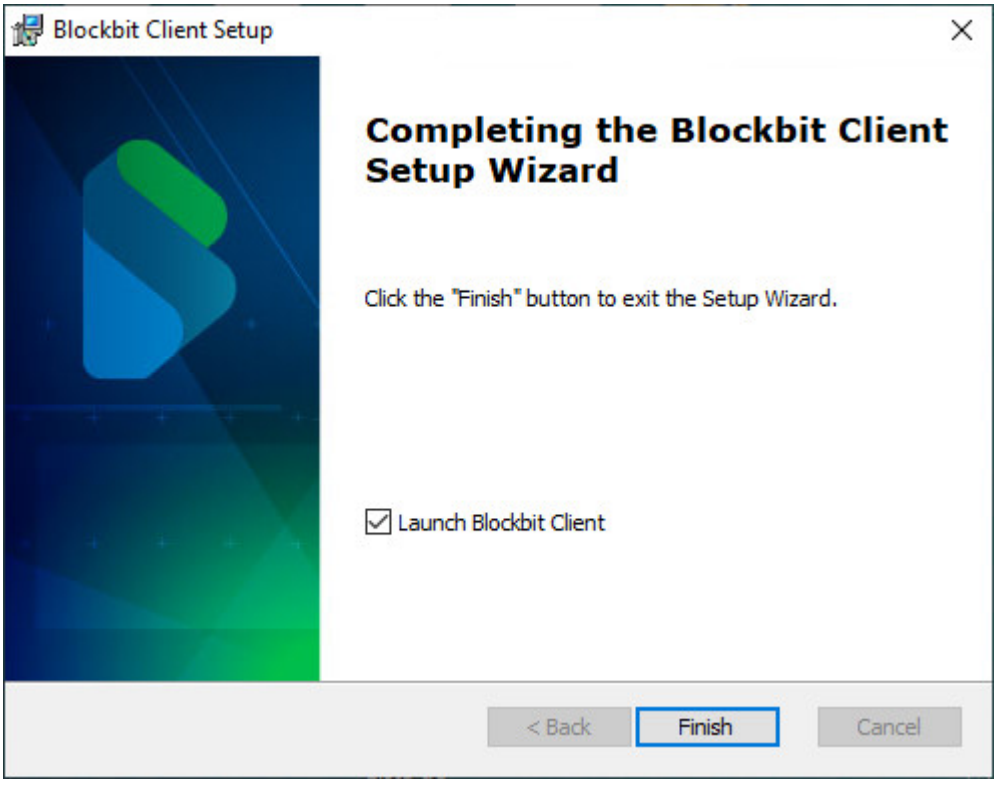
For more information on connection, see this page.

In addition, the Blockbit Client also logs logs to the Windows Event Manager. As shown below:



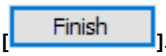
For more information about logs on Windows events, see this page.

After completing the installation process, the following screen will be displayed:



InstallShield Wizard Completed

If this is not your first time installing Blockbit Client or is updating it, your connection profiles will be stored in your Windows system folder and will be automatically added in your new installation..

Click in **[**  **]**.

Installation finished!

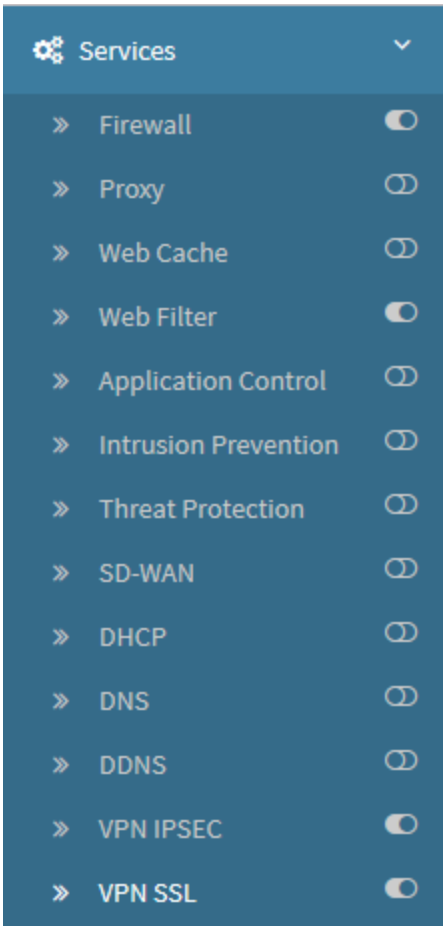
After installation is complete, the system will create an Agent icon on the desktop.

Desktop Shortcut

Finally, it will be necessary to make a configuration in the NGFW, more information follows:

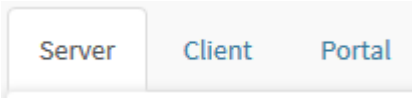
SSL VPN configuration

Access the NGFW that will be used to authenticate and in the Services menu, click the VPN SSL option:



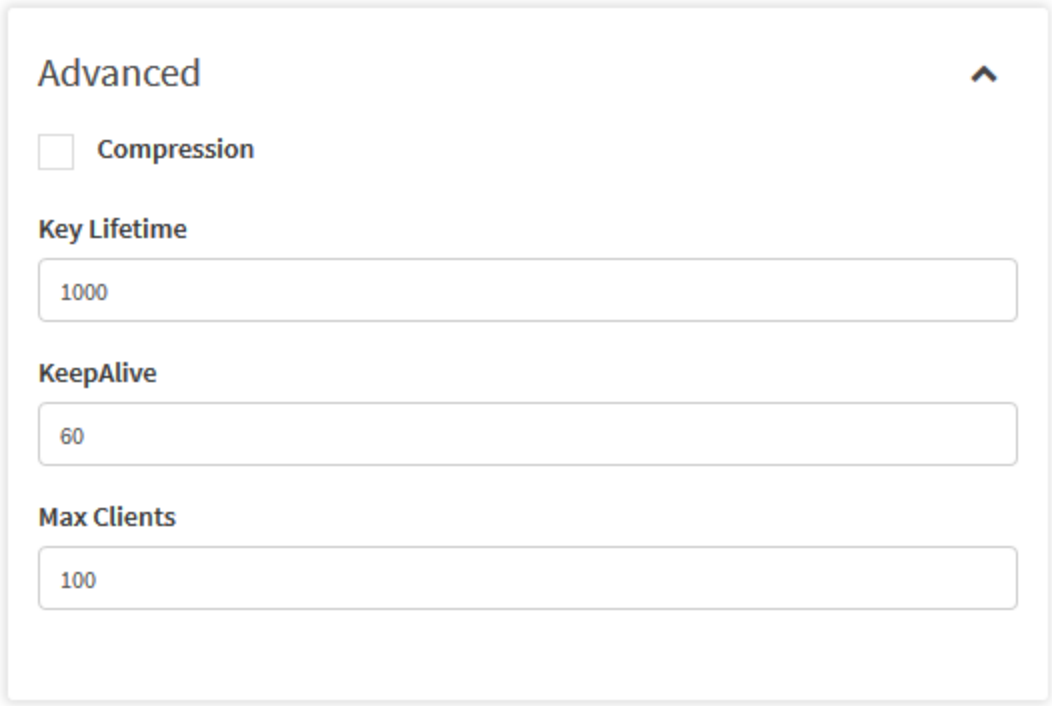
Services - VPN SSL

If it is not selected, click on the Server tab:



VPN SSL - Server

Access the Advanced panel at the bottom of the screen and expand it by clicking **[ ]**;



VPN SSL - Server - Advanced

On this panel, make sure that the compression option is enabled, otherwise the Blockbit Client will not work correctly.

Compression enabled

For more information on SSL VPN, see this page.

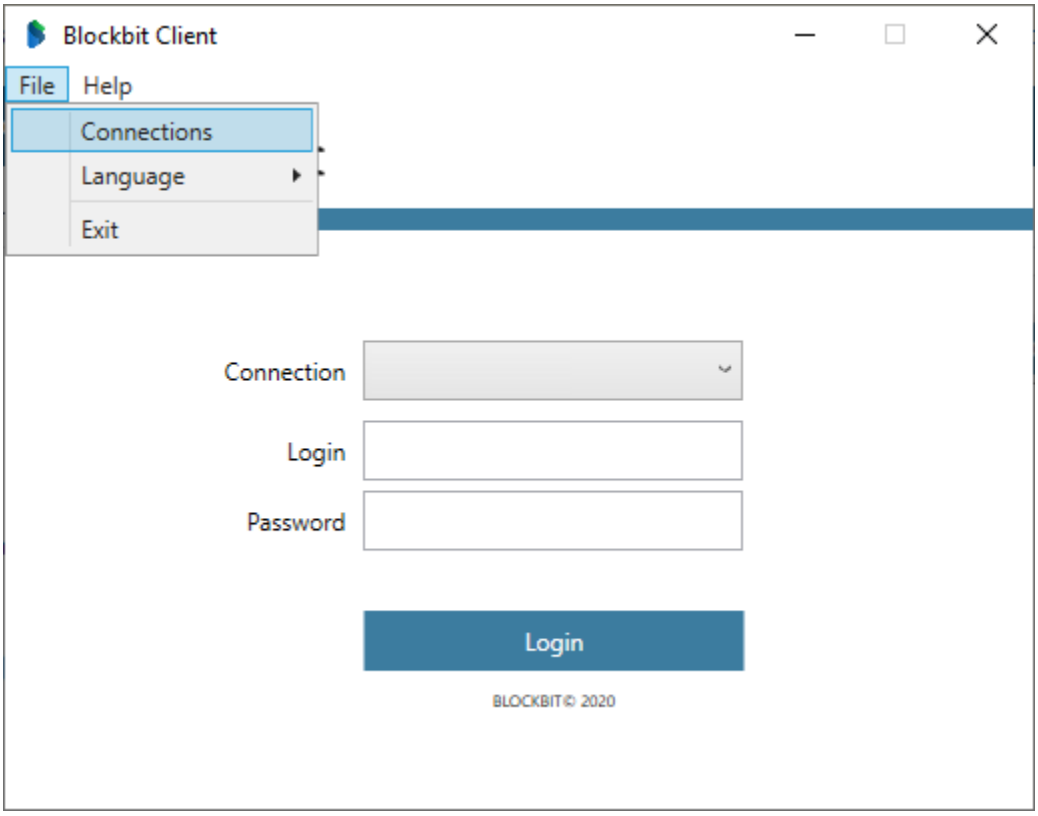
This concludes the installation and preparation of the Blockbit Client for your use. Next, we will see more information on how to configure it, for this purpose visit this page.

Blockbit Client configuration

The Blockbit Client allows the administrator to create **[N]** access profiles for the same installation on the local computer.

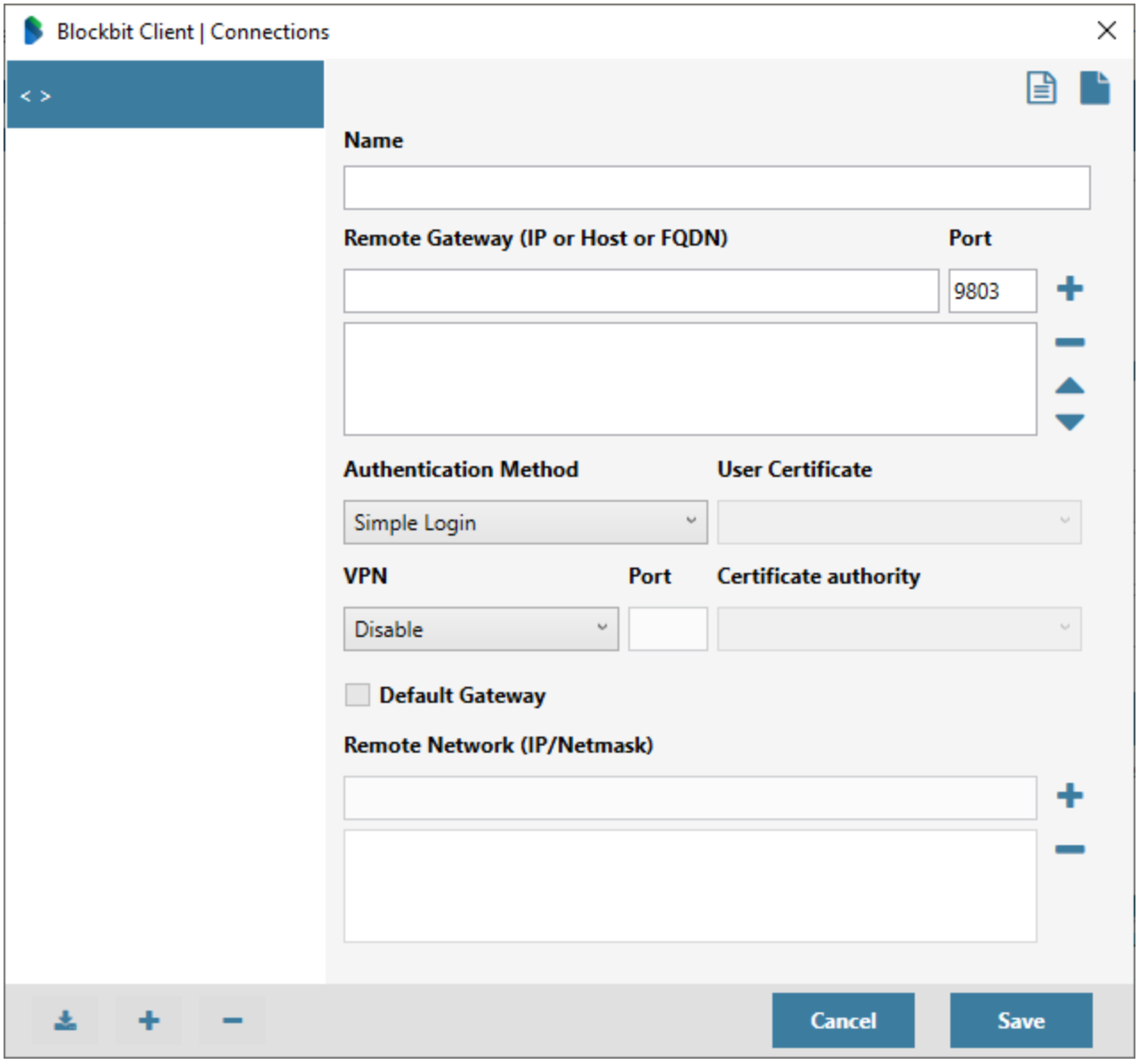
When opening it for the first time, as not even a connection has been configured, the "Connections" screen will be displayed automatically.

If a connection profile has already been installed, to access this screen, just click on "File" at the top of the window and select the "Connections" option, as shown below:



Blockbit Client - File - Connections

When selecting this option or in the case already mentioned above (newly installed Blockbit Client) the window below will be displayed:



Blockbit Client configuration

To create a profile you must configure the form according to the connection specifications with the respective Blockbit NGFW server. Next we will analyze each field in detail:

- ***Name*:** Connection profile name. Ex.: Default Auth;
- ***Remote Gateway*:** Enter the IP addresses, host or FQDN of the Blockbit NGFW servers and click **[ ]** to add it to the list, if you want to remove it, click **[ ]** and use the **[ ]** and **[ ]** arrows to change the priority. It is possible to add 3 remote Gateway addresses. The VPN connection service (IPSEC or SSL) tries to connect at the secondary address if it is unable to establish the connection from the Primary (the address at the top having higher priority). Ex.: utm.labblockbit.com;
- ***Authentication Method*:** Select between the authentication method to be used, which can be:

If you choose to authenticate with a certificate, you need to enable the NGFW option "Verify user certificate" in *Settings - Authentication - Settings*. Then, import this certificate into the "Current User" and select it in the connection configuration of the Blockbit Client.

The certificate must have the NGFW IP or a hostname that resolves the name to the NGFW IP, so that the client has the same data (IP or equal hostname) to make the connection.

For certificate authentication, you must have the server CA installed on the user's computer and use the signed gateway in the service certificate.

To use VPNs, it is necessary to install user and CA certificates on the user's station. See this page for more information on how to install.

- **Windows Login:** By selecting this option the Blockbit Client will recognize the user authenticated locally on the device or on the Windows network, as the authentication user for the Blockbit NGFW. The system will use the Active Directory credentials, without having to use the password. For an example, see this page;
- **Windows Login + Certificate:** When selecting this option, in addition to recognizing the user authenticated locally on the device or on the Windows network, the Blockbit Client will now perform two-factor authentication by adding the requirement of the digital user certificate - SSL during login. When selecting this method, the user will need to enter the portal, generate the certificate and install it using the Current User option (not local machine) so that his certificate is displayed in the "User Certificate" field. For an example, see this page;

For local networks, if you use the profiles above it is possible to transfer the Client with the main settings through a Windows GPO.

- **Simple Login:** If this option is selected, the user will need to use the user name and password to connect to the Blockbit NGFW. Ex .: **Jhonny.muller@ead.labblockbit.com.** This method also uses Active Directory credentials to authenticate. For an example, see this page;
- **Simple Login + Certificate:** With this option selected, in addition to using the “User Name” and “Password”, the Blockbit Client will now perform two-factor authentication, adding the requirement of the digital user certificate - SSL during login. For an example, see this page;
- ***Login + Certificate* (*IPSEC legacy*):** This option is used specifically to maintain Blockbit Client compatibility with the NGFW 2.0.4 and below, including 1.5. Blockbit Client accesses using digital certificate. Therefore, it will be necessary to complete the **Remote Network** field with information from the IPSEC VPN used. For an example, see this page;

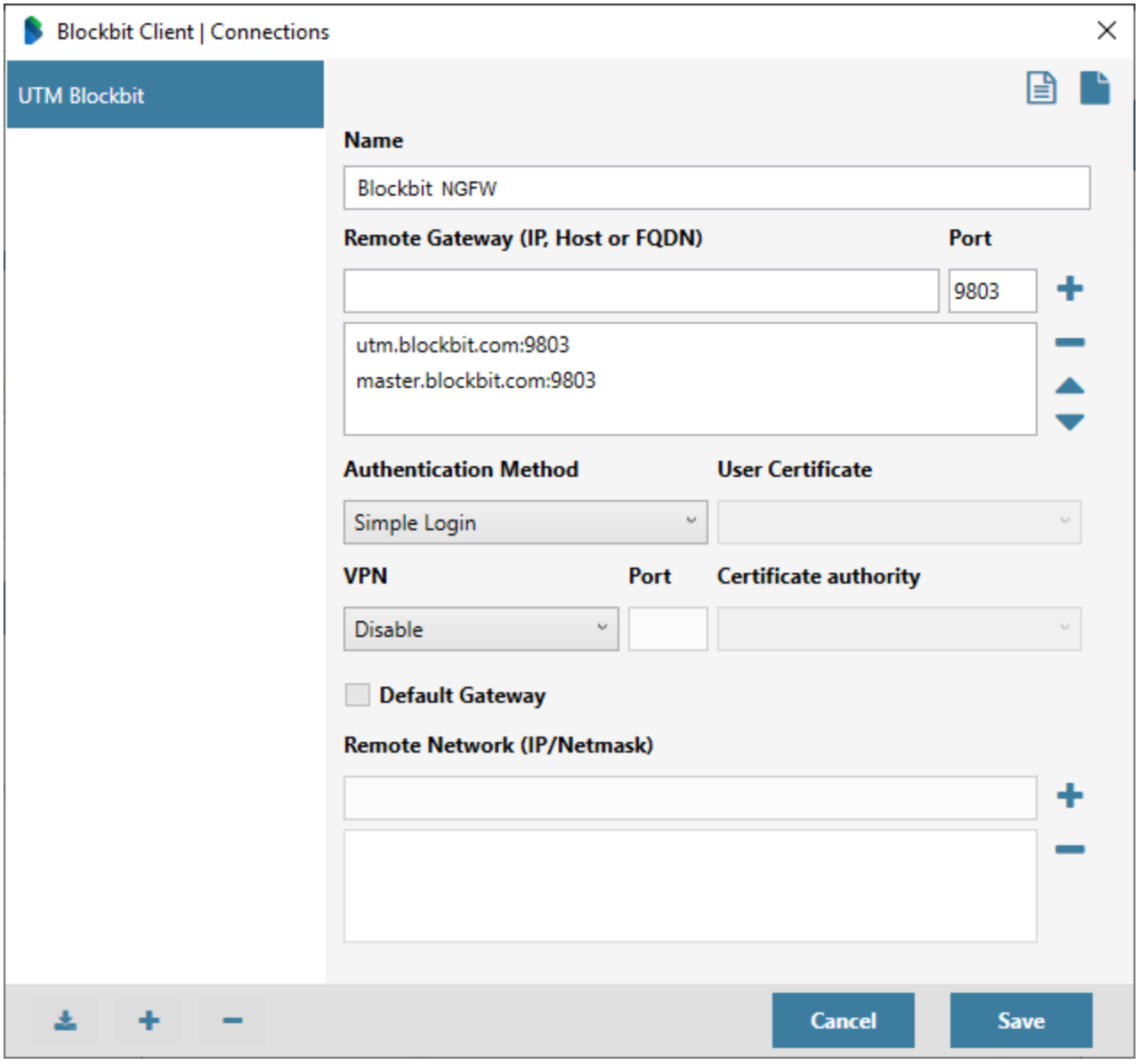
If your version is lower than NGFW 2.0.5 and you are using the Blockbit Agent with IPSEC VPN, when migrating to the Blockbit Client, the IPSEC VPN will only work if **Login + Certificate (IPSEC Legacy)** mode is used.

- ***User Certificate:*** If you have selected an authentication method that requires a certificate, you will need to import it and select it in this field. If you have not selected the relevant option, this field will be disabled. To display it in this list, it is necessary to install on the current user (not on the local machine). For more information, see this page;
- **VPN:** Select the type of VPN that will be used to connect automatically, there are two options available:
  - **Disable:** In this case, access will be local, so the **"Port"** field and the **"Default Gateway"** checkbox are disabled;
  - **SSL:** If this option is selected, the **"Port"** field will need to be filled with the SSL port (by default the system uses port 9443). On the right, the ***Certificate Authority*** field will be enabled, inform it which Root CA will be used, see this page for more information on Certificate Installation or this page for more information on how to configure the NGFW to use an SSL VPN;
- ***Port*:** The connection port for the authentication service. The default port is 9443. Ex.: 9803;
- **Certificate Authority:** When the SSL option is selected in the VPN field, this field will be enabled. Its function is to allow the selection of which Root CA will be used by the SSL VPN. *To display the CA in this list, it is necessary to install the certificate on the local machine (not the local user) and save it in the Trusted Root Certification Authority folder*. For more information, see this page;
- **Default Gateway[☑]:** By checking this checkbox, the VPN will now use the default gateway, this means that a route will be closed with the NGFW and all connections will go completely through the firewall (respecting its policies). If this check box is not selected, the connection will be completely disconnected over the user's computer's local network, but closing routes with the IPs added in the Remote Network list (IP / Netmask).
- ***Remote Network* (*IP/Netmask*):** If the check box above is checked, this field will be enabled for editing. Enter the IPs or Netmasks that will be used remotely and click **[+]** to add it to the list, if you want to remove it, click **[−]**.

In case of connection failure with the gateway, a record is added in the Log.

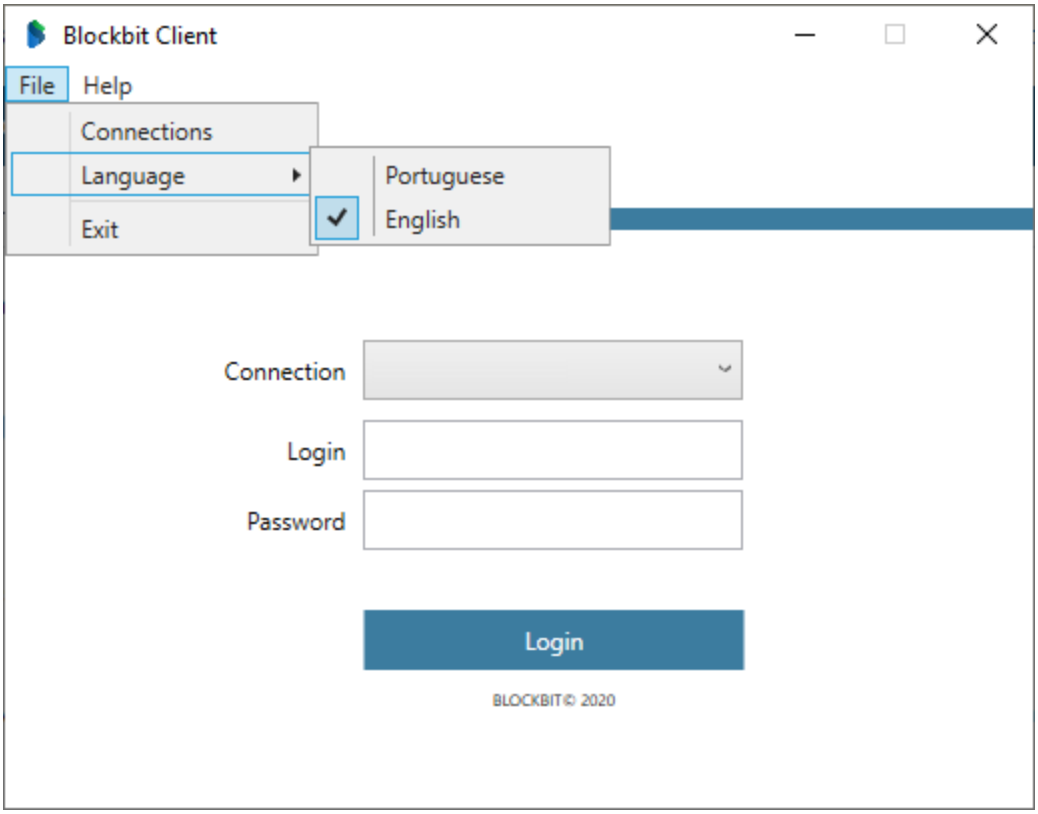
Click **[Save]** to create the profile and finish the settings or **[Cancel]** to return to the previous screen.

After saving the settings the profile will have been created successfully, as shown in the image below:



Blockbit Client - Configured

Finally, the Blockbit Client is available in Portuguese and English. To change the language, just click "File" at the top of the window and select the "Language" option, as shown below:



Blockbit Client - File - Language

This ends the process of configuring the Blockbit Client profiles.

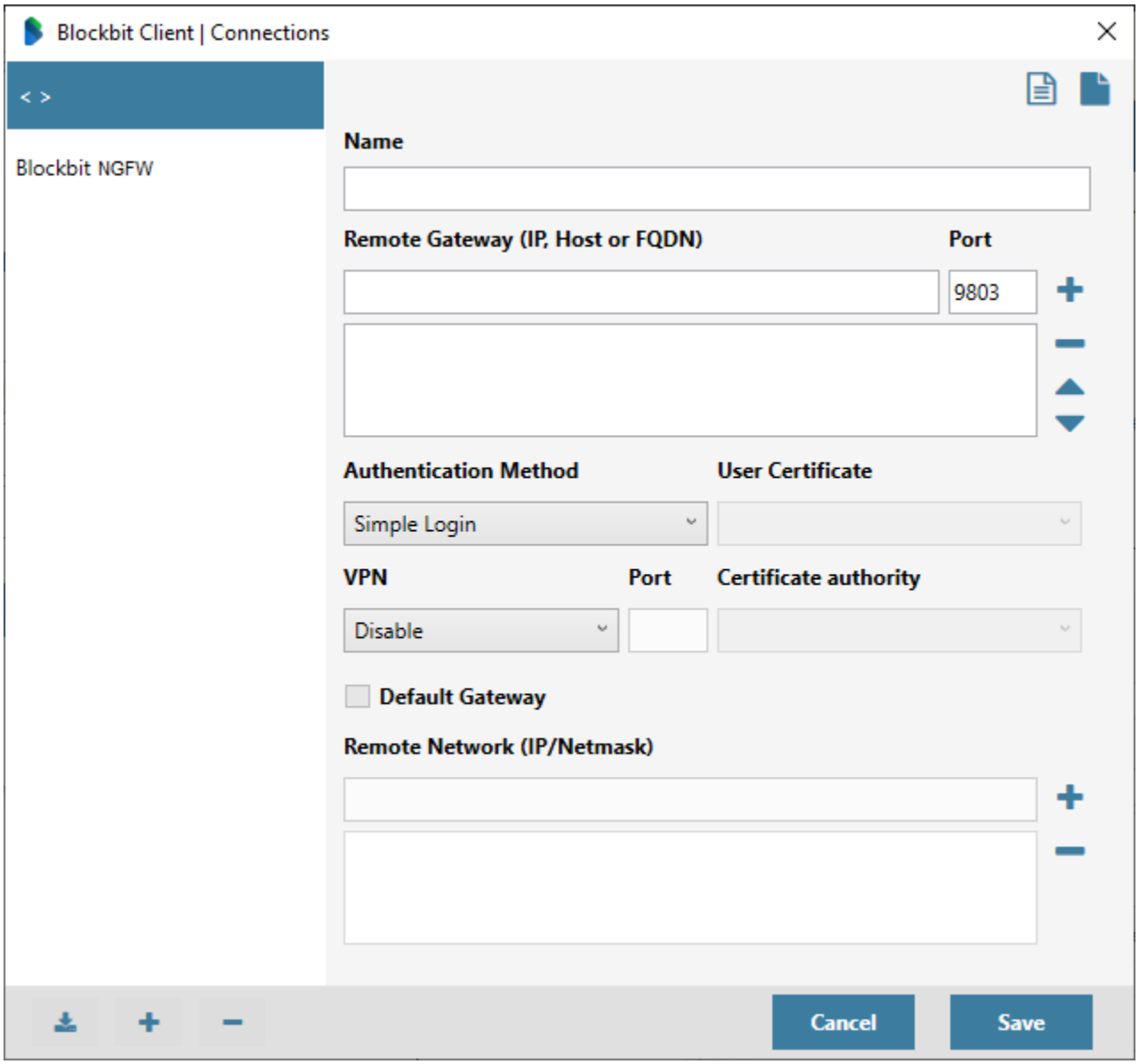
To view examples of configuring connection profiles, see this page.

For more information on how to use these profiles to make a connection, see this page.

See this page for a step-by-step how to install certificates.

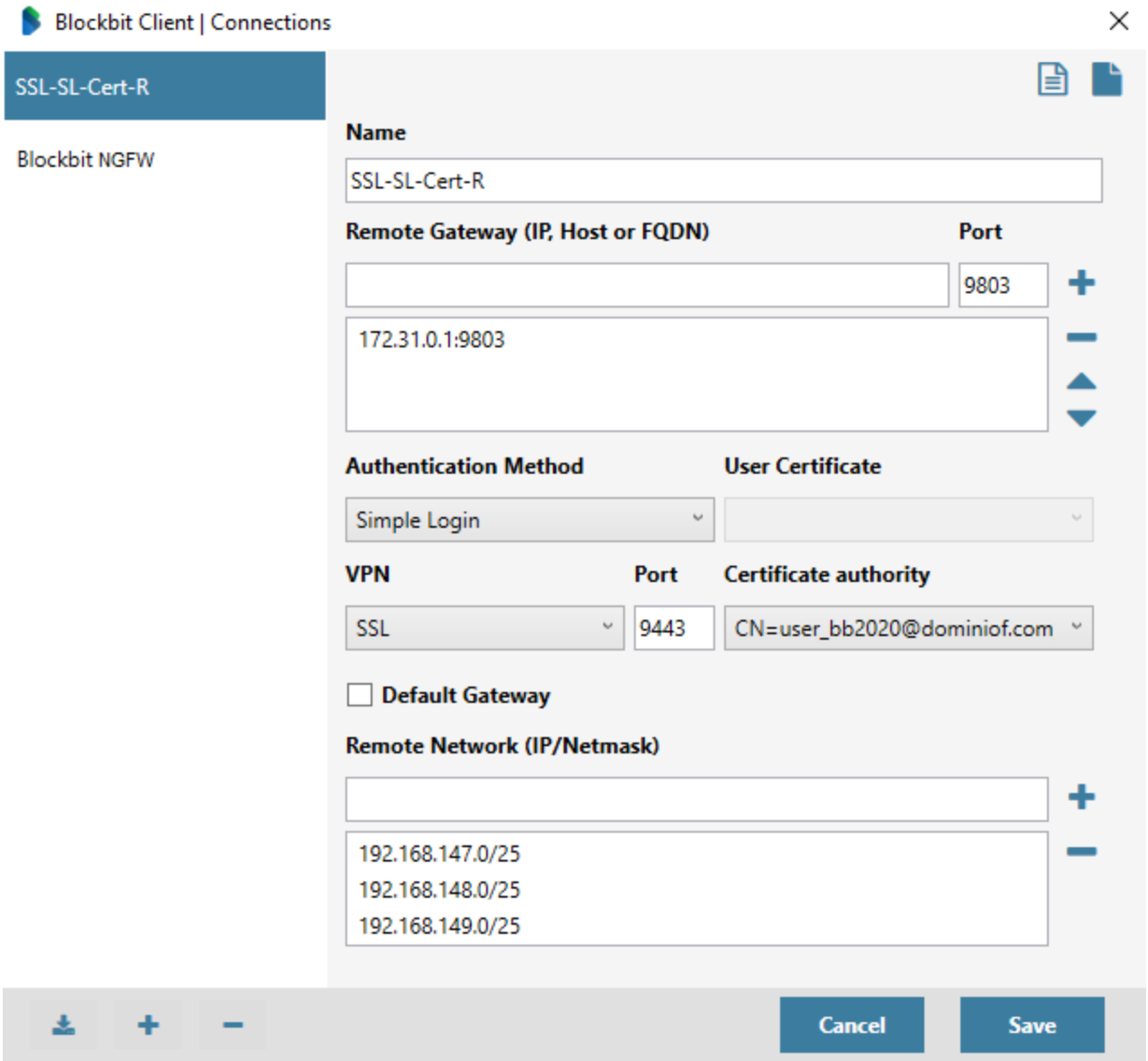
Adding a new profile

To add a new connection profile, click on the **[+]** button located in the lower left corner. A new connection profile form will be displayed:



Blockbit Client - Connections - New Profile

After clicking on this button, just complete the form in the same way as shown on this page. For example:



Blockbit Client - Connections - New Profile - Example

Click [Save] to create the profile and finish the settings or [Cancel] to return to the previous screen.

If the connection profile requires the installation of a certificate, see this page for more information.

Next, we'll check how to Remove a Profile.

Installation of Certificates

In the Blockbit Client in profiles that use certificates to authenticate or use VPN, it is mandatory to install the CA on the local machine, in addition the certificate must be enabled in the authentication settings in the NGFW.

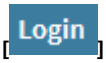
If the authentication on the Blockbit Client presents the error "Connection failed", even after installing the NGFW CA, it is necessary to enable the verification of the CA located in Authentication - Settings tab;

On this page we will demonstrate how to perform:

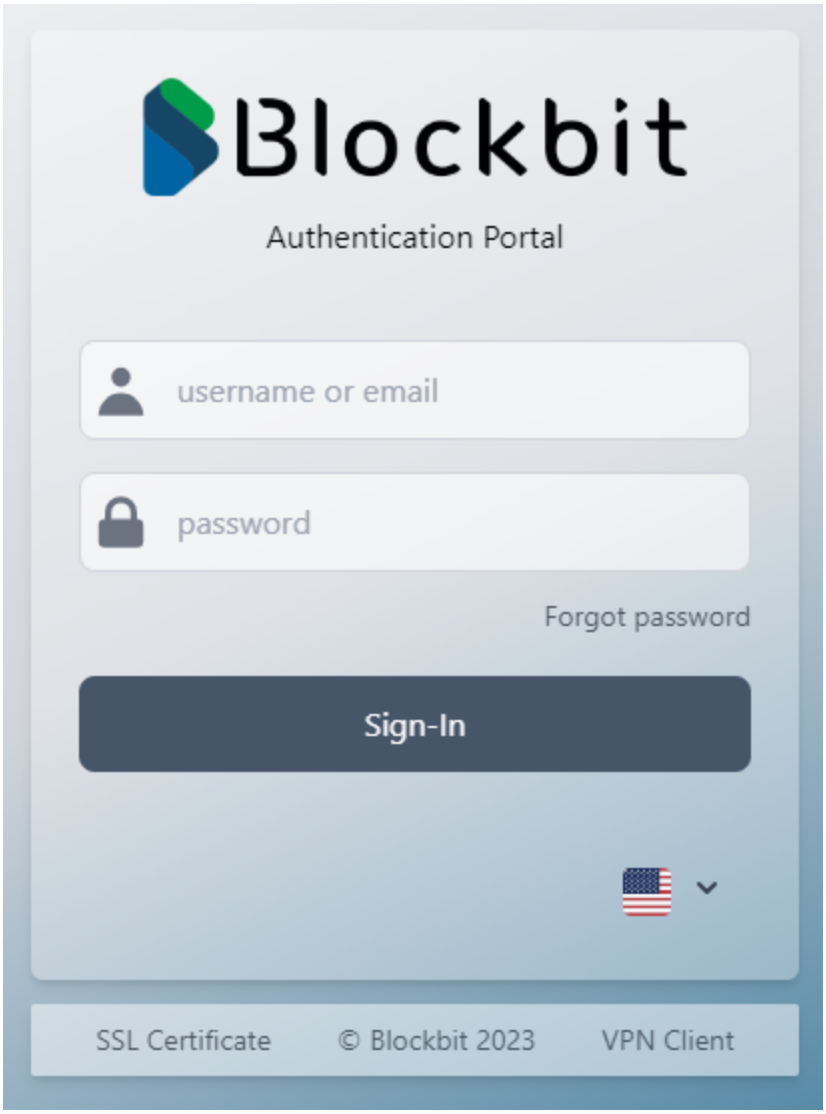
- Installing User Certificates;
- Installation of CAs.

Next we will analyze how to install the certificates.

Installing User Certificates

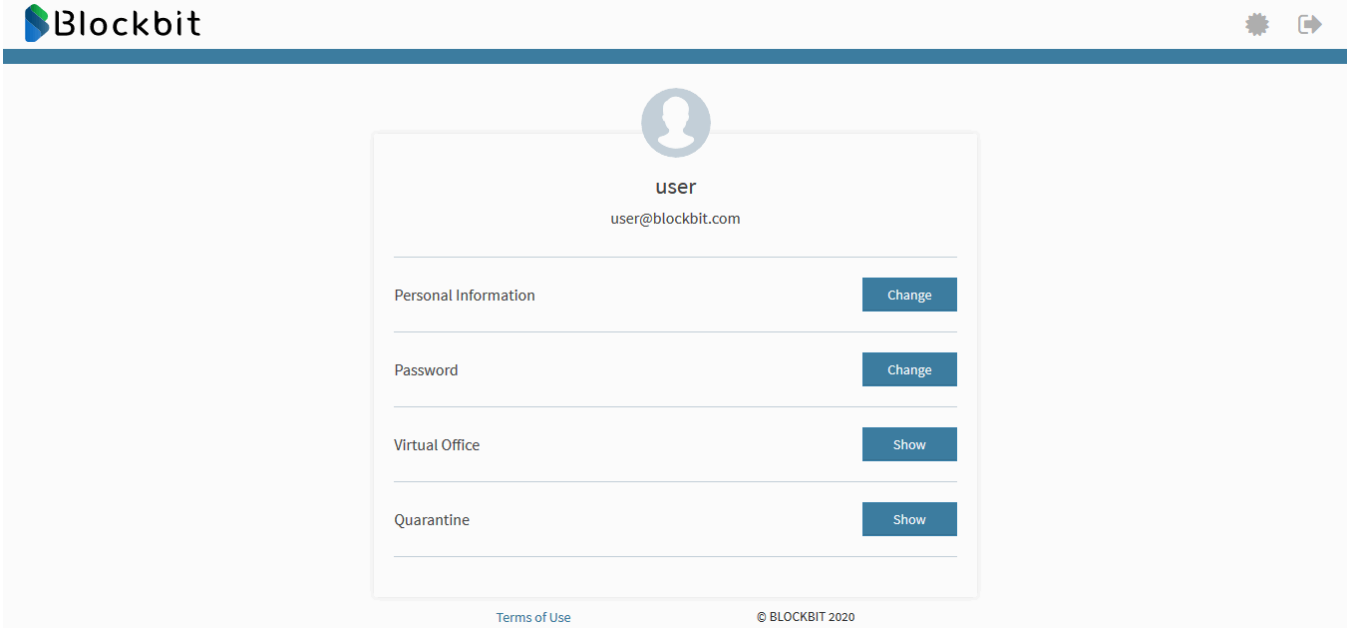
First access the *captive portal* and log in with the user to be used, after filling out the form click on the **[** 

] button:



Portal - Certificate

The following window will appear:

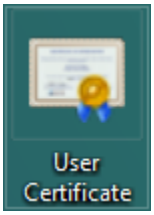


Portal - Logged

Download the user certificate by clicking the **[**  **]** button located in the upper right corner of the screen.

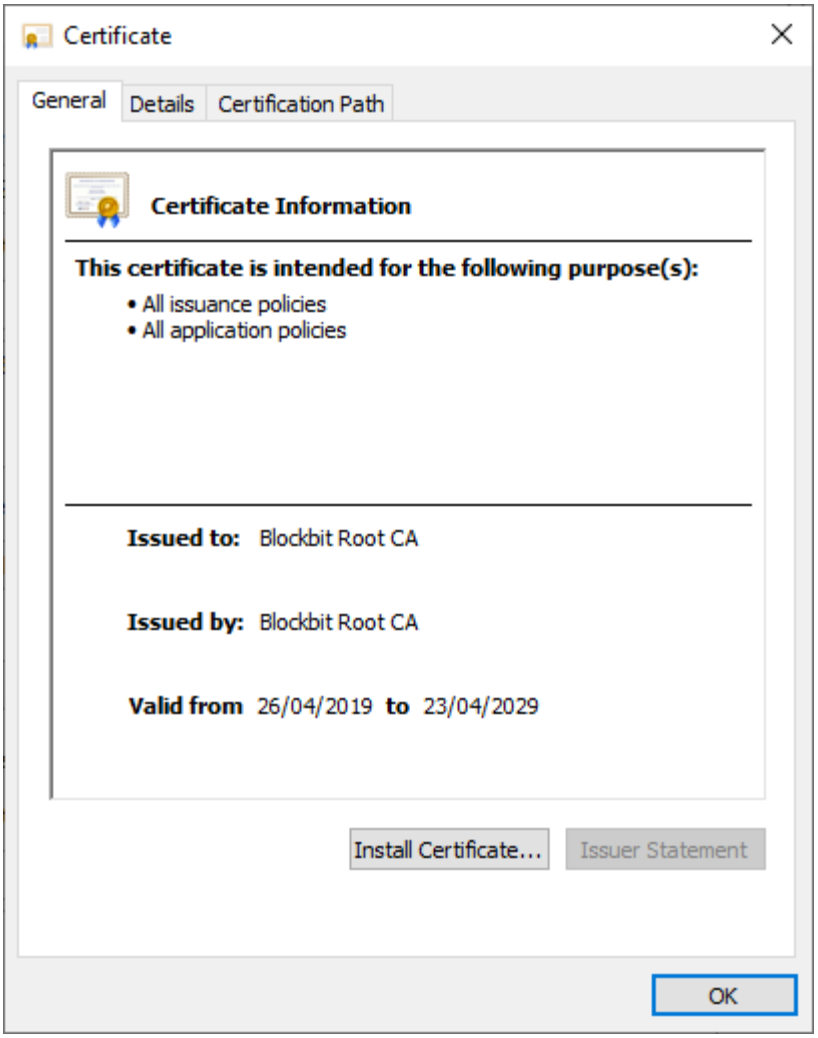
If it is necessary to install the CA too, to make it easier, it is recommended to rename the file in order to distinguish it from the CA.

When the download is complete, click on the certificate to open it:

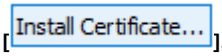


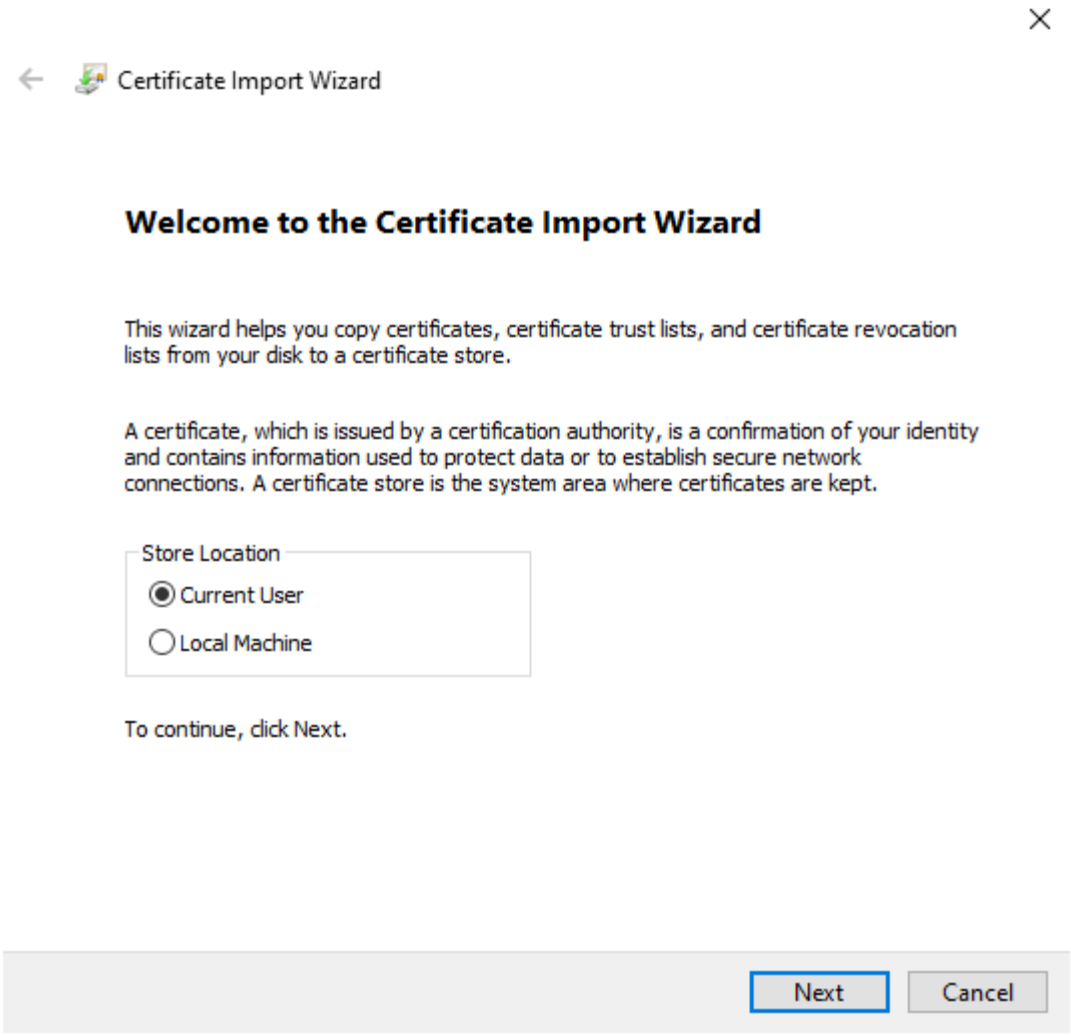
User Certificate

The following window will appear:



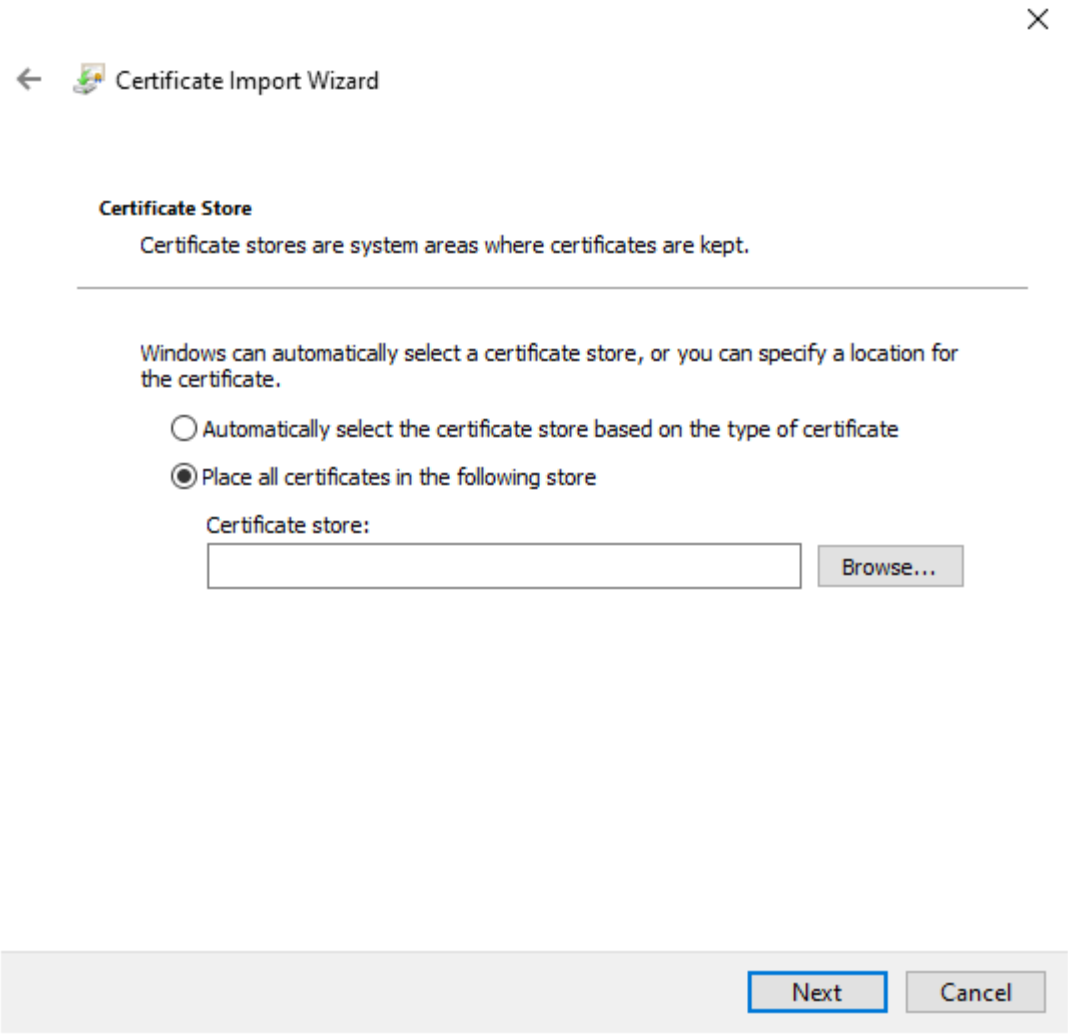
Certificate Information

Click **[**  **]**, the following window will appear:



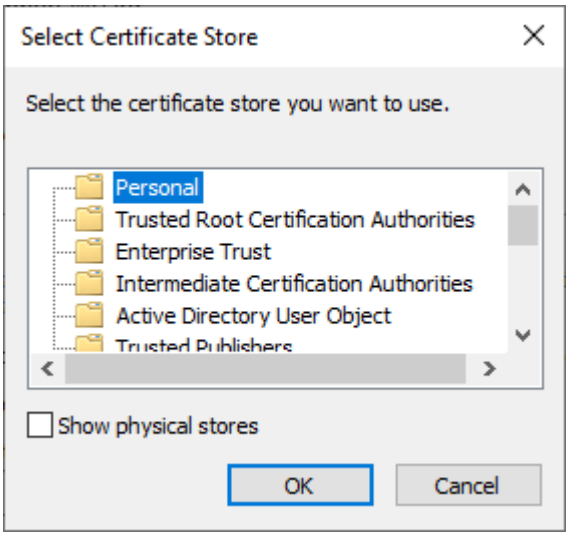
Certificate Import Wizard

Make sure that ***Current User*** [◉] is selected and click the [Next] button.



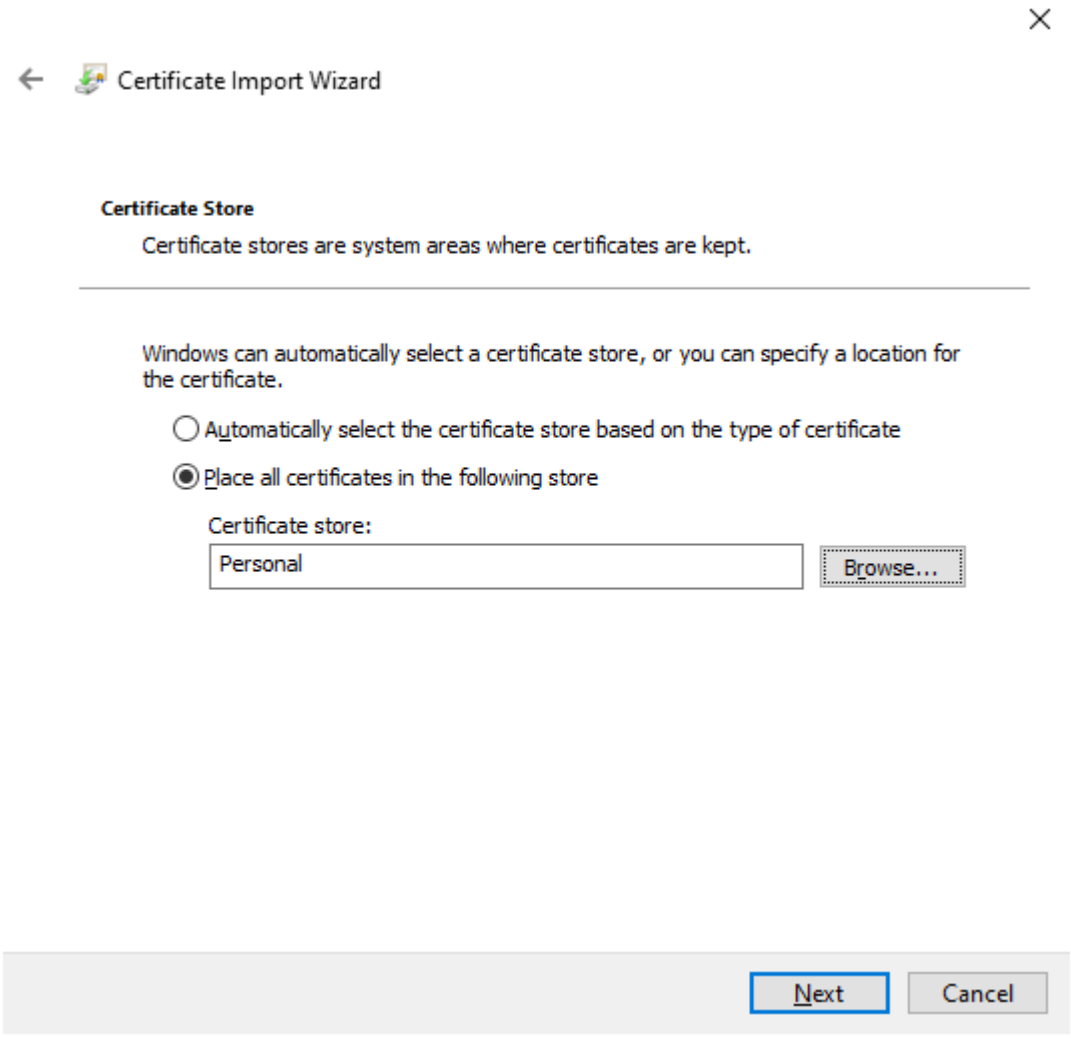
Certificate Store

Select the option ***Place all certificates in the following stores*** **[** **]** and click the **[** Browse... **]** button to select where the certificate will be stored, the following window will be displayed:



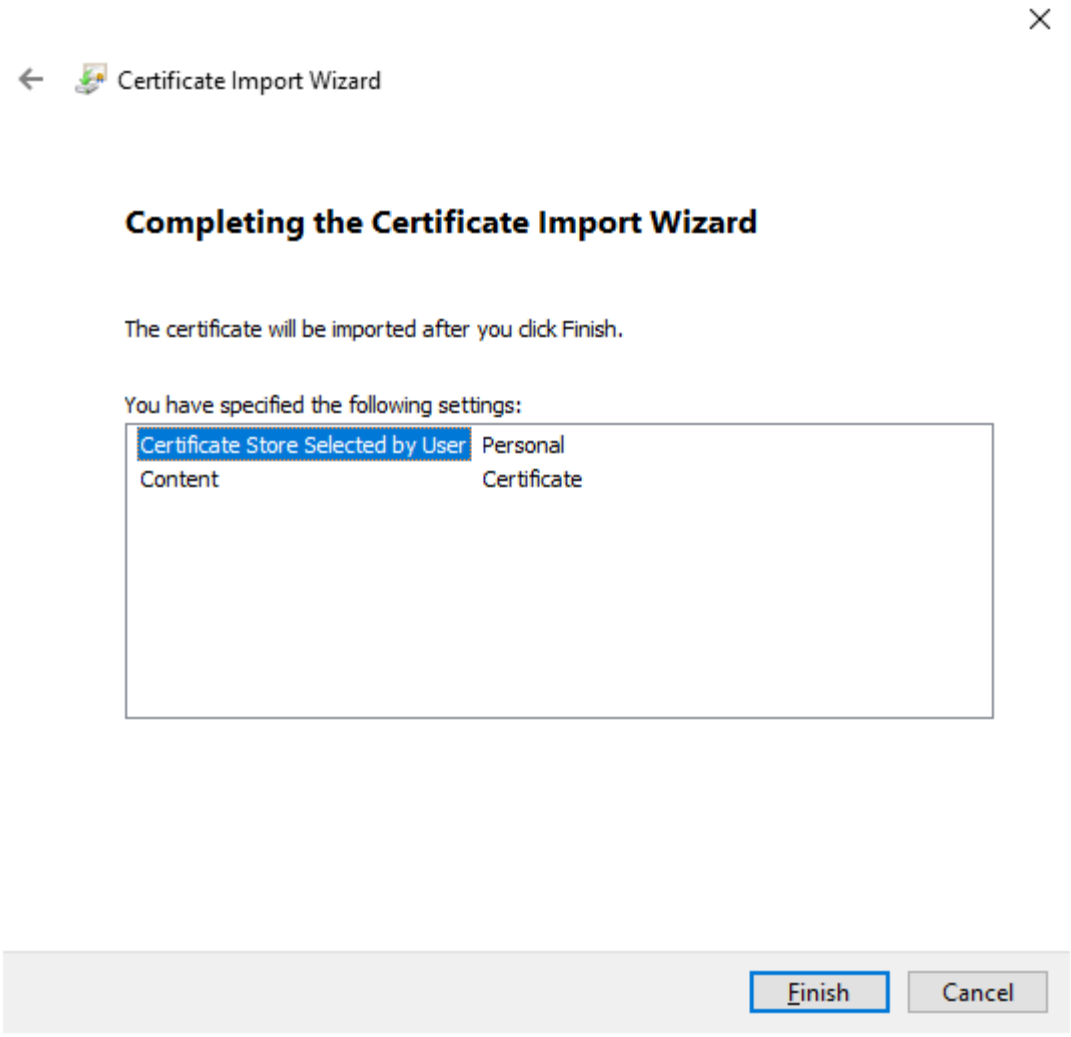
Select Certificate Store

In Select Certificate Store, make sure that the **Personal** option is selected and click [OK], the following screen will be displayed:



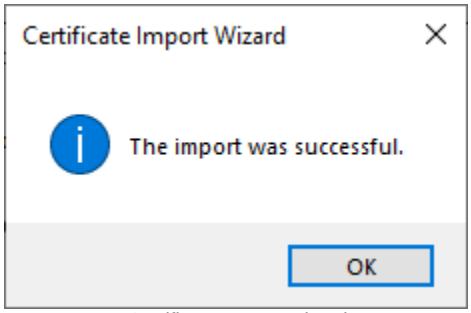
Certificate Store - Selected Store

Click on the [Next] button the following screen with a summary of the certificate import will be displayed:



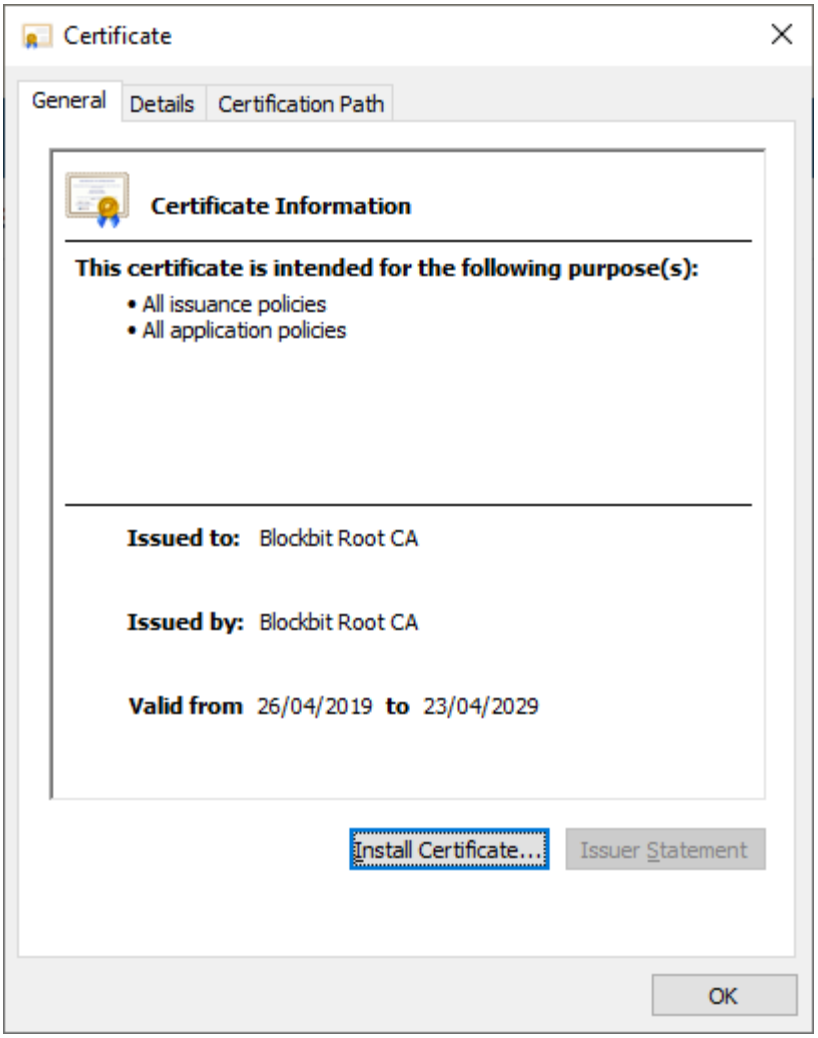
Certificate Import Wizard - Selected Store

Click the **[** Finish **]** button to perform the import:



Certificate Import Wizard

Click on the **[** OK **]** button, the ***certificate information*** screen will be displayed again:



Certificate Information

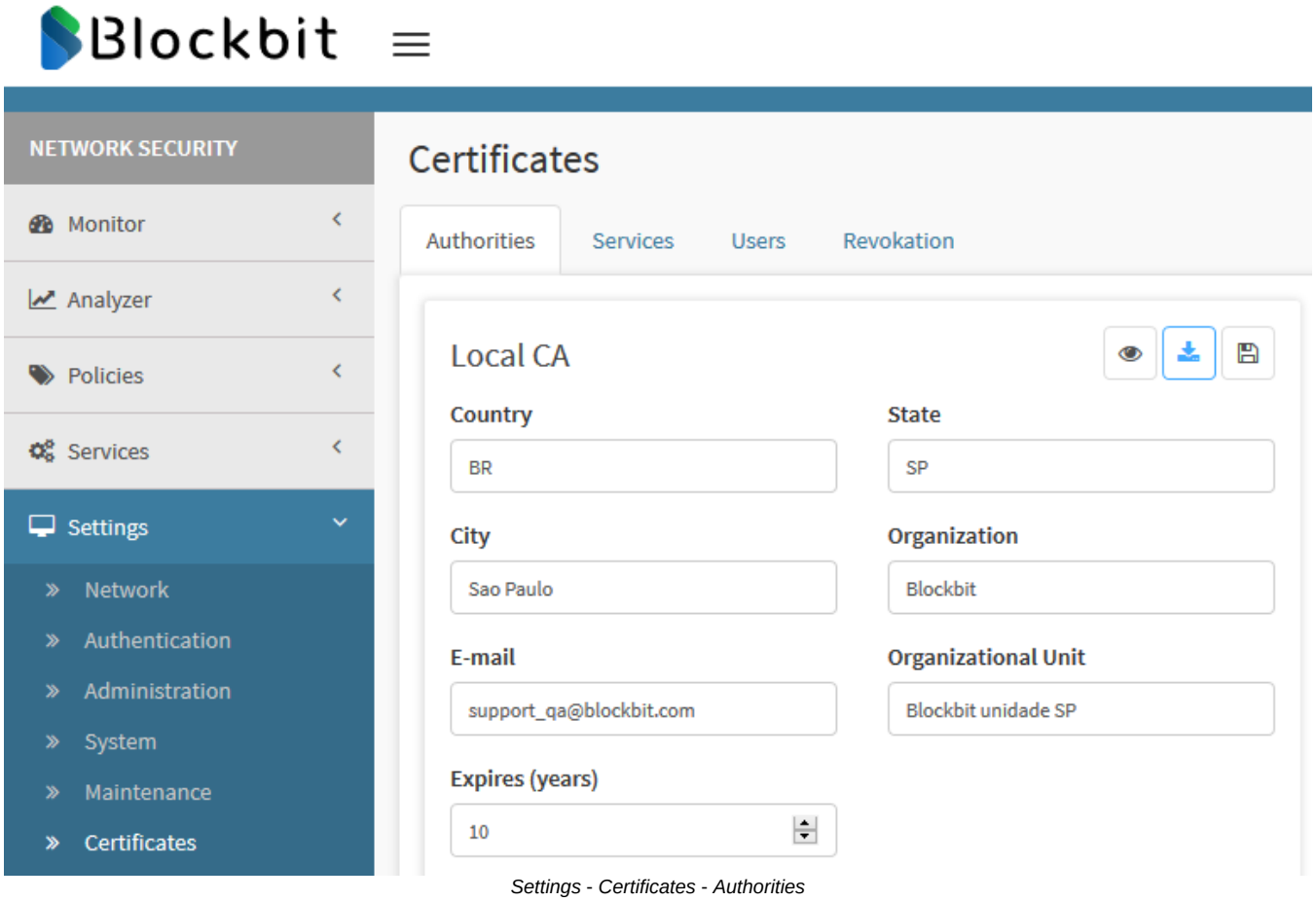
Click **[** OK **]** to finish installing the user's certificate.

Next we will detail how to install a CA.

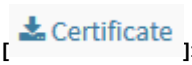
Installation of CAs

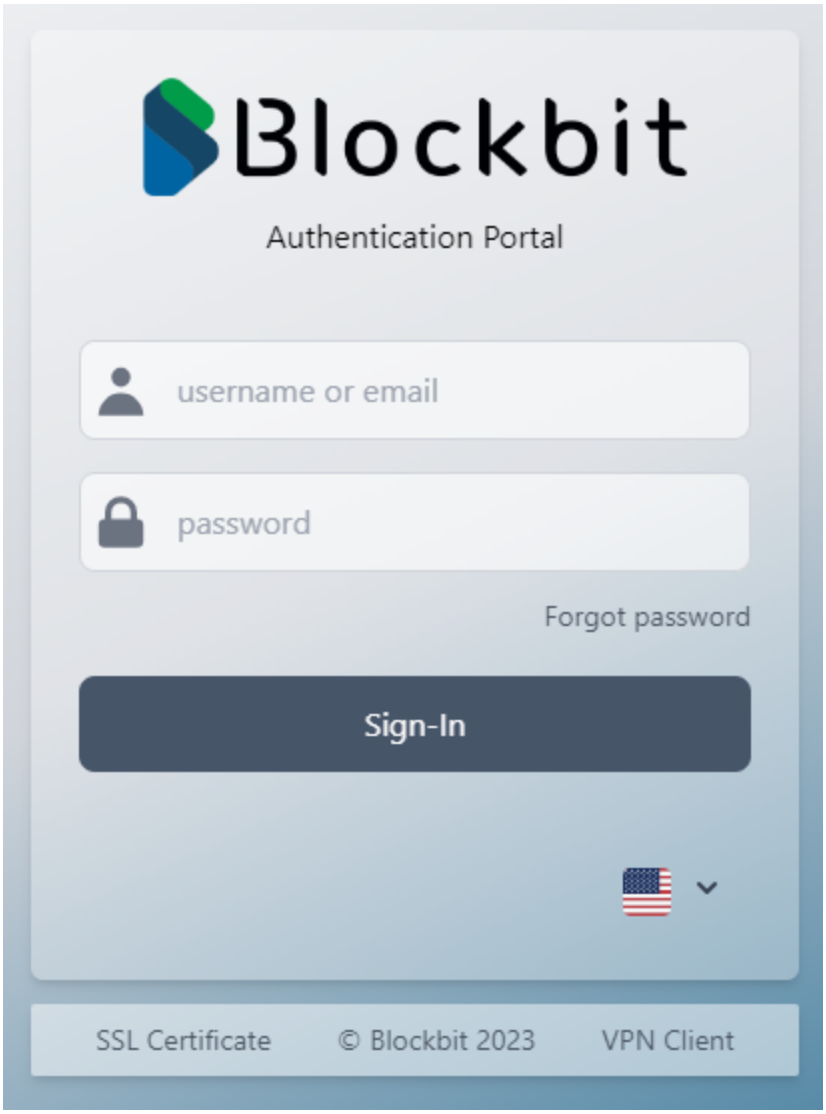
There are two ways to download the CA: If you are an administrator, you can access the settings menu, option certificates, in the authorithies tab in NGFW (for more information, see this page).

Once this is done, click on the **[** **]** button, as shown below:



Settings - Certificates - Authorities

The other way to download the CA is through the *captive portal*, clicking **[**  **]**:

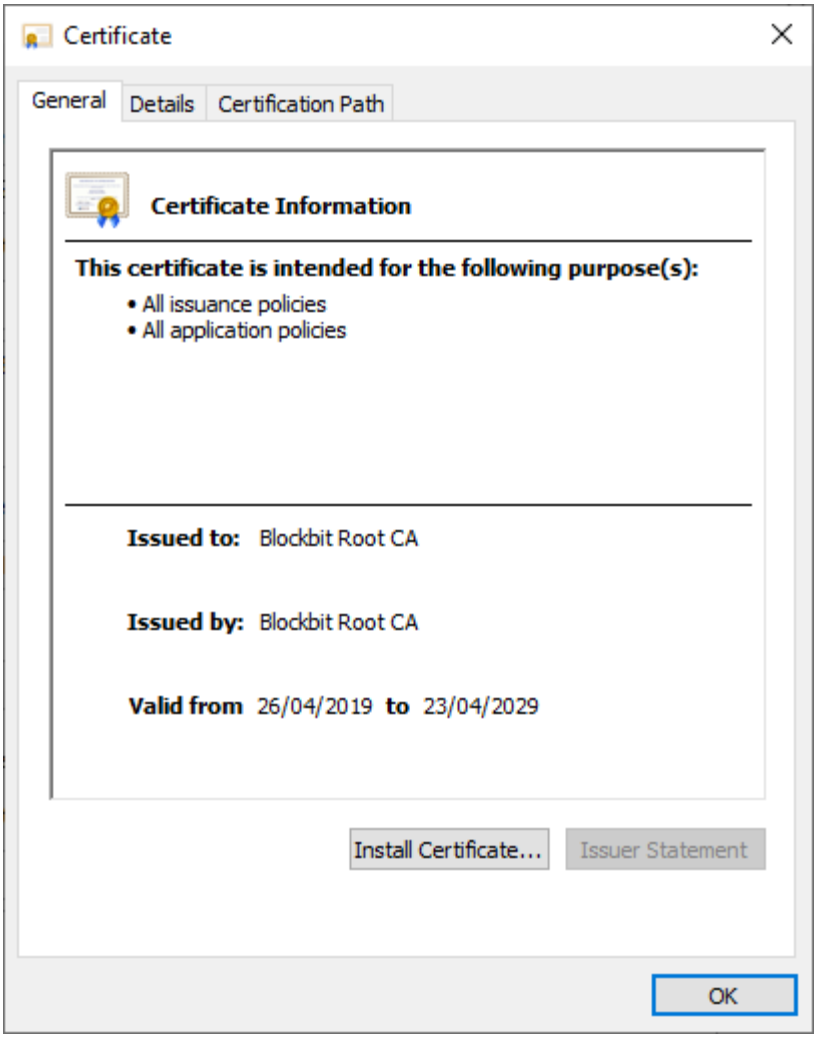


Portal - Certificate

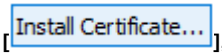
When the download is complete, click the icon to open the certificate:

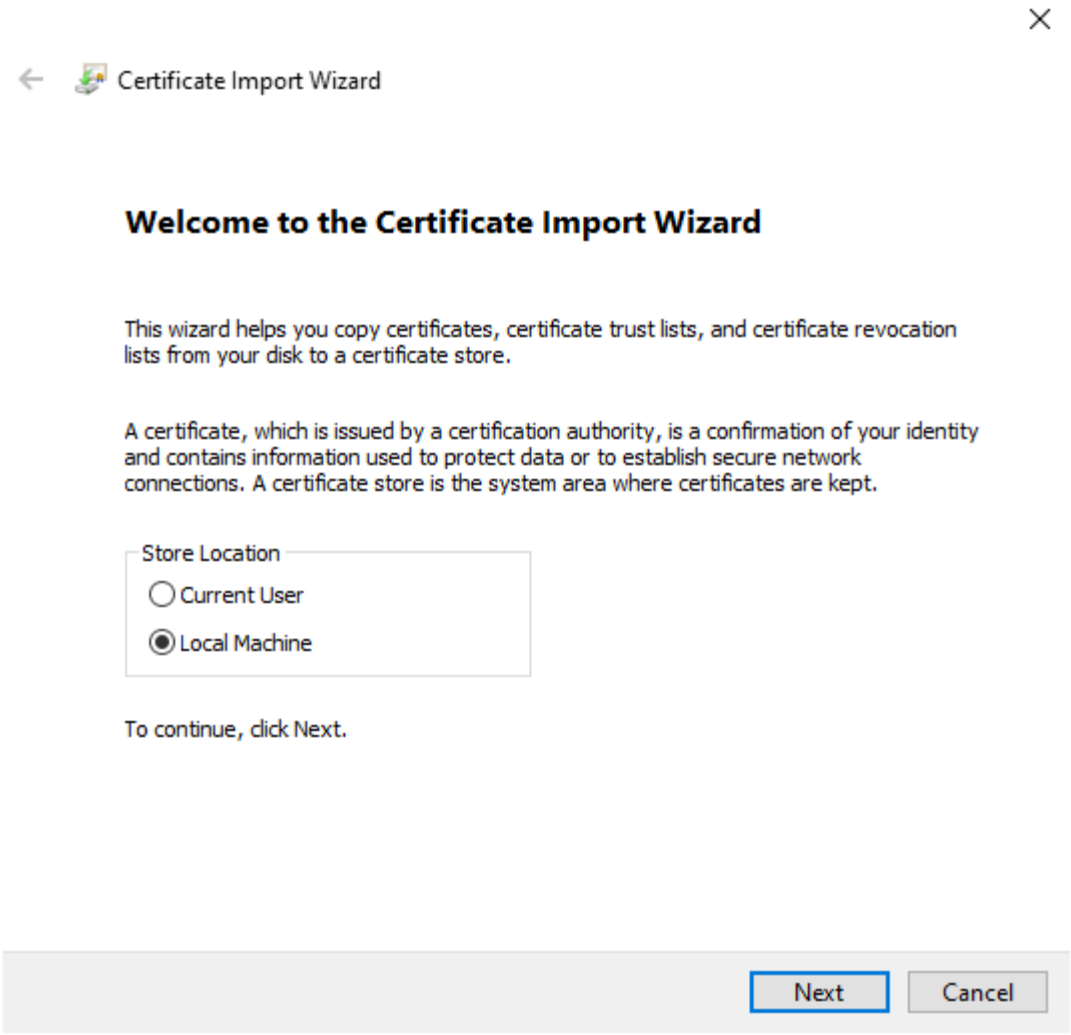
Local Root CA

The following window will appear:



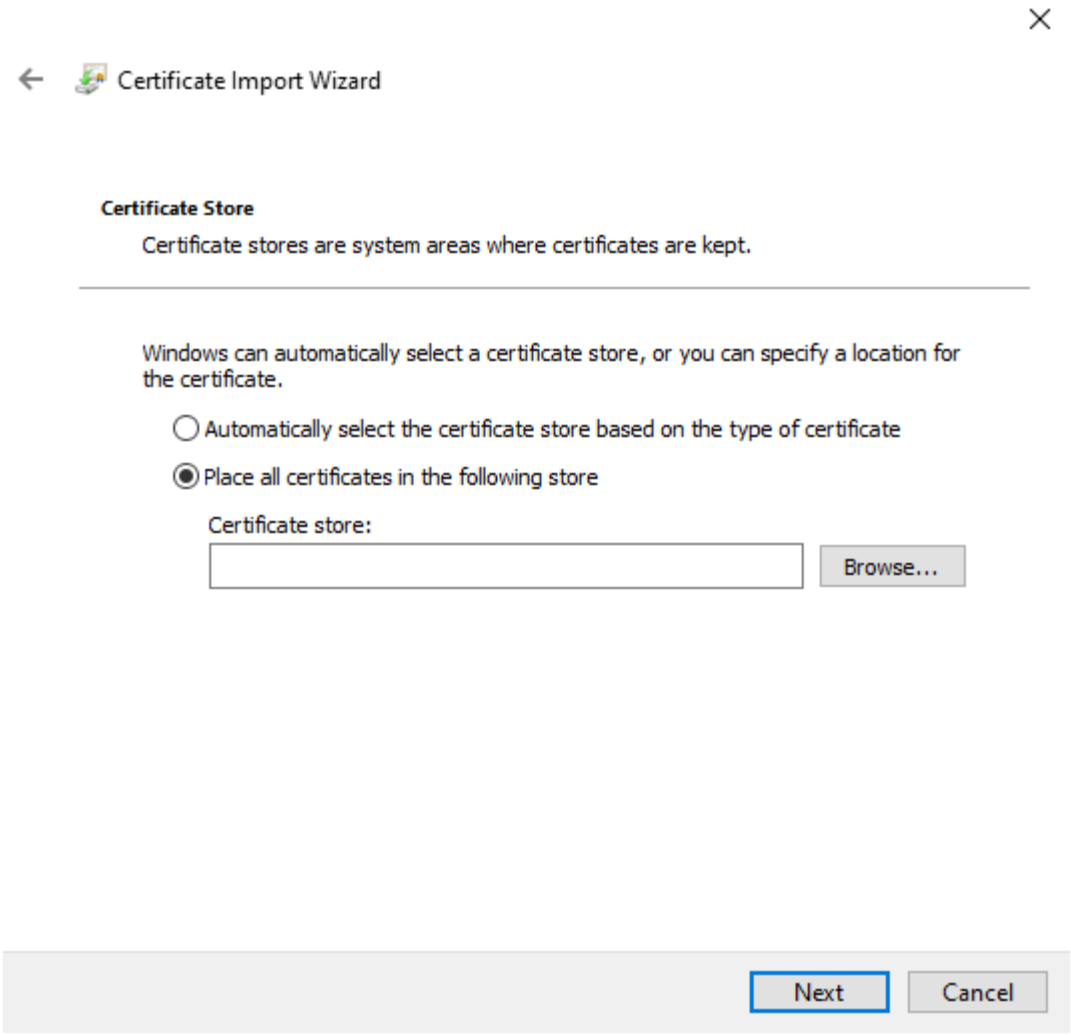
Certificate Information

Click **[**  **]**, the following window will appear:



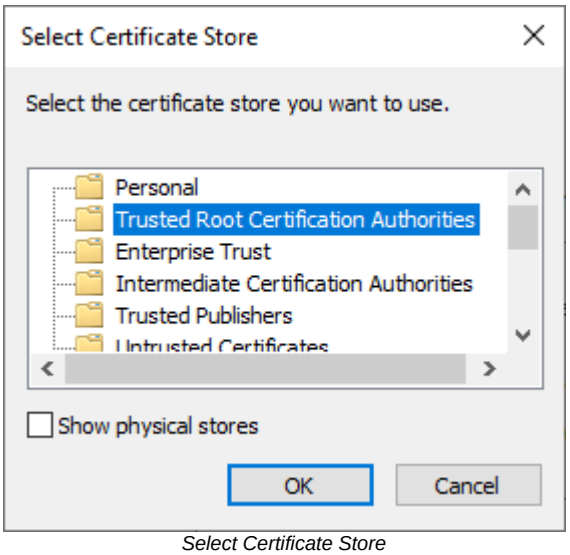
Certificate Import Wizard

Make sure that ***Local Machine*** [◉] is selected and click the [Next] button.



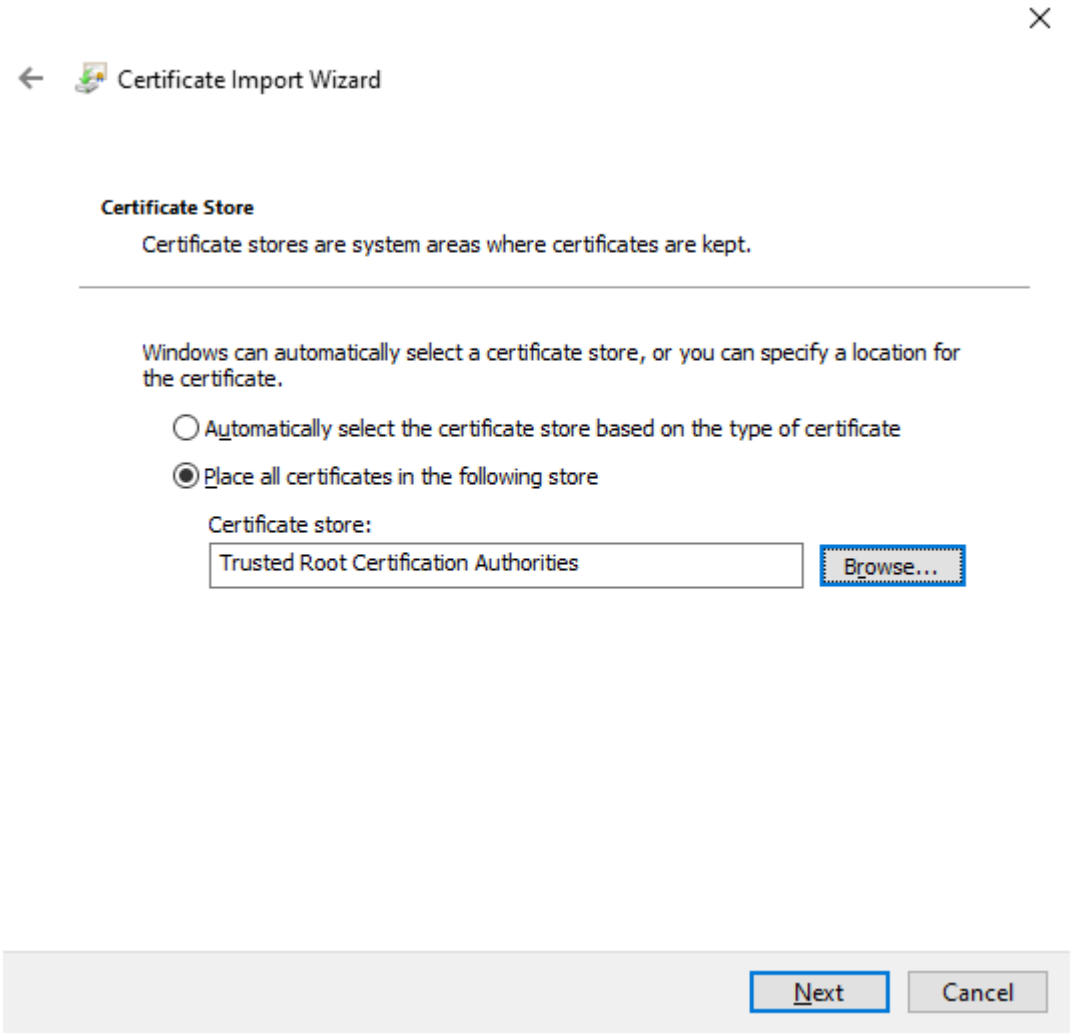
Certificate Store

Select the option ***Place all certificates in the following stores*** **[** **]** and click the **[** Browse... **]** button to select where the certificate will be stored, the following window will be displayed:



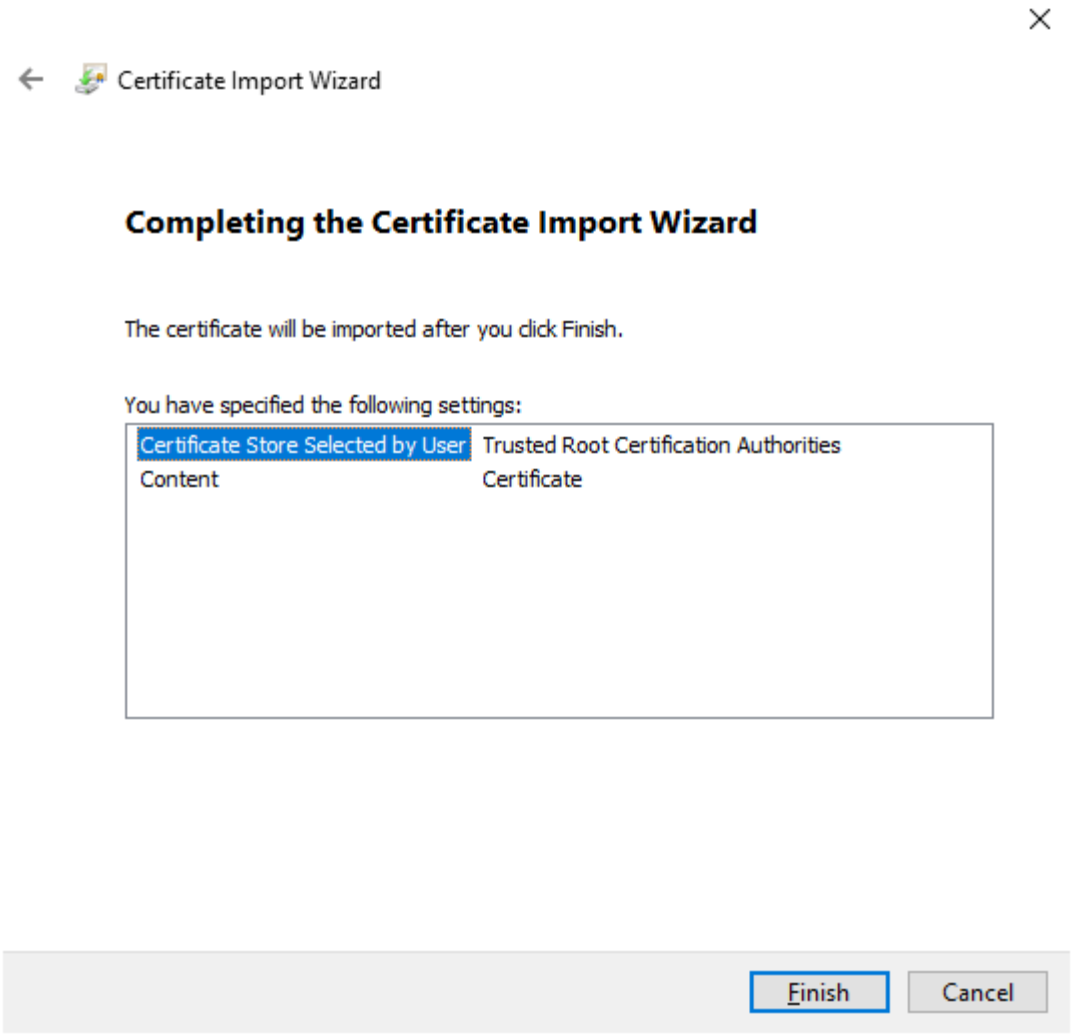
Select Certificate Store

In Select Certificate Store, make sure that ***Trusted Root Certification Authorities*** is selected and click on [OK], the following screen will be displayed:



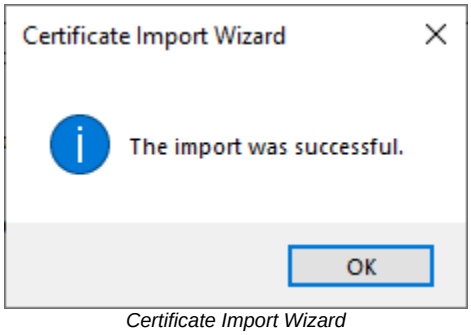
Certificate Store - Selected Store

Click on the [Next] button the following screen with a summary of the certificate import will be displayed:



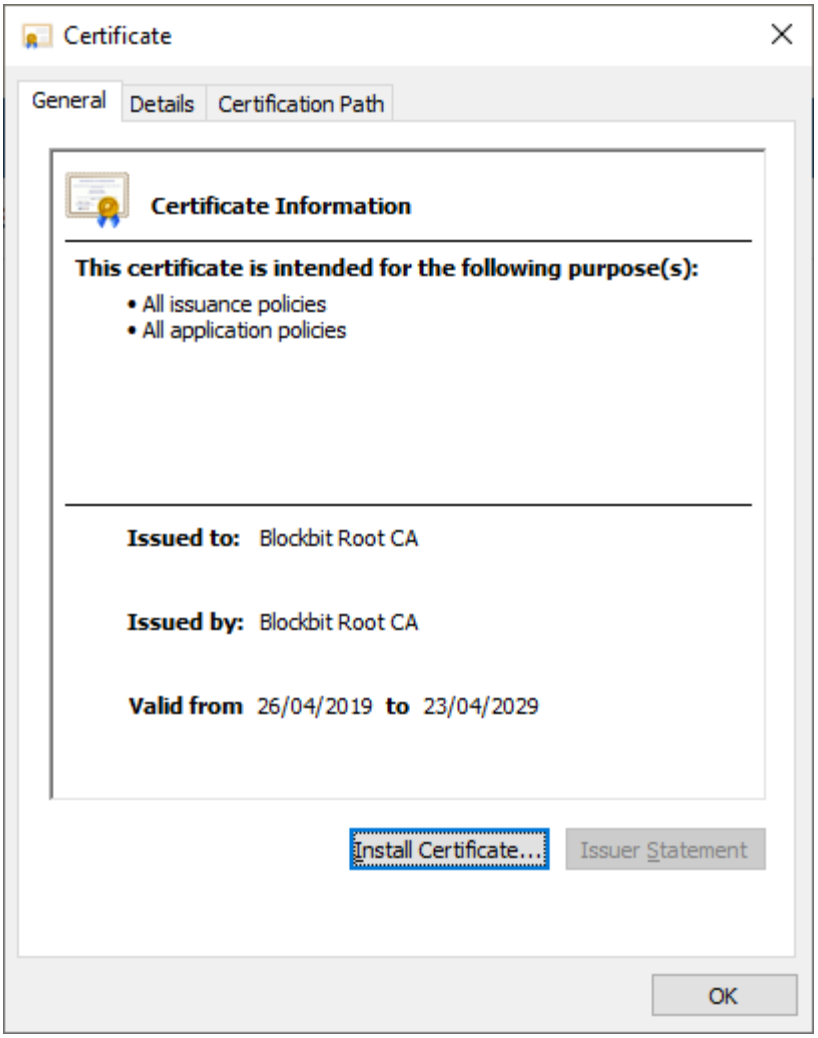
Certificate Import Wizard - Selected Store

Click the **[** Finish **]** button to perform the import:

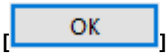


Certificate Import Wizard

Click the **[** OK **]** button, the ***certificate information*** screen will be displayed again:



Certificate Information

Click **[**  **]** to complete the CA installation.

This completes the installation of the required certificates.

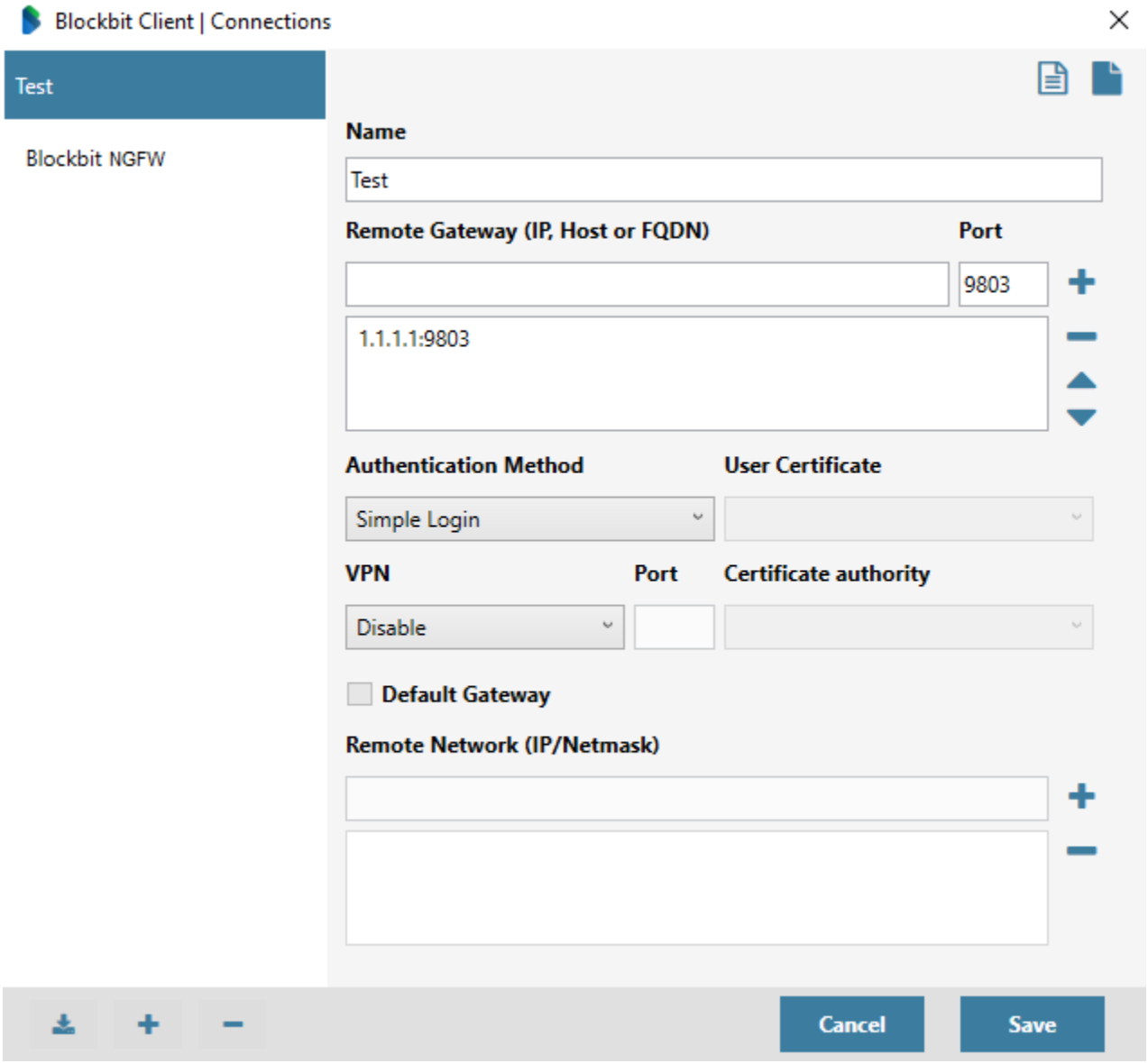
Finally, back in the Blockbit Client, just select the certificate that was installed in **Personal** in the User Certificate field (in the step Installing User Certificates);

And in Certificate Authority select the one that was installed in ***Trusted Root Certification Authorities*** (in step Installation of CAs).

For more information on configuring connection profiles, see this page.

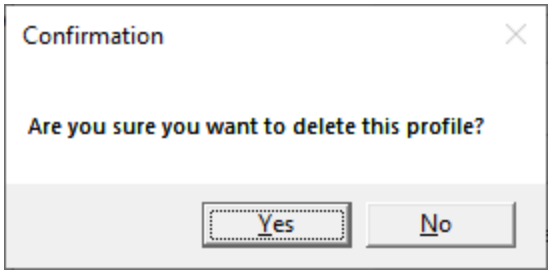
Profile Removal

To delete a connection profile, select it from the menu on the left, as shown below:

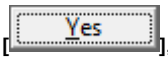


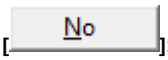
Blockbit Client - Connections - Selected

Once this is done, click on the **[ ]** button located in the lower left corner, the following message will be displayed:



Are you sure you want to delete this profile?

To proceed with the deletion, just click **[** 

], otherwise click **[** 

];

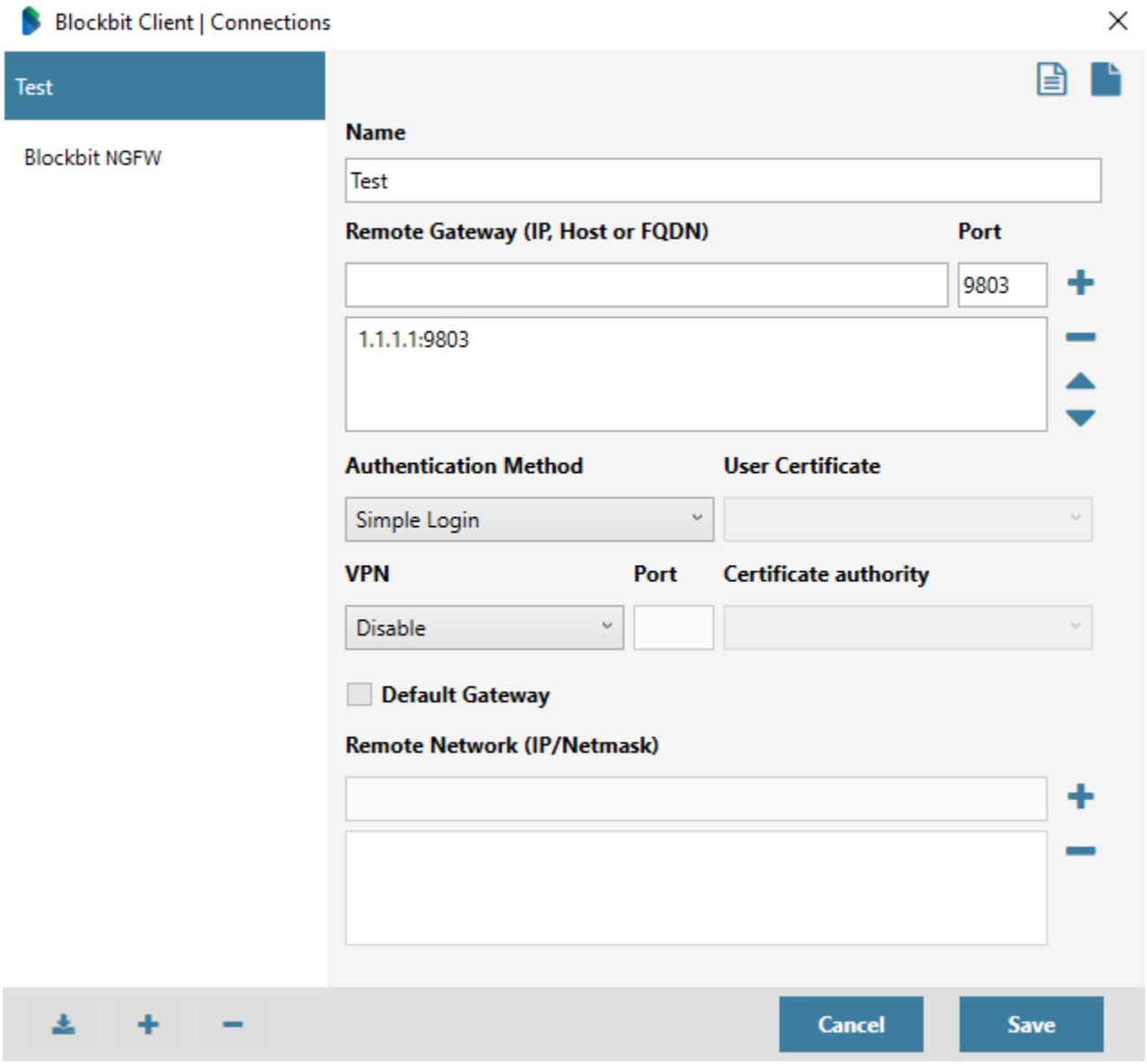
Next, we will analyze how to Import and export a Profile.

Profile Export and Import

On this page we will demonstrate the process of exporting and importing a connection profile.

Profile Export

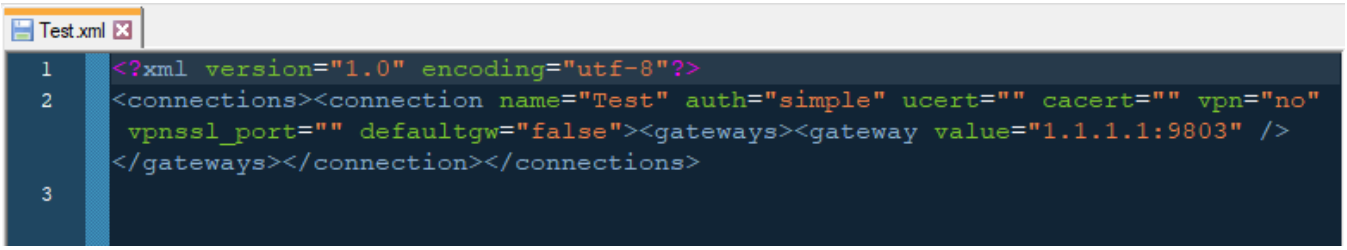
Initially, before exporting a profile, select it from the left side menu, as shown below:



Blockbit Client - Connections - Selected

That done, when clicking on the **[**  **]** icon located in the upper right corner of the window, an XML file will be generated, save it in a safe place.

The profile is an XML file containing the information added when creating the selected profile, an example follows:



Blockbit Client - Connections - *Exported Profile*

This concludes the export process.

Below we will demonstrate how to import this connection profile.

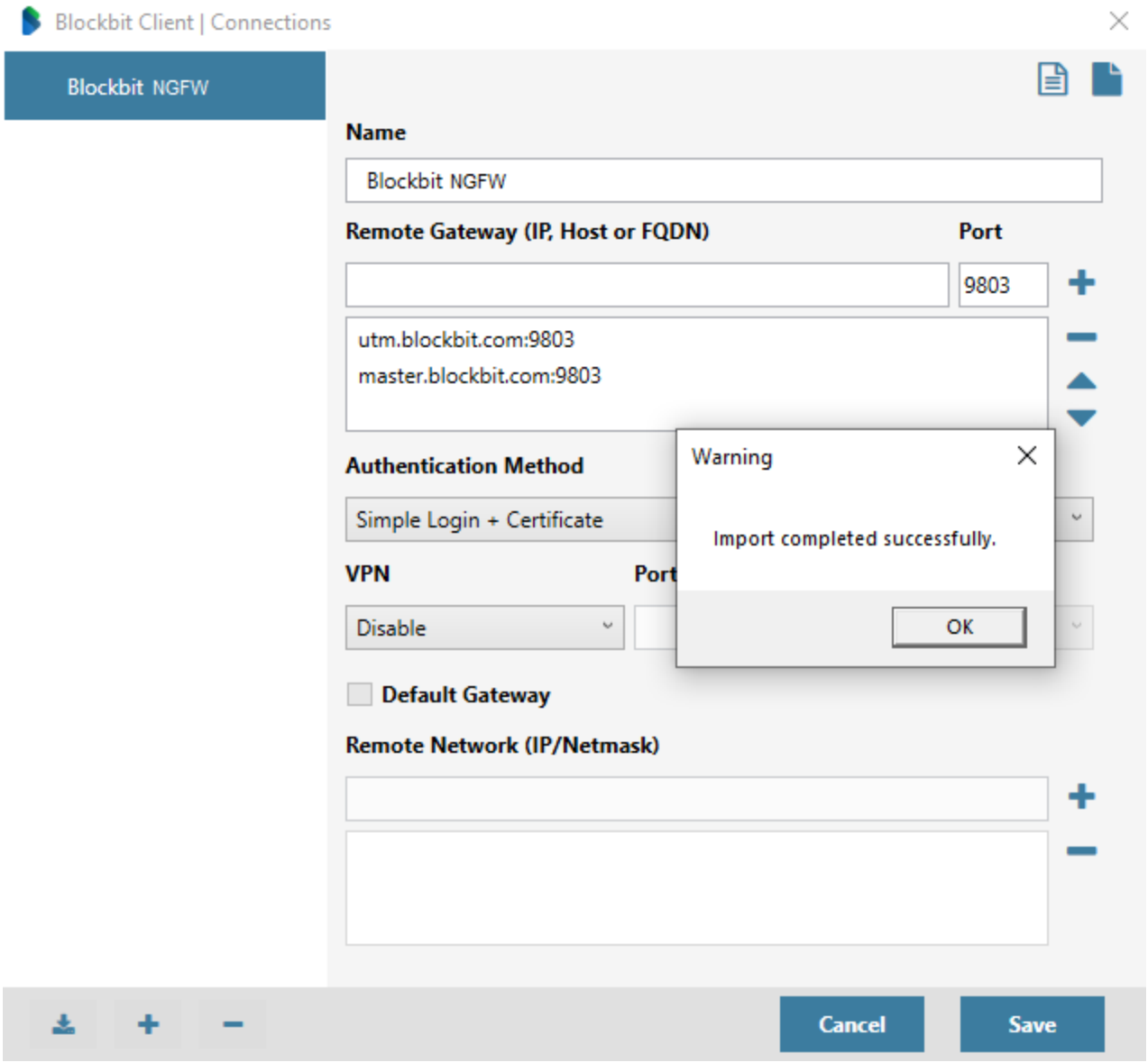
Profile Import

As we will do the demo on the same Blockbit Client, we will remove the "Test" profile to allow import. For more information on removing profiles, see this page.

Importing an XML file, containing certificates, either from CA or user (or both), will only be possible if the same certificates are installed on the machine performing the import, otherwise the error message "Invalid XML file" will be displayed.

To perform the import, click on the **[** **]** icon located in the lower left corner of the window and just select the XML profile to be imported.

If the XML was imported successfully, the message below will be displayed:

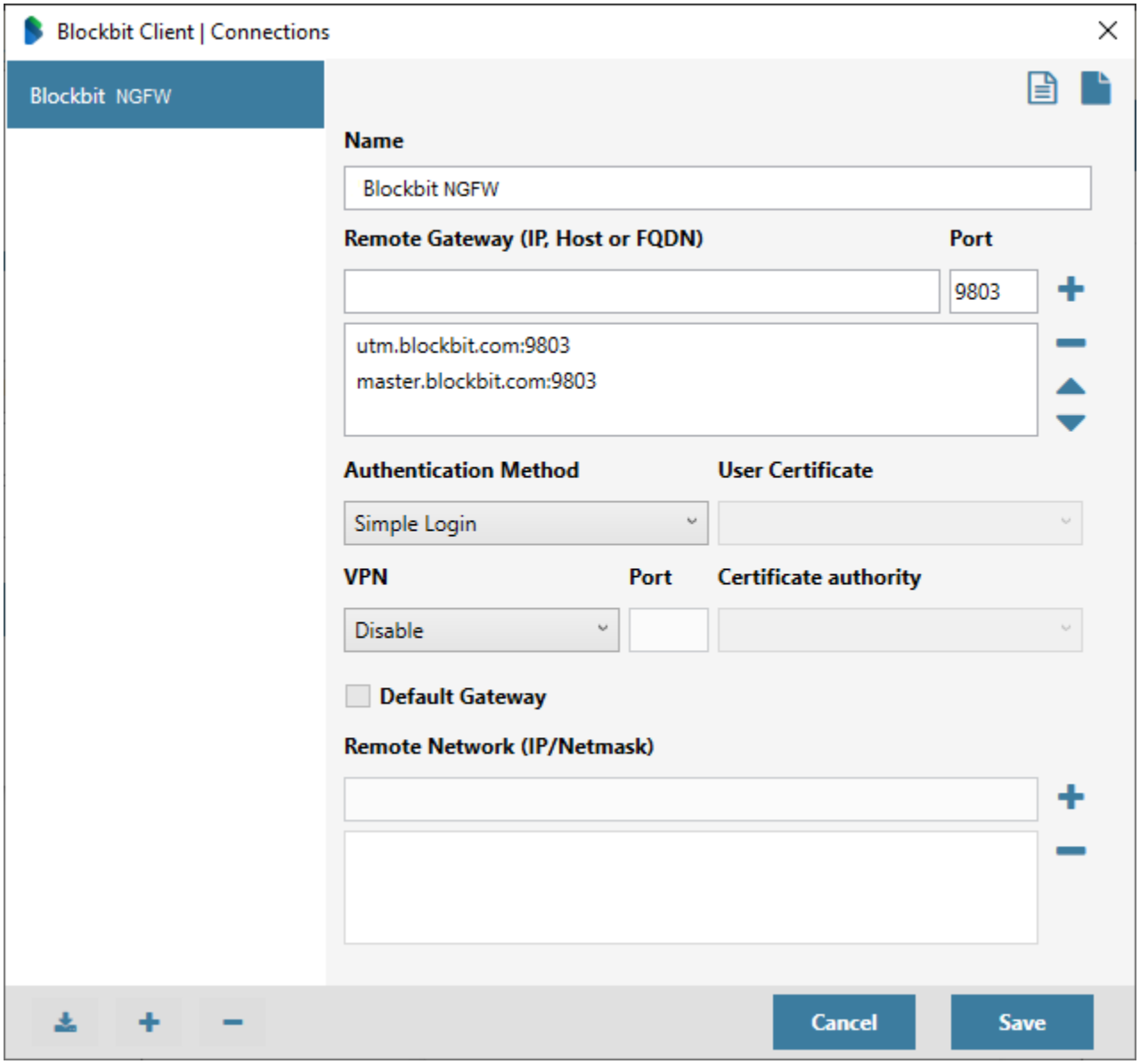


Blockbit Client - Connections - Import Completed Successfully

Next, we will analyze how to perform the Export of the connection log.

Exporting the connection log

To export a connection log, select the connection profile you want to export, as shown:



Blockbit Client - Connections - Export Log

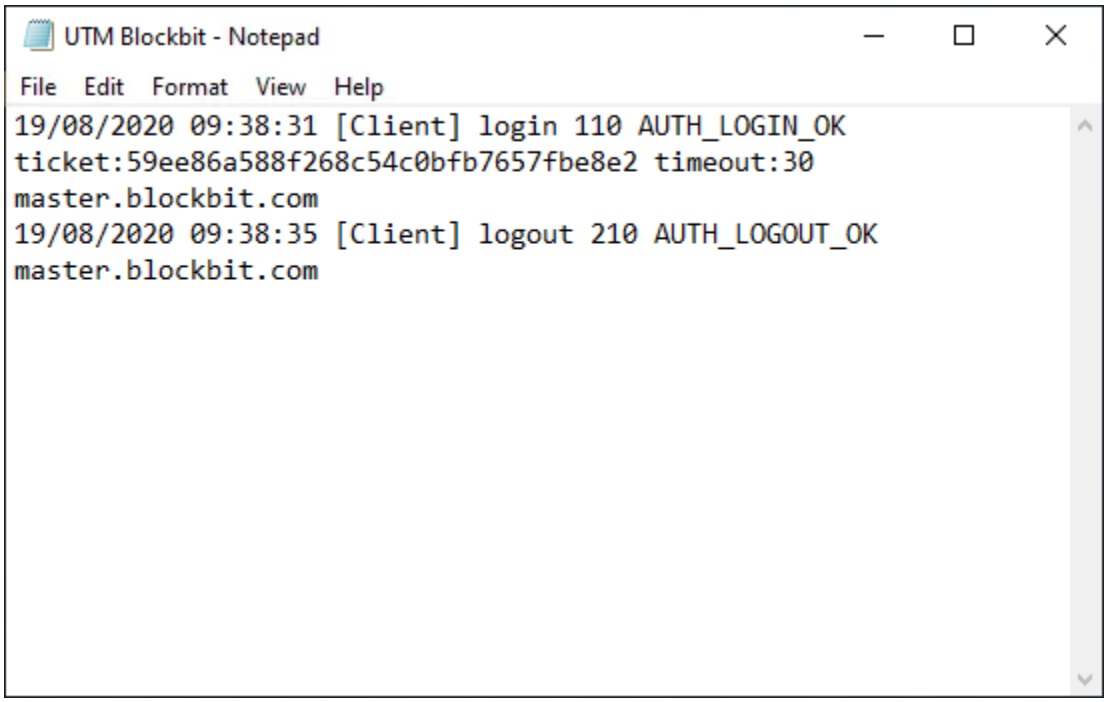
That done, click the **[**  **]** button located in the upper right corner and save the log in a safe place.

The log is a text file with information regarding the connection events of the selected profile, in case of connection failure with the gateway, a record is made in the log, however if the connection occurs normally, it will be recorded when the connection occurred, the connection status, login authentication event (successful) and etc.

In addition, every 30 seconds, the Client makes a keepalive by sending a request to the NGFW that was configured in the connection profile, in order to check: Authentication, data traffic and if the user remains authenticated. If the administrator drops the user's authentication or something happens to cause this connection to be interrupted, the keepalive will make 5 attempts to make sure the authentication is on the air. If it fails, the Client will drop the vpn. However, if nothing abnormal occurs, the keepalive will be executed again every 30 seconds.

ATTENTION: Only the Client saves the log only of the last connection that was made with the selected profile. This means that if more than one connection attempt is made, the log prior to the current connection will be overwritten.

Following is an example of Log:



Blockbit Client - Connections - Exported Log

In addition to this feature, the Blockbit Client also displays *Logs in the Windows Event Manager*.

Next, we'll look at how to make a Connection using Blockbit Client.

Configuration Examples

As a way to demonstrate the varied range of configuration possibilities in the Blockbit Client, in this session we will display various connection profiles of the Blockbit Client.

The types of connection profiles that will be shown are:

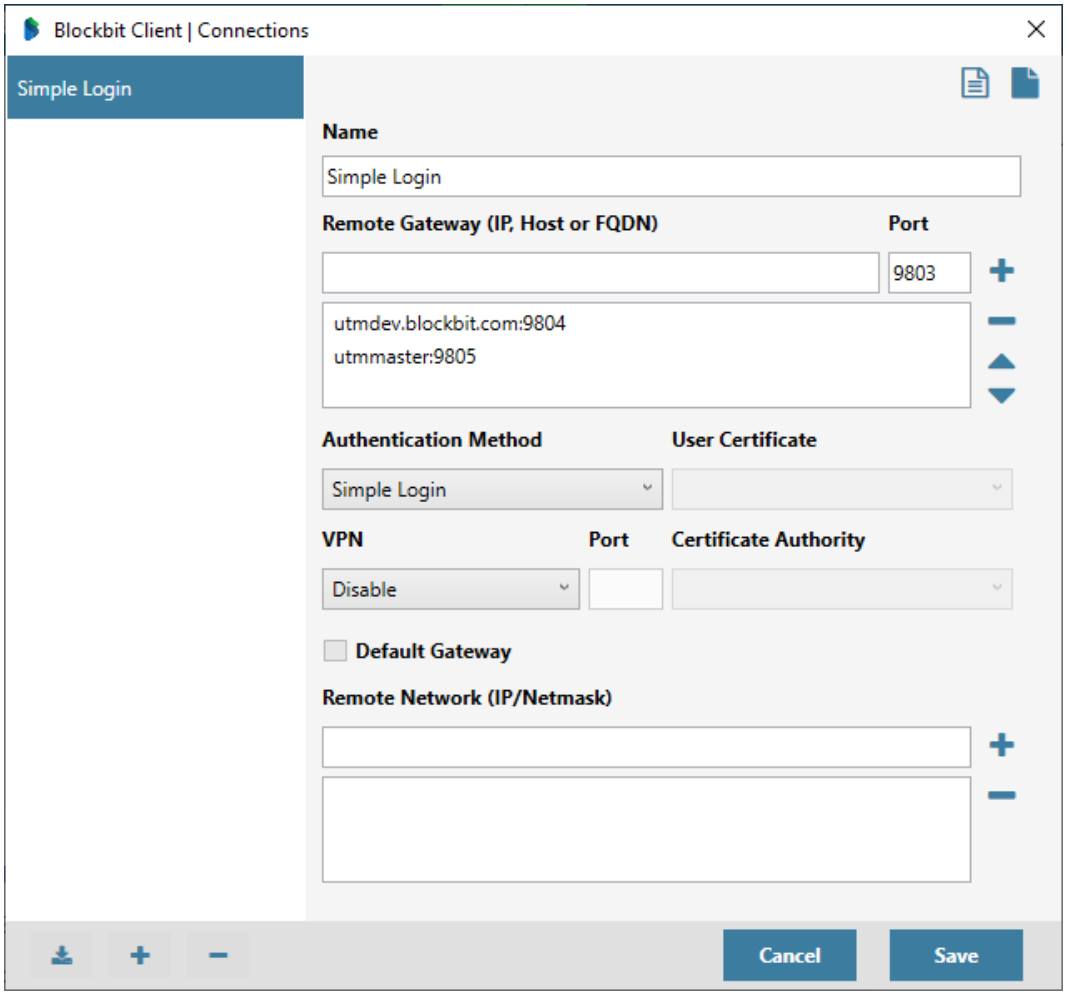
- *Simple Login*;
- Simple Login + Certificate;
- *Windows Login*;
- *Windows Login* + Certificate;
- Simple Login with SSL VPN;
- Simple Login + Certificate with SSL VPN;
- Simple Login + Certificate with SSL VPN and Remote Network;
- *Login* + Certificate *IPSEC Legacy*;
- *Login + Certificate IPSEC Legacy with Remote Network*.

For more information on adding profiles, see this page.

Simple Login

In the Simple Login authentication method, authentication is performed on the local machine (using the user configured in AD), unlike Windows Login, in this method the user must enter his login and password manually.

To configure a profile with Simple Login authentication method, complete the form as indicated below:



Blockbit Client - Login Simples

- ***Name*:** Enter the name that will be used in the profile. Ex.: Simple Login;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: utmmaster:9805 and utmdev.blockbit.com:9804;
- ***Authentication Method*:** In the authentication method, just select the option "Simple Login".

To finish, click [Save] otherwise, click [Cancel] to undo these settings.

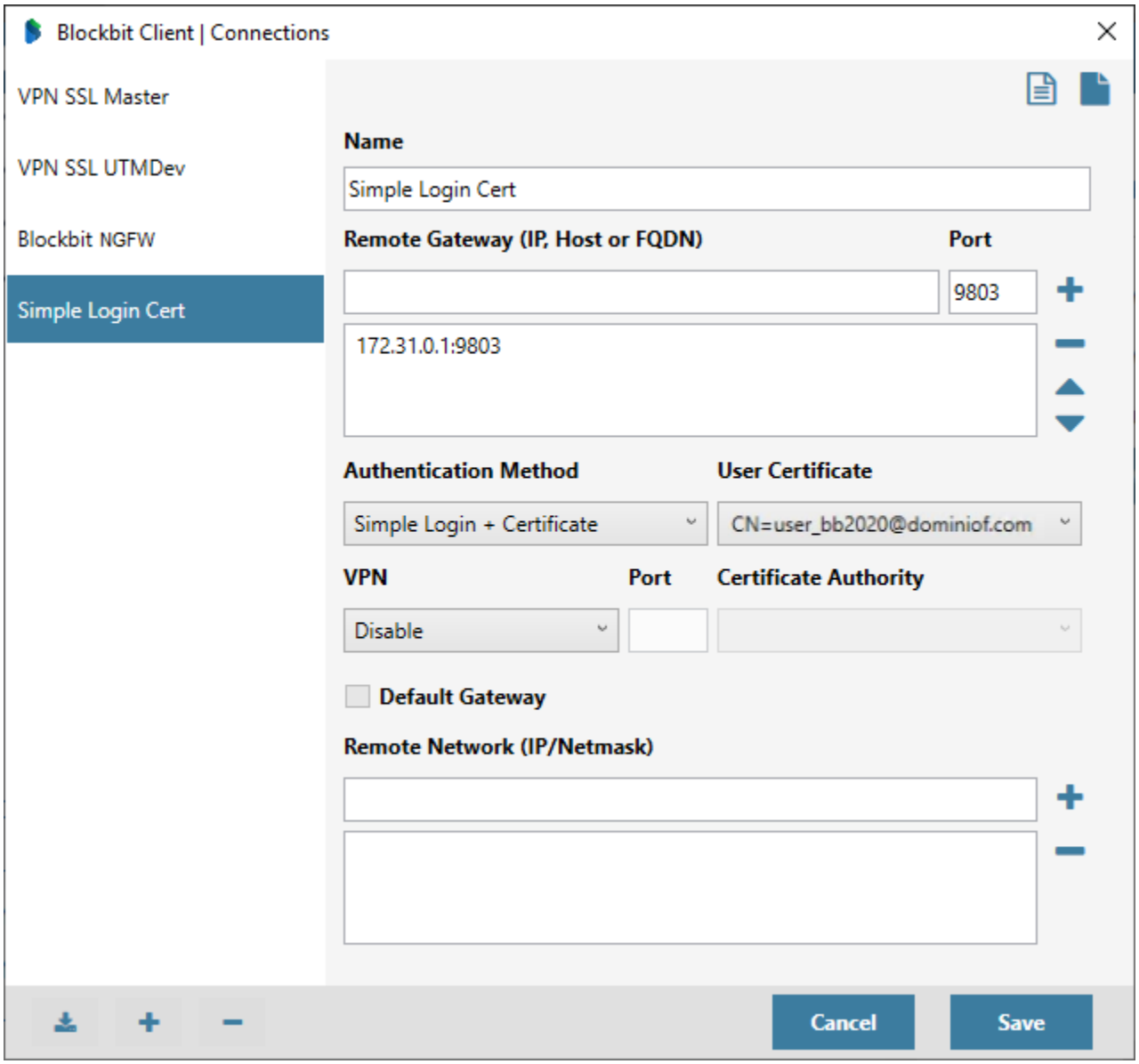
To view other configuration examples, see this page.

Simple Login + Certificate

The Simple Login + Certificate authentication method acts like the Windows Login method, but for the certificate to be displayed in the field, the user will need to log into the portal, generate his certificate and install it as Current User (not on the local machine).

In order for the NGFW to require the certificate on authentication, it is necessary to access the Settings menu, click on the Authentication option and on the Settings tab, select the Verify user certificate check box. After enabling this option, just give an Apply so that every time the Client tries to authenticate with the NGFW the certificate is required.

To configure a profile with Simple Login + Certificate authentication method, complete the form as indicated below:

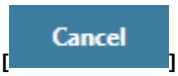


Blockbit Client - Simple Login + Certificate

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: Simple Login Cert;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Simple Login + Certificate";
- **User Certificate:** Select the certificate that the user will use in this connection profile.

To finish, click **[** 

] otherwise, click **[** 

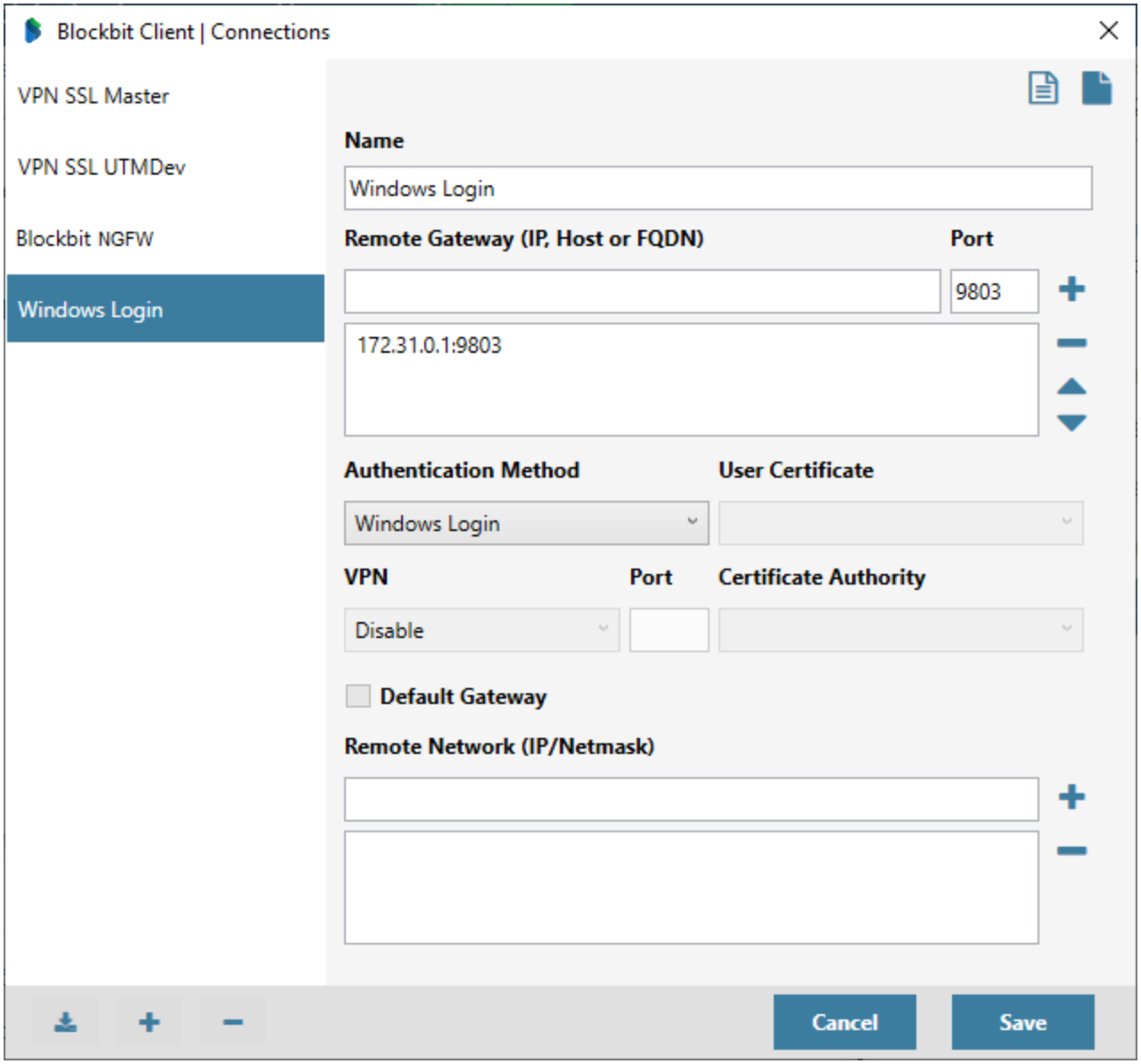
] to undo these settings.

To view other configuration examples, see this page.

Windows Login

In the Windows Login authentication method, authentication is performed on the local machine (using the user configured in AD), this authentication method does not require a password during login.

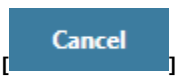
To configure, complete the form as indicated below:



Blockbit Client - Windows Login

- ***Name*:** Enter the name that will be used in the profile. Ex.: Windows Login;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Windows Login".

To finish, click **[** 

] otherwise, click **[** 

] to undo these settings.

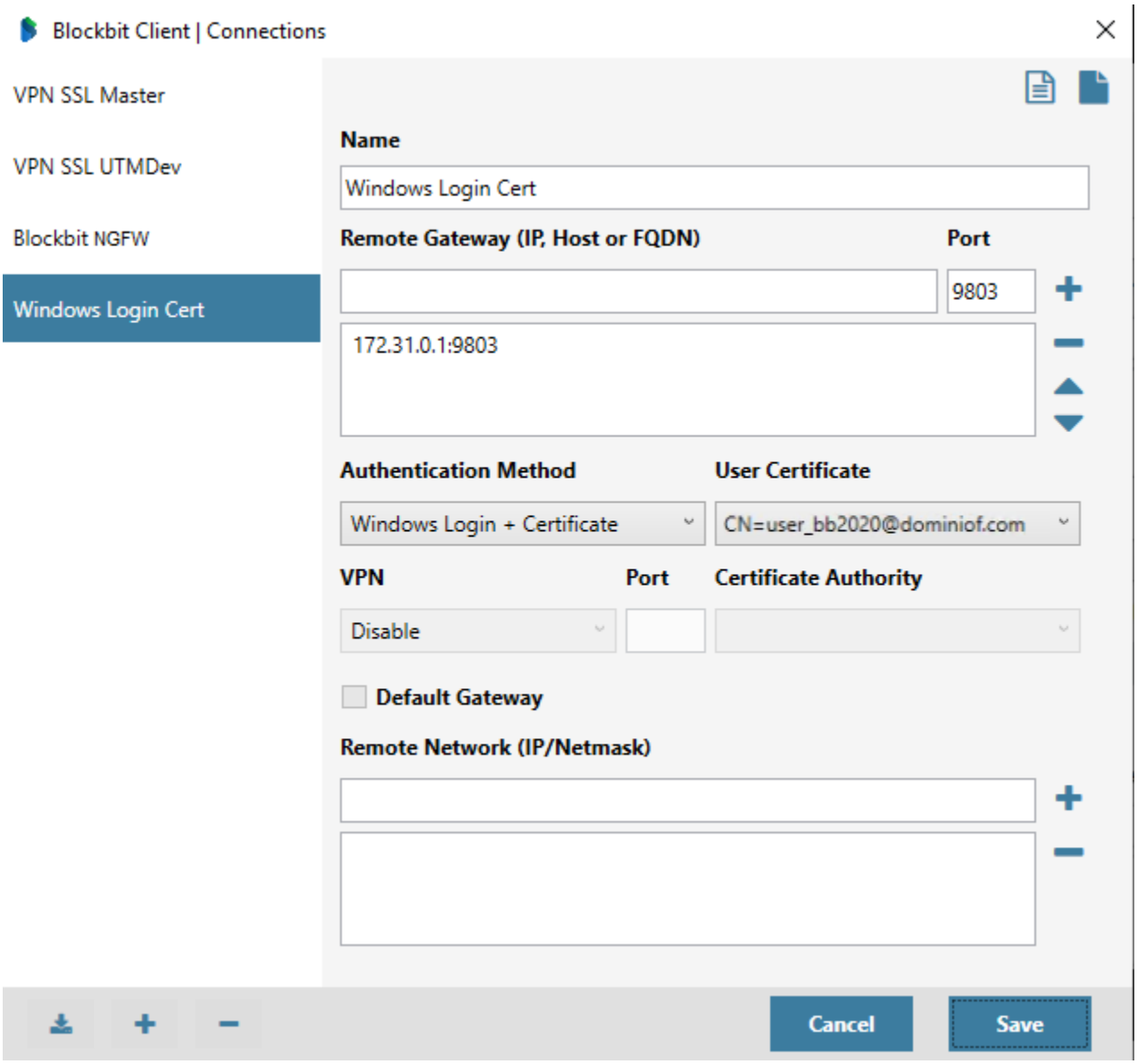
To view other configuration examples, see this page.

Windows Login + Certificate

The Windows Login + Certificate authentication method acts like the Windows Login method, but in order for the certificate to be displayed in the field, the user will need to enter the portal, generate his certificate and install it as Current User (not on the local machine).

In order for the NGFW to require the certificate on authentication, it is necessary to access the Settings menu, click on the Authentication option and on the Settings tab, select the Verify user certificate check box. After enabling this option, just give an Apply so that every time the Client tries to authenticate with the NGFW the certificate is required.

To configure a profile with Windows Login + Certificate authentication method, complete the form as indicated below:

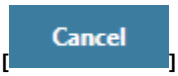


Blockbit Client - Windows Login + Certificate

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: Windows Login Cert;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Windows Login + Certificate";
- **User Certificate:** Select the certificate that the user will use in this connection profile.

To finish, click **[** 

] otherwise, click **[** 

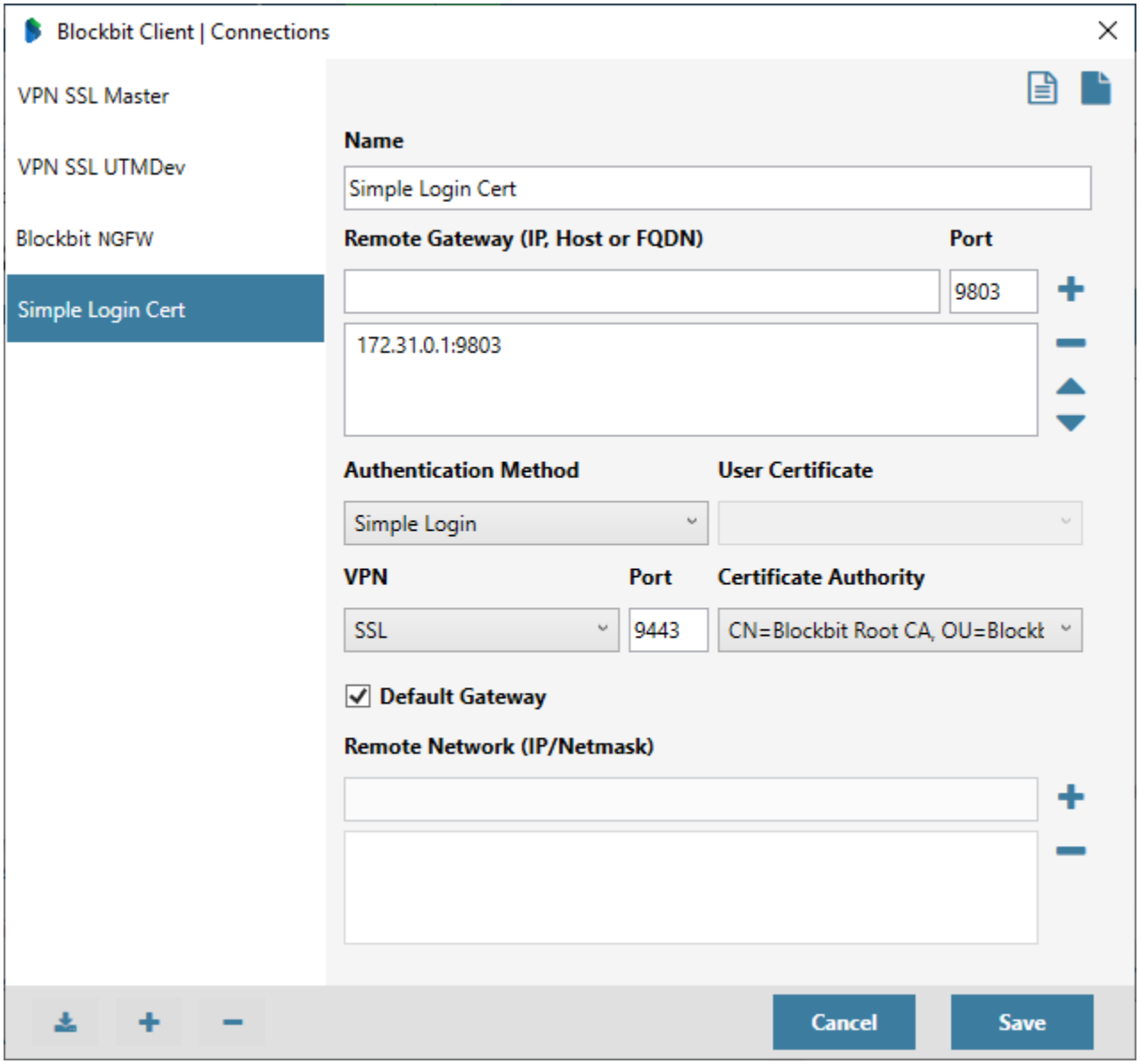
] to undo these settings.

To view other configuration examples, see this page.

Simple Login with SSL VPN

For more information on how Simple Login works, see this page. When using this authentication method, it is possible to configure the SSL VPN, the default port to be used is 9443 (which can be changed) and to use SSL it will be necessary to install the CA as a Trusted Authority, for more information, see this page.

To configure a profile with "Simple Login with SSL VPN" authentication method, complete the form as indicated below:



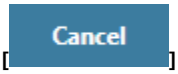
Blockbit Client - Simple Login with SSL VPN

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: Simple Login Cert;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Simple Login";
- ***VPN*:** Select the "SSL" option;
- ***Port*:** Add the port to be used. In this case we will use the standard port. Ex.: 9443;

- ***Certificate Authority*:** Select the CA to be used. It must be installed on the user's machine;
- ***Default Gateway* [☑]:** Enable this checkbox so that only 172.31.0.1:9803 is routed through the VPN.

To finish, click **[** 

] otherwise, click **[** 

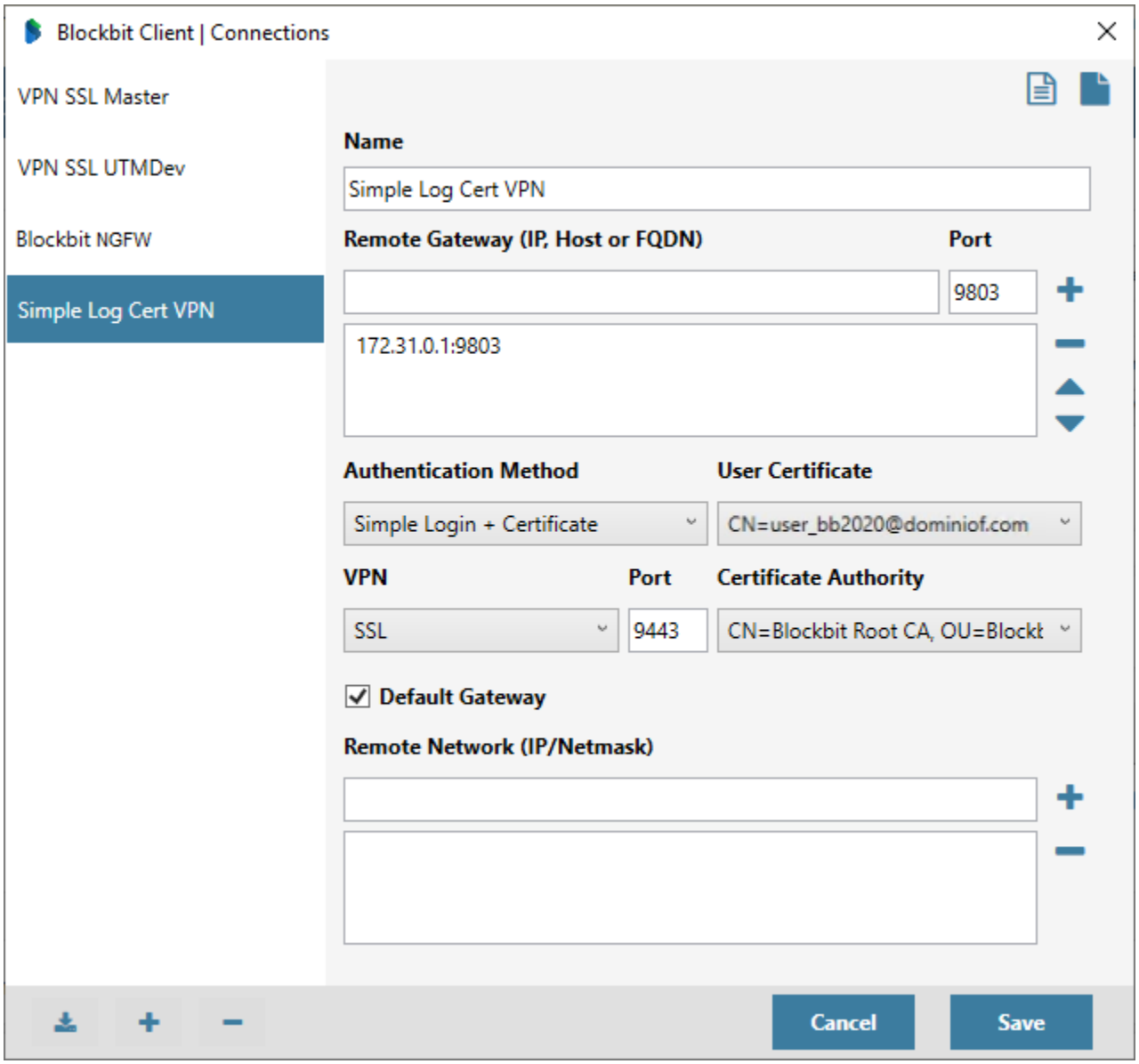
] to undo these settings.

To view other configuration examples, see this page.

Simple Login + Certificate with SSL VPN

For more information on how Simple Login with Certificate works, see this page. When using this authentication method, it is possible to configure the SSL VPN, the default port to be used is 9443 (which can be changed) and to use SSL it will be necessary to install the CA as a Trusted Authority, for more information, see this page.

To configure a profile with "Simple Login + Certificate with SSL VPN" authentication method, complete the form as indicated below:



Blockbit Client - Simple Login + Certificate with SSL VPN

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: Simple Log Cert VPN;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Simple Login + Certificate";
- **User Certificate:** Select the certificate that the user will use in this connection profile;
- ***Certificate Authority*:** Select the CA to be used. It must be installed on the user's machine;
- **VPN:** Select the "SSL" option;
- ***Port*:** Add the port to be used. In this case we will use the standard port. Ex.: 9443;

- **Default Gateway [☑]:** Enable this checkbox so that only 172.31.0.1:9803 is routed through the VPN.

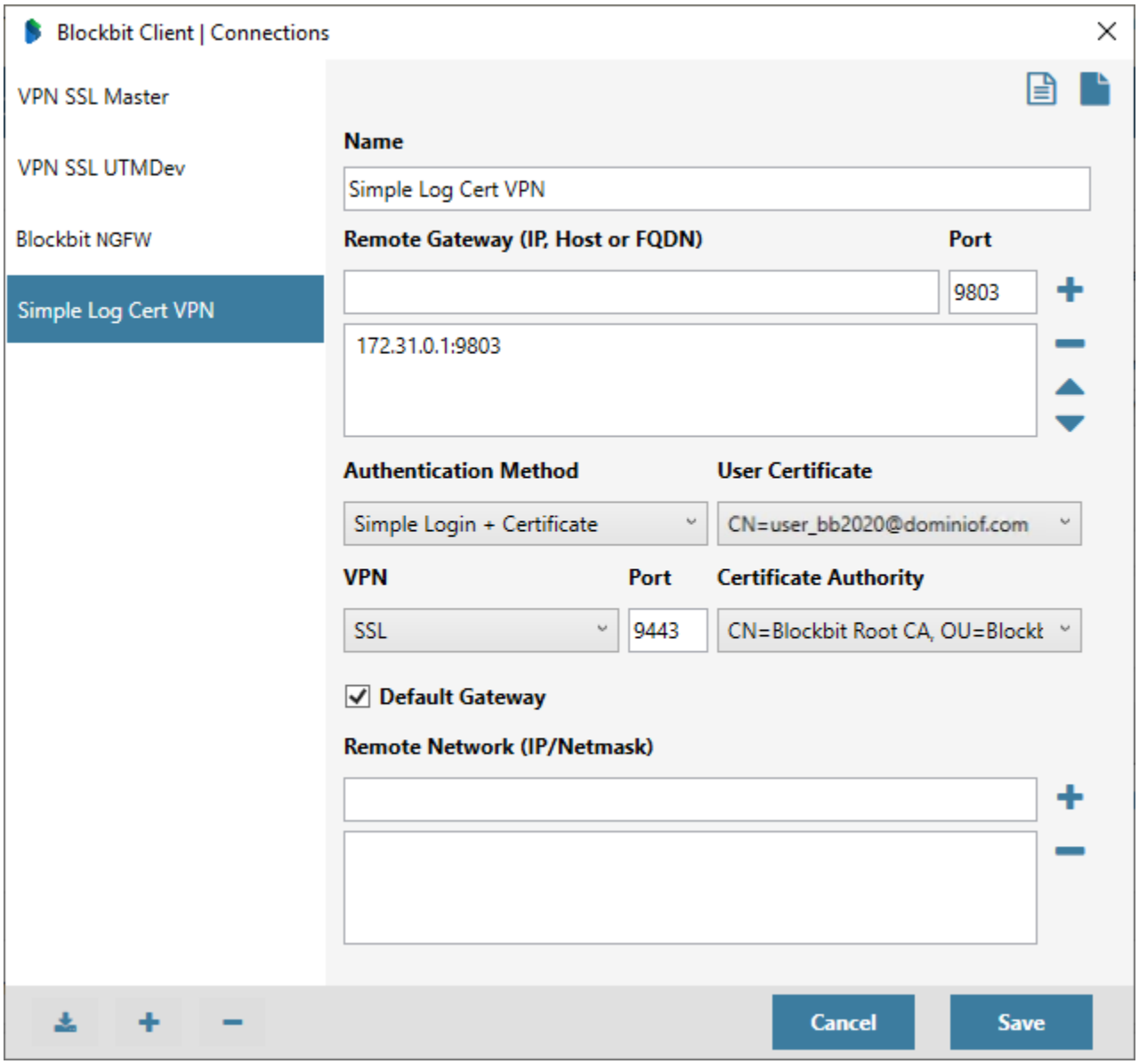
To finish, click **[Save]** otherwise, click **[Cancel]** to undo these settings.

To view other configuration examples, see this page.

Simple Login + Certificate with SSL VPN and Remote Network

For more information on how Simple Login with Certificate works, see this page. When using this authentication method, it is possible to configure the SSL VPN, the default port to be used is 9443 (which can be changed) and to use SSL it will be necessary to install the CA as a Trusted Authority, for more information, see this page.

To configure a profile with "Simple Login + Certificate with SSL VPN and Remote Network" authentication method, complete the form as indicated below:



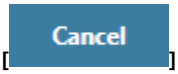
Blockbit Client - Simple Login + Certificate with SSL VPN and Remote Network

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: SimLogCertVPNRemote;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Simple Login + Certificate";
- **User Certificate:** Select the certificate that the user will use in this connection profile;
- ***Certificate Authority*:** Select the CA to be used. It must be installed on the user's machine;

- **VPN:** Select the "SSL" option;
- ***Port*:** Add the port to be used. In this case we will use the standard port. Ex.: 9443;
- **Remote Network:** Add the remote networks that will be used. Ex.: 192.168.149.0/25, 192.168.148.0/25 and 192.168.147.0/25.

To finish, click **[** 

] otherwise, click **[** 

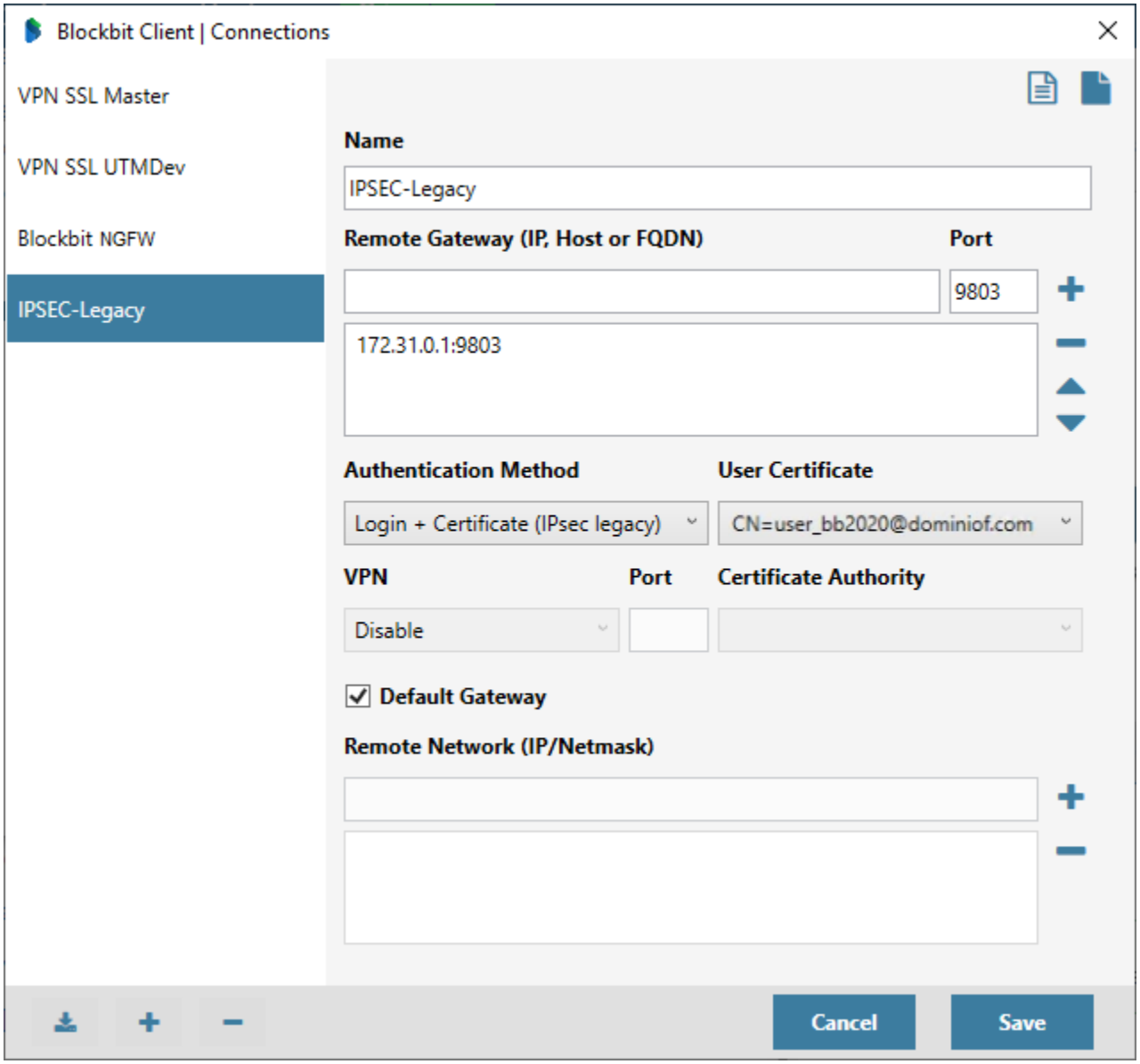
] to undo these settings.

To view other configuration examples, see this page.

Login + Certificate IPSEC Legacy

The authentication method Login with IPSEC Legacy Certificate basically performs the same process that was done in SSL, however for the certificate to be displayed in the field, the user will need to enter the portal, generate his CA and install it as a Local Machine (not as Current User)

To configure a profile with the "Login + IPSEC Legacy Certificate" authentication method, complete the form as indicated below:

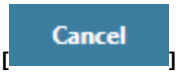


Blockbit Client - Login + Certificado IPSEC Legacy

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: IPSEC-Legacy;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Login + Certificate (IPSEC Legacy)";
- **User Certificate:** Select the certificate that the user will use in this connection profile.

To finish, click **[** 

] otherwise, click **[** 

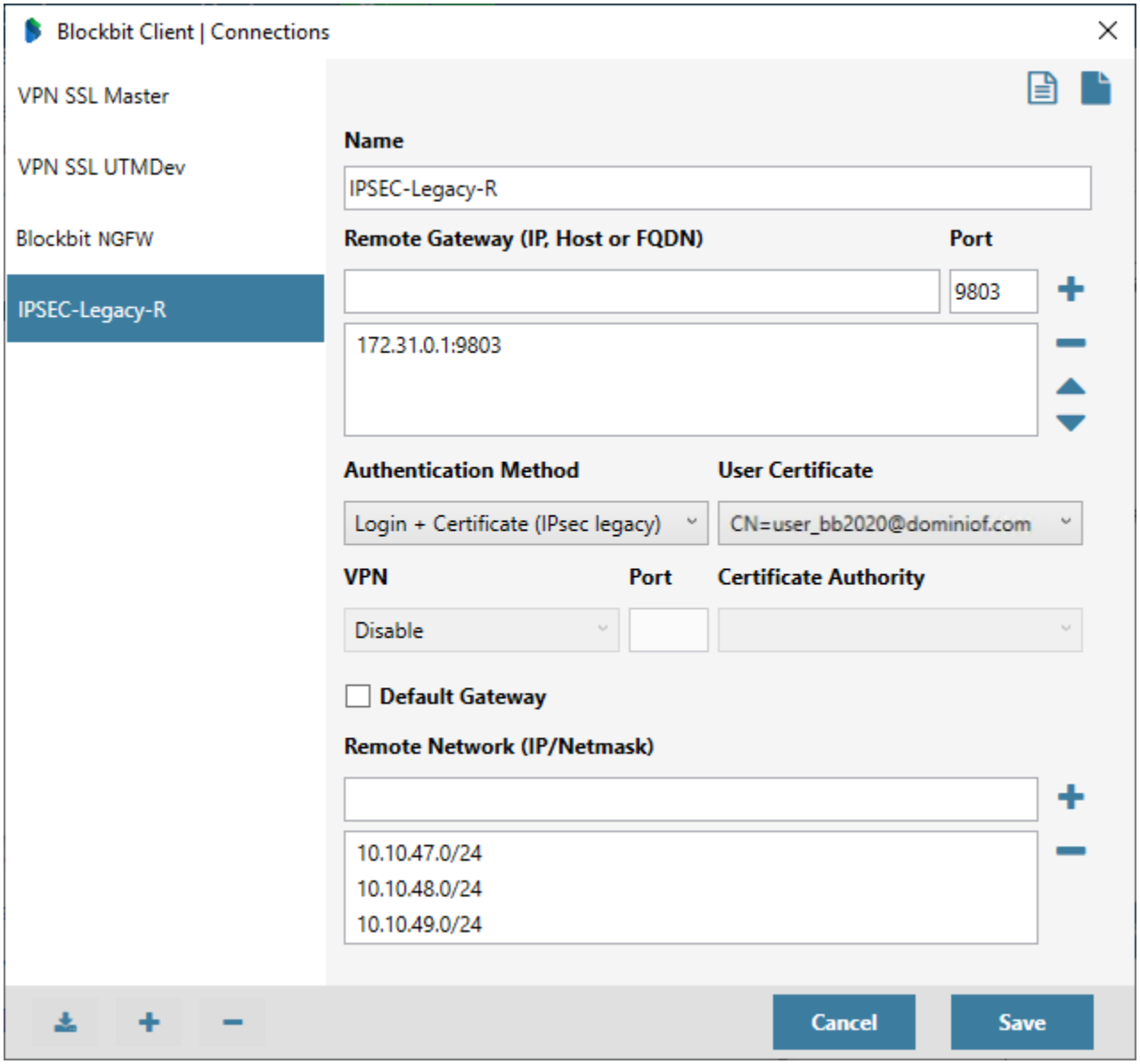
] to undo these settings.

To view other configuration examples, see this page.

Login + Certificate IPSEC Legacy with Remote Network

The authentication method Login with IPSEC Legacy Certificate basically performs the same process that was done in SSL, however for the certificate to be displayed in the field, the user will need to enter the portal, generate his CA and install it as a Local Machine (not as Current User).

To configure a profile with the "Login + IPSEC Legacy Certificate with Remote Network" authentication method, complete the form as shown below:

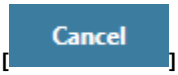


Blockbit Client - Login + IPSEC Legacy Certificate with Remote Network

For more information on how to install certificates, see this page.

- ***Name*:** Enter the name that will be used in the profile. Ex.: IPSEC-Legacy-R;
- ***Remote Gateway/Port*:** Add remote gateways and their ports. Ex.: 172.31.0.1:9803;
- ***Authentication Method*:** In the authentication method, just select the option "Login + Certificate (IPSEC Legacy)";
- **User Certificate:** Select the certificate that the user will use in this connection profile;
- **VPN:** Select the "IPSEC" option;
- **Remote Network:** Add the remote networks that will be used. Ex.: 10.10.49.0/32, 10.10.48.0/32 e 10.10.47.0/32.

To finish, click **[** 

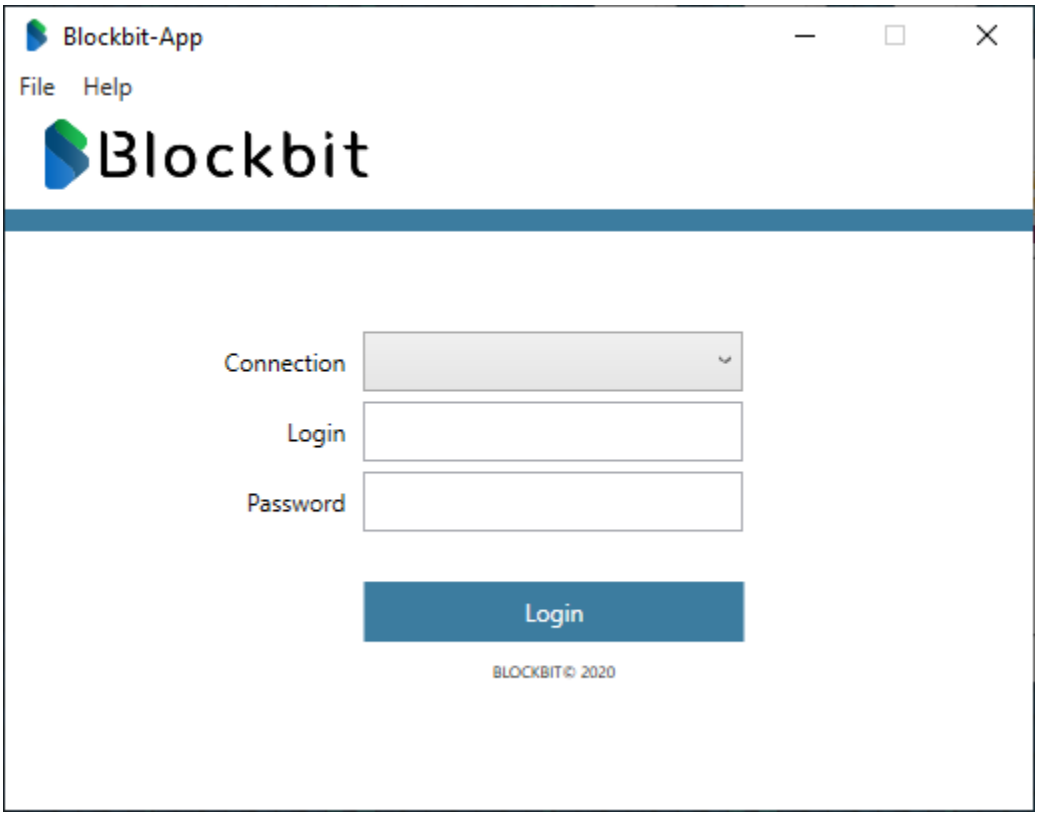
] otherwise, click **[** 

] to undo these settings.

To view other configuration examples, see this page.

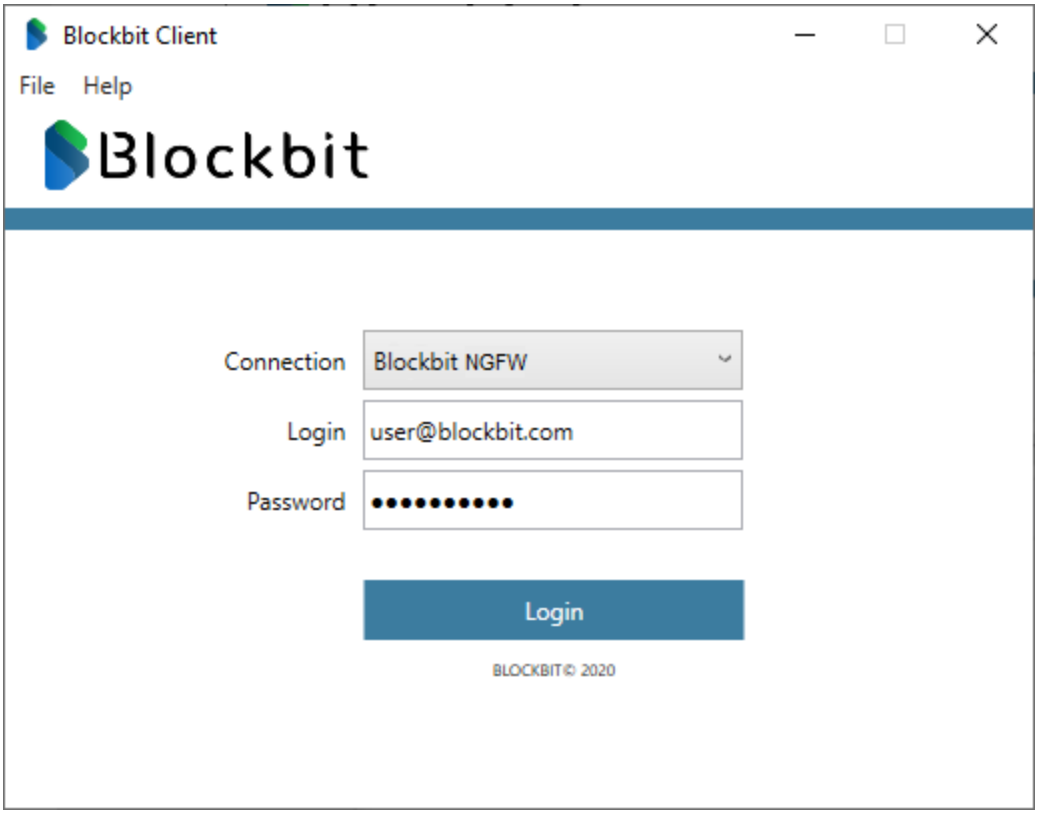
Connection using Blockbit Client

After creating and saving the connection profile, the user will be automatically redirected to the home screen, as shown below:



Login screen

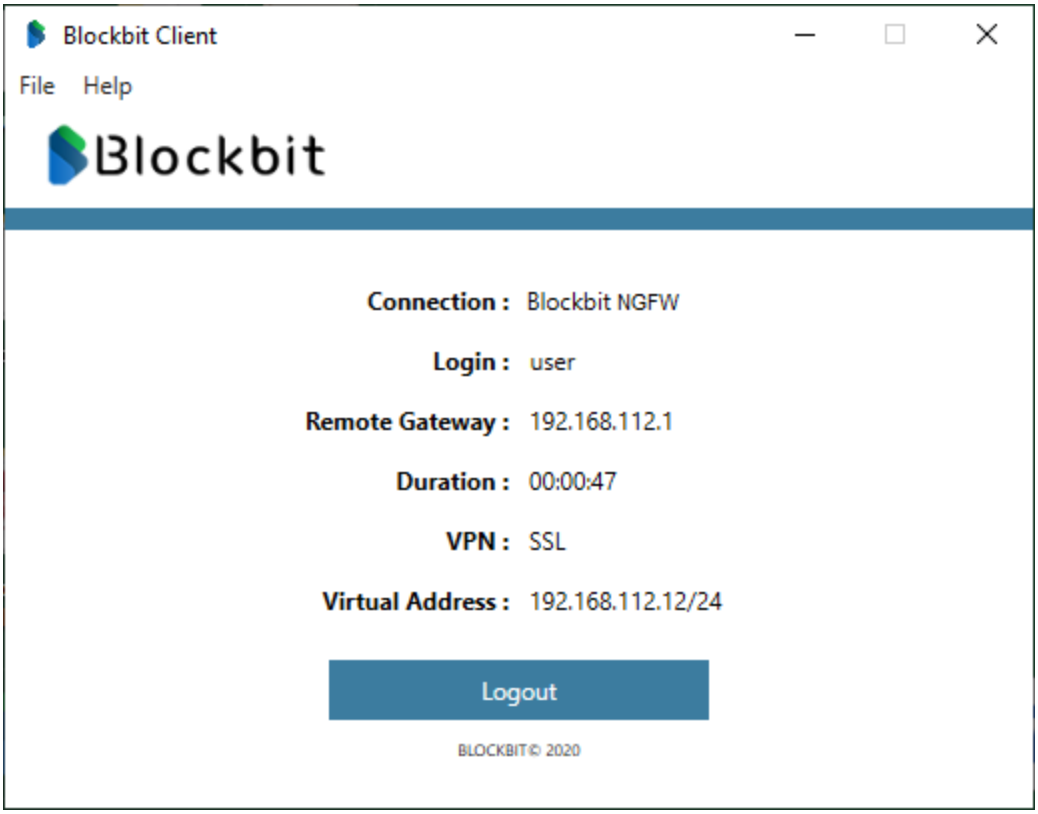
Complete the fields as shown:



Login Screen - Complete

- ***Connection*:** Select the desired connection profile. For example, the profile created in the previous session. Ex.: *Blockbit NGFW*;
- ***Login*:** Enter the login that will be used for the connection. Ex.: user@blockbit.com;
- ***Password*:** Enter the password that will be used in the connection. Ex.: q1Q!q1Q!.

To make the connection, click [Login], if the authentication was successful, the screen below will be displayed.

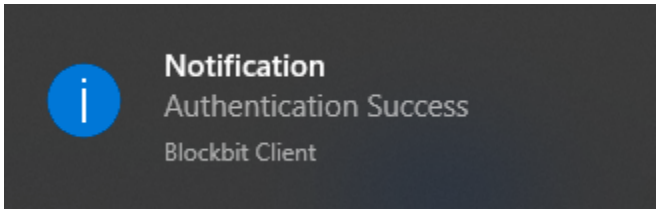


Blockbit Client - Connected

The information displayed on this screen is:

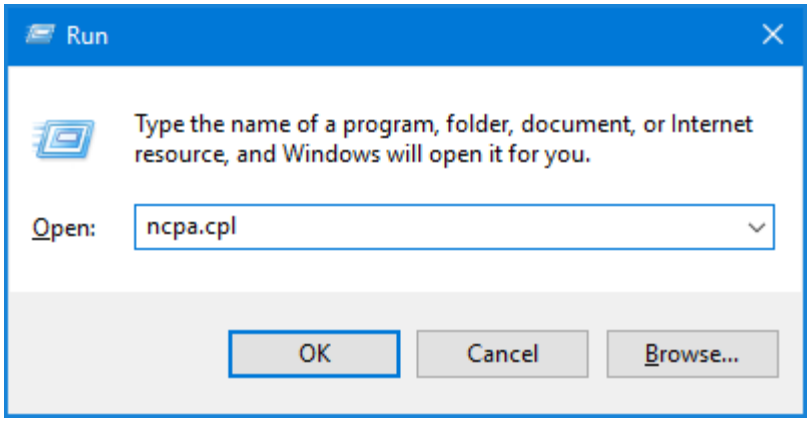
- ***Connection*****:** Displays the name of the connection profile;
- ***Login*****:** Displays which user is logged;
- ***Remote Gateway*****:** Displays the IP of the remote address that was used to make the connection;
- ***Duration*****:** Shows how long the user has been logged on;
- ***VPN*****:** Shows what type of VPN is being used;
- ***Virtual Address*****:** Displays the virtual IP that has been associated with the user on this connection.

In addition, a message confirming the connection will appear in the lower right corner of your screen.



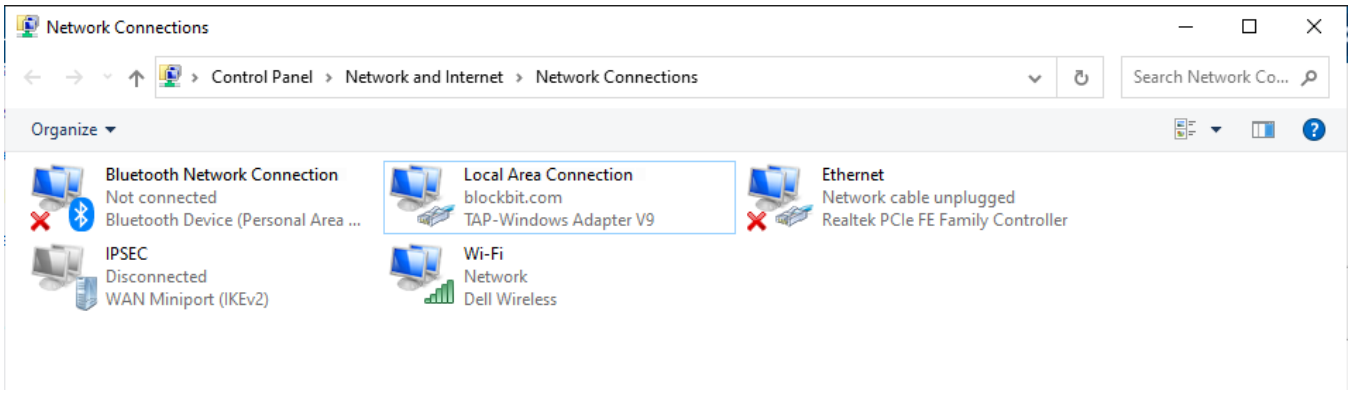
Connection confirmation message

During the installation process of the Blockbit Client the TAP interface is created, it is disabled in the background when there is no connection between VPN tunnels being activated at the time of connection. To view it, type the command ***Windows + R***, or select "Run" in your Start Menu, the window below will be displayed, in its text field, type "ncpa.cpl" and click **[** OK **]** (or "press Enter "):



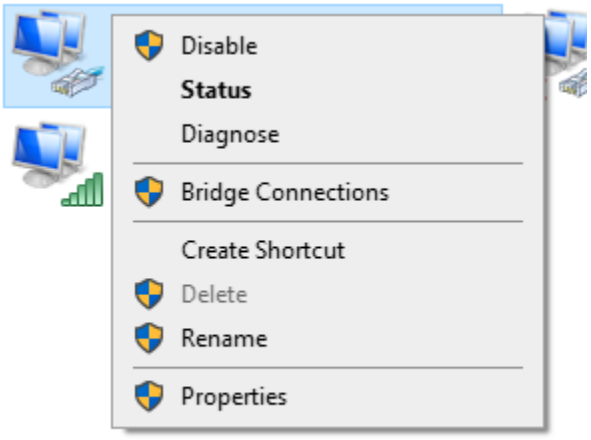
Run - control panel

The "Network Connections" window will be displayed, as shown below, it is possible to view the TAP interface:



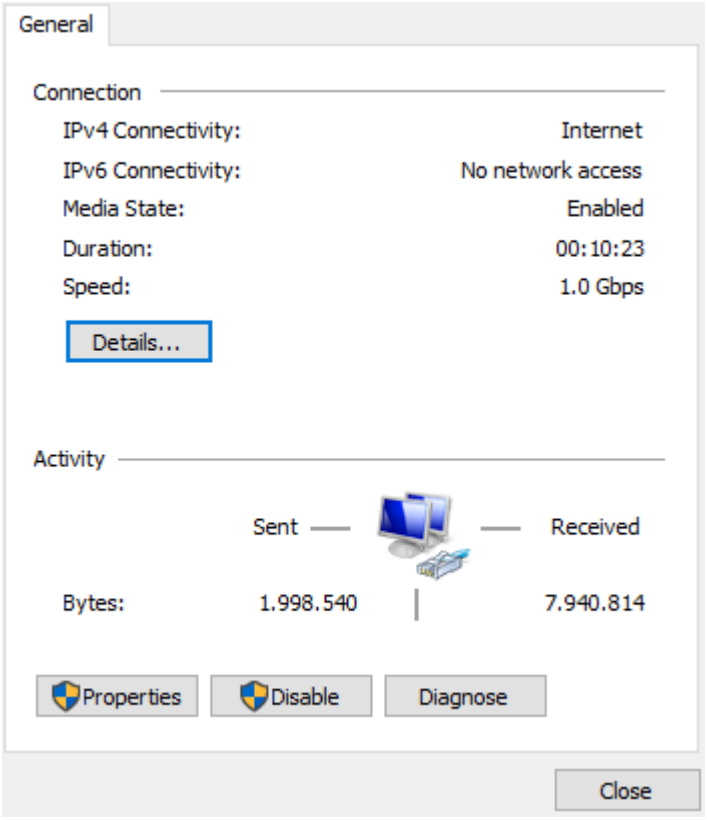
Network Connections

When a VPN is established, the interface is automatically activated, as shown above. The Blockbit Client uses this interface for communication between tunnels. For more information, click on Status, as shown below:

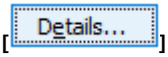


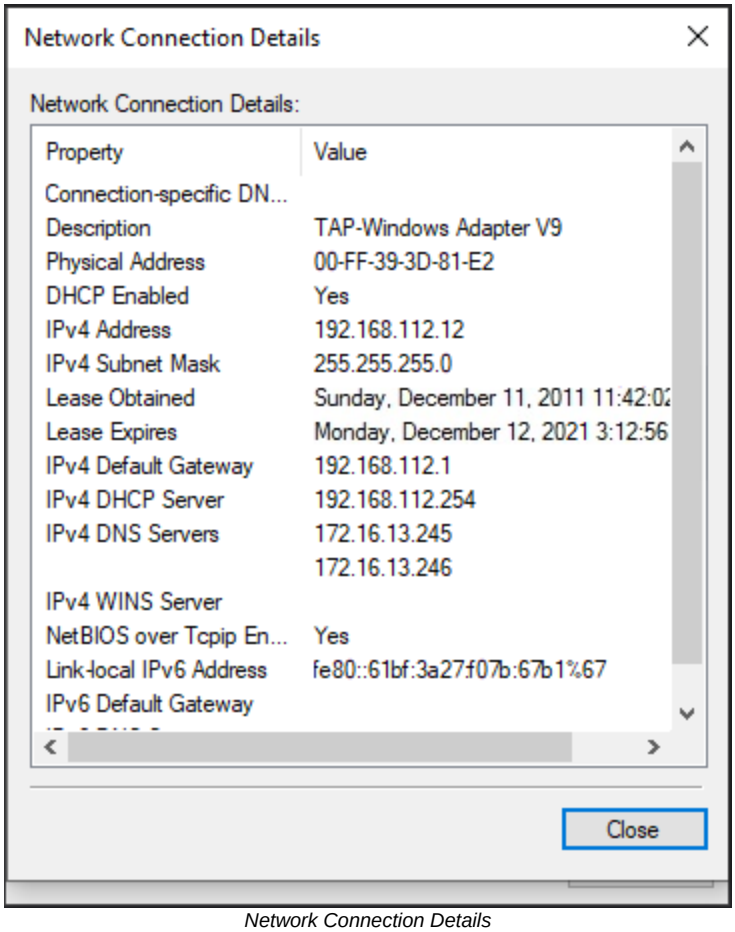
Local Area Connections - Status

The panel below will appear:



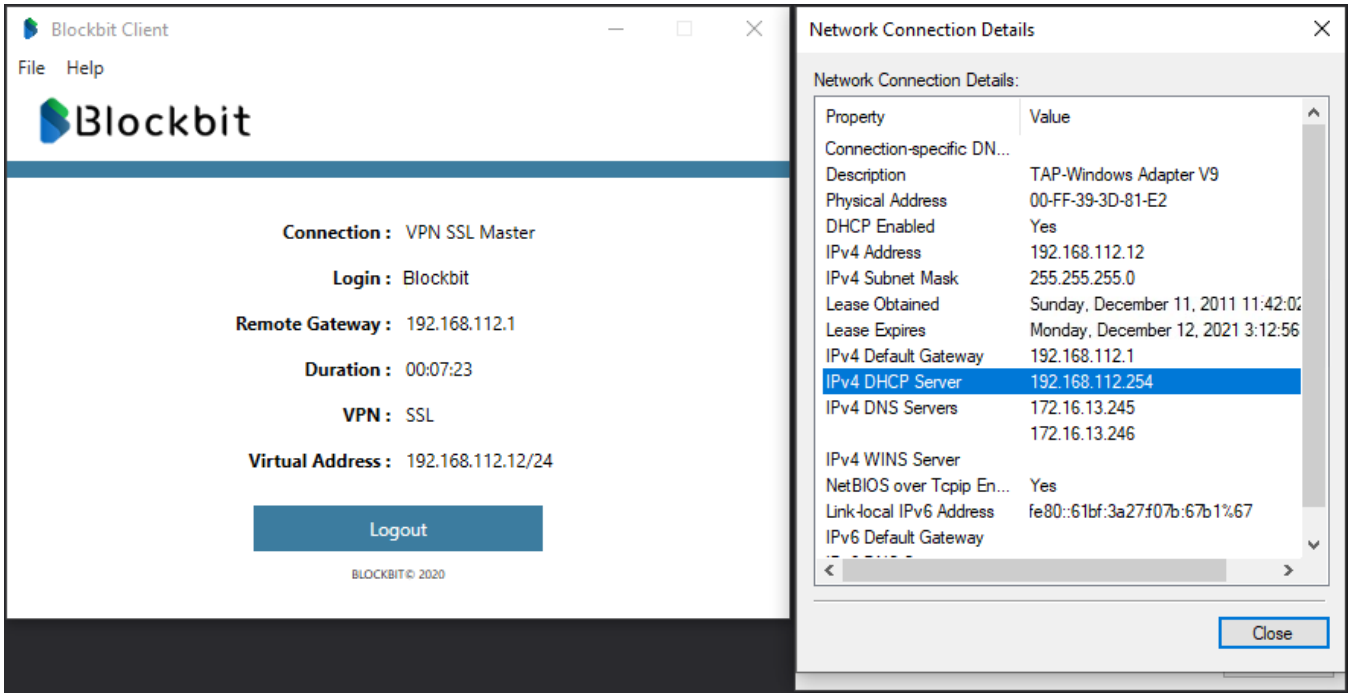
Local Area Connections

Click the **[**  **]** button, the connection details will be displayed:



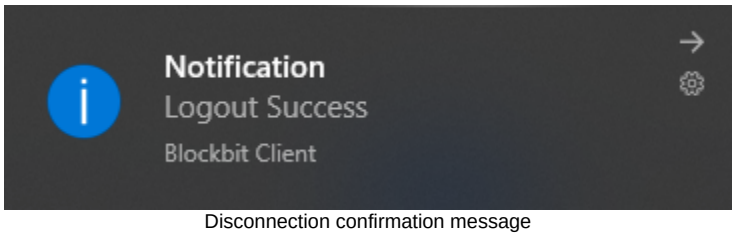
Network Connection Details

In the Network Connection Details window you can see some useful information about the connection, for example, the IP on the interface is the same as that associated with the virtual address:



Network Connection Details - Example

Finally, to disconnect, just click the **[** Logout **]** button.



Disconnection confirmation message

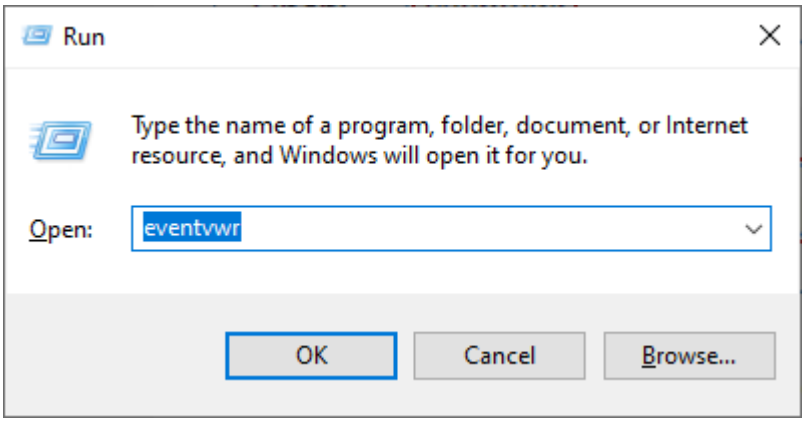
This completes the connection and disconnection using the Blockbit Client.

For more information on how to perform the configuration, see that page.

Logs in the Windows Event Manager

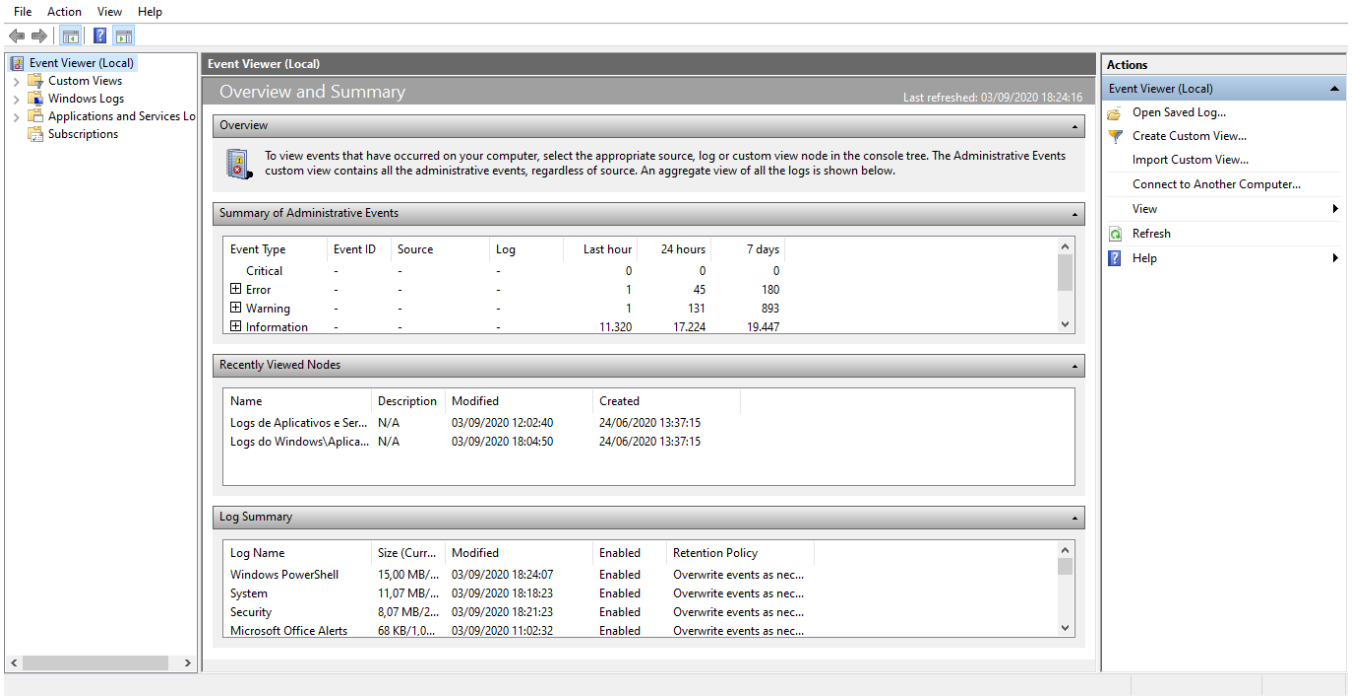
When installing the Blockbit Client, the **Blockbit_Log** is automatically added to the Windows Event Manager, recording data about the sessions and allowing the administrator to perform analysis or troubleshooting of the accesses.

To access Blockbit_Log, just follow the steps below, type the command ***Windows + R***, or select "Run" in your Start Menu, the window below will be displayed, in its text field, type "ncpa.cpl" and click on **[OK]** (Or "hit Enter"):



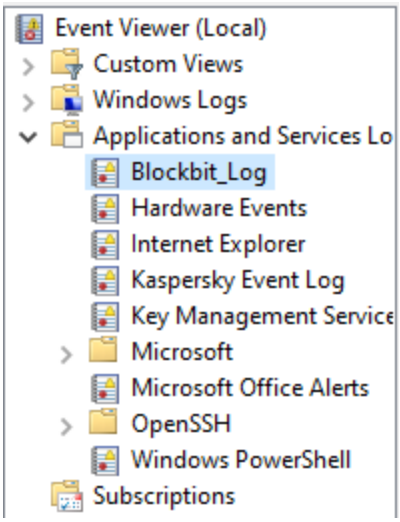
Run - Event Viewer

The Windows Event Manager window will appear, as shown below:



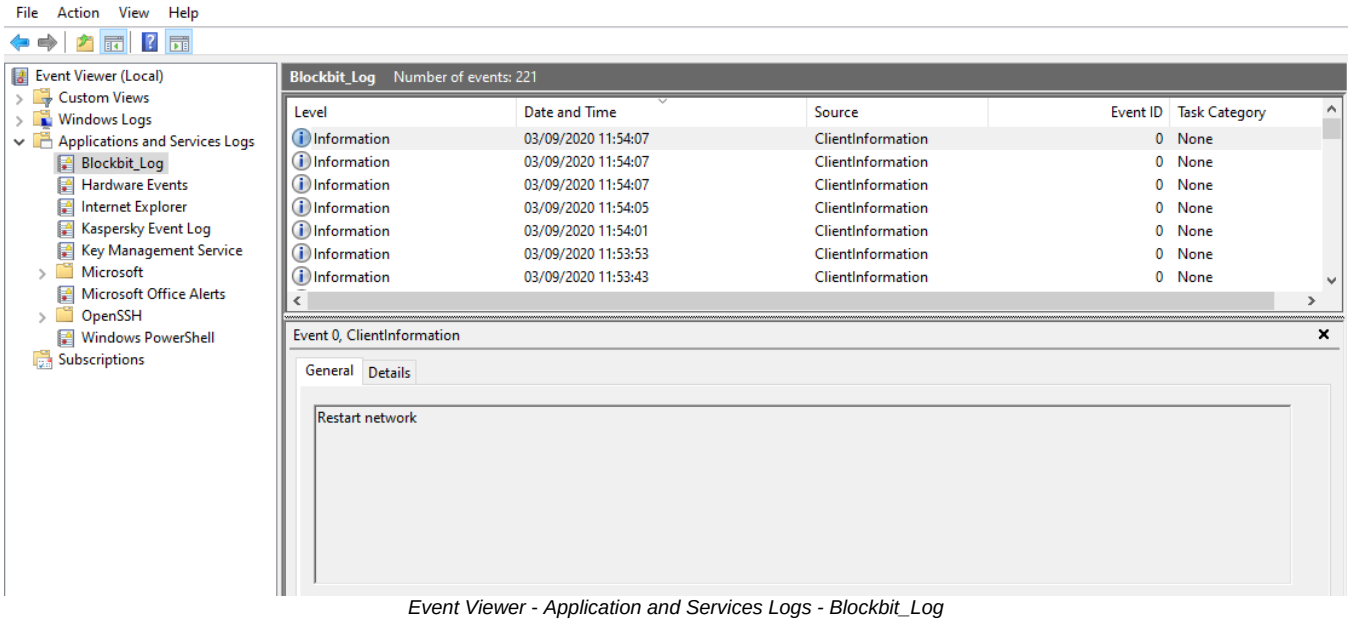
Event Viewer

On the left, expand **Application and Services Logs** and click **Blockbit_Log**:



Event Viewer - Application and Services Logs

When accessing **Blockbit_Log**, the administrator has access to all events registered by the system, as shown below:



Event Viewer - Application and Services Logs - Blockbit_Log

In addition to this feature, the Blockbit Client also has its own option to export connection logs, for more information see this page.

This concludes the configuration and installation of the Blockbit Client.

NGFW - Blockbit Client - Versions

Here you can find all the changelogs and installation files for the Blockbit Client.

Installation Files

Version	Compatible with the following versions of the NGFW:	CHECKSUM
Blockbit Client 1.2.4	1.5, 2.0, 2.1, 2.2, 2.3 and 2.4	e90053f040257711db69239e302bd709
Blockbit_Client_1.2.3	1.5, 2.0 and 2.1	6eca2927fd8c94e793b321114a1a5642
Blockbit Client 1.2.2	1.5, 2.0 and 2.1	530ab6bfc59e686f803839aea7f3dfe2
Blockbit Agent	1.5	b5a101541b8bd027b3f68f8a2321684f

Changelogs

Blockbit Client 1.2.4 Version

Blockbit Client 1.2.0 Version

Blockbit Client 1.2.0 Version

Code	Description
APP-208	Split Tunneling implemented to partially route VPN traffic
APP-209	Implemented the connection profile import functionality
APP-210	Implemented the VPN connection logs export functionality
APP-212	Implemented several improvements in the layout and basic functionalities of the application in order to improve usability
APP-213	Added secondary Gateway address registration
APP-214	Improvements applied to the Client connection flow
APP-215	Added functionality for automatic import of settings in the Installer
APP-226	Implementation of session keepalive service
APP-227	Implementation of the connection profile exporter

Blockbit Client 1.2.4 Version

Code	Description
EPS-269	Improvement done in the user’s certification.
EPS-272	Improvement done in the connection with the Windows’ TAP tunel.
EPS-277	Improvement done in the Client’s setup.
EPS-281	Improvement done in the Client’s startup.
EPS-285	Improvement done in the connection through the VPN SSL.

NGFW - REVISIONS' HISTORY

Document Version Control

DATE	DESCRIPTION OF THE CHANGES
17/06/2017	Release of the manual.
28/02/2018	3rd revision, correction and structural changes.
09/09/2018	Update to the NGFW 1.5 version.
08/10/2018	4th revision, correction.
31/10/2018	Update to the NGFW 1.5.2 version.
20/12/2018	5th revision, correction.
07/01/2019	Update to the NGFW 1.5.4 version.
22/03/2019	Migration of the NGFW's manual to the Confluence platform.
23/04/2019	Update to the NGFW 1.5.5 version.
10/03/2020	Update to the NGFW 2.0 version.
18/05/2020	Update to the NGFW 2.0.3 version.
22/06/2020	Update to the NGFW 2.0.4 version.
04/09/2020	Update to the NGFW 2.0.5 version.
04/11/2020	Update to the NGFW 2.0.6 version.
14/12/2020	Update to the NGFW 2.0.7 version.
25/03/2021	Update to the NGFW 2.0.8 version.
17/05/2021	Update to the NGFW 2.0.9 version.
23/08/2021	Update to the NGFW 2.0.10 version.
24/08/2021	Update to the NGFW 2.0.11 version.
30/05/2022	Update to the NGFW 2.0.12 version.
02/08/2022	Update to the NGFW 2.0.13 version.
25/03/2021	Update to the NGFW 2.1.0 version.
23/08/2021	Update to the NGFW 2.1.1 version.
22/09/2021	Update to the NGFW 2.2.0 version.
30/05/2022	Update to the NGFW 2.2.1 version.
02/08/2022	Update to the NGFW 2.2.2 version.
31/10/2022	Update to the NGFW 2.3.0 version.
27/02/2023	The (NGFW) 2.4.0 version has been released.

UTM - INTRODUCTION

Thank you for choosing Blockbit NGFW.

This Administrator's Guide aims at assisting you and your company in the process of installation, configuring and using the Blockbit NGFW. At the end of this Guide, you will be able to use all the functionalities and resources necessary for its operation.

The Blockbit NGFW is a state-of-the-art multifunctional cybersecurity product that includes the main features for network security: As a Next Generation Firewall (NGFW), Authentication, Antimalware, IPS (Intrusion Prevention System), IPSec VPN, SSL VPN, Secure Web Gateway, ATP (Advanced Threat Protection), Dashboard, Reporting and more.

All of the Blockbit NGFW's services are managed through a single console, centered on a single interface.

Operating in all layers of the OSI model (Open Systems Interconnection), with advanced security features and having all its management done through an easy to navigate web interface, the Blockbit NGFW offers all the protection you need, centralized in a single device.

As main differentials, we have:

- **Advanced Threat Protection:** Innovative security, including real-time detection and protection against malware, malicious callbacks and even unknown attacks;
- **Advanced Application Control:** Easily manage access to services and applications, thanks to the function of assigning "names" instead of "addresses or ports", management is streamlined, which improves security and reduces the need for knowledge of protocols;
- **Antivirus and AntiMalware:** Count on advanced features, such as integrated Antivirus and AntiMalware, to prevent the execution of unauthorized and potentially dangerous applications. Scan password-protected files and scan traffic using HTTP / HTTPS protocols to stop malicious downloads;
- ***Timeline*:** Being visible only by administrators and managers, the Timeline allows the monitoring of the history of accesses, threats detected and applications running in an exclusive timeline;
- **Flexible Bandwidth Control:** Manage the bandwidth of connections according to their respective priorities, being able to define access speeds for users, groups, web categories, types of service and more;
- **Unified Policy Panel:** Defining compliance policies and access levels can be created and applied by groups in a simple and innovative way, reducing configuration errors and security breaches caused by simplifying user rules, user groups, services and running applications;
- **Link Balancing by Policy:** Manage multiple links in a revolutionary way, assign data connections according to each security policy, have greater flexibility in determining: Connections by network addresses, connection content, web categories, applications, users, user groups and more;
- **Remote Access without Client Application:** Using technology natively compatible with Windows, iOS and Android systems, the Blockbit NGFW allows your users to securely connect to your network, without the need to install any additional software.

UTM - Features

- **Next Generation Firewall:** By increasing the protection capacity against attacks, Blockbit goes beyond the traditional firewall, uniting the best in network security in a single solution. Blockbit NGFW's Next Generation Firewall simplifies the creation of complex policies and rules using addresses, users, groups, applications, threats and services presented as unified named objects, which makes it easier to understand policies while maintaining maximum control;
- ***VPN SSL*:** From any workstation, using only a browser, it is possible to access a Web portal that offers access to internal applications, configured in an easy and intuitive way with maximum security and privacy;
- ***QoS*:** Providing prioritization and bandwidth control in compliance policies quickly and efficiently, this advanced QoS feature allows you to categorize traffic based on its importance, also enabling the prioritization of packets using DSCP and TOS protocols;
- ***VPN IPSEC*:** Our VPN has a robust IPSec implementation, a standard that guarantees interoperability with other products on the market and goes further, offering even more encryption and security options;
- **SSL Inspection:** Currently, a large part of the web traffic is made through encrypted connections, Blockbit NGFW, allows you to inspect the encrypted content of your choice through compliance policies, allowing full control over access and use of all protection features: How Advanced Protection Against Threats and Content Filtering;
- **High Availability:** Blockbit products support high availability (High Availability) with the ability to maintain an appliance in backup mode, allowing it to go into operation quickly in the event of a failure with the primary appliance. It transparently maintains Firewall and User Authentication sessions, minimizing downtime as much as possible;
- **Cloud application control:** With the advancement of the Internet, applications such as Facebook, Youtube, Google, Twitter, LinkedIn, Dropbox and others have become very popular. Blockbit NGFW allows full control over access to cloud control applications, allowing your employees to stay focused on what is needed for productivity, without distractions;
- **Content Filtering:** Having more than 40 million addresses classified in more than 80 categories and still counting on signatures of web browsers, our content filter works in conjunction with SSL Inspection, enabling complete control over any type of content that can be accessed. It is possible to monitor access through the simplified creation of compliance policies, specifying users, groups, IPs, bandwidth and priority usage, links, browser and version, size of downloads, web applications, time limit and much more;
- **Centralized Management Support:** With integration with Blockbit GSM (Global Security Management) it is possible to manage multiple devices through a single central point;
- **Other resources:**
  - *IPv6*;
  - Captive portal with Social authentication (Facebook, Twitter, Google);
  - Advanced and Dynamic Routing;
    - *BGPv4+*;
    - *OSPFv2* e v3;
    - *RIPv1*, v2 e *RIPng*;
    - *IGMP*;
    - Multicast routing (PIM-SM).
  - *VLAN*;
  - *Dynamic DNS*;
  - Active Directory / LDAP integration;
  - *SNMP*;
  - *DHCP Server*;
  - *Proxy*:
    - Email filtering (*POP3*/S e *SMTP*/S);
    - *HTTP* and *HTTPS*;
    - *FTP*.
  - *Link Aggregation – Ethernet Bonding* (802.3ad);
  - Among others…

UTM - Environment check for installation

This guide provides information on how to configure and manage Blockbit NGFW, before proceeding, check the installation requirements. Remember that we offer full support through our service channels, who will be more than happy to help you.

Installation requirements

Make sure internet communication is active, licensing processes, system updates and databases require internet connection.

Minimum installation requirements:

- Processing: 2 x Cores x86_x64;
- Memory: 4GB RAM;
- Storage: 32GB.

 The above requirements support up to 50 users, for up to 15 users the recommended is: 4 x Colors x86_x64, 4 GB of RAM and 32 GB of disk. For more users, please consult a **Blockbit Reseller** or one of our experts.

Virtualization platform: VMware, XenServer, KVM and ProxMox.

Public cloud platforms: AWS, Azure, Oracle, Google and IBM.

To proceed with the installation and configuration you need an SSH client, serial console and a web browser. Below is a list of recommended minimum applications:

Web browser:

- *Mozilla Firefox* version 45;
- *Google Chrome* version 51.

Remote access (*SSH* and Console):

- *PUTTY*;
- *CygWin*;
- *MobaXterm*.

UTM - About the Administrator's Guide

This guide was developed especially for you administrator, all sections have been structured in order to make the installation process quick and easy. The entire step-by-step is presented with examples, facilitating understanding and clarifying doubts.

Throughout the guide, you can find some symbols followed by text, they are intended to alert you to an important note or note regarding that section.

Let's get to know these symbols:

- **Alert:** Refers to notes or notes that you should follow very carefully during the installation process of the Blockbit NGFW:

 Example of an Alert message.

Alert Symbol

- **CLI - Command Line Interface**: Also known as Shell, it refers to the commands that must be typed, next to this symbol the command to be typed will be arranged:

Command Line
`Command line example.`

Symbol – *CLI – Command Line Interface*

- **Tip:** It refers to suggestions that have the function of facilitating the installation process of the Blockbit NGFW:

 Example of a Tip message.

Symbol – "Tip"

- **Note:** Refers to notes or notes that have the function of assisting the installation process of the Blockbit NGFW:

 Example of a Note message.

Symbol – "Note"

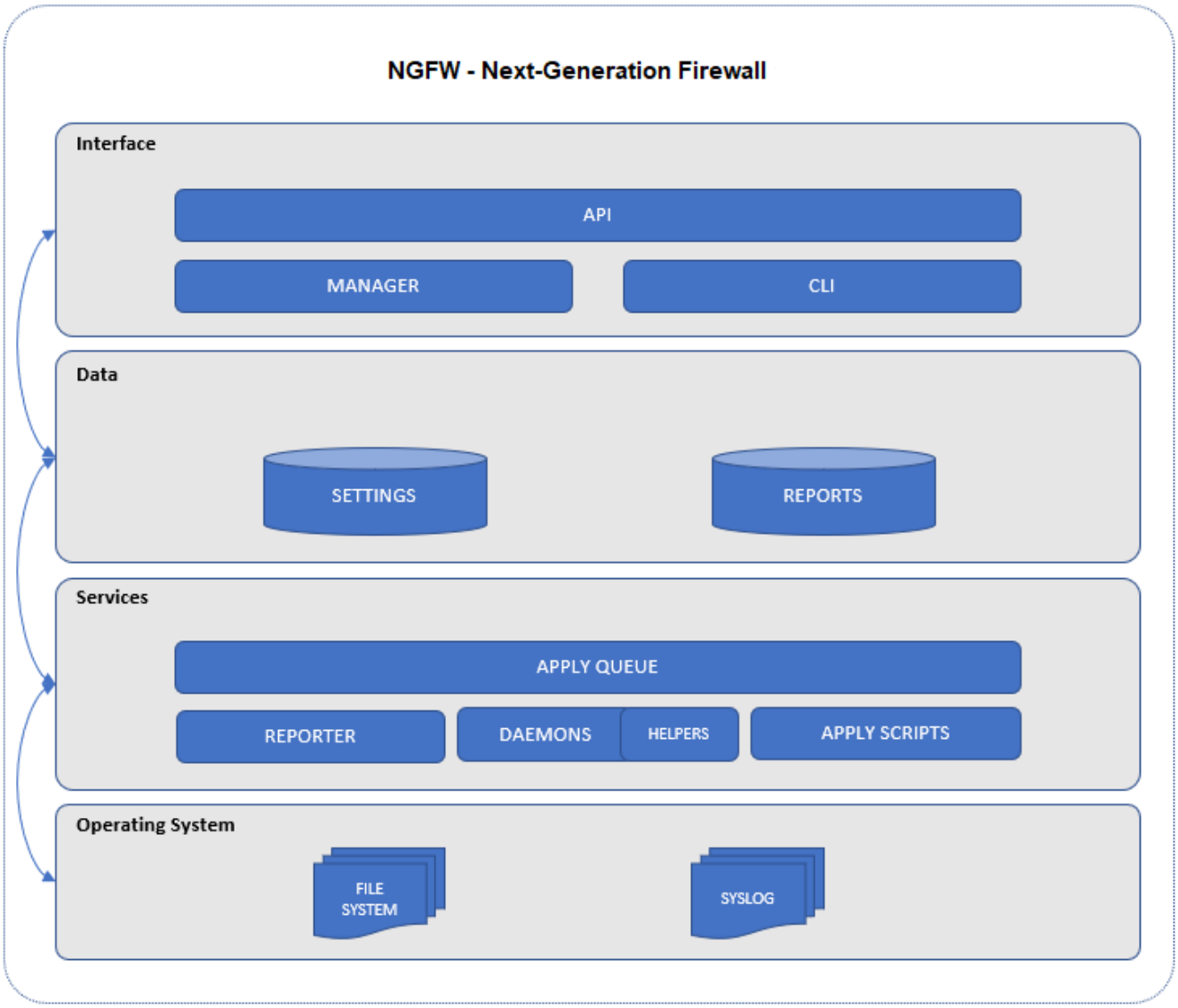
- **Information:** Refers to additional information regarding the Blockbit NGFW:

 Example of an Information message.

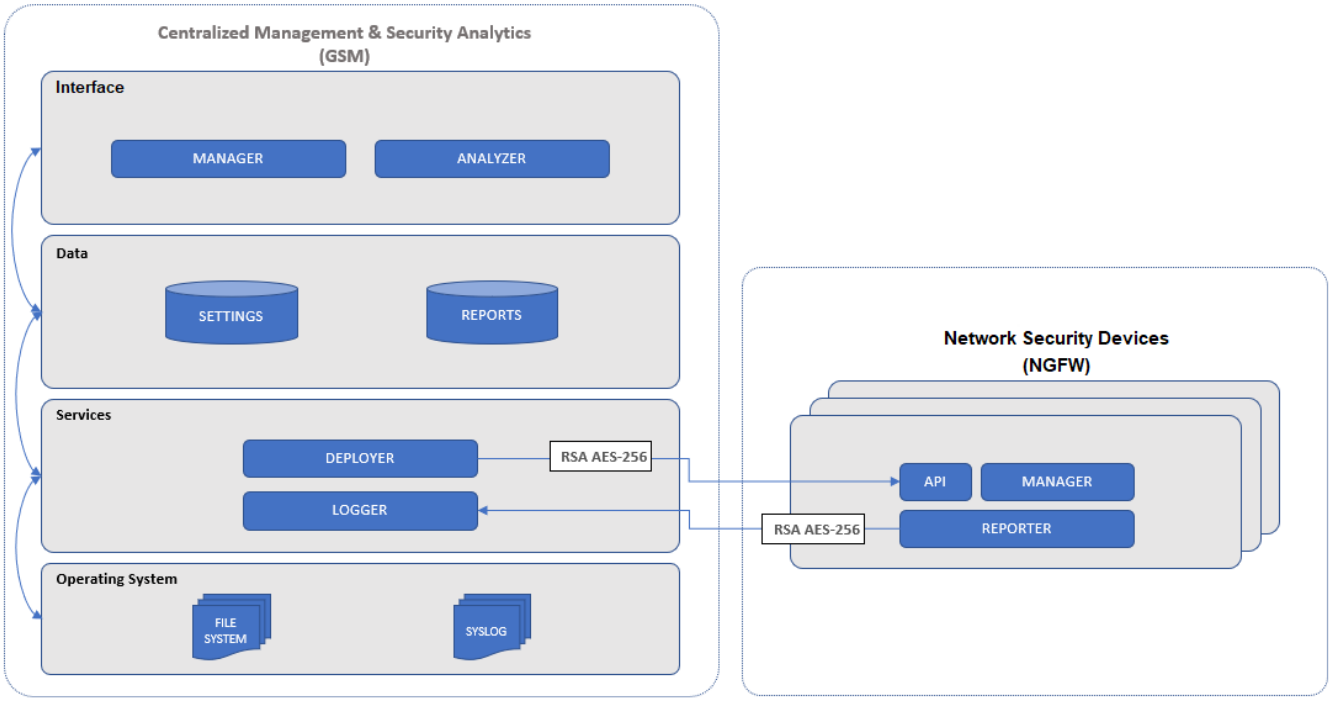
Symbol – "Information"

UTM - ARCHITECTURE

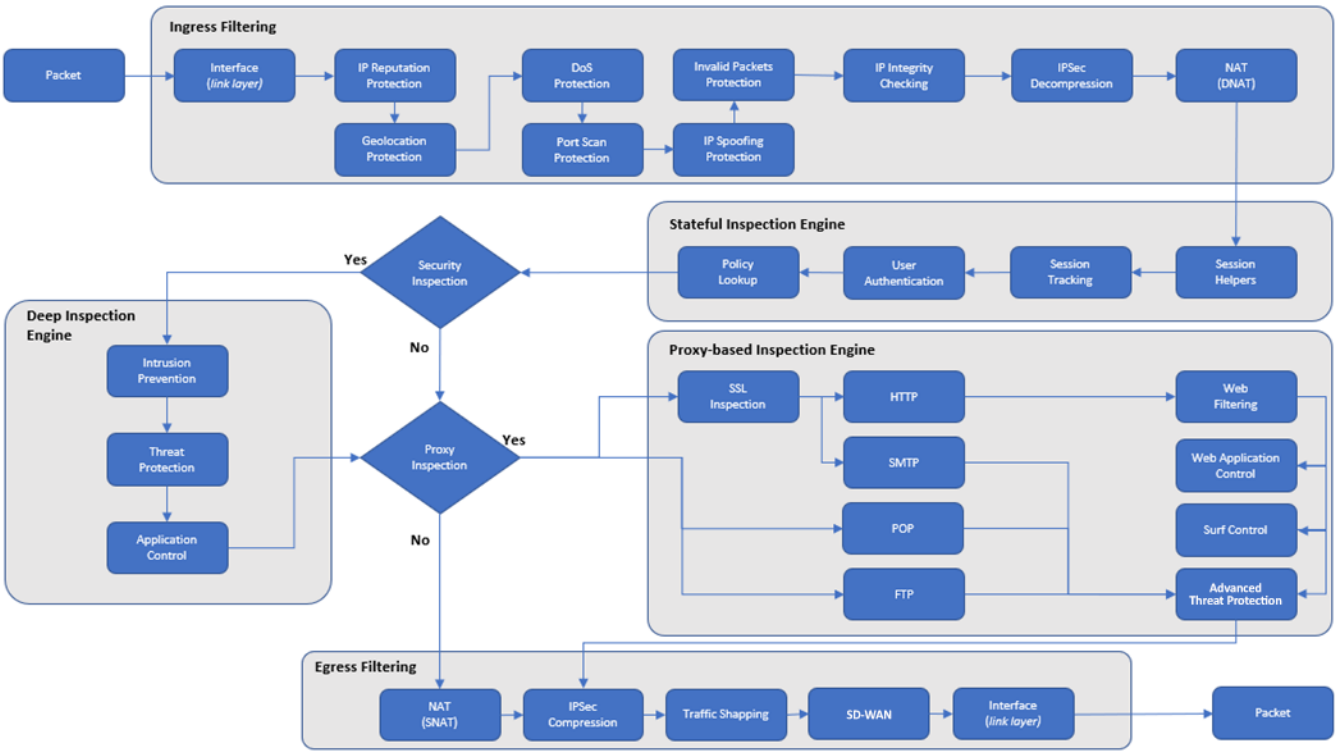
The Blockbit NGFW architecture is presented by a set of component layers, which, when integrated, define the technical aspects related to the services offered by the system. The image below represents the integration of the modules.



System Architecture - Management



System Architecture - Centralized Management



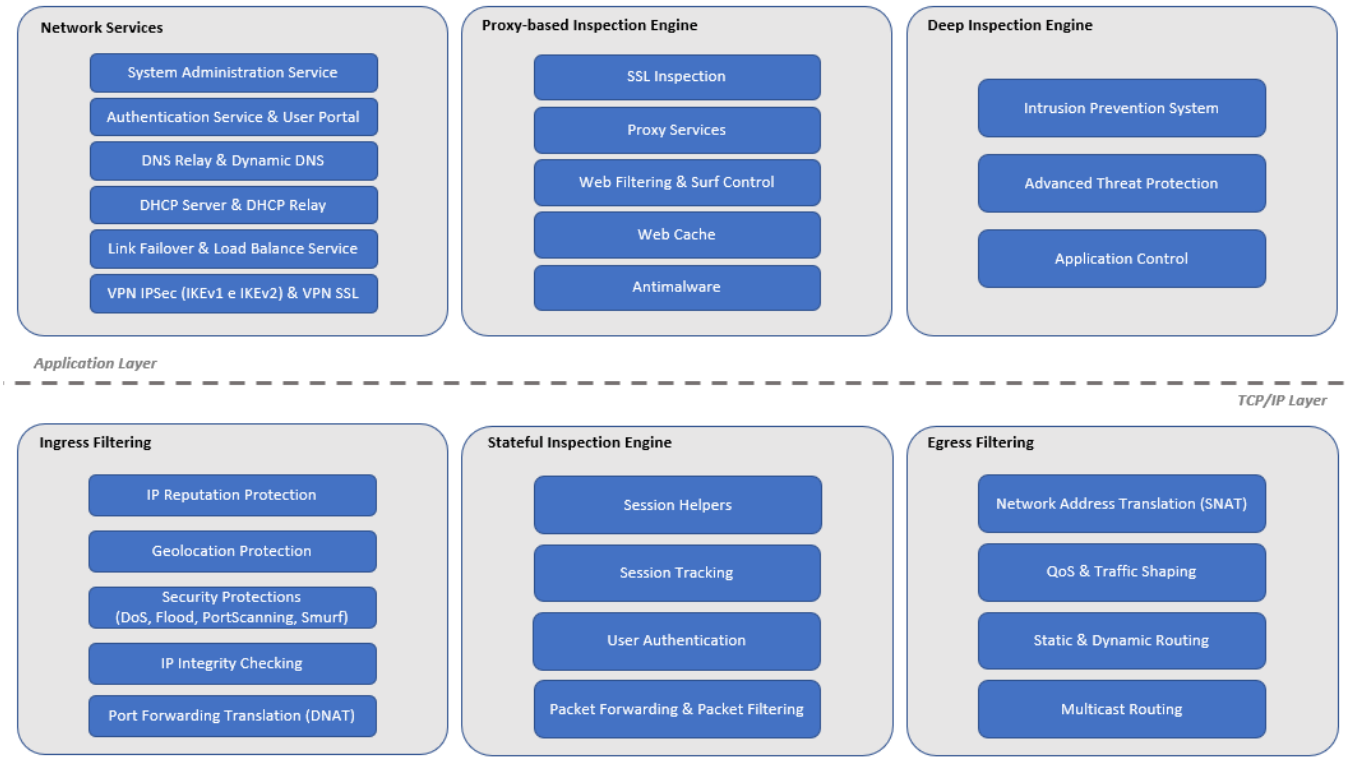
Packetflow

Next, the architecture modules will be detailed.

Architecture - Component Models

The architecture is divided into the following component models:

- *API*;
- *Frontend*;
- *Backend*;
- *Data storage*;
- *Operating System*.



Components

Next, we will explain these models.

Architecture - API

The Application Programming Interface (API) is the WEB management layer, which is executed through an API, which follows the RESTful specification with data transfer in JSON format. It can be used to integrate the product with third-party tools and other Blockbit products, such as Blockbit GSM and Blockbit EPS (End Point Security). All requests are authenticated using a key enabled by the system administration user and authentication is performed using the BASIC method of the HTTP protocol.

Architecture – *Frontend*

Frontend is the development layer that provides the presentation interface and system controls. Through its resources, it is possible for the administrator to access any type of information and execute the configuration commands in the Blockbit NGFW services.

Thanks to the interfaces available in the Frontend layer, it is guaranteed that the end user does not have direct access to the components available in the deeper layers of the system architecture.

The system was designed to offer two types of interfaces in the Frontend layer:

- ***Manager*:** It is a WEB application for device administration. In it, the administrator defines all the system configuration parameters, performs Scans and performs the vulnerability management;
- ***Portal*:** It is another Web application, where users of the network that are inspected, have access to some system resources, eg: Authentication portal, personal data, sessions, certificates, reports, password change, quarantine and Virtual Office;
- ***Console*:** The CLI console provides access to several commands for configuration and diagnostics. This interface can be accessed through connection via an SSH and serial terminal.

Architecture – *Data storage*

In the system, the Database is divided into 3 parts:

- ***Settings*:** Intermediate layer, serves for storage and transfer of information between Frontend and Backend components. Through the database system, Frontend writes settings and parameters that will be applied to the Backend components and the Operating System;
- ***Definitions***: Stores intelligence data and system definitions, such as compliance rules and malicious signatures, among others;
- ***Reports*:** Database where the reports of the entire system are recorded after a scan.

Architecture – *Backend*

Backend is the layer that provides commands and programs that apply requested configurations, being executed through Frontend interfaces for Scanner services and the Operating System.

Thanks to the system having a modular feature, having independent services between them, the information between the Frontend and Backend resources are transported through two encrypted paths and authenticated by key: Database or SSH Connection.

- ***Apply Queue*:** The execution of commands between the Frontend interfaces and the Backend services, are carried out through a command queue within the database. This queue organizes these commands by priority, to ensure that service settings are applied in the correct order by the system;
- ***Apply Scripts*:** Read the configuration parameters stored in the database and rewrite those settings in the services and the operating system;
- ***Daemons*:** These are the main programs that implement the network traffic inspection services in the product, they are processes executed in the background (background) by the system;
- ***Helpers*:** They are programs coupled with daemons and complement their functions, most of the time, they are executed through PIPE;
- ***Summarizers*:** These are programs that collect information from system logs, summarizing the statistics in order to store them in the reporting databases. Thanks to the high flow of information collected by the system, these programs were developed with a view to execution every 5 minutes.

Architecture – Operational System

The Blockbit NGFW's Operating System is also maintained by Blockbit's research and development team, where the open source tool packages used in the implementation of the services are made available.

To simplify compatibility with Appliances and ensure performance when running services, Blockbit NGFW runs on an Operating System with a Linux Kernel based on Intel x86_x64 architecture.

UTM - INSTALLATION

Blockbit NGFW can be installed in two types of Appliances: Hardware and Virtual, which are compatible with the following solutions: VMware, XenServer and KVM.

Next, we will exemplify how to install Blockbit NGFW using VMware ESXi 6.5.0 software.

- Importing the Virtual Machine;
- Starting Virtual Machine - First Access;
- Recordings of images on flash drives.

UTM - Importing the Virtual Machine

Initially, it is important to consider the minimum characteristics of the Virtual Appliance, as shown in the table below:

Table - Minimum characteristics of the Virtual Appliance

Model	Memory	Disk	CPU	Frequency	Interfaces
BBv-2	4 GB	32 GB	2	2.00 GHz	4
BBv-5	4 GB	32 GB	4	2.42 GHz	4
BBv-10	8 GB	32 GB	4	2.42 GHz	4
BBv-30	8 GB	120 GB	4	2.42 GHz	6
BBv-100	8 GB	120 GB	8	3.40 GHz	8
BBv-1000	16 GB	240 GB	8	4.00 GHz	9, with a limit of up to26
BBV-2000	32 GB	240 GB	16	5.00 GHz	9, with a limit of up to 26
BBv-10000	64 GB	480 GB	32	3.20 GHz	9, limitless
BBV-15000	96 GB	480 GB	40	3.20 GHz	9, limitless

To import, download the Open Virtual Appliance (OVA) from the Blockbit NGFW, which can be requested through the Trial registration on our website: http://www.blockbit.com.

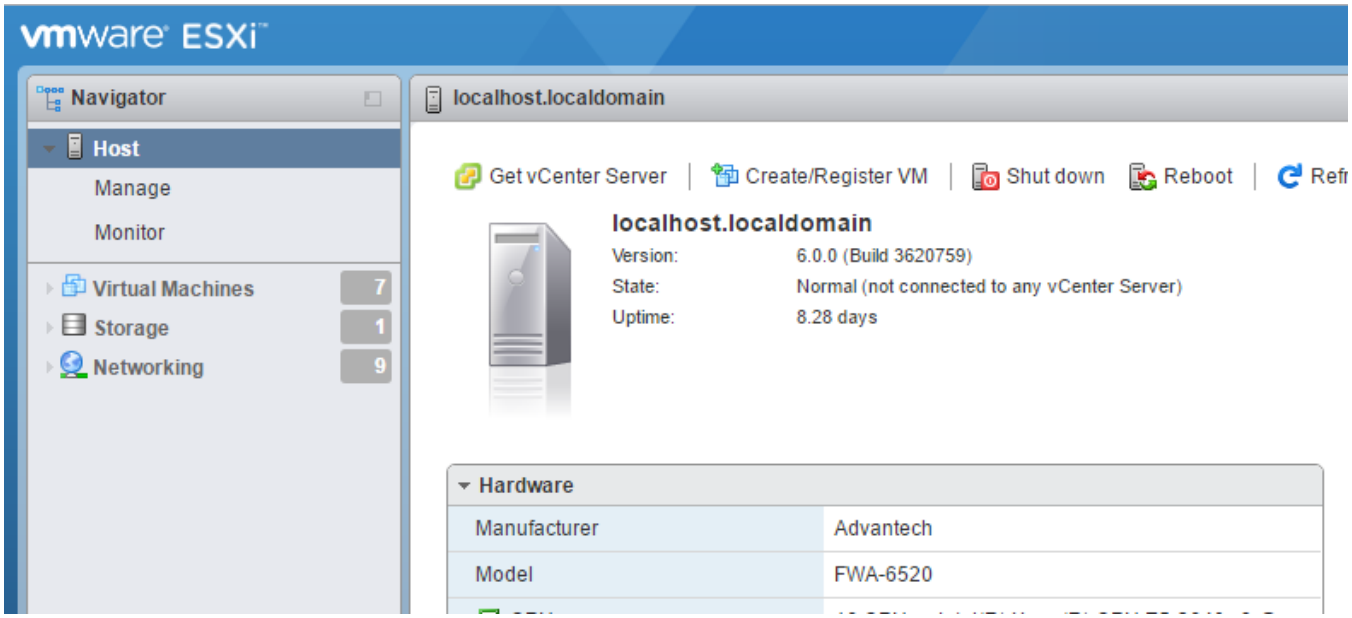
1. Using your preferred web browser, access the VMware ESXi management console on the VMware Host Client;

2. Fill in the fields with the following information:

- ***User name*****:** User registered in VMware;
- ***Password*****:** User password;
- Click on the "***Log in***" button.

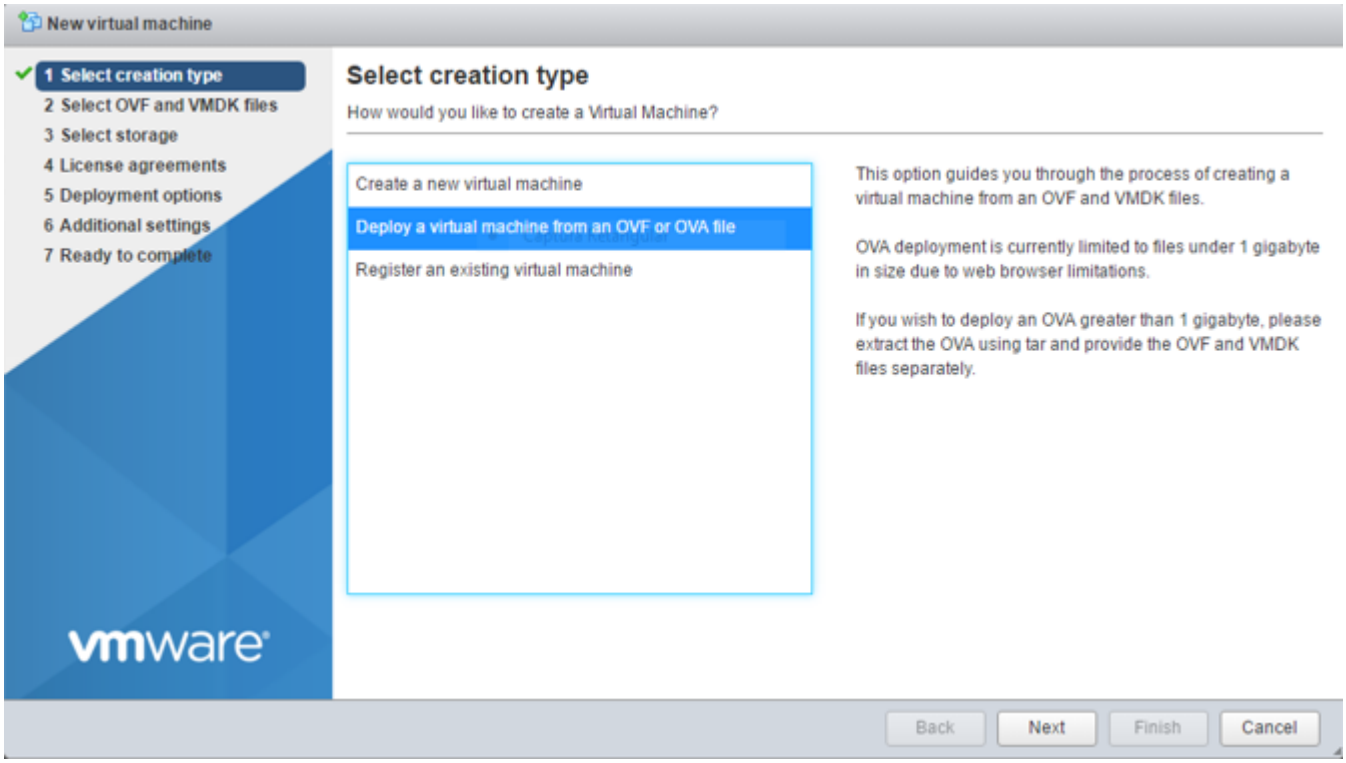
Login VMware

3. Click on "Create / Register VM";



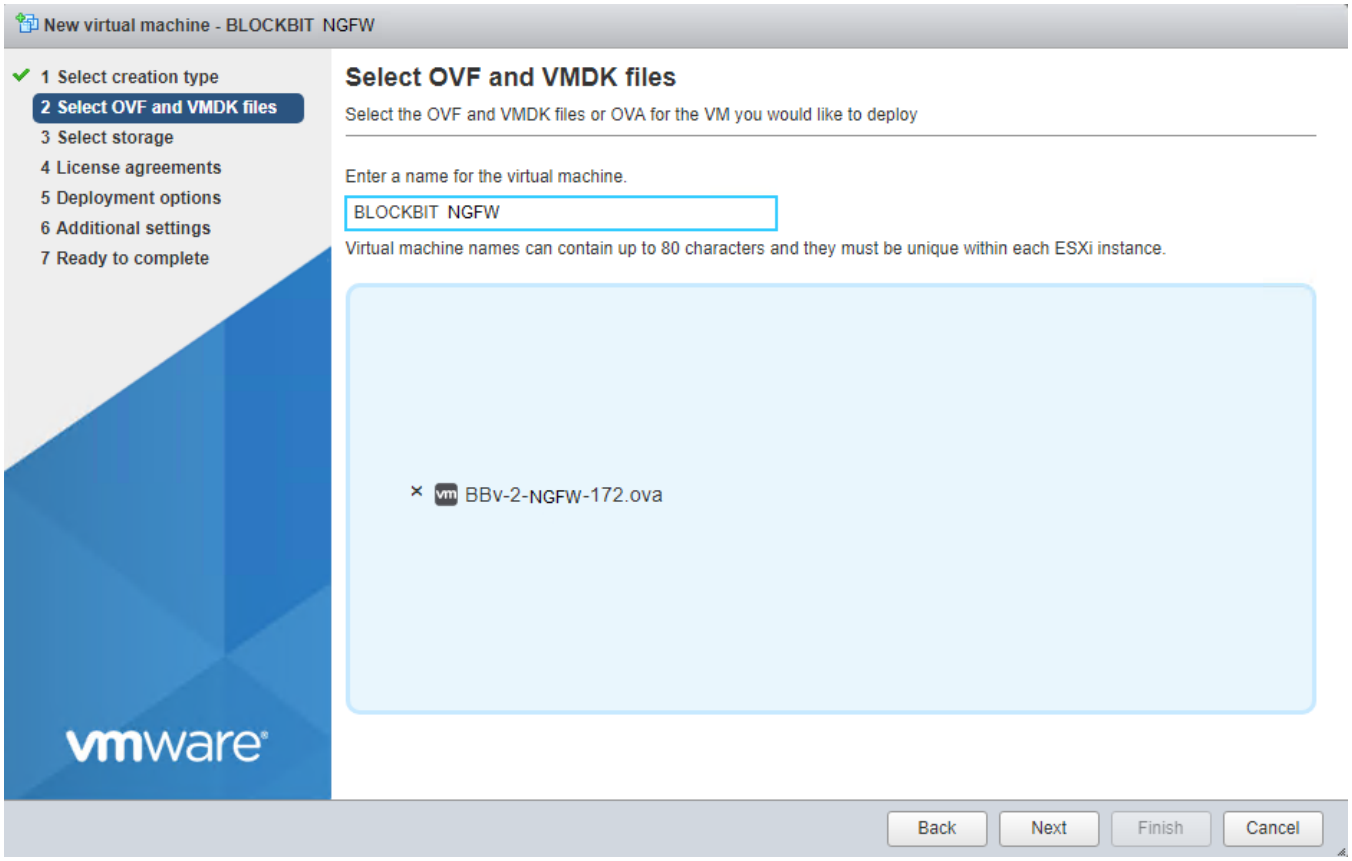
Console VMware

4. Select the option “Deploy a virtual machine from an OVF or OVA file”;



Select creation type

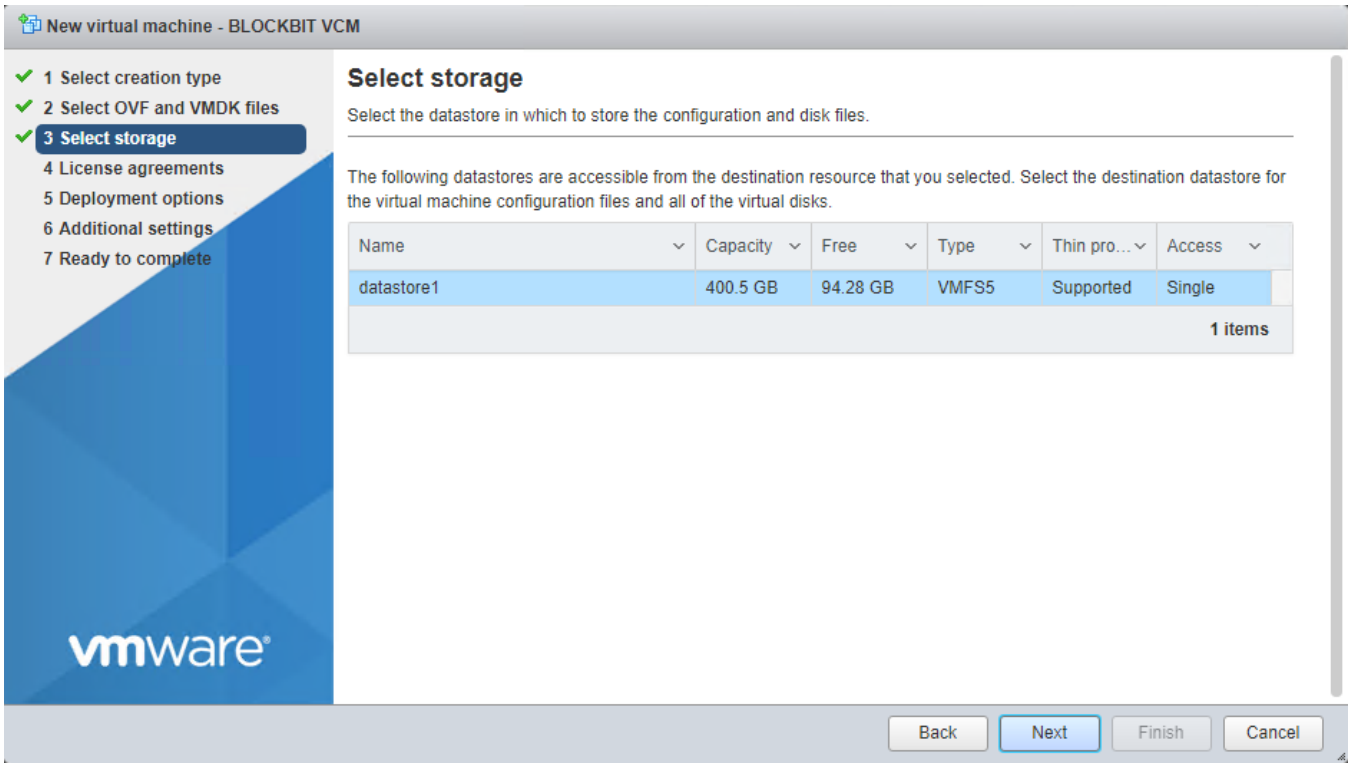
- Click the “Next” button.
- Select the image of the Blockbit NGFW that has been downloaded from the Blockbit website and enter the name of the machine in the field “Enter a name for the virtual machine”. Ex.: Blockbit NGFW;



Select OVF and VMDK files

- Click the “Next” button;

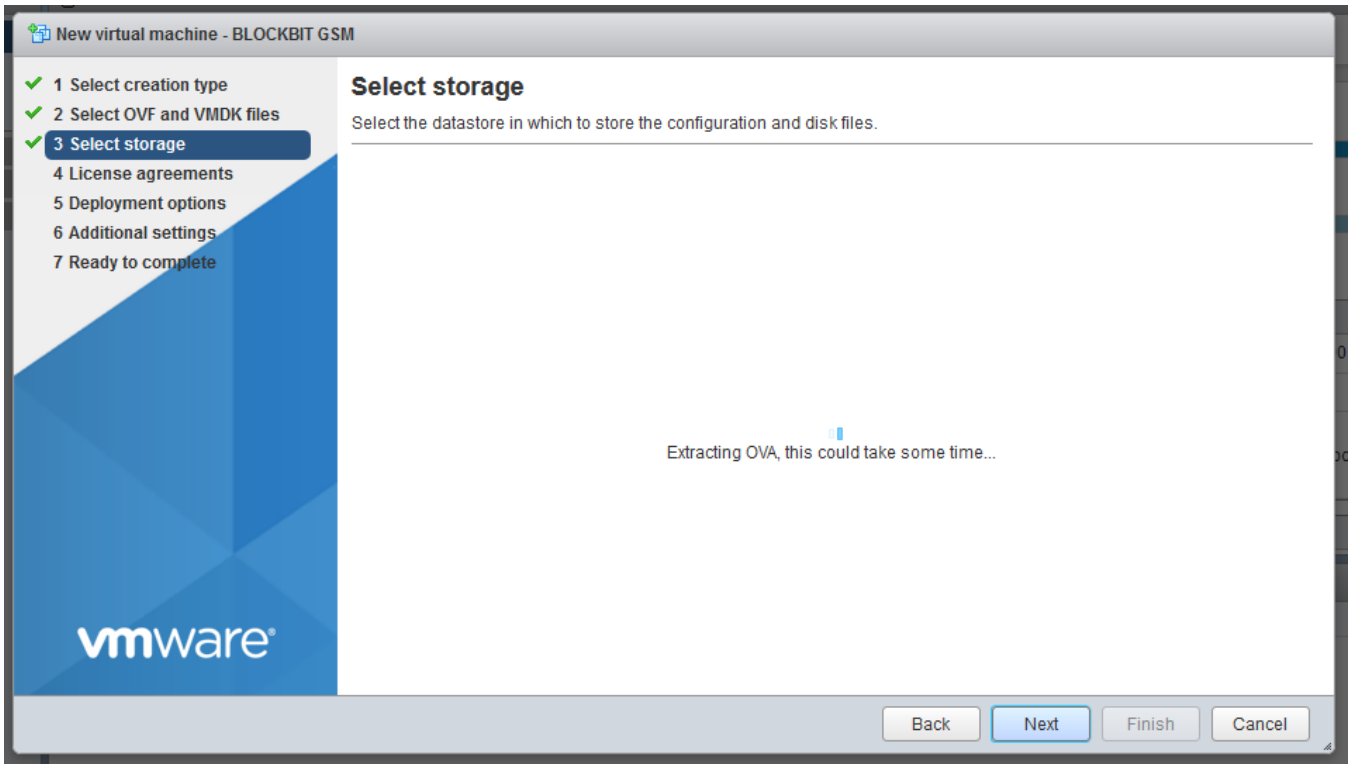
5. Select the desired storage. Ex .: datastore1;



Select Storage

- Click the “Next” button;

6. Wait for the OVA to upload. While uploading, the following message will appear: “Extracting OVA, this could take some time ...”. Wait for the completion of this process, which should occur automatically;

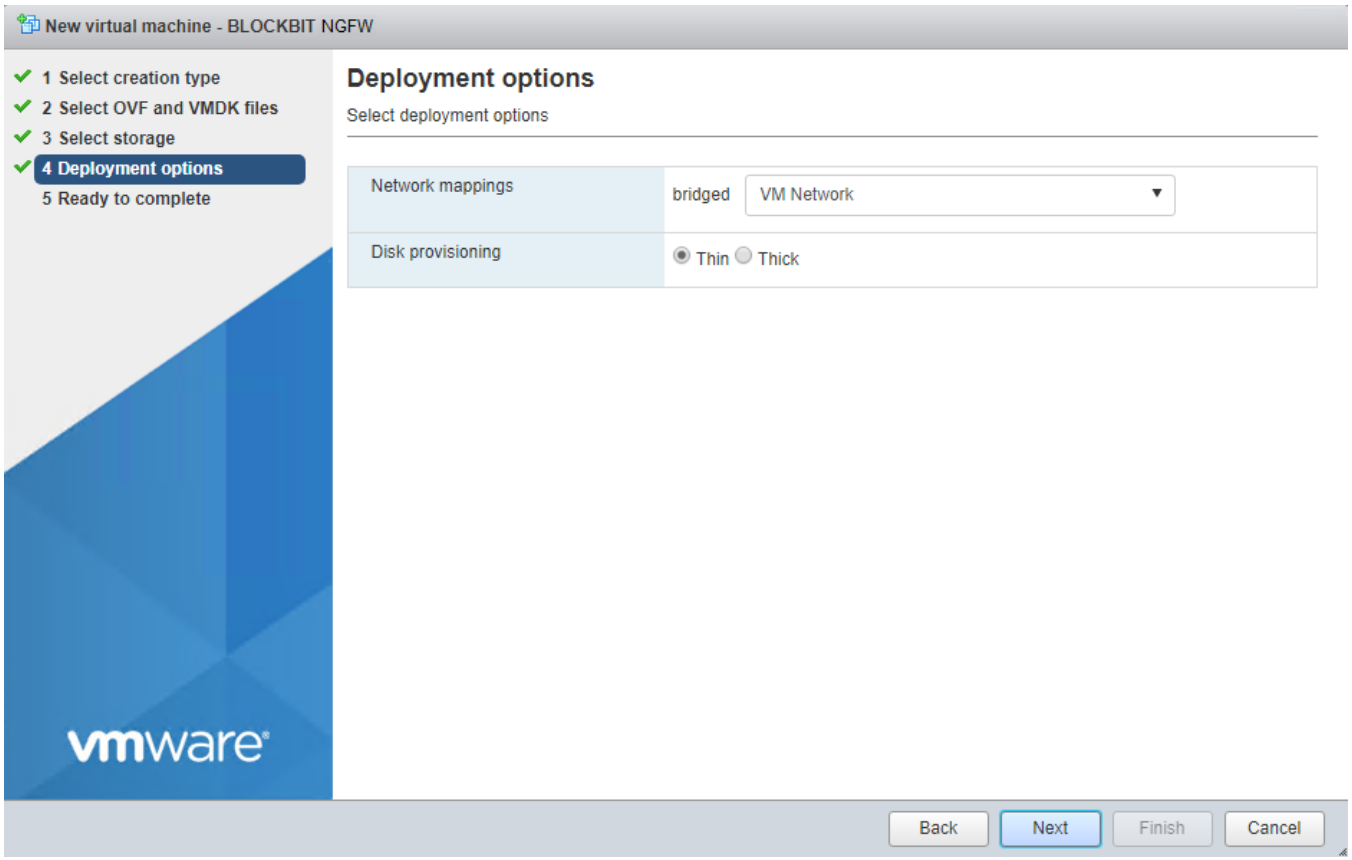


Select Storage – "Extracting OVA, this could take some time..."

7. Configure virtual machine settings:

- ***Network mappings*:** Set the network mode appropriate for your environment. Ex .: Mode bridged;
- ***Disk provisioning*:** Set the option to your preference. A brief description of the options follows.:
    - **Thick Disk:** These are disks fully allocated in the datastore, that is, if you create a Thick disk with 20GB, it will occupy 20GB of your datastore;
    - ***Thin Disk*:** It is a type of disk that allocates only the space that is written by the virtual machine's operating system. For example, if you create a 20GB disk for a VM, it will initially occupy only a few KB / MB in the datastore, however, the moment you start writing data to it through the operating system, its size can reach up to 20GB limit.

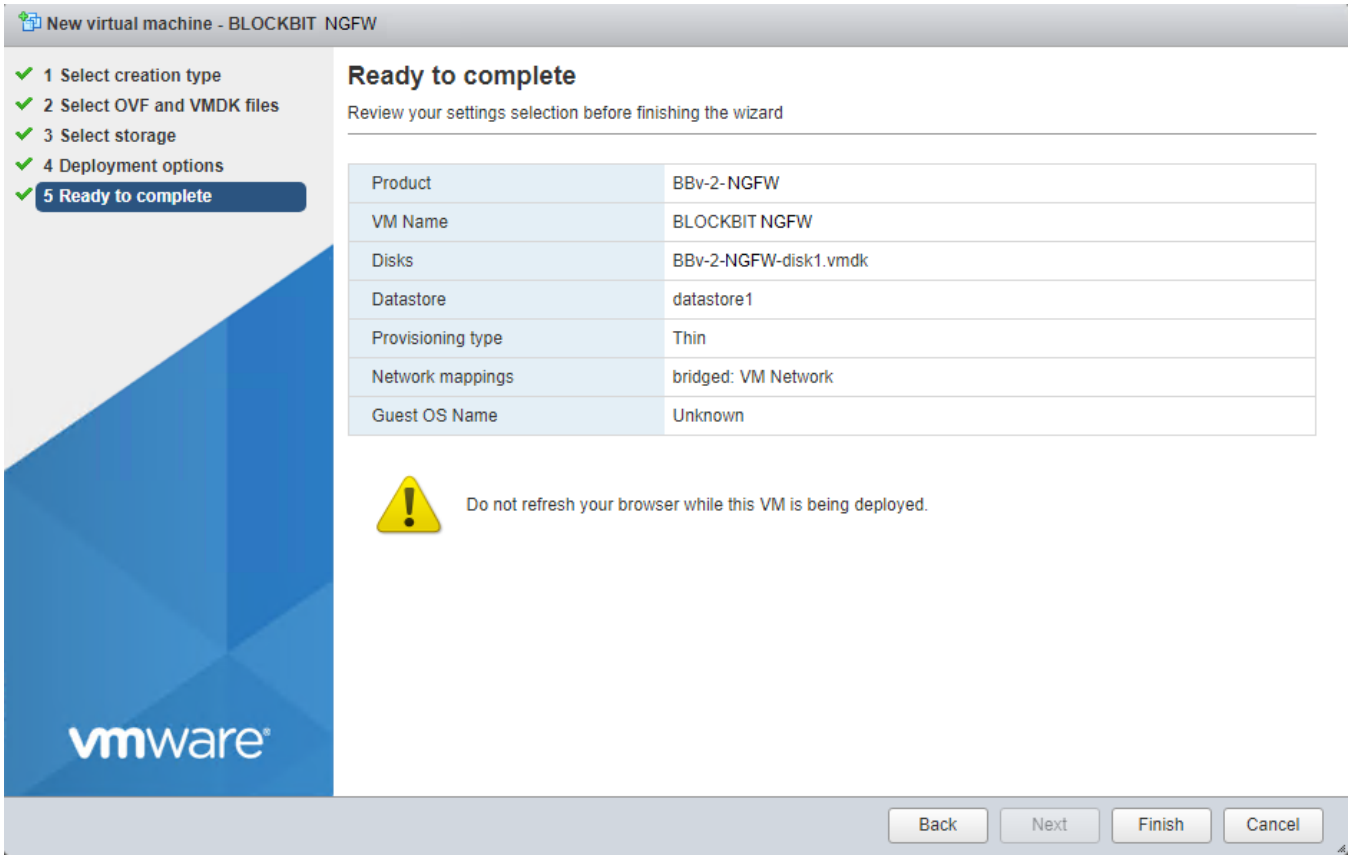
For more information, see the VMware manual. In this example, the configuration "Disk provisioning - Disco Thin" will be used.



Deployment options

- Click the "Next" button.

8. Review the configured settings before finalizing upload;



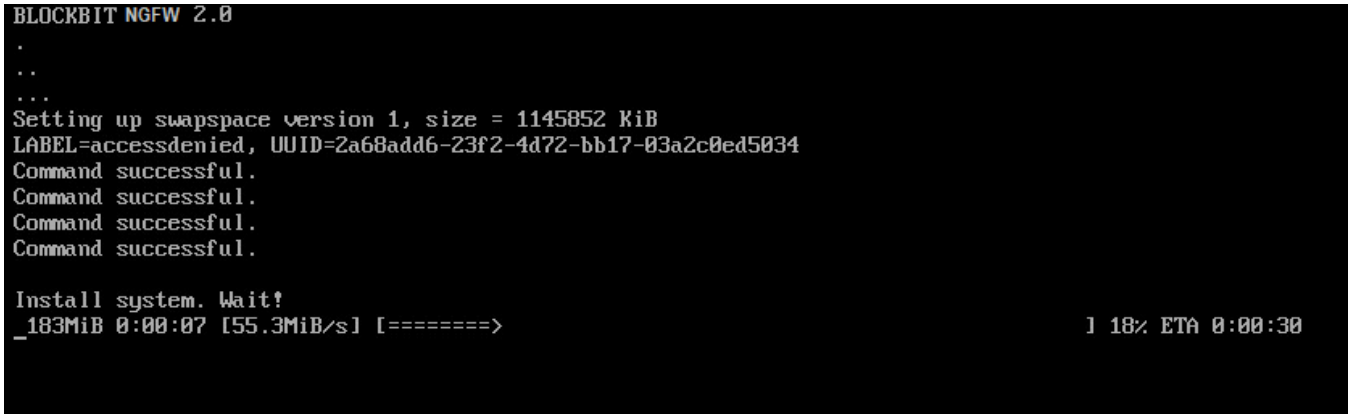
Ready to complete

- Click the "Finish" button.

The import is complete, just click on the “Power on” button to start the virtual machine and proceed to install Blockbit NGFW.

UTM - Starting Virtual Machine - First Access

When starting the virtual machine for the first time, the following screen will be displayed:



Starting the Blockbit NGFW for the first time

The virtual machine startup process shown below is the same for both Hardware Appliances and Virtual Appliances. There is no need to perform any steps, just wait until the login screen is released.

Tela de *login* – Blockbit NGFW

You will now need to configure the IP. To do this, perform the following steps:

1. ***Localhost login*:** Log in through the CLI console;
2. After performing the Authentication in the CLI console, fill in the following fields:

- ***Login*:** admin
- ***Pass*:** admin

It is highly recommended to change the default password for the "admin" console user. To change the default password, it is necessary to create a secure password. This password must contain at least 8 characters with upper and lower case letters, numbers and special characters.

To change the password, type the command below:

```
Type the passwd command and type "Enter".
Enter the current "password" and type "Enter".
Enter the new password and confirm it.
```

After performing this procedure the password will have been successfully changed.

3. Change the IP address of the Blockbit NGFW;

The default IP address for Blockbit Network Security is 192.168.1.1. This IP is used on the eth1 port. In this guide we will use the IP address 172.16.102.136 as an example. If you want to change it, follow the steps below:

Detalhes da configuração:

***IP*:** 172.16.102.136
***Mask*:** 255.255.255.0
Default Gateway: 172.16.102.1

If you need to check your appliance's UUID, enter the command [show-uuid]

In older versions of the NGFW, the management interface was eth0, as of NGFW 2.0 this interface is used for Zero Touch Provisioning, for more information, check the GSM manual.

Taking that into consideration:

Eth0 is the main interface, it is a dynamic WAN interface, used for internet access and device provisioning;

Eth1 is the management interface with the default IP for NGFW configuration, it will be configured next.

Enter the commands:

```
ifconfig eth1 172.16.102.136/24 up
ifconfig eth1 down
ifconfig eth1 up
route add default gw 172.16.102.1 dev eth1
```

After performing this procedure, the IP address will have been changed.
With the command below it is also possible to edit the IP address of the Blockbit NGFW:

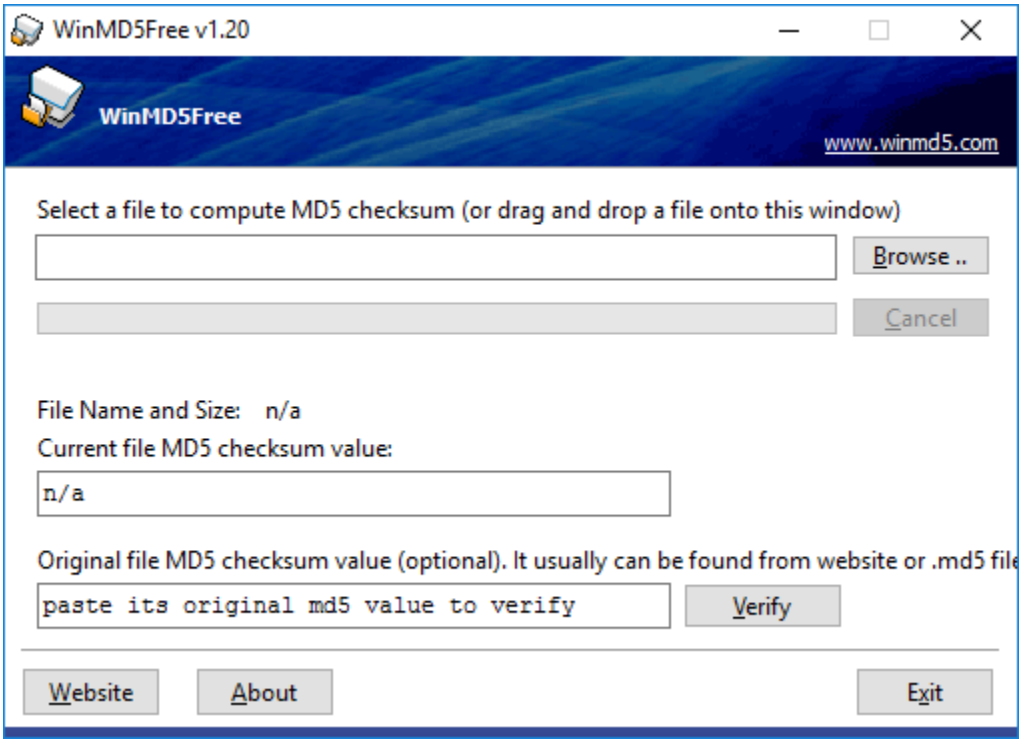
```
Type the command blockbit>changeip.
Hit "Enter".
```

UTM - Recording the installation image on flash drive

On the Blockbit website download the corresponding installation image.
The images must be downloaded and saved to a folder on the computer. Check the MD5SUM of the files to ensure they are not corrupted. The application to perform MD5SUM on Microsoft Windows is WinMD5Free (http://www.winmd5.com/), to perform this verification follow the steps below:

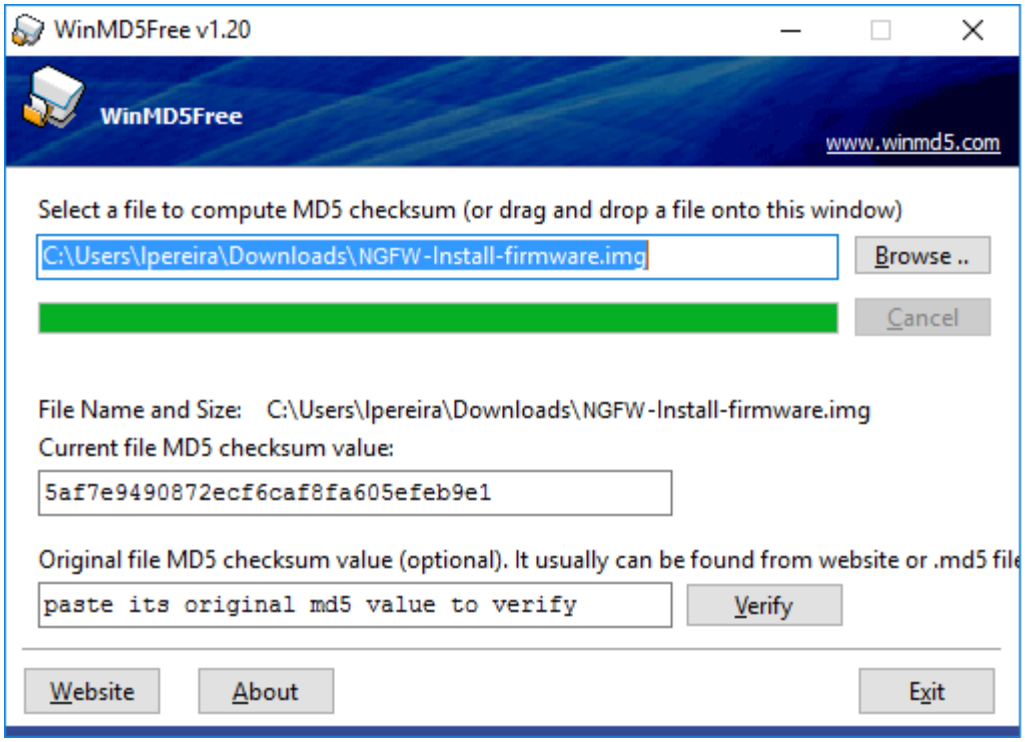
Checking files

1. Open the application, the following screen will be displayed:



WinMD5

2. Select the image file and wait for the calculation:



MD5 Check

3. Compare the values obtained from the two images in WinMD5 with the respective values saved in the section.

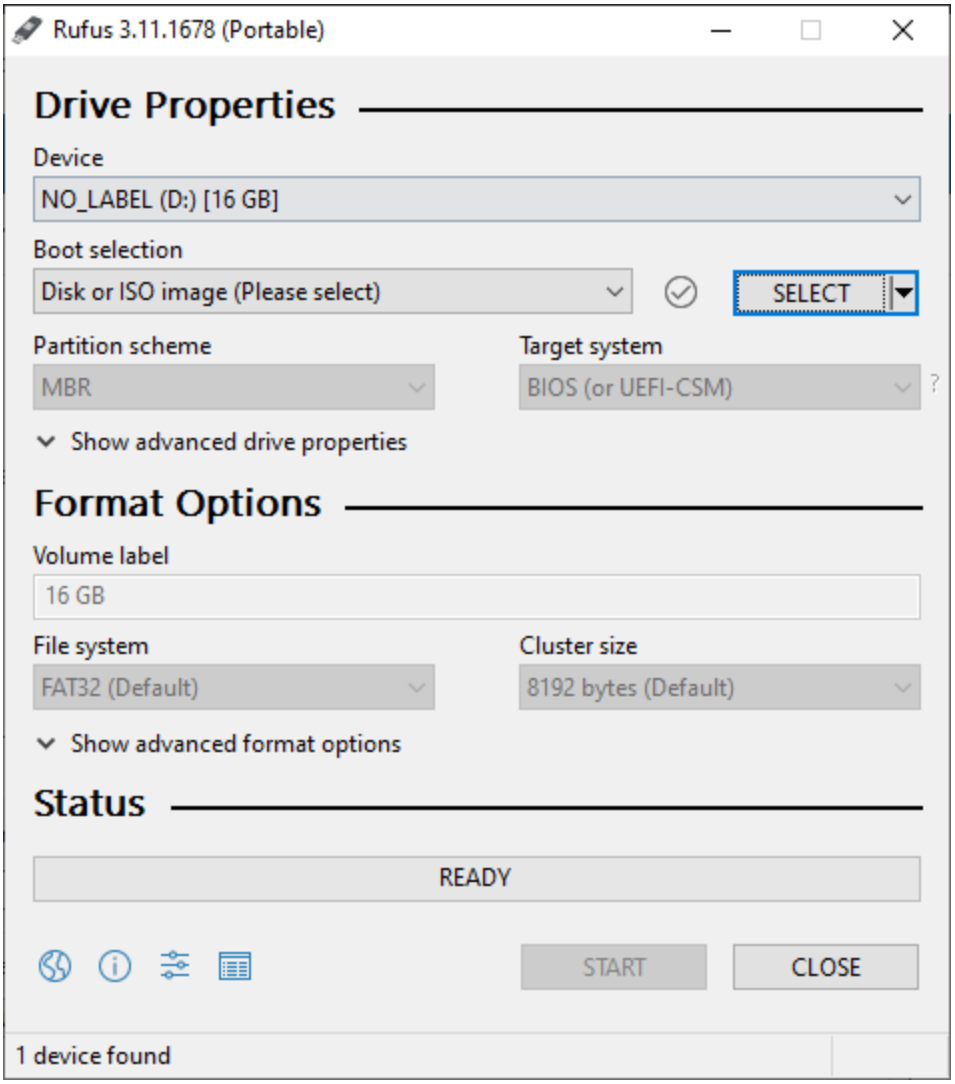
Recording the images

To record the images it is necessary the Rufus application that can be downloaded by clicking on this link: https://rufus.ie/.

1. Insert a pendrive, at least 8 GB;

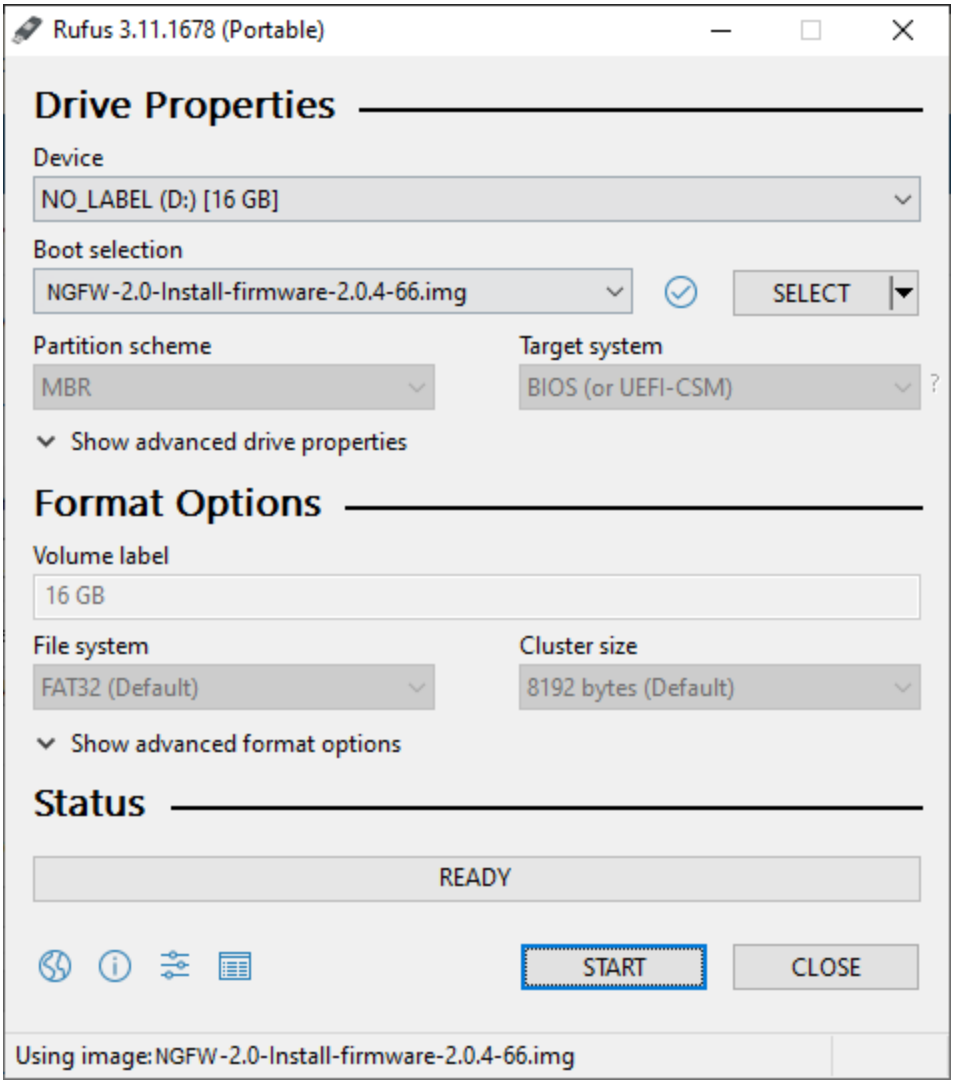
This pendrive will be used exclusively for installing the image, that is, it should not have any files, if necessary, make a format.

2. Upon opening the application, the following screen will be displayed:



Rufus

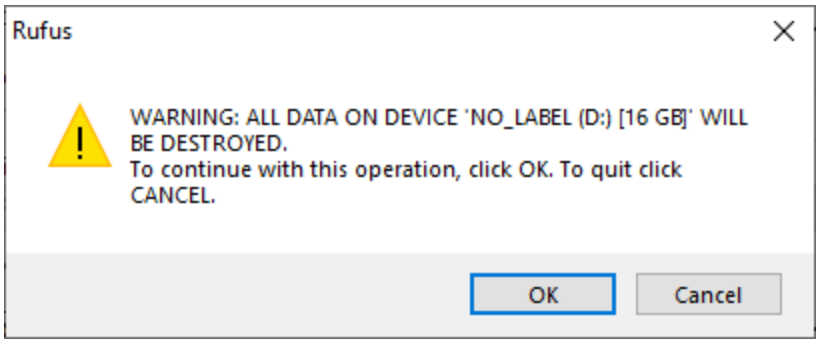
3. Click on [SELECT] and select the appropriate image to be saved on the pendrives. Ex.: NGFW-Install-firmware.img;



Recording the image

4. If it is not selected, select the Device corresponding to the USB stick that you want to record the image. *Ex.*: NO_LABEL (D:) [16 GB];

5. To save the image click on **[** START **]**, when doing this, the message below will be displayed;



WARNING

6. Click **[** OK **]** and wait for the recording to complete successfully;

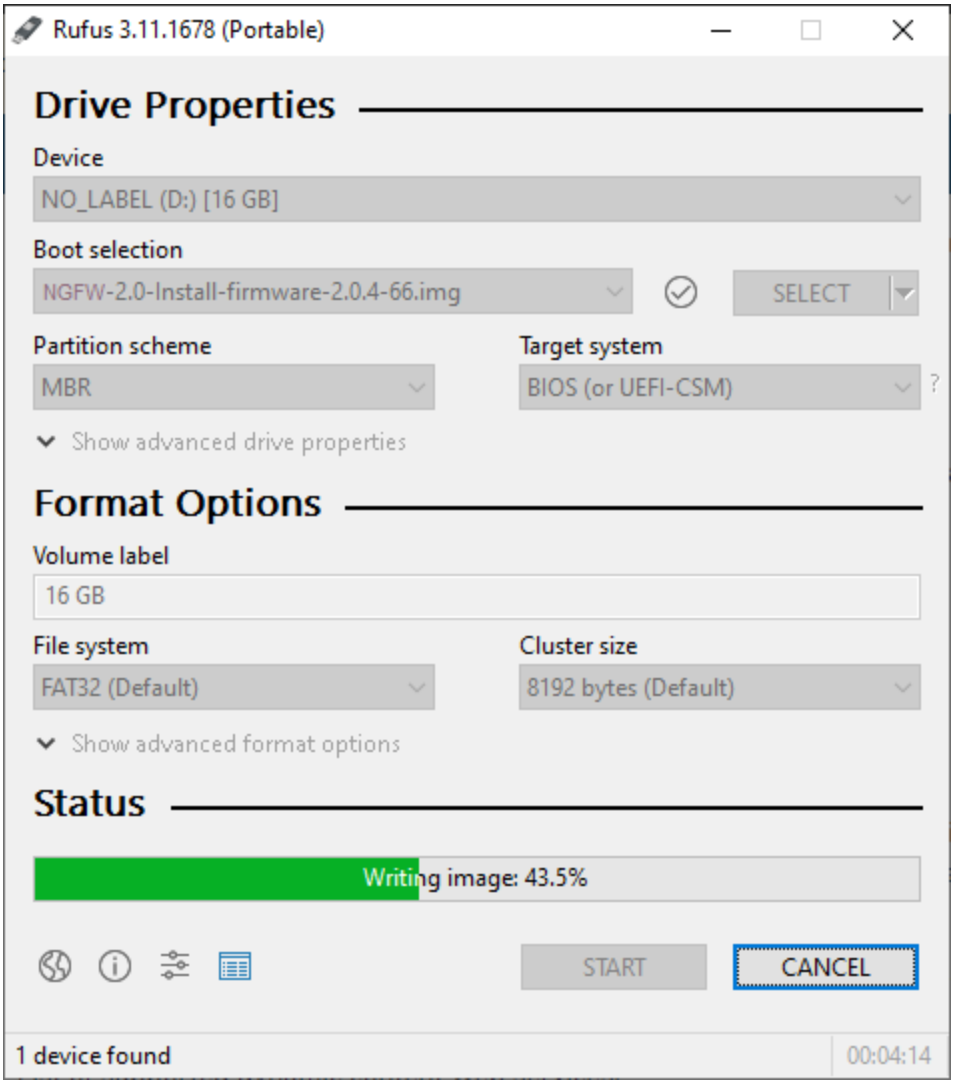
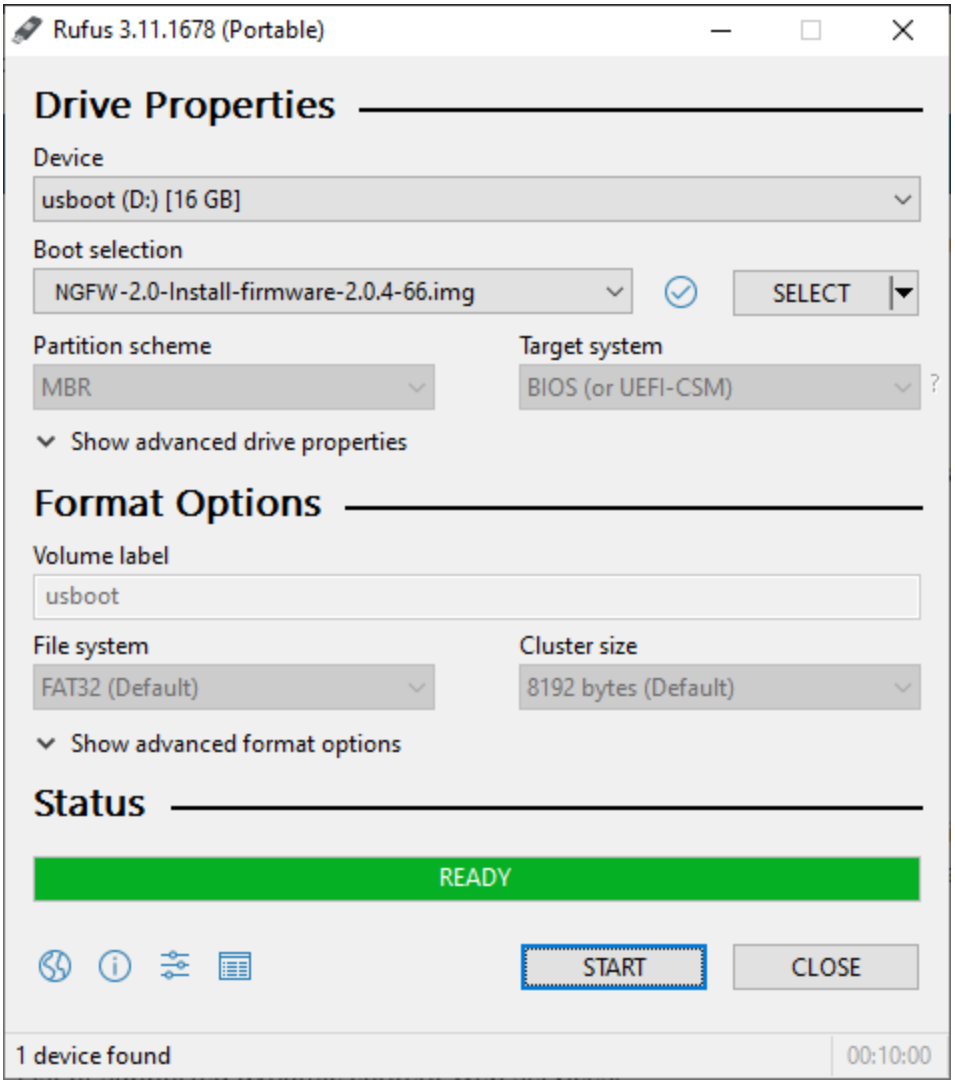


Image recording progress

7. After completing the progress bar, click **[** CLOSE **]** to close Rufus.



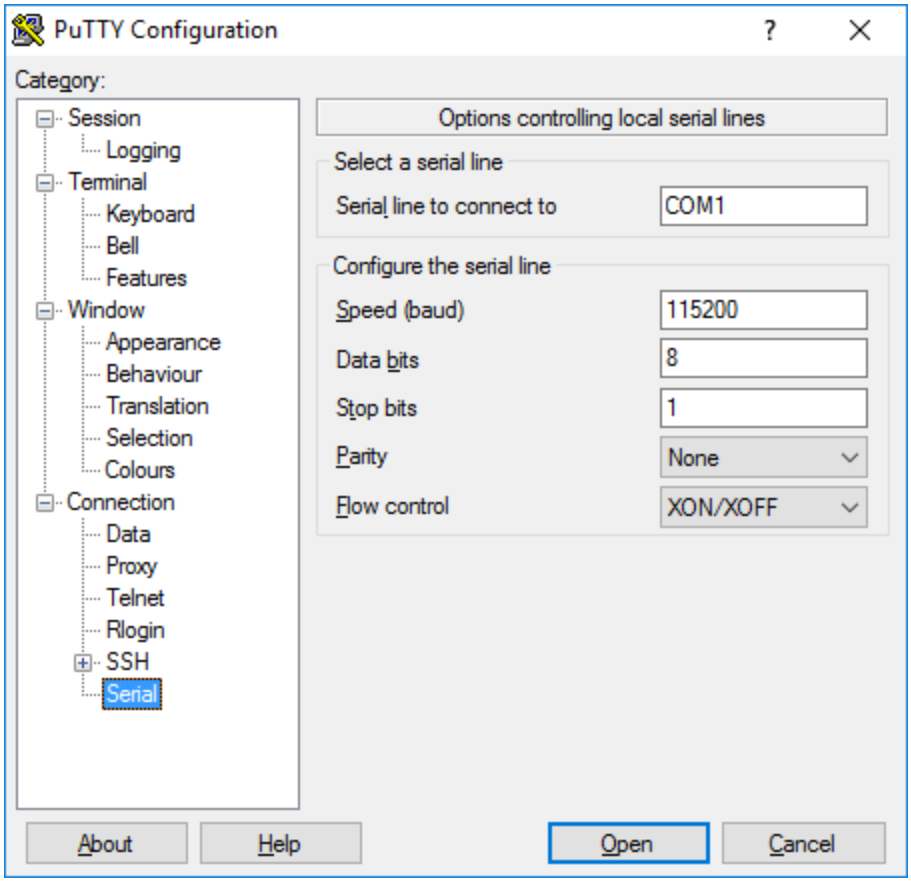
Rufus - Completed

Console Access - Putty

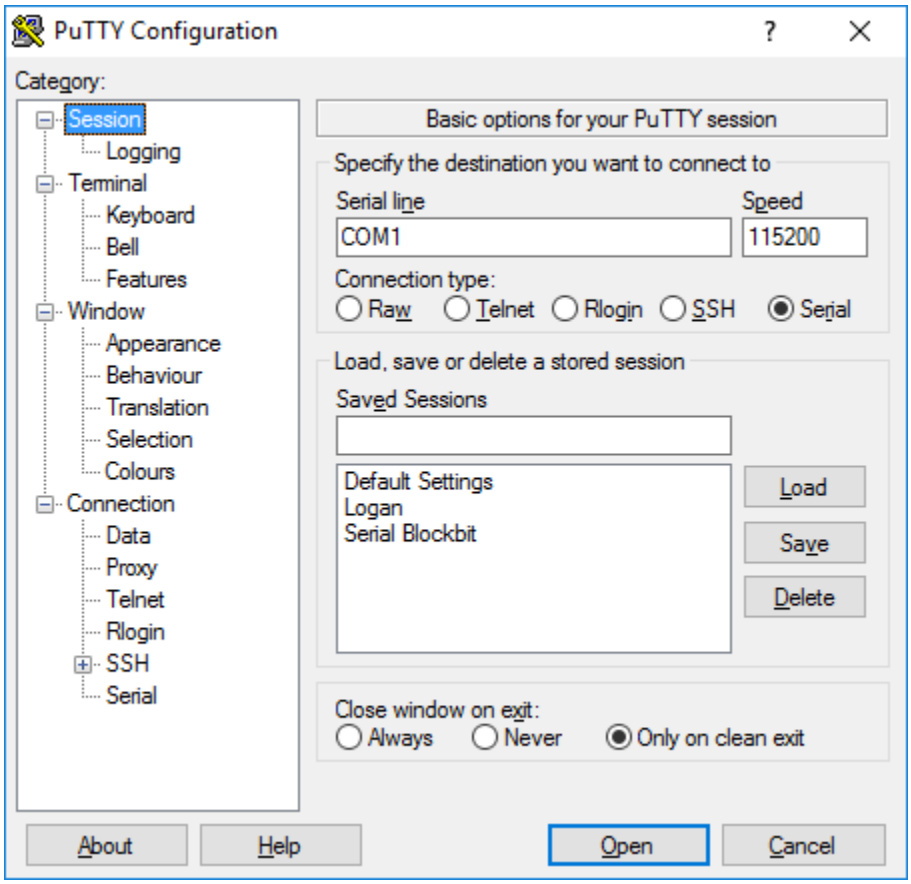
Before starting the following procedures, the Putty application must be available on the machine where the connection to the Equipment will be made. Putty is free and open source terminal emulation software.

Now configure the terminal emulator with the following parameters:

- Port: COM1 (a porta pode variar, verifique seu gerenciador de dispositivos do *Windows*);
- Standard transmission rate: 115200;
- Standard data bits: 8;
- Standard stop bits: 1;
- Standard parity: None.



Putty Settings



Putty Connect

UTM - EXCEPTION CONFIGURATION

This section will introduce how to configure an exception in web browsers: Google Chrome and Mozilla Firefox.
When performing the first access to the Blockbit NGFW Web Interface, it is normal for browsers to issue a security alert reporting a certificate error. This is because the browser does not recognize any certifying authority that validates access to this page as reliable. Therefore, it is necessary to configure the exception in the web browser.
To configure the exception, follow the steps:

1. Connect to your internet browser and access the address: https://172.16.102.136:98. If you have changed the IP address, use the changed IP;

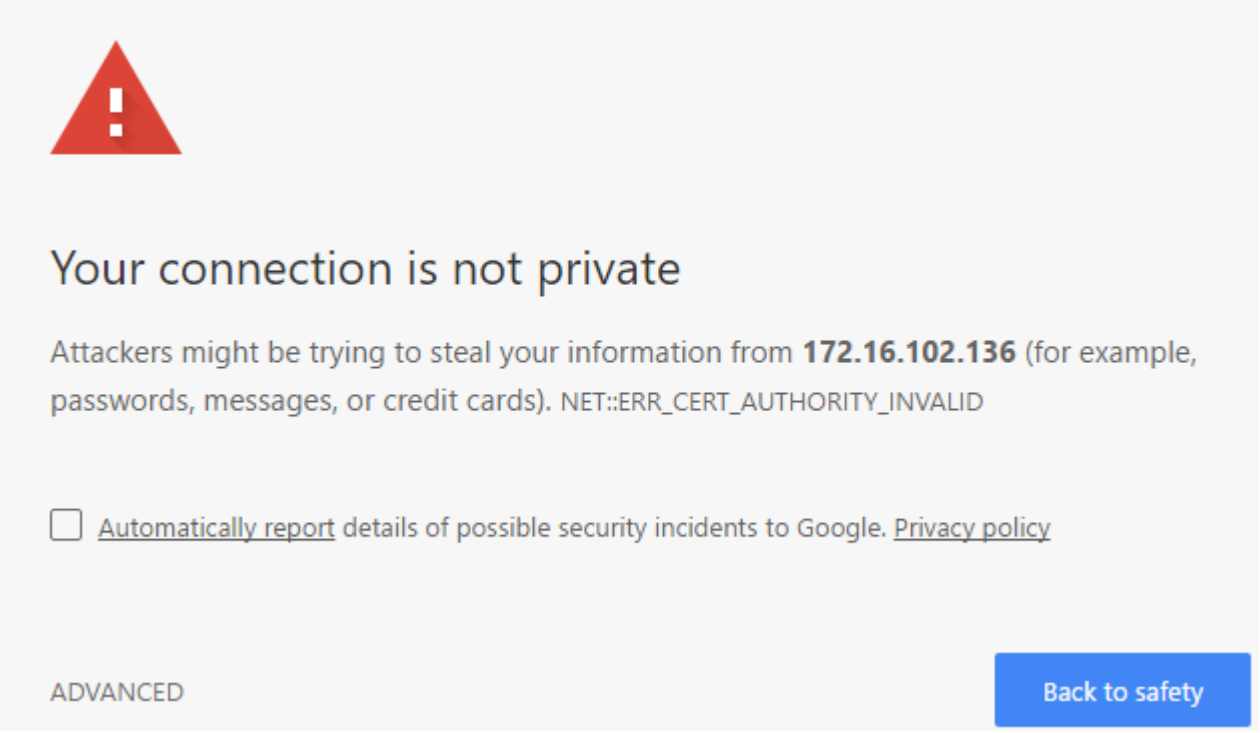
If the browser issues a **SECURITY ALERT**, follow the recommendations below.

Each browser has a procedure to release the connection as trusted. Follow the directions on how to proceed.

Setting exception in Google Chrome

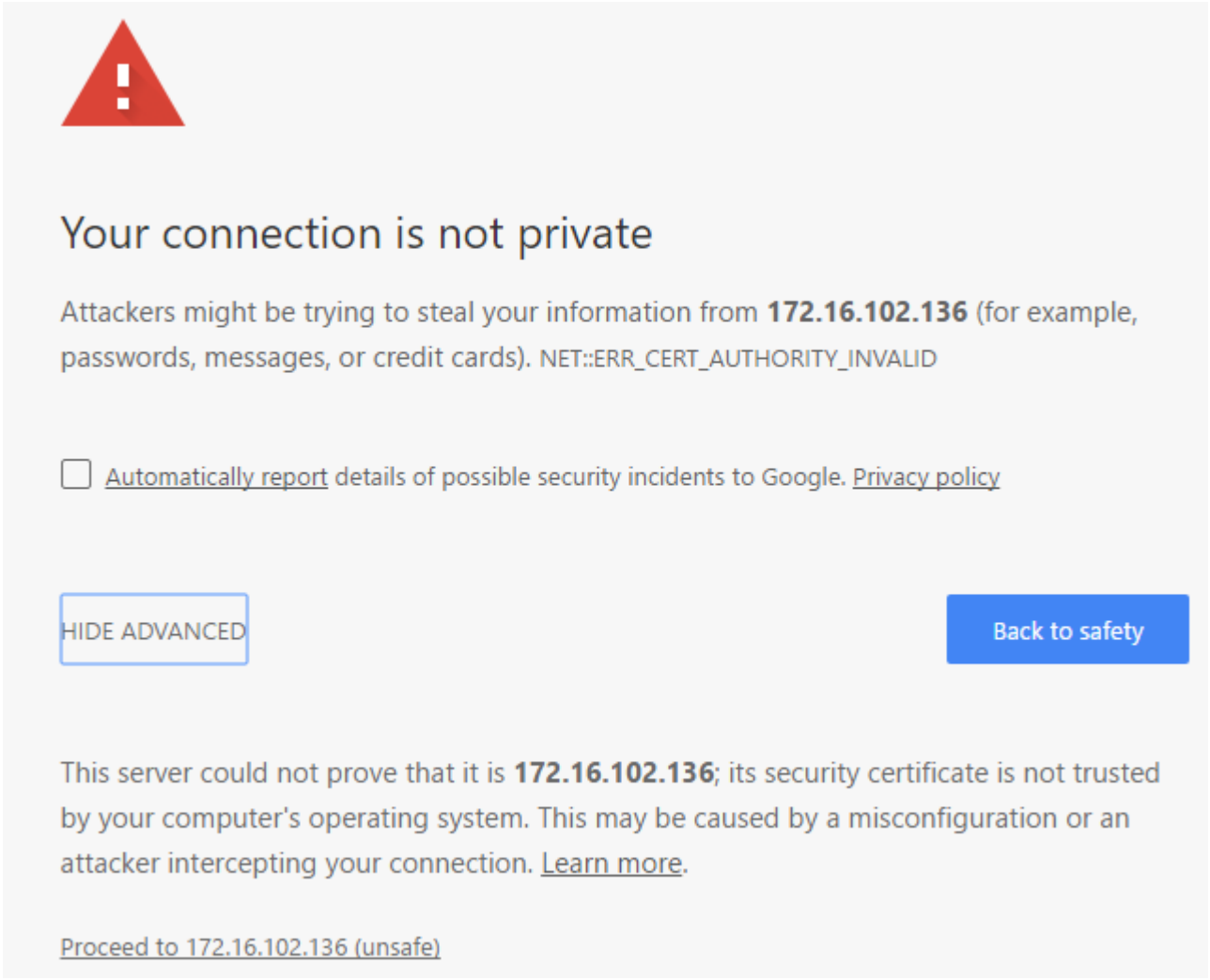
To configure the exception in Google Chrome, follow these steps:

1. Click the "Advanced" button;



Chrome exception - "Advanced" button

2. Click on the "Proceed to 172.16.102.136 (unsafe)" link to accept this page as trusted;



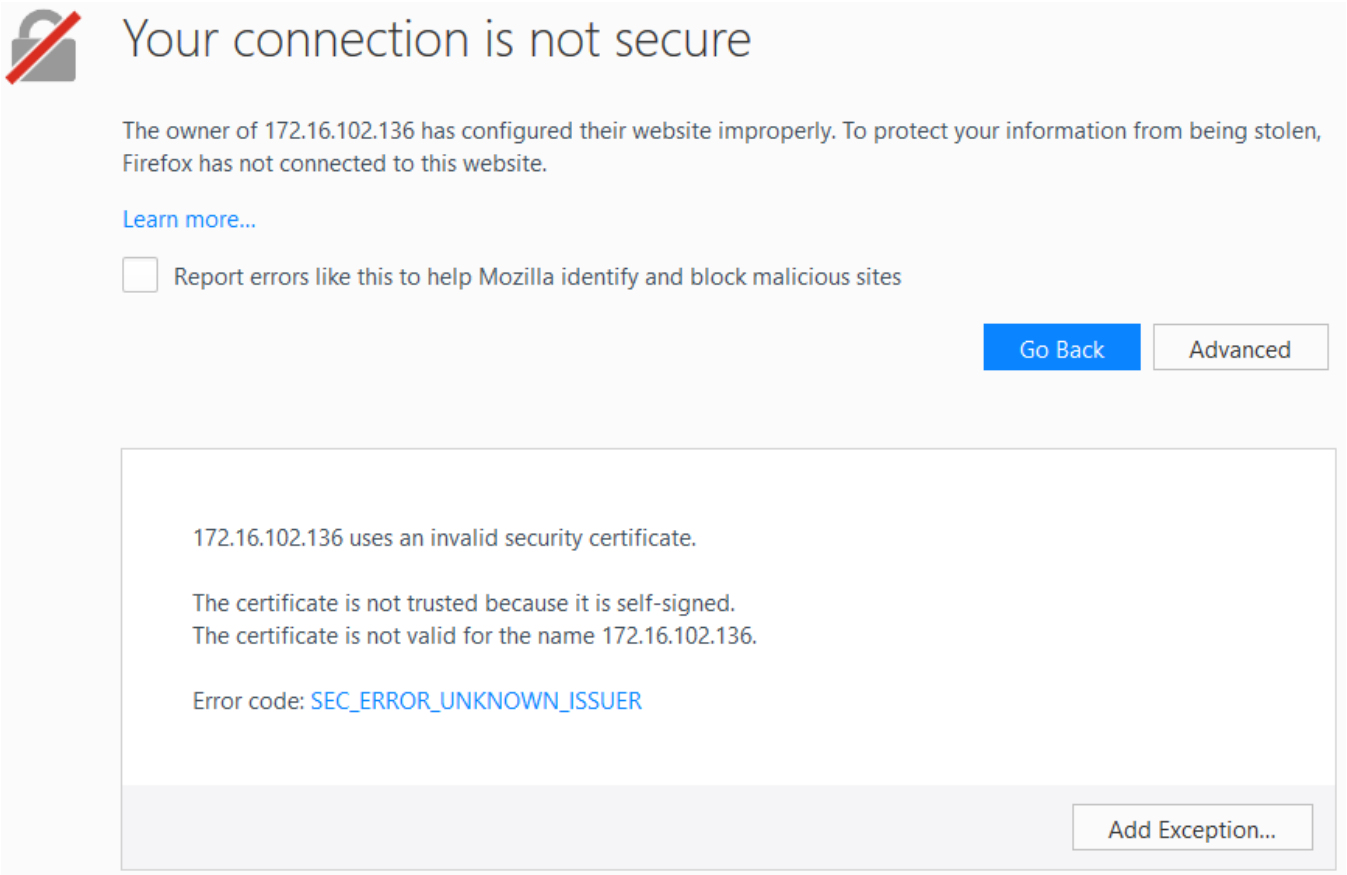
Chrome exception - "Proceed to 172.16.102.136 (unsafe)"

Exception setting in Google Chrome was successful.

Setting exception in Mozilla Firefox

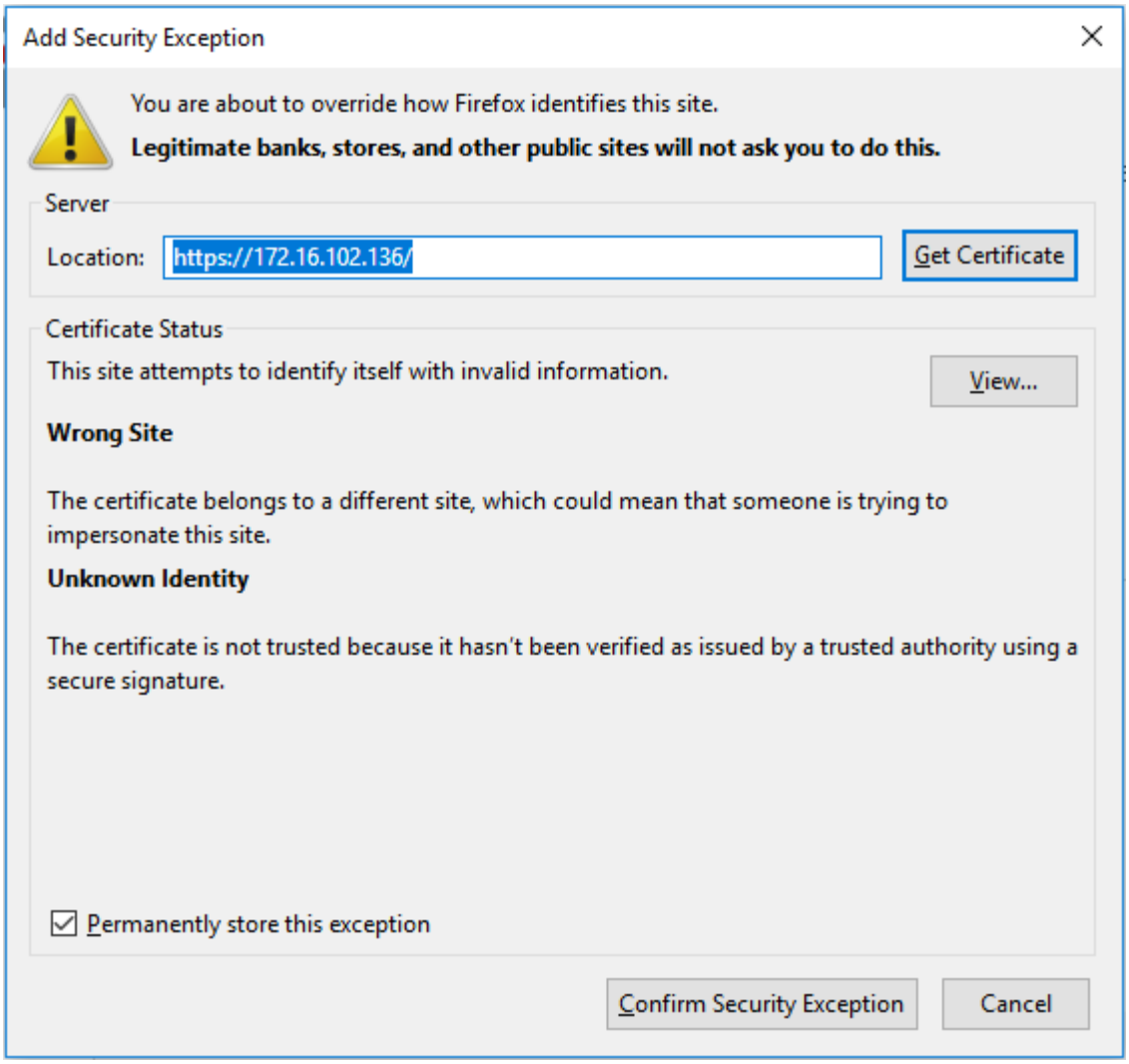
To configure the exception in Mozilla Firefox follow these steps:

1. Click the "Advanced" button;
2. Click the "Add Exception ..." button;



Mozilla Firefox exception - Your connection is not secure

3. Click on the "Confirm Security Exception" button.



Mozilla Firefox Exception - Confirm Security Exception

Exception configuration in Mozilla Firefox was successfully performed.

UTM - INSTALLATION ASSISTANT

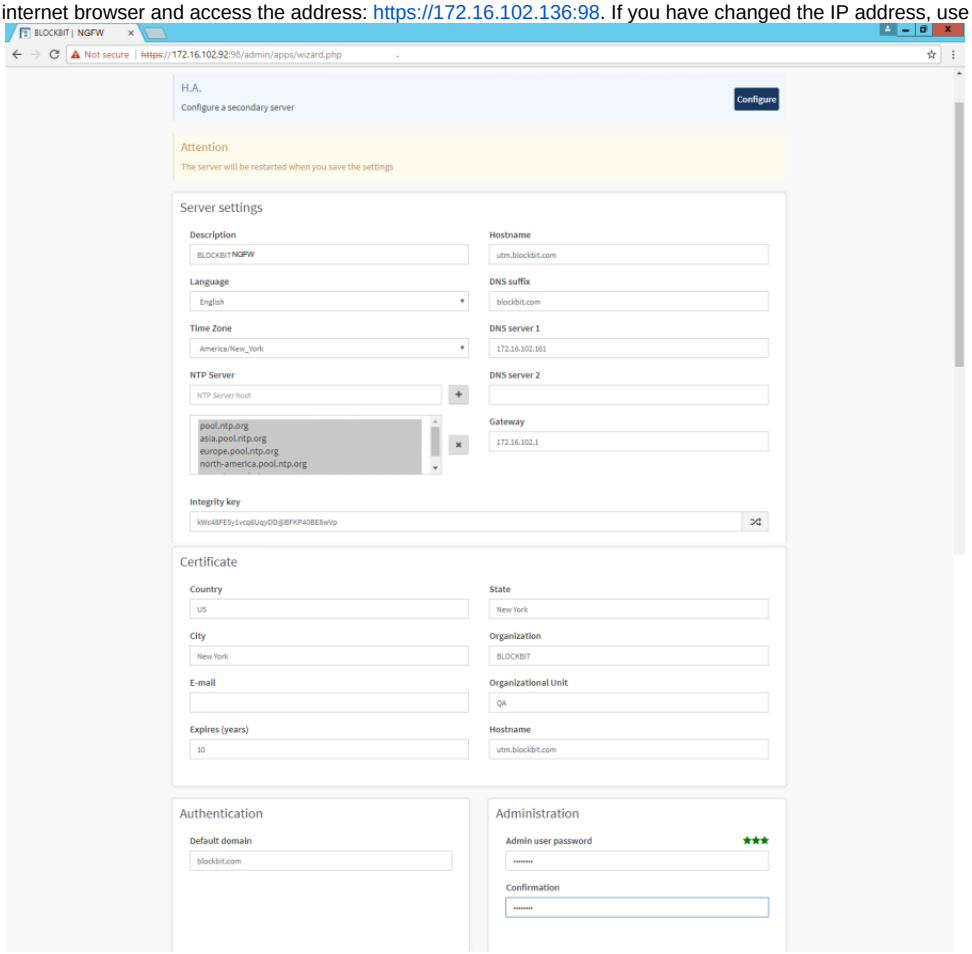
This section will introduce how to configure the Blockbit NGFW Installation Wizard.

The installation process and the correct completion of all fields required by the form will be presented below..

Installing the Blockbit NGFW

To install BLOCKBIT NGFW, follow these steps:

1. Connect to your internet browser and access the address: https://172.16.102.136:98. If you have changed the IP address, use the changed IP;



Installation Wizard

2. Enter the following data in the "Server settings" frame, for the initial network settings of the Blockbit NGFW:

- ***Description*:** Field to describe the name of the server. Ex .: Blockbit NGFW;
- ***Language*:** Select the default language. Ex .: English;
- ***Time Zone*:** Select the time zone in which your business is located. Ex .: America / New York;
- ***NTP Server*:** Set the clock synchronization server. Ex .: pool.ntp.org;
- ***Hostname*:** Hostname. It can be anyone as long as it complies with the FQDN - Fully Qualified Domain Name standard. Ex: utm.blockbit.com;
- ***DNS suffix*:** Network domain. Ex.: blockbit.com;
- ***DNS server 1*:** Set the DNS server for the network or the internet. Ex .: 176.16.102.161;
- ***DNS server 2*:** Set the secondary DNS for your network or the internet;
- ***Gateway*:** Set the default route for the network. Ex .: 176.16.102.1;
- ***Integrity key*:** System integrity key, used in the encryption process of backup files. This field is automatically generated.

3. Enter the following data in the "Certificate" frame, this information will be used to create the SSL certificate in the Blockbit NGFW administration console:

- ***Country*:** Define the country. Ex.: *US*;

- ***State*:** Define the state. Ex.: *New York*;
- ***City*:** Define the city. Ex.: *New York*;
- ***Organization*:** Set your company name. Ex.:Blockbit;
- ***E-mail*:** Set the administrator email. Ex.: admin@blockbit.com;
- ***Organizational Unit*:** Define the department. Ex.: QA;
- ***Expires (years)*:** Set the certificate validity time. Ex.: 10 anos;
- ***Hostname*:** Set the FQDN for the certificate. Ex.: utm.blockbit.com.

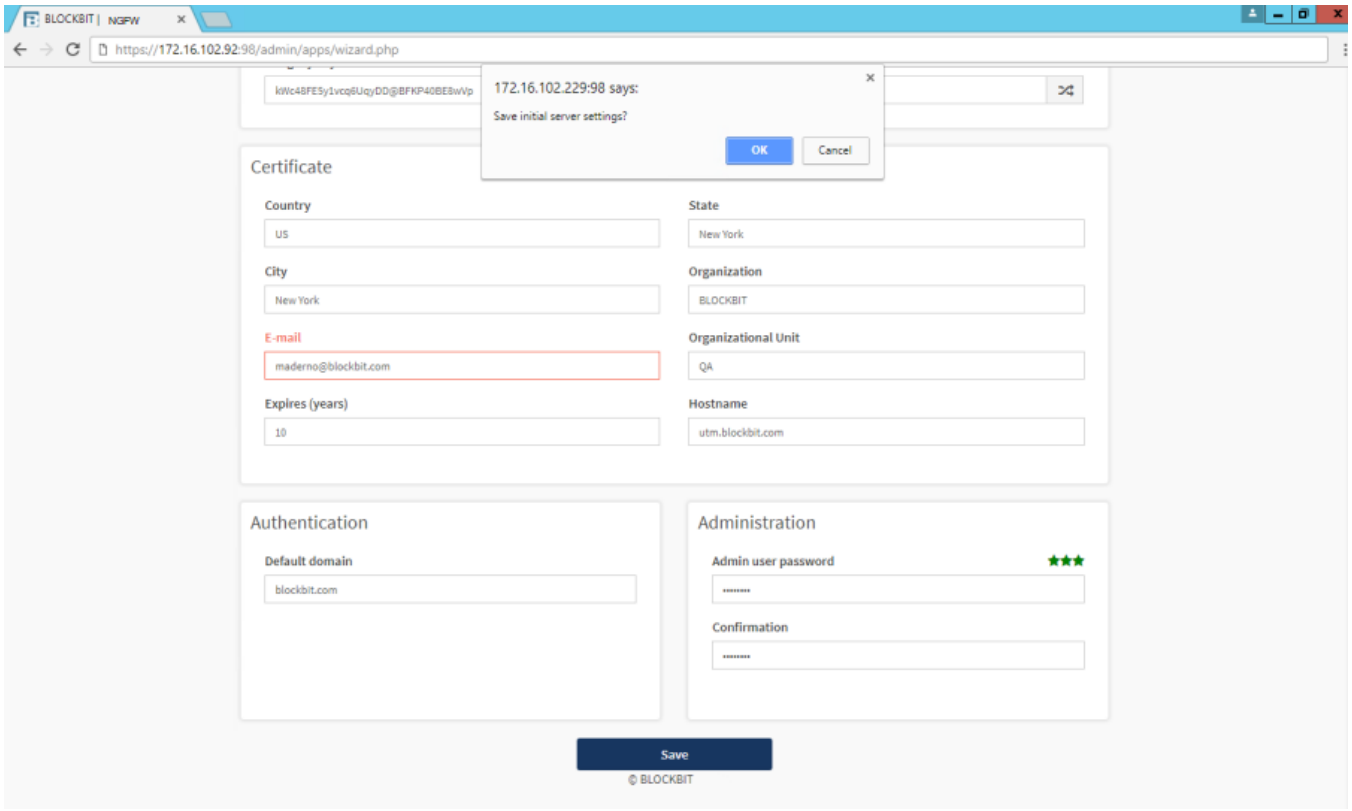
4. Enter the following data in the "Authentication" frame, define the default local domain for authentication of Blockbit NGFW users.

- ***Default domain***: Defina o domínio *default* de autenticação. Ex.: blockbit.com.

5. Enter the following data in the "Administration" frame, the password for the "admin" user of the Blockbit NGFW administration console:

- ***Admin user password***: Enter a password of at least eight characters. The password must contain uppercase, lowercase letters and special characters. Ex .: q1W @ e3R $;
- ***Confirmation Save***: Confirm the password entered above.

6. Click the "Save" button. The screen below will be displayed asking for confirmation, when clicking "ok" the system will apply the settings and will be restarted.



Installation Wizard – Form

- Click the "OK" button. The system will apply the settings and be rebooted.

After completing these steps, the Installation Wizard will have been successfully completed.
Wait for initialization, the browser will AUTO-REFRESH the address of access to the WEB interface and return to the login interface.

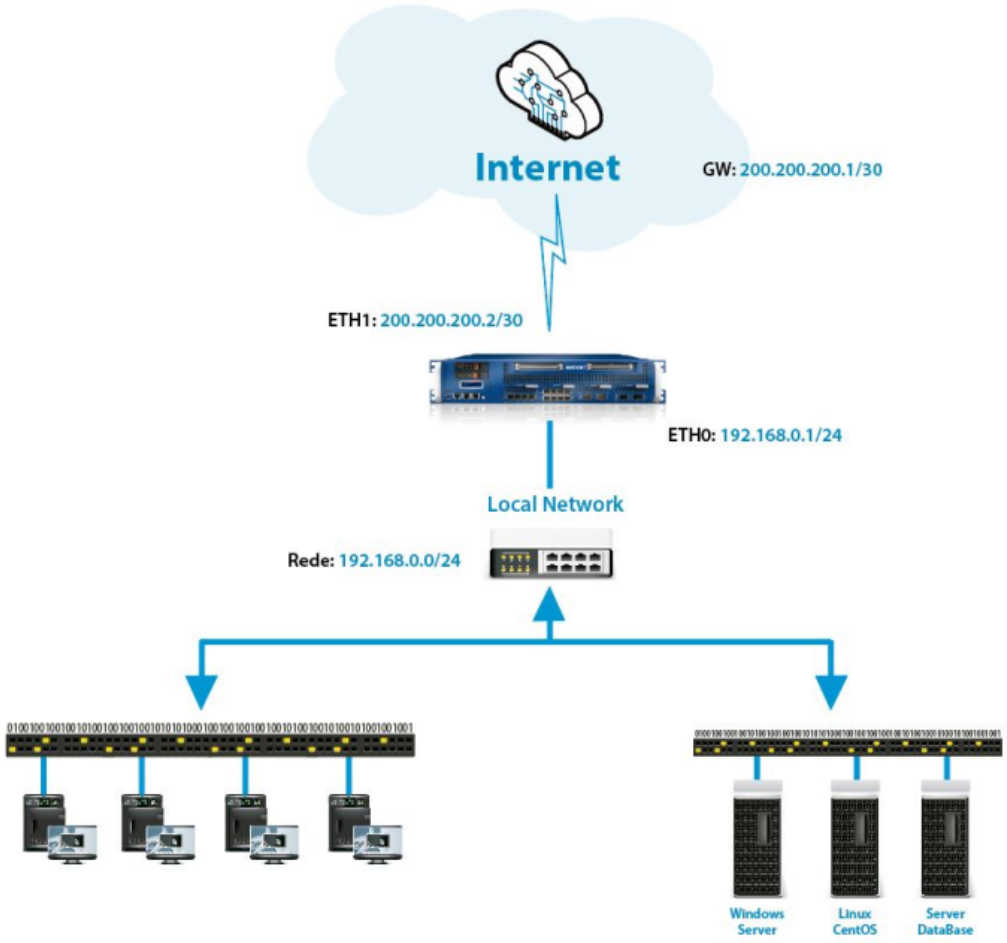
BLOCKBIT NGFW administration LOGIN screen

UTM - NETWORK ENVIRONMENT

This section will present an example of a network environment. In Blockbit NGFW, you can install two server configurations: Standalone and H.A. For better contextualization, we will use a fictitious topology, but very common among the likely environments that should use Blockbit NGFW.

Blockbit NGFW – *Standalone*

In this configuration, only one dedicated server is installed.

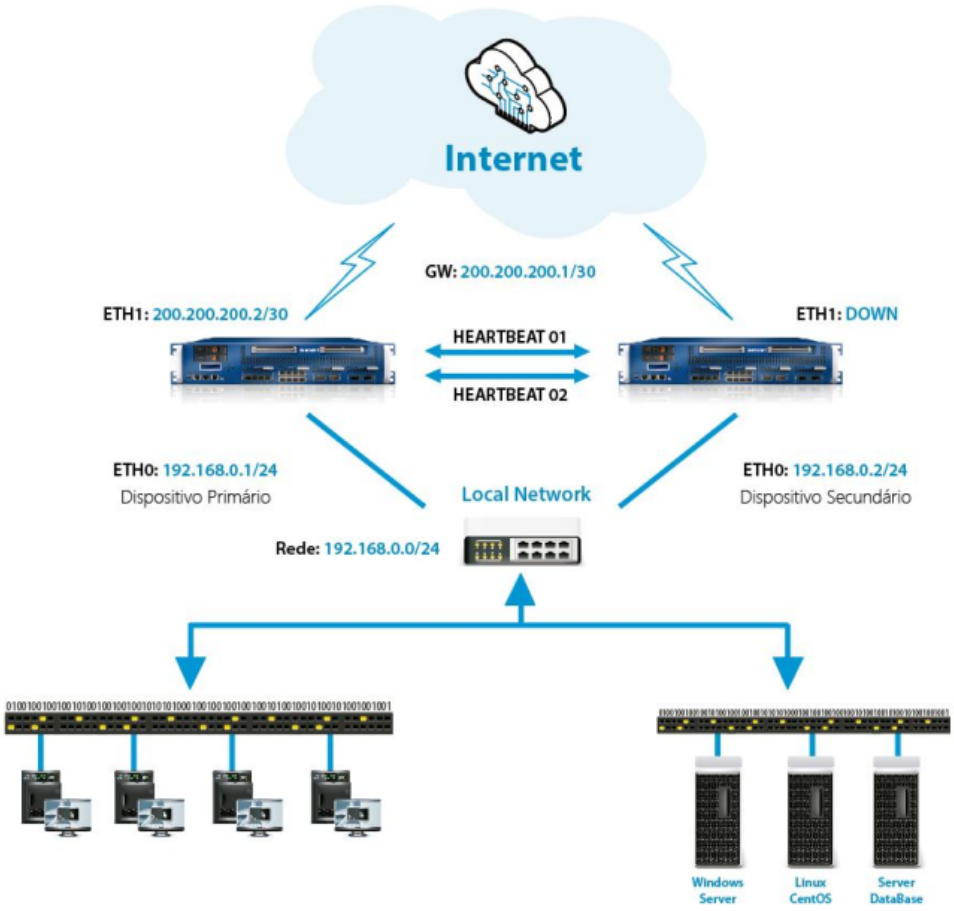


Network topology - Blockbit NGFW Manager

The advantages of using this topology are: Machine savings and ease of implementation.

Blockbit NGFW – *H.A.*

In this configuration, two servers are installed. That is, a Primary server and a Secondary server.



Network topology - Blockbit NGFW H.A.

The advantages of using this topology are: High availability and flexibility.
To illustrate the Blockbit NGFW installation and configuration process, during this manual we will create a network based on the following IP addressing table as an example:

Table 1 – IP addressing

NAME	EXTERNAL IP ADDRESS	INTERNAL NETWORK
Blockbit NGFW	172.16.102.93	172.16.102.0/24
Windows Server	172.16.102.81	172.16.102.0/24
Linux CentOS	172.16.102.39	172.16.102.0/24
Windows 7	172.16.12.223	172.16.12.0/23
Windows 10	172.16.12.224	172.16.12.0/23
Site	www.blockbit.com	104.239.173.143/32

UTM - WEB INTERFACE

This section will demonstrate how to access the Blockbit NGFW Web Interface.
Blockbit NGFW has a modern interface, easy to use and responsive, that is, it is able to adapt to the screen of any device used for access (tablets, smartphones, notebook, etc.). This ensures agility and ease for your company, being accessible at any time and place.

To access the Blockbit NGFW Web Interface, follow the guidelines on this page.

To license the NGFW, check this page.

Accessing the Web Interface – Blockbit UTM

Use one of the recommended browsers.

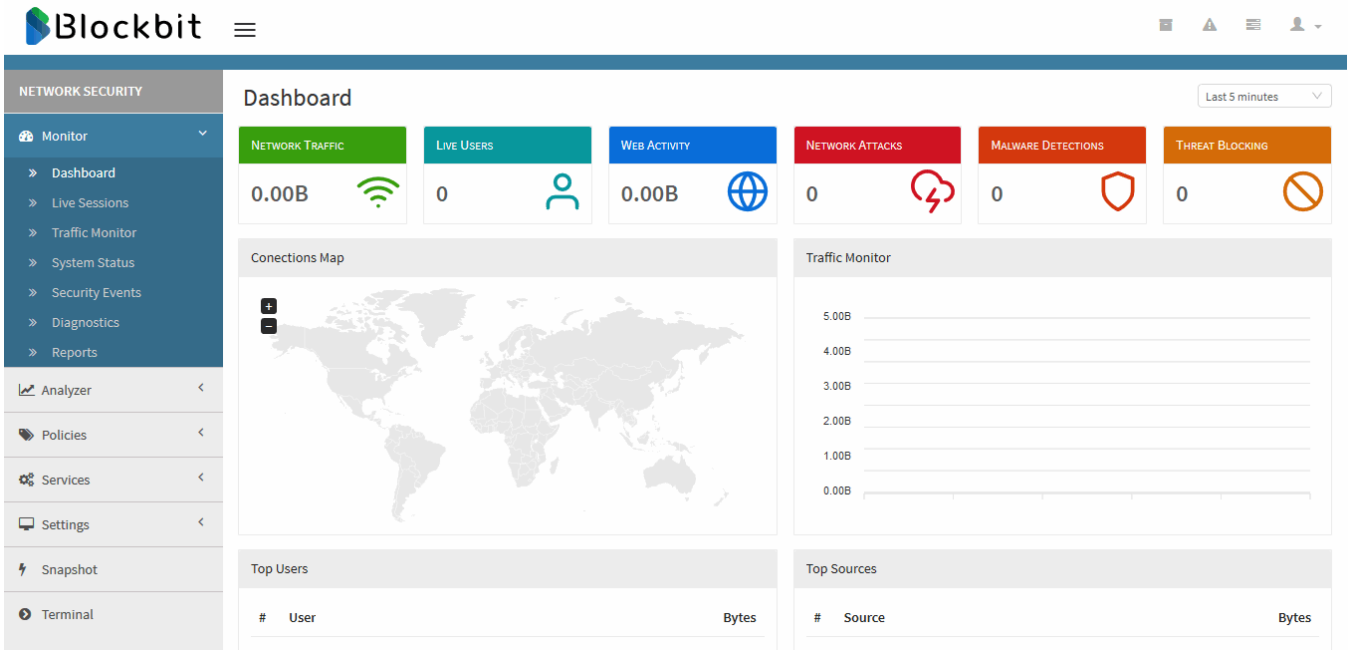
1. Connect to the internet and access the address: https://172.16.102.136:98. If you have changed the IP address, use the latest IP;
2. Access using the following data:

- ***User*:** The registered user's login, in addition, if the email has been registered, it is possible to use it to login. Eg: admin;
- ***Password*:** Registered password;
- ***English*:** The desired language is defined to access the Web Interface. The available languages are English and Portuguese. Ex.: English.

Login screen – Blockbit NGFW

- Click the [Login] button to access the Web Interface.

The main screen of the Blockbit NGFW will be displayed, called Dashboard.



Blockbit NGFW main screen – *Dashboard*

For more information on Licensing, click on this page.

If you want to see more information about the web interface, click on this page.

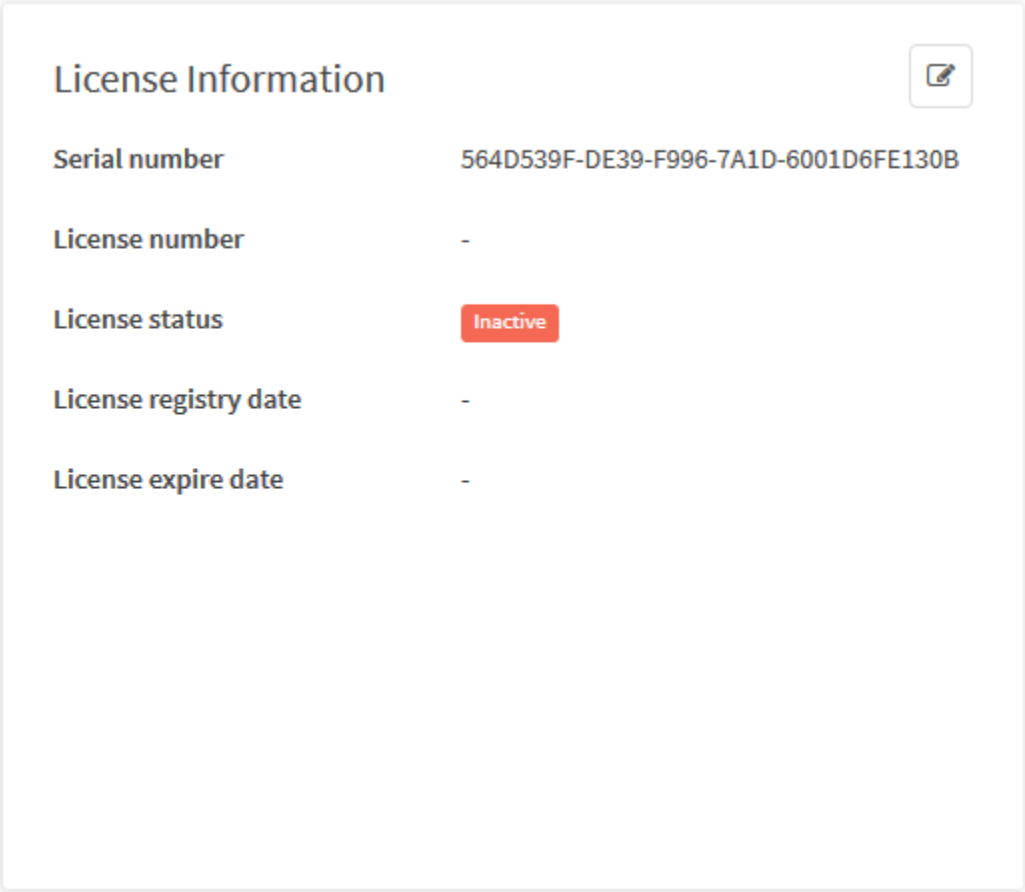
Accessing the Web Interface – Licensing

To use the features of Blockbit NGFW it is necessary to license your installation, follow the steps below:

To license Blockbit Network Security, you must be connected to the internet and have access to Port 443 without a proxy at the following addresses:
https://license.blockbit.com
https://update.blockbit.com

To apply or renew the activation license it is necessary to provide the UUID - Universal Unique Indicator of your Blockbit NGFW.

1. To view the UUID of your device, access the Settings menu, on the System tab:



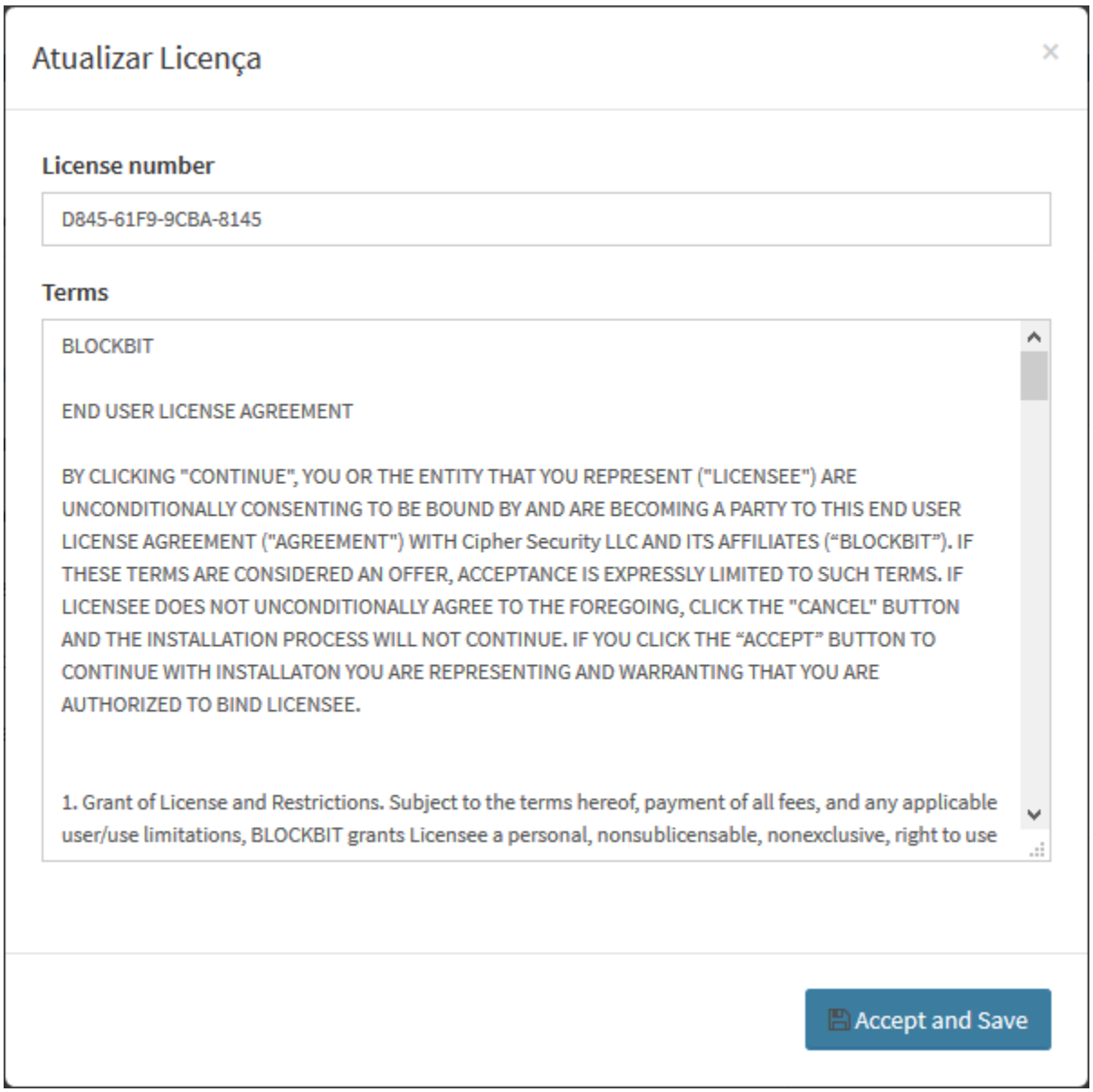
Dashboard – System

- The License Information widget will inform the Serial Number (or UUID): Ex.: 564D539F-DE39-F996-7A1D-6001D6FE130B.

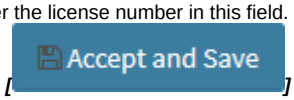
It is also possible to discover the UUID using the "show-uuid" command on the console. For more information check this page: [show-uuid].

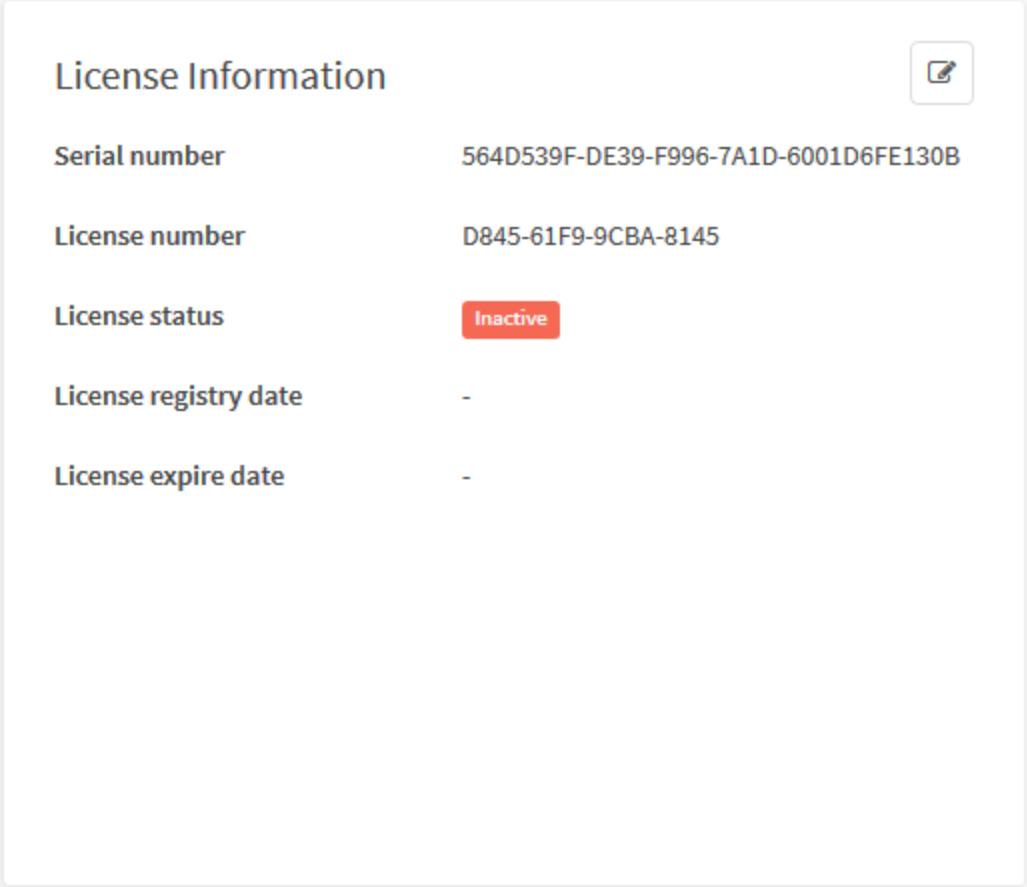
- Copy the UUID and forward it to your service channel, so that your license number is provided;
- You will receive the License number code from your service channel. Ex .: D845-61F9-9CBA-8145.

2. Click on [ ], the screen below will be displayed:



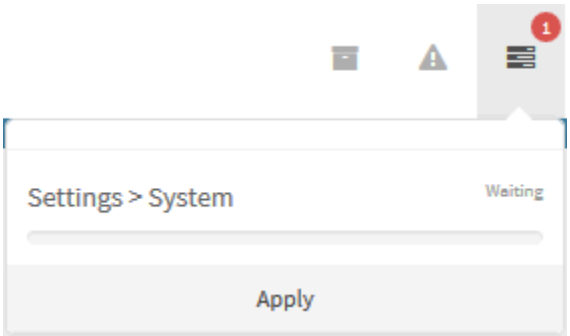
Update License

- ***Serial Number*:** Enter the license number in this field. Ex.: D845-61F9-9CBA-8145;
- After that click on the ***[***  ***]*** button the screen below will be displayed

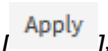


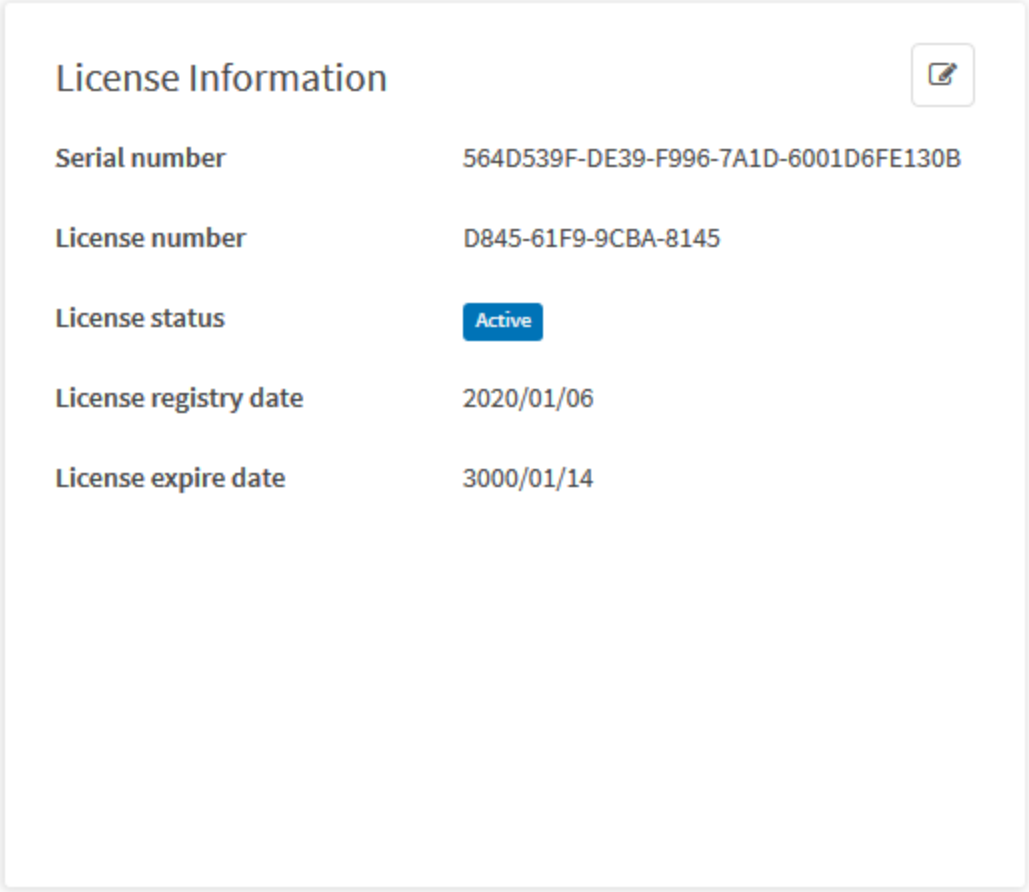
Update License - Inactive

After saving the license, the request will be sent to a command queue where it can be applied on the system. To access the command queue, click **[**  **]** . The screen below shows the command queue waiting to be run;



Apply queue

- After clicking ***[***  ***]***, wait until the system applies the settings for product licensing. As shown below:



Update License - Active

This concludes the product licensing.

ATTENTION: If the equipment is not connected to the licensing system for 180 days, then the Blockbit NGFW will have its licenses deactivated. To reactivate the license it is necessary to contact Blockbit'S official channels and request the license release.

For more information on Basic NGFW Operation, click on this page.

If you want to see more information about the web interface, click on this page.

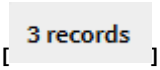
UTM - BASIC OPERATION

Blockbit NGFW is composed of some basic functionalities that are available in several different panels, in order to facilitate its use, follows a basic guide on how to use these resources:

Search bar

The search bar is located at the top of the panels and makes it possible to locate specific items.

Search Bar

In the records area **[** 

] displayed in front of the search bar, the amount of records found by the search or present is displayed before searching.

To remove the keywords entered in the search bar, click the **[** **]** button, if the search bar is blank, click the search **[**  **]** button to return to the initial screen

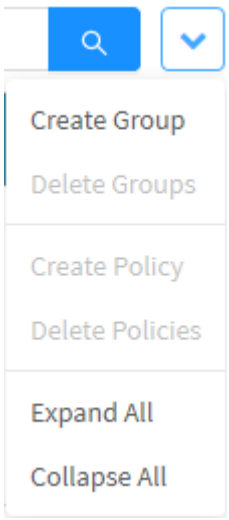
To perform the search, add the desired keyword and click the search button **[**  **]**.

Actions menu

The action menu is located at the top right of the panel:

Actions menu button

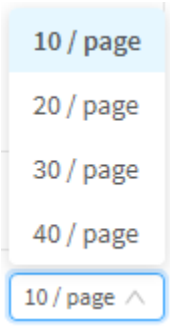
When clicking on this button, a menu with a set of contextual options to the panel where it is located will be displayed, for example:



Actions menu

Results per page

At the bottom of the screen, you can select how many results will be displayed per page, with a minimum of 10 and a maximum of 40 items per page.



Results per page

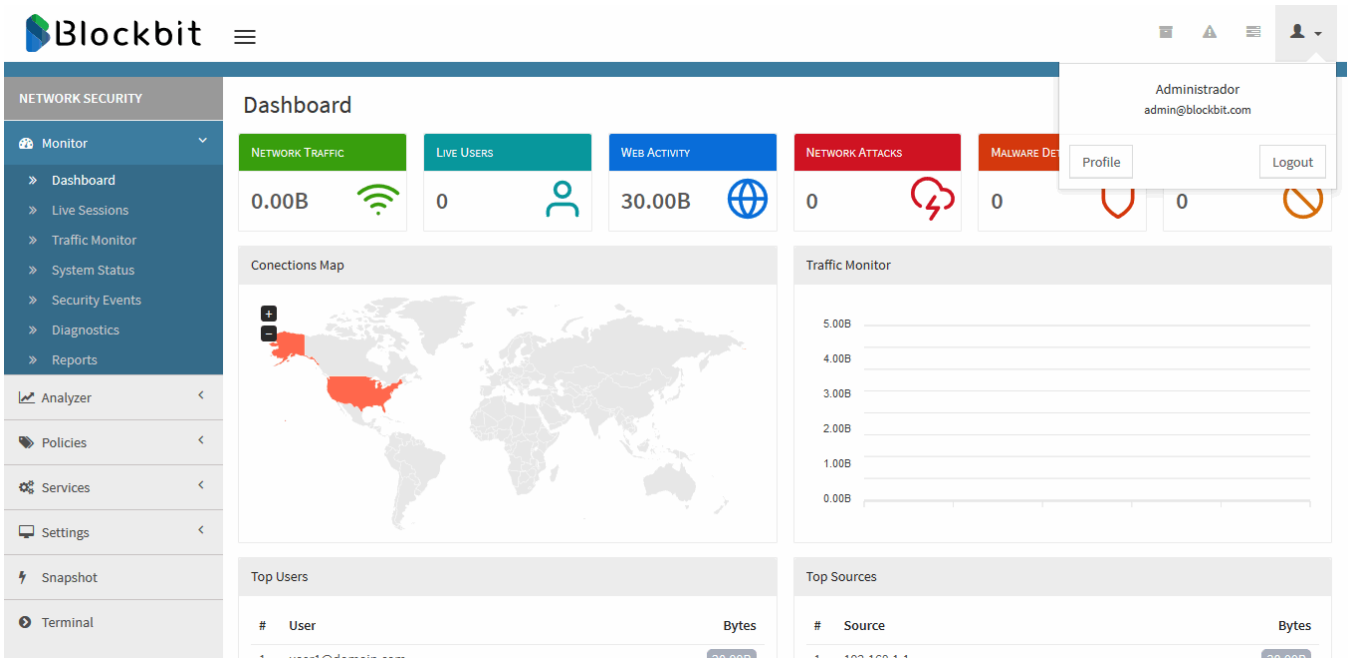
Finally, as for navigation, the “Navigation Page ” buttons allow the navigation through the pages.

Page Navigation

UTM - USER PROFILE MENU

The user profile menu is located in the upper right corner of the screen. To access, just click on the user icon [ ].

In the screen below the user menu appears under the “admin” name, this is because that was the name registered in the item “Name” in the *Installation Assistant chapter*.



User profile menu

The user profile menu consists of the options:

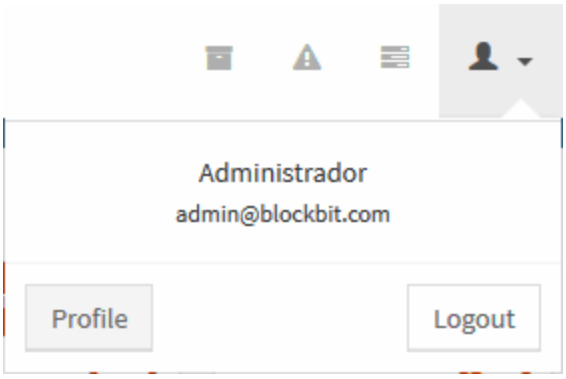
- *Profile*;
- *Logout*.

They will be explained in detail below.

UTM - Profile

In the “Profile” option, it is possible to edit the user's profile information. To access it, follow these steps:

1. At the top right corner. Click on the “Profile” option;

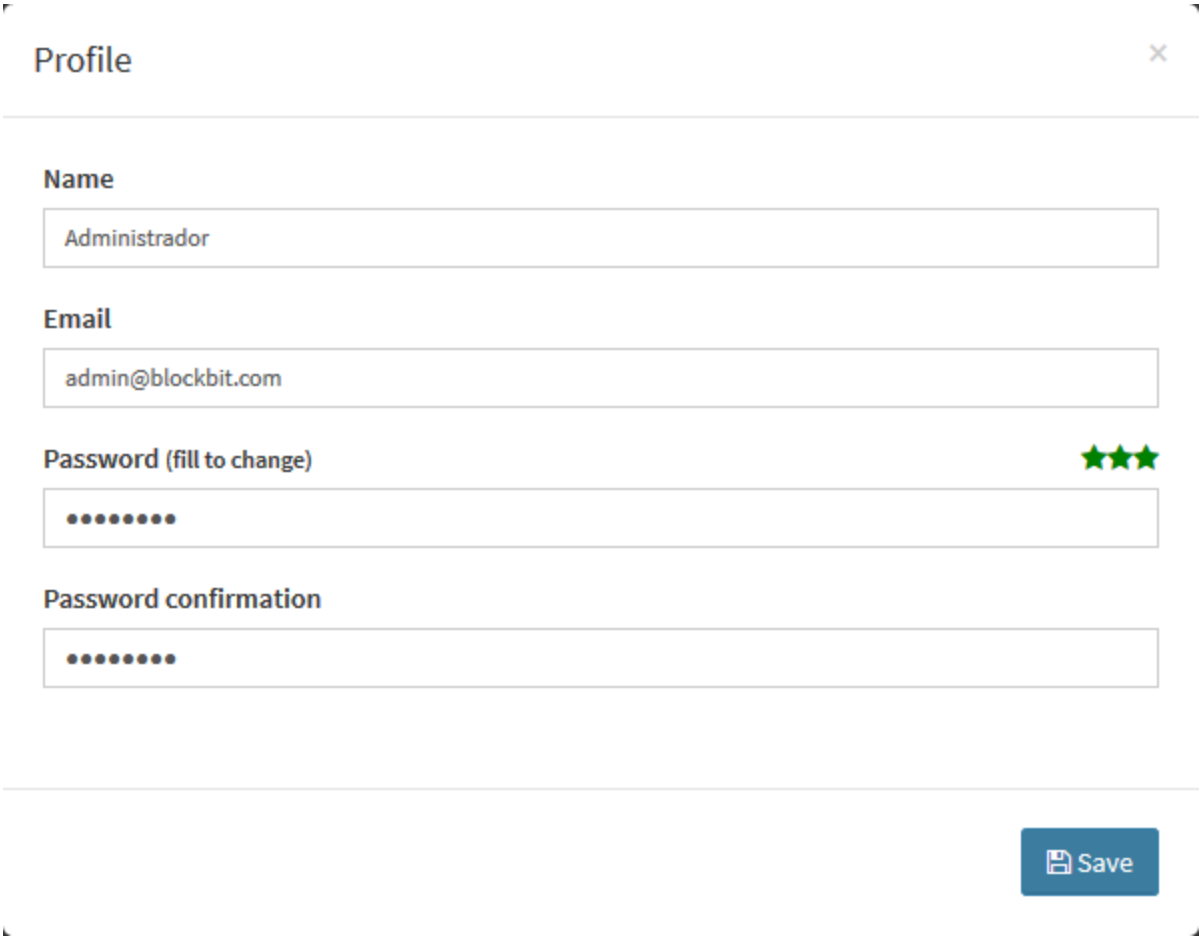


User menu - “Profile” button

2. Make the desired profile editing changes. This screen contains the following information:

- ***Name*:** The name of the registered user;
- ***Email*:** The registered user's email. This field is used to login to the Blockbit GSM;
- ***Password*:** If you want to change the password, enter it in this field;
- ***Password Confirmation*:** If necessary, confirm the password entered in the previous item.

The password must contain uppercase, lowercase, numbers, must be longer than 4 characters, and cannot contain the following special characters: " & | ; > < ' .



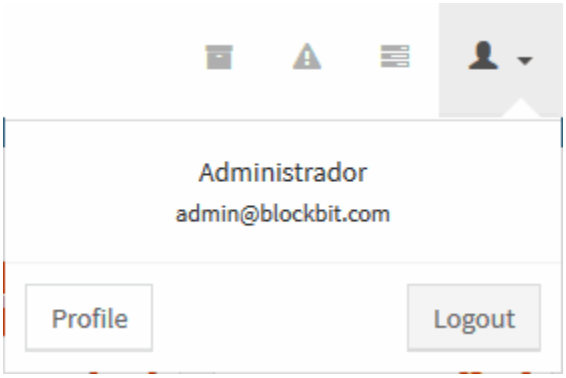
User menu - Edit Profile

To exit this window, just click **[** **]** at the top right of the screen to return to the previous window.

Click the **[**  **]** button to save the changes, if the password has been changed, the system will update and request that Login is performed again.

UTM - Logout

At any time it is possible to leave the system. Just click on the “Logout” button.



User menu - “Logout” button

This will take the user back to the "Login" page.

UTM - COMMAND QUEUE

When executing commands between the Frontend interfaces and the system's Backend services, all these instructions are ordered according to priority by the command queue, making sure that the settings are applied in the correct order.

To view the command queue, just click on the icon located at the top right of the screen, next to the user menu:

Command queue

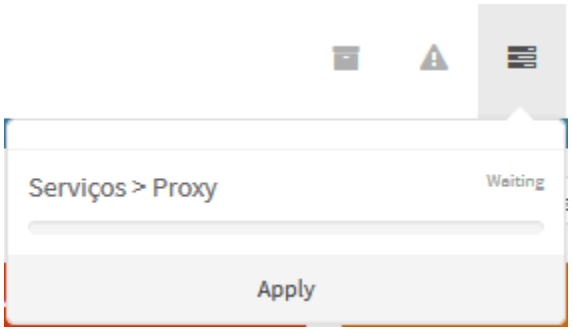
This section will demonstrate how to apply commands and changes made to Blockbit NGFW.

If the execution of any command is pending in the command queue, the icon will denote this showing with a red mark the amount of commands waiting:

Icon indicating pending commands

It is important to note that: The command queue always considers the last change made. Therefore, if you have regretted any configuration, just redo it and apply the command queue.

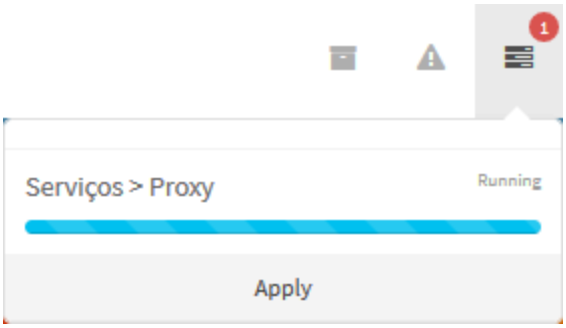
When clicking on the icon, a screen will appear listing everything that needs to be applied, as shown below:



Pending command queue

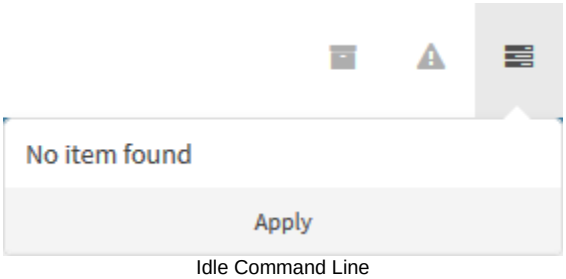
In this queue, the path to the command, its current status, the progress bar until its completion is displayed and finally, the apply button to execute all the commands in this list.

To apply all commands, just click on the **[** Apply **]** button, the process will start, as exemplified by the image below:



Command queue in progress

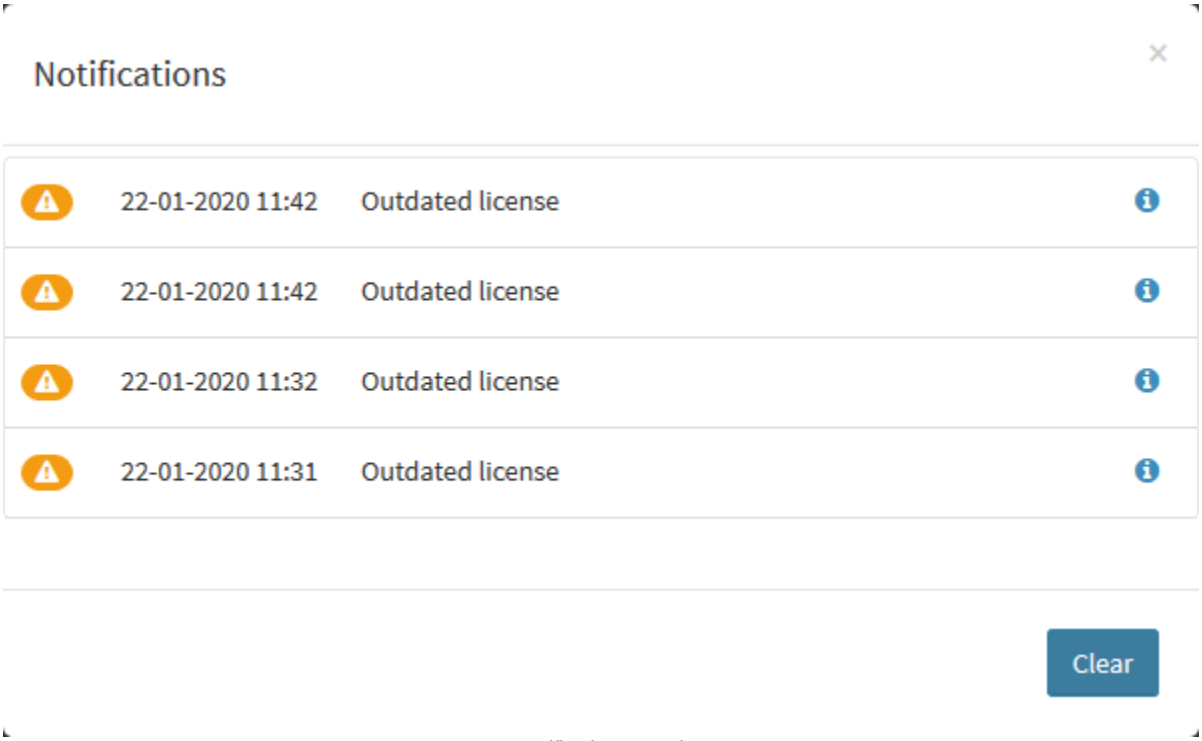
At the end of this process or if there is no command to be applied, the list will be displayed in white:



Idle Command Line

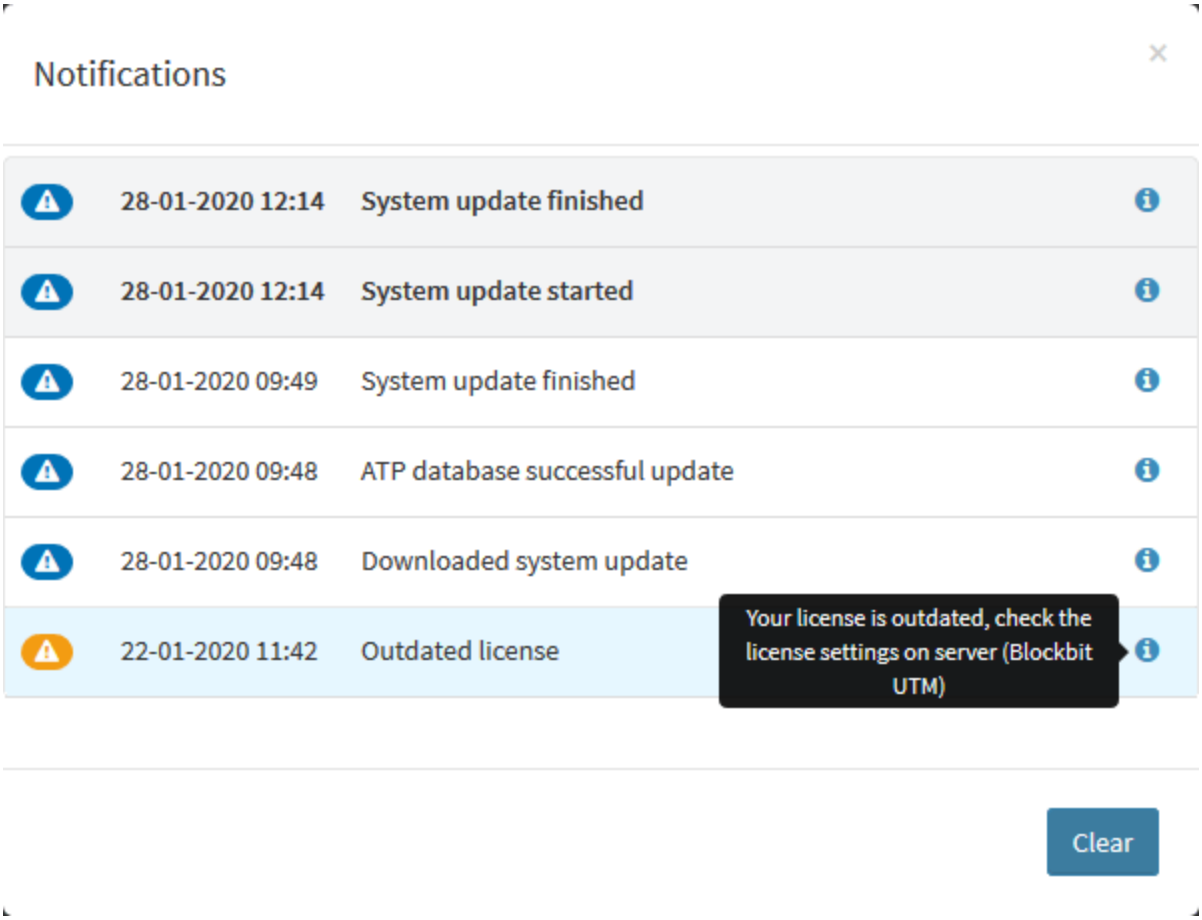
UTM - NOTIFICATIONS

Some events that will occur in Blockbit NGFW will generate alerts, these will be displayed in the notification panel, located in the upper right corner of the screen, next to the command line. To view notifications, click on the notifications icon **[ ]**.



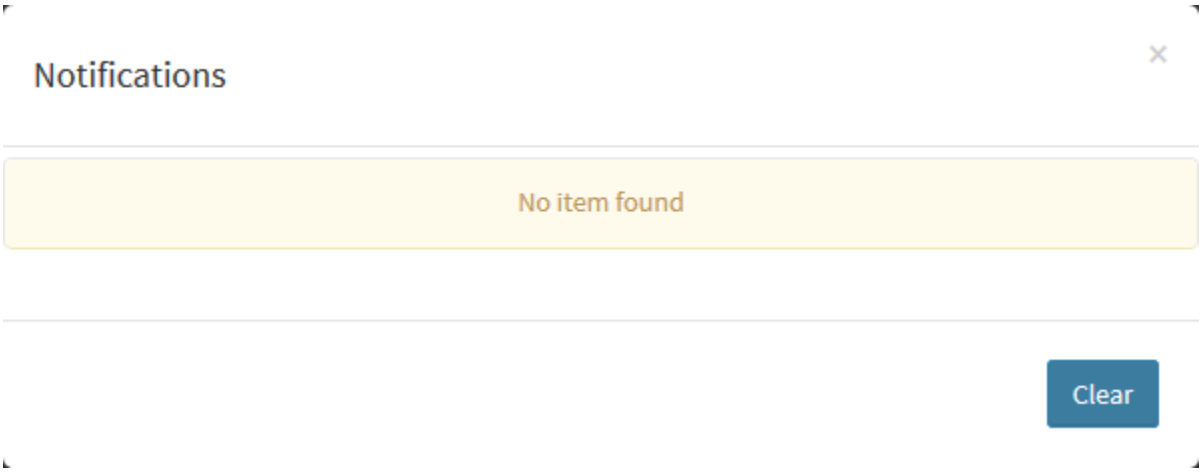
Notifications Panel

To learn more about the notification, leave the mouse over the information icon **[ ]**, a window with relevant details will be displayed:



Notifications Panel - Information

If you want to clear the notification panel, click the [Clear] button.



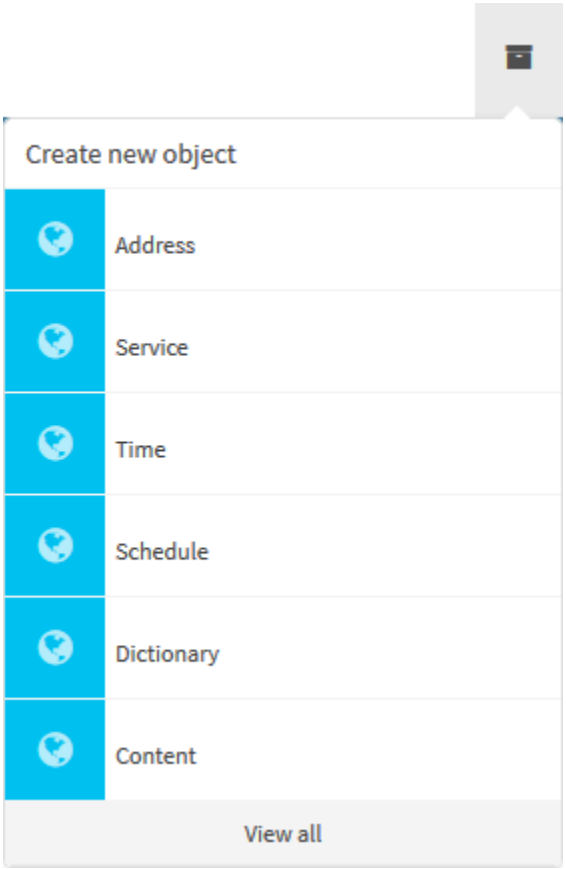
Notifications Panel - No item found

Finally, to close the window, click outside it or on the [×] located at the top of the screen.

UTM - OBJECT MENU

To speed up the Blockbit NGFW configuration process, at the top of the screen the objects menu provides the possibility to create an object immediately or access the objects panel.

To access the objects menu, just click on the objects [ ] icon.

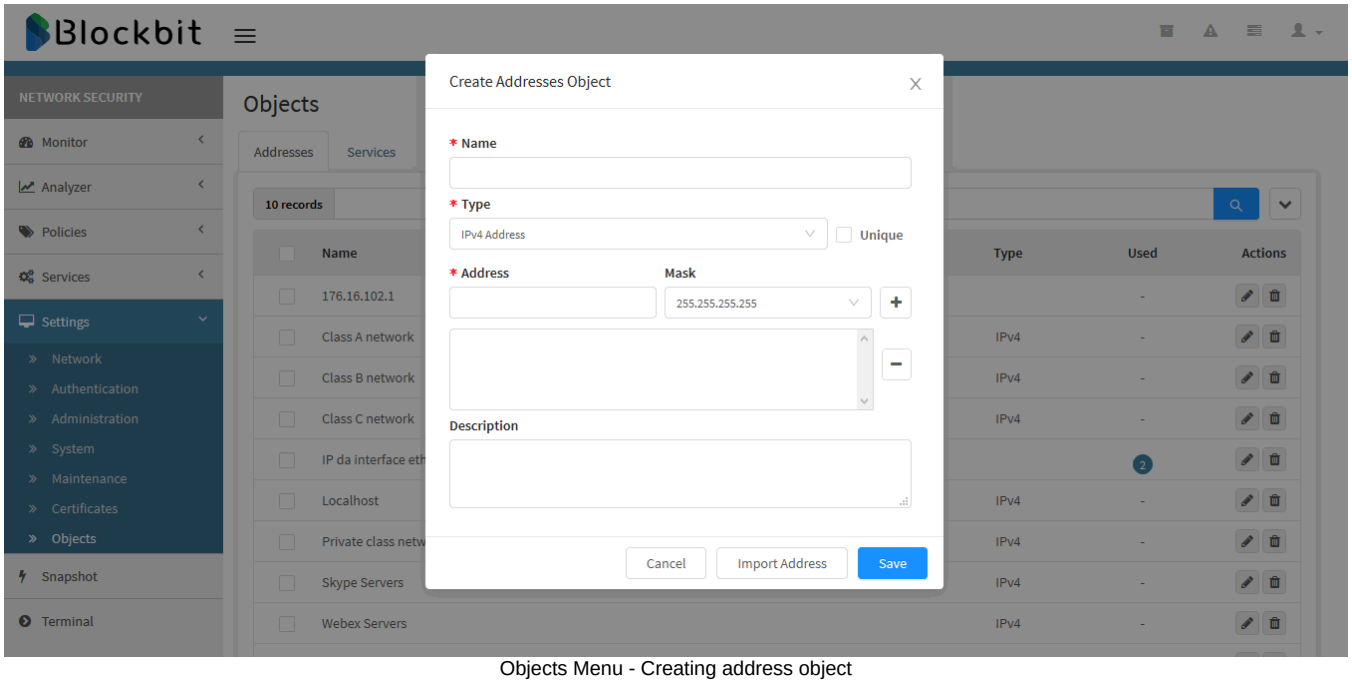


Objects Menu

The menu consists of all types available in the object panel:

- *Address*;
- *Services*;
- *Times*;
- *Schedules*;
- *Dictionaries*;
- *Contents*.

When you click on any of these options, an object creation window will appear identical to the one displayed in the object panel, for example:



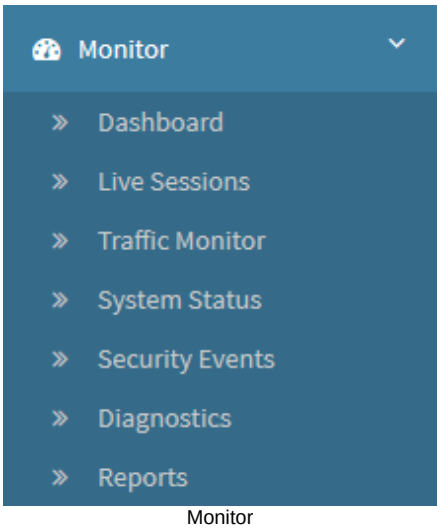
Objects Menu - Creating address object

Finally, when you click [View all], you will be redirected to the object screen.

UTM - MONITOR

In the Monitor, the information collected in the security modules is gathered and displayed in summary form by users, groups, services, policies, web filter, applications, threats, among others.

This feature provides a comprehensive and dynamic view of events on the network and its users, enabling more accurate management and facilitating decision making.
Through the Monitor, the administrator can quickly understand what is happening on the network, without spending time correlating thousands of log lines or events.



Monitor

Contains the options:

- *Dashboard*;
- *Live Sessions*;
- *Traffic Monitor*;
- *System Status*;
- *Security Events*;
- *Diagnostics*;
- *Reports*.

Monitor - Dashboard

The Dashboard displays in real time the current state of the system in a centralized and consistent way through various logs summarizing the main system events, user access history, traffic monitor and several other records that can be used for risk analysis, behavior and impact on bandwidth usage.

The Dashboard provides real-time access in a centralized and consistent way to several summarized logs, events of the main system services, user history and several other records.

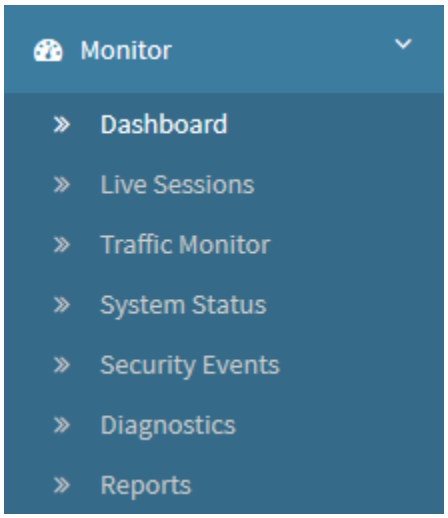
These resources can be used to analyze user behavior, risk and impact on bandwidth usage, it also displays alerts, notifications in real time and can be triggered through scheduling.

The Dashboard displays information for the last 5 minutes or the last hour.

The Dashboard displays information regarding the last 5 minutes or the last hour on your widgets (Traffic Monitor will always display the last 5 minutes thanks to it being a real-time monitor).

By default, all information in the detailed reports, for all modules, is stored for 7 (seven) days or until reaching 70% of disk usage. If the maximum storage capacity is reached, the retention of this information will be interrupted. If you want to change this storage limit, access System - Logging tab in settings.

When you log in to Blockbit NGFW, the "Dashboard" option in the "Monitor" menu will be automatically selected. If necessary, it is possible to access the “Dashboard” by clicking on the option located in the vertical side menu, as shown below.



Monitor – Dashboard

The screen below will appear:

Dashboard

Last 5 minutes

Network Traffic	Live Users	Web Activity	Network Attacks	Malware Detections	Threat Blocking
0.00B	0	0.00B	0	0	0

Conections Map

Traffic Monitor

Top Users

#	User	Bytes

No Data

Top Sources

#	Source	Bytes

No Data

Top Services

#	Service	Bytes

No Data

Top Policies

#	Policy	Bytes

No Data

Top Categories

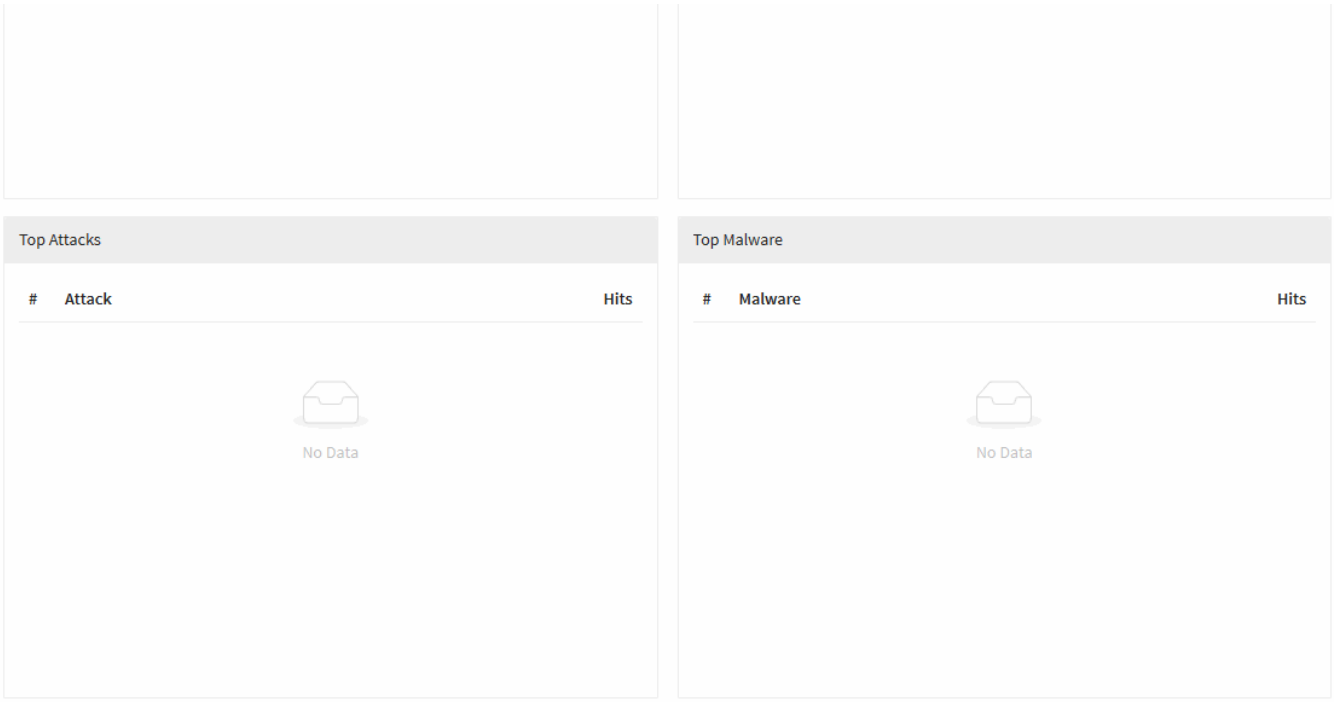
#	Category	Bytes

No Data

Top Applications

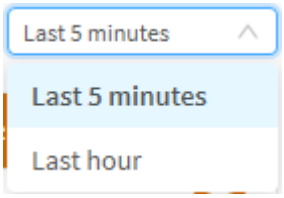
#	Application	Hits

No Data



Dashboard – Overview

The Monitor - Dashboard window allows you to display the information of the last 5 minutes or the last hour, through the menu located at the top right of this screen, as shown in the image below:



Dashboard – Menu

- ***Last 5 minutes*:** When selecting this option, all graphs will start showing the results for the last 5 minutes. By default, this option will be pre-selected;
- ***Last Hour*:** When selecting this option, all graphs will start showing the results for the last hour.

Traffic Monitor's function is to display information in real time and will always display the last 5 minutes. The 5 minute or 1 hour selection applies to other widgets that show summarized data.

The reports and graphs available on the Dashboard are:

- *Network Traffic*;
- *Live Users*;
- *Web Activity*;
- *Network Attacks*;
- *Malware Detections*;
- *Threat Blocking*;
- *Connections Map*;
- *Traffic Monitor*;
- *Top Users*;
- *Top Sources*;
- *Top Services*;

- *Top Policies*;
- *Top Categories*;
- *Top Applications*;
- *Top Attacks*;
- *Top Malware*.

Next, we'll look at each of the Dashboard components.

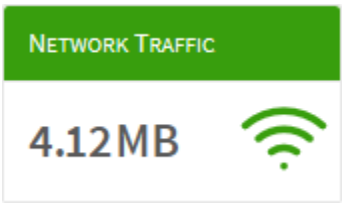
Dashboard - Widgets

The main function of the Dashboard is to provide a holistic view of the system in real time in a clear and objective way, for which the panel is composed of several widgets, focused on displaying specific data of the current state of the system.

Next we will analyze each one of them:

Network Traffic

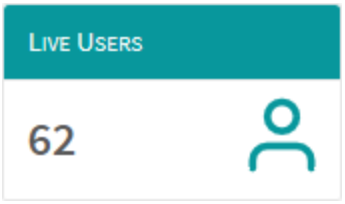
The "Network Traffic" widget displays the total volume of all network traffic carried out on all Blockbit NGFW network interfaces.



Dashboard – Network Traffic

Live Users

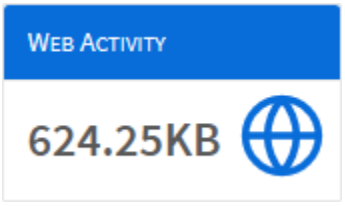
The "Live Users" widget displays how many users are currently online on Blockbit NGFW.



Dashboard – Live Users

Web Activity

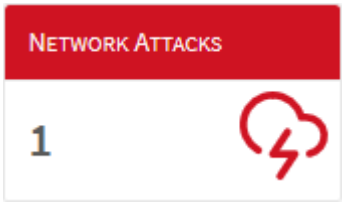
The "Web Activity" widget displays the total of all web activity performed in real time on Blockbit NGFW.



Dashboard – Web Activity

Network Attacks

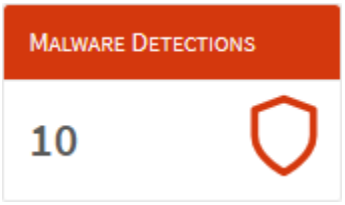
The "Network Attacks" widget displays the total volume of attack attempts performed on all Blockbit NGFW network interfaces.



Dashboard – Network Attacks

Malware Detections

The "Malware Detections" widget displays the total number of malware detected on all Blockbit NGFW network interfaces.



Dashboard – Malware Detections

Threat Blocking

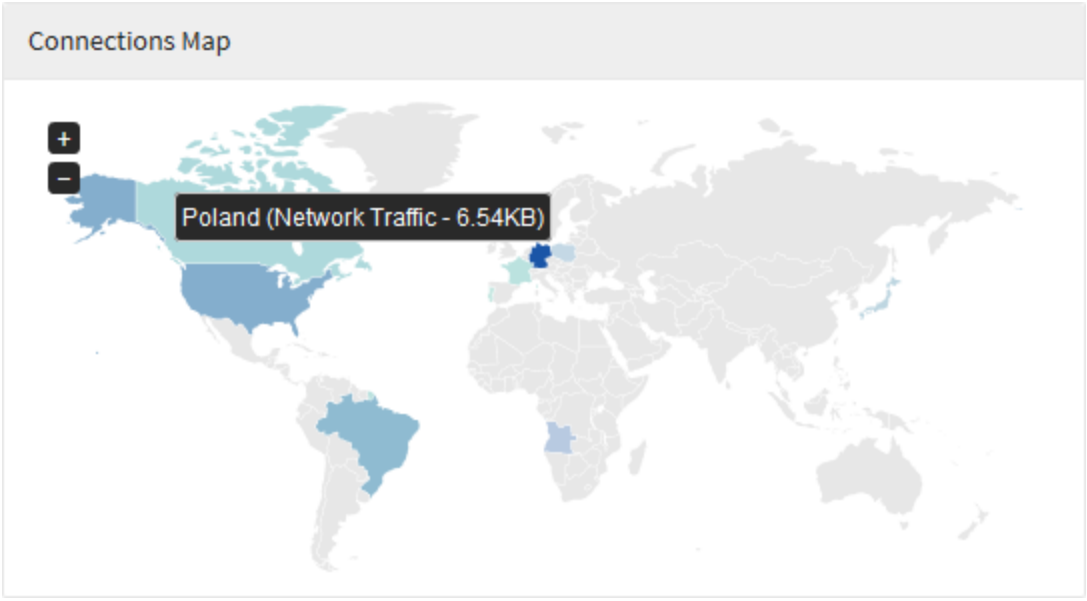
The "Threat Blocking" widget displays the total number of threats blocked using all Advanced Threat Protection (ATP) module techniques across all Blockbit NGFW network interfaces.

Dashboard – Threat Blocking

Connections Map

In “Connections Map” the destination of the connections of the network users is displayed, the global map shows in a colored legend the amount of accesses made by the users.

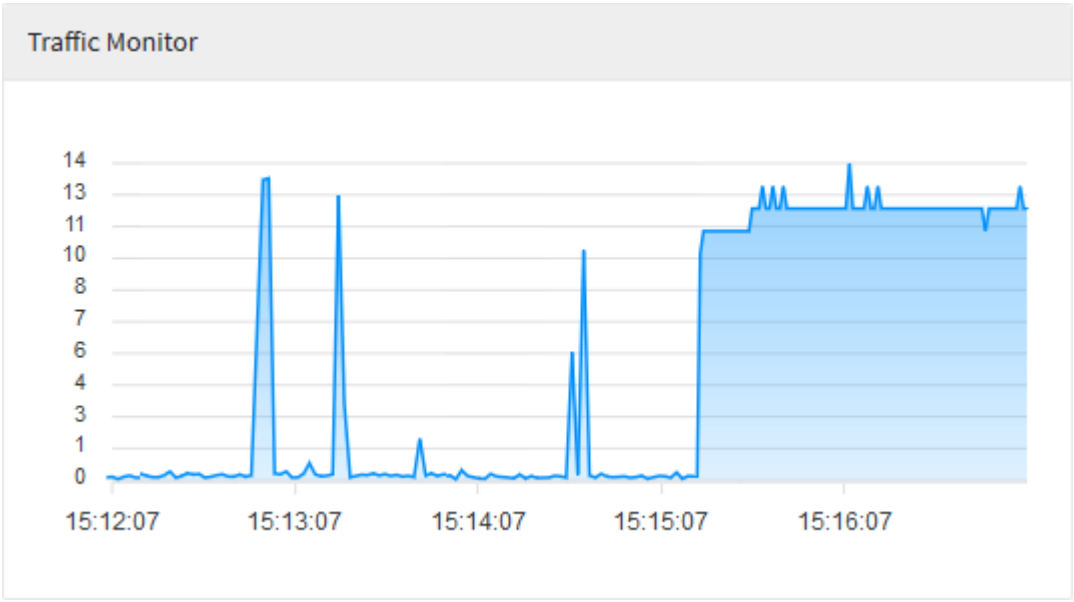
In addition, when hovering over the countries, the country for that value is highlighted on the map and a total number of accesses is displayed.



Dashboard – Connections Map

Traffic Monitor

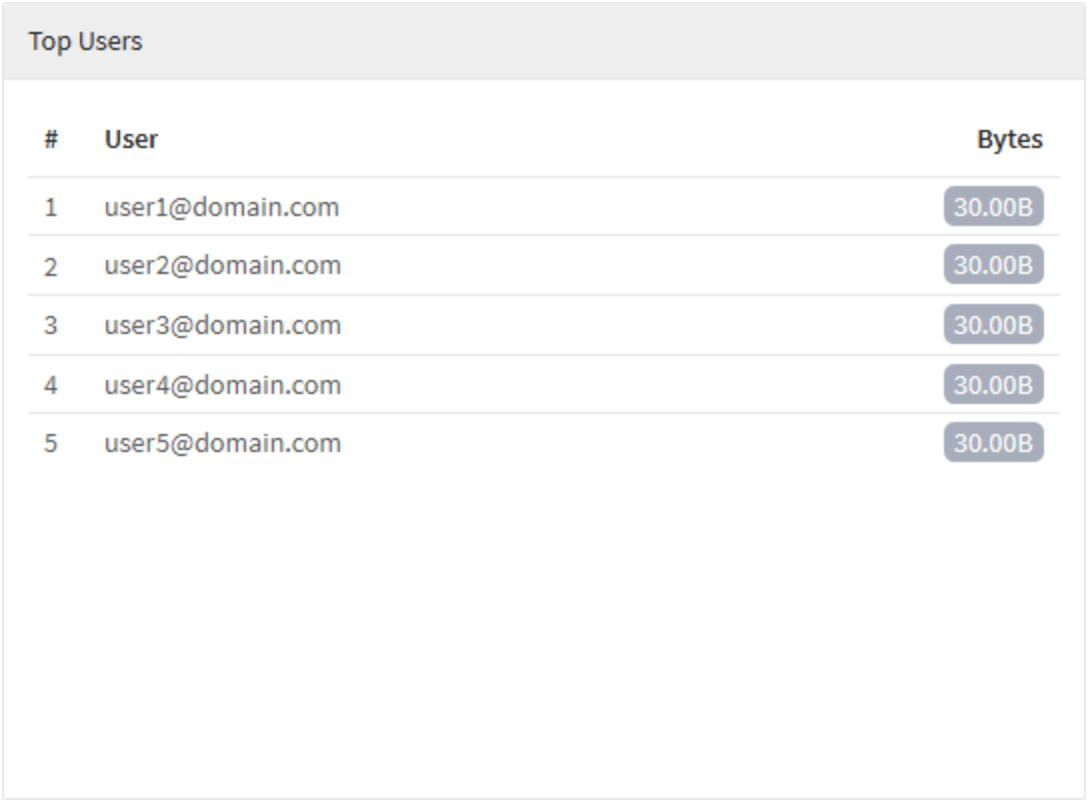
In “Traffic Monitor”, it is possible to view network traffic in real time. When you mouse over the graph, a summary of all traffic for the period is displayed.



Dashboard – Traffic Monitor

Top Users

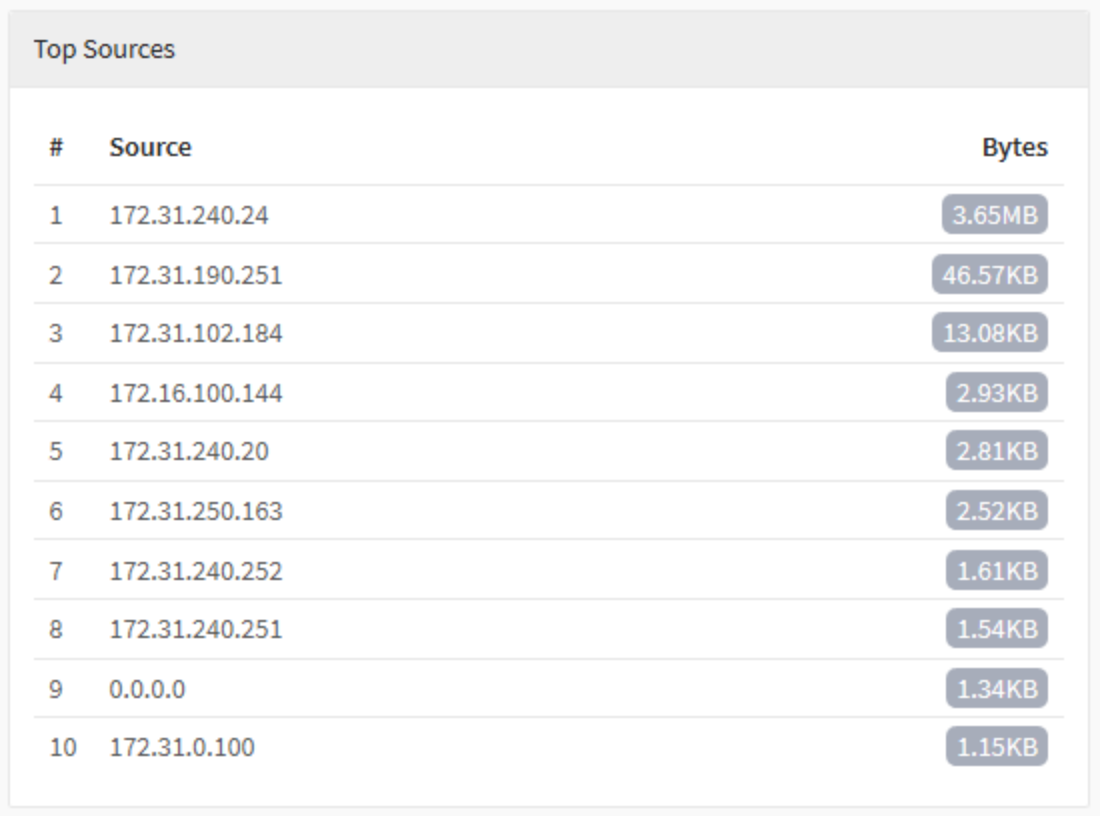
In “Top Users”, we have a list of ten users classified by order of the largest amount of accesses and their respective consumption and respective use.



Dashboard – Top Users

Top Sources

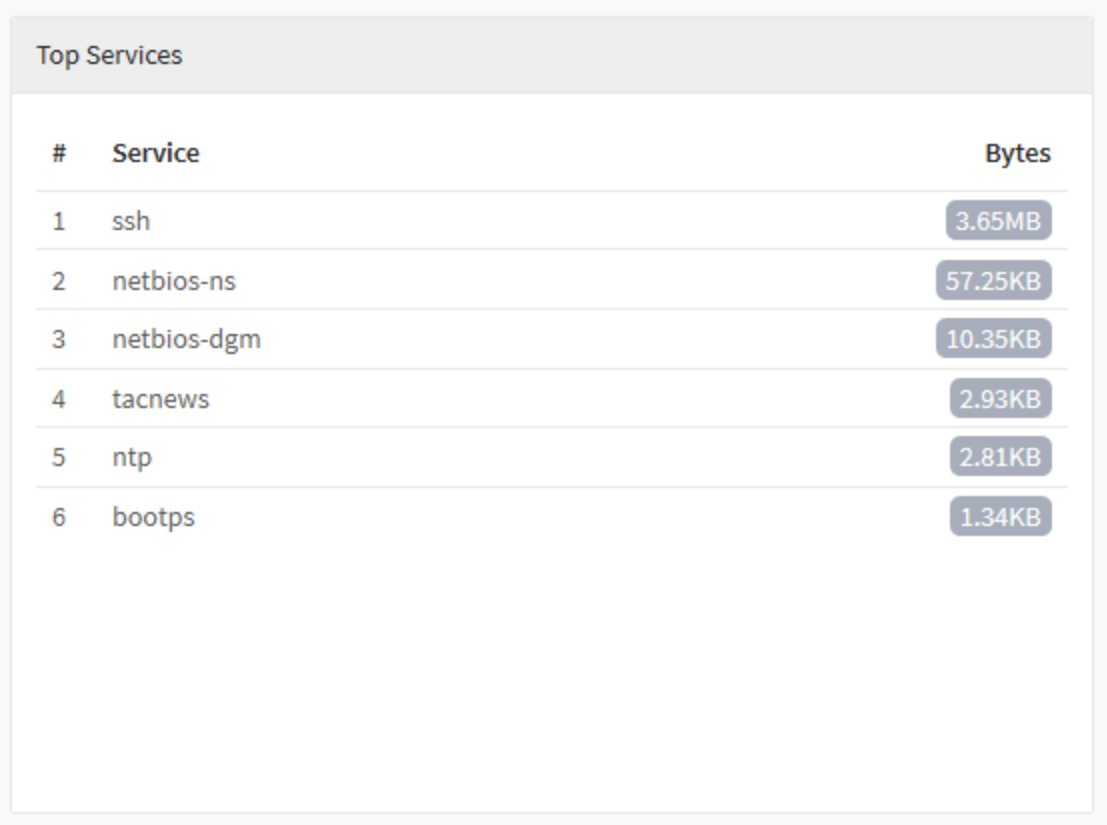
In “Top Sources”, we have a list of ten major sources of network traffic classified by order of access and their respective use.



Dashboard – Top Sources

Top Services

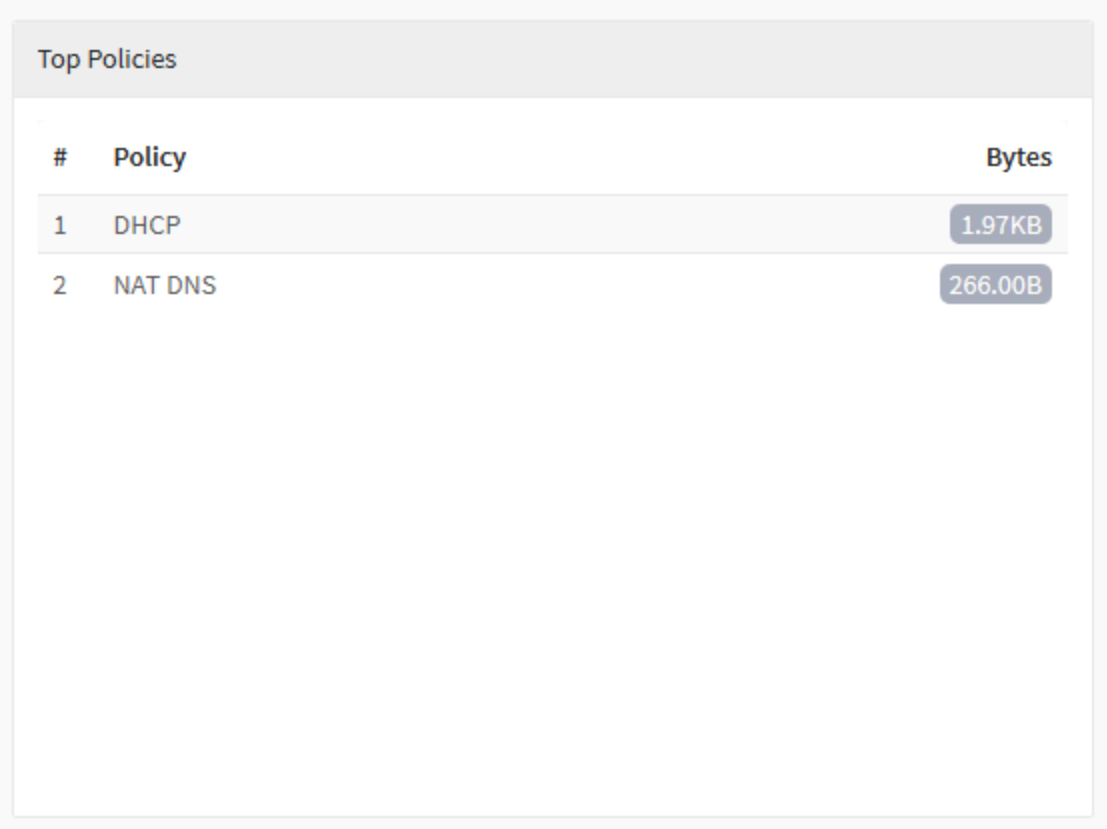
In “Top Services”, we have a list of ten types of services most used, these being classified by order of use.



Dashboard – Top Services

Top Policies

In “Top Policies”, we have a list of the ten most applied policies in order of the highest amount of use and their respective consumption.



Dashboard – Top Policies

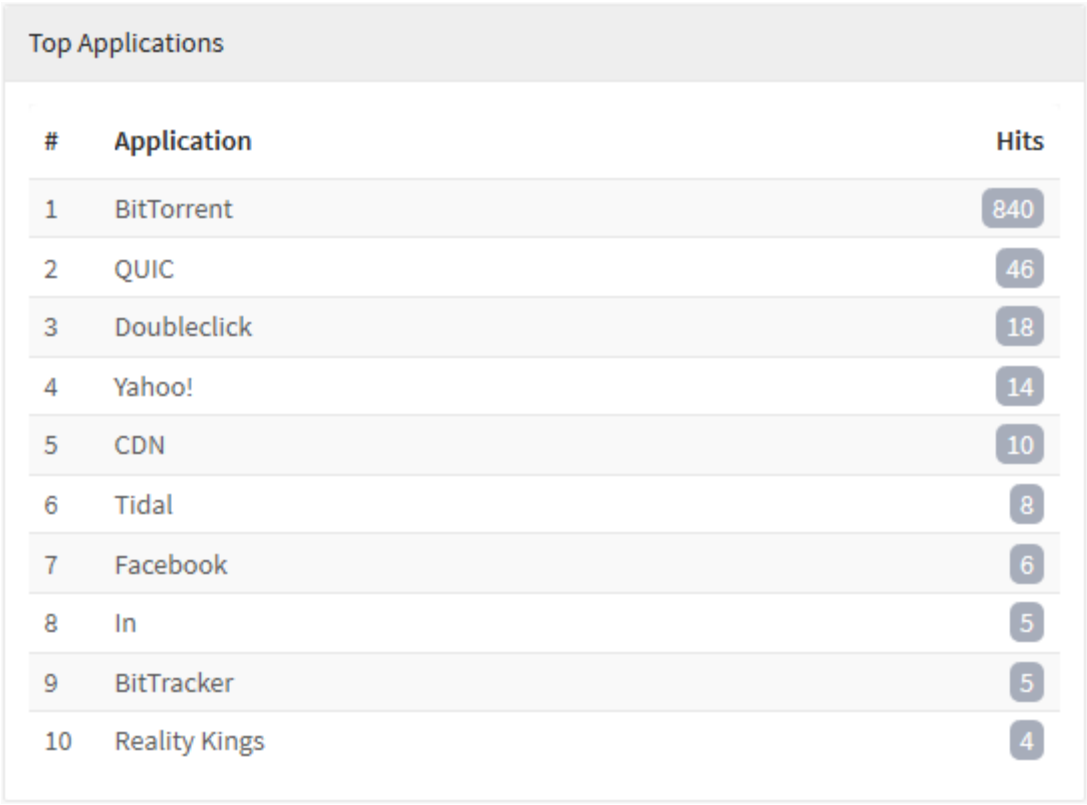
Top Categories

In “Top Categories”, we have a list of the ten categories classified in order of the highest amount of accesses and their respective use.

Dashboard – Top Categories

Top Applications

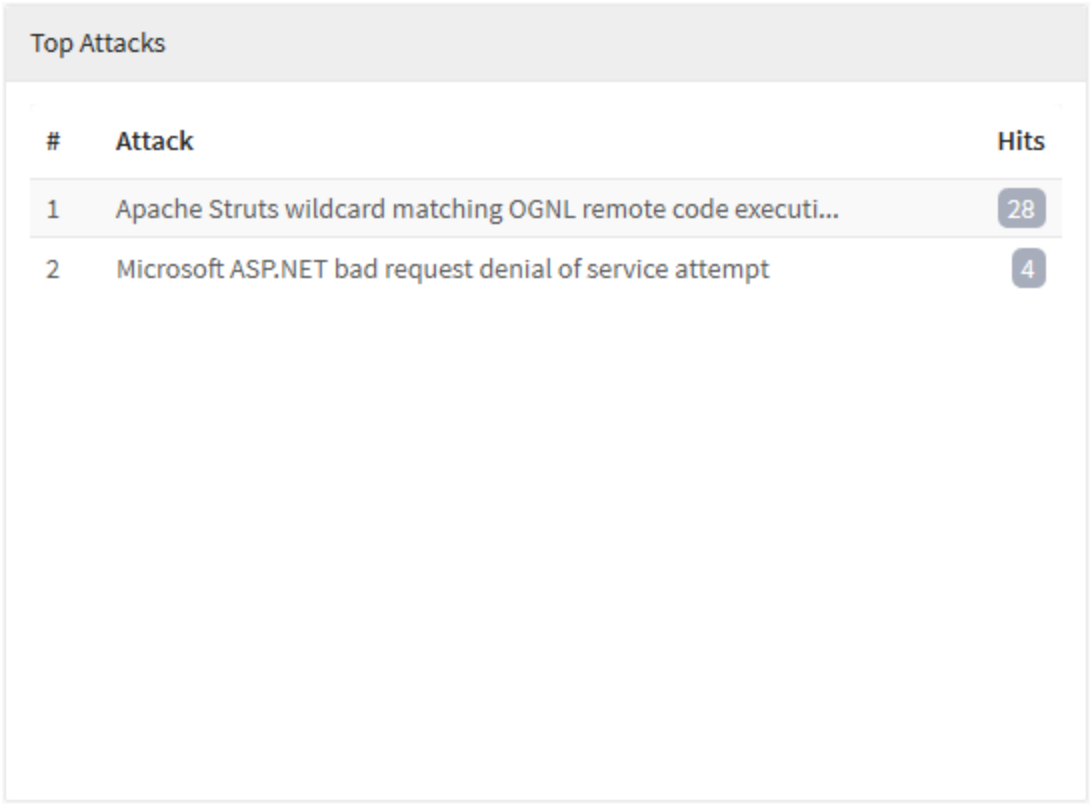
In “Top Applications”, we have a list of ten types of most used applications, which are classified by order of use.



Dashboard – Top Applications

Top Attacks

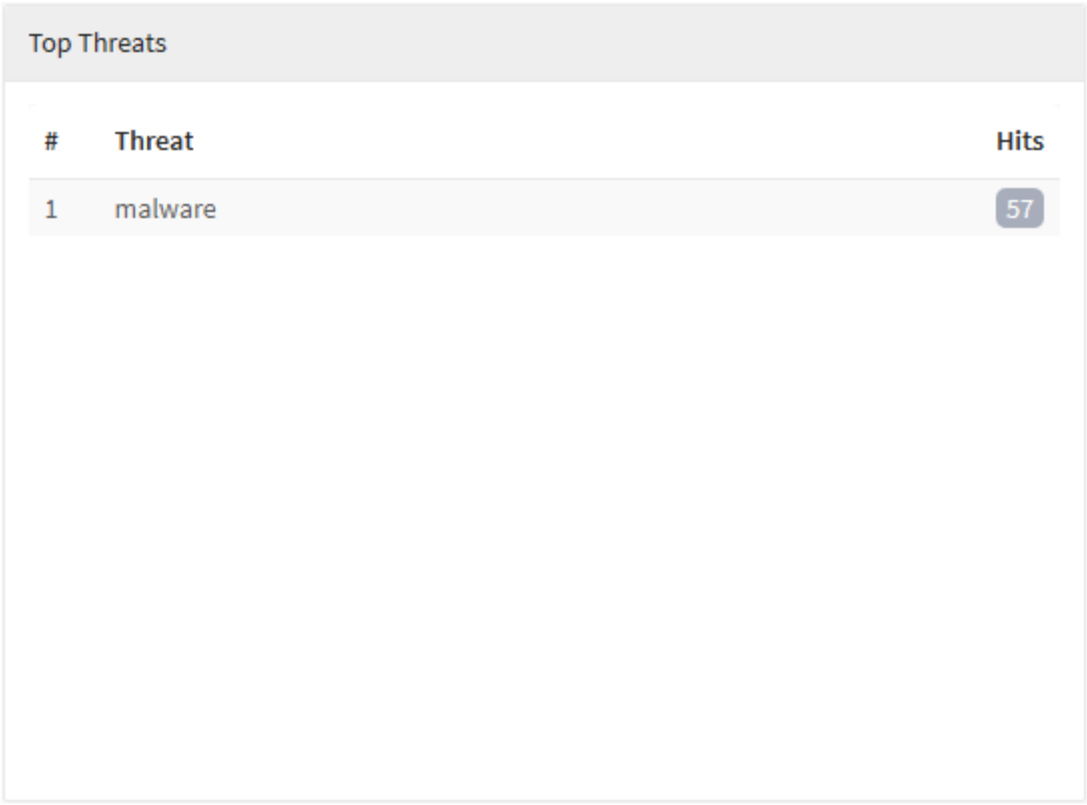
In “Top Attacks”, we have a list of the ten most recurrent types of cyber attacks, which are classified in order of occurrence.



Dashboard – Top Attacks

Top Threats

In “Top Threats”, we have a list of the ten most recurrent threat types, which are classified in order of occurrence.



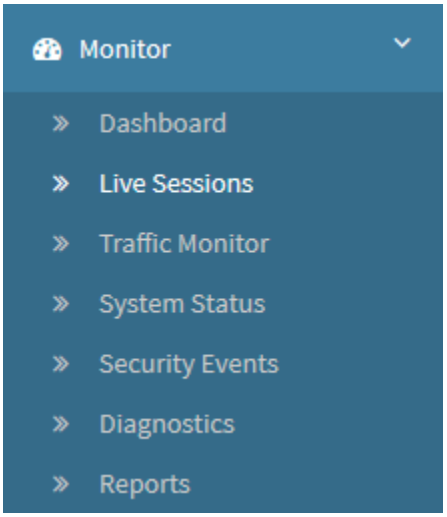
Dashboard – Top Threats

To access more specific reports, check the options available in the Analyzer.

Monitor - Live Sessions

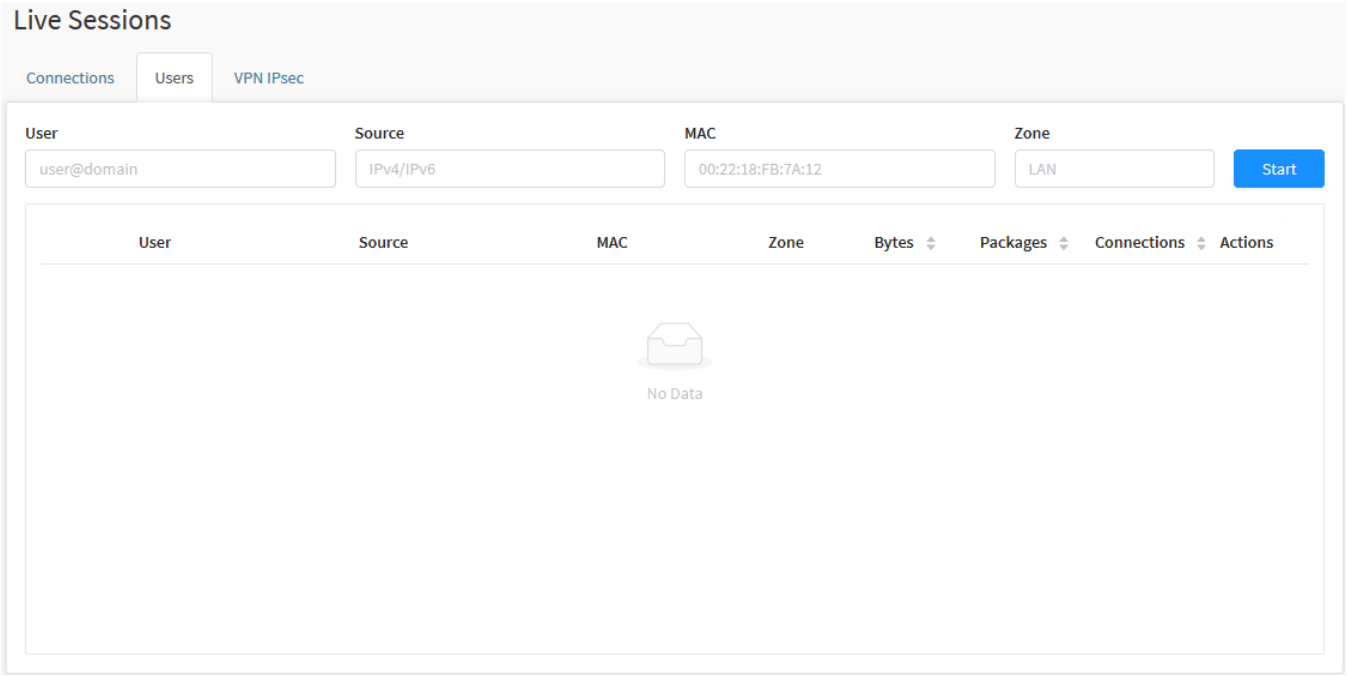
This feature allows the administrator to monitor network traffic in real time, determining with certainty which access (or attempt) generated the log. The system is divided into two types: Firewall and Web, the first monitors all traffic carried out on the firewall and the second monitors all web traffic.

To access this screen, just select the option “Live Sessions”.



Monitor – Live Sessions

The screen below will be displayed:



Monitor - Live Session - Live Connections

The Live Sessions screen has the following tabs:

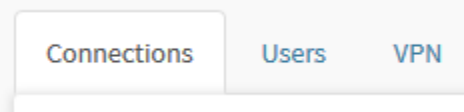
- *Connections*;
- *Users*;
- *VPN*.

Next we will analyze the components of the Live Connections tab.

Live Sessions - Connections

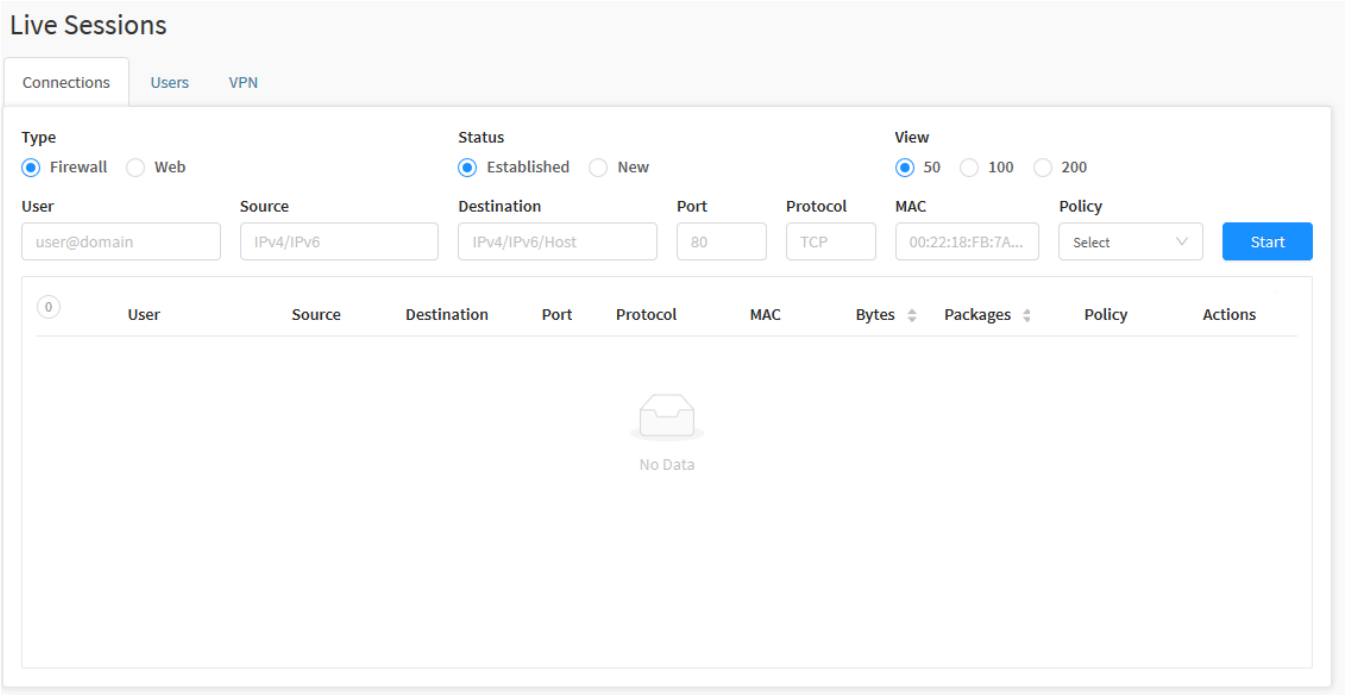
In this tab it is possible to check the current activity on the firewall and on the web, filtering by user, origin, destination, port, protocol or policy.

To access, if the tab is not selected, click on "Connections".



Connections tab

The “Connections” screen will appear, as shown by the image below:



Connections

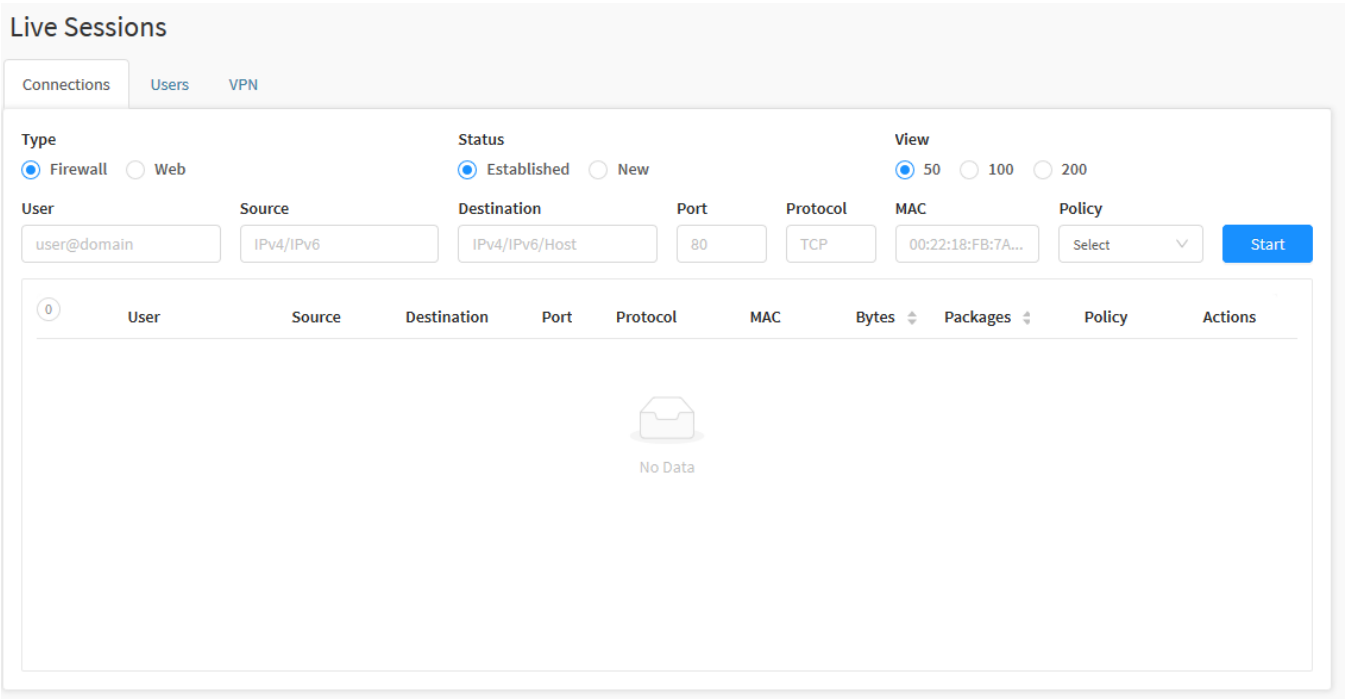
This session will cover:

- Components of this panel;
- Monitoring of all traffic carried through the firewall;
- Monitoring of all traffic carried out on the web.

Next, we will analyze the components of this panel.

Connections - Components

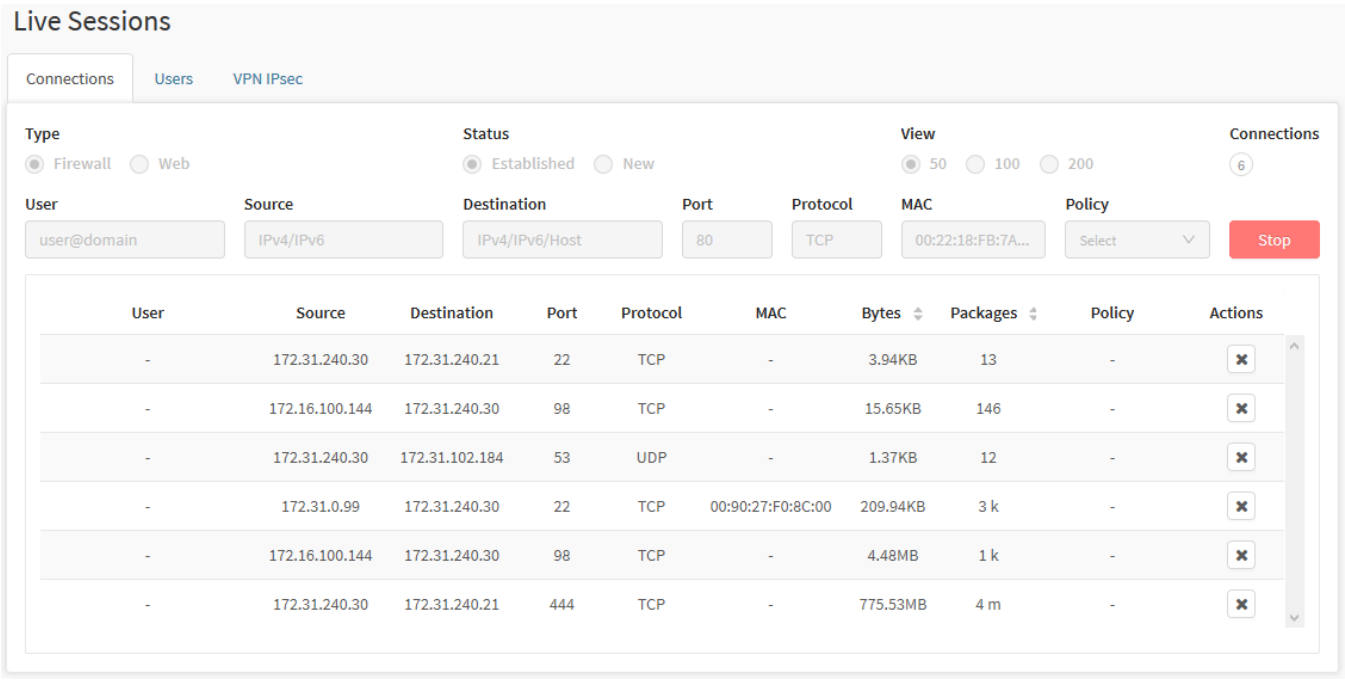
The Live Connections panel is made up of the following features:



Connections

- ***Type:*** Determines the type of monitoring between options:
  - ***Firewall[ ]*:** When you select this option, you choose to monitor all traffic carried out at the firewall;
  - ***Web[ ]*:** When you select this option, you choose to monitor all web traffic. This type of monitoring only checks for new connections, disabling the status field.
- **Status:** Determines the type of state that will be monitored among the options:
  - ***Established[ ]*:** When selecting this option, the established TCP connections and their details will be displayed. This option disables the view field;
  - **New[ ]:** When selecting this option, new connections (accepted, rejected and blocked) will be displayed in which policy the connection was handled.
- **View[ ]:** Determines the amount of results displayed, which can be from 50, 100 to 200 results;
- **User:** In this field, it is possible to determine a user, to be used as a filter during monitoring;
- **Source:** In this field, it is possible to determine a source IP, to be used as a filter during monitoring;
- **Destination:** In this field, it is possible to determine a destination IP, to be used as a filter during monitoring;
- **Port:** In this field, it is possible to determine a port, to be used as a filter during monitoring;
- **Protocol:** In this field, it is possible to determine a protocol type, to be used as a filter during monitoring;
- **Policy:** In this drop-down list, it is possible to determine a policy, to be used as a filter during monitoring. The policies available in this list are created in UTM - POLICIES.

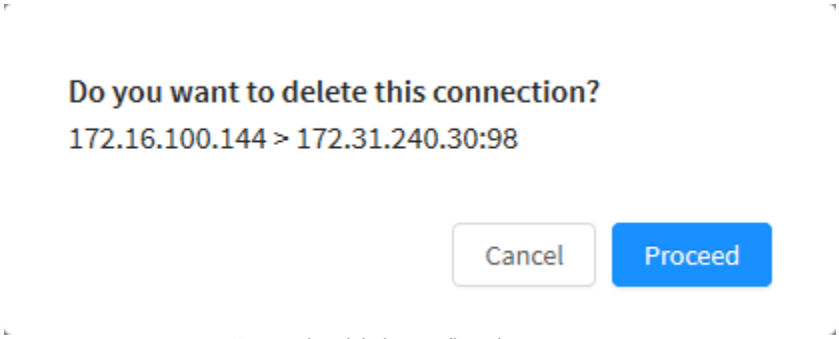
The results are displayed in the table below the options:



Connections - Results

Next, we will analyze each component of this table:

- ***User:*** Displays the user related to access, otherwise it has a "-";
- ***Source:*** Displays the IP of the access source;
- ***Destination:*** Displays the access destination IP;
- ***Port:*** Displays the port used to access;
- ***Protocol:*** Displays the protocol used to access;
- ***Policy:*** Displays the policy applied to access, if it has no relevant policy, it displays a "-";
- ***Actions:*** *Allows you to delete the connection by clicking on the* ***[✖]*** *button, a confirmation window will be displayed as shown below*:



Connection deletion confirmation message

ATTENTION: Some applications have resources to renew or maintain the connection, because of these characteristics, this option will not necessarily interrupt every type of connection. To make sure that the block will be implemented, it is recommended to create a policy preventing access. For more information on creating policies, see this page.

Click the **[** Proceed **]** button to delete the connection or **[** Cancel **]** to close this window

Connection successfully deleted

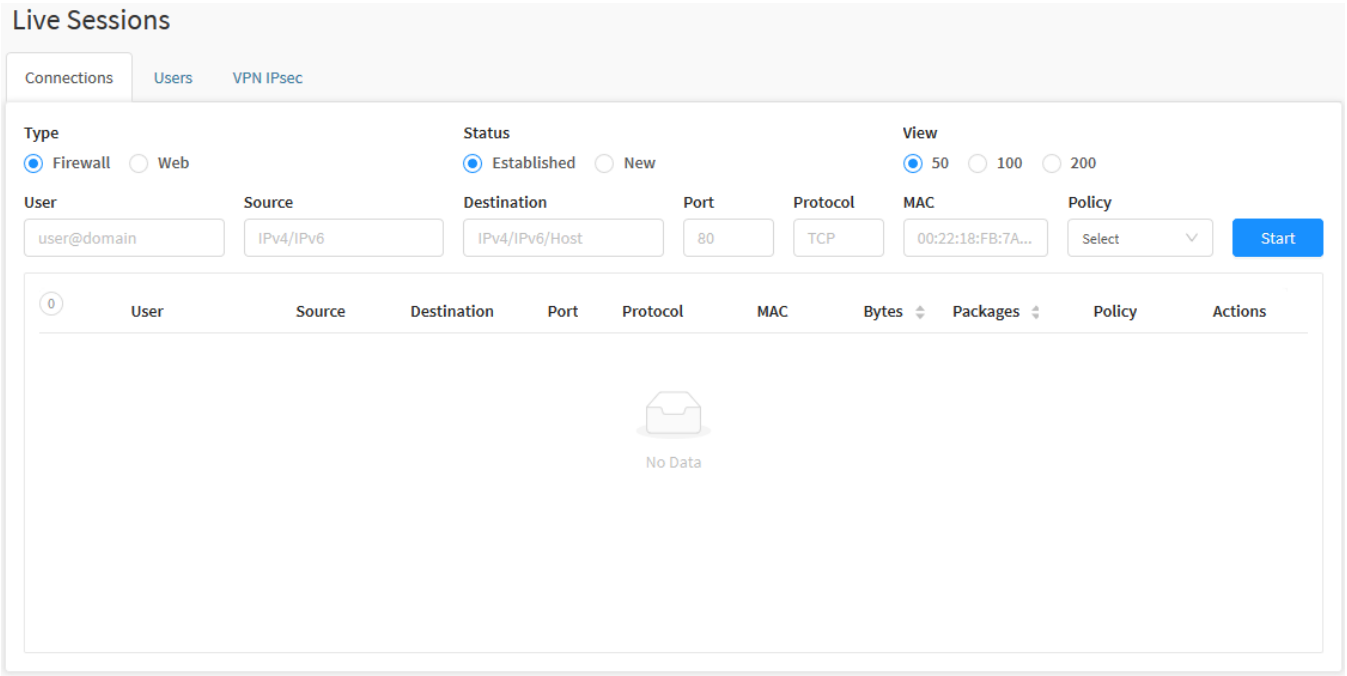
Finally, to perform the monitoring, just click **[** Start **]**. If a monitoring is already being performed, you can stop it by clicking **[** Stop **]**.

Connections - Firewall

The following will show some examples of how to monitor active connections on the firewall.

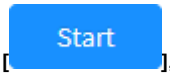
Firewall - Established

To perform the monitoring, configure the Live Connections tab as shown below:

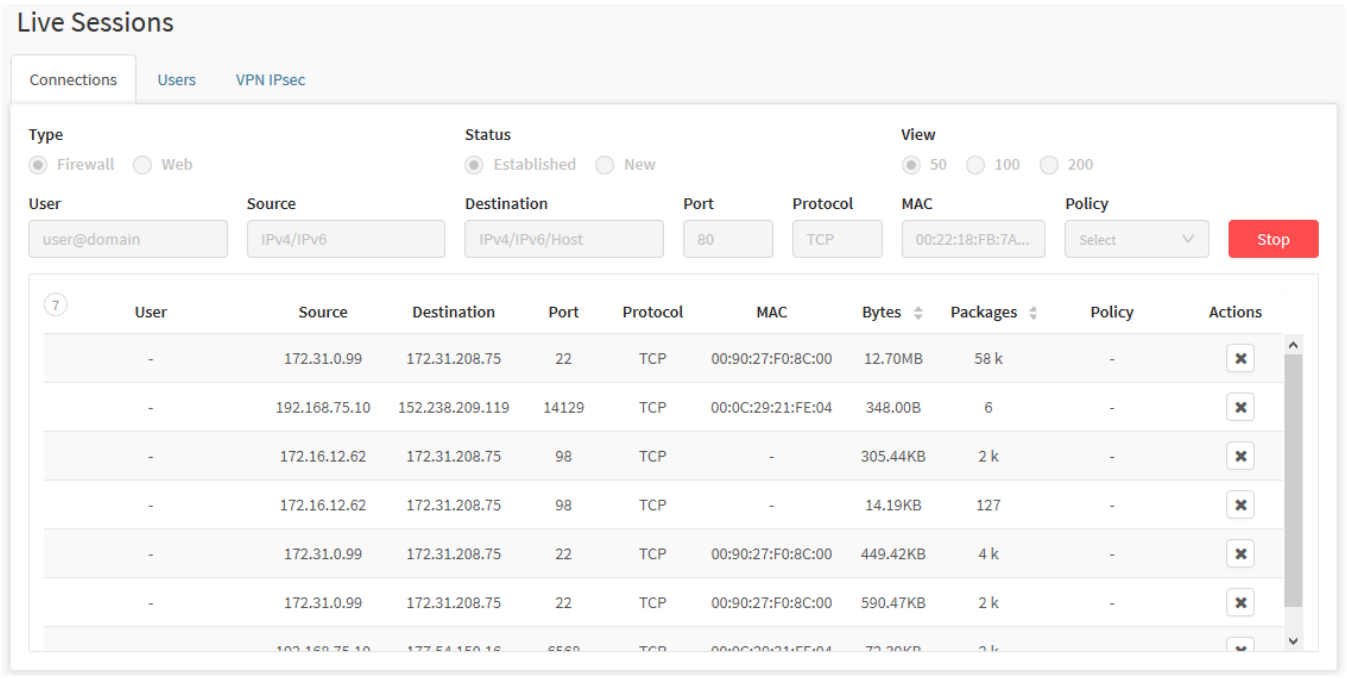


Connections- Firewall - Established

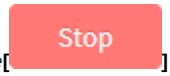
- ***Type:*** Select the Firewall option;
- ***Status:*** Select the Established option;

Once this is done, click the **[** 

], button, the results will be displayed as shown below:



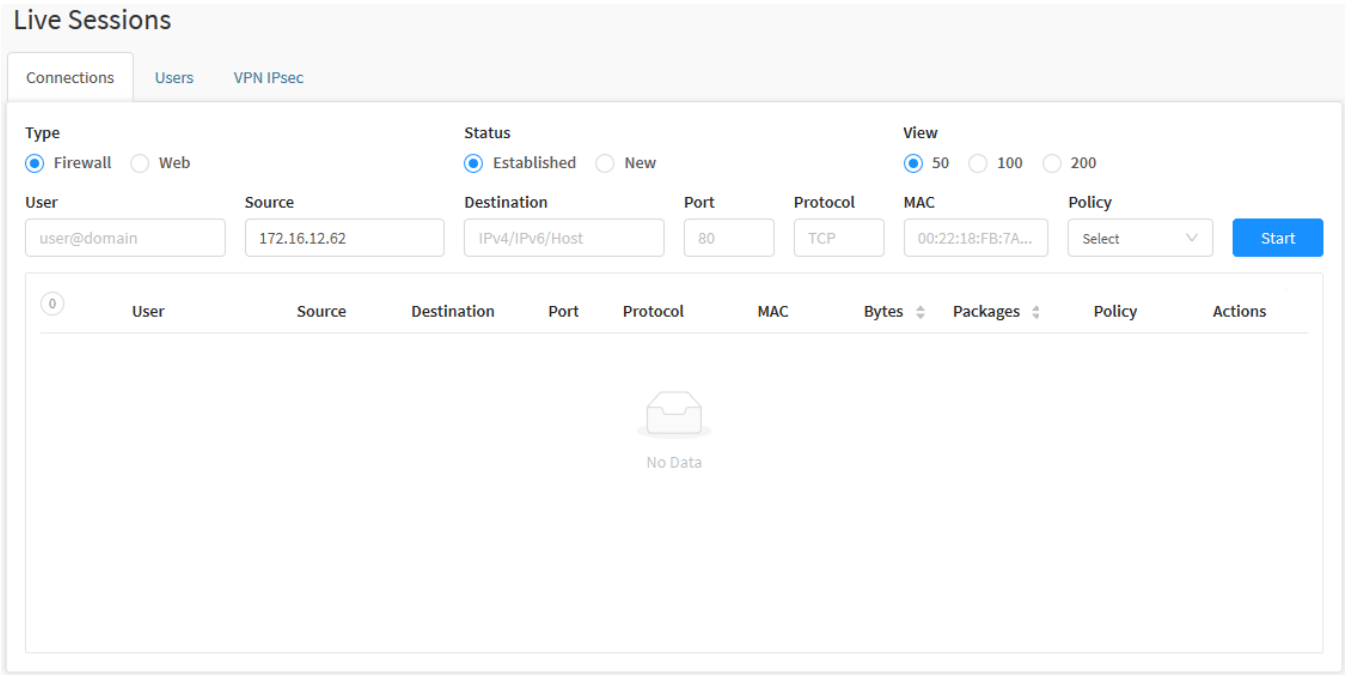
Connections - Firewall - Established - Results

To stop monitoring, just click the **[**  **]** button.

Firewall - Established - Source

It is also possible to perform a search filter by grouping of type Source and Destination when the status is of type Established.

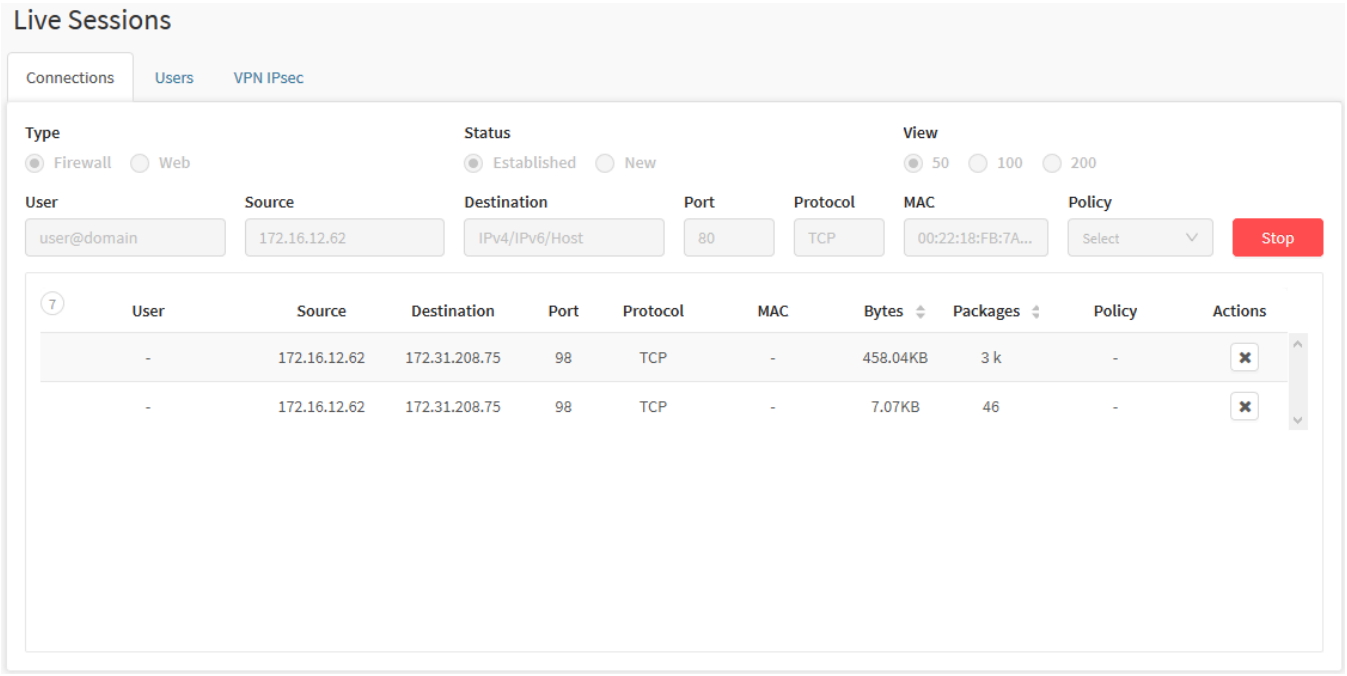
Here is an example of how to perform source IP monitoring:



Connections - Firewall - Established - Source IP

- ***Type:*** Select the Firewall option;
- ***Status:*** Select the Established option;
- ***Source*****:** Enter the source IP to be filtered. Ex .: 172.16.12.62.

Once this is done, click on the **[** Start **]** button, the results will be displayed as shown below:

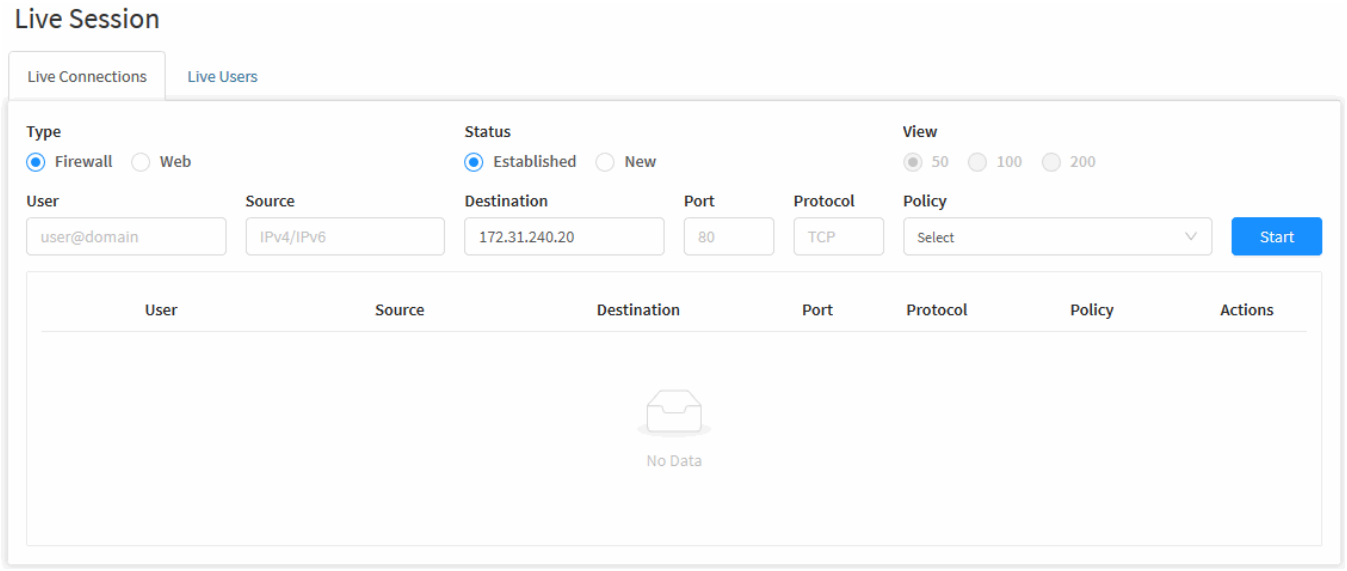


Connections - Firewall - Established - Source IP - Results

*To stop monitoring, just click the***[** Stop **]** button.

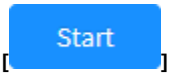
Firewall - Established - Destination

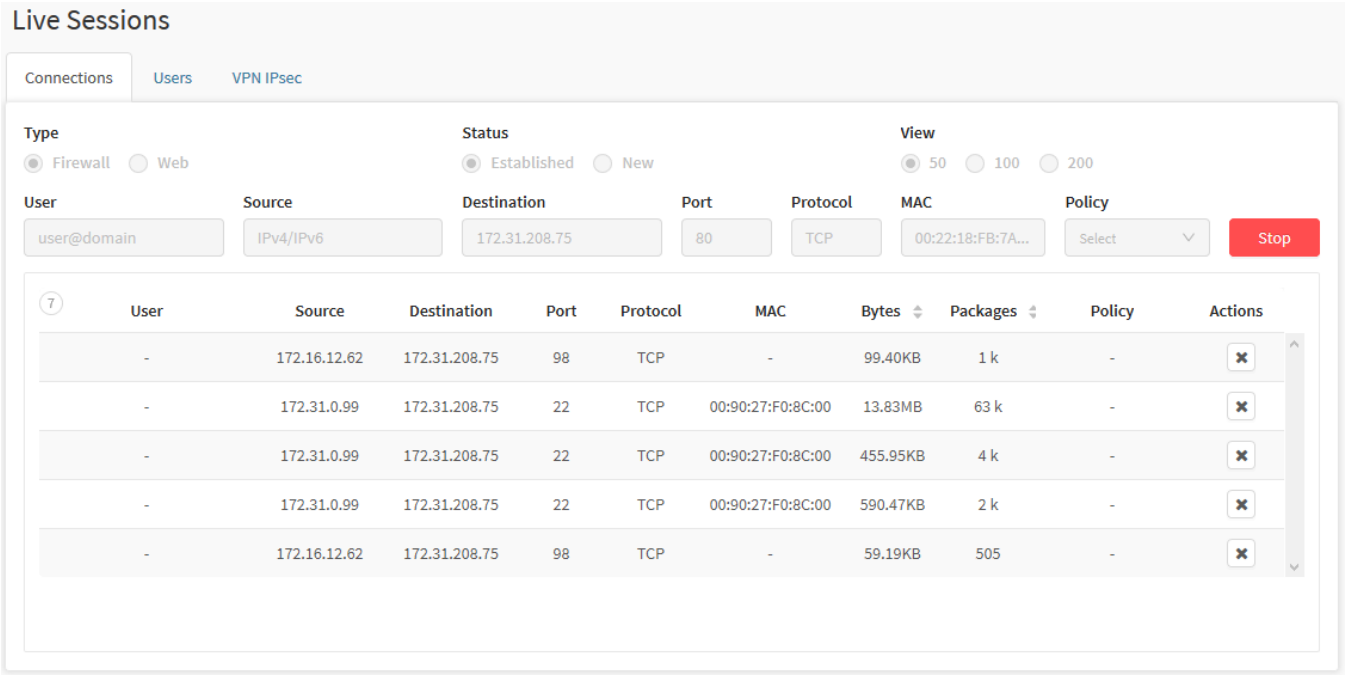
The following is an example of how to perform destination IP monitoring:



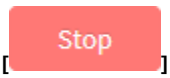
Connections - Firewall - Established - Destination IP

- ***Type:*** Selecione a opção *Firewall*;
- ***Status:*** Selecione a opção *Established*;
- ***Destination*****:** Digite o *IP* de destino que será filtrado. Ex.: 172.31.208.75.

Once this is done, click on the **[**  **]** button, the results will be displayed as shown below:

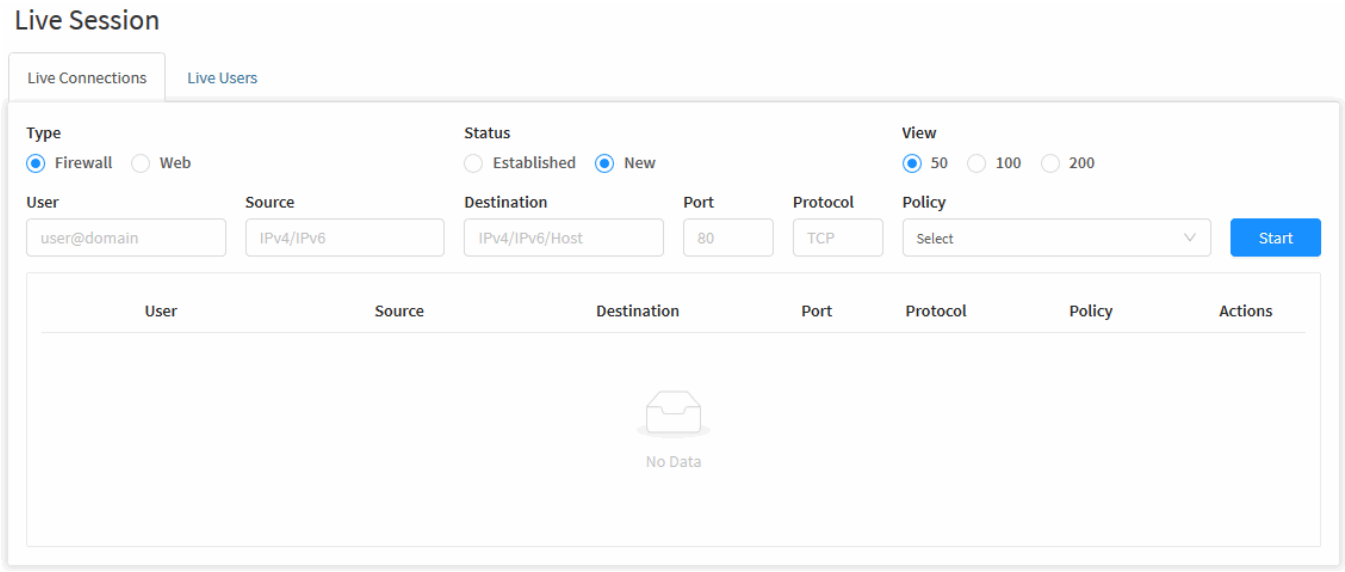


Connections - Firewall - Established - Destination IP - Results

To stop monitoring, just click the **[**  **]** button.

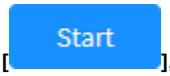
Firewall - New

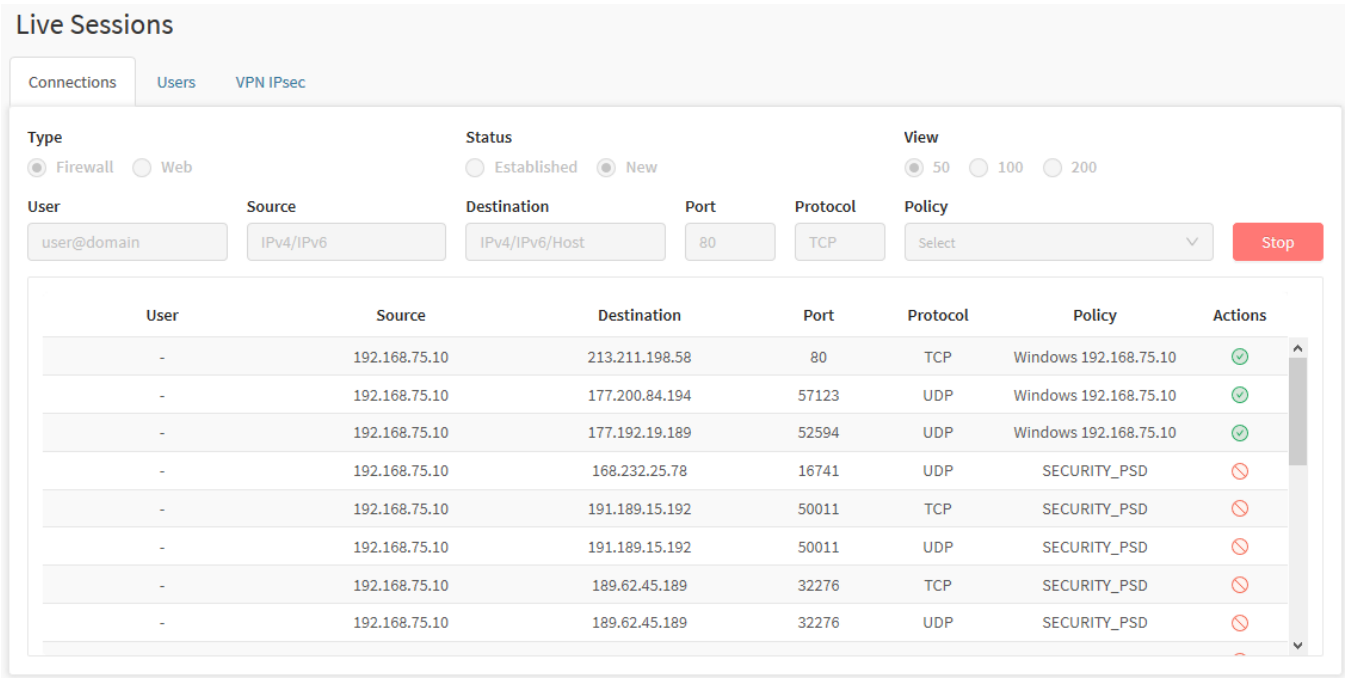
By clicking on the status New and type Firewall, it is possible to monitor new accesses.



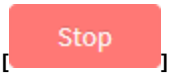
Connections - Firewall - New

- ***Type:*** Select the Firewall option;
- ***Status:*** Select the New option.

Once this is done, click on the **[**  **]**, button, the results will be displayed as shown below:



Connections - Firewall - New - Results

To stop monitoring, just click the **[**  **]** button.

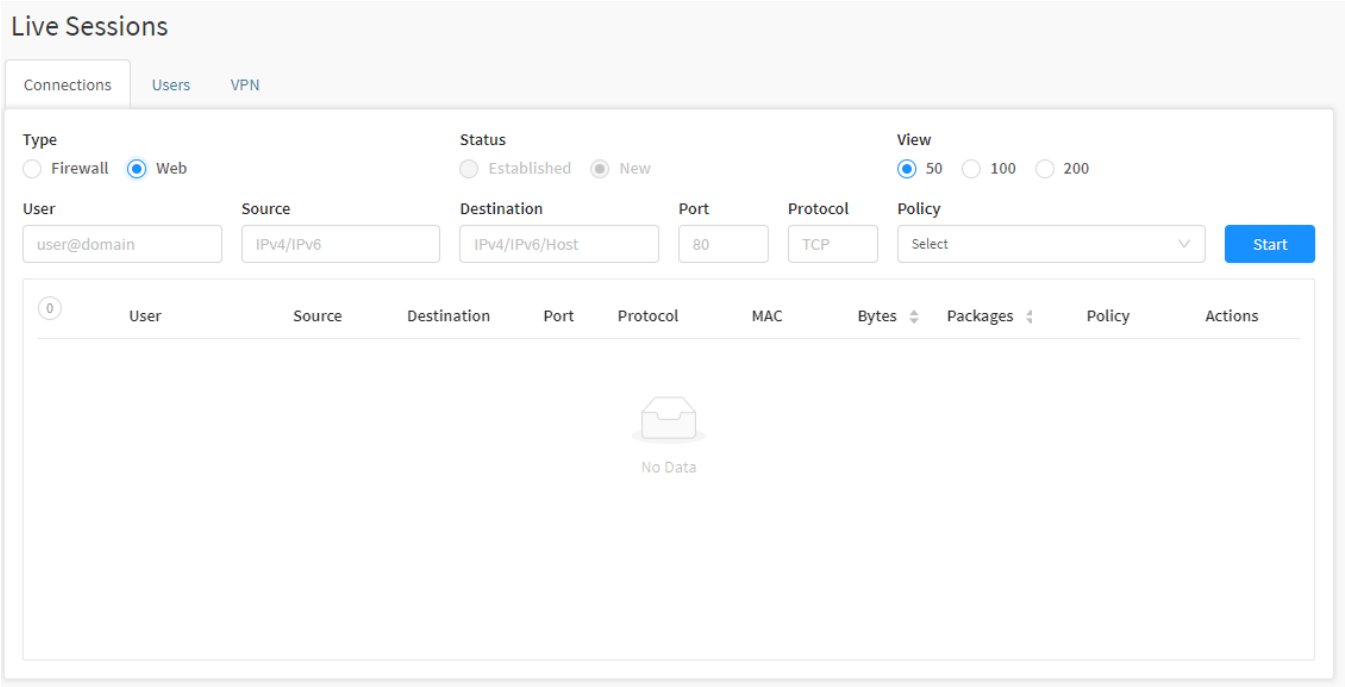
For more information about each field on this screen, check this page.

Connections - Web

Below are some examples of how to monitor all web traffic

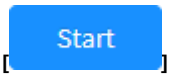
Web - New

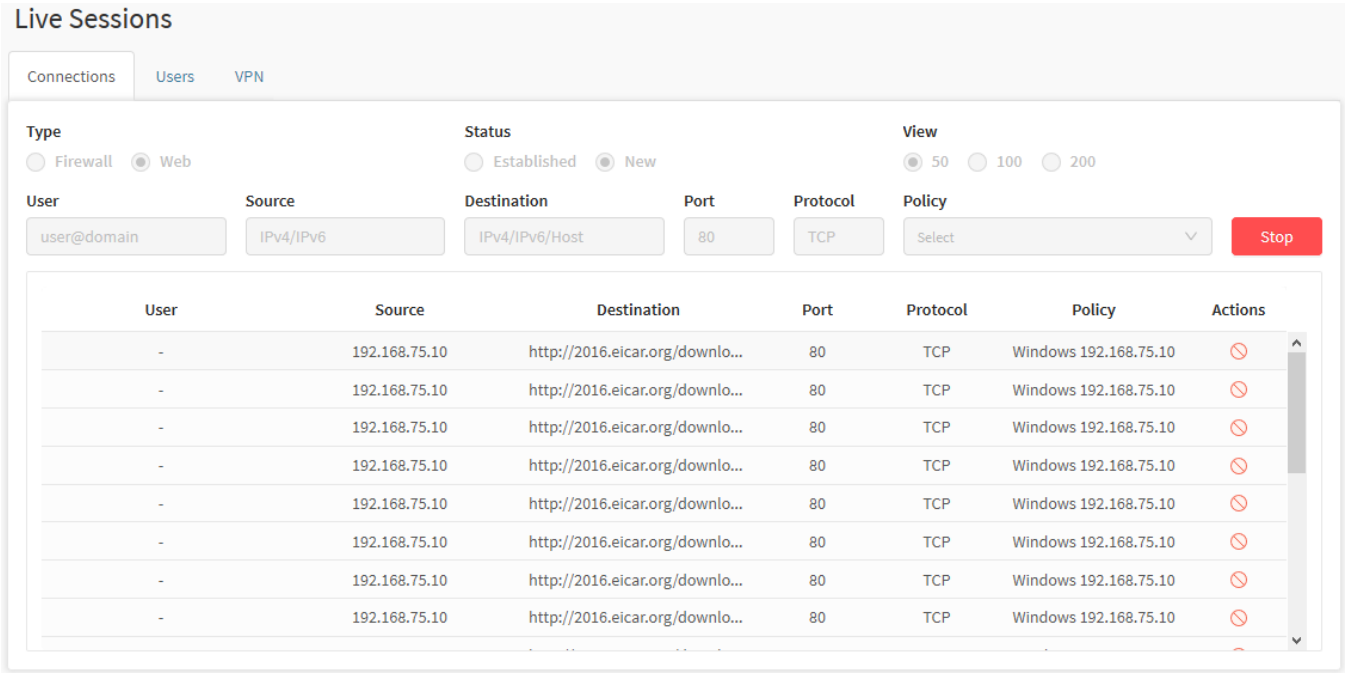
To perform the monitoring, configure the Connections tab as shown below:



Connections - Web - New

- ***Type:*** Select the Web option;
- ***Status:*** The New option will be automatically selected;

Once this is done, click the **[**  **]** button, the results will be displayed as shown below:



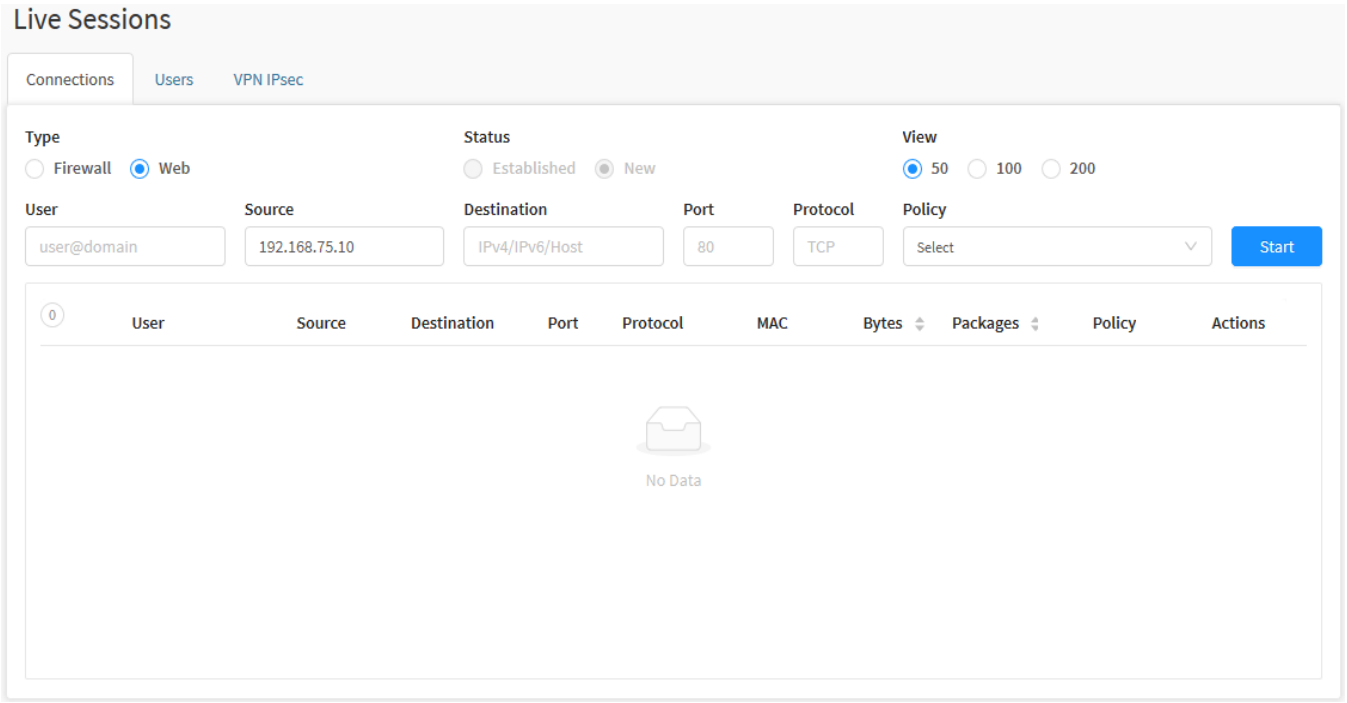
Connections - Web - *New - Results*

To stop monitoring, just click the [Stop] button.

Web - New - Source

It is also possible to perform a search filter by grouping of type Source and Destination when the status is of type New.

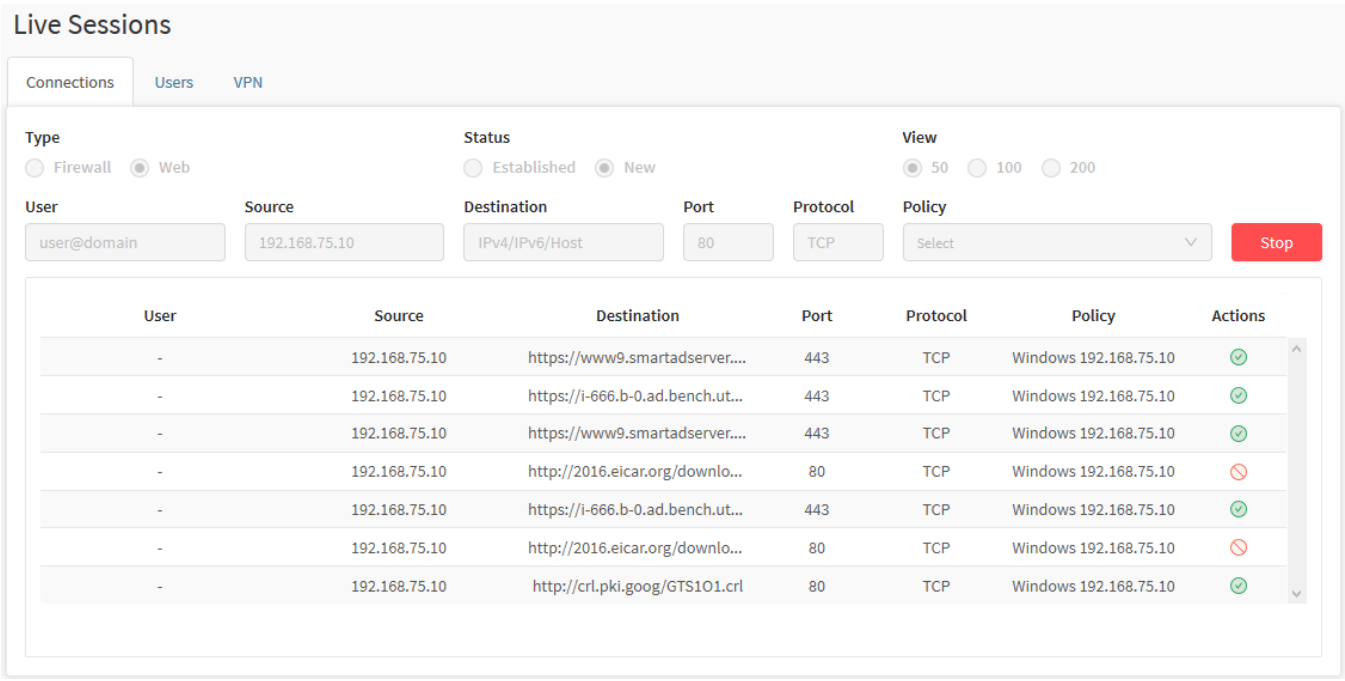
Here is an example of how to perform source IP monitoring:



Connections - Web - New - Source IP

- ***Type:*** Select the Web option;
- ***Status:*** The New option will be automatically selected;
- ***Source*****:** Enter the source IP to be filtered. Ex .: 192.168.75.10.

Once this is done, click the **[** Start **]** button, the results will be displayed as shown below:



Connections - Web - New - Source IP - Results

To stop monitoring, just click the **[** Stop **]** button.

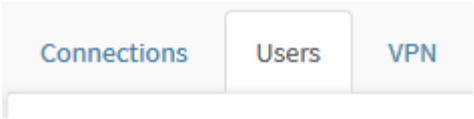
For more information about each field on this screen, check this page.

Live Sessions - Users

The panel available on the Live Users tab has the function of monitoring access, but specifically focused on users.

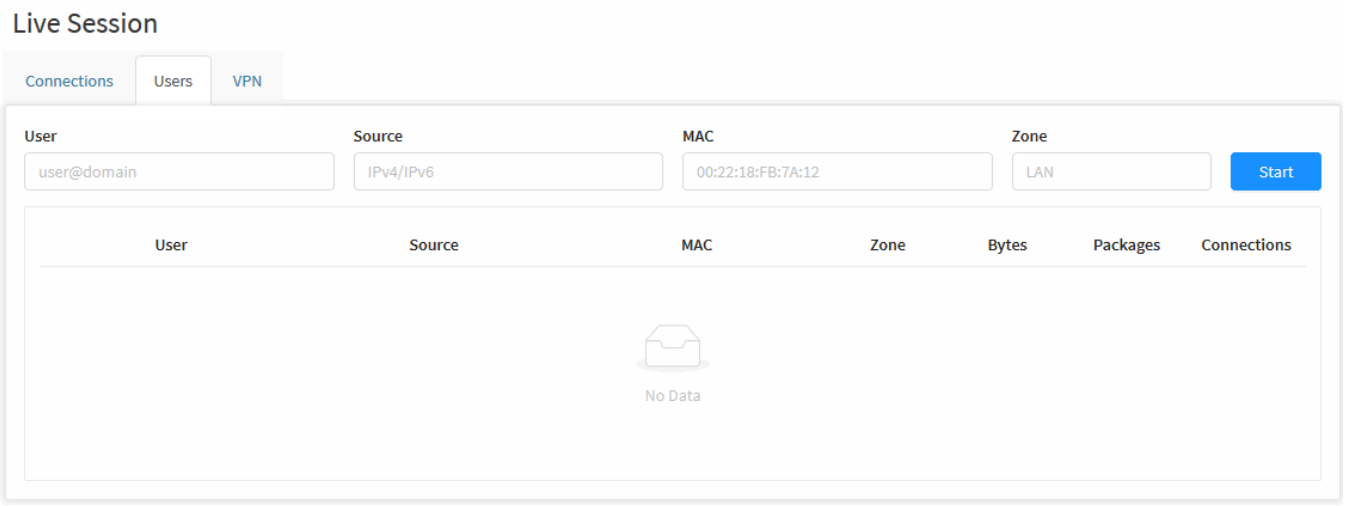
As in "Live Connections", it is possible to apply filters in order to generate more specific reports.

To access, click on the "Live Users" tab.



Users tab

The “Live Users” screen will appear, as shown by the image below:



Live Session - Users

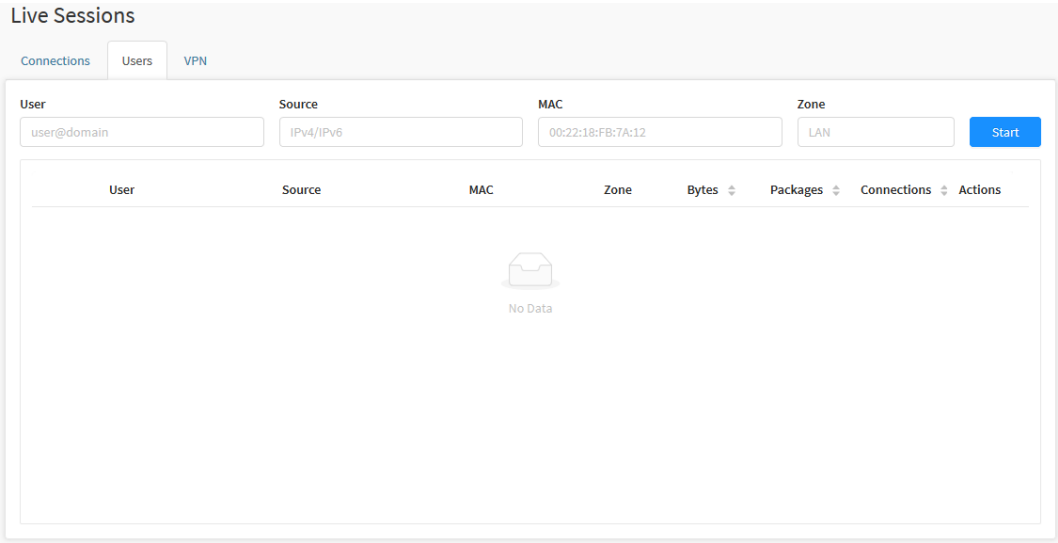
This session will cover:

- Components of this panel;
- How to perform monitoring;

Next, we will analyze the components of this panel.

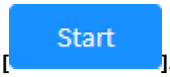
Users - Components

The Users panel is made up of the following features:

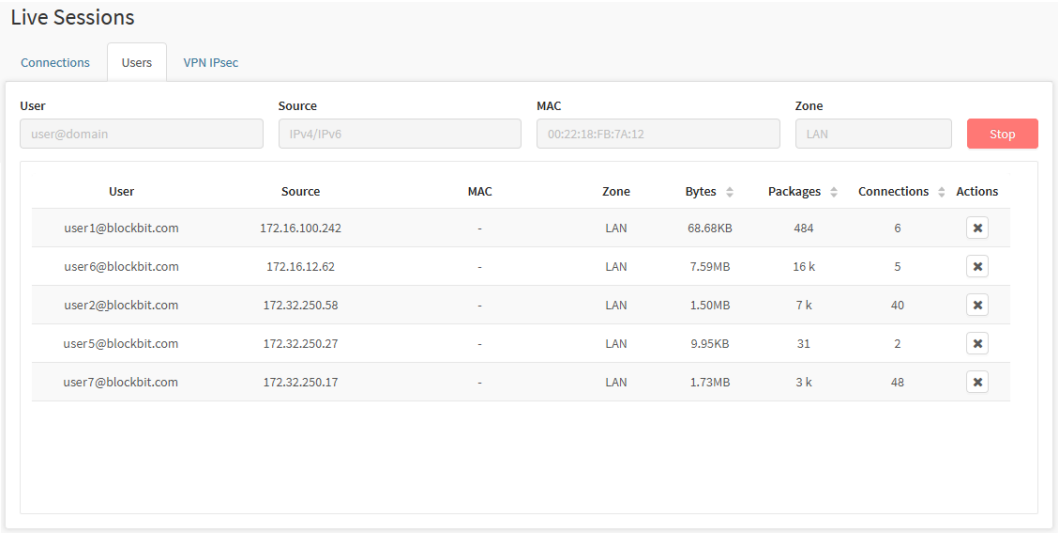


Users

- ***User:*** In this field, it is possible to determine a user, to be used as a filter during monitoring;
- **Source:** In this field, it is possible to determine a source IP, to be used as a filter during monitoring;
- **MAC:** In this field, it is possible to determine a physical address, to be used as a filter during monitoring;
- **Zone:** In this field, it is possible to limit the monitoring to a specific network zone.

To perform the monitoring, just click [

]. The results are displayed in the table below the options:

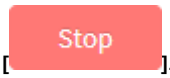


Live Users - Results

Next, we will analyze each component of this table:

- ***User:*** Displays the user related to access;

- ***Source:*** Displays the IP of the access source;
- ***MAC:*** Displays the user's physical address;
- ***Zone:*** Displays the Access Zone;
- ***Bytes:*** Displays consumption of access traffic;
- ***Packages:*** Displays the amount of packets exchanged during the user's traffic;
- ***Connections*****:** Displays the amount of connections made by the user.

If a monitoring is already being performed, you can stop it by clicking **[** 

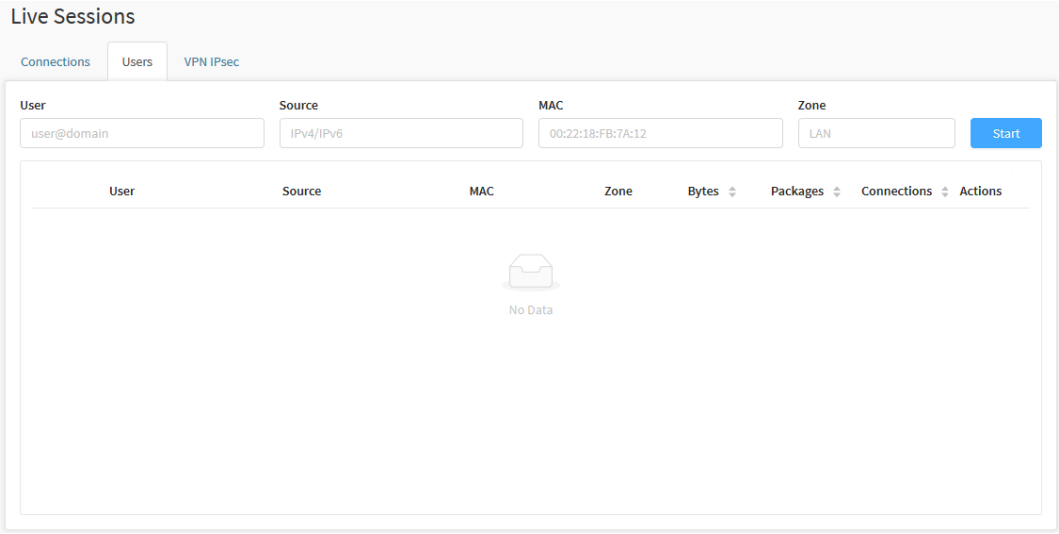
].

Users - Monitoring

Below are some examples of how to monitor users active connections.

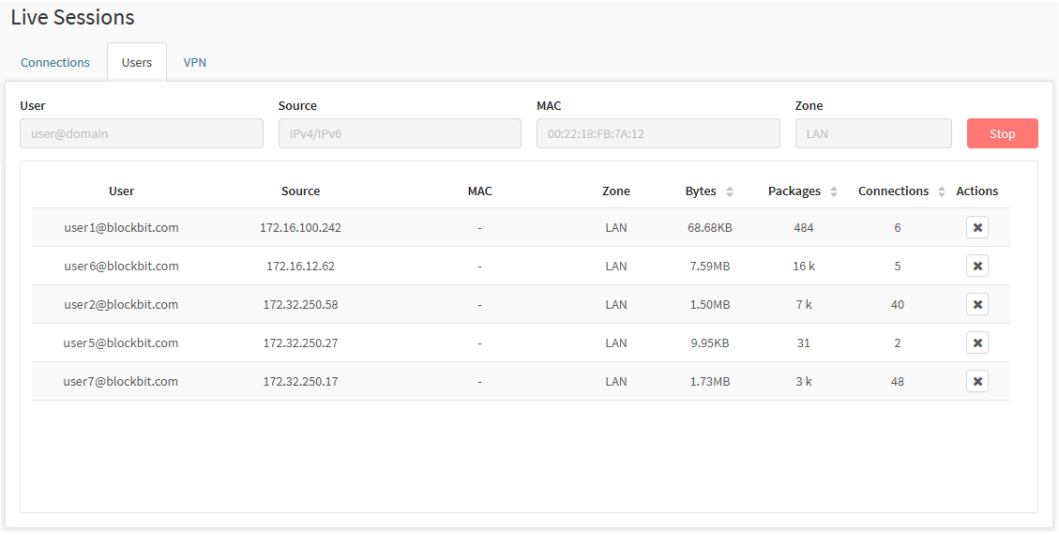
Monitoring in general

In order to perform monitoring in general, no configuration is necessary.



Users - No Filters

Simply click on [Start] to start monitoring.

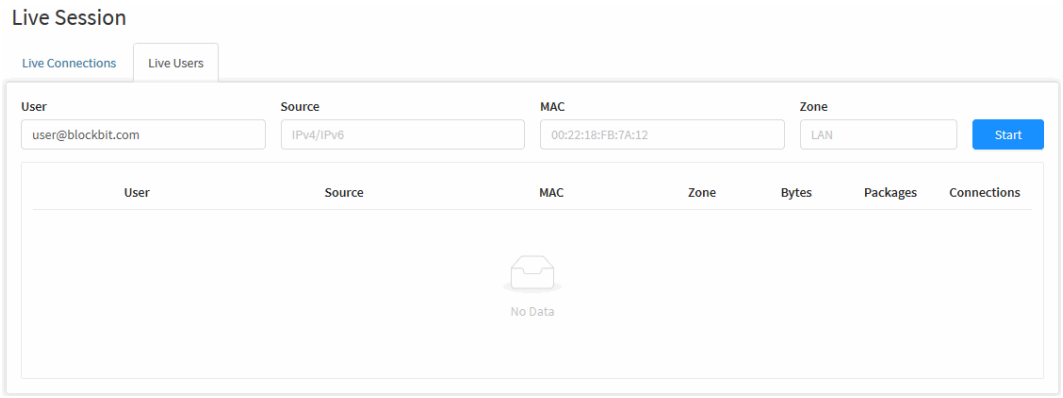


Live Users - No Filters - Results

You can stop monitoring by clicking [Stop].

Monitoring a specific user

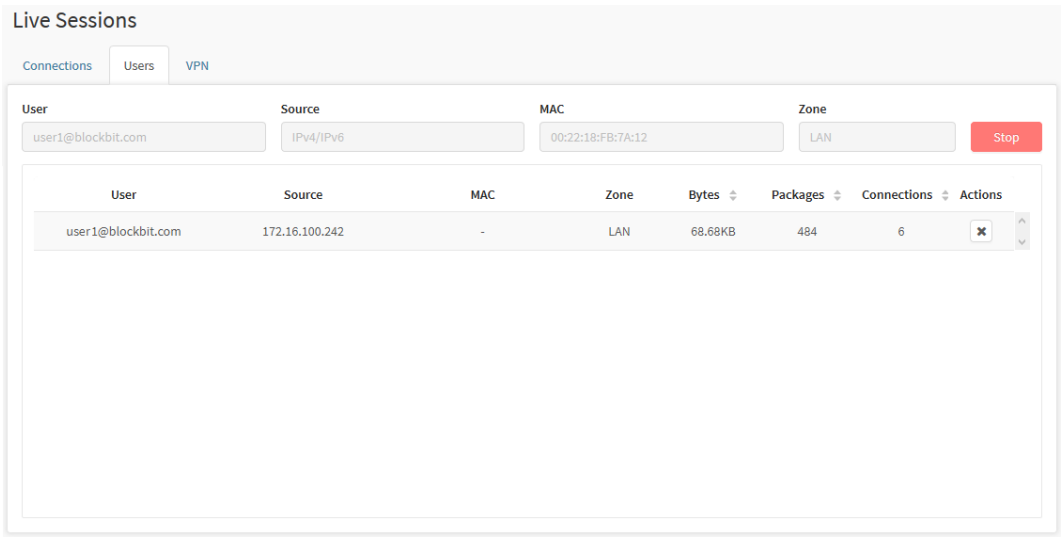
To monitor a specific user, add the desired filters as shown below:



Live Users - Filtered by user

- ***User:*** Using any of the fields it is possible to generate a filter, in this case we will filter by user. Ex.: user1@blockbit.com;

FOnce this is done, click on the [Start] button, the results will be displayed as shown below

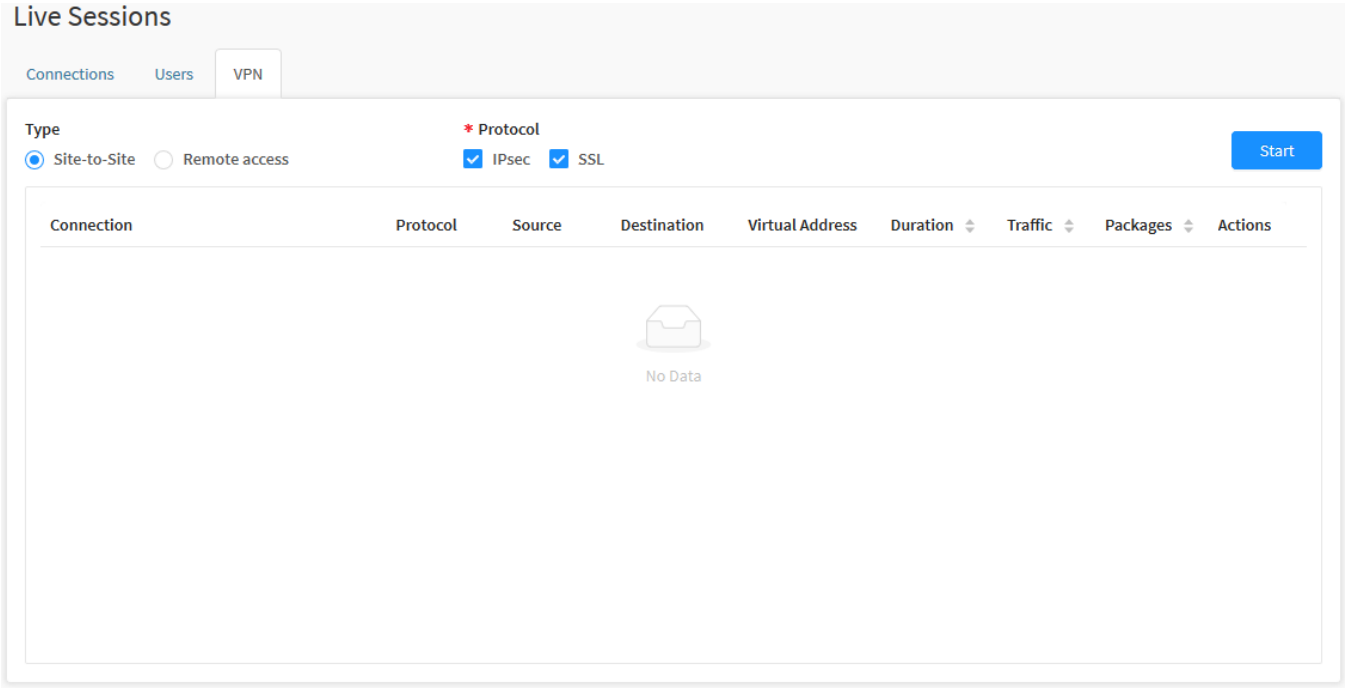


Live Users - Filtered by user - *Results*

To stop monitoring just click on the [Stop] button.

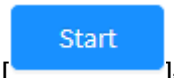
Live Sessions - VPN

This feature allows the administrator to view the status of the established VPN tunnels, the available information is:

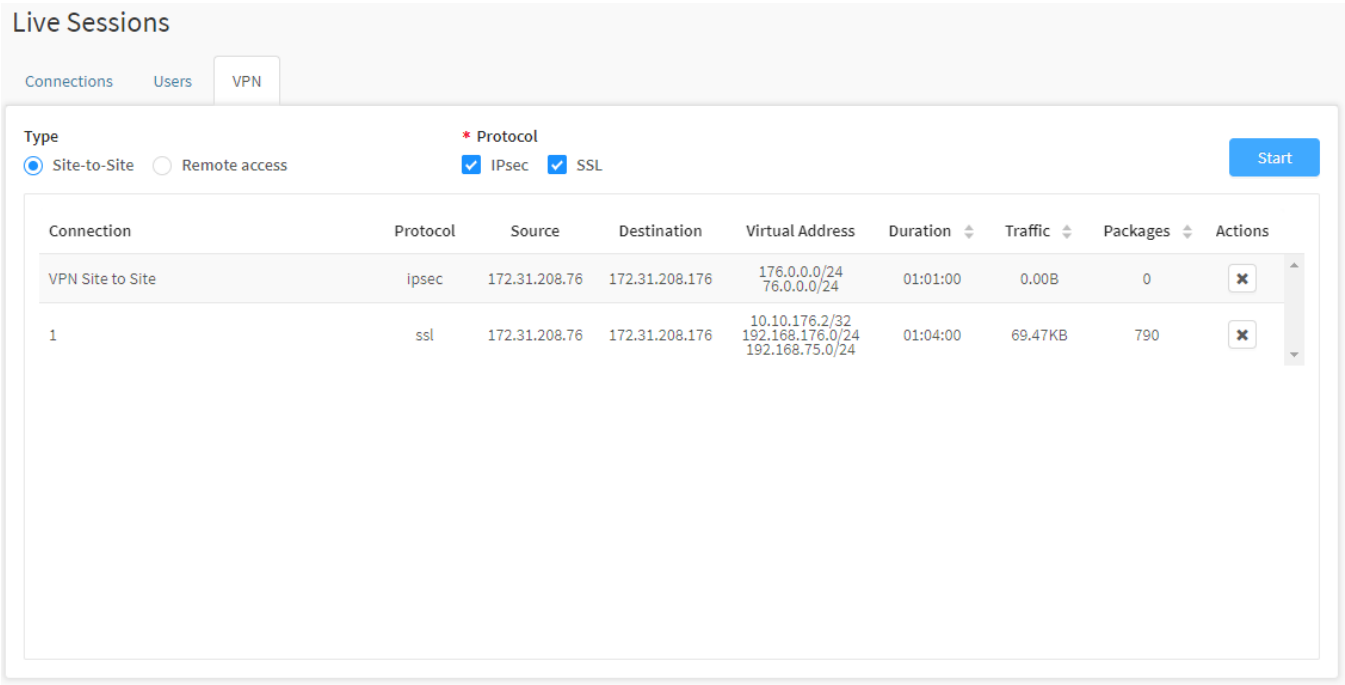


Live Sessions - VPN

- ***Type:*** The type of connection, of the VPN in question. It can be *site-to-site* or *remote access*;
- ***Protocol:*** *Defines the VPN protocol. IPsec and SSL*;

When starting the monitor by clicking **[** 

], the results will be displayed according to the type of connection and the selected protocol, as shown below:



Live Sessions - VPN - Results

The columns display the following information:

- ***Connection***: Tunnel name;
- ***Protocol:*** *Displays the VPN protocol (IPsec or SSL)*.
- ***Source*****:** Tunnel local gateway IP address;
- ***Destination*****:** IP address of the remote tunnel gateway;
- ***Virtual Address:*** *Displays the virtual IP address of the VPN*;
- ***Durantion*****:** Displays how long the VPN connection has been established. The connection date is displayed as a tooltip;
- ***Traffic:*** Displays current VPN traffic;
- ***Packages*****:** Number of packets trafficked;
- ***Actions:*** View the removal option:
  - **[** ✖ **]** This option serves to bring down a VPN tunnel. Note that these tunnels will not reconnect on their own.

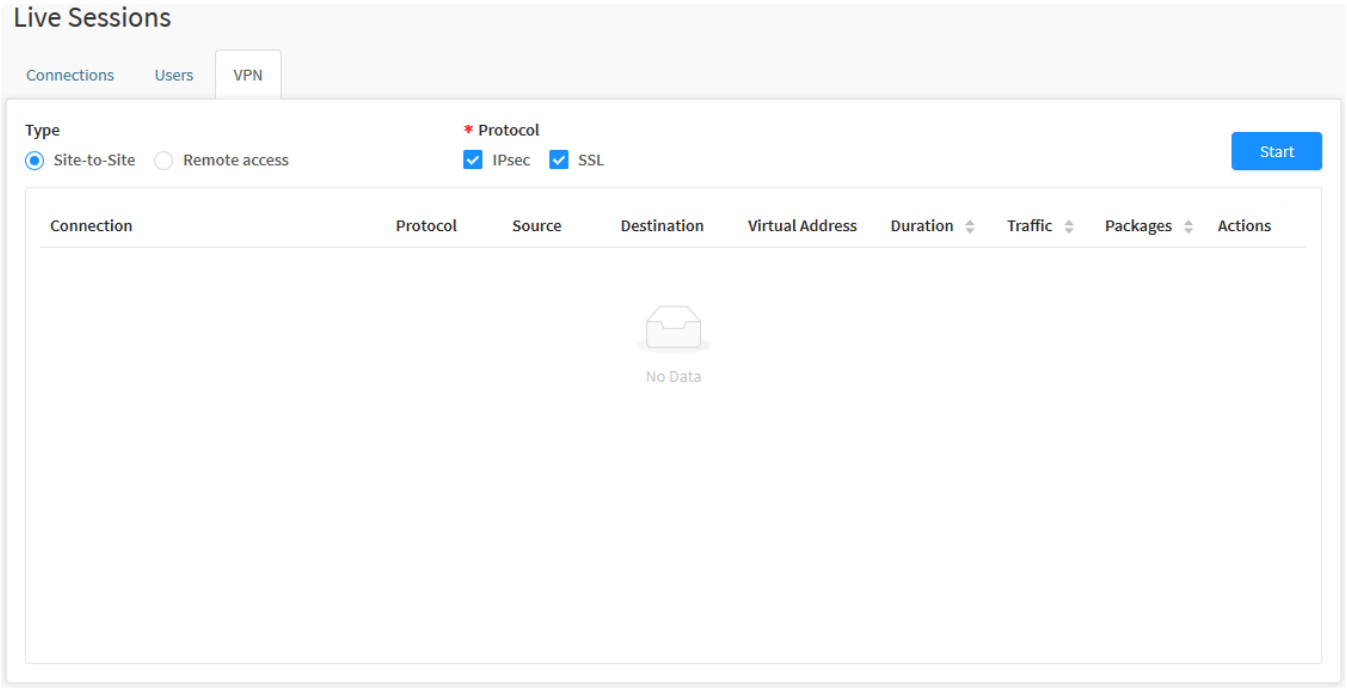
When taking down a VPN tunnel using the option above, it will NOT reconnect (regardless of whether it is configured to connect automatically).

For more information on how to configure an IPSEC VPN tunnel, check this page.

For more information on configuring SSL VPN, check this page.

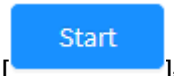
To stop a monitoring that is being performed, click **[** Stop **]**.

This feature allows the administrator to view the status of the established VPN tunnels, the available information is:

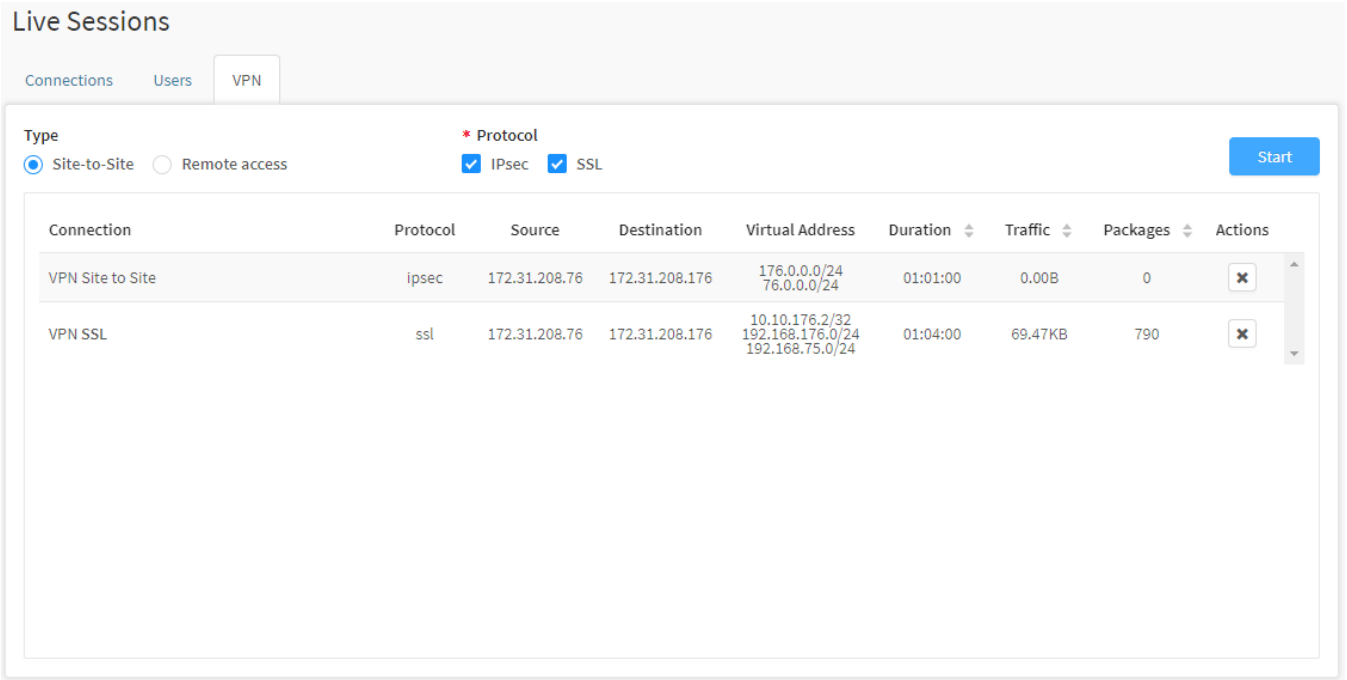


Live Sessions - VPN

- ***Type:*** The type of connection, of the VPN in question. It can be *site-to-site* or *remote access*;
- ***Protocol:*** *Defines the VPN protocol. IPsec and SSL*;

When starting the monitor by clicking **[** 

], the results will be displayed according to the type of connection and the selected protocol, as shown below:



Live Sessions - VPN - Results

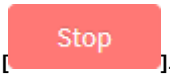
The columns display the following information:

- ***Connection***: Tunnel name;
- ***Protocol:*** *Displays the VPN protocol (IPsec or SSL)*.
- ***Source*****:** Tunnel local gateway IP address;
- ***Destination*****:** IP address of the remote tunnel gateway;
- ***Virtual Address:*** *Displays the virtual IP address of the VPN*;
- ***Durantion*****:** Displays how long the VPN connection has been established. The connection date is displayed as a tooltip;
- ***Traffic:*** Displays current VPN traffic;
- ***Packages*****:** Number of packets trafficked;
- ***Actions:*** View the removal option:
  - **[**  **]** This option serves to bring down a VPN tunnel. Note that these tunnels will not reconnect on their own.

When taking down a VPN tunnel using the option above, it will NOT reconnect (regardless of whether it is configured to connect automatically).

For more information on how to configure an IPSEC VPN tunnel, check this page.

For more information on configuring SSL VPN, check this page.

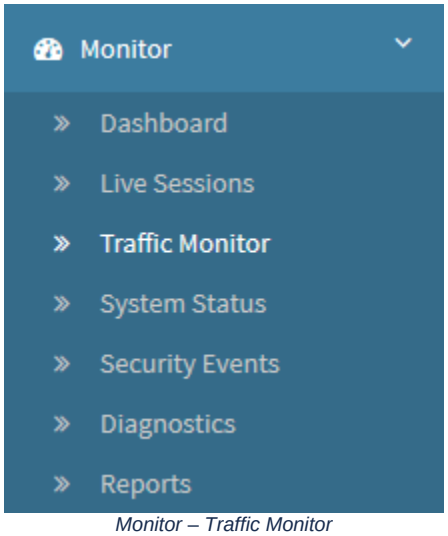
To stop a monitoring that is being performed, click **[** 

].

Monitor - Traffic Monitor

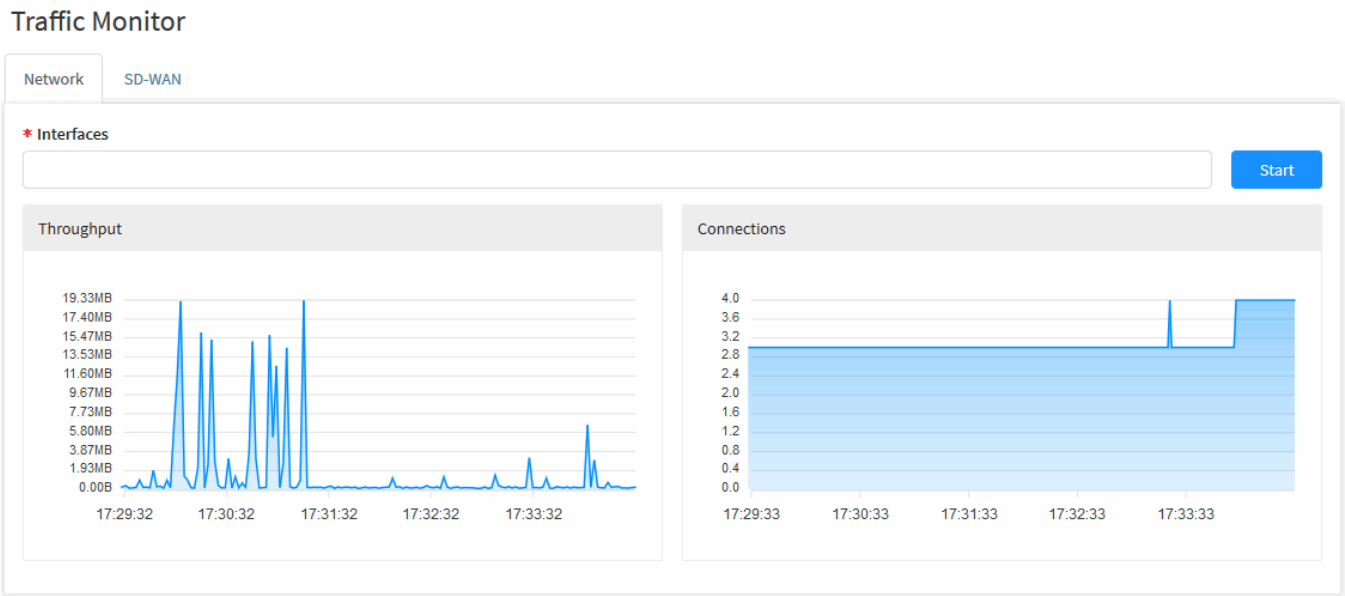
As its name implies, Traffic Monitor, allows network and SD-WAN traffic to be monitored, through this resource the administrator can view the actual network traffic or histogram (Network Throughput), by interfaces, number of simultaneous connections and network traffic for each PIPE (QoS). In addition, it is also possible to view the performance of the SD-WAN according to its interfaces and performance indexes.

To access this screen, just select the option “Traffic Monitor”.



Monitor – Traffic Monitor

A tela abaixo será exibida:



Monitor - Traffic Monitor - Network

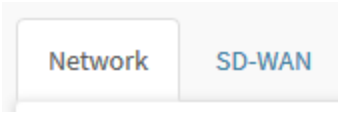
The Traffic Monitor screen has the following tabs:

- *Network*;
- *SD-WAN*.

Traffic Monitor - Network

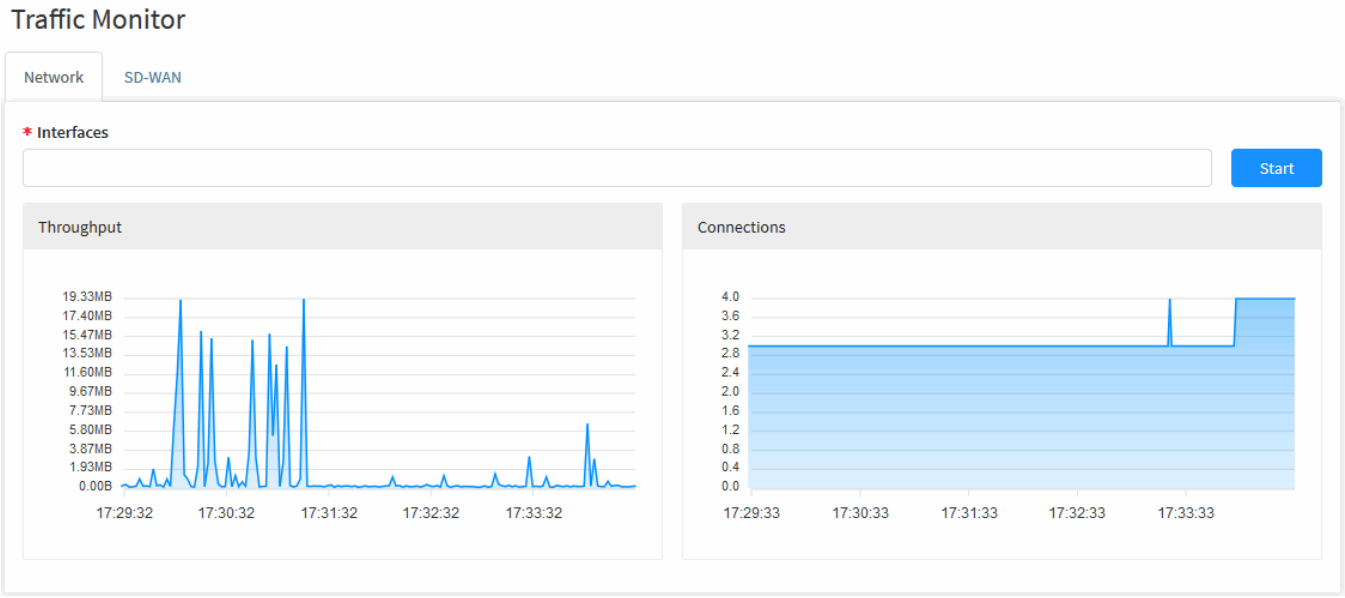
In the Network tab of Traffic Monitor, it is possible to check in real time the performance and traffic carried out on the network.

To access, if the tab is not selected, click on "Network".



Network Tab

The screen shown below will appear:

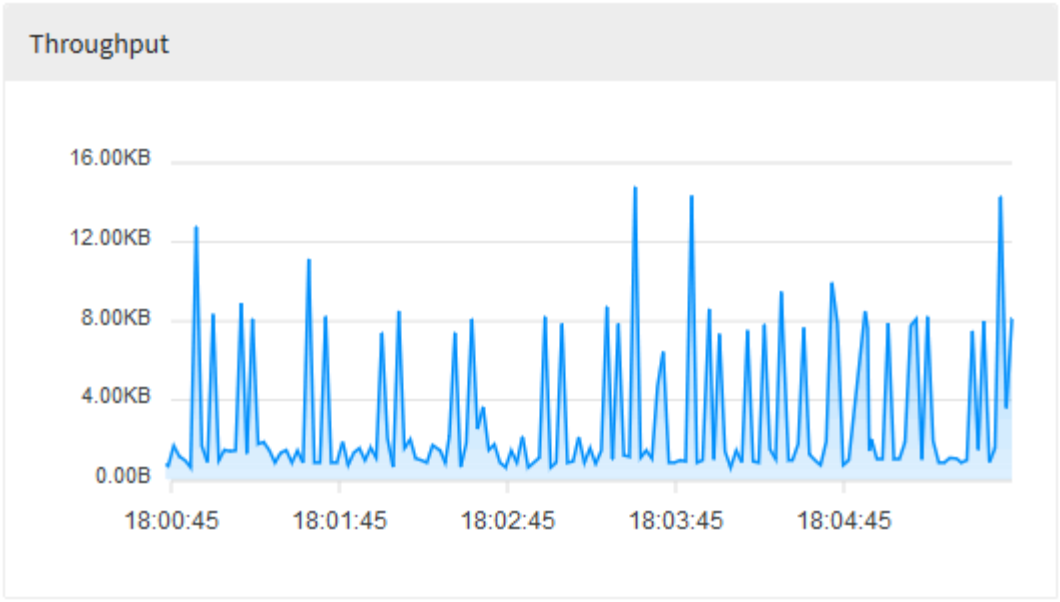


Traffic Monitor - Network

Next we will analyze each component of this screen:

Throughput Graph

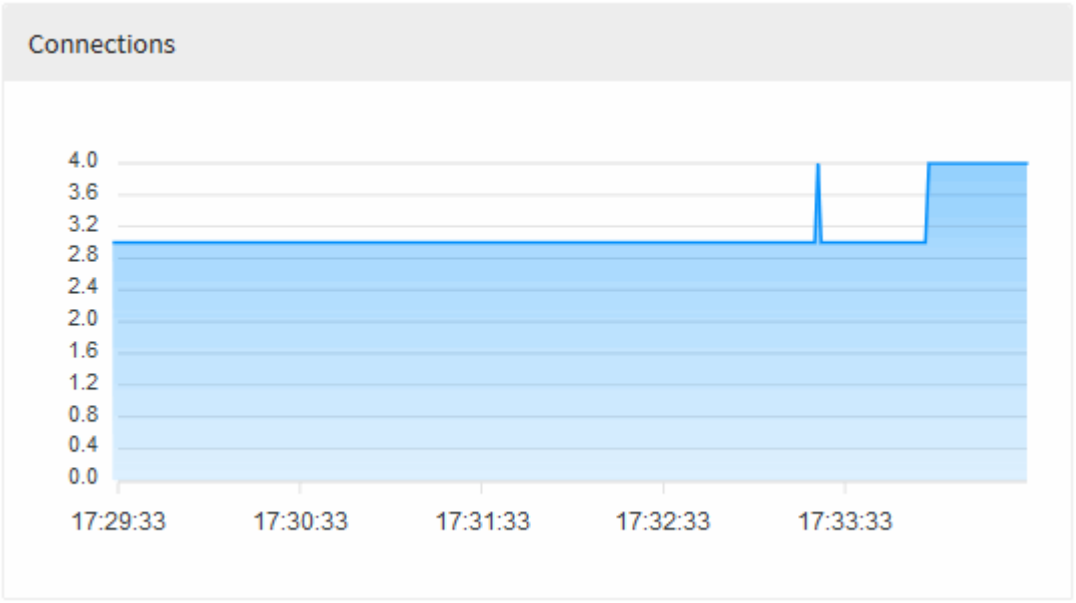
The Throughput graph shows the historical performance of the network in real time. When hovering the mouse over, it is possible to view a summary of the selected period.



Traffic Monitor - Network - Throughput

Connections Graph

The Connections graph shows a history of simultaneous connections and the consumption that your traffic causes in real time. By hovering the mouse over, it is possible to view a summary of the selected period.

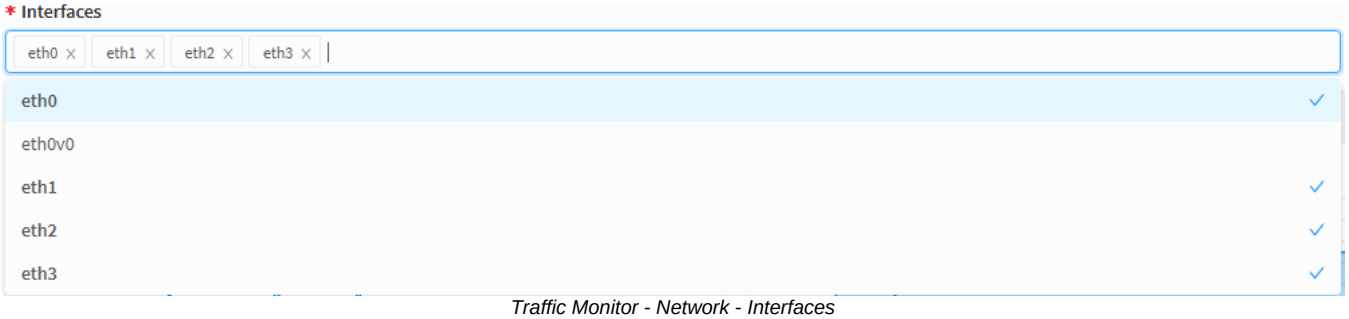


Traffic Monitor - Network - Connections

Real-time interface monitoring

The bar located at the top of the screen serves to monitor the network interfaces that are selected in real time.

It is possible to add the interfaces to be monitored, to do so, type or select them from the list, as shown in the image:

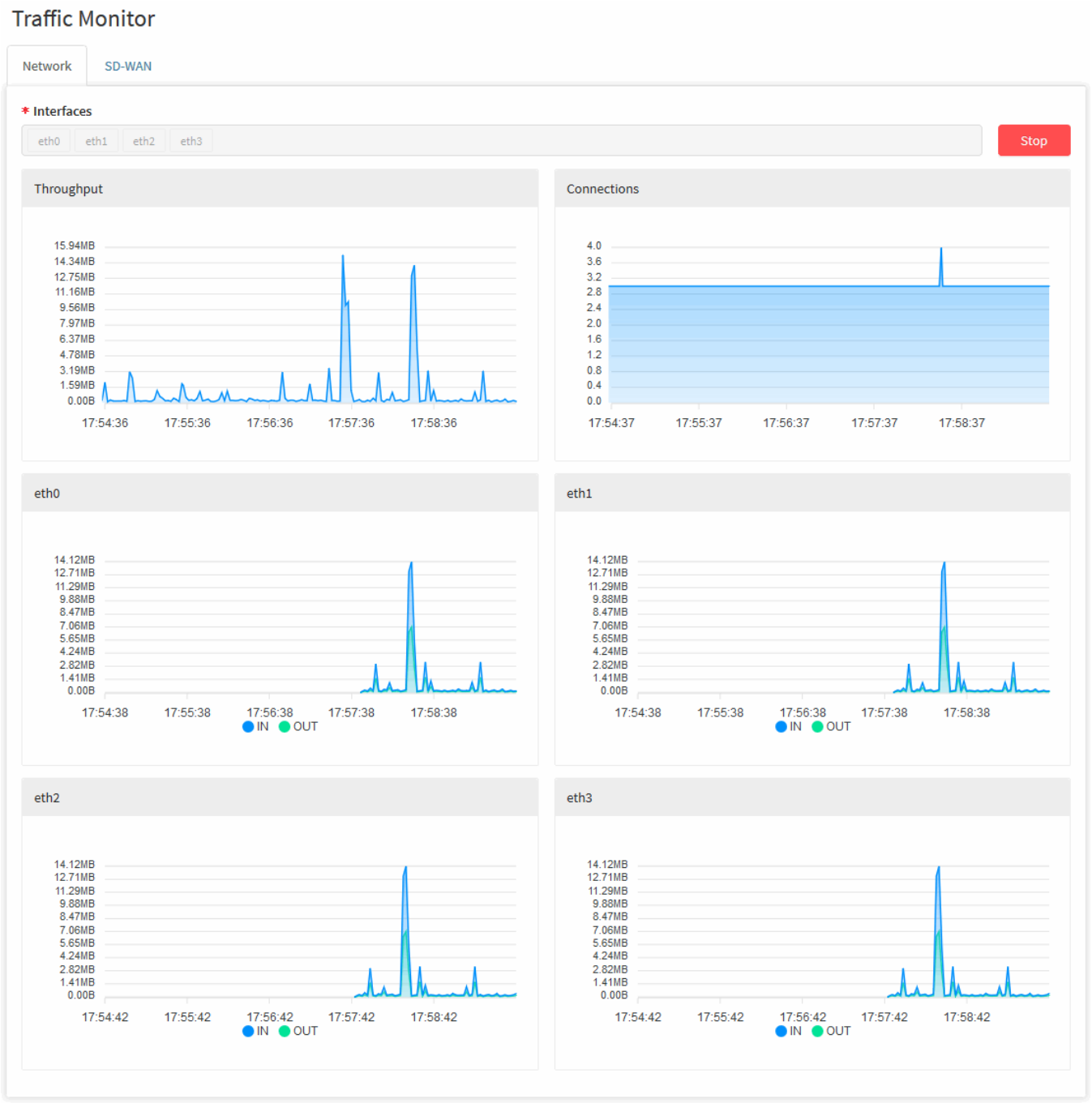


Traffic Monitor - Network - Interfaces

The maximum number of interfaces that can be added for real-time monitoring is 4.

Click the **[** Start **]** button to start monitoring

New charts will be added below the Throughput and Connections charts and real-time monitoring will start, as shown below:

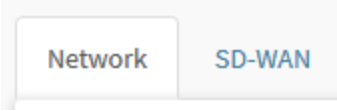


Traffic Monitor - Network - Real-time interface monitoring

If a monitoring is already being performed, it is possible to stop it by clicking [Stop].

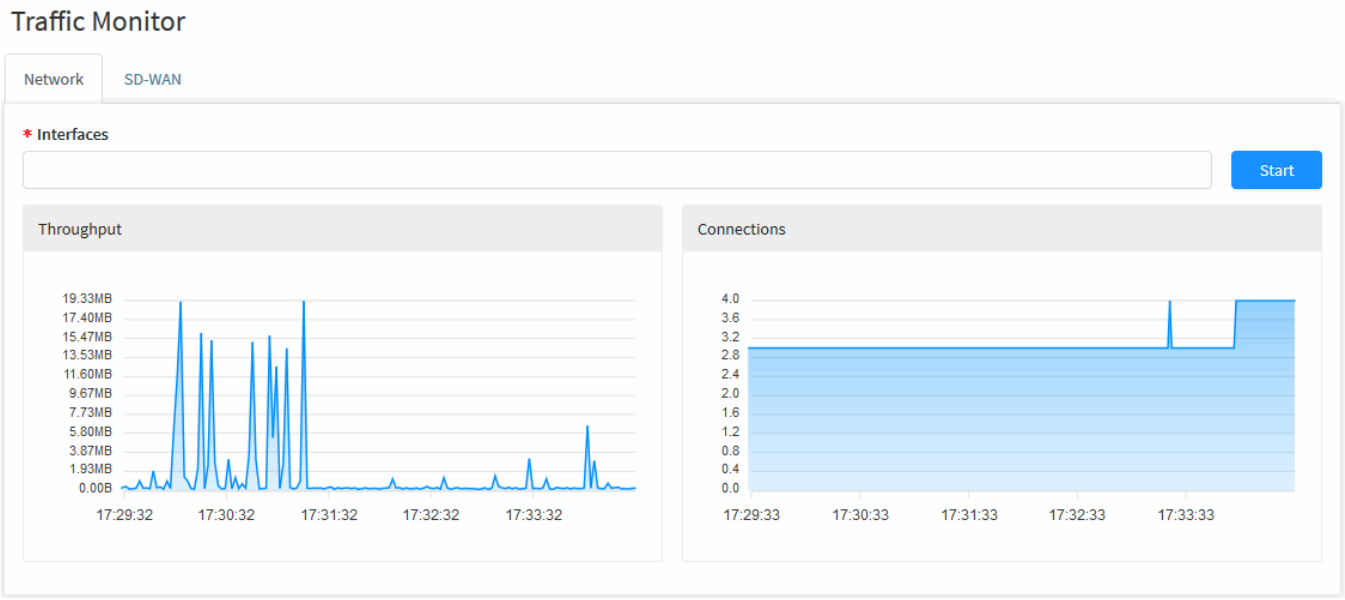
On the Network tab of the Traffic Monitor, it's possible to follow the network performance and traffic in real time.

To access it, if the tab is not selected, click on "Network".



Network Tab

The screen shown below will appear:

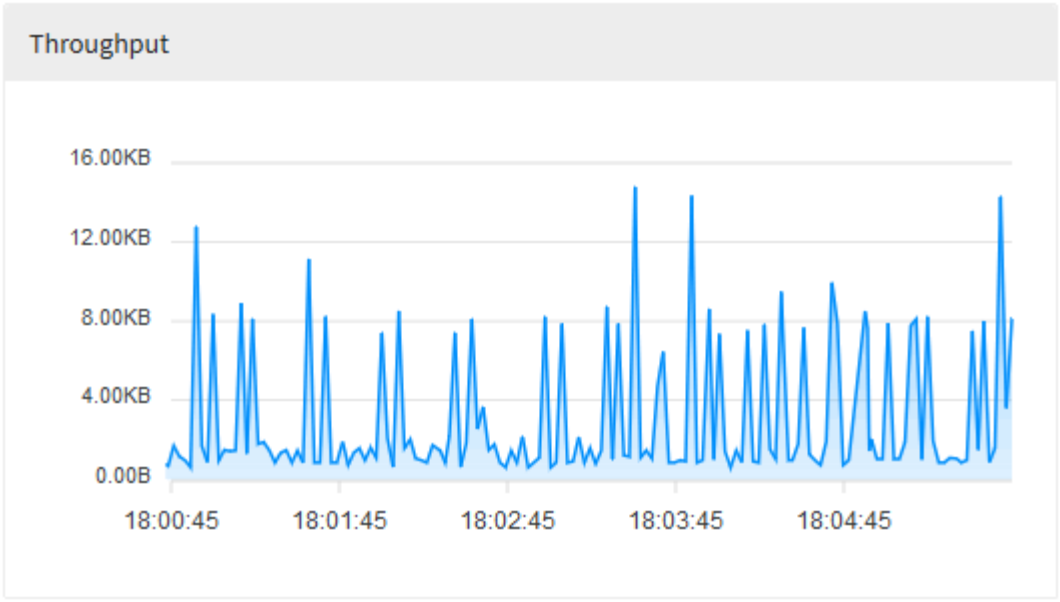


Traffic Monitor - Network

Next, we will analyze each component of this screen:

Throughput Graph

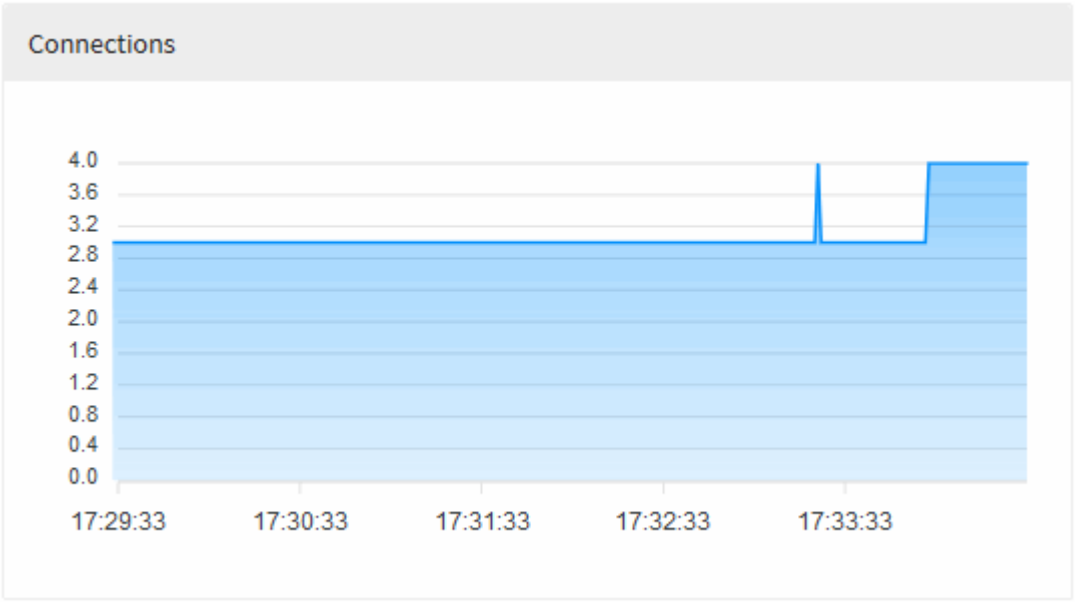
The Throughput graph shows the historical performance of the network in real time. When hovering the mouse over, it is possible to view a summary of the selected period.



Traffic Monitor - Network - Throughput

Connections Graph

The Connections graph shows a history of simultaneous connections and the consumption that your traffic causes in real time. By hovering the mouse over, it is possible to view a summary of the selected period.

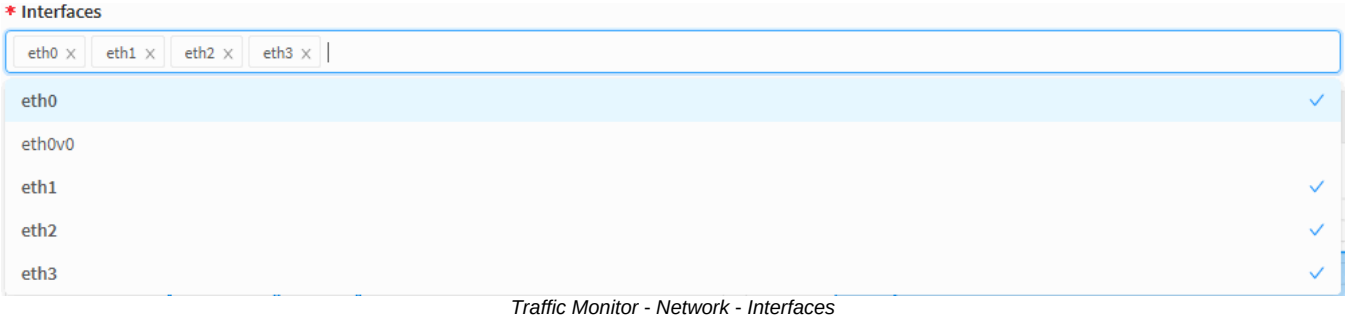


Traffic Monitor - Network - Connections

Real-time interface monitoring

The bar located at the top of the screen serves to monitor the network interfaces that are selected in real time.

It is possible to add the interfaces to be monitored, to do so, type or select them from the list, as shown in the image:

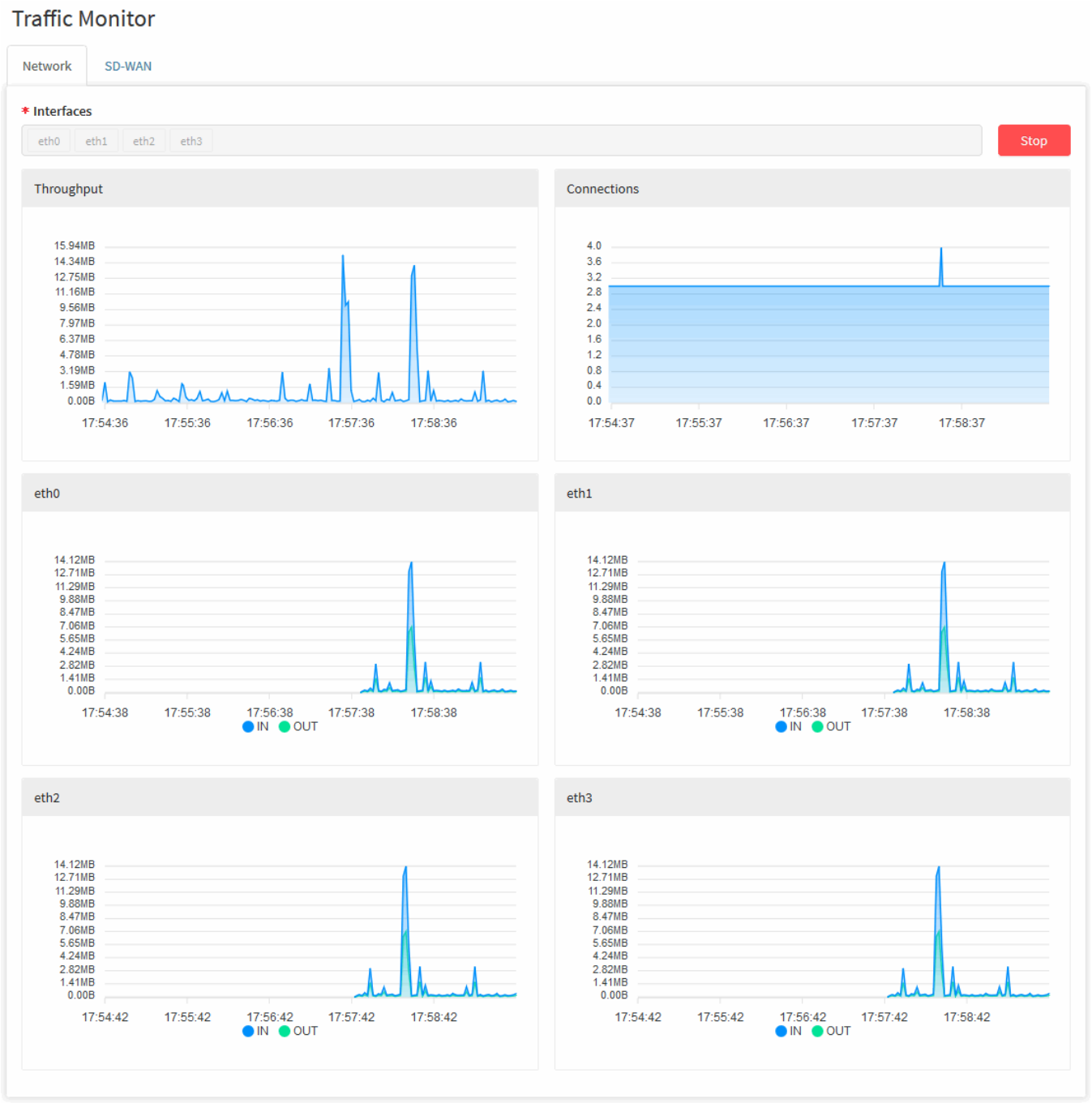


Traffic Monitor - Network - Interfaces

The maximum number of interfaces that can be added for real-time monitoring is 4.

Click the **[** Start **]** button to start monitoring

New charts will be added below the Throughput and Connections charts and real-time monitoring will start, as shown below:



Traffic Monitor - Network - Real-time interface monitoring

If a monitoring is already being performed, it is possible to stop it by clicking [Stop].

Traffic Monitor - SD-WAN

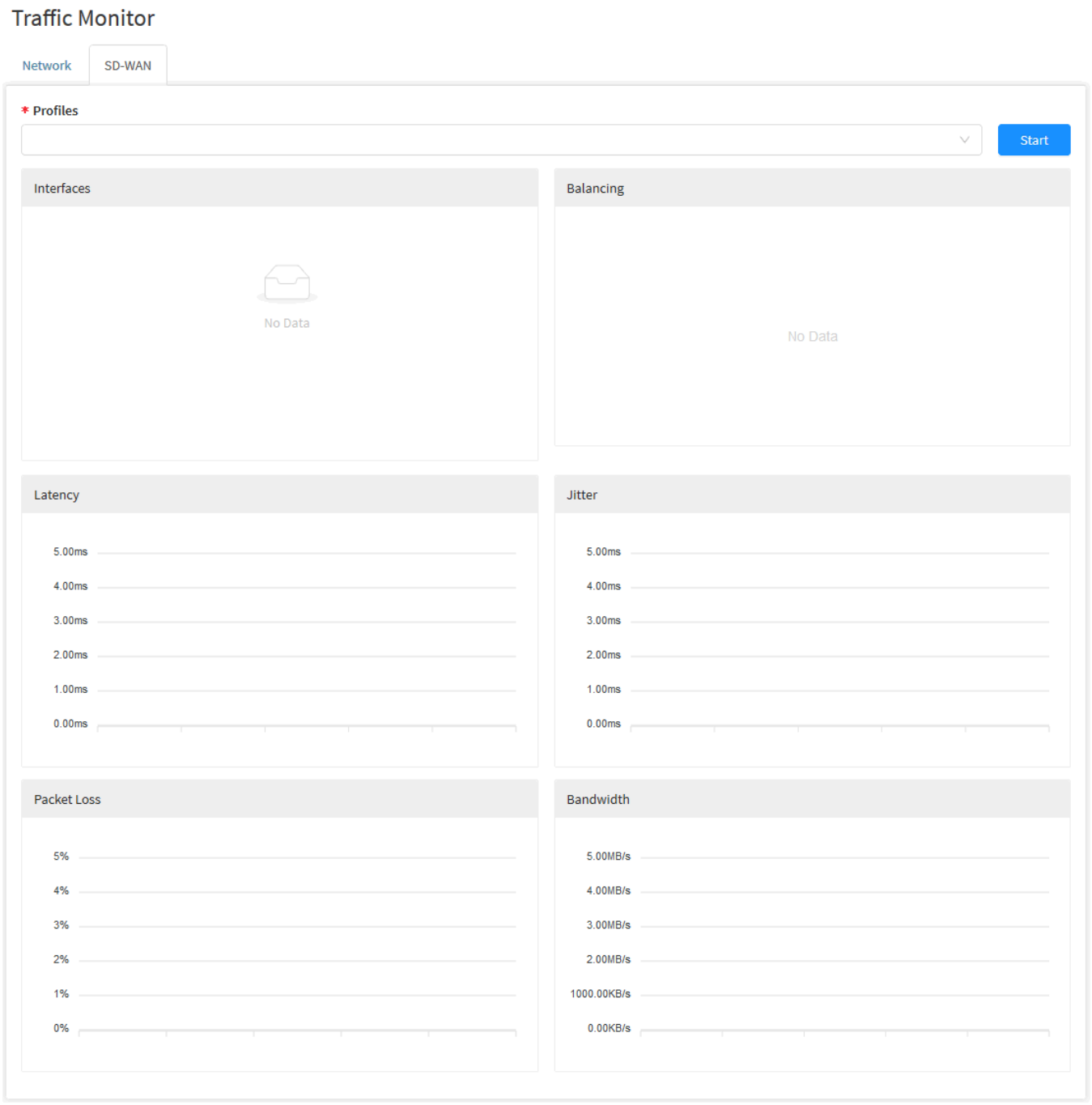
In the Traffic Monitor's SD-WAN tab, it is possible to monitor the performance of the SD-WAN interfaces, performance indexes and profiles in real time.

To monitor the SD-WAN, it is necessary to have a previously configured SD-WAN profile, for more information on this, check the Services - SD-WAN chapter.

To access, if the tab is not selected, click on "SD-WAN".

SD-WAN tab

The screen shown below will appear:



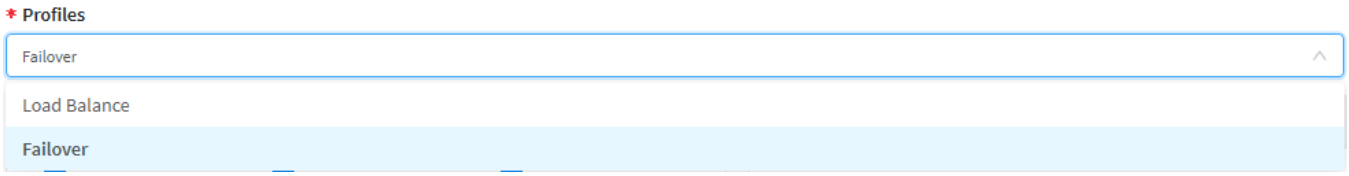
Traffic Monitor - Network

Next we will analyze each component of this screen:

Real-time SD-WAN monitoring

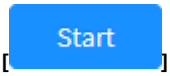
The bar located at the top of the screen serves to monitor the selected SD-WAN profiles in real time.

To do so, select it from the list, as shown by the image:

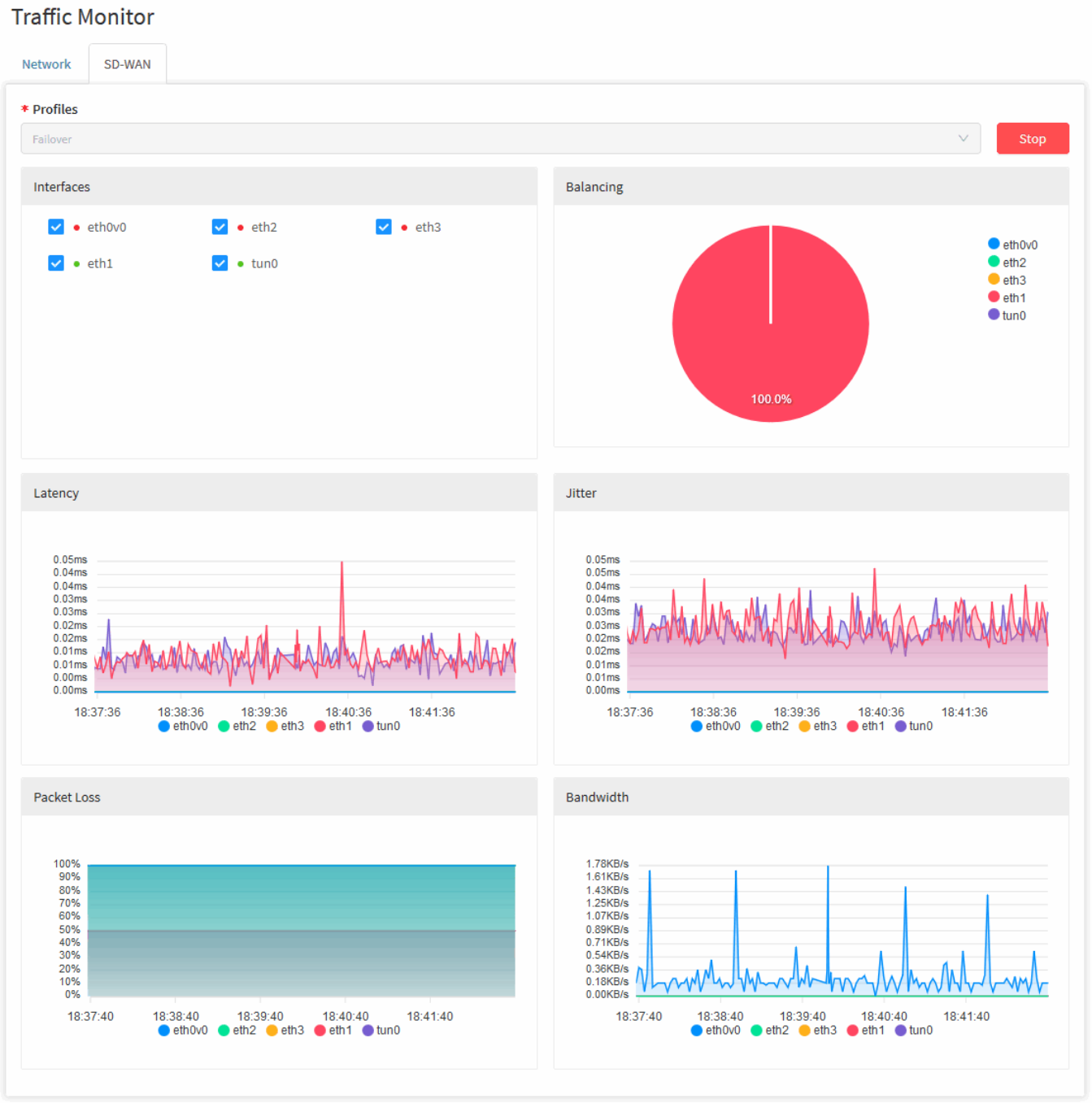


Traffic Monitor - SD-WAN - Interfaces

You can only monitor a single SD-WAN profile at a time.

Click the **[**  **]** button to start monitoring.

The graphs will be built according to the selected profile and real-time monitoring will start, as shown below:

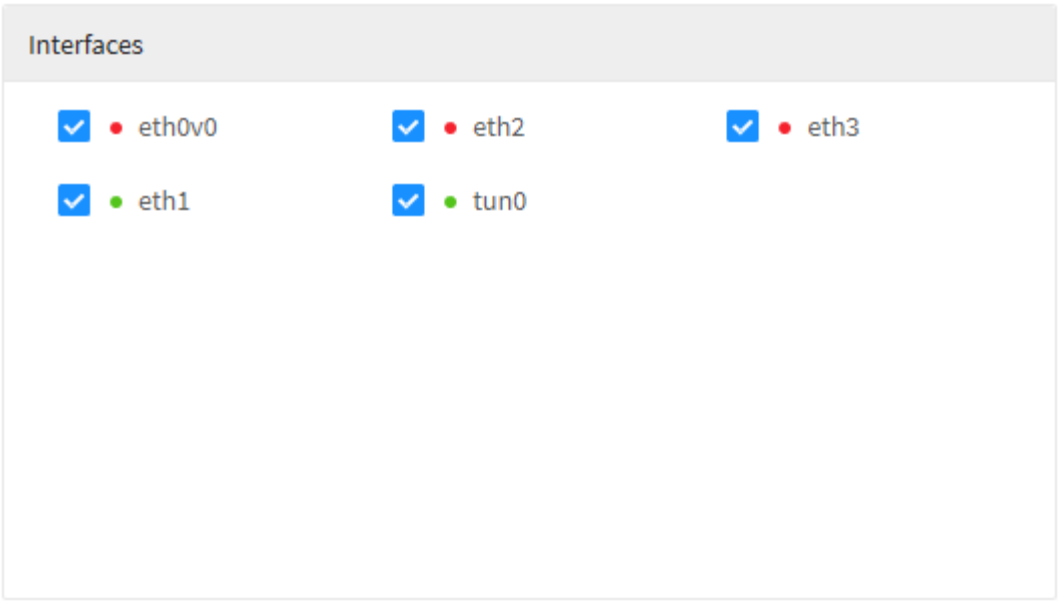


Traffic Monitor - *SD-WAN* - Real-time monitoring

If a monitoring is already running, you can stop it by clicking [Stop].

Interface Panel

After choosing the SD-WAN profile to start monitoring, this panel will display all interfaces for the selected profile.

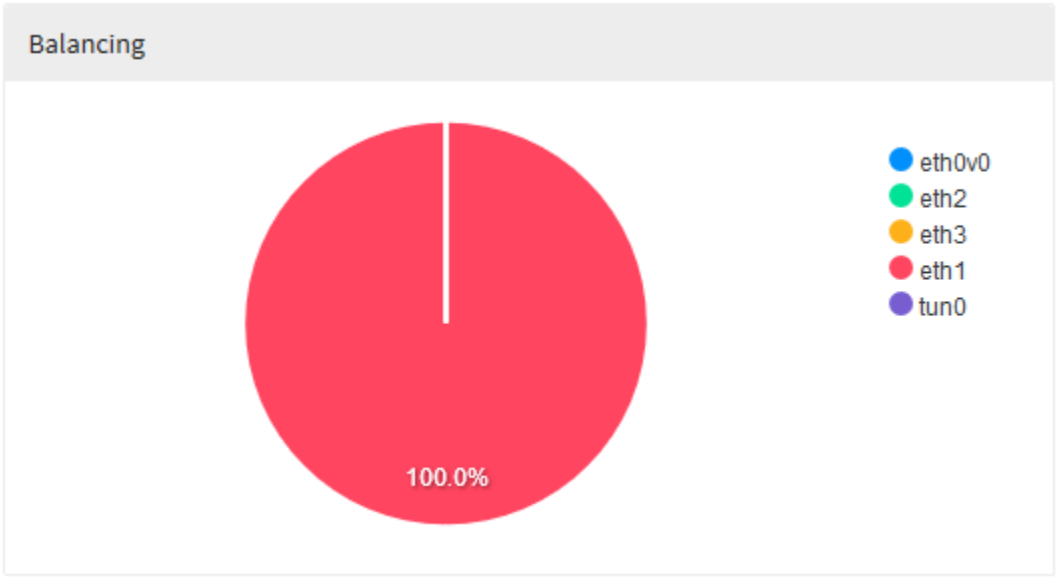


Traffic Monitor - SD-WAN - Interfaces panel

When you uncheck [ ] the checkbox for the interface, your information will be hidden from all graphics until your box is checked [ ] again.

Balancing Graph

This panel displays a graph representing the traffic balanced percentage of each interface.

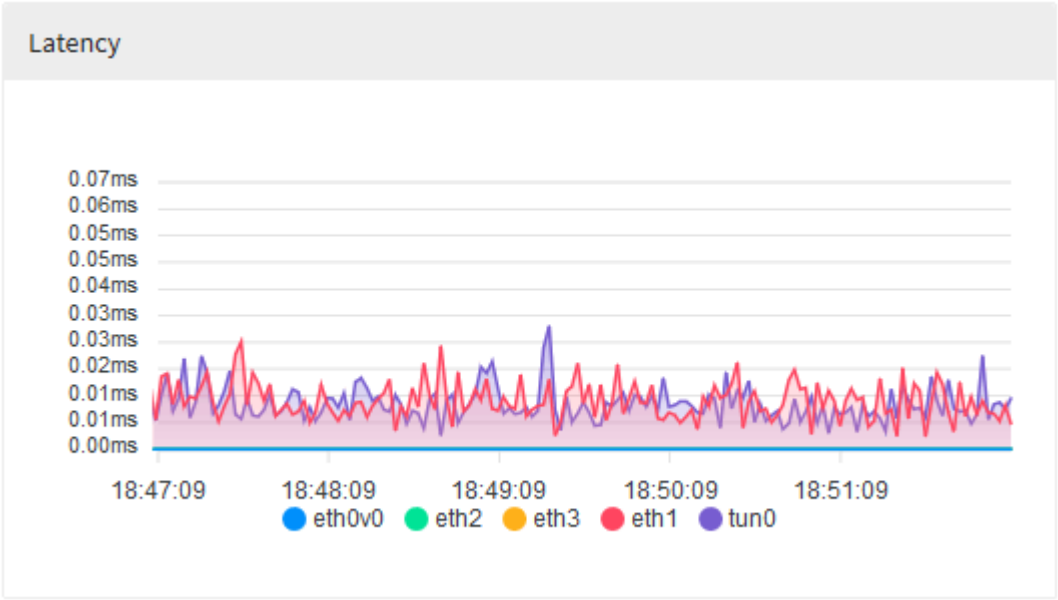


Traffic Monitor - SD-WAN - Balancing Panel

When hovering the mouse over the graph or the interfaces in the side legend, it is possible to view a summary for the period and the selected interface.

Latency Graph

This panel displays a graph showing the SD-WAN's performance history according to the real-time latency index.

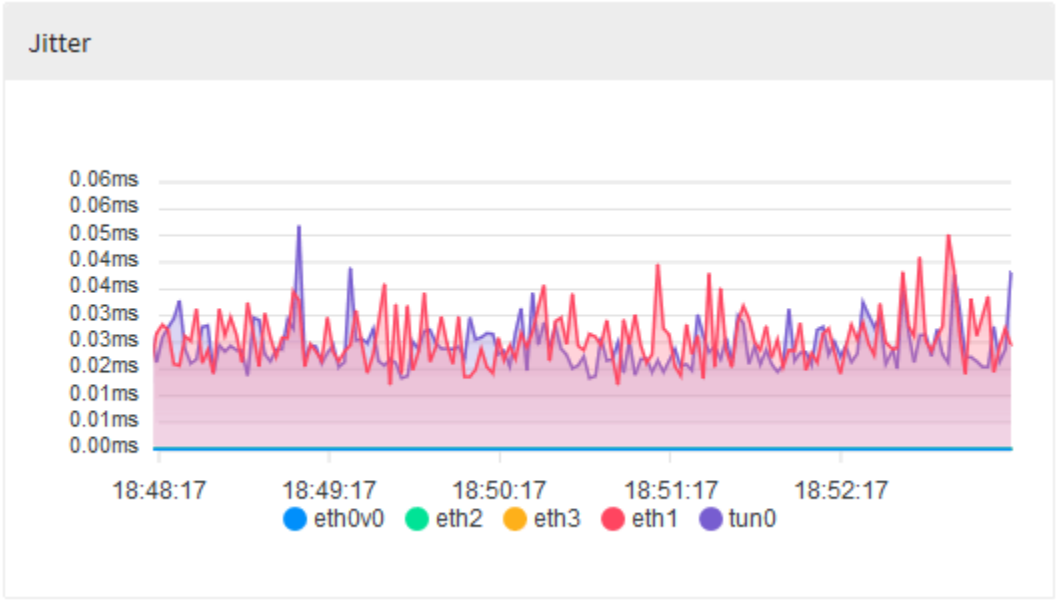


Traffic Monitor - SD-WAN - Latency Graph

When hovering the mouse over the graph or the interfaces in the lower legend, it is possible to view a summary for the period and the selected interface.

Jitter Graph

This panel displays a graph showing the SD-WAN's performance history according to the real-time jitter index.

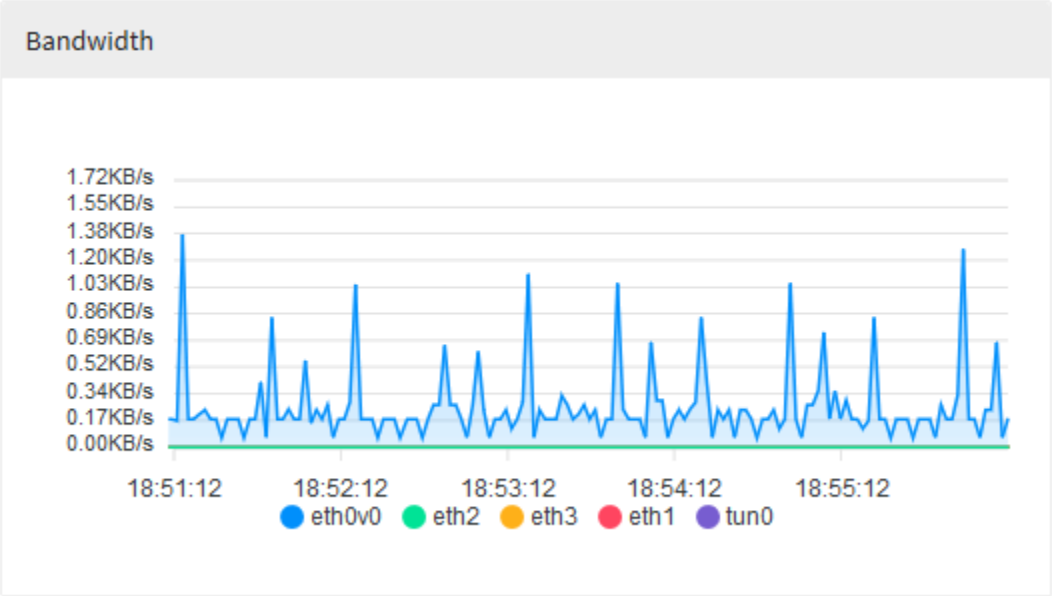


Traffic Monitor - SD-WAN - Jitter Graph

When hovering the mouse over the graph or the interfaces in the lower legend, it is possible to view a summary for the period and the selected interface.

Packet Loss Graph

This panel displays a graph showing the SD-WAN's performance history according to the real-time bandwidth index.



Traffic Monitor - SD-WAN - Bandwidth

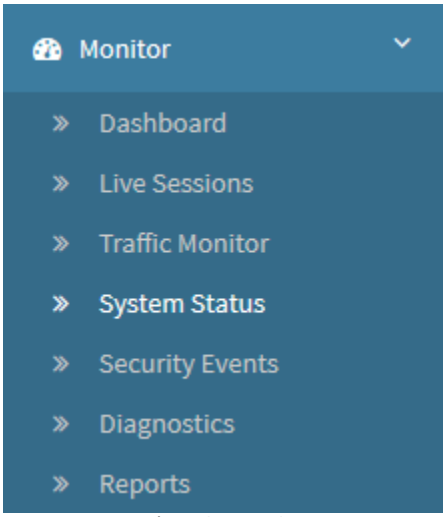
When hovering the mouse over the graph or the interfaces in the lower legend, it is possible to view a summary for the period and the selected interface.

For more information on the SD-WAN, check the Services - SD-WAN chapter.

Monitor - System Status

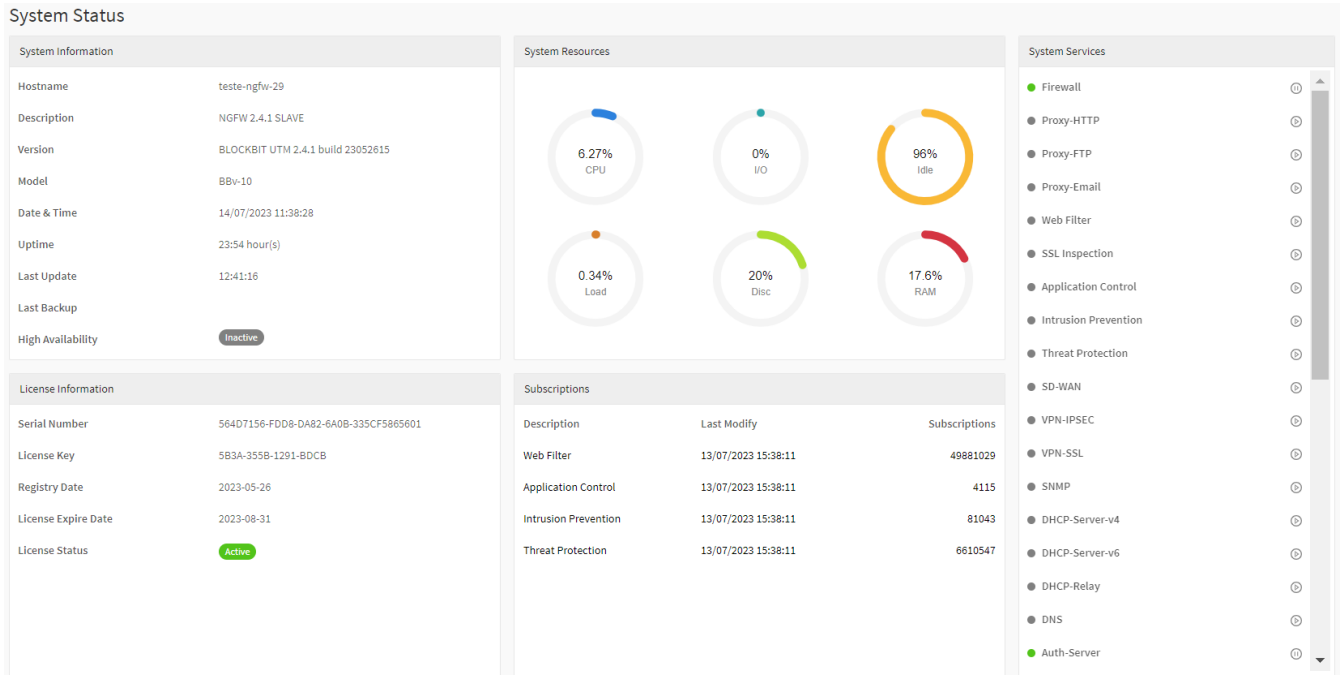
This feature allows the administrator to view "System", "License" and "Subscriptions" databases and information on the WEB interface, also allowing to view and change the "Status of modules and services".

To access this screen, just select the option “System Status”.

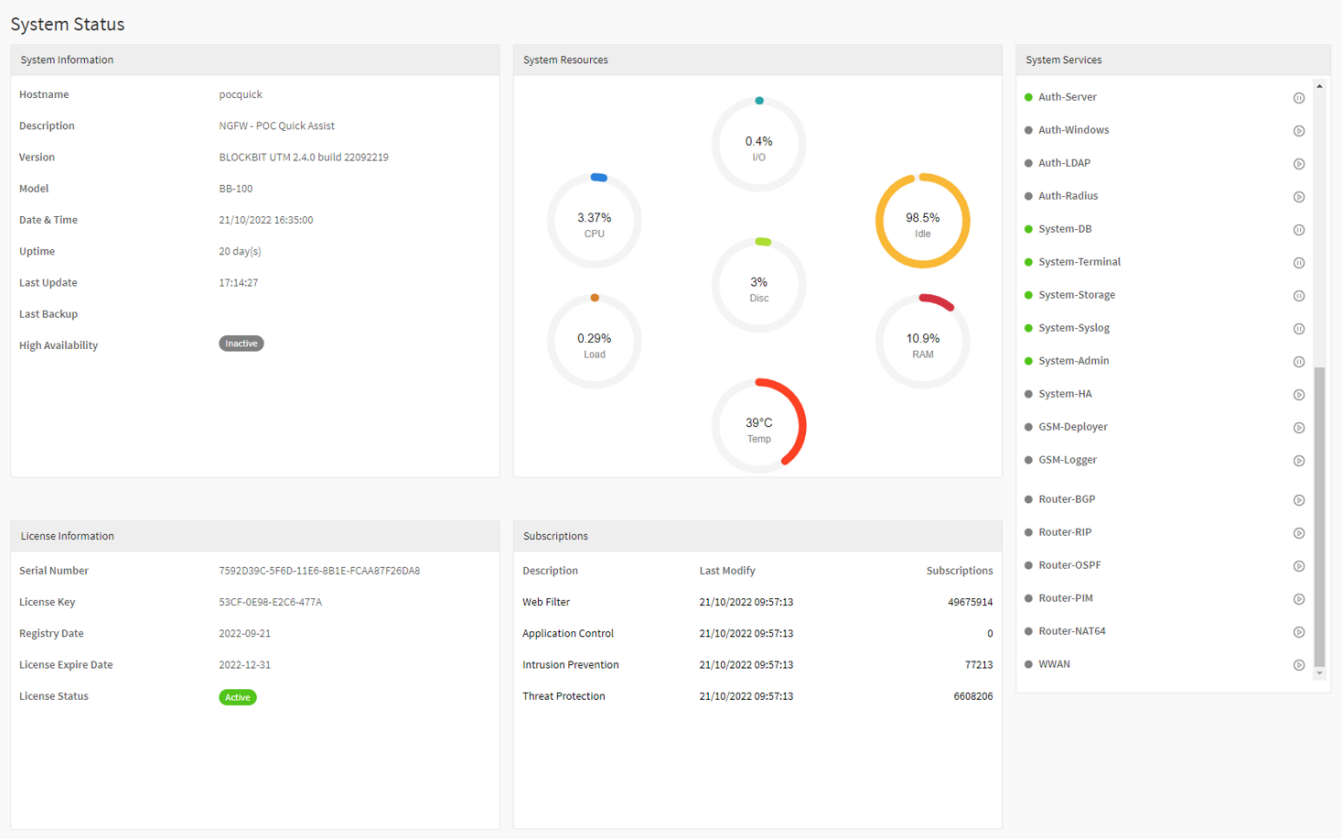


Monitor - System Status

The screen below will appear:



System status - Virtual appliance view



System status - Physical appliance view

Please note that when using physical appliances, the temperature display widget will be shown alongside the others.

This panel is composed of:

- ***System Information:*** General device information;
- ***System Resources:*** Hardware features of the device;
  - CPU usage (%);
  - Input and Output (I/O) (%);
  - Availability (%);
  - *Load Average* (%);
  - Disk Usage (%);
  - RAM memory (%);
  - CPU temperature (°Celsius).
- ***License Information:*** BLOCKBIT Device Number (UUID) and license identification information;
- ***Subscriptions:*** Status of update bases;
  - *Antimalware*;
  - *ATP – Advanced Threat Protection* – (Applications);
  - *ATP – Advanced Threat Protection* – (IP reputation);
  - *ATP – Advanced Threat Protection* – (Threats);
  - *IPS – Intrusion Prevention System* (*IPS*);
  - *WGS* (Browsers);
  - *WGS* (Applications);
  - *WGS* (Site categories and URLs).
- ***System Services:*** Status of services and resources.

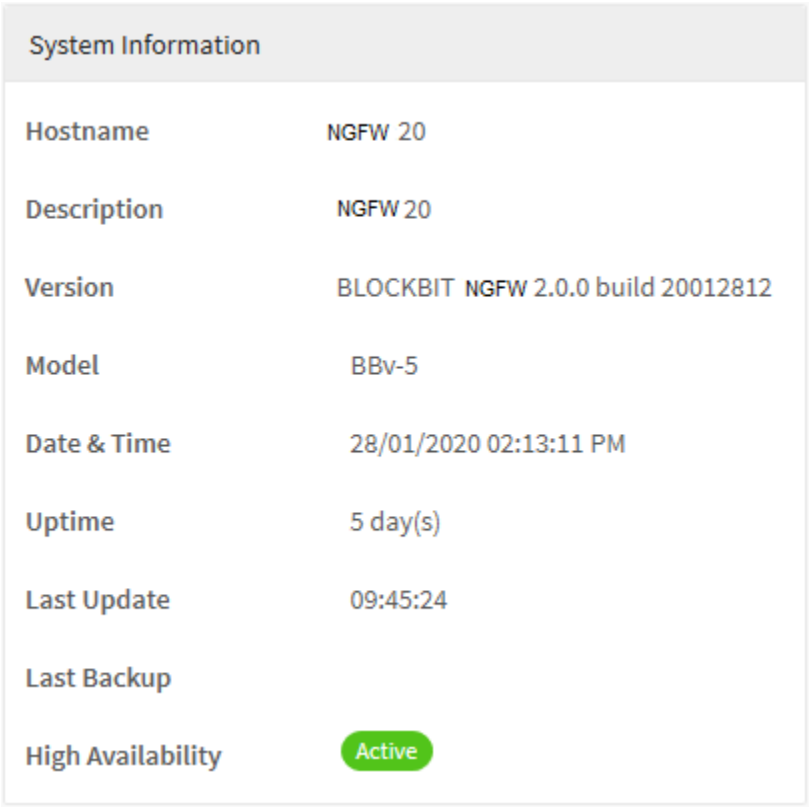
System Status - Widgets

Next, we will analyze each component of the widgets on this screen.

System *Information*

The “Information” widget displays Blockbit NGFW firmware information, such as:

- ***Hostname*:** DNS name configured on the device. Ex.: utm.blockbit.com;
- ***Description*:** Inform the application name. Ex.: Blockbit NGFW;
- ***Version*:** Reports the version and build of the application. Ex.: BLOCKBIT NGFW 2.0.0 build 20020413;
- **Model:** Inform the equipment model, if it is an appliance. Ex.: BBv-5;
- ***Date & Time*:** Reports the system date and time. Ex.: 05/02/2020 10:59:57 AM;
- ***Uptime*:** Reports the time in hours that the system is active. Ex.: 23:40 hour(s);
- ***Last Update*:** Determines when the last update was. Ex.: 11:14:56;
- ***Last Backup*:** Determines when the last backup was;
- ***High Availability*:** Defines whether High Availability is active or not.

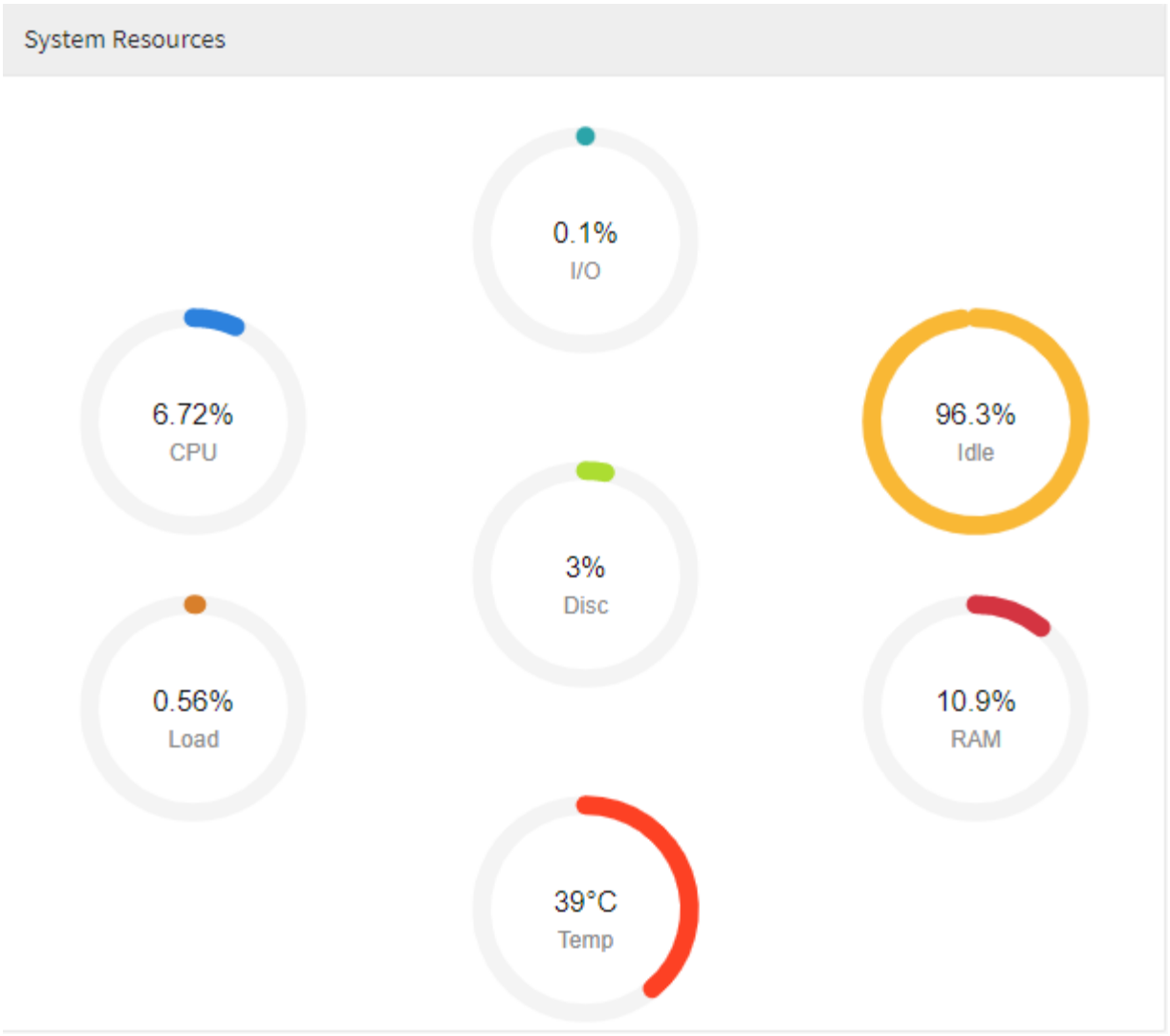


Dashboard - System Information

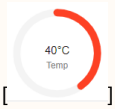
System Resources

The “Resources” widget displays information about the Blockbit NGFW hardware resource, such as:

- ***CPU*:** Displays the percentage of system CPU usage in real time. Ex .: 2.25% utilization;
- **I/O:** Displays the percentage of use of the capacity for writing and reading the system disks. Ex .: 19.1%;
- ***Idle*:** Displays the percentage available for CPU usage. Ex .: 97.8%;
- ***Load*:** Reports the average CPU usage of the system (load average) for the last 5 minutes. Ex .: 0.23%;
- ***Disc*:** Reports the% of space used on the system disks. Ex .: 20.3%;
- ***RAM*:** Displays the percentage of system RAM usage in real time. Ex .: 22.9% utilization;
- ***Temp:*** Shows the temperature of the CPU in Celsius degrees.



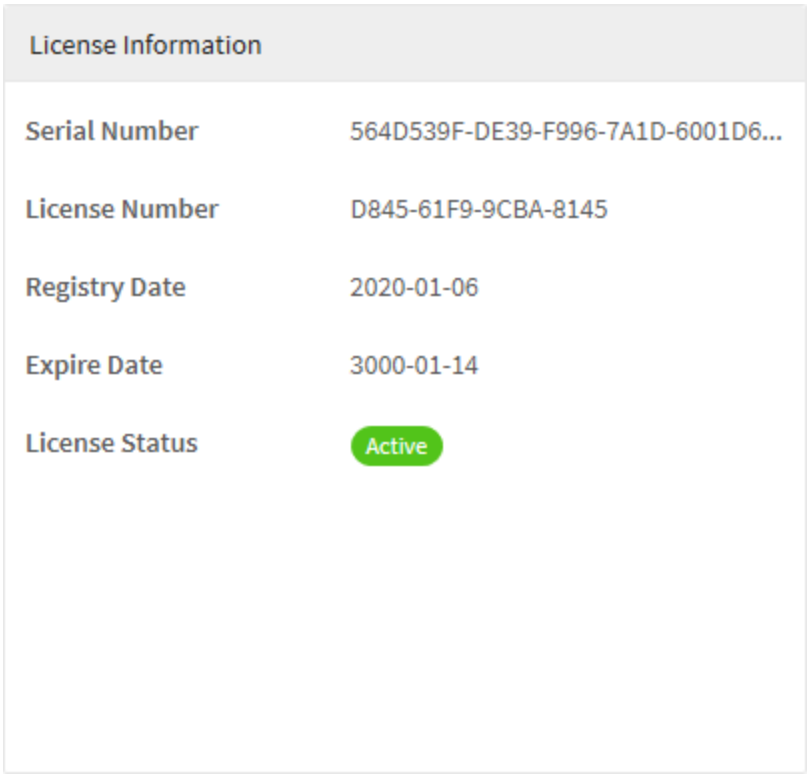
Dashboard – System Resources

 Note that the Temp widget [] will NOT be displayed on a virtual appliance. This feature will only be made available if a physical appliance is in use.

License Information

The “License” widget displays Blockbit NGFW activation license information, such as:

- ***Serial Number*:** Displays the appliance's unique identification code (UUID). This ID is used to identify the hardware for validating the use license;
- ***License Number*:** Displays the license number of the appliance. Ex .: D845-61F9-9CBA-8145;
- ***Registry date*:** Displays the date the license was registered on the system. Ex .: 2017-12-18;
- ***Expire Date*:** Displays the system license expiration date. Ex.: 2018-01-31;
- ***License Status*:** Displays the status of the license, active or inactive.



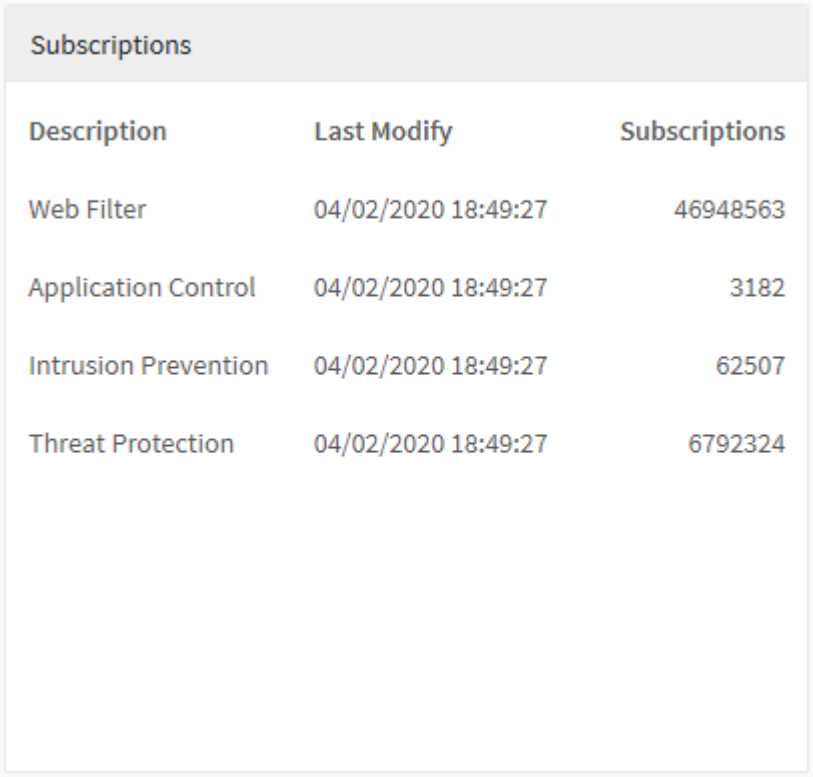
Dashboard – License Information

Subscriptions

The “Subscriptions” widget displays the latest modification, subscriptions and information from the Blockbit NGFW subscription bases, such as:

- ***Web Filter***;
- ***Application Control***;
- ***Intrusion Prevention***;
- ***Threat Protection***.

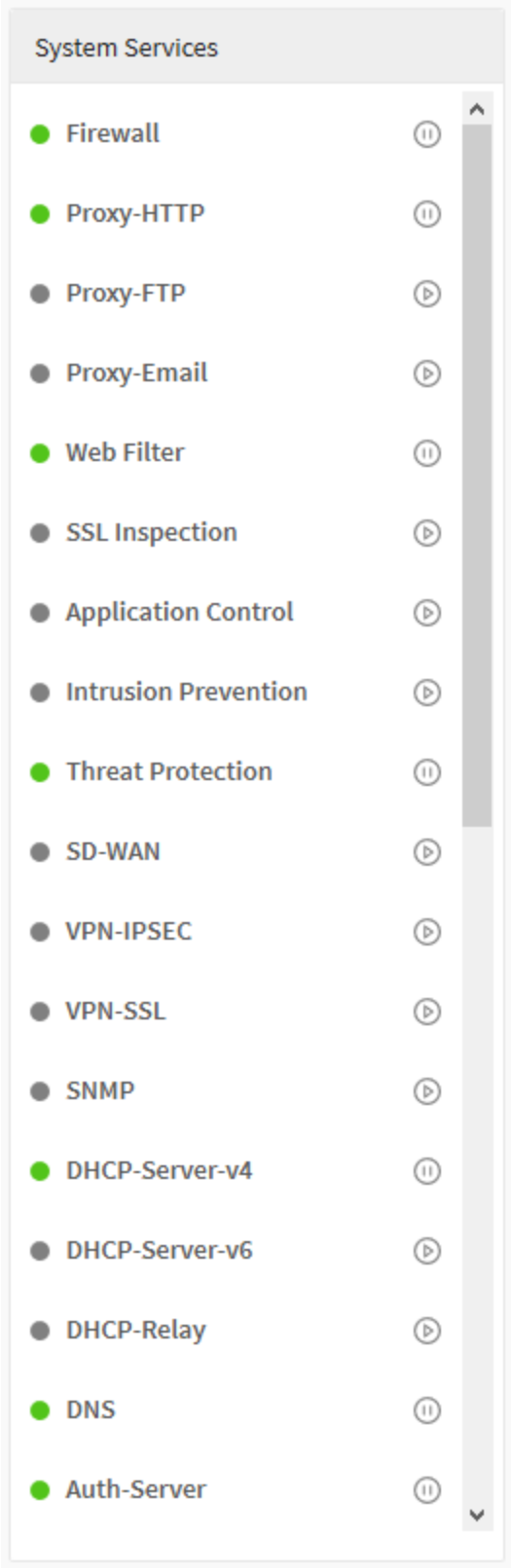
All databases are constantly updated by Blockbit, guaranteeing the effectiveness and safety of the environment.



Dashboard – Subscriptions

Services

The “Service” widget displays the status of Blockbit NGFW services and features, enabling you to restart or stop them:



Dashboard – Services

You can view the service status on this panel, as follows:

- **Active [●];**
- **Inactive [●].**

In "Services" it is possible to restart and stop the services, next to the service name, follow the buttons:

- **Start [ ]**;
- **Stop [ ]**.

> It is not possible to stop some specific services.

To stop a stopped service, click on **[ ]**, the notification below will be displayed.

Stop service

To activate a stopped service, click on **[ ]**, the notification below will be displayed.

Start service

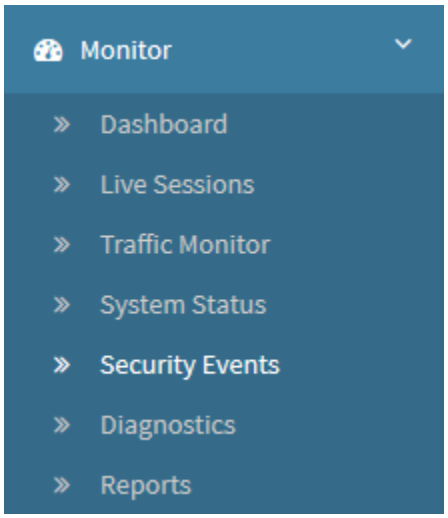
Monitor - Security Events

The "Security Events" panel's main function is to display all instances of Blockbit NGFW.

This panel has some features that allow a more detailed in-depth analysis: Through this panel it is possible to perform a search according to personalized queries, to analyze specific incidents and eventualities, allowing a much more precise and efficient administration.

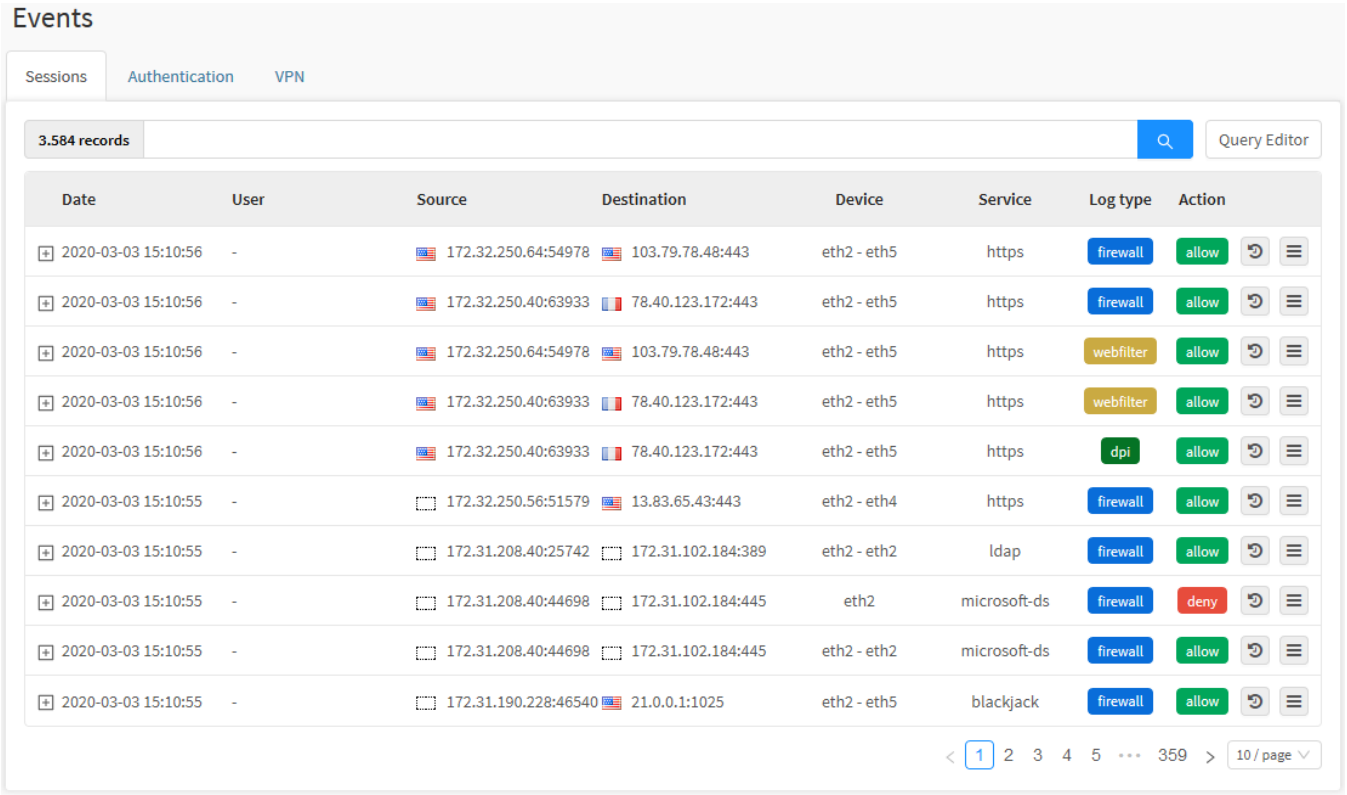
The main difference between the reports displayed in Events and those in Analyzer is:
In Events, a connection record is generated with zeroed attributes (bytes and packets), after disconnection another event is generated recording these attributes, the traffic and the connected time.
In Analyzer, the reports are summarized every 5 minutes, generating reports from time to time with data generated in the period.

To access this screen, just select the option "Security Events".



Monitor - Security Events

The screen below will appear:



Events

ATTENTION: It is not possible to generate detailed logs without having applied an inspection policy. For more information, see this page.

This screen contains the following tabs:

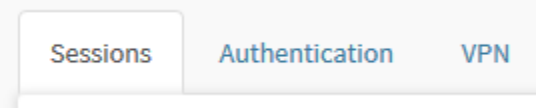
- *Sessions*;
- *Authentication*;
- *VPN*.

Next, the components of the events panel will be analyzed.

Security Events - Sessions

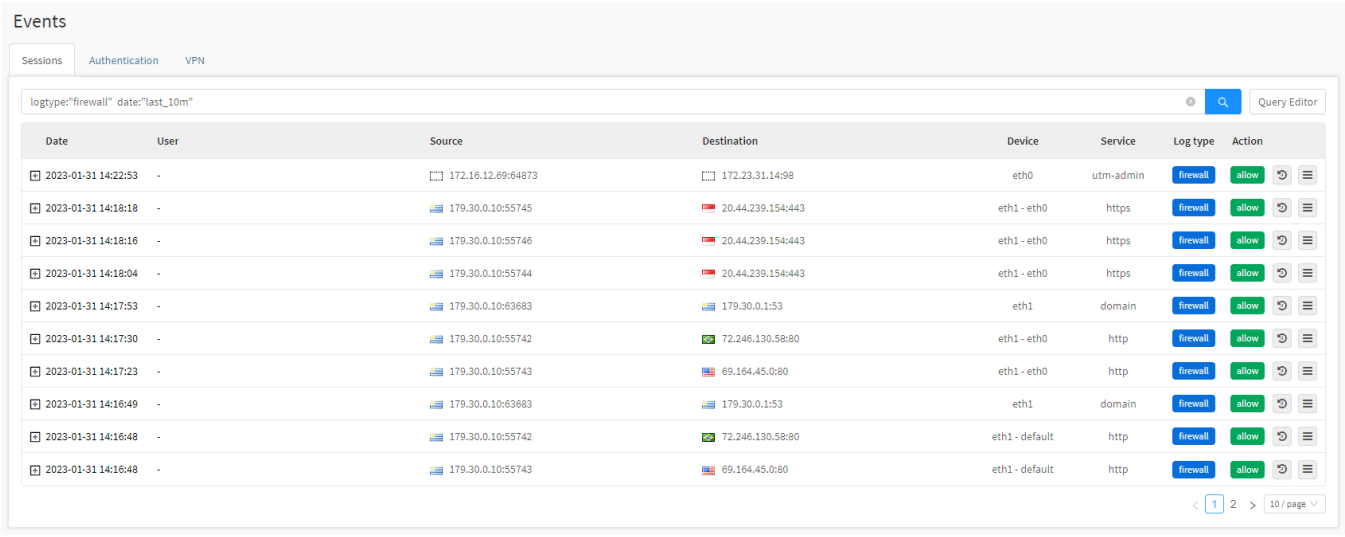
In Sessions we have a record of all events detected in the sessions of this device.

To access, if the tab is not selected, click on "Sessions".



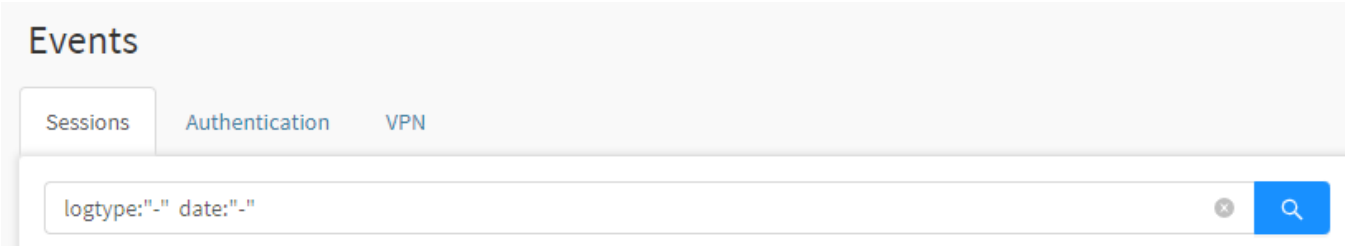
Sessions tab

The screen shown below will appear:

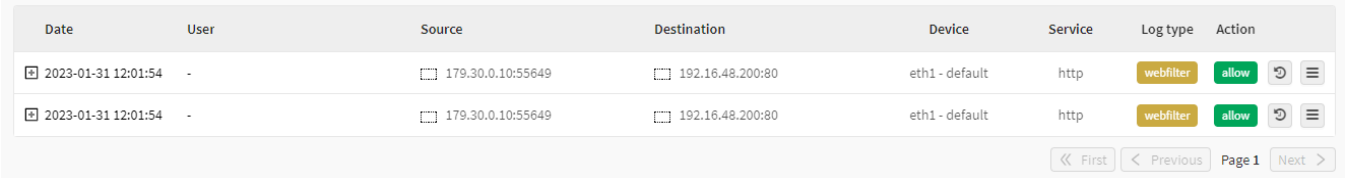


Security Events – Sessions

In the search bar, it is possible to change the "logtype" to also view other types of serviços and the period you need to verify. Check the example below.



Events - Sessions - Search bar



Events - Sessions - logtype:"webfilter"

This panel consists of the *Query Editor* and the following columns:

- ***Expand[ ]:*** Expand the event, for more information check this page;
- ***Date*****:** We have the exact date and time for this event;
- ***User:*** The user who generated this event;
- ***Source*****:** We have the source of this event, an IP address. This filed is also usable as a filter for searches;
- ***Destination*****:** We have the destination of this event, another IP address. This filed is also usable as a filter for searches;
- ***Device:*** Defines the device that generated this event. This filed is also usable as a filter for searches;
- ***Service*****:** We have the service tied to this event. This filed is also usable as a filter for searches;
- ***Log Type*****:** Determines the type of record for this event. This filed is also usable as a filter for searches;
- ***Action:*** *It defines what action the policies took regarding this event. This filed is also usable as a filter for searches;*
- ***Search* com *ID*[ ]:** Allows you to search using the event ID as a filter;
- **Event view[ ]:** Allows you to access the Event view *window.*

Next, we'll look at how to expand an event to see more information about it.

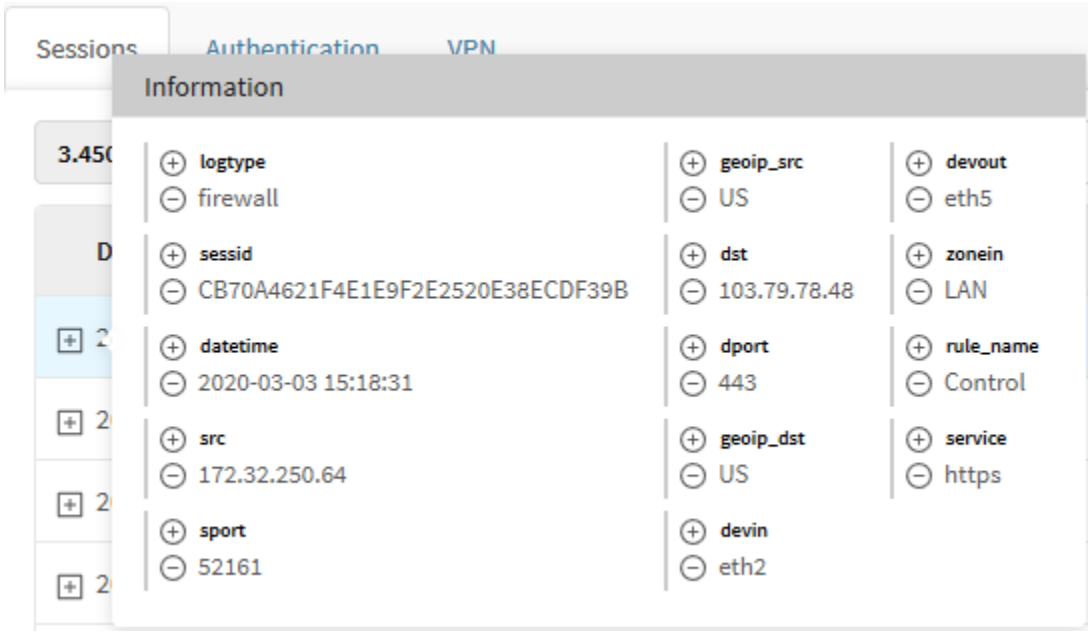
Sessions - Event View

The Event View **[**  **]** button displays further details of the event in question, as shown in the image below:

Sessions - Event View

Sessions - Expand Sessions

Right next to the event's date side we have an **[⊞]** icon which, when selected, will expand the selection and display more information about that specific event.



Events – Log Events – Expanded

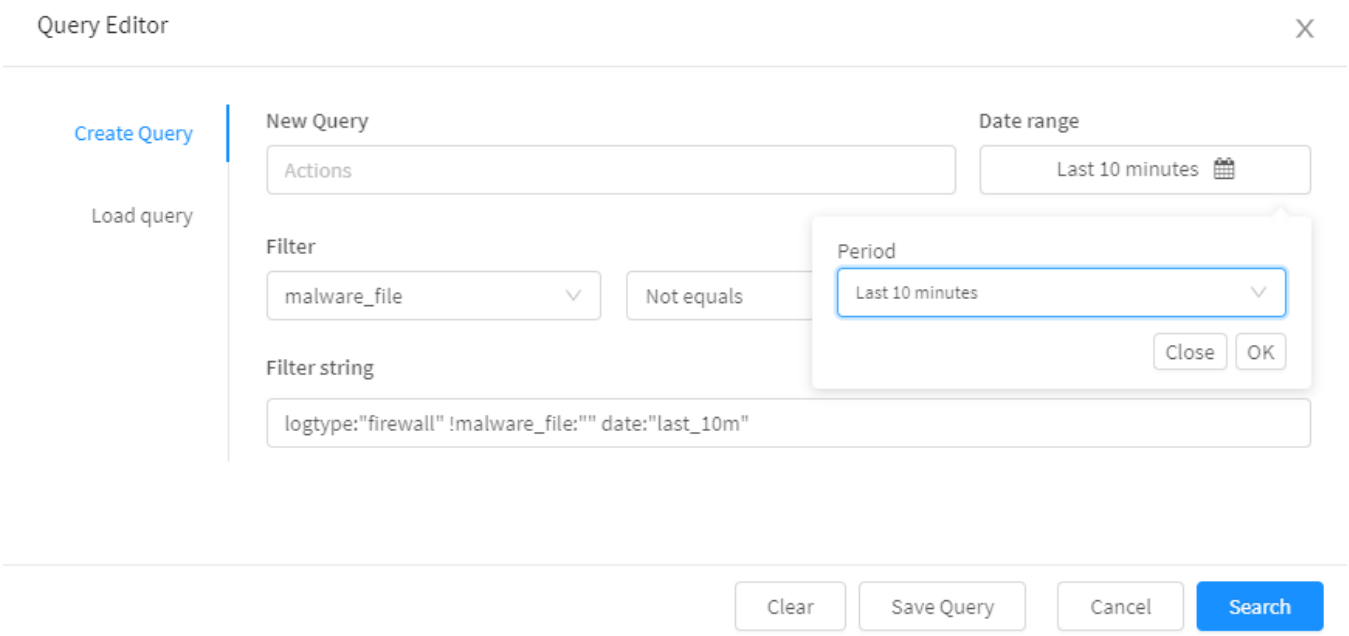
By clicking on the **[⊕]** icon, the information in front of it is used as a filter and a search is performed.

By clicking on the **[⊖]** icon, the information is removed from the filter and a search is performed.

Next, let's look at the Query Editor.

Sessions - Query Editor

Through the query editor, it is possible to create, edit and save a query to perform an in-depth search of events, by clicking on the [Query editor] button the following window will be displayed:

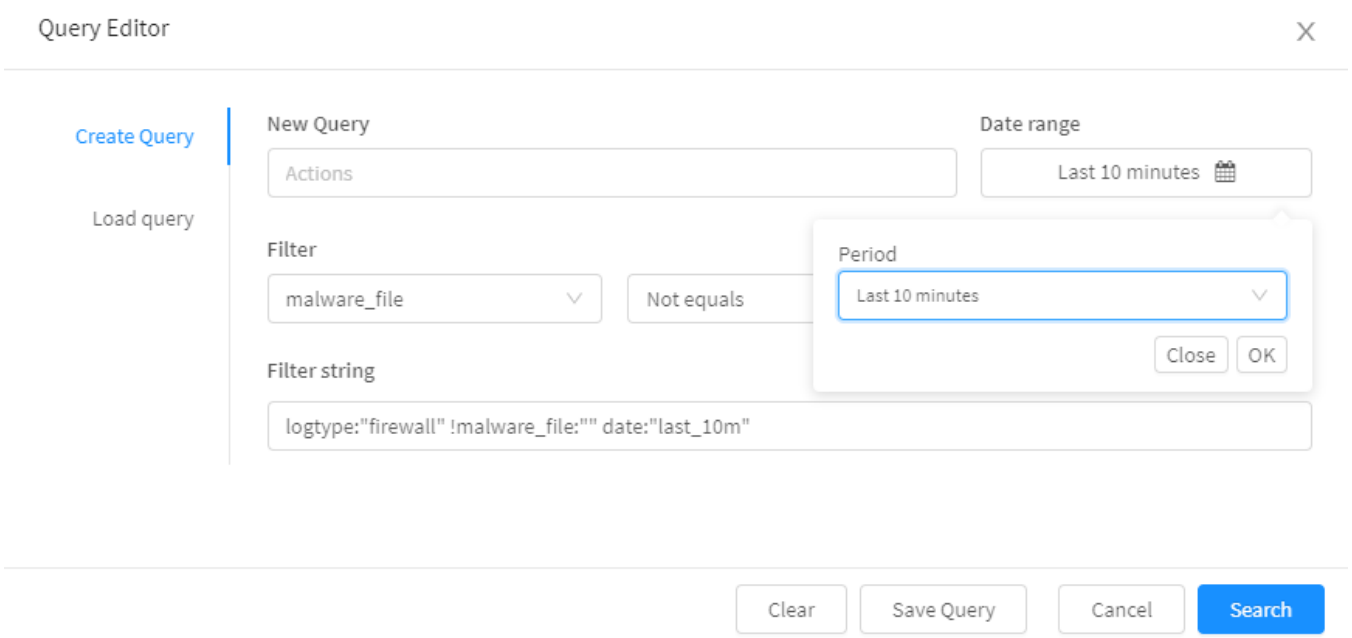


Events - Query Editor

Next we will analyze each field in this window:

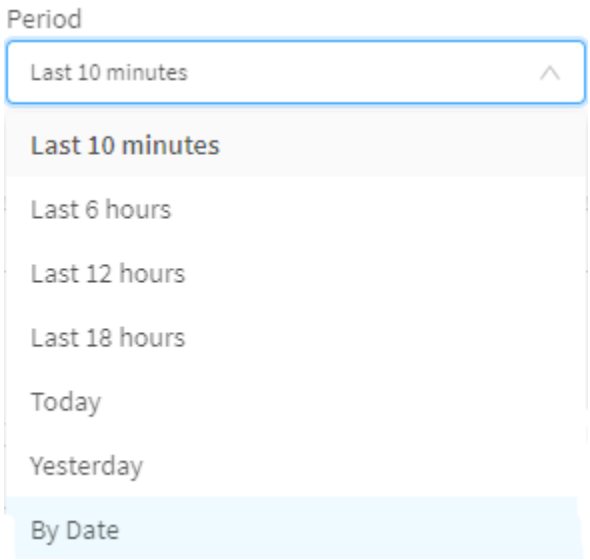
Events - Query Editor - Create query

In the "Create query" tab it is possible to configure how the query will act:



Events - Query Editor - Create query

- ***New query:*** Determines what the query name will be. *Ex.: Last 7 days;*
- ***Date range:*** Allows you to determine a period to filter results more accurately, possible options are:



Date Range's options

  - **Last 10 minutes:** Shows the results for the last 10 minutes;
  - **Last 6 hours:** Shows the results for the last 6 hours;
  - **Last 12 hours:** Displays the results for the last 12 hours;
  - **Last 18 hours:** Shows the results for the past 18 hours;
  - **Today:** Displays results specifically for today's date;
  - **Yesterday:** Displays results specifically for yesterday;
  - **By date:** Sets a specific date.

⚠ For more information, regarding the filters shown in the filter selection box, check this page of the GSM manual.

- ***Filter:*** This checkbox allows you to select the type of filter used by the query*;*

- **logtype:** Selects the log by its type, the available options for this filter are: Webfilter, Firewall, DPI, IPS, ATP;
- **src:** Makes the selection by the origin IP, this filter accepts IPv4 or IPv6 addresses as value: Ex.: 172.16.12.171;
- **dst:** Makes the selection by the destination IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 172.16.12.171;
- **sport:** This filter enables the selection by an origin port, ports are accepted as value: Ex.: 1 to 65535;
- **dport:** This filter enables the selection by a destination port, therefore, ports are accepted as value. Ex.: 1 to 65535;
- **protocol:** This filter allows the selection by protocol, the available options are: tcp, udp, icmp, ip;
- **service:** In this case, the selection is made by service, the accepted values are based on the IANA's table, for more information consult this page;
- **devin:** By making the selection by the entry device, this filter accepts interfaces, in order to learn how to create them, click here;
- **devout:** In this filter the selection is made by the output device, the accepted values are user-created interfaces, for more information on how to create them, check this page;
- **zonein:** This filter enables the selection by the entry zone, the accepted values are zones configured in the NGFW's interfaces. *Ex.: LAN, WAN, DMZ, etc. F*or more, click here;
- **zoneout:** This filter makes the selection by output zone possible, the accepted values are the zones that can be configured in the NGFW's interfaces. Ex.: LAN, WAN,DMZ, etc. For more information check this *page.*
- **client_mac:** This one makes the selection by MAC address, so it accepts physical addresses. Ex.: 94:e6:f7:58:5d:db;
- **client_user:** This filter makes the selection by user, it accepts e-mails as values. Ex.: user@blockbit.com;
- **client_ip:** This filter makes the selection by the client's IP, the accepted values are IPv4 and IPv6 addresses. Ex.: 172.16.9.153;
- **geoip_src:** In this case the selection is made by the GeoIP's origin (IP address Geolocation), the accepted values are each coutry's abbreviation. Ex.: BR, US, CA, CN, etc;
- **geoip_dst:** Makes the selection by the GeoIP's destination (IP address Geolocation), the accepted values are each coutry's abbreviation. Ex.: BR, US, CA, CN, etc;
- **rule_name:** This filter makes the selection by the rule name, hence the name of the rules created in the NGFW are used as value, for more information, click here;
- **rule_action:** Makes the selection based on the action that the rule takes, this filter accepts the following options as value: *Allow, Alert* or *Deny. Ex.: Deny;*
- **web_category:** This filter enables the selection by web category, and accepts them as value. Ex.: Information Technology, Web Mail, Personal Network Storage and Backup, etc.
- **web_site:** Makes the selection by sites, this filter accepts URLs as value. Ex.: https://www.blockbit.com;
- **web_method:** Makes the selection by the HTTP methods, this filter accepts as value the POST and GET methods. Ex.: POST.
- **web_mime:** This filter allows the selection by MIME-Type, and also using this parameter as value. Ex.:"application/octet-stream",
- **ips_profile:** This one makes the selection by the Intrusion Prevention profile system, the accepted value is the profile name, for more on this, click here;
- **app_name:** This filter makes it possible to select by the application name. Ex.: Google APIs;
- **app_category:** Makes the selection by the application's category, which is also used as value. Ex.: web;
- **malware_file:** Makes the selection by the type of *malware* file;
- **malware_md5:** Selects by the malware's MD5*;*
- **malware_status:** Selection by the malware's status;
- **malware_name:** Selection by the *malware*'s name;
- **threat_class:** This filter makes the selection by the threat's class. Ex.: Potentially Bad Traffic;
- **threat_category:** Makes the selection by the threat's category. Ex.: USER_AGENTS;
- **threat_sid:** Selects by the threat's SID, this filter uses the threat's SID as value. Ex.: 2027916;
- **threat_name:** This filter makes the selection by the threat's name. Ex.: Poison Null Byte;
- **threat_impact:** In this case, the selection is made based on the threat's impact. Ex.: High, Medium, Low;
- **threat_dump:** Selects by the threat's dump. This filter accepts the threat's dump as value.
- **threat_payload:** Makes the selection by the threat's payload;
- **flow*:*** Shows the NAT that has been applied and which was the assigned address, alogside the IP address.

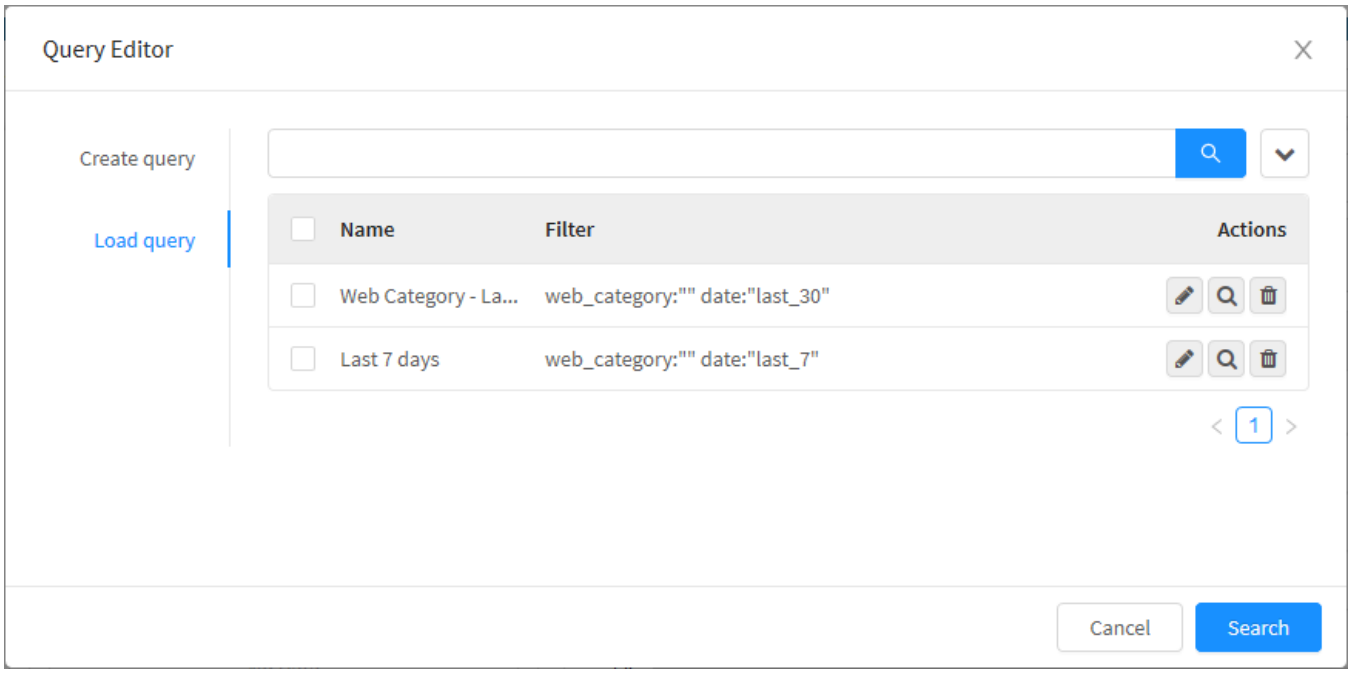
- ***Contain/Not Contain:*** This checkbox basically acts as a logical query filter operator;
  - ***Contain:*** Will display all results that contain the value of the next checkbox;
  - ***Not Contain:*** Will display all results that do NOT contain the value of the next checkbox.
- ***Value:*** This box determines the value that will be used to filter the query;
- ***Filter string:*** After editing the previous fields, click on **[** + **]** to display the string used by the search in this text box. You can manually edit this line of code.

To clear the configured query, click the **[** Clear **]** button. If you want to cancel click on the **[** Cancel **]** button. To perform a search using the query click on the **[** Search **]** button.

To save the query, click the **[** Save query **]** button.

Events - Query Editor - Load query

In the "Query Editor" tab it is possible to manage saved queries, this panel is composed of a search bar and an action button with the function of deleting all the selected fields, next we will analyze each component of this panel:



Events - Query Editor - Load Query

- ***Select[ ]:*** Allows you to select the desired query;
- ***Name:*** *Displays the name of the query;*
- ***Filter:*** Displays the string used by the search;
- ***Actions*****:** Displays a set of contextual buttons;
  - ***Edit[ ]*****:** Edit the query settings;
  - ***Search[ ]*****:** Performs a search using the query;
  - ***Delete[ ]*****:** Removes the query.

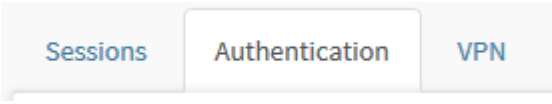
If you want to cancel click on the **[** Cancel **]** button. To perform a search using the selected query, click the **[** Search **]** button.

Next we will analyze the Event View.

Security Events - Authentication

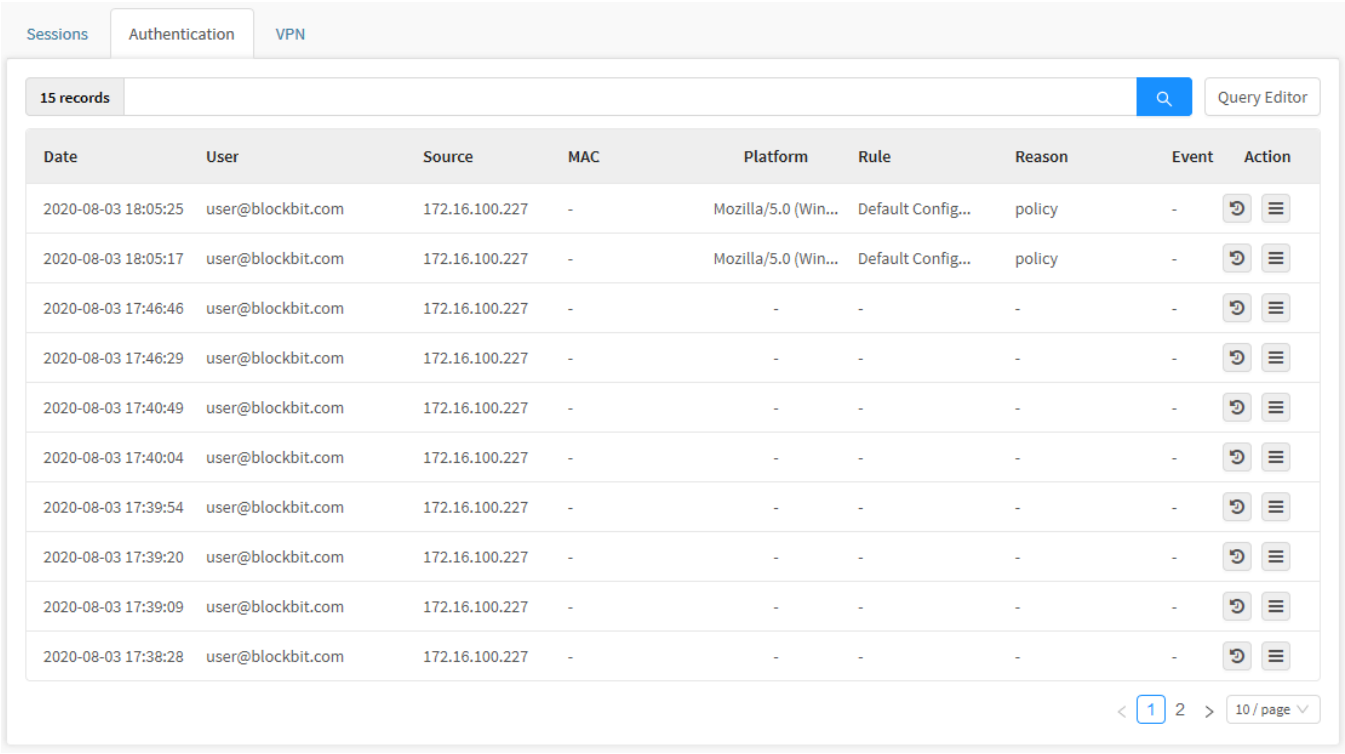
In Authentication we have a record of all authentication events detected on this device.

To access, click on "Authentication".



Authentication Tab

The screen shown below will appear:



Security Events - Authentication

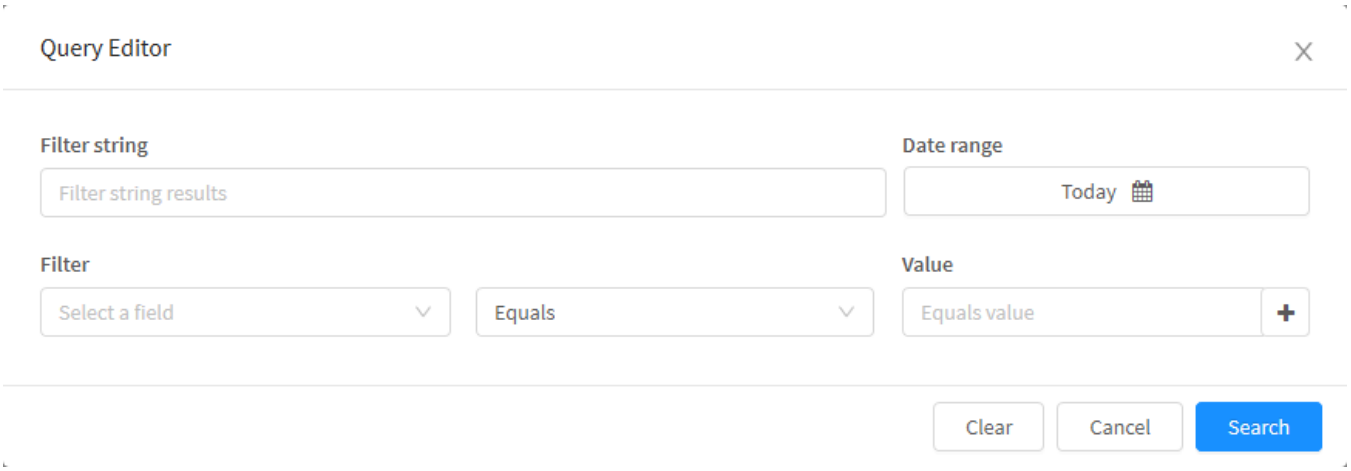
This panel consists of the *Query Editor* and the following columns:

- ***Date*:** We have the exact date and time for this event;
- ***User:*** The user who generated this event. This field can also be used as a filter for searches;
- ***Source IP*:** The source IP address of the user's device. This field can also be used as a filter for searches;
- ***MAC:*** *The physical address of the user's device*. This field can also be used as a filter for searches;
- ***Platform*:** Which platform was used by the user to access. This field can also be used as a filter for searches;
- ***Rule*:** Which authentication rule has been applied to the user, for more information about these rules, see this page. In addition, this field can also be used as a filter for searches;
- ***Reason*:** Displays the reason why this log was generated. This field can also be used as a filter for searches;
- ***Event*:** Displays the event that generated this log. *This field can also be used as a filter for searches;*
- ***Action*:** Displays the following buttons:
  - ***Session ID*** [ ]**:** Clicking on this button will perform a search with a query using specifically the session ID of the selected event;
  - ***Description*** [ ]**:** By clicking on this button the *Description* window will be displayed.

Next, let's look at the Query Editor.

Authentication - Query Editor

Through the Query Editor, it is possible to create, edit and save queries to perform an in-depth search of events, by clicking on the **[** Query editor **]** button the following window will be displayed:



Authentication - Query Editor

- ***Filter string:*** When editing the Date Range, Filter and Value fields, the string used by the search will be displayed in this text box. You can also manually edit this line of code;
- ***Date range:*** Allows you to determine a period to filter results more accurately, possible options are:
  - **By date:** Determines a specific date;
  - **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
  - **Today:** Displays results specifically for today's date;
  - **Yesterday:** Displays results specifically for yesterday;
  - **Last 7 days:** Specifically filters results from the last 7 days;
  - **Last 30 days:** Specifically filters results from the last 30 days;
  - **This month:** Displays results for this month;
  - **Last month:** Displays results for the last month.
- ***Filter:*** This check box allows you to select the type of filter used by the query*;*

For more information, regarding the filters shown in the filter selection box, check this page of the GSM manual.

- ***Equals/Contain/Not Contain:*** This checkbox basically acts as a logical query filter operator;
  - ***Equals:*** It will display all results that are exactly equal to the value of the next checkbox;
  - ***Contain:*** Will display all results that contain the value of the next checkbox;
  - ***Not Contain:*** Will display all results that do NOT contain the value of the next checkbox.
- ***Value:*** This box determines the value that will be used to filter the query.

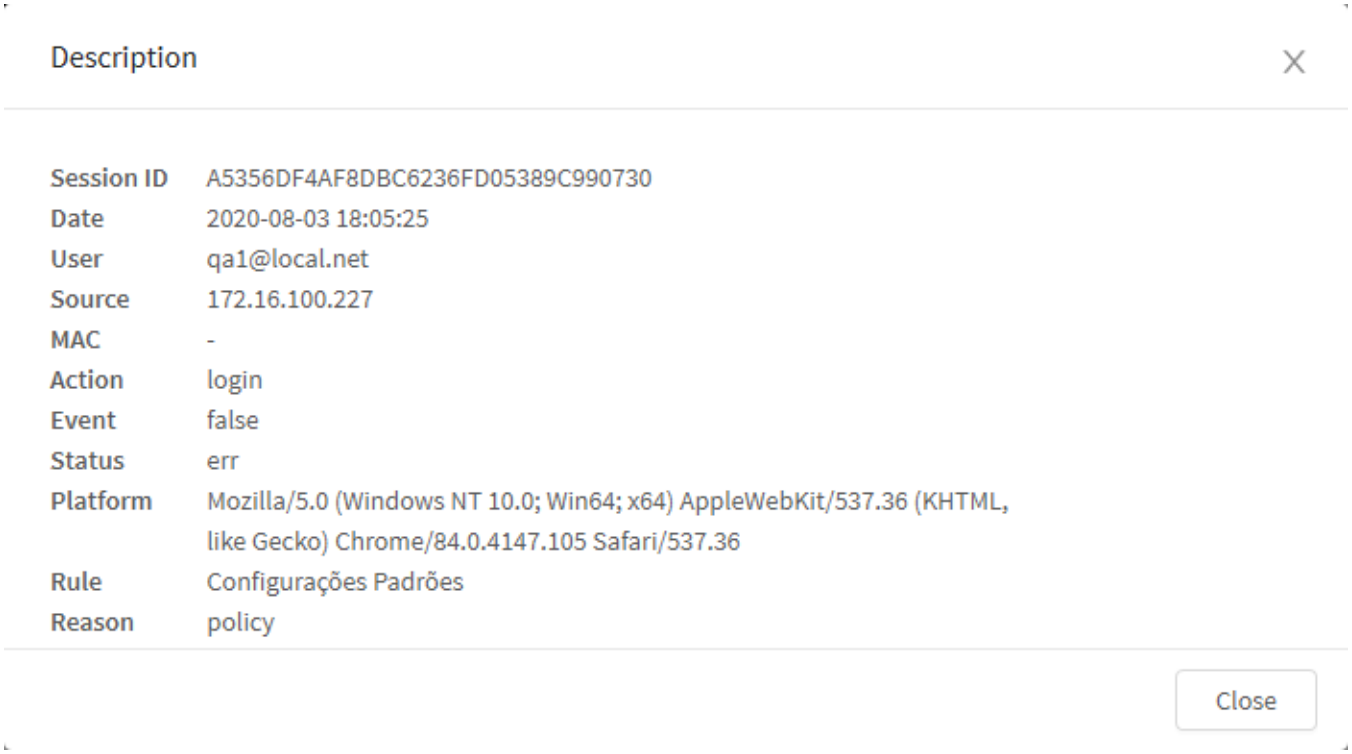
After editing the previous fields, click **[** + **]** to display the string used by the search in the Filter String text box

To clear the configured query, click the **[** Clear **]** button. If you want to cancel, click the **[** Cancel **]** button. To perform a search using the query, click the **[** Search **]** button.

Next we will show how the *Description* button works.

Authentication - Description

The ***Description***[ ] button displays more in-depth details of the event in question, as shown in the image below:



Sessions - Event View

- ***Session ID*:** Displays the session ID of the user who caused the event;
- ***Date*:** Displays the date of the event;
- ***User*:** Identifies the user who generated this event;
- ***Source*:** Displays the IP address that originated the event;
- ***MAC*:** Defines the physical address of the device that originated the event;
- ***Action*:** Determines what action taken caused the event;
- ***Event*:** Displays True if the Login has been done via SSO (Single Sign On), otherwise it will display False;
- ***Status*:** Determines the state of the event;
- ***Platform*:** Displays information of the platform used by the user who caused the event;
- ***Rule*:** Displays the name of the rule that was used, for more information see this page;
- ***Reason*:** Displays the reason for creating the event. Below is a list with the caption of possible reasons:
    - **src:** Remote Address;
    - **time:** Schedule;
    - **date:** Period;
    - **user_agent:** Platform;
    - **user:** User/Group;
    - **zone:** Network Zone;
    - **no_policy:** No policies found;
    - **user_blocked:** Blocked user;
    - **timeout:** Session timeout;
    - **policy:** Affected by a Policy.

Click **[ ]** or **[Close]** to close this window.

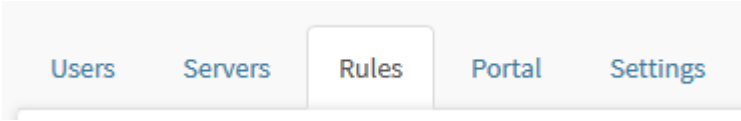
Authentication - Rules

This screen aims to manage the authentication service through control policies, which enable allowing or blocking access to a service based on preset conditions or define parameters from the users sessions that had their sessions authenticated through a specific service.

These authentication policies are applied in both captive portal and client authentication services.

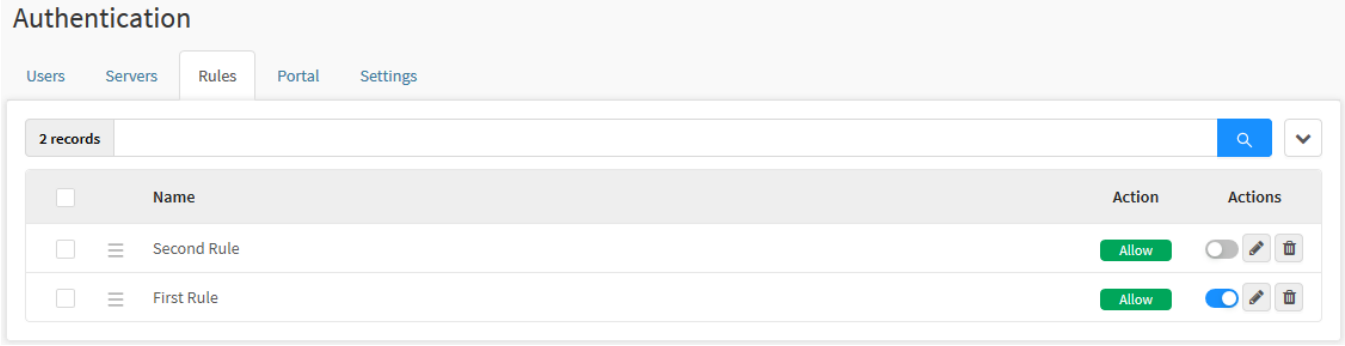
In terms of policies, those are managed by "Priority", and are applied based on the "First match wins" method (The first among the matching elements has the priority). However, policies located above have priority, while those below have less priority and the action applied is the first one that fits these conditions.

To set up these options, click on the Rules tab:



Rules tab

The following screen will be displayed:



Authentication - Servers

In this section we will analyze:

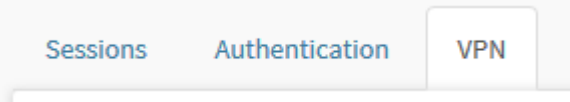
- How to create, edit and delete these Policies;
- The components of this tab.

Next, each component will be analyzed.

Security Events - VPN

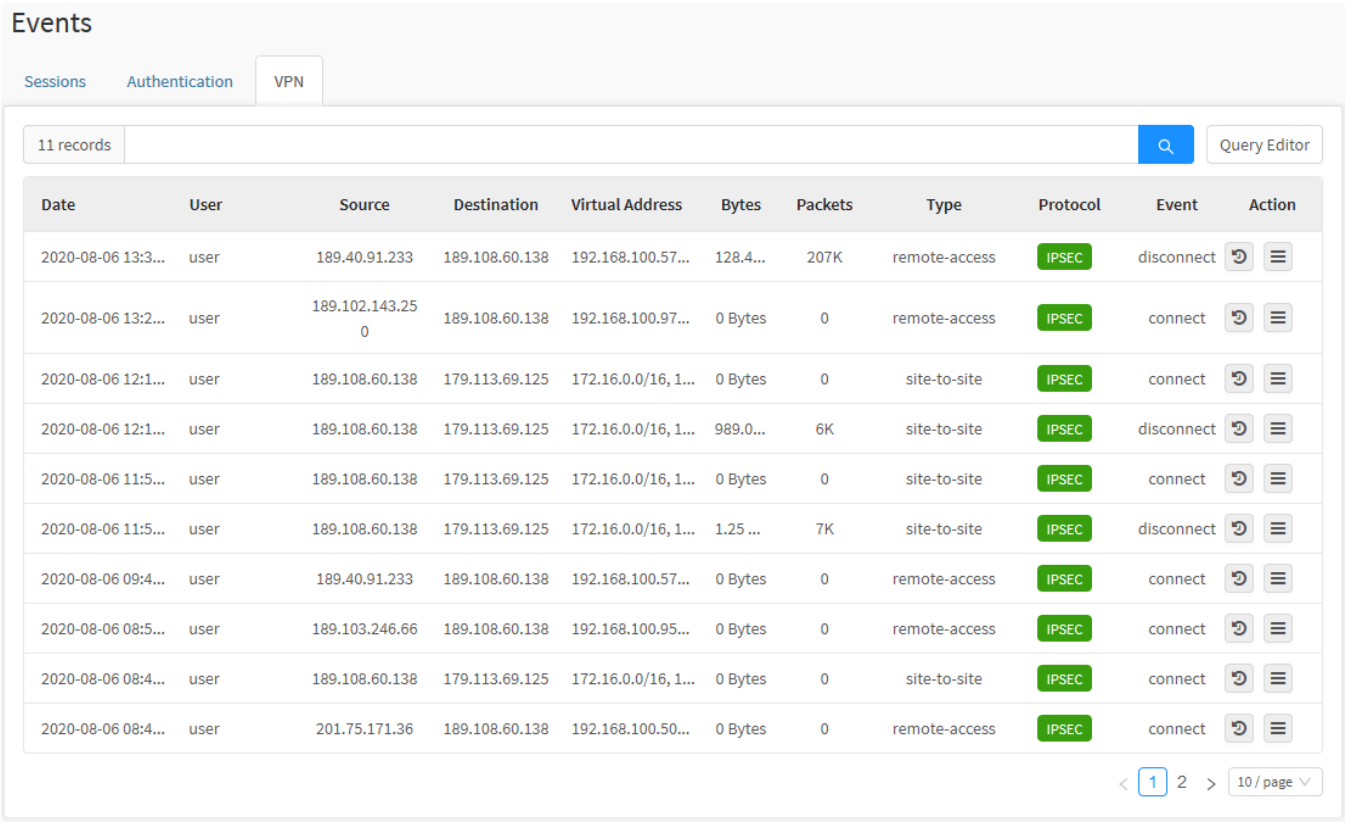
In VPN we have a record of all events generated by the VPN profiles of this device.

To access, click on "VPN".



VPN tab

The screen shown below will appear:



Security Events - VPN

This panel consists of the *Query Editor* and the following columns:

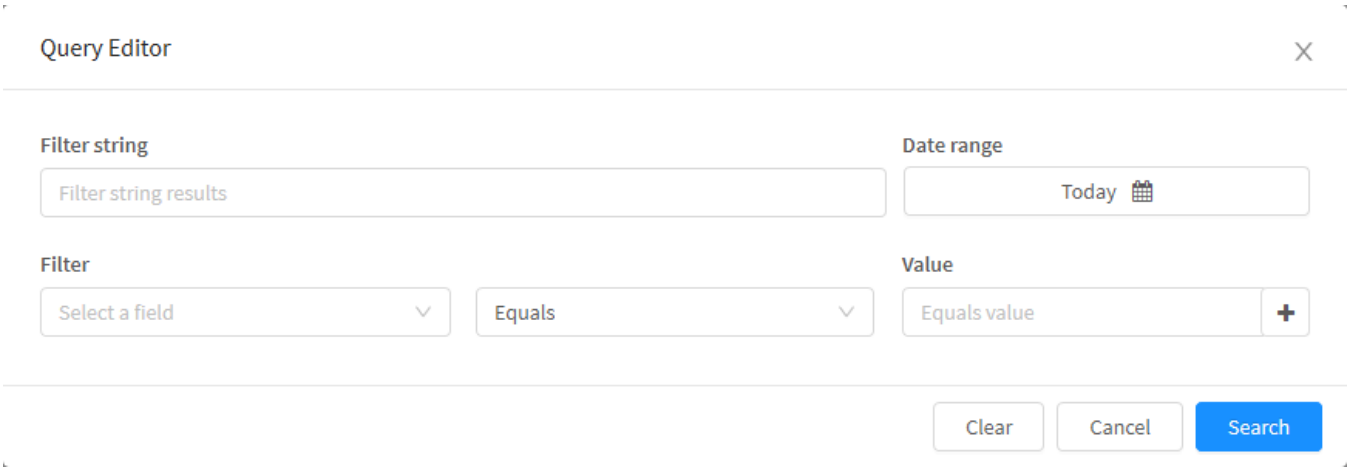
- ***Date*:** We have the exact date and time for this event;
- ***User:*** The user who generated this event. This field can be used as a filter for searches;
- ***Source*:** We have the source of this event, an IP address. This field can be used as a filter for searches;
- ***Destination*:** We have the destination of this event, another IP address. This field can be used as a filter for searches;
- ***Virtual Address*:** Displays the virtual address of the VPN;
- **Bytes:** Displays VPN Bytes traffic;
- **Packets:** Displays VPN packet traffic;
- ***Type:*** *Determines the type of VPN. Eg remote-access.*
- **Protocol:** Sets the type of VPN encryption protocol. Eg: IPSEC;
- **Event:** Specifically displays the event that generated the log. This field can be used as a filter for searches;
- ***Action*:** Displays the following buttons:
  - ***Session ID* [ ]:** Clicking on this button will execute a search with a query using specifically the VPN ID of the selected event;

- ***Description*** **[]:** When clicking on this button the *Description* window will be displayed.

Next, let's look at the Query Editor.

VPN - Query Editor

Through the Query Editor, it is possible to create, edit and save queries to perform an in-depth search of events, by clicking on the [Query editor] button the following window will be displayed:



VPN - Query Editor

- ***Filter string:*** When editing the Date Range, Filter and Value fields, the string used by the search will be displayed in this text box. You can also manually edit this line of code;
- ***Date range:*** Allows you to determine a period to filter results more accurately, possible options are:
  - **By date:** Determines a specific date;
  - **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
  - **Today:** Displays results specifically for today's date;
  - **Yesterday:** Displays results specifically for yesterday;
  - **Last 7 days:** Specifically filters results from the last 7 days;
  - **Last 30 days:** Specifically filters results from the last 30 days;
  - **This month:** Displays results for this month;
  - **Last month:** Displays results for the last month.
- ***Filter:*** This check box allows you to select the type of filter used by the query*;*
  - **user:** This filter selects by user, and accepts e-mails as values. Ex.: user@blockbit.com;
  - **src:** Makes the selection by the origin IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 172.16.12.171;
  - **dst:** Makes the selection by the destination IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 172.16.12.171;
  - **virtual_address:** Makes the selection by the VPN's virtual IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 192.168.200.4/32;
  - **type:** Selects based on the VPN's connection type. Ex.: remote-access, site-to-site, etc;
  - **protocolo:** This filter allows the selection of a VPN's cryptography protocol. The available options are: SSL or IPSEC;
  - **event:** Makes the selection by a specific event. Ex.: connect, disconnect, etc.

- ***Equals/Contain/Not Contain:*** This checkbox basically acts as a logical query filter operator;
  - ***Equals:*** It will display all results that are EXACTLY equal to the value of the next checkbox;
  - ***Contain:*** Will display all results that contain the value of the next checkbox;
  - ***Not Contain:*** Will display all results that do NOT contain the value of the next checkbox.
- ***Value:*** This box determines the value that will be used to filter the query.

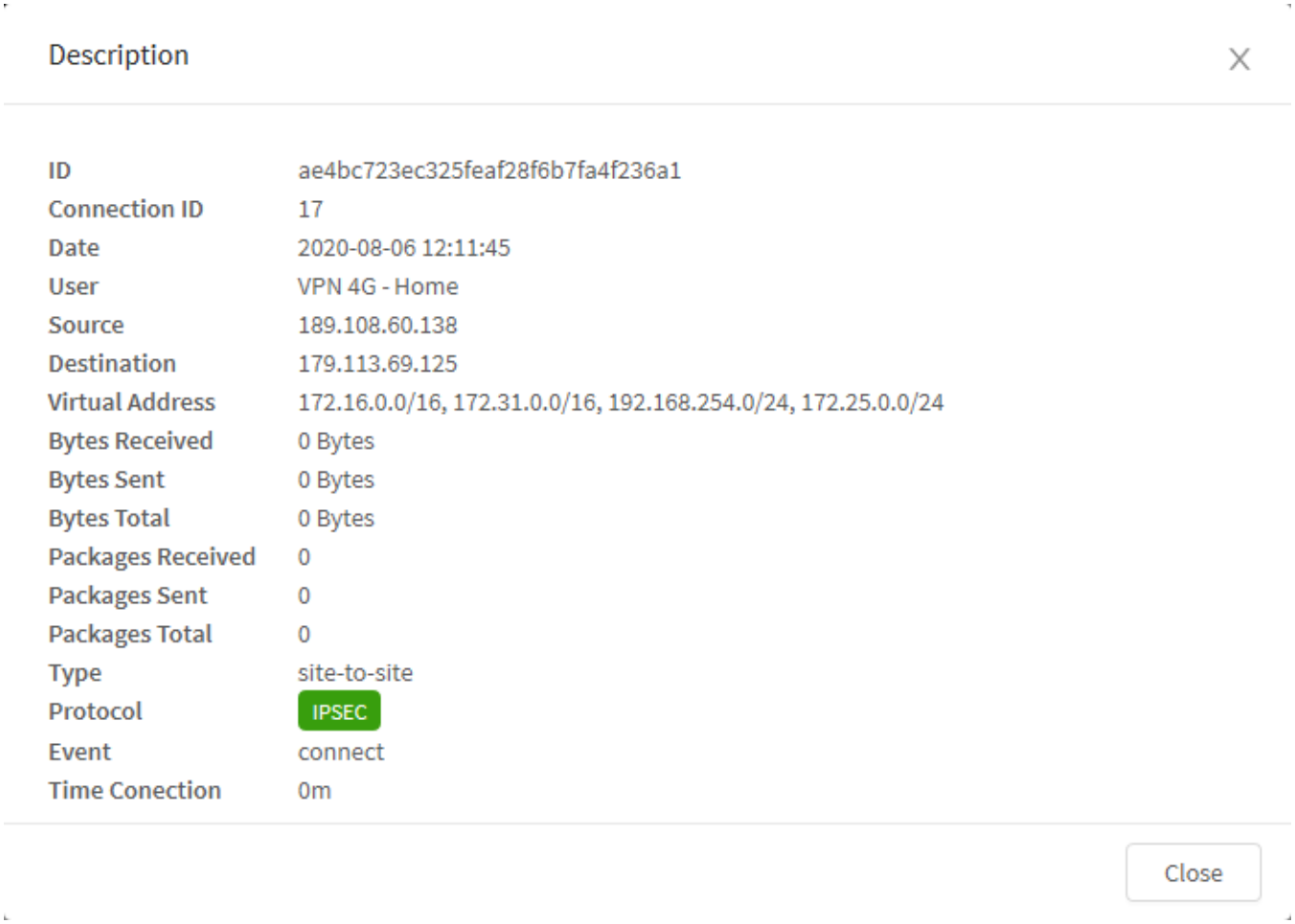
After editing the previous fields, click [+] to display the string used by the search in the Filter String text box

To clear the configured query, click the [Clear] button. If you want to cancel, click the [Cancel] button. To perform a search using the query click the [Search] button.

À seguir vamos exibir o funcionamento do botão *Description*.

VPN - Description

The ***Description***[ ] button displays more in-depth details of the event in question, as shown in the image below:



Sessions - Event View

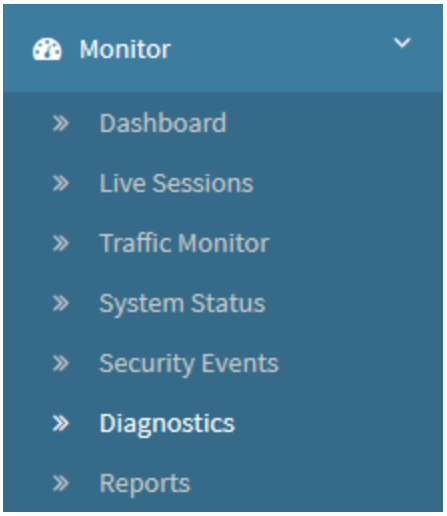
- ***ID*****:** Displays the session ID of the user who caused the event;
- ***Connection ID*****:** Displays the connection ID of the user who caused the event;
- ***Date*****:** Displays the date of the event;
- ***User*****:** Identifies the user who generated this event;
- ***Source*****:** Displays the source IP address of the event;
- ***Destination*****:** Displays the destination IP address of the event;
- ***Virtual Address:*** Displays the virtual IP address of the VPN;
- ***Bytes Received:*** *Displays the amount of Bytes received*;
- ***Bytes Sent:*** Displays the amount of Bytes sent;
- ***Bytes Total:*** *Displays the total number of Bytes sent and received*;
- ***Packages Sent:*** Displays the total number of packets sent;
- ***Packages Total:*** Displays the total packets sent and received;
- ***Type:*** *Displays the type of VPN;*
- ***Protocol:*** *Sets the type of VPN encryption protocol;*
- ***Event*****:** Specifically displays the event that generated the log;
- ***Time Connection*****:** Displays how long the user has been logged in.

Click **[ ]** or **[ ]** to close this window.

Monitor - Diagnostics

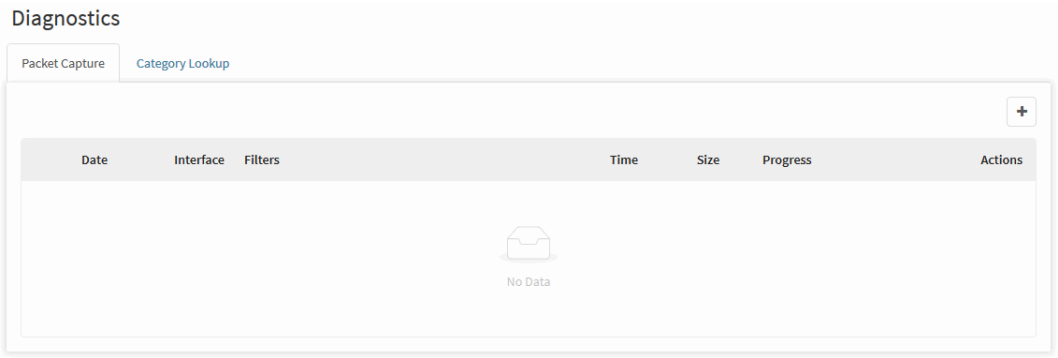
The "Diagnostics" panel has the function of capturing packages and consulting how a particular website was categorized.

To access this screen, just select the option “Diagnostics”.



Monitor - Diagnostics

The screen below will appear:



Diagnostics - Packet Capture

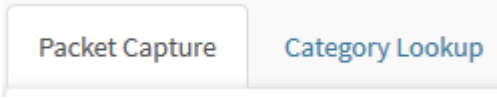
The Diagnostics panel consists of two tabs:

- *Packet Capture*;
- *Category Lookup*.

Diagnostics - Packet Capture

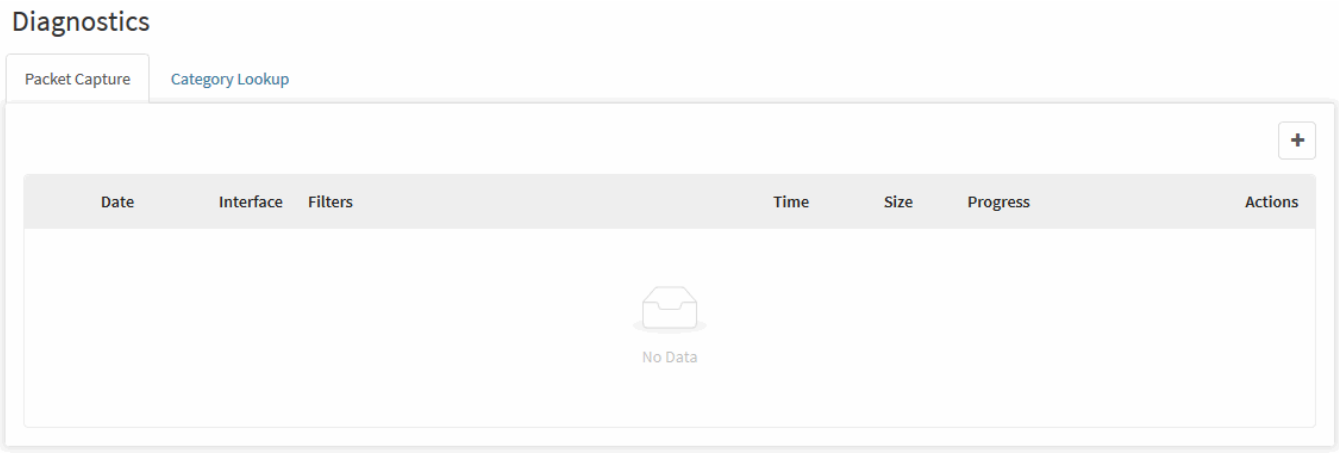
This feature allows the administrator to collect dump in PCAP format, with filters, of any traffic filtered by Blockbit NGFW.

To access, click on the "Packet Capture" tab.



"*Packet Capture*" Tab

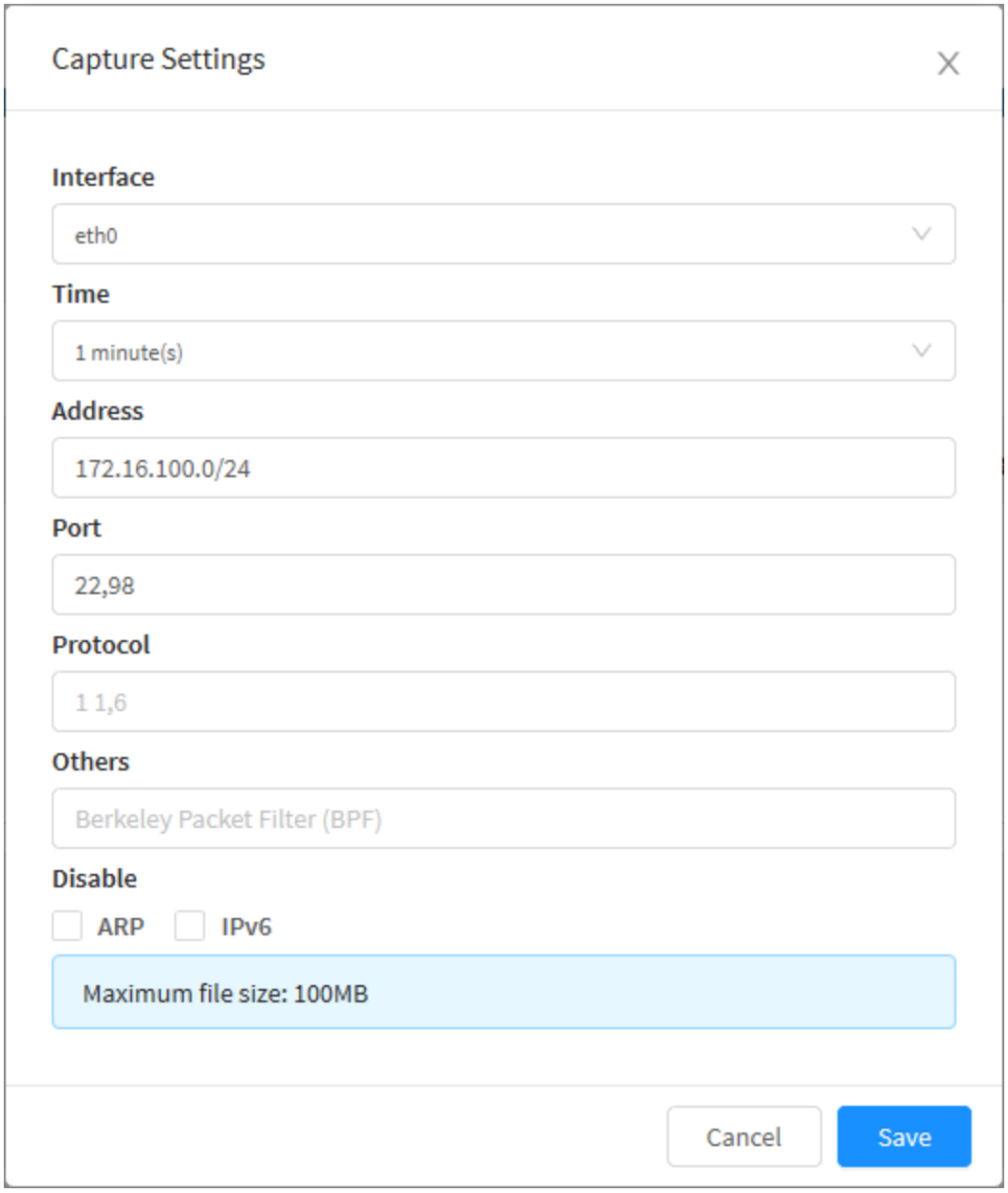
The screen below will be displayed.



Packet Capture

To capture packets, follow the steps below:

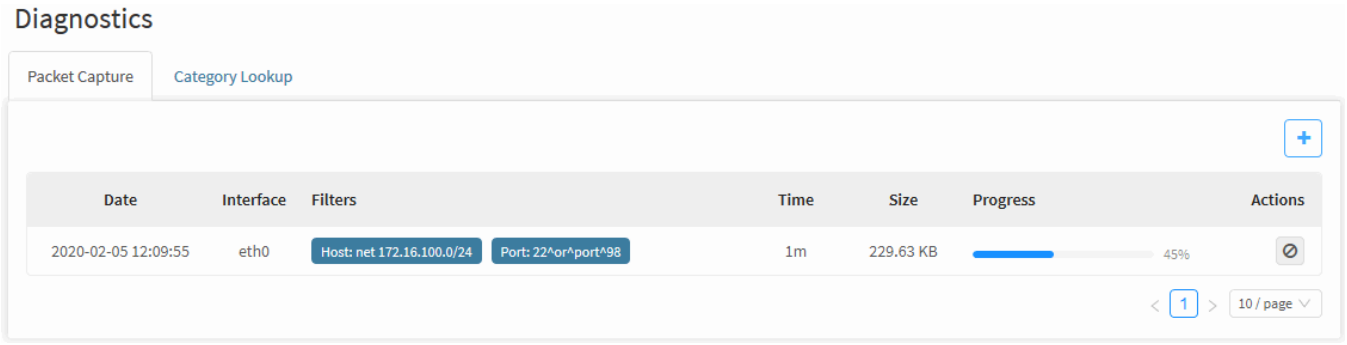
When clicking on the **[**  **]** button, the window below will be displayed.



Add packet capture

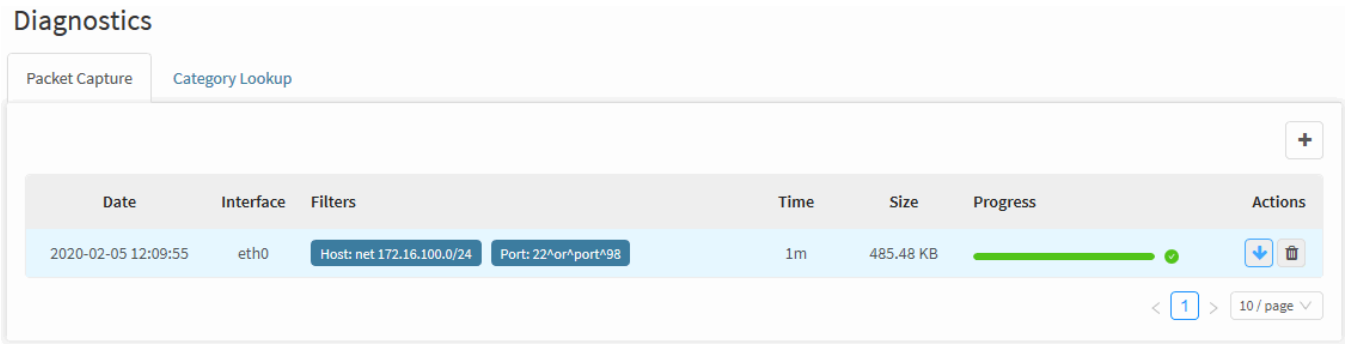
- ***Interface*:** Define the interface on which to monitor. Ex.: eth0;
- ***Time*:** Set the time for monitoring. Ex.: 30s;
- ***Address*:** Define IP or network address on which to monitor. Ex.: 172.16.100.0/24;
- ***Port*:** Define the port or port range on which to monitor. Ex.: 22,98;
- **Protocol:** Define the protocol that will perform the monitoring;
- ***Others*:** In this field it is possible to perform filters using commands based on the **Berkeley Packet Filter (BPF)**;
- [☑] ***Disable ARP*:** This option disables ARP monitoring on the interface;
- [☑] ***Disable IPv6*:** This option disables the monitoring of the IPv6 protocol.

If you want to cancel, click [Cancel]. After filling in the fields click on the [Save] button and the system will start monitoring as shown in the screen below.



Packet Capture – Progress

Wait for the progress bar to finish, the captured data is available for download by clicking on the **[ ]** button to be analyzed later.

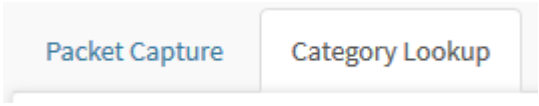


Packet Capture – Download

Diagnostics - Category Lookup

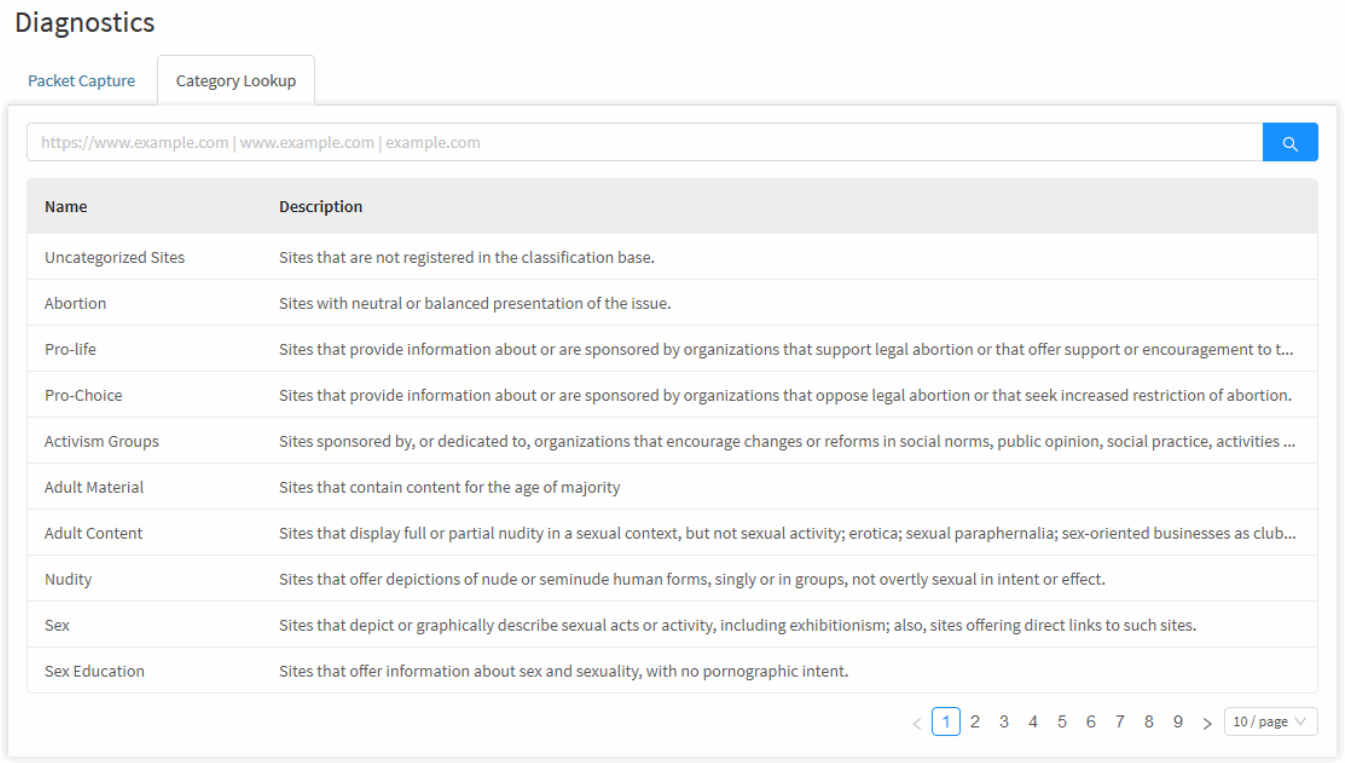
This screen has the function of consulting the categorization of sites. It is an SWG database (Secure Web Gateway), a reputation base of Urls, browsers, files and web applications, which comprises about 88 categories and subcategories.

To access click on the "Category Lookup" tab.



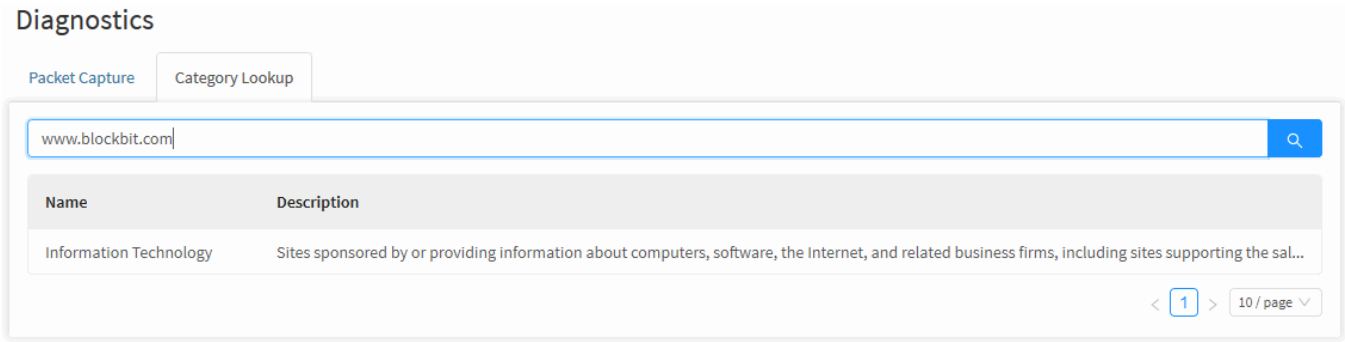
Category Lookup tab

The screen below will be displayed:



Diagnostics - Category Lookup

It is possible to search the category that a particular site classified in the base of the Web Filter by typing a url in the search bar at the top of the page and clicking the **[**  **]** button, the system will consult the base and inform which category the site is in.



Diagnostics - Category Lookup - Search

Below a table stating the name of the categories and their respective description.

Description of categories

Name:	Description:
Drug abuse	Sites that discuss, encourage or provide information about drugs that are controlled, banned or regulated in any way, and their abuse; Also on consumer articles related to the use or abuse of these drugs.
Alcohol and tobacco	Sites that contain information, promote or allow the sale of alcoholic beverages, tobacco products, and all associated articles and accessories. The websites of self-help groups, such as Alcoholics Anonymous, which are part of the Health category, are excluded..
Personal ads and dating	Sites that promote interpersonal relationships, excluding those specific to gays or lesbians.
Advertising	Sites that contain ad servers.
Weapons	Sites that contain information, promote or permit the sale of weapons and related articles.
Personal network storage / backup	Sites that store personal files on Internet servers, for backup or exchange purposes. Ex.: Digital photo and album storage services.
Activism related to reproductive rights	Sites that feature neutral or balanced discussions of the subject are classified in the main category (Activism related to reproductive rights).
Job Searches	Sites that contain information about or that allow you to search for jobs.
Sport Hunting / Gun Clubs	Club sites interested in weapons, catalogs or lists of such club sites. This category includes war game and paintball sites.
Web Chat	Sites that host chat services (web chat via HTTP) or chat rooms (chat rooms via IRC (Internet Relay Chat)), homepages dedicated to IRC and sites that offer forums or discussion groups.
Peer-to-peer file sharing	Sites that provide client computer software enabling non-hierarchical file sharing and transfer.
Shopping	Sites where you can make online purchases of consumer products, but not sexual items, related to investments, computer software or hardware, nutritional supplements, alcohol and tobacco, travel services, vehicles and parts or weapons. Includes sites dedicated exclusively to the sale of sporting and religious articles.
Internet communications	Sites that allow instant messaging or email exchange.
Illegal / objectionable content	Sites that contain information about, or encourage, crime (except computer-related crimes), unethical, dishonest behavior, or how to avoid indictment.
Mature content	Sites that contain partial or total nudity, that represent or define a sexual orientation context, but that do not contain sexual activity itself; sexual articles; erotic and other publications that present or discuss issues related to sex, close to pornography; companies whose businesses are of a sexual nature, such as nightclubs, hellos, escort services, websites with password / verification. Includes sites where you can purchase such products and services online.
Online brokerage and trading	Sites that enable active trading in the capital market and the management of financial investments.
Freeware / Software Download	Sites whose primary function is to provide software and freeware downloads.
Education	Sites sponsored or that support or offer education information.
Sex education	Sites that contain information about sex and sexuality, without pornographic intent.
Web Email	Sites that host web-based email systems. Any web-based email service, whether by browser or software.

Entertainment	Sites that contain information about, or promote, movies, radio and television without news, books, humor, music and magazines (except for adults, business, electronic games, computers, alcohol and tobacco, health, hobbies, sports, tourism , vehicle or weapons).
Sports	Sites that contain information about, or that promote, sports, active games and recreation. Sites dedicated to a specific current event that requires a category of its own due to content that can cause objections, demand for bandwidth or potential loss of productivity. Some of these sites simply disappear after a while; others are reviewed after 90 days, for reclassification purposes.
Special events	Sites dedicated to a specific current event that requires a category of its own due to content that can cause objections, demand for bandwidth or potential loss of productivity. Some of these sites simply disappear after a while; others are reviewed after 90 days, for reclassification purposes.
Gays and lesbians	Sites that contain information about, or that offer products and services to, people with a homosexual lifestyle, including sites where you can shop online, but not those of a sexual nature or related to specific topics.
Bandwidth management	Sites that have high bandwidth consumption.
Productivity management	Sites that can hinder productivity.
Government	Sites sponsored by government agencies or government agencies, at all levels of government (ie, ending in .gov)
Activism groups	Sites sponsored by, or dedicated to, organizations that encourage changes or reforms in social norms, public opinion, social practice, activities and economic relations. Excludes commercially sponsored sites, sites dedicated to electoral policies or legislation, the issue of abortion, sites that preach hate or violence.
Political groups	Sites sponsored by, or containing information about, political parties and interest groups focused on elections or legislation.
Hacking	Sites that contain information or that encourage access to or illegal, or questionable, use of software or communication equipment.
Hobbies	Sites that contain information about, or that promote, pastimes that are mostly sedentary in nature, but that do not include electronic, video, or online games or games.
Web Hosting	Sites of organizations that provide hosting services or community top-level domain pages on the web.
Properties	Sites that contain information about renting, buying and selling residential properties.
Computer Security Information	Sites that contain information or tools oriented to the security of computer systems.
Cultural institutions	Sites sponsored by museums, galleries, theaters (but not cinemas and other cultural institutions).
Educational Institutions	Sites sponsored by schools and other educational institutions or by groups and teachers or students, or that relate to educational events or activities.
Gambling and betting	Sites that contain information about, or that promote, gambling and betting, or that allow you to do so online. Sites where there is a risk of losing money.
Games	Sites that contain information about, or that promote, electronic or video games, computer games, role play (online role-play, but not those that contain card or board games; also sites that allow you to play or offer games online (including sites with sweepstakes and contests).
Internet auctions	Sites where you can participate in online auction, items purchased and sold by individuals.
Lingerie and swimsuits	Sites that contain photos or graphic images of models in suggestive, but not indecent or obscene clothing; images suggestive of nudity and female breasts. It also includes sites that contain photos and artistic material with women with little clothing.
Marijuana	Sites whose primary function is to provide specific information about marijuana or promote its use.
Reference Materials	Sites offering reference materials such as atlases, dictionaries, encyclopedias, statistical data, (white papers) and yellow pages.
Educational materials	Sites whose primary function is to provide historical, scientific information, research pages, or teaching materials.
Bad taste	Sites that could not be classified in any other category, but that contain offensive, grotesque, frightening, dismal material, without containing anything appreciable.
Search engines and portals	Sites that make it possible to search the Web, in news groups, or indexes or directories of the same.

Medicines or drugs (as defined by U.S. law)	Sites sponsored or that support or offer information about medicines or drugs.
Prescription drugs	Sites that provide information about approved drugs and their medical use.
Improper monitoring and invasion of privacy	Sites or pages that can download software that, without the user's knowledge, or without their permission, monitor it.
MP3	Sites that allow you to download MP3 files or that act as catalogs for sites of this type.
Business and Economy	Sites sponsored by, or dedicated to, individual companies that do not offer e-commerce and not firms related to the computing and commerce sector on the Internet or the sale of alcoholic beverages and cigarettes / tobacco, travel services, vehicles or weapons. Includes commercial, but non-residential real estate brokers.
News and media	Sites that contain real-time news, including those sponsored by newspapers, magazines, specialist or academic magazines, radio stations, television networks, telegraph services, but not those that provide stock exchange quotes or those related to sports.
Nudity	Sites that display human nudity or half-nakedness, of individuals or groups, and that are not openly sexual in character.
Service and Philanthropic Organizations	Sites sponsored or that support or offer information about organizations dedicated to doing good as their main activity.
Work and Professional Organizations	Sites sponsored or that support or offer information about organizations dedicated to professional development or workers' interests.
Social Organizations	Sites sponsored or that support or offer information about dedicated organizations.
Social Organizations and Affiliations	Sites sponsored or that support or offer information about organizations primarily dedicated to socialization or common interests other than philanthropy or professional development.
Military organs	Sites sponsored by military agencies or organizations (ending in .mil)
Pedophilia	Sites that encourage pedophilia or that provide images or texts with pedophile content.
Alternative publications	These are the online equivalents of tabloid newspapers. Note: This category may contain sexual material.
Message boards and clubs	Social and business club sites, personal or business discussion groups, and list servers that are not classified in any other category.
Racism / hate	Sites that encourage the identification of racial groups, defamation or submission of groups (identified by race or otherwise, or the superiority of a particular group.
Internet radio and TV	Sites whose primary function is to provide radio and TV programs on the Internet.
Religion	Sites that contain information about, or that promote, religions.
Non-traditional religions	Sites that contain information about, or that promote, religions that are not in category 22.2 and other non-traditional religions, or semi-religious topics, including cults.
Traditional religions	Sites that contain information about, or that promote, Buddhism, Bahai, Christianity, Christian science, Hinduism, Islam, Judaism, Mormonism, Shinto, Sikhism; also, atheism sites.
Restaurants and gastronomy	Sites that contain lists, reviews and advertisements, or that promote services related to gastronomy, buffets and restaurants.

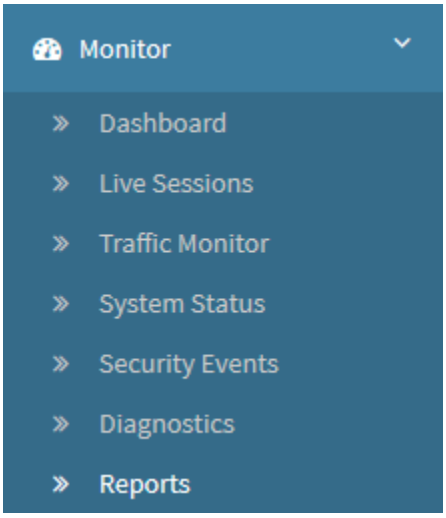
Health	Sites that contain information or guidance about personal health or medical services, health insurance, procedures or devices, but that are not related to drugs. Includes self-help groups.
Financial data and services	Sites that contain news and stock quotes, bonds and other financial vehicles, investment advice; but do not offer online trading or brokerage. Includes banks, credit unions, credit cards and life insurance companies.
Sex	Sites that feature images of sexual acts or activities, or that describe them graphically, including exhibitionism.
Proxy avoidance systems	Sites that contain information about how to avoid proxy server roles or how to gain access to URLs in order to avoid the proxy server.
Instant messaging systems	Sites that allow instant messaging.
Sites in favor of freedom of choice	Sites sponsored by, or dedicated to, organizations that encourage freedom of choice.
Militancy / extremism sites	Sites that contain information about what they promote, or that are sponsored by activism groups that preach anti-government actions.
URL translation sites	Sites that offer online URL translation.
Malicious Sites	Sites that contain code that intentionally modifies user systems without their consent, or that causes harm.
Sites for adults	Sites containing adult content.
Personal Web Sites	Sites published by individuals for personal use or exchange; are not published by any organization.
Pro-life sites	Sites sponsored by, or dedicated to, organizations that encourage life.
Pay-to-surf sites	Sites that pay the individual to surf, or to send email.
Society and lifestyles	Sites that contain information on everyday matters, excluding sex, entertainment, jobs, sports, and the topics covered by the subsections below.
Spyware	Sites or pages that can download software that, without the user's knowledge, or without their permission, generates HTTP traffic (with the exception of simple user identification and validation.
Streaming media	Sites whose primary function is to provide streaming media content, such as movie trailers.
Unregulated supplements / compounds	Sites that contain information about, or that encourage, the use of chemical substances (such as those in natural compounds, for example not controlled by the US Food and Drug Administration (Food and Drug Administration)).
Information Technology	Sites sponsored by, or containing information about, computer and Internet companies.
Internet telephony	Sites that enable users to make phone calls over the Internet, or obtain information or software for that purpose.
Tourism	Sites that contain information about, or that promote, various travel-related services, including sites where you can shop or book online.
Vehicles	Sites that contain information about, or that promote, vehicles, including sites where you can buy parts or vehicles online.
Violence	Sites that contain information about, or that promote, acts of violence. Sites that contain an excess of obscenity or indecent language may be placed in this category, if they are not in the category (bad taste).

The categories presented here can be used in the creation of Web Filter profiles, for more information about this process check this page.

Monitor - Reports

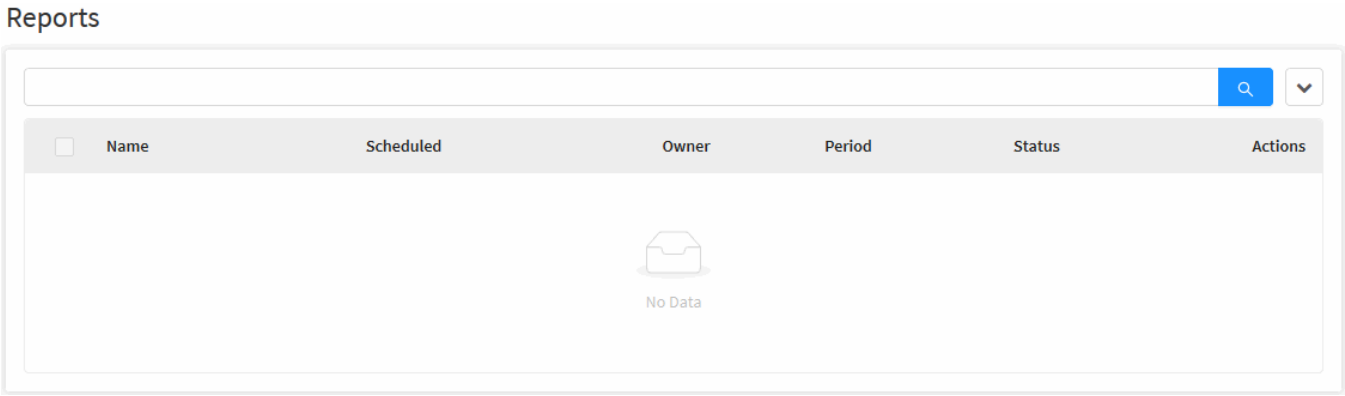
The function of this option is to manage the automatic and periodic creation of customized reports, allowing selection of specific characteristics of the selected devices.

To access and manage the automatic creation of reports, click on the “Reports” icon located on the left side:



Analytics - Reports

The reports screen will be displayed.



Reports

In this session we will analyze:

- How to add and delete reports;
- Column details on this screen;
- Examples of how to generate specific reports.

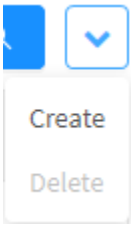
Next, we will analyze the function of each component of this screen.

Monitor - Reports - Actions menu

At the top right of the screen we have the actions menu:

Reports – Actions Menu Button

When clicking on this button the menu below is displayed:



Reports – Actions menu

The menu consists of the following options:

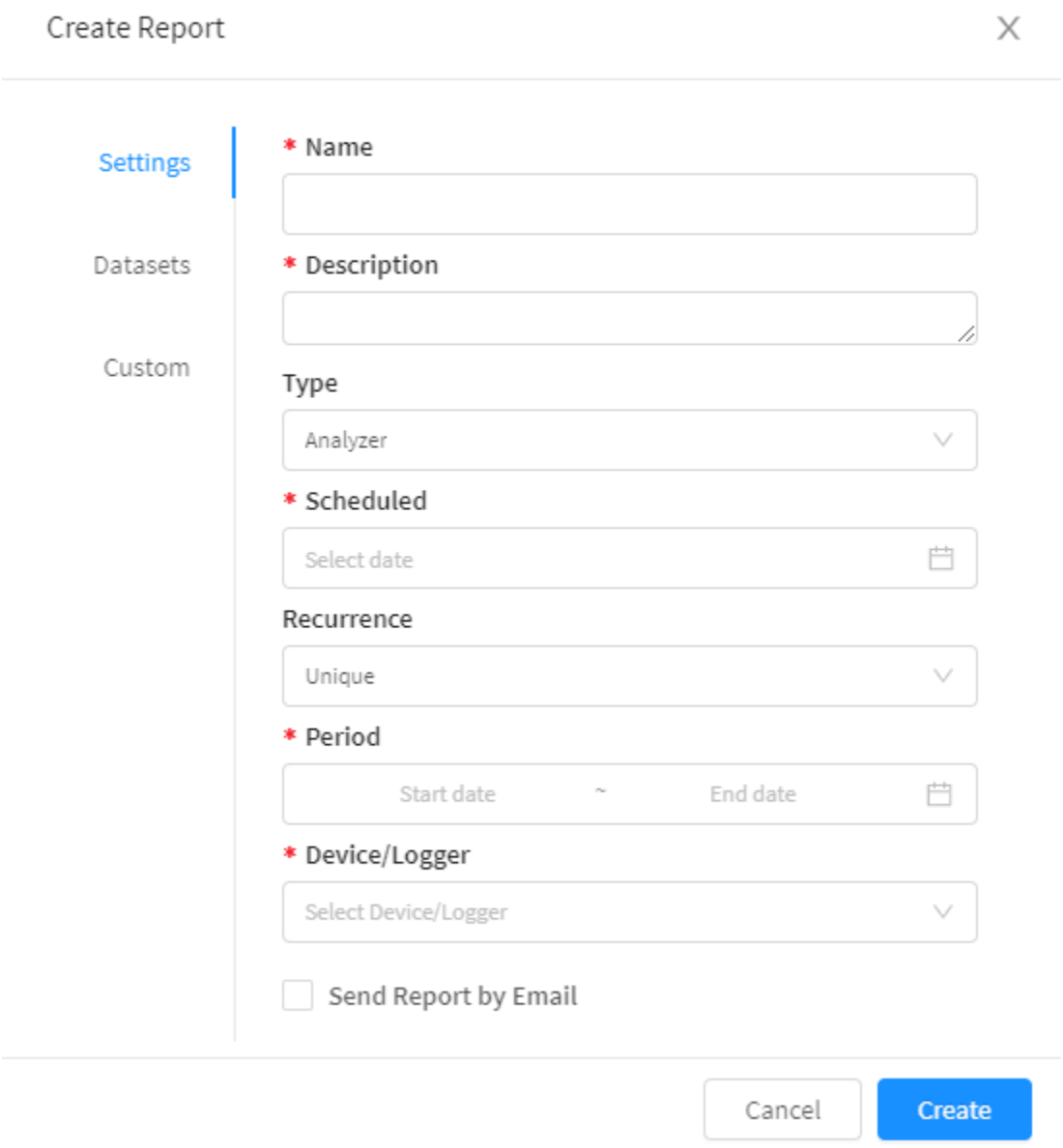
- *Create*;
- *Delete*.

Next, each action menu option will be detailed.

Monitor - Reports - Actions menu - Create Report

In the create reports option it is possible to set up from which functionality the information in Monitor Reports will be displayed. It is possible to configure Firewall, Web Filter or even VPN logs reports. Next, we will see how to select and configure these reports.

To create an automatic report click on “Create”, the following screen will be displayed, with the “Settings” side tab pre-selected:

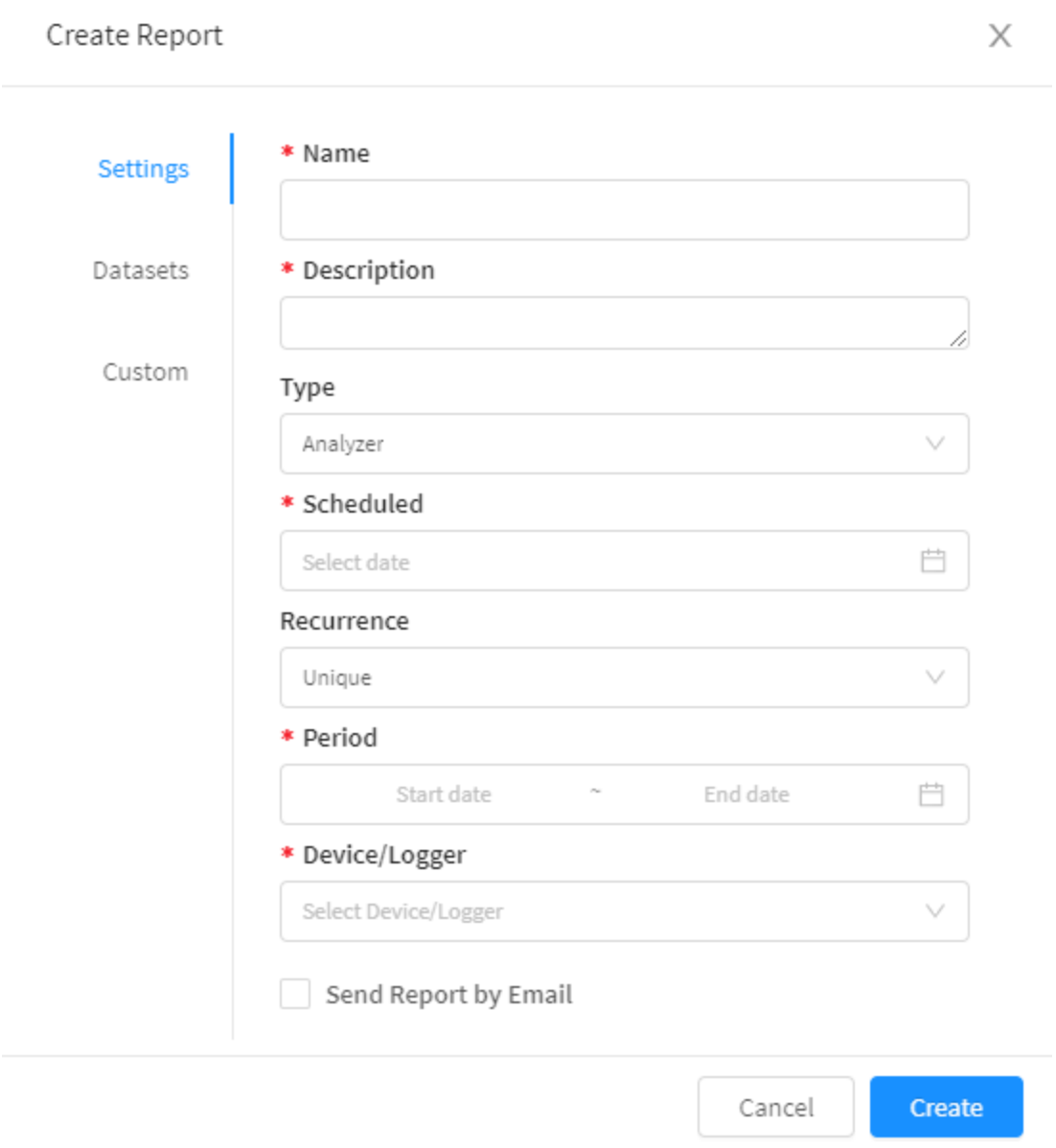


Reports – Create Report

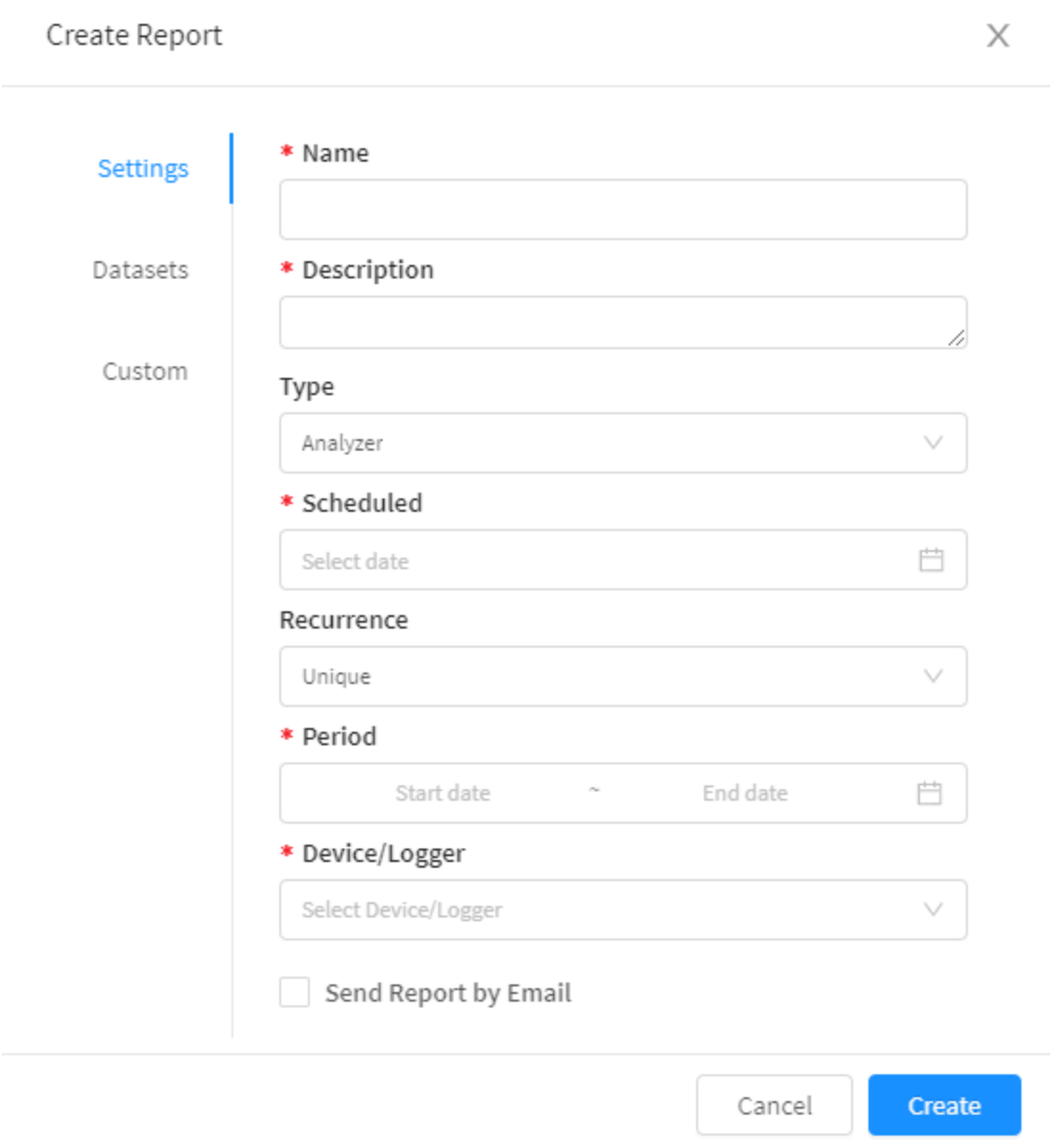
This window consists of the following side tabs:

- *Settings*;
- *Datasets*;
- *Custom*.

Next, we will analyze the contents of this window and all its tabs.



Settings tab



Reports – Create Report - Settings

Below we will analyze each field in this panel:

- ***Name*:** The report name. Ex.: *Firewall Report*;
- ***Description*:** The report description. Ex.: Firewall Report;
- ***Type*:** This drop-down menu determines the options that will be available in the “Datasets” tab, we have the following options:
  - ***PDF report:***
    - ***Analyzer:*** *Creates a PDF report with analyzer information about the selected service or the activities of a specific user*.
  - ***CSV report:***
    - ***Log Session:*** Creates a CSV report on user sessions, contains information such as: session ID, date and time of access, user identification, MAC address, service used and etc.;
    - ***Log Authentication:*** *Creates a CSV report with logs of system authentication events*;
    - ***Log VPN:*** *Creates a CSV report on all accesses using VPN, contains information such as: VPN ID, date and time of access, destination and origin IP, traffic information of packets, bytes received and sent and etc.*
  - ***Top Hits*:** Generates a Top Hits report, in the Datasets tab it is determined the amount of hits to be sampled and the filters to be used;
  - ***Top Bytes*:** Generates a Top Bytes report, in the Datasets tab it is determined the amount of bytes to be sampled and the filters to be used;
  - ***Log*:** Allows the creation of a customized report, in Datasets it is possible to use customized Queries and determine the filters to be used.
- ***Scheduled*:** Displays the schedule date for when this report will run;
- ***Recurrence:*** Period within which the report will run, choose between daily, weekly or monthly;
- ***Period*:** Determines the period when the data will be analyzed by the logger in the NGFWs. Ex.: When selecting from January 1, 2023 to February 5, 2024, all data that exists outside that period, will not be displayed in the "Report".

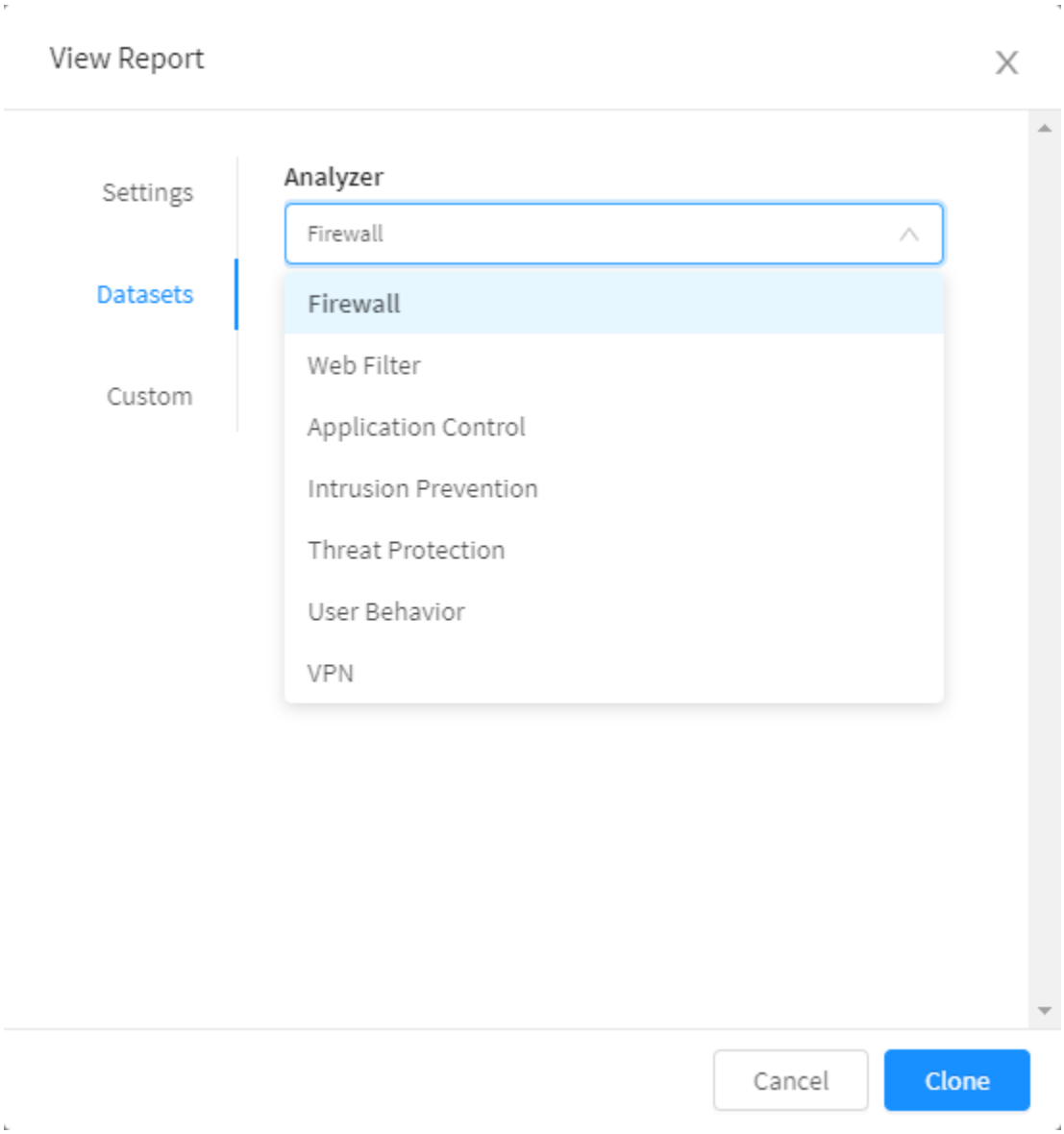
- ***Device/Logger*:** The device from which the data will be analyzed is selected to generate the report.
- ***Send report by e-mail:*** Mark this option [Send Report by Email]to receive the reports generated in analytics via e-mail, as often as they are generated.

It's important to remember that to receive the reports it is necessary to configure the e-mail.

Next we will analyze the contents of the Datasets side tab;

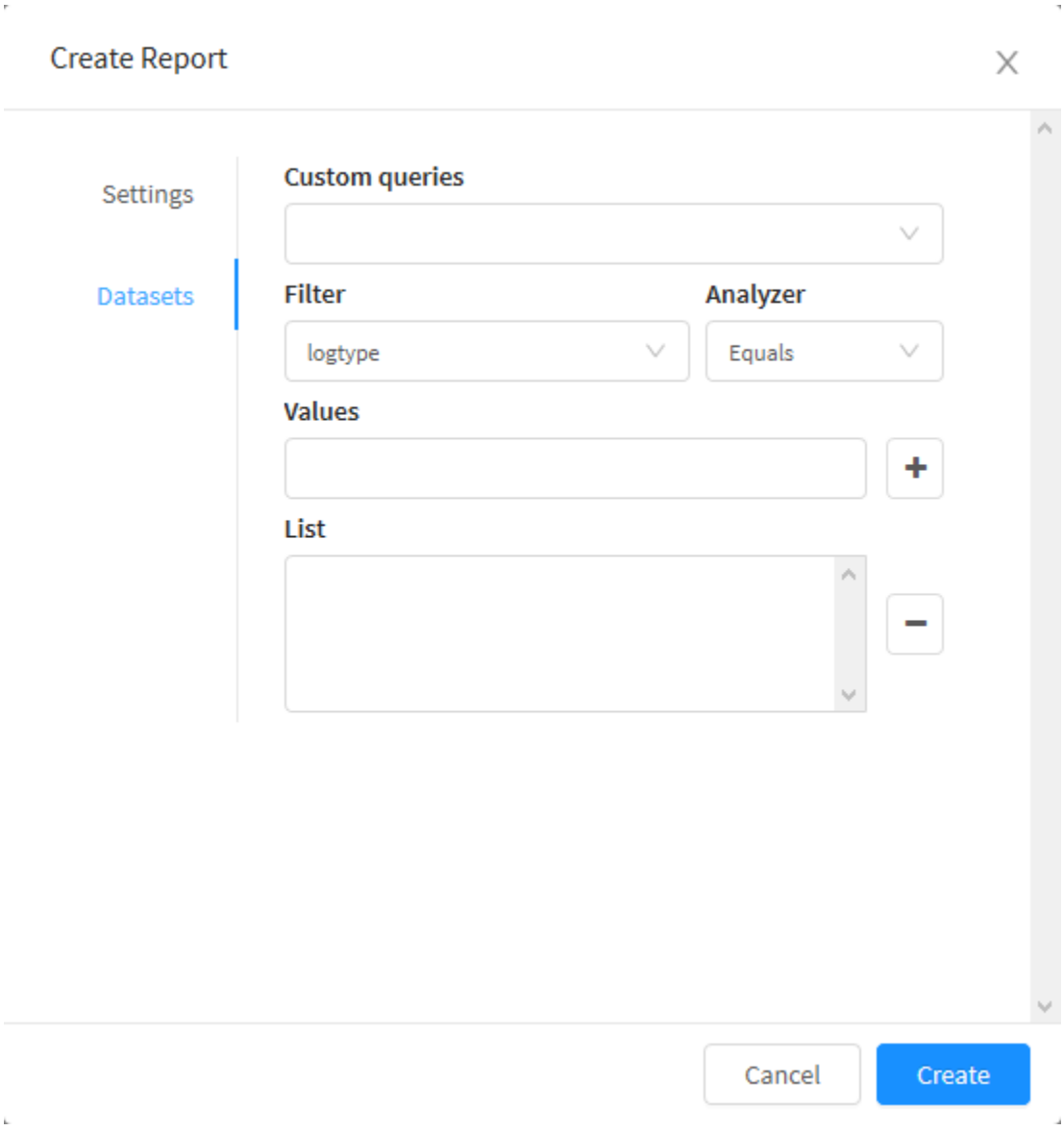
Datasets tab

The “Datasets” tab determines the types of data that will be used in the creation of the reports, as previously mentioned, the components of it are determined by the “Type” checkbox of the “Settings” tab. If you selected the "Analyzer" option, the "Datasets" tab can be configured according to the options below:



- ***Firewall*:** Displays information equivalent to Analyzer - Firewall, for more information see this page;
- ***Web Filter*:** Displays information equivalent to Analyzer - Webfilter, for more information see this page;
- ***Application Control*:** Displays information equivalent to Analyzer - Application Control, for more information see this page;
- ***Intrusion Prevention*:** Displays information equivalent to Analyzer - Intrusion Prevention, for more information see this page;
- ***Threat Protection*:** Displays information equivalent to Analyzer - Threat Protection, for more information see this page;
- ***User Behavior*:** Displays information equivalent to a specific user's access. When selecting this option, the "Select a user" field will be displayed, select the user on which it will be based;
- ***VPN*:** Displays information equivalent to Analyzer - VPN, for more information see this page;

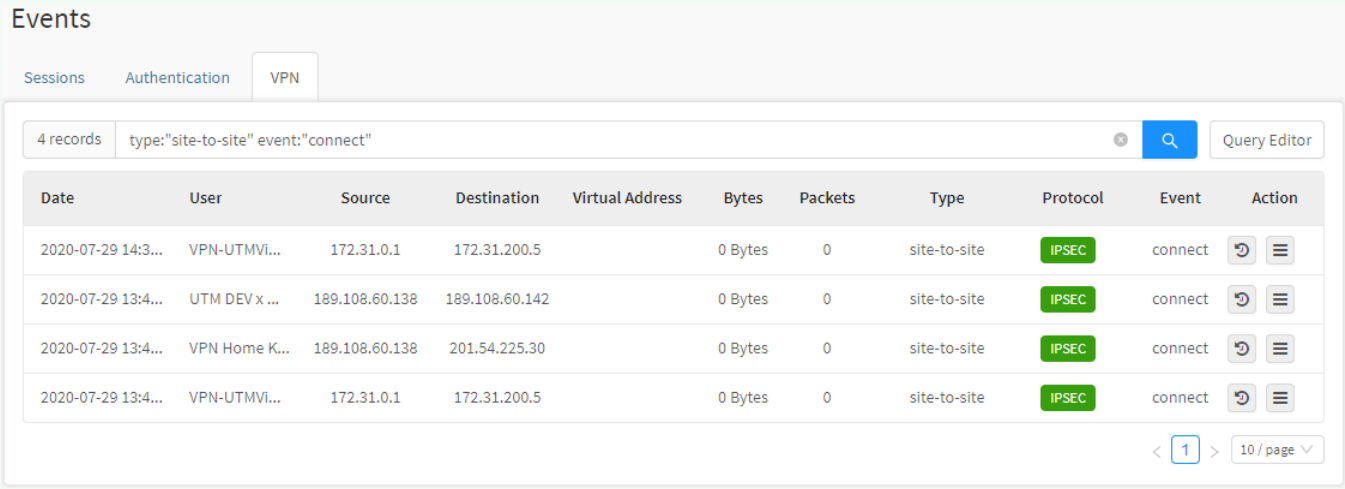
If you selected the "Log Session" option, the "Datasets" tab can be configured according to the options below:



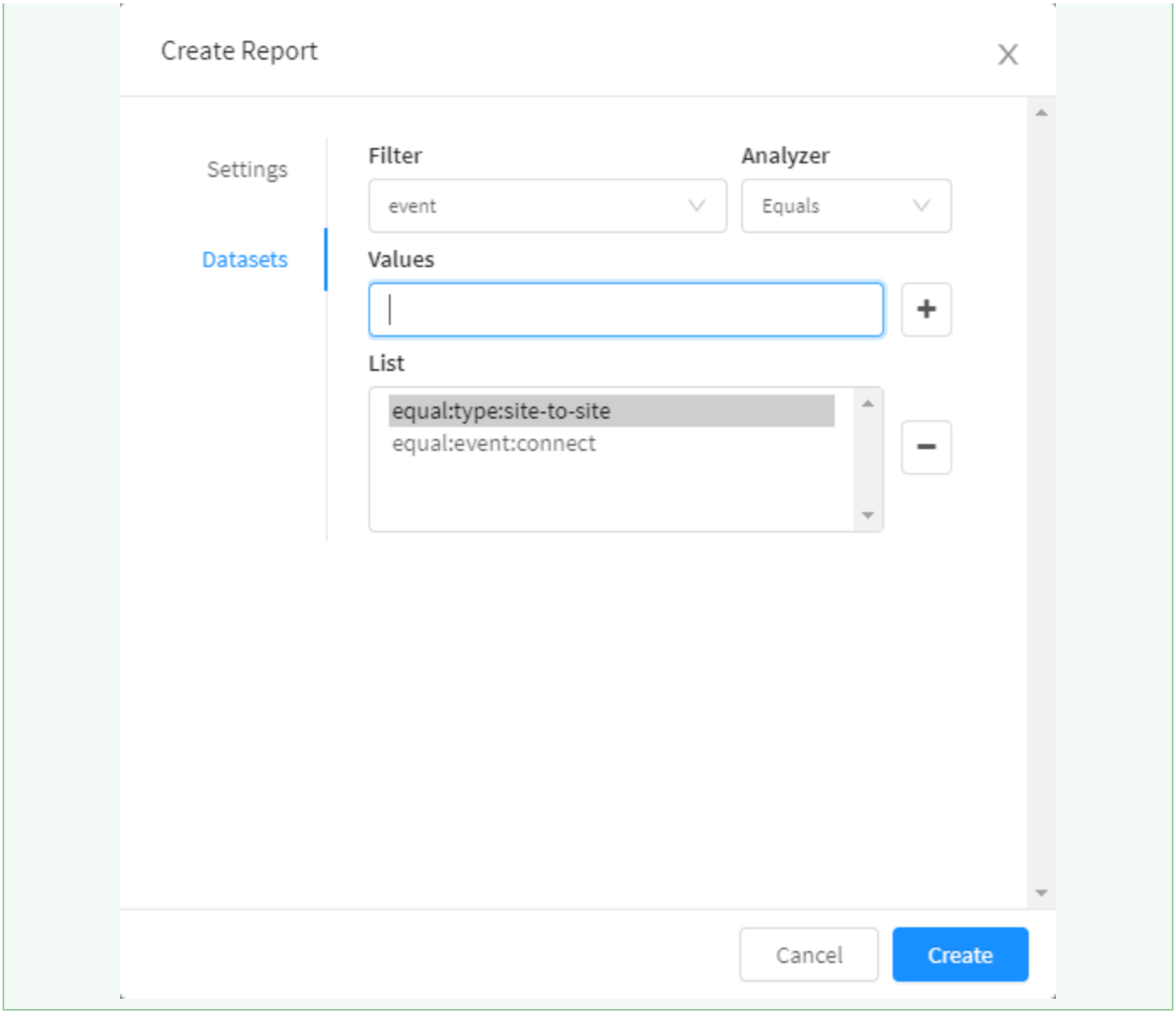
Reports – Create Report - Datasets - Log Session

In order to facilitate the configuration of the report's dataset: Note that the syntax used in Security Events is the same used in this window.

For example, if the goal is to create a report on VPN site-to-site where you hear a connection event, just click on the columns in Security Events - VPN and pay attention to the syntax that will be displayed in the search bar, as can be seen below:

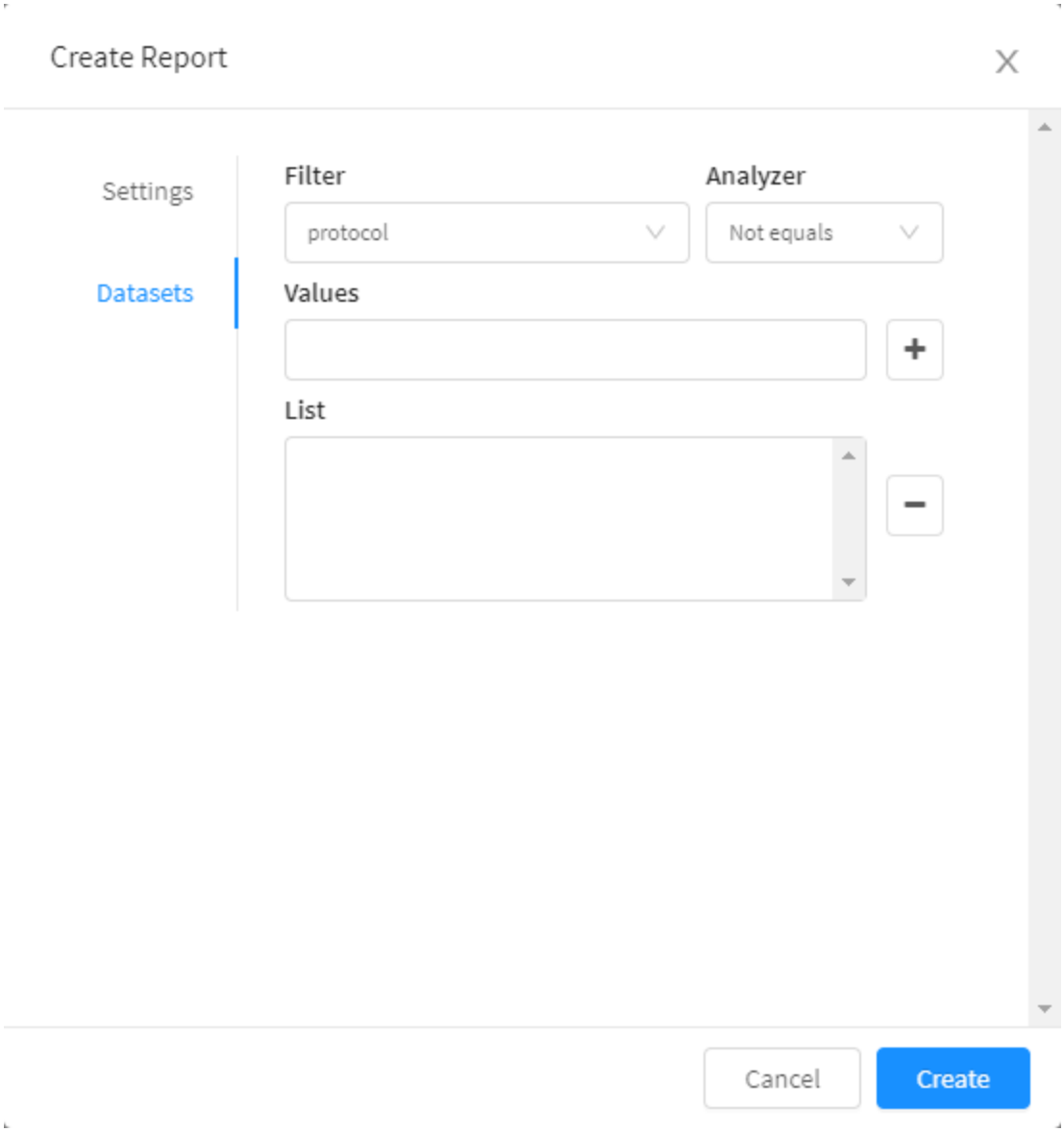


After done, back in Create Report - Datasets, replicate the same syntax using the panel's options, here's an example:



- ***Custom Queries*:** Allows selection of customized queries. The queries that appear in this field are those created in Security Events, see this page for more information;
- ***Filter*:** Determines which filter will be used. Ex.: dst;
- ***Analyzer*:** Determines which operation will be performed on the filter. Ex.: not equals;
- ***Values*:** Defines the value that will be linked to the operation and the filter. Click **[+]** to add to the list or select an entry already added and click **[−]** to remove from the list. Ex.: 1.1.1.1;
- ***List*:** Basically displays the additions made based on the previous options. Ex.: not_equal:dst:1.1.1.1.

If you selected the option "Authentication Log" or "VPN Log", the "Datasets" tab can be configured according to the options below:



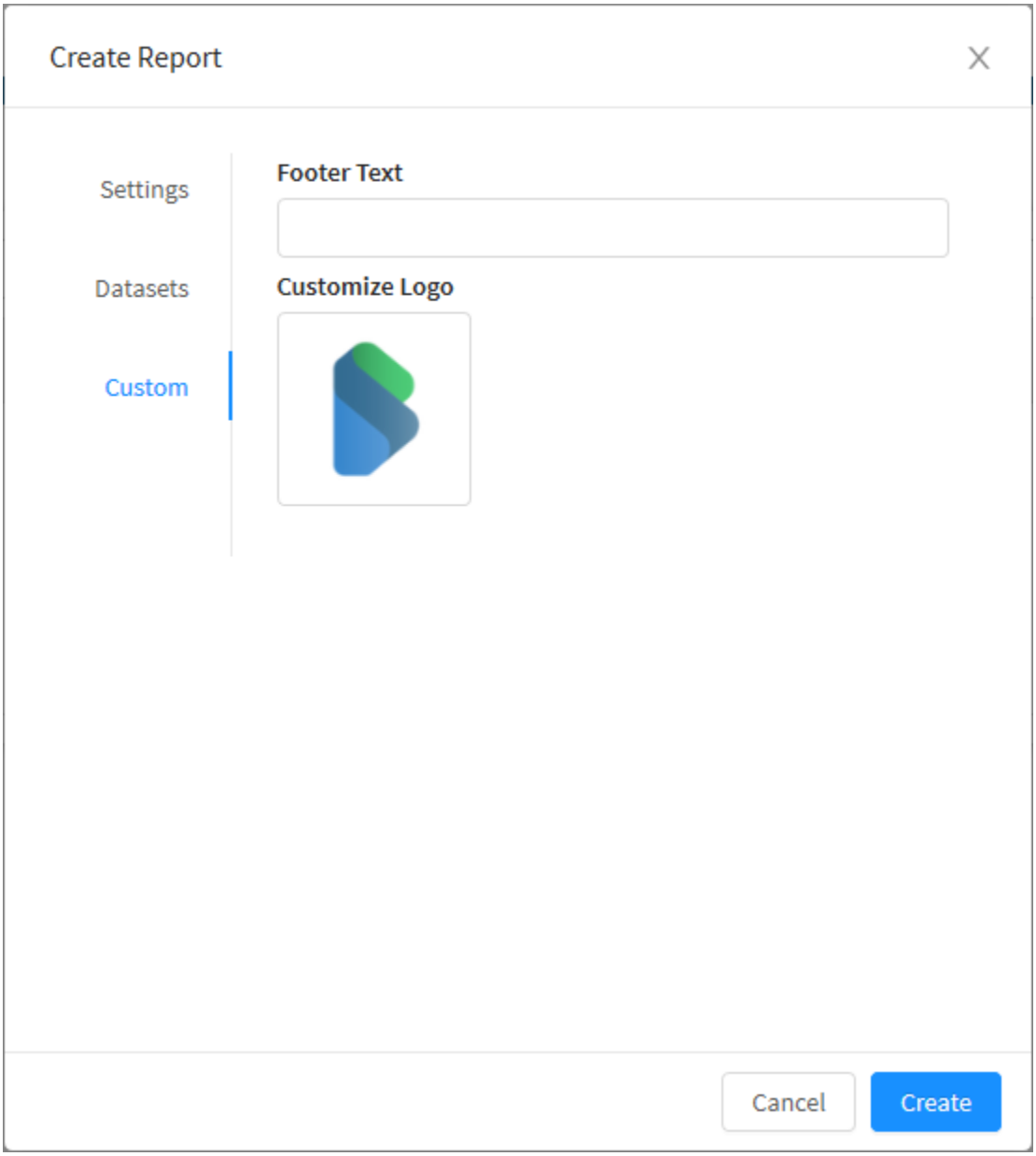
Reports - Create Report - Datasets - Authentication Log or VPN Log

- ***Filter*:** Determines which filter will be used. Ex.: dst;
- ***Analyzer*:** Determines which operation will be performed on the filter. Ex.: not equals;
- ***Values*:** Defines the value that will be linked to the operation and the filter. Click **[+]** to add to the list or select an entry already added and click **[−]** to remove from the list. Ex.: 1.1.1.1;
- ***List*:** Basically displays the additions made based on the previous options. Ex.: not_equal:dst:1.1.1.1.

Next we will analyze the content of the "Custom" side tab, it will only be displayed if the report type is "Analyzer";

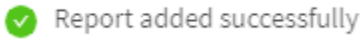
Custom tab

In the tab "Custom" it is possible to determine the text that will be footed in "Footer" and customize the "Logo" that will appear in the report.



Reports – Create Report - Custom

Click the [Cancel] button to exit this window, or click [Create] to schedule the report. If you want to issue it immediately, configure it to run on today's date.



Report successfully added

After these steps, the report will have been successfully created.

For examples of how to create the reports, visit this page.

If you want more information on how to delete a report, see this page.

Examples - Creating Reports

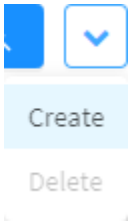
Next, we will exemplify the creation of some examples of reports as a way to demonstrate good practices. The models presented aim to guide and serve as a basis for the user to create their own reports according to their preference and need.

We will carry out the demonstration by creating the following reports:

- Example 1 - Firewall report*;*
- Example 2 - Webfilter report for foreign access destination that was allowed by the policies*;*
- Example 3 - Site-to-site VPN connection report with specific source and destination*.*

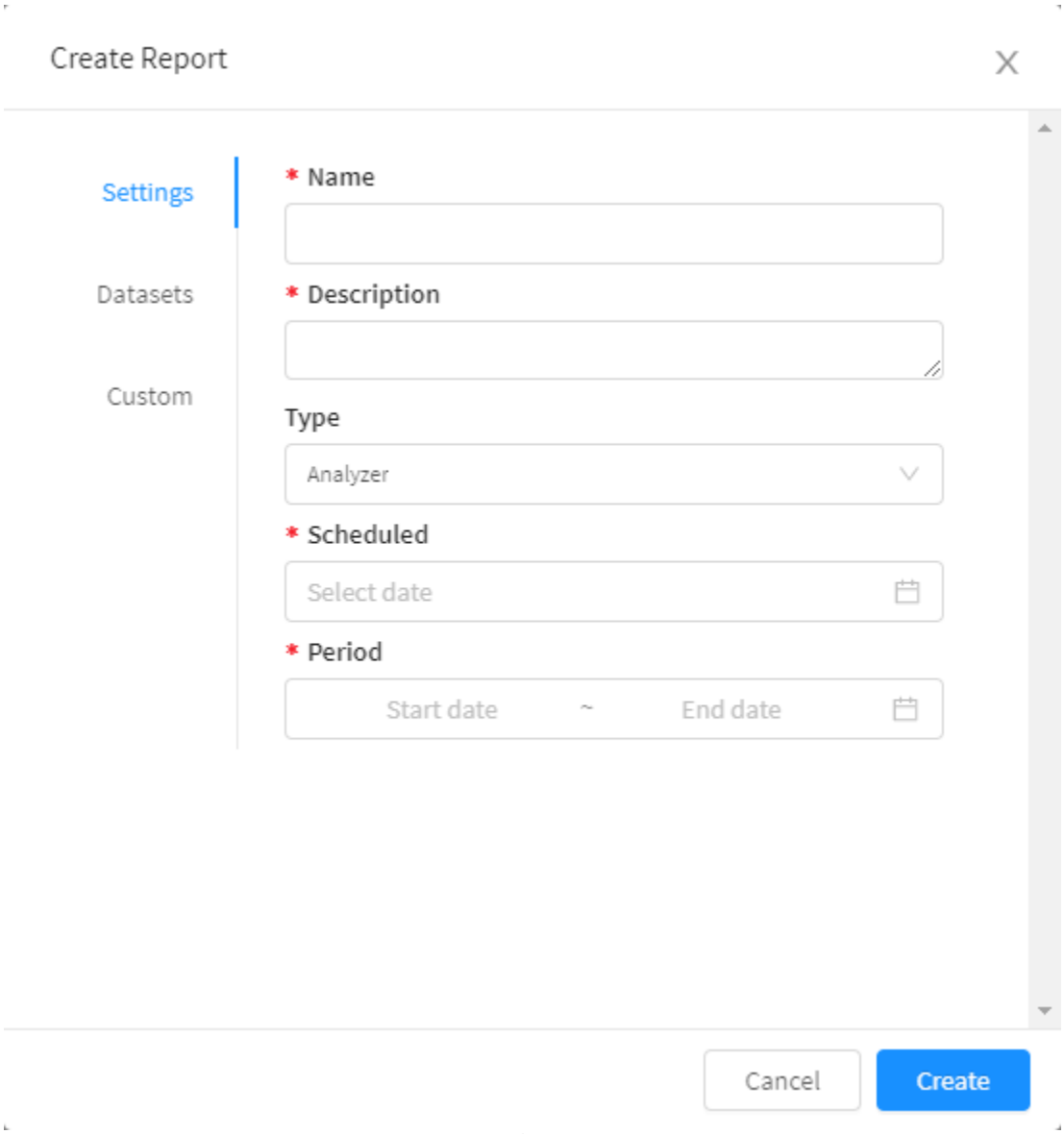
Example 1 - Firewall Report

To generate a firewall report, first click on the actions menu [ ] and select the "create" option:



Actions menu - Create

The "Create Report" window will be displayed as shown below:

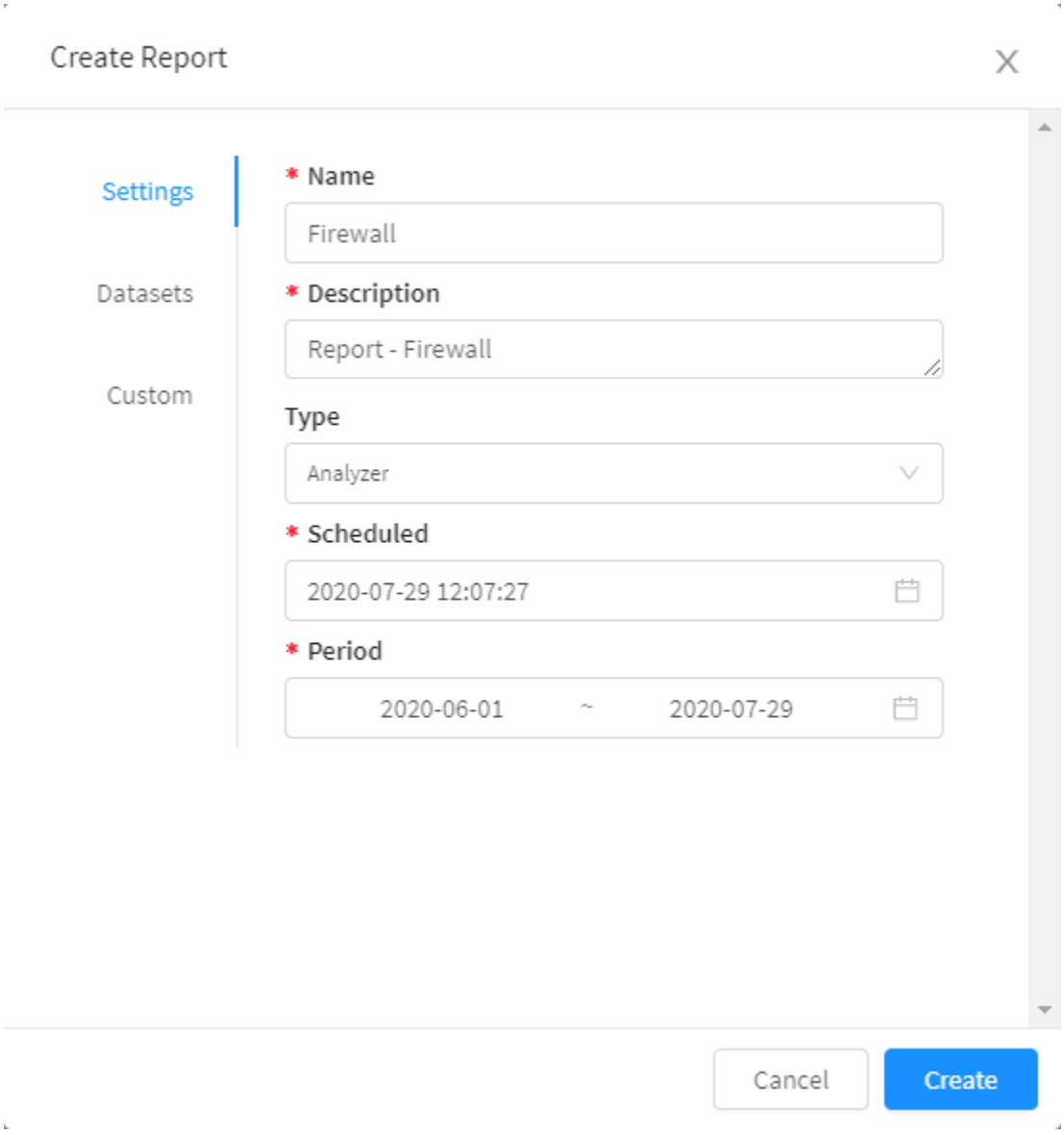


Reports - Create Report

In the "Settings" tab, follow the instructions below.

Settings

Complete the form as follows:



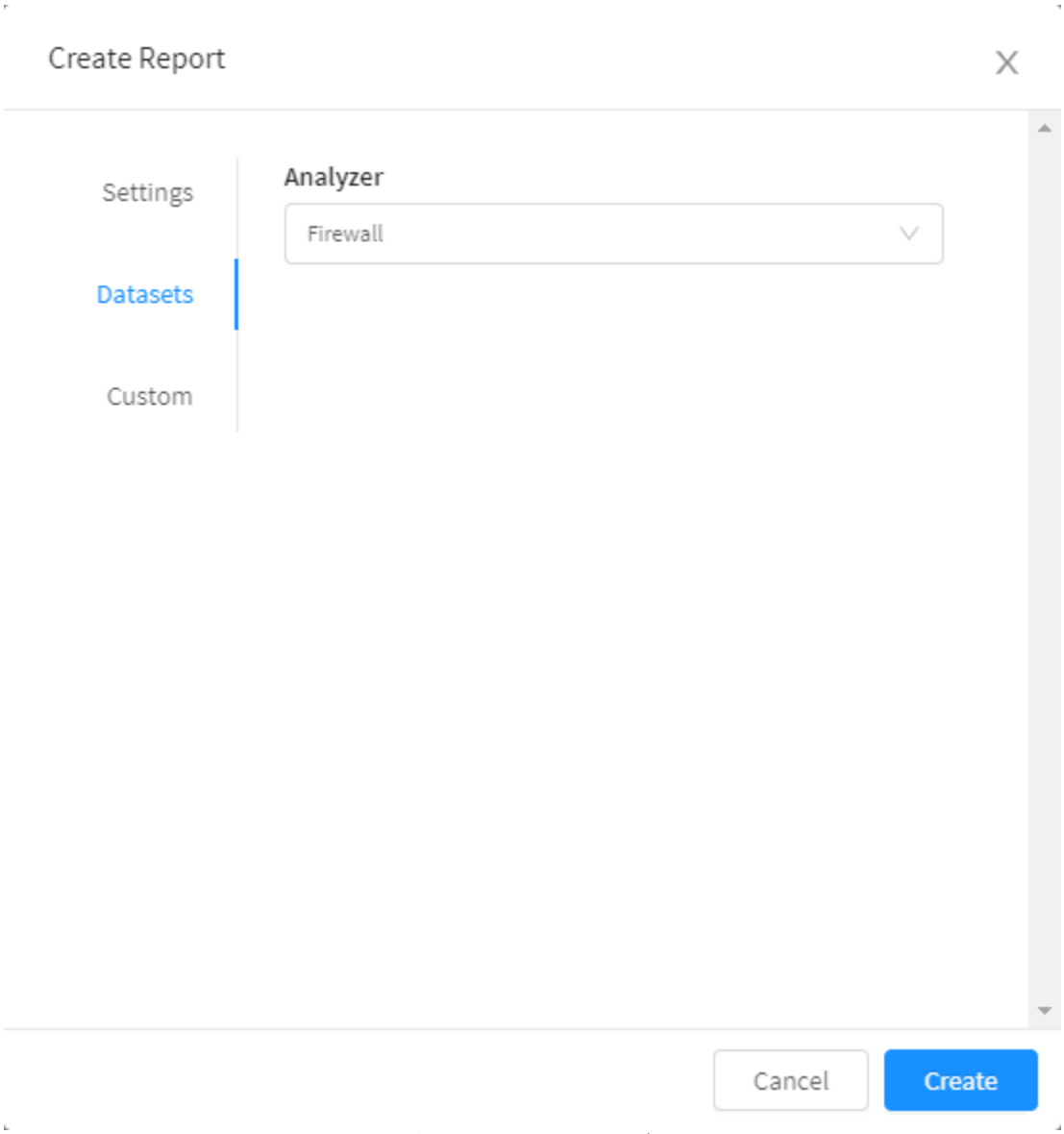
Create Report - Settings tab

- ***Name*:** Type "Firewall";
- ***Description*:** Type "Report - Firewall";
- ***Type*:** Select the "Analyzer" type report;
- ***Scheduled*:** Select a date and time to schedule the creation of the report;
- ***Period*:** Select a starting and ending period.

When finished, access the "Datasets" side tab.

Datasets

Select the option according to the example:



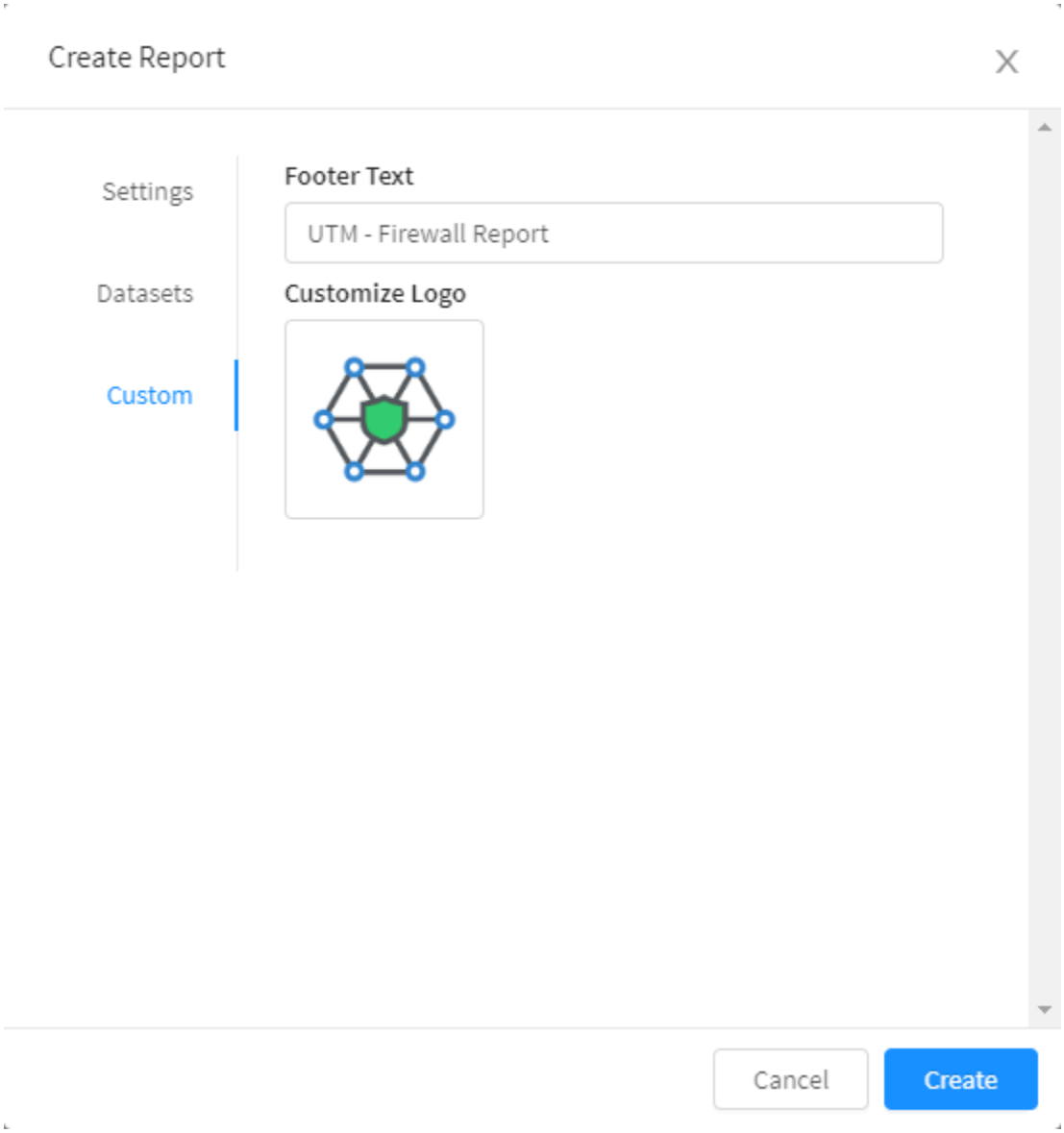
Create Report - Datasets tab

- ***Analyzer*:** Select the "Firewall" option.

When finished, access the "Custom" side tab.

Custom

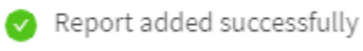
This tab depends on the user's design. In the example, we set up as shown below:



Create Report - Custom tab

- ***Footer Text*:** At the bottom, type "NGFW - Firewall Report";
- ***Customize Logo*:** Upload your company logo. In this example, we use the NGFW icon.

After configuring each tab according to the example definition applied, click [Create].



Report successfully added

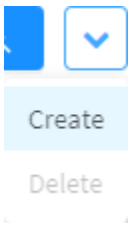
After these steps, the report will have been successfully created.

To see example 2, click on this link.

Example 2 - Web Filter report on accesses to foreign destinations allowed by Policies

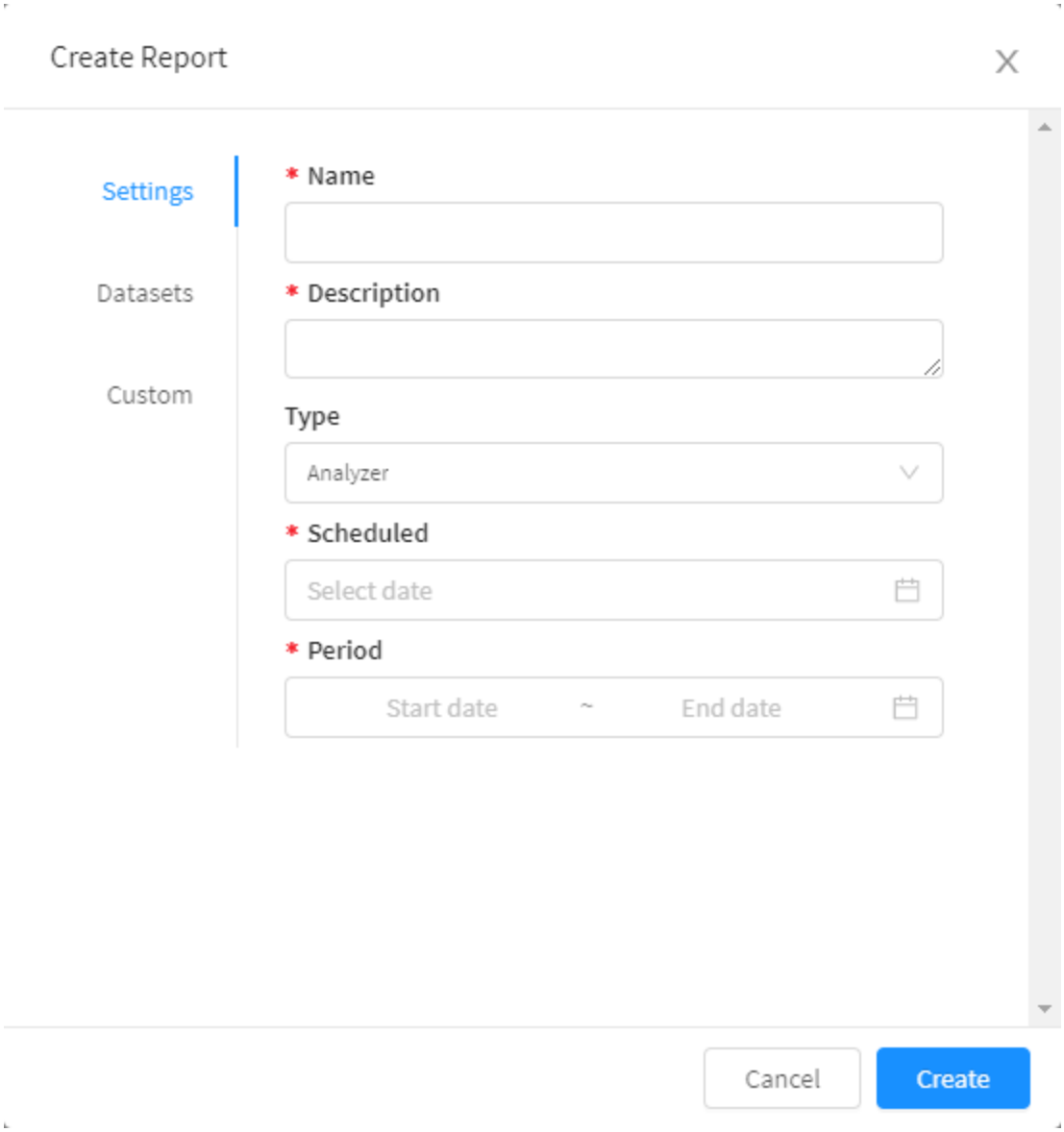
In this example, we will create a Web Filter report to display all connections that have been made to foreign sites where the policy has allowed access.

To generate a Web Filter report, first click on the actions menu **[ ]** and select the "create" option:



Actions menu - Create

The "Create Report" window will be displayed as shown below:

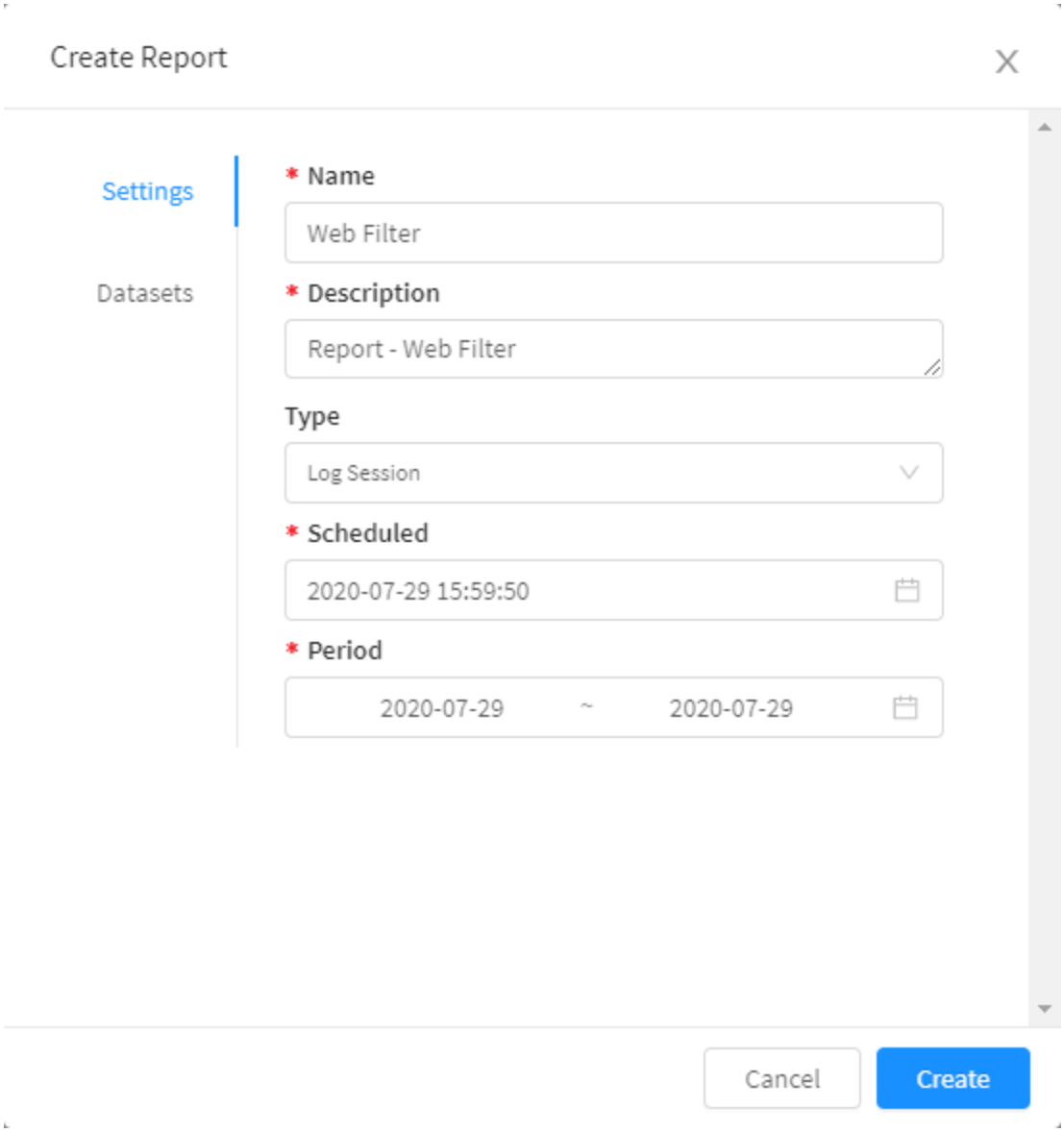


Reports - Create Report

In the "Settings" tab, follow the instructions below.

Settings

Complete the form as follows:



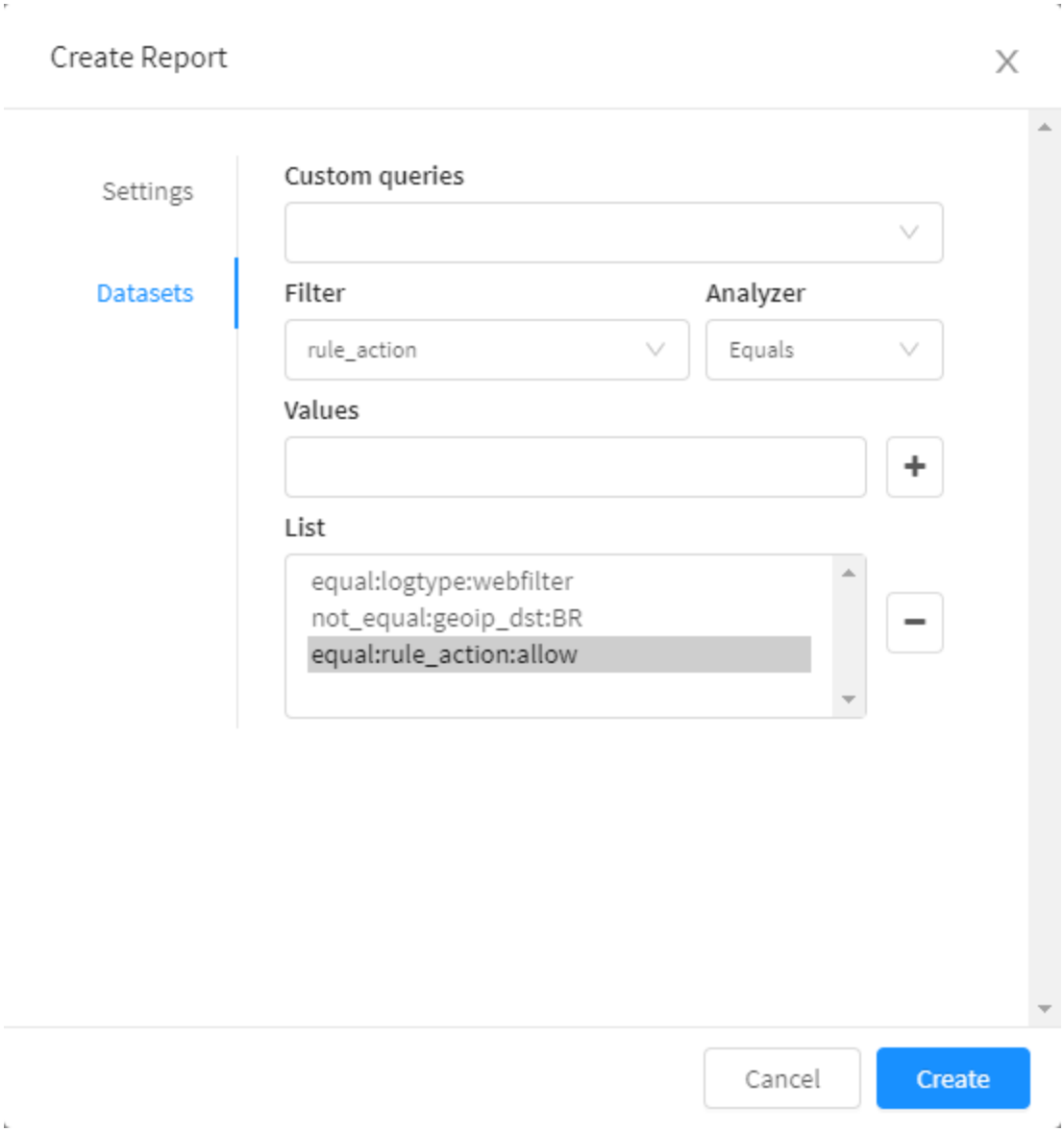
Create Report - Settings Tab

- ***Name*:** Type "Web Filter";
- ***Description*:** Type "Report - Web Filter";
- ***Type*:** Select the "Log Session" report;
- ***Scheduled*:** Select a date and time to schedule the creation of the report;
- ***Period*:** Select a starting and ending period.

When finished, access the "Datasets" side tab.

Datasets

Select the option according to the example:



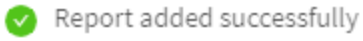
Create Report - Datasets Tab

In this tab we will add 3 conditions:

- ***Log Type Web Filter:*** In **Filter,** select "logtype", leave the **Analyzer** as "equals", in **Values** type "webfilter" and click the **[ ]** button to add it to the list;
- ***Foreign destination geographic location:*** In **Filter**, select "geoip_dst", in **Analyzer** select "Not Equals", in **Values** type "BR" and click the **[ ]** button to add it to the list;
- ***Policy allowed access:*** In **Filter**, select "rule_action", leave the **Analyzer** as "equals", in **Values** type "allow" and click the **[ ]** button to add it to the list;

After adding these conditions, the report will be created specifically for Web Filters whose access to foreign destinations permitted by Policies.

After configuring each tab according to the example definition, click **[Create]**.



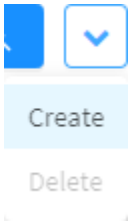
Report successfully added

After these steps, the report will have been successfully created.

Example 3 - Site-to-site VPN connection report with specific source and destination

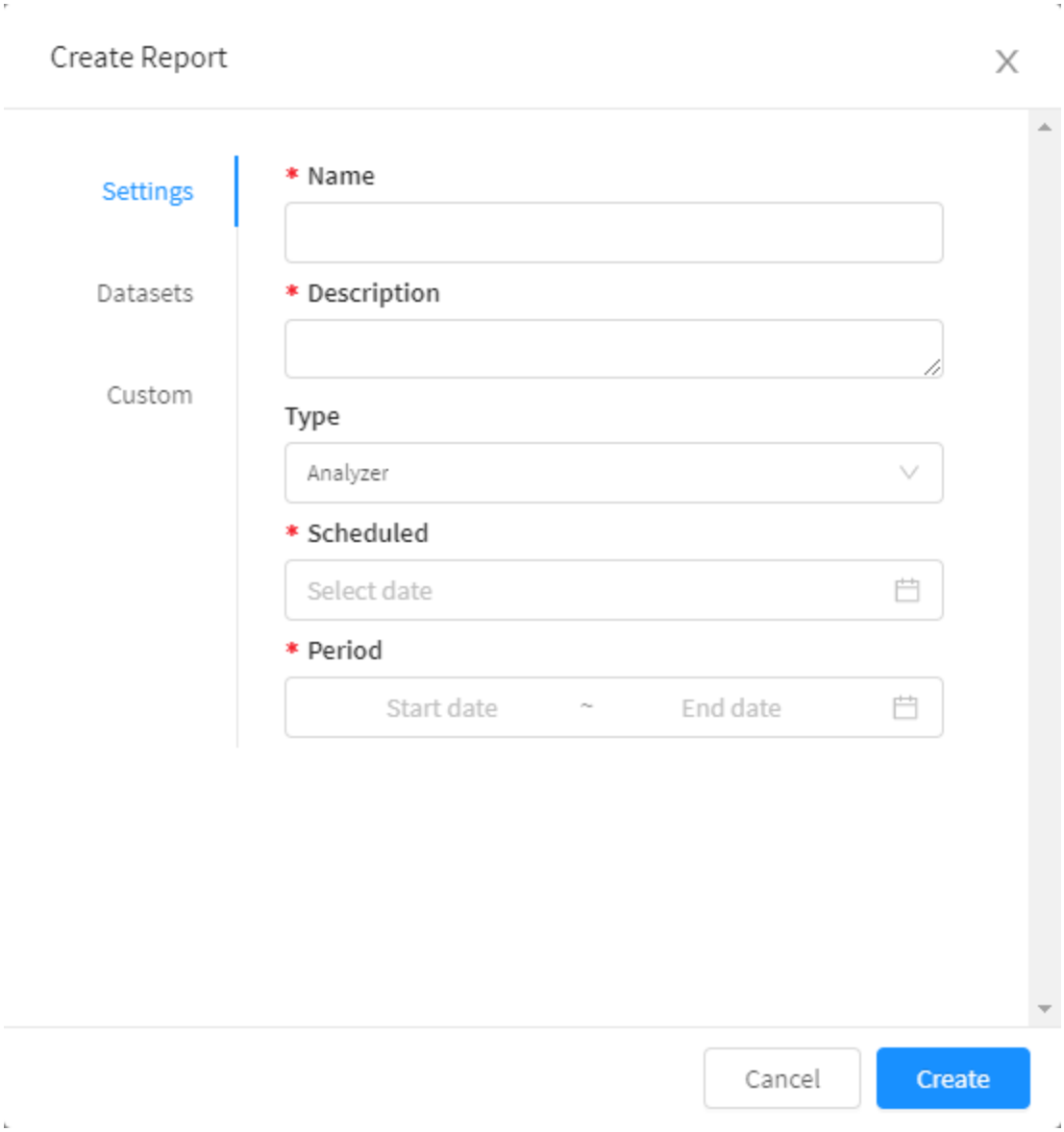
In this example we are going to create a site-to-site VPN connection report in order to locate all accesses made within a specific source and destination IP.

To generate a VPN report, first click on the actions menu **[** **]** and select the "create" option:



Actions menu - Create

The "Create Report" window will be displayed as shown below:

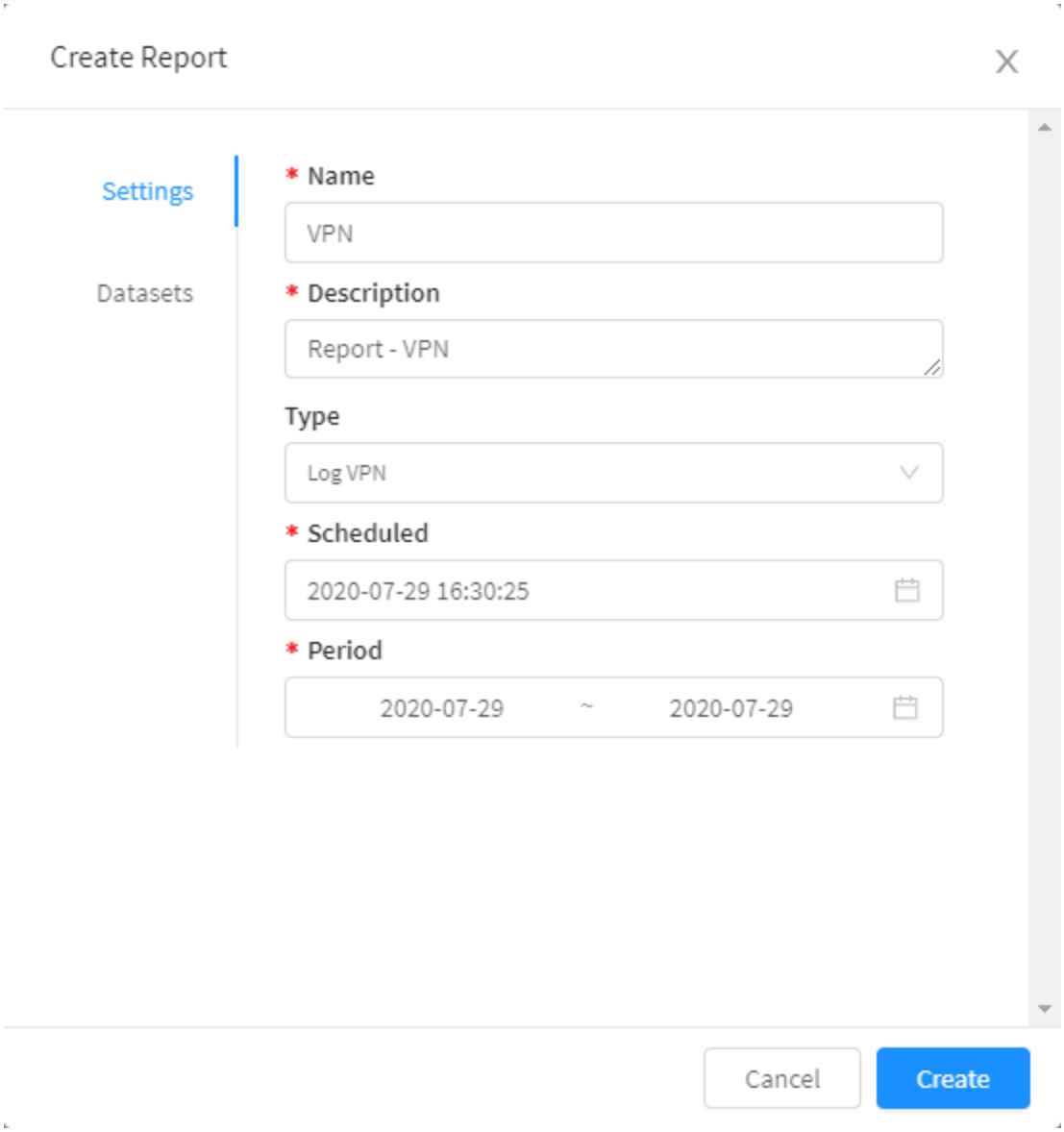


Reports - Create Report

In the "Settings" tab, follow the instructions below.

Settings

Complete the form as follows:



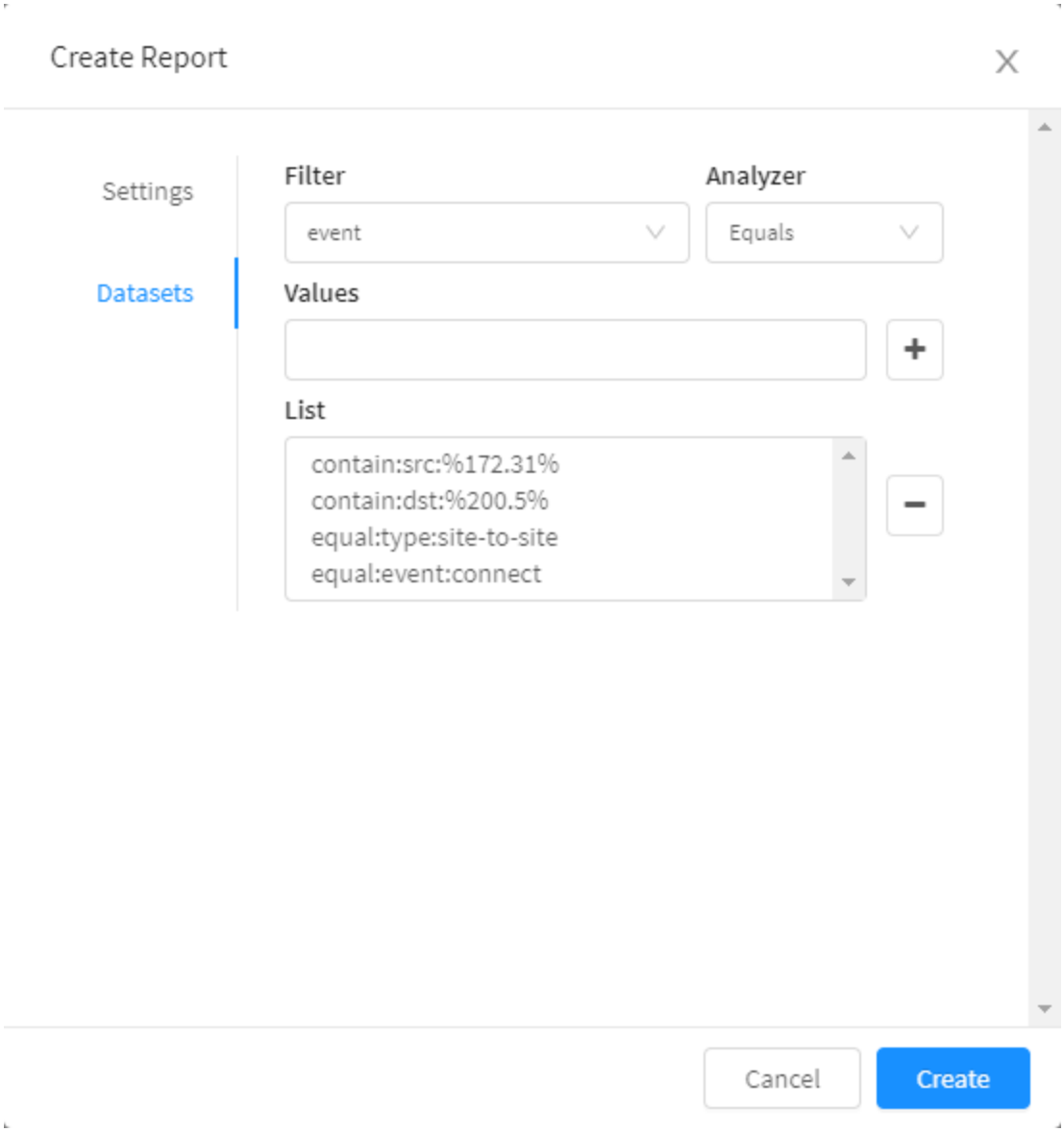
Create Report - Settings Tab

- ***Name*:** Type "VPN";
- ***Description*:** Type "Report - VPN";
- ***Type*:** Select the "Log VPN" report;
- ***Scheduled*:** Select a date and time to schedule the creation of the report;
- ***Period*:** Select a starting and ending period.

When finished, access the "Datasets" side tab.

Datasets

Select the option according to the example:



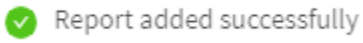
Create Report - Aba *Datasets*

In this tab we will add 4 conditions:

- ***The source IP starts with 172.31:*** In **Filter**, select "src", in **Analyzer** select "Contain", in **Values** type "172.31" and click the **[+]** button to make the addition in the list;
- ***The destination IP has 200.5:*** In **Filter**, select "dst", in **Analyzer** select "Contain", in **Values** type "200.5" and click the **[+]** button to make the addition in the list;
- ***The VPN type is site-to-site:*** In **Filter**, select "type", leave the **Analyzer** as "equals", in **Values** type "site-to-site" and click the **[+]** button to add it to the list;
- ***We just want connection events:*** In **Filter**, select "event", leave the **Analyzer** as "equals", in **Values** type "connect" and click the **[+]** button to add it to the list;

After adding these conditions the report will be created specifically for site-to-site VPNs whose source IP has "172.31" the destination IP has "200.5" and a connection is made.

After configuring each tab according to the example definition applied, click [Create].



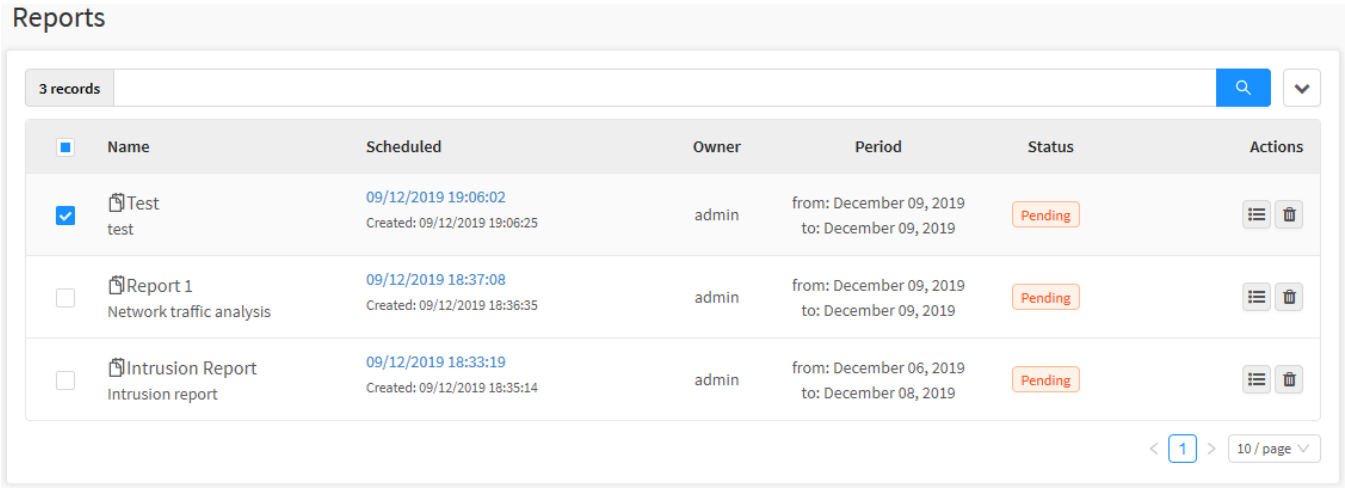
Report successfully added

After these steps, the report will have been successfully created.

Monitor - Reports - Actions menu - Delete

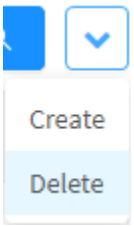
Through the “Delete” button it is possible to erase the selected Reports. To delete via the Actions menu, follow these steps:

1. Select which Report (s) you want to delete. To select, just click with the mouse on the checkbox located next to the name. In the selected reports the checkbox will change from gray to blue **[ ]**. Ex.: *Test*;



Reports - Selection of Reports to delete

2. Enter the **actions menu [ ]** and click on the “Delete” option.



Reports – Delete

3. The notification message will appear to confirm the deletion of the selected Reports:

Reports – Report deletion message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

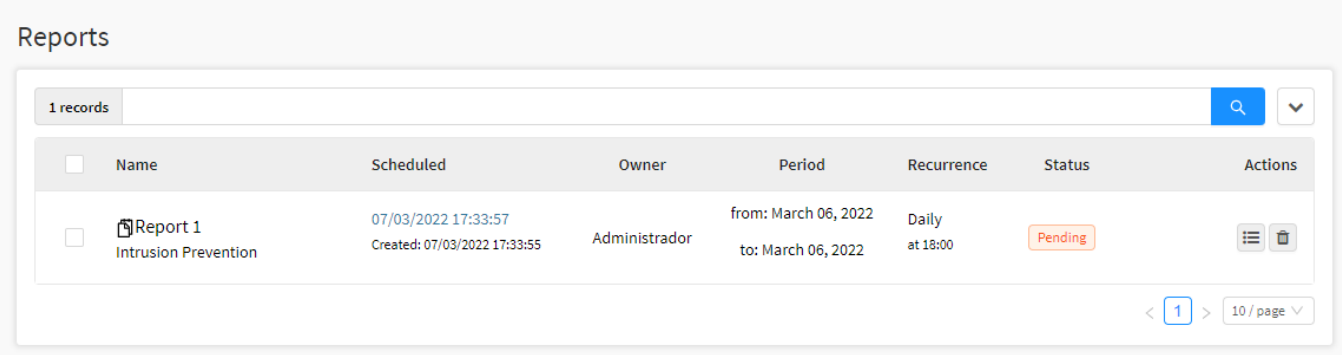
Profile successfully deleted

After performing these procedures, the reports will have been successfully deleted.

Next, we will analyze the columns displayed on the Monitor Reports screen.

Monitor - Reports - Columns

We will explain each column of the Reports tab:



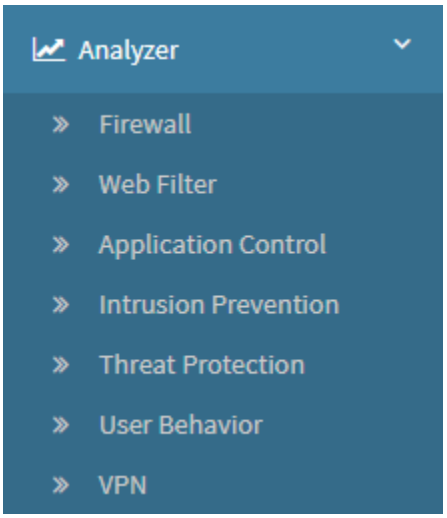
Reports

- **Select [ ]:** Allows you to select a report;
- ***Name*:** Displays the name of the report registered in the *Create* option of the action menu. Just below the name is the description registered in the same menu;
- ***Scheduled*:** Displays the schedule for when the report will run, just below that date the date when this process was created;
- ***Owner*:** Displays the user responsible for creating this schedule;
- ***Period*:** This is where the period when data will be extracted from the system is recorded;
- ***Recurrence:*** This is how often the Report will run;
- ***Status*:** The current production status of the report is displayed. Can be:
  - ***Visualize*** [Visualize]**:** You can view the report by clicking this button;
  - ***Download*** [Download]**:** It is possible to download the PDF or CSV report by clicking this button;
  - ***Pending*** [Pending]**:** If the report has not yet been generated, it will be marked with this status.
- ***Actions*:** Buttons with essential functions for interacting with reports:
  - **Visualize [ ]:** Allows you to edit the settings of the Report added in the *Create* option of the actions menu;
  - **Delete [ ]:** Deletes the selected report.

UTM - ANALYZER

In addition to the dashboard already presented, Blockbit NGFW, has a “Reports” management feature that returns essential information for the administration and management of events and information that gathers SUMMARIZED and DETAILED data from the main services. All system reports are stored on the server for 7 days.

The main difference between the reports displayed in Events and those in Analyzer is:
In Events, a connection record is generated with zeroed attributes (bytes and packets), after disconnection another event is generated recording these attributes, the traffic and the connected time.
In Analyzer, the reports are summarized every 5 minutes, generating reports from time to time with data generated in the period.



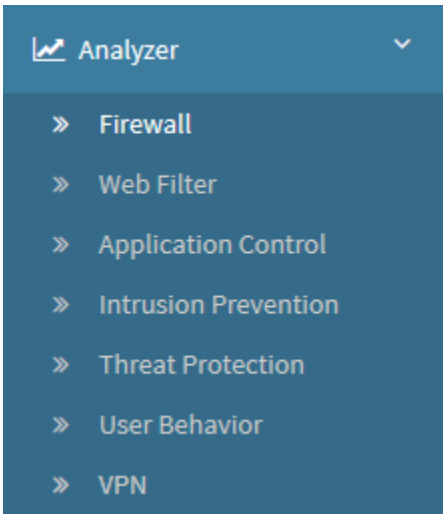
Analyzer

Contains the options:

- Firewall;
- Web Filter;
- Application Control;
- Intrusion Prevention;
- Threat Protection;
- User Behavior;
- VPN.

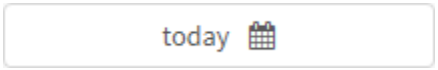
UTM - Firewall

To access network traffic reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “Firewall” option.



Firewall

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

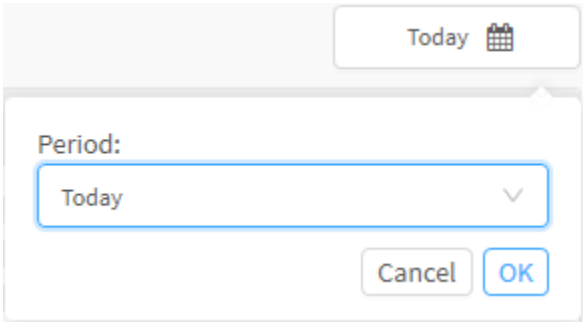


Firewall - Date check box

Its purpose is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



Firewall – Date Selection

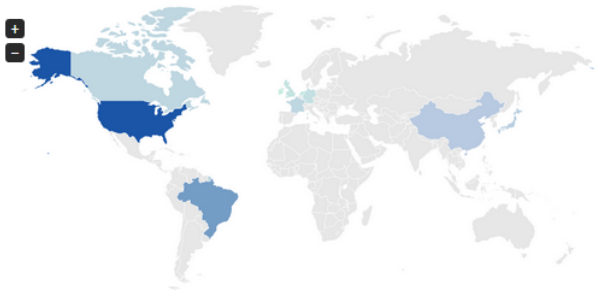
To close this window, click **[** Cancel **]** button or, after selecting the desired date, click **[** OK **]** button;

The screen below will appear:

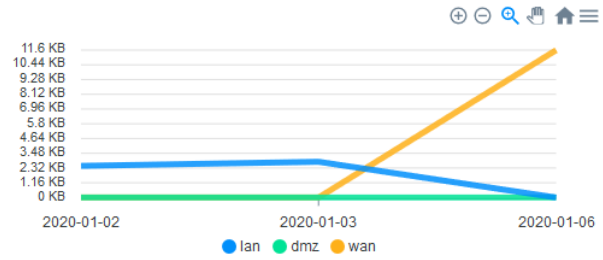
Firewall

last_30 | Blockbit

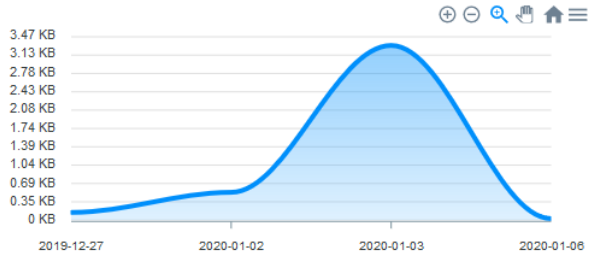
Geolocation Hits



Zone Traffic

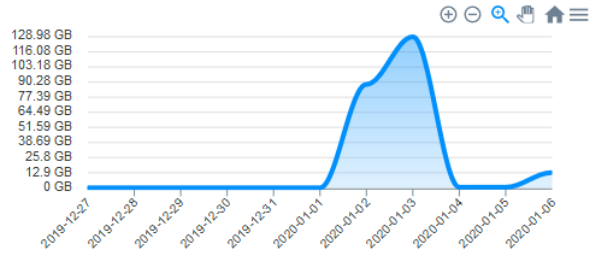


Top User



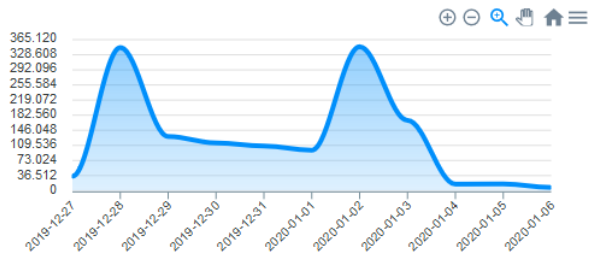
#	User	Traffic
1	user1@domain.com	4.01 KB

Top Service



#	Services	Traffic
1	98	186.67 GB
2	443	44.11 GB
3	22	544.88 MB
4	80	901.93 KB
5	123	808.32 KB
6	53	594.77 KB
7	54648	2.44 KB
8	41648	2.13 KB

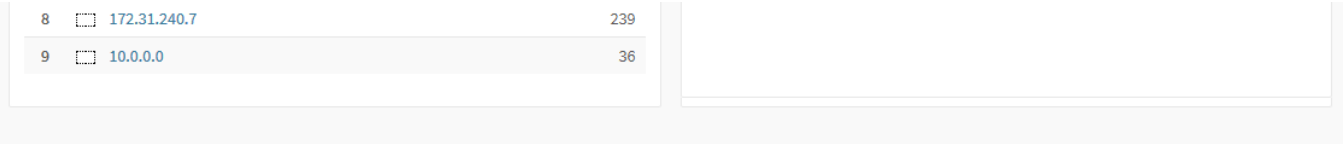
Top Source



#	Source	Hits
1	172.31.102.184	905.849
2	172.31.0.100	279.991
3	172.31.240.250	149.249
4	172.31.240.252	55.368
5	192.168.1.1	327
6	0.0.0.0	301
7	192.168.15.1	280

Top Policy

#	Policy	Traffic
1	Content Block (Wifi)	4.55 GB
2	ByPass	1.88 GB
3	Block - files	1.44 GB
4	ByPass Wifi	235.76 MB
5	Block streaming	231.9 MB



Analyzer - Firewall

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom;
- **[ ]:** Its function is to remove the zoom;
- **[ ]:** It serves to make a selection zoom;
- **[ ]:** Serves to move the graph;
- **[ ]:** Reset the graph to the starting position;
- **[ ]:** Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

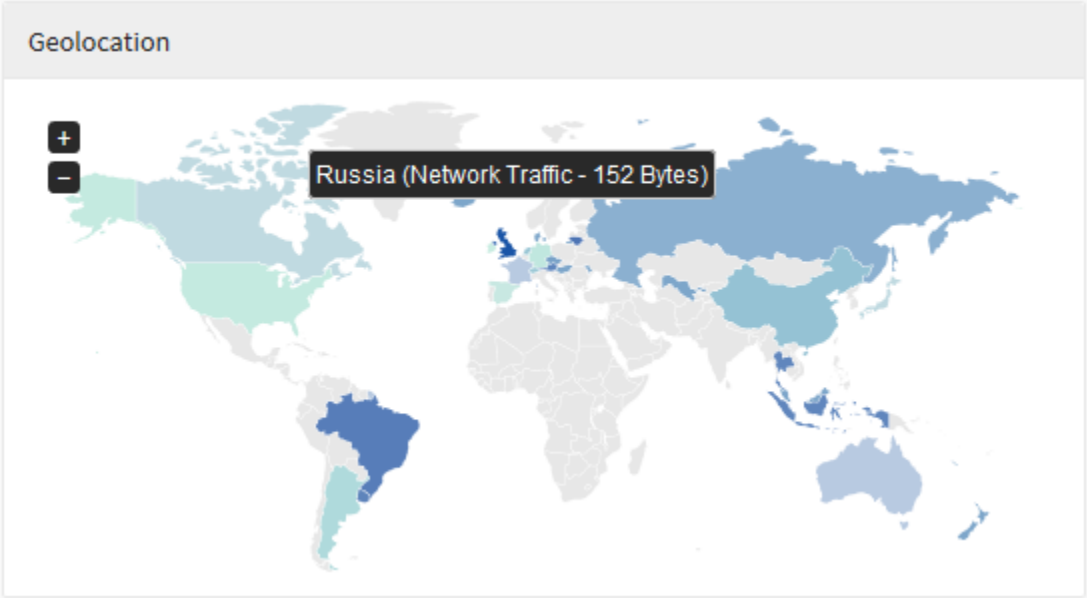
To perform a search, type a term in the search bar and click the search **[ ]** button.

Next, we will analyze in detail the components of “Firewall”:

- *Geolocation*;
- *Zone Traffic*;
- *Top User*;
- *Top Service*;
- *Top Source*;
- *Top Policies*.

UTM - Firewall – Geolocation

In “Geolocation” the destination of the connections of the network users is displayed, the global map demonstrates through a colored legend the amount of accesses made by the users. When hovering the mouse over the countries a total number of accesses is displayed, when doing the same with the legend it is possible to view an average, in addition, the country referring to this value is highlighted on the map.

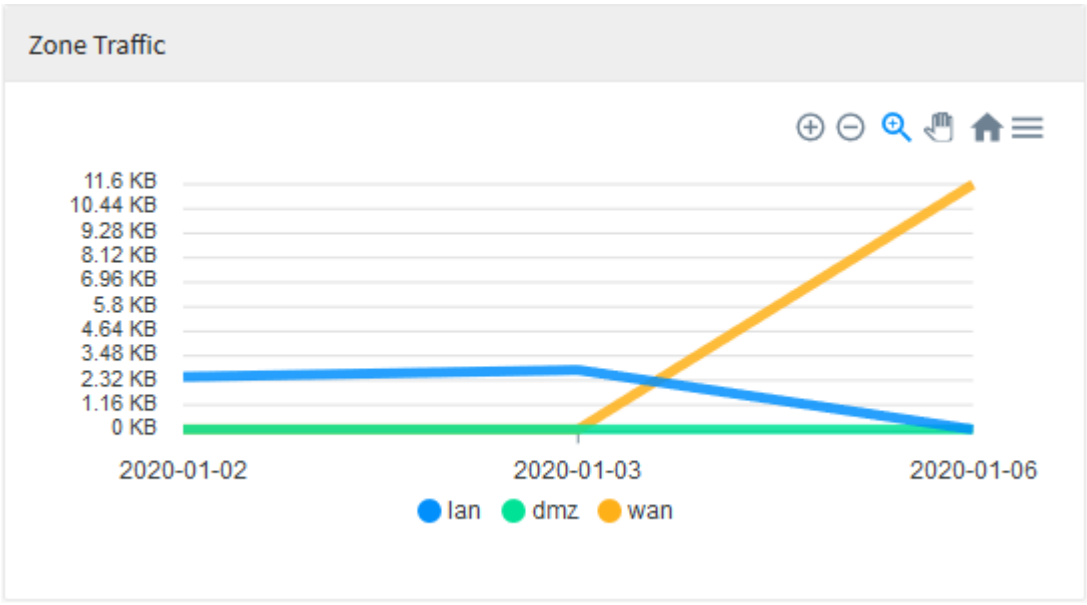


Firewall – Geolocation

UTM - Firewall – Zone Traffic

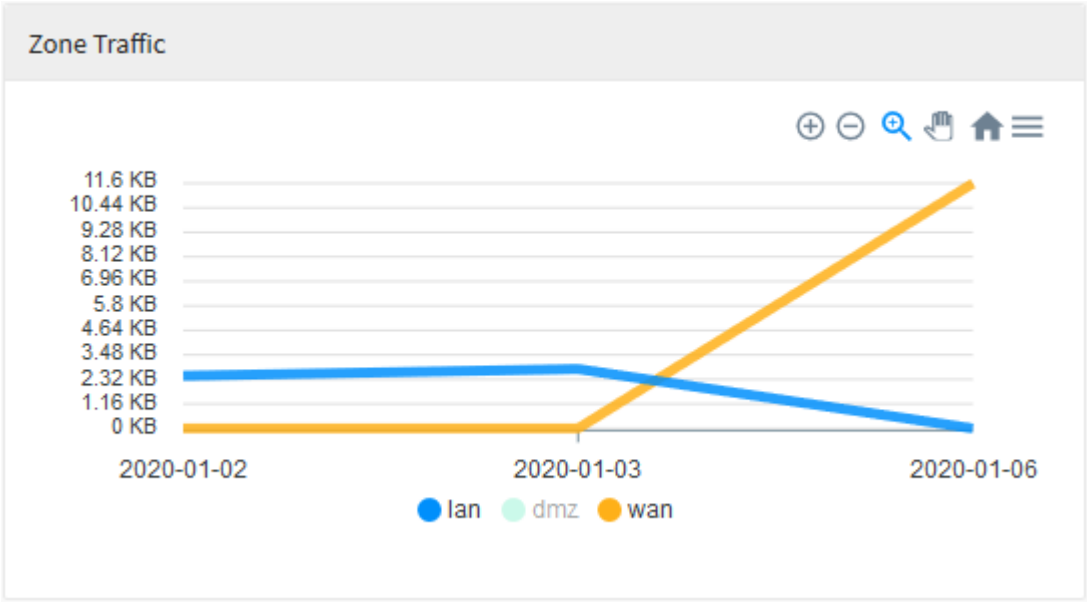
In “Zone Protection” we have a graph showing the amount of traffic in a given zone, through a line graph it is possible to observe these amounts being illustrated over a period of time. When clicking on the type of network used (for example: “LAN”, “DMZ”, “WAN” and etc.), the diagram is changed in order to display the selected option, which allows to analyze the traffic in more detail according to with selected dates.

For more information about the navigation menu at the top of this graph, check this page.



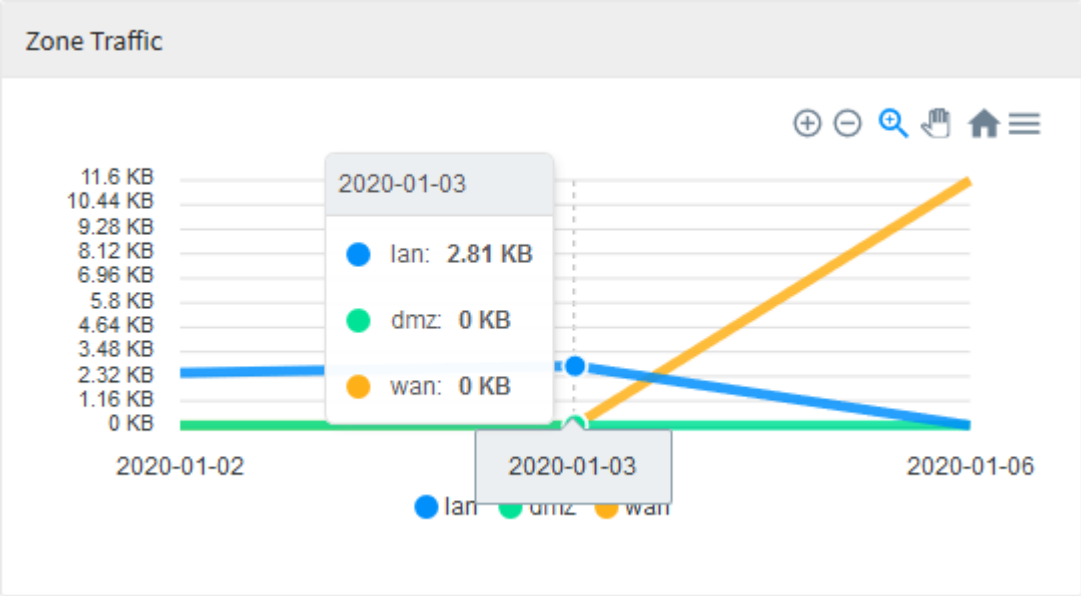
Firewall – Zone Traffic

You can click on the legends below the graph to hide any of the lines in order to illustrate the relevant information, as shown below:



Firewall – Zone Traffic - Hidden DMZ line

When you move your mouse over the graph, a summary of all traffic for the period is displayed, as shown on the image below:

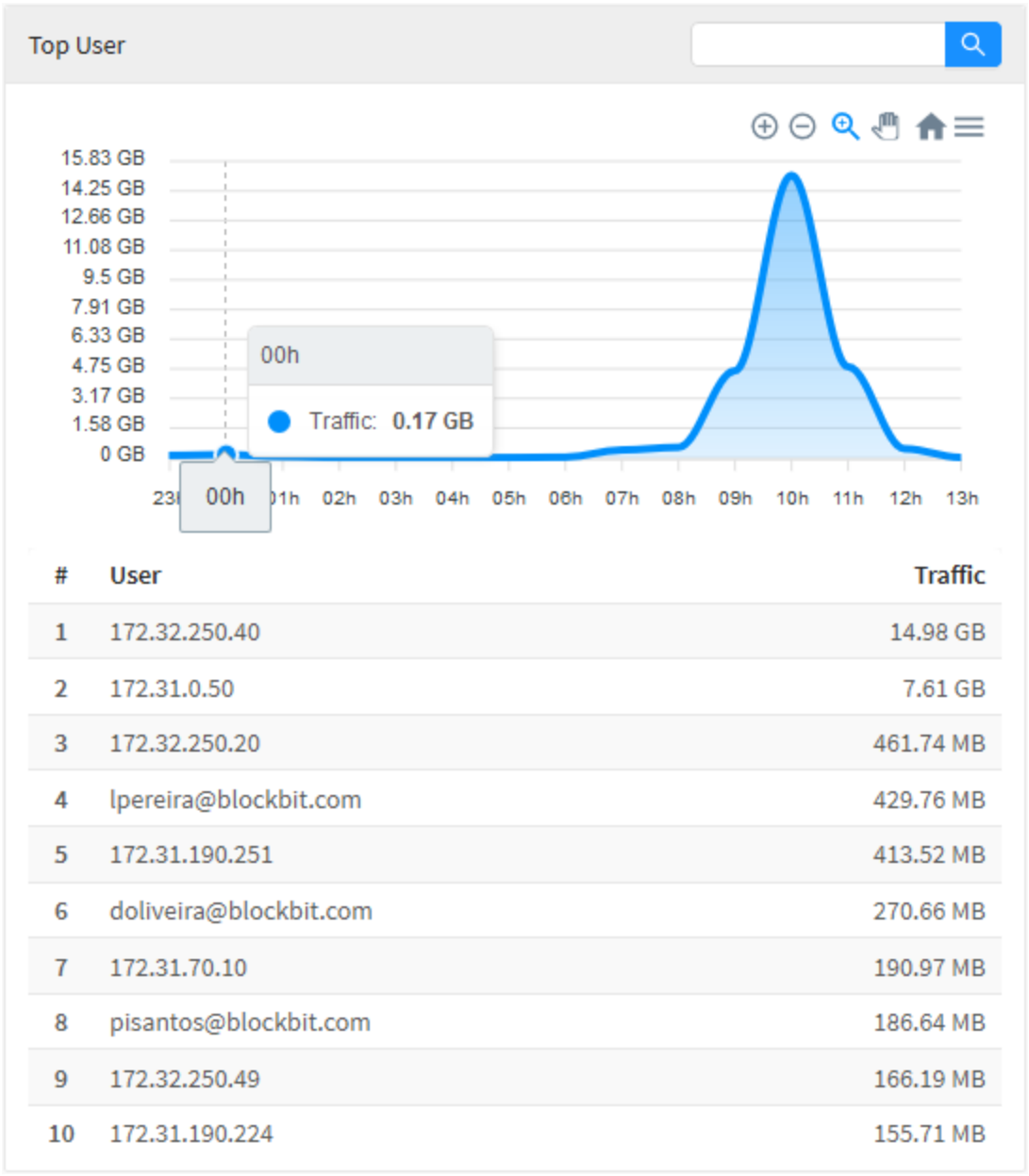


Firewall – Zone Traffic - Summary of results

UTM - Firewall – Top User

In "Top User" there is a diagram showing by date when there was the highest network traffic and a list showing ten users classified by order of use of Gigabytes. When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

For more information about the navigation menu and the search bar at the top of this graph check this page.



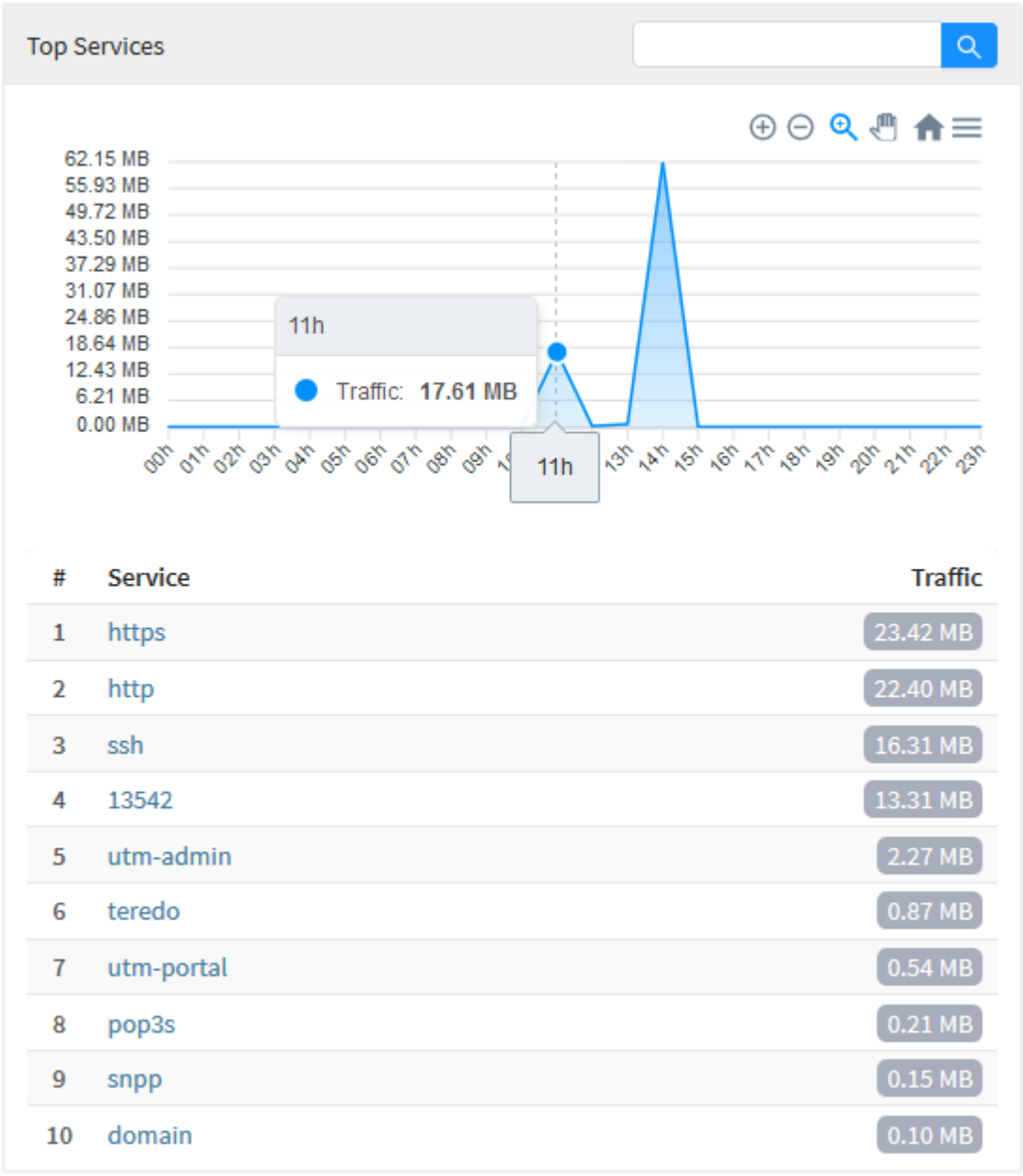
#	User	Traffic
1	172.32.250.40	14.98 GB
2	172.31.0.50	7.61 GB
3	172.32.250.20	461.74 MB
4	lpereira@blockbit.com	429.76 MB
5	172.31.190.251	413.52 MB
6	doliveira@blockbit.com	270.66 MB
7	172.31.70.10	190.97 MB
8	pisantos@blockbit.com	186.64 MB
9	172.32.250.49	166.19 MB
10	172.31.190.224	155.71 MB

Firewall – Top User

UTM - Firewall – Top Service

In “Top Service” there is a diagram showing by date when there was more network traffic and a list showing the ten most used types of services, these being classified in order of use of Gigabytes. When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below.

For more information about the navigation menu and the search bar at the top of this graph check this page.

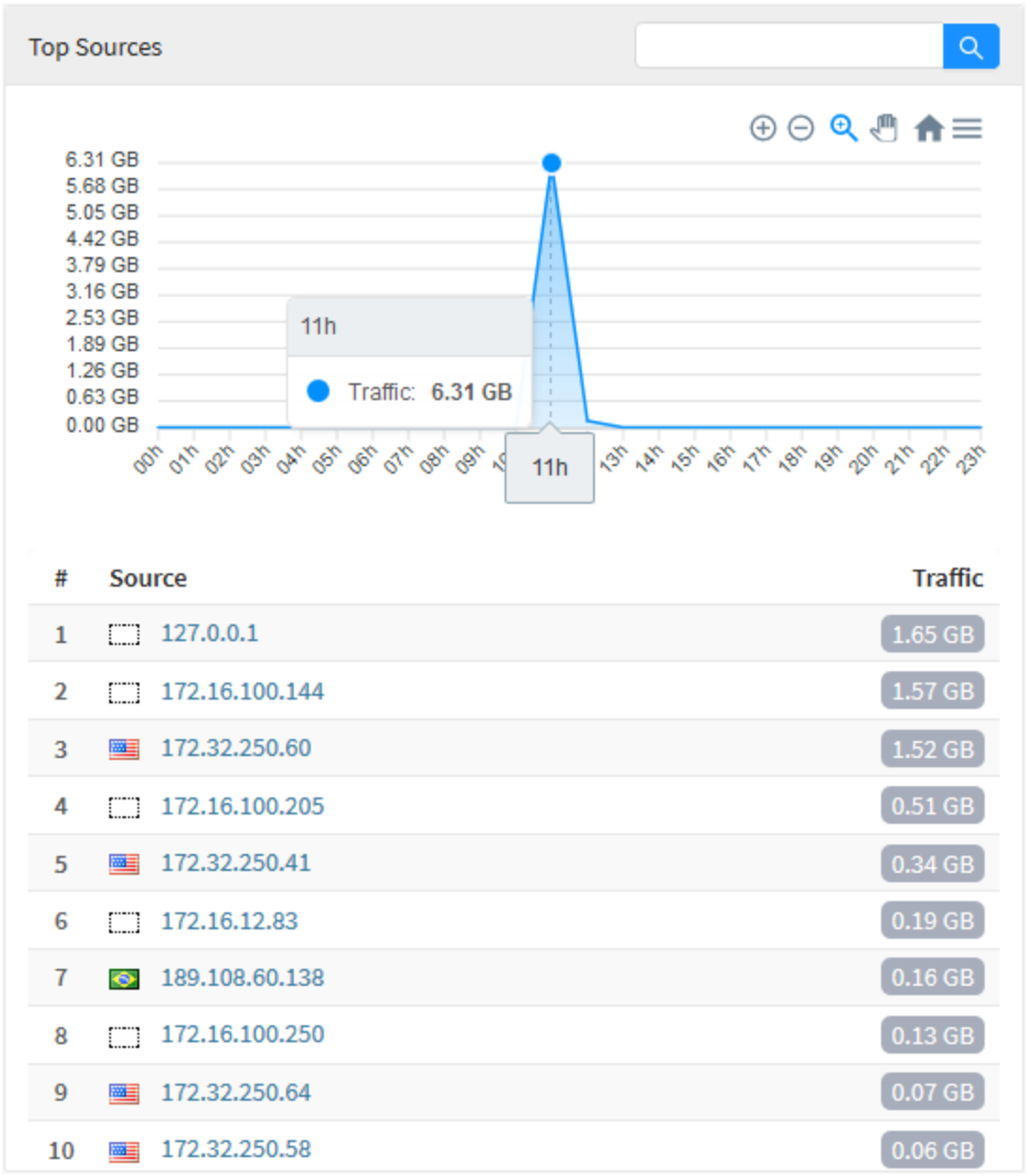


Firewall – Top Service

UTM - Firewall – Top Source

In “Top Source” there is a diagram showing by date when there was more network traffic and a list showing the ten largest sources of network traffic classified by order of use. When you hover your mouse over the graph, the network traffic for a given period is displayed, as shown in the image below. Finally, when you click on one of these IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected IP.

For more information about the navigation menu and the search bar at the top of this graph check this page.

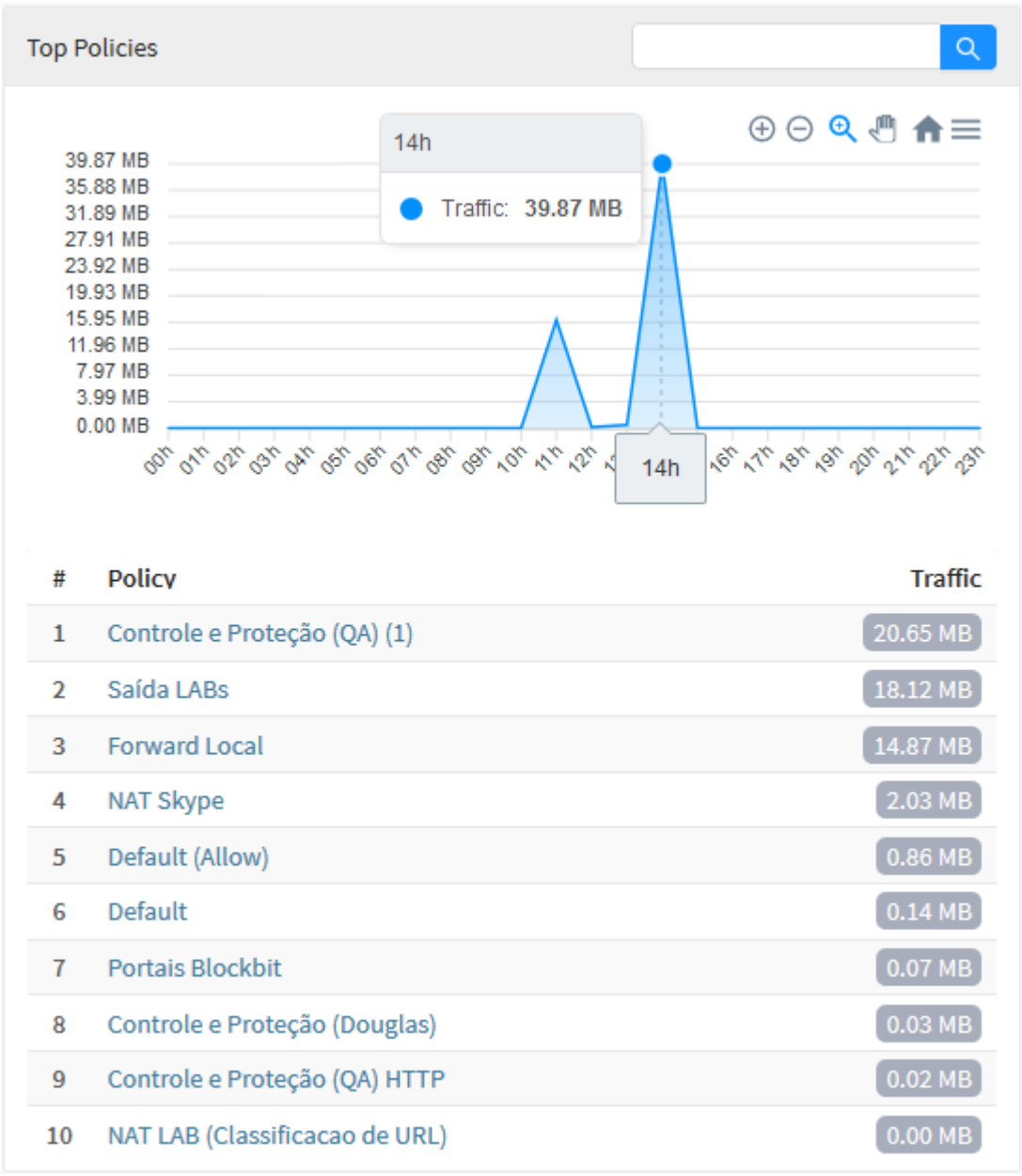


Firewall – Top Source

UTM - Firewall – Top Policies

In “Top Policies” there is a diagram showing by date when there was more network traffic and a list showing the ten most used types of policies, these being classified according to their Gigabytes usage. When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below.

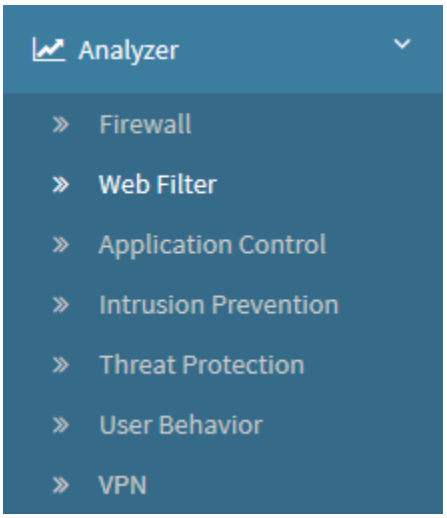
For more information about the navigation menu and the search bar at the top of this graph check this page.



Firewall – Top Policies

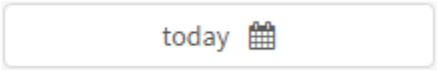
UTM - Web Filter

To access the web filter reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the option “Web Filter”.



Web Filter

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

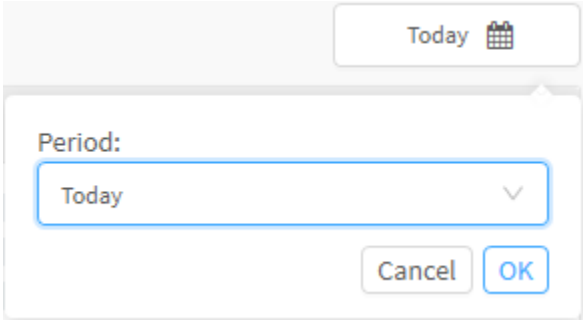


Web Filter - Date check box

Its purpose is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



Web Filter - Date Selection

To close this window, click the **[** Cancel **]** button or, after selecting the desired date, click the **[** OK **]** button:

Web Filter

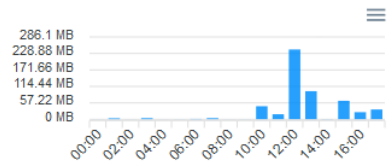
today | Blockbit

Total Traffic
544.35 MB

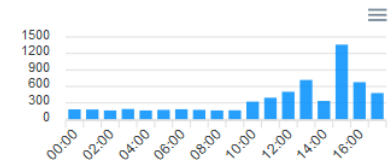
Allowed Sites
6.528

Denied Sites
87

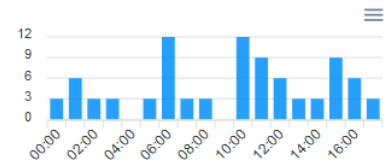
History



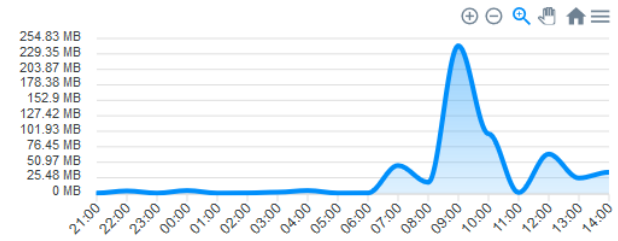
History



History



Users



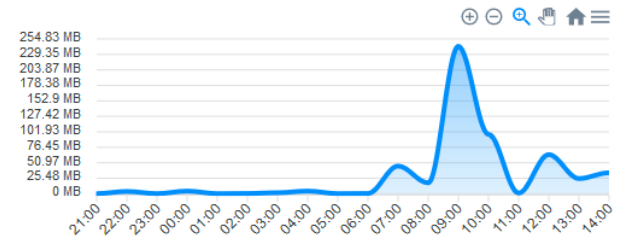
Total Traffic
544.35 MB

Total Hits
6.615

Top Users

#	Name	Hits	Traffic
1	172.32.250.24	84	205.75 MB
2	172.32.250.40	1.353	91.02 MB
3	ccsantos@blockbit.com	262	80.51 MB
4	172.32.250.41	139	43.23 MB
5	172.32.250.8	46	39.52 MB
6	172.32.250.99	166	39.18 MB
7	172.32.250.46	351	18.15 MB
8	172.32.250.1	80	12.29 MB
9	doliveira@blockbit.com	166	3.02 MB
10	172.32.250.49	506	2.74 MB

History Profiles



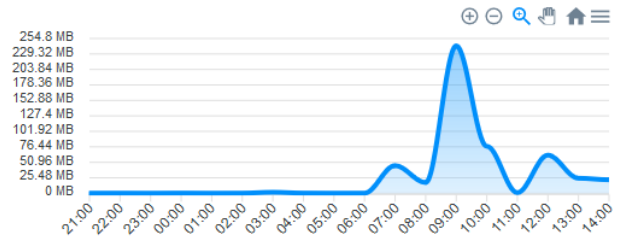
Total Traffic
544.35 MB

Total Hits
6.615

Top Profiles

#	Name	Hits	Traffic
1	Content Filtering (Wifi)	3.847	347.06 MB
2	ByPass SSL (Wifi)	2.681	197.29 MB
3	Block - filestreamingservice	87	0 Bytes

History Categories

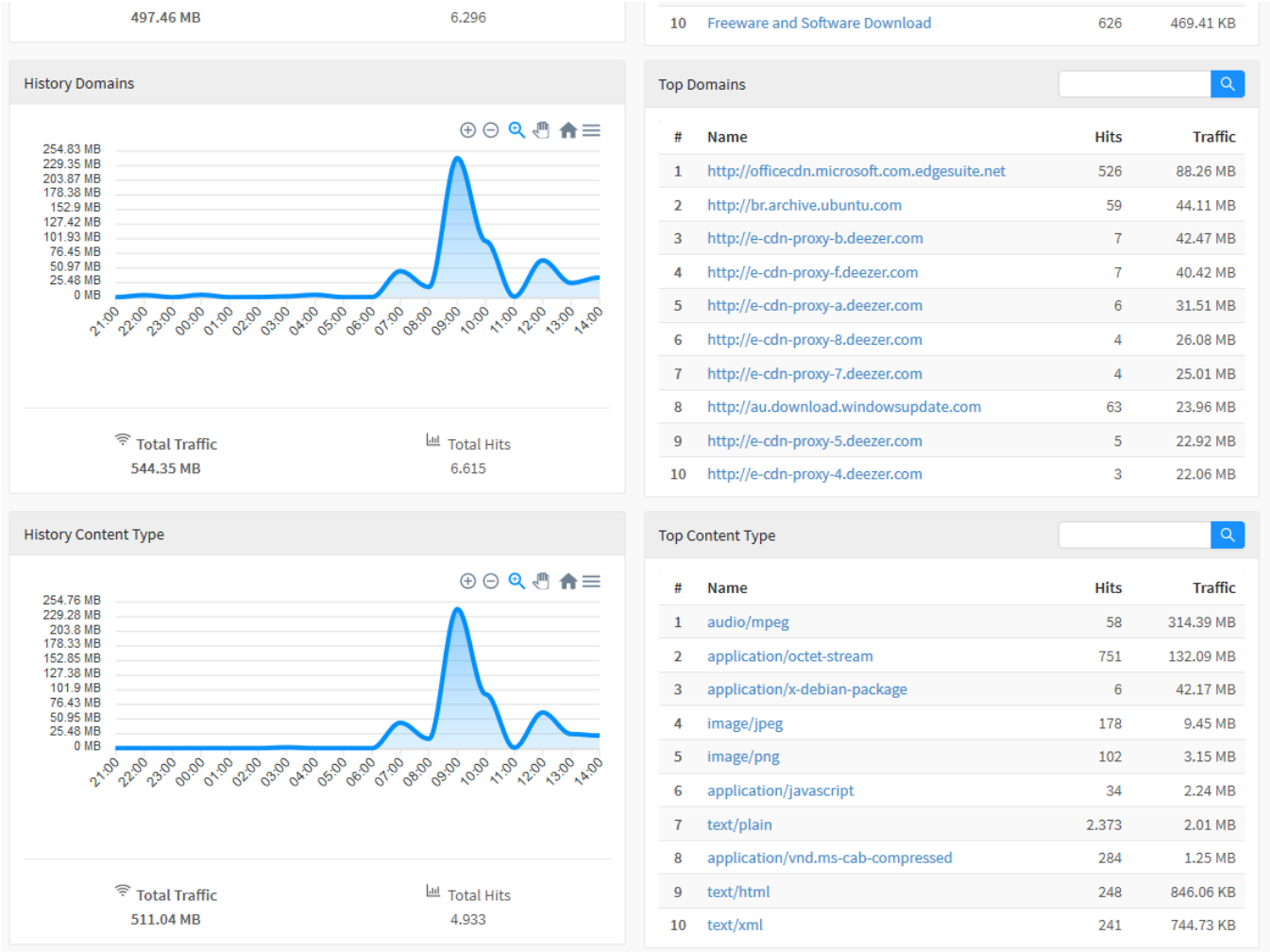


Total Traffic

Total Hits

Top Categories

#	Name	Hits	Traffic
1	Proxy Avoidance	52	276.34 MB
2	Information Technology	4.375	185.8 MB
3	Streaming Media	17	21.13 MB
4	Restaurants and Dining	93	6.86 MB
5	Business and Economy	190	1.93 MB
6	Government	20	1.56 MB
7	Search Engines and Portals	613	1.04 MB
8	News and Media	12	690.69 KB
9	Travel	7	657.2 KB



Analyzer - Web Filter

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom-in;
- **[ ]:** Its function is to zoom-out;
- **[ ]:** It serves to make a zoom selection;
- **[ ]:** Serves to move the graph;
- **[ ]:** Resets the graph to the starting position;
- **[ ]:** Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the search **[ ]** button.

Next, we will analyze in detail the components of “Web Filter”:

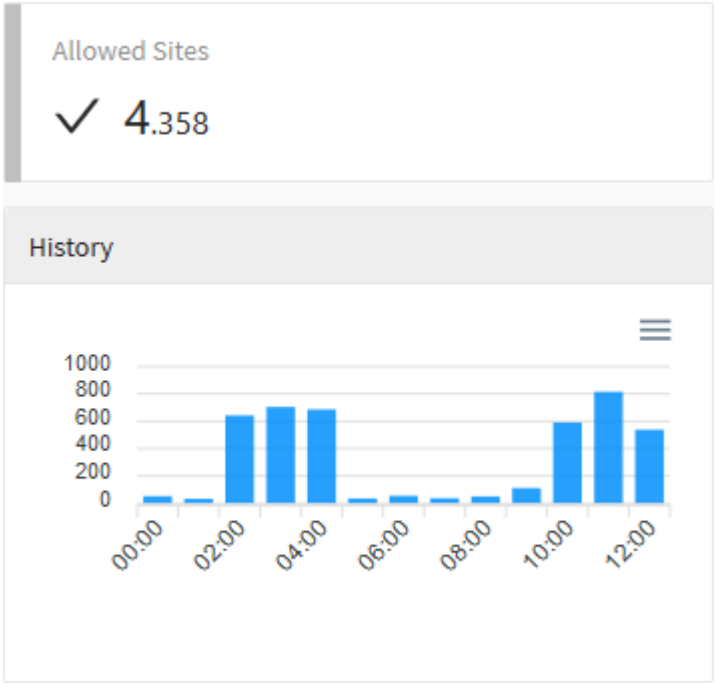
- *Total Traffic* and *History*;
- *Allowed Sites* and *History*;
- *Denied Sites* and *History*;
- *Users - Total Traffic* and *Total Hits*;
- *Top Users*;
- *History Profiles - Total Traffic* and *Total Hits*;
- *Top Profiles*;
- *History Categories - Total Traffic* and *Total Hits*;

- *Top Categories*;
- *History Domains - Total Traffic* and *Total Hits*;
- *Top Domains*;
- *History Content Types - Total Traffic* and *Total Hits*;
- *Top Content Type*.
- Top Domain By Time.

UTM - Web Filter - Allowed Sites and History

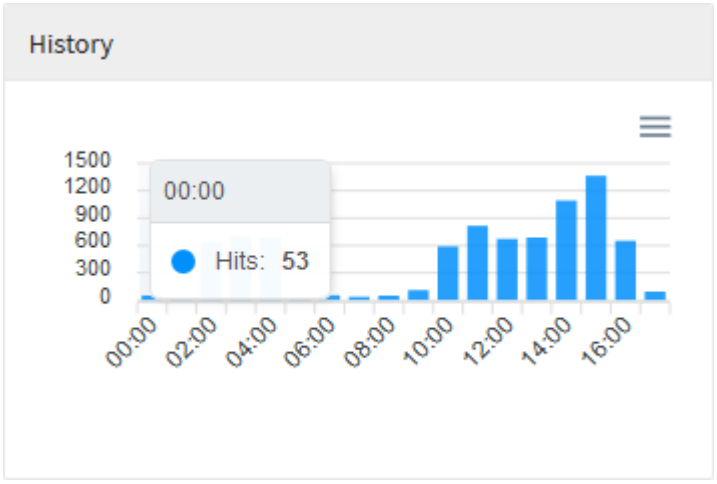
The "Allowed Sites" panel displays a total of pages that have been authorized following the policies. Just below, the history is shown in a bar graph showing the amount of accesses per day.

For more information about the navigation menu at the top of this graph, check this page.



Web Filter – Allowed Sites

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

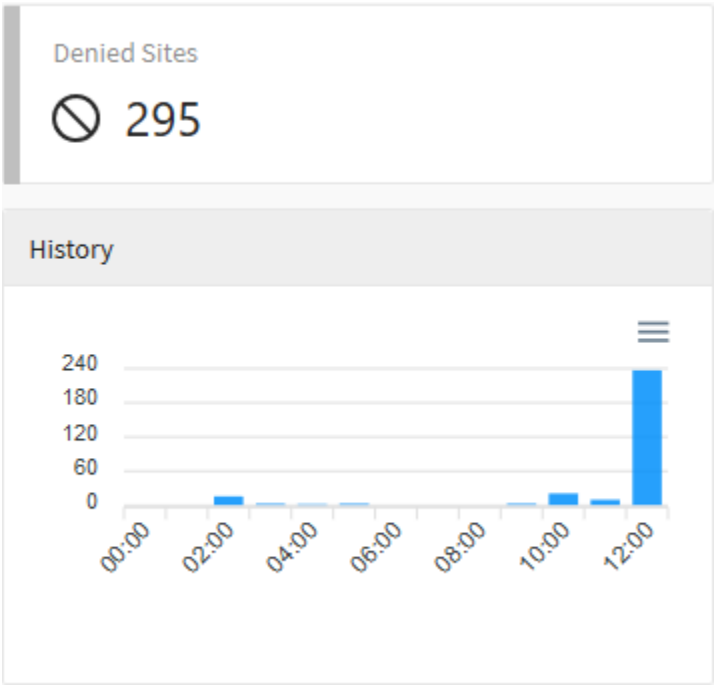


Web Filter – Allowed Sites - Period Summary

UTM - Web Filter - Denied Sites and History

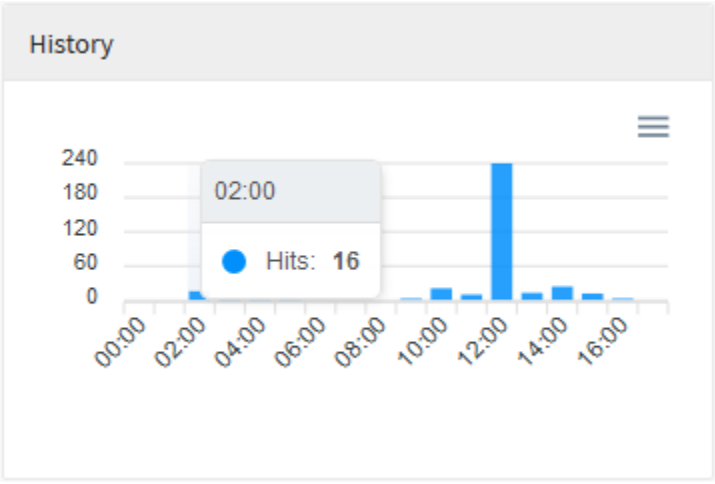
The “Denied Sites” panel shows a sum of all pages that, according to the policies, were denied access. Below, the history is shown in a bar graph showing the amount of accesses per day.

For more information about the navigation menu at the top of this graph, check this page.



Web Filter – Denied Sites

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

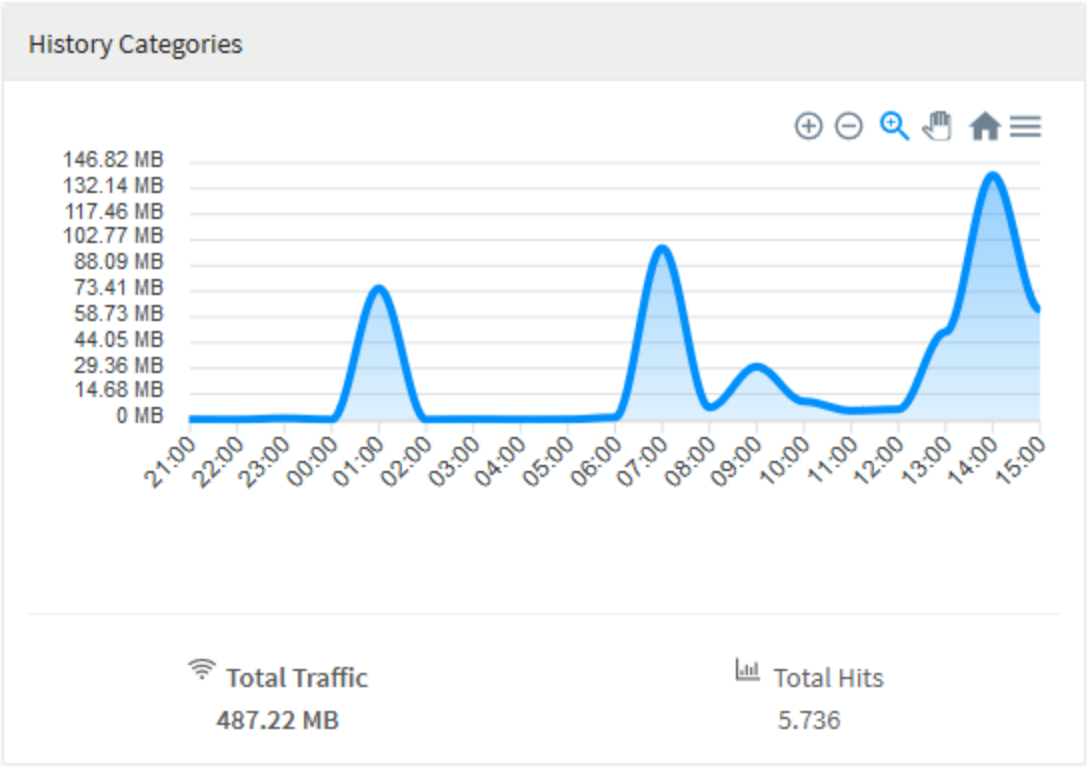


Web Filter – Denied Sites - Period Summary

UTM - Web Filter - History Categories - Total Traffic and Total Hits

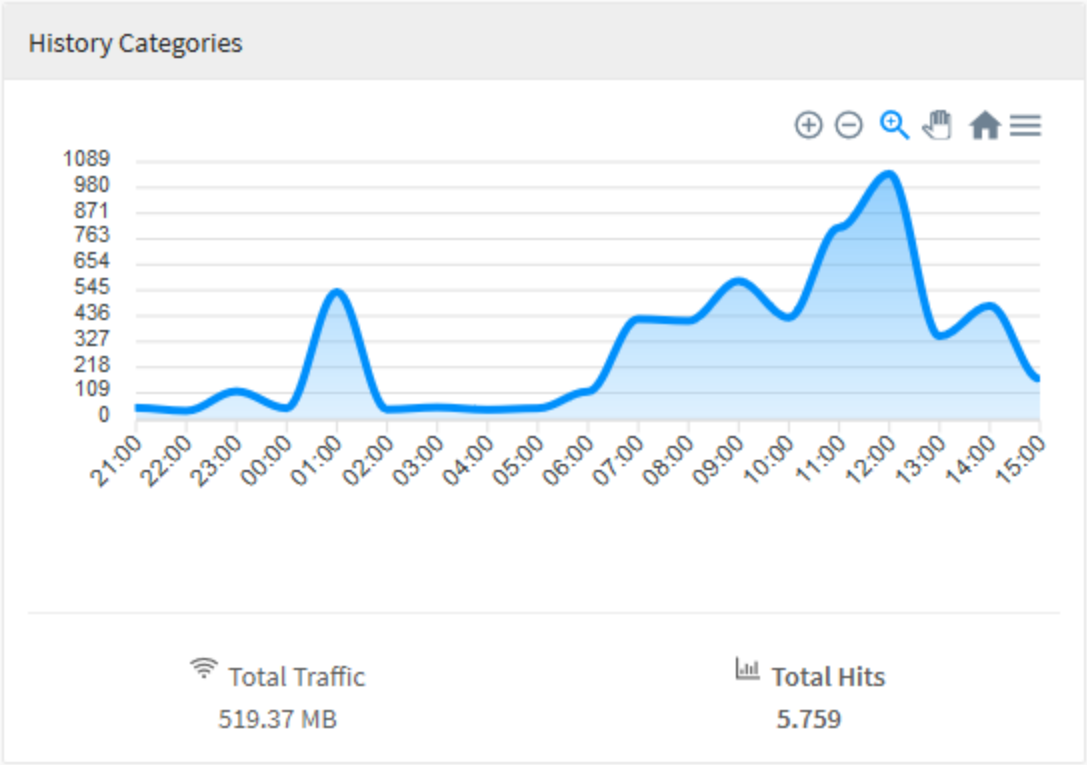
In “History Categories”, we have a graph that displays information specifically related to network categories, its function is to demonstrate when some category was applied in one of the accesses. In this area we have “Total Traffic” where the total network traffic is displayed in Gigabytes per day and “Total Hits” which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this page.



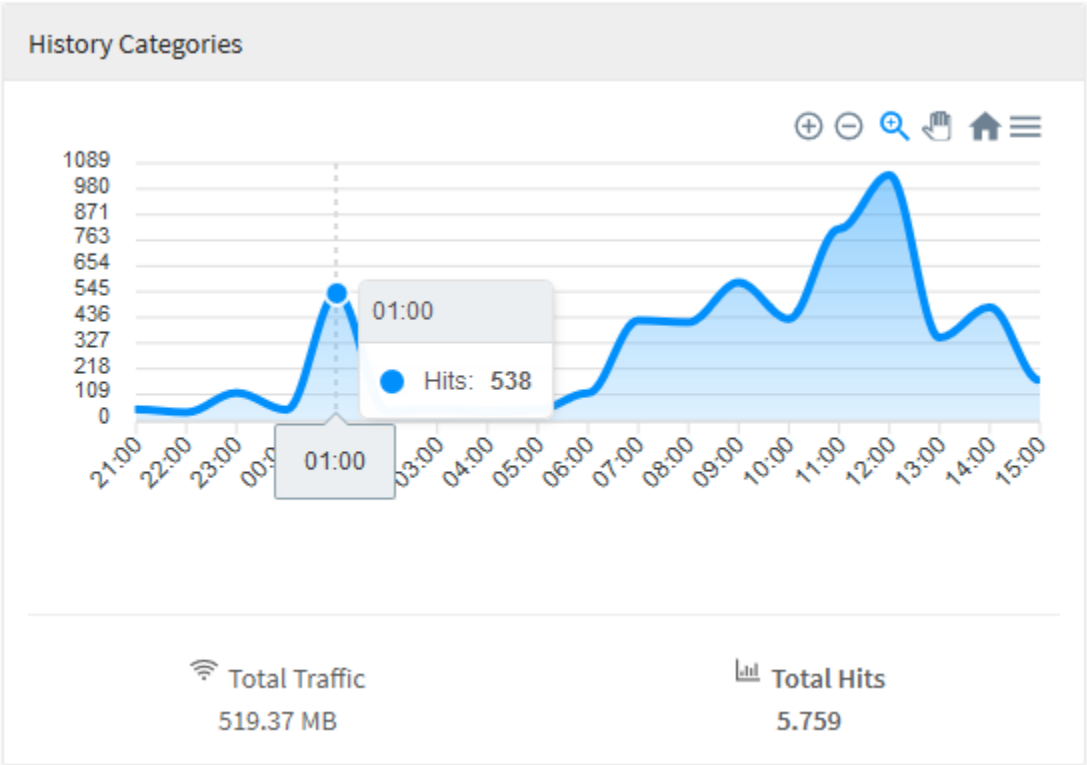
Web Filter – History Categories – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Categories – Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

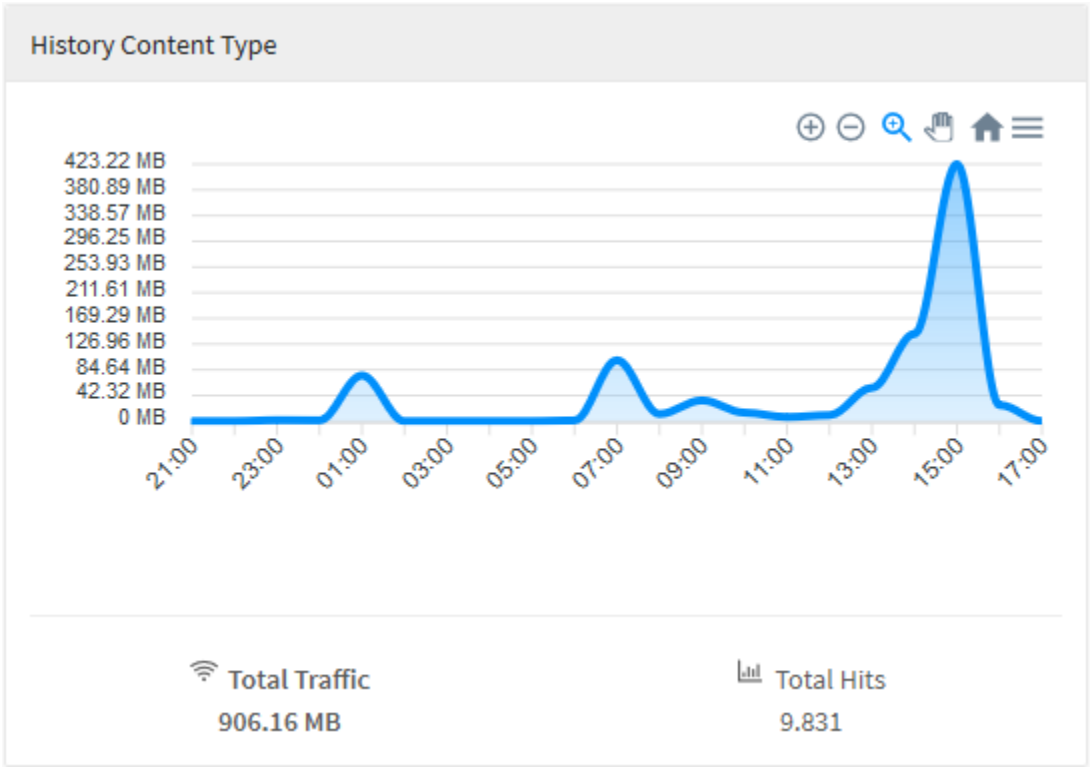


Web Filter – History Categories – Period summary

UTM - Web Filter - History Content Types - Total Traffic and Total Hits

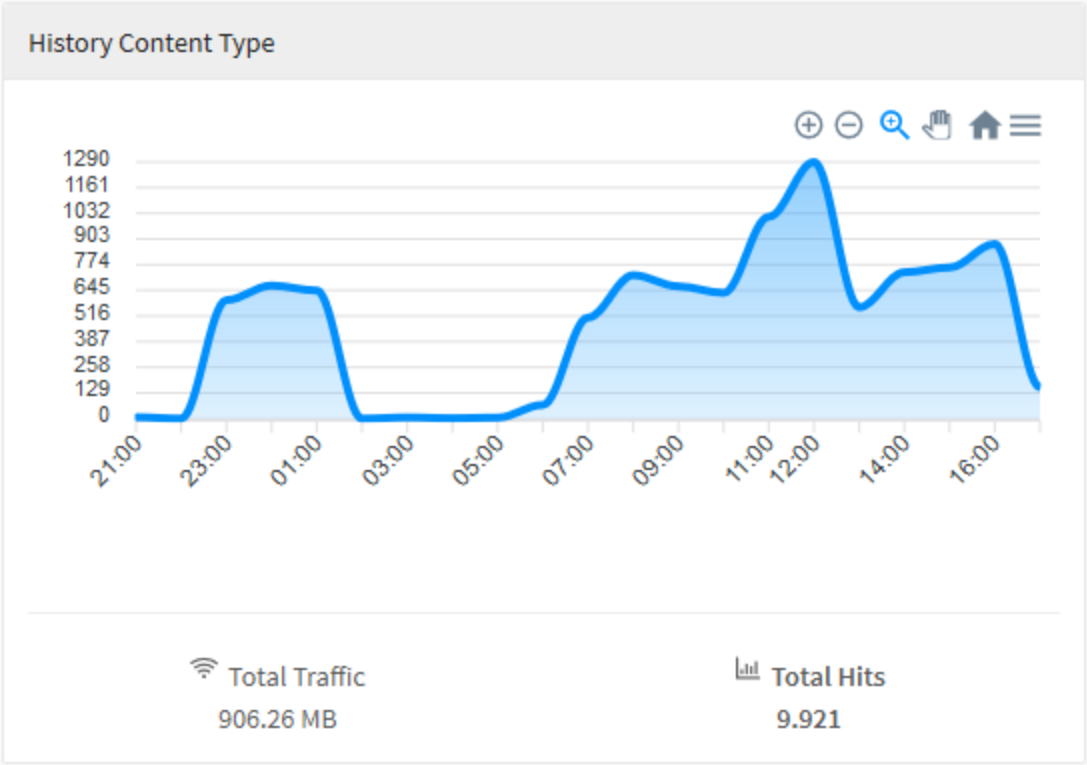
In “Content Type”, we have a graphic whose function is to demonstrate when some type of content has been accessed. In this area we have “Total Traffic” where the total network traffic is displayed in Gigabytes per day and “Total Hits” which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this page.



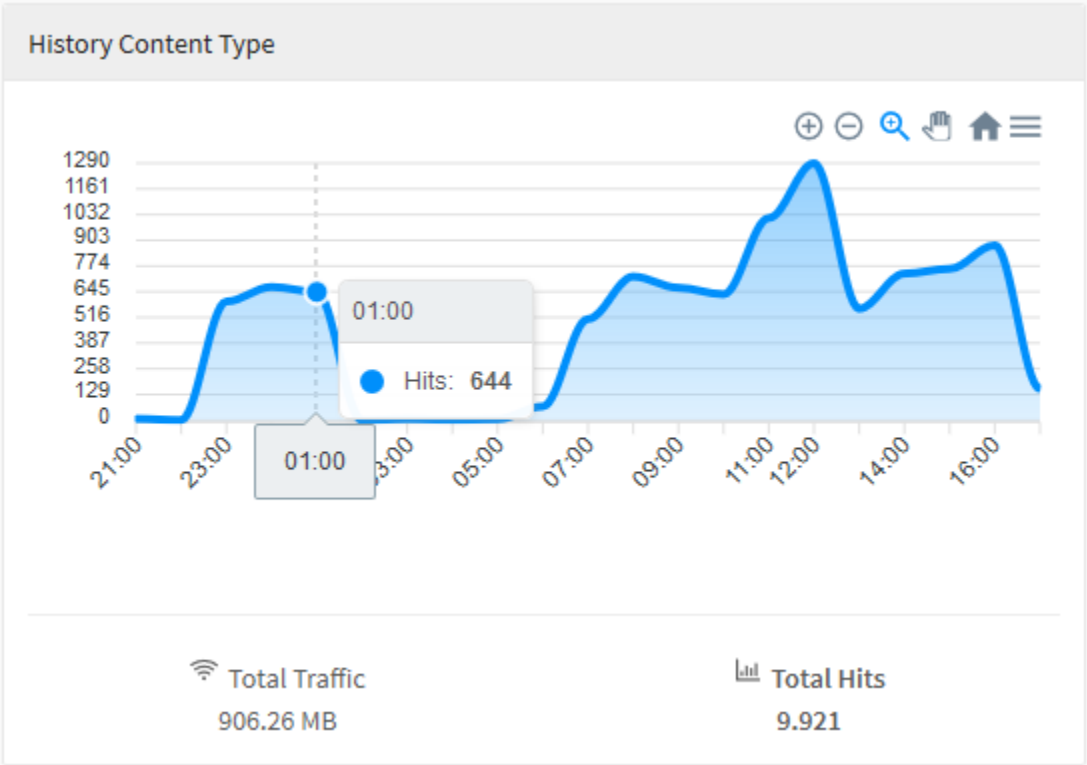
Web Filter – History Content Type – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Content Type – Total Hits

When you mouse over the graph, a summary of the period is displayed, as shown in the image below:

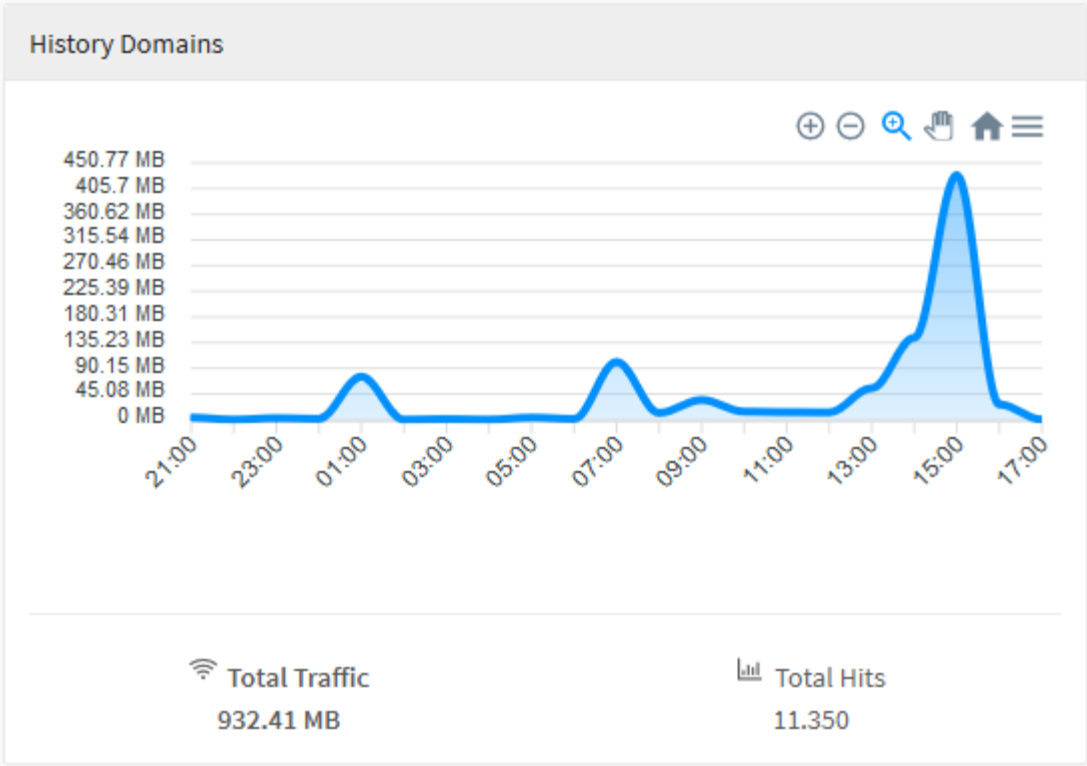


Web Filter – History Content Type - Period Summary

UTM - Web Filter - History Domains - Total Traffic and Total Hits

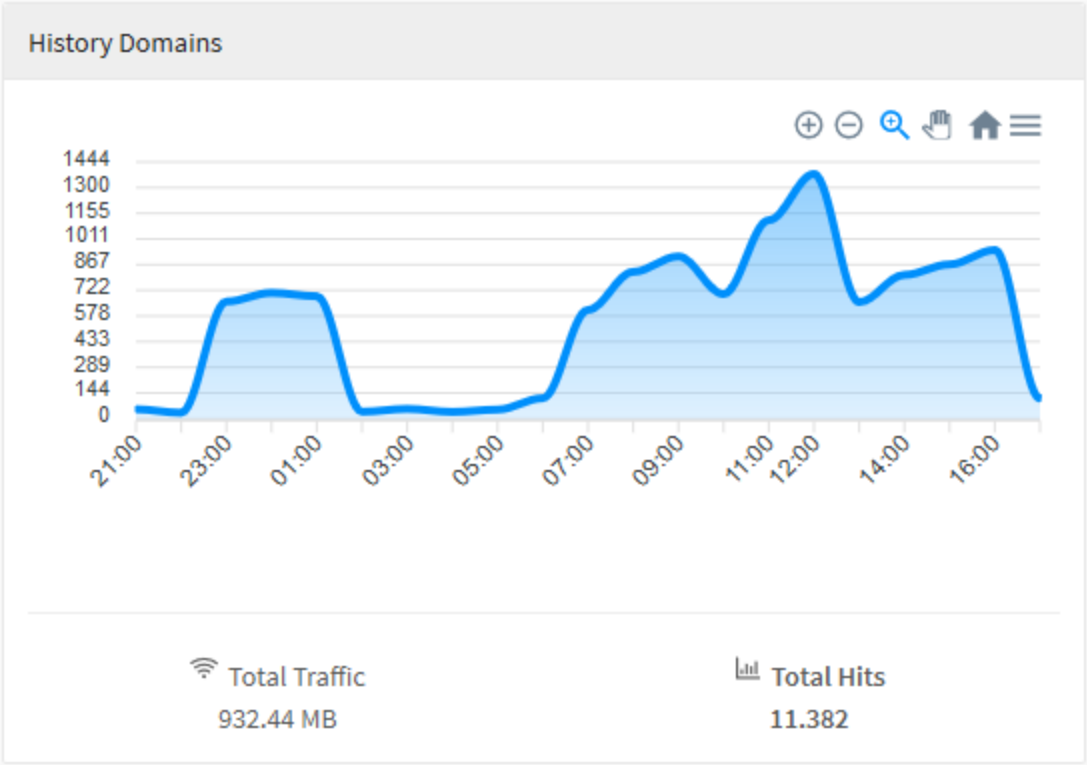
In “History Domains”, we have a graph that displays information specifically related to domain access, its function is to demonstrate when a domain has been accessed. In this area we have “Total Traffic” where the total traffic in Gigabytes per day and “Total Hits” is displayed, which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this page.



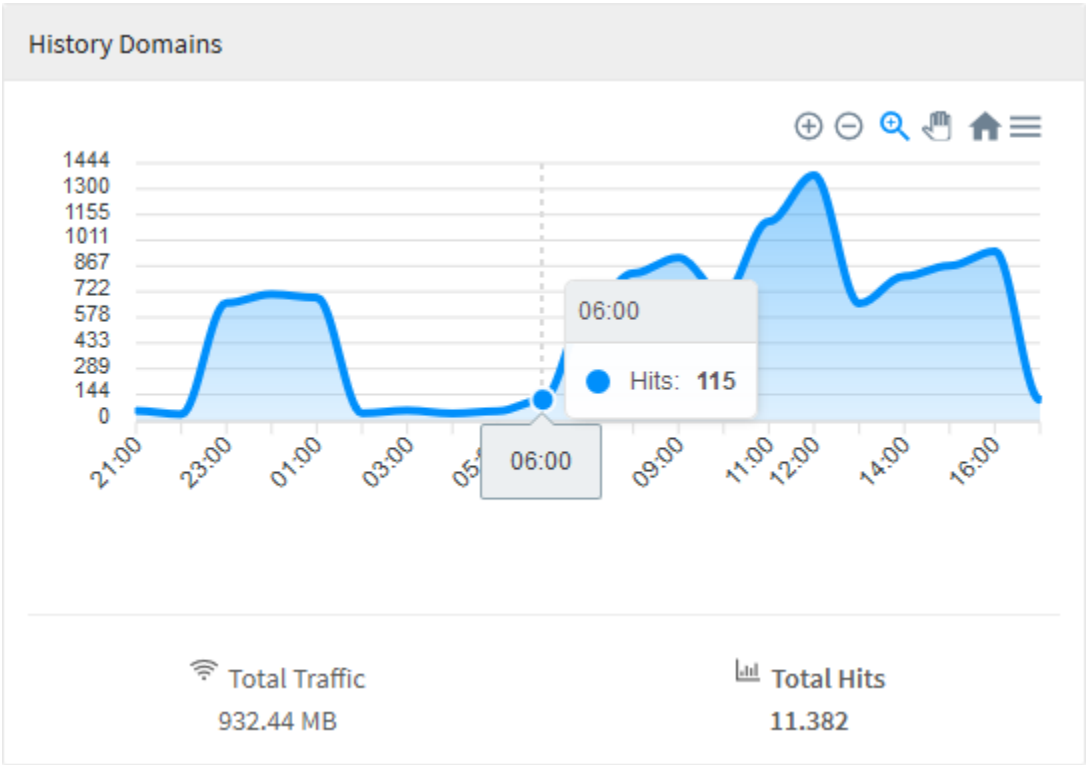
Web Filter - History Domains - Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter - History Domains - Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

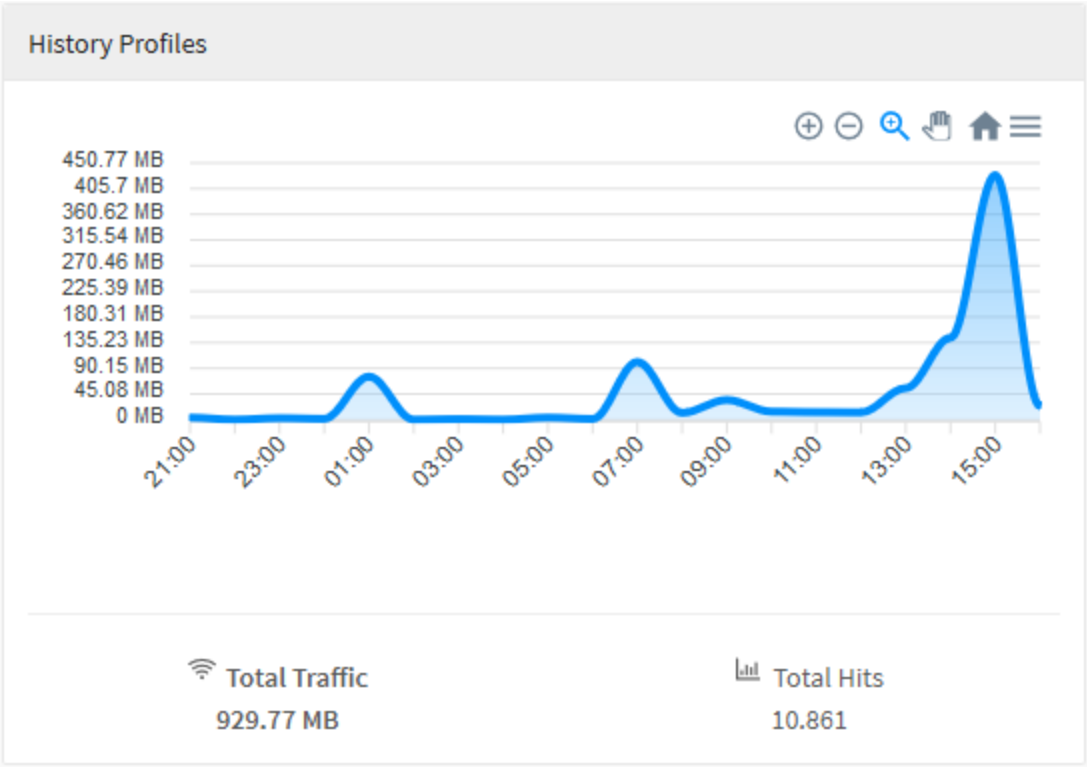


Web Filter - History Domains - Period Summary

UTM - Web Filter - History Profiles - Total Traffic and Total Hits

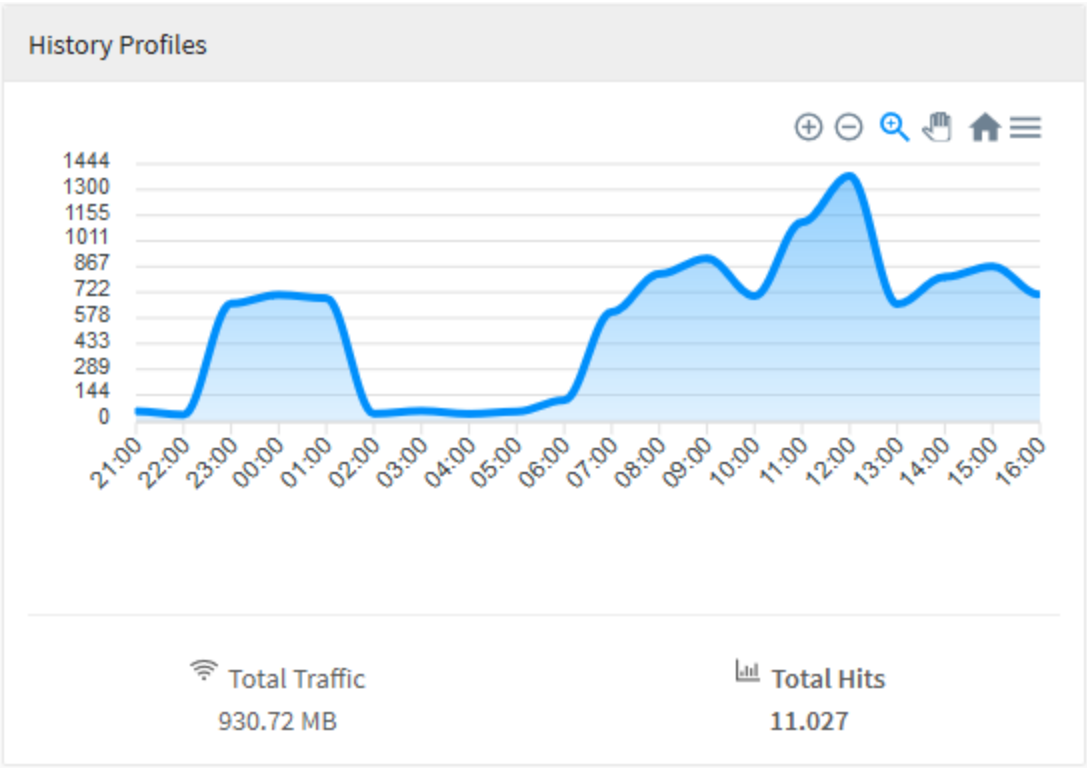
In “History Profiles”, we have a graph that displays information specifically related to the profiles of the network, its function is to demonstrate when some profile was used in an access. In this area we have “Total Traffic” where the total network traffic is displayed in Gigabytes per day and “Total Hits” which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this page.



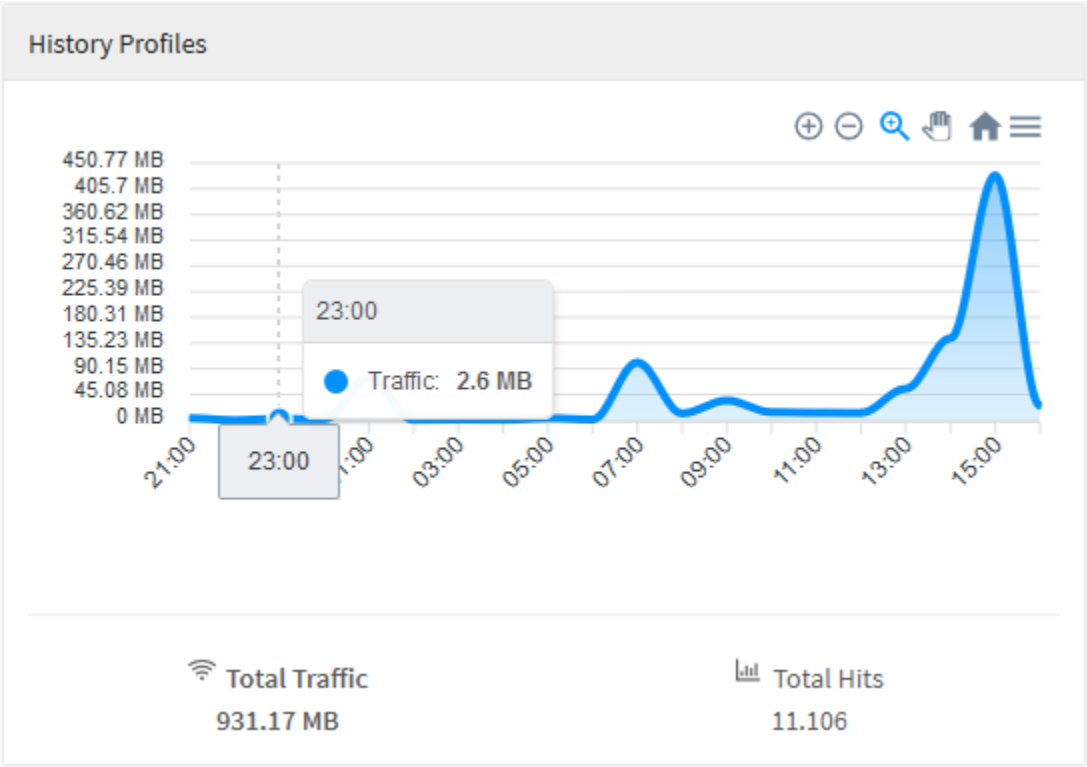
Web Filter – History Profiles – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Profiles – Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

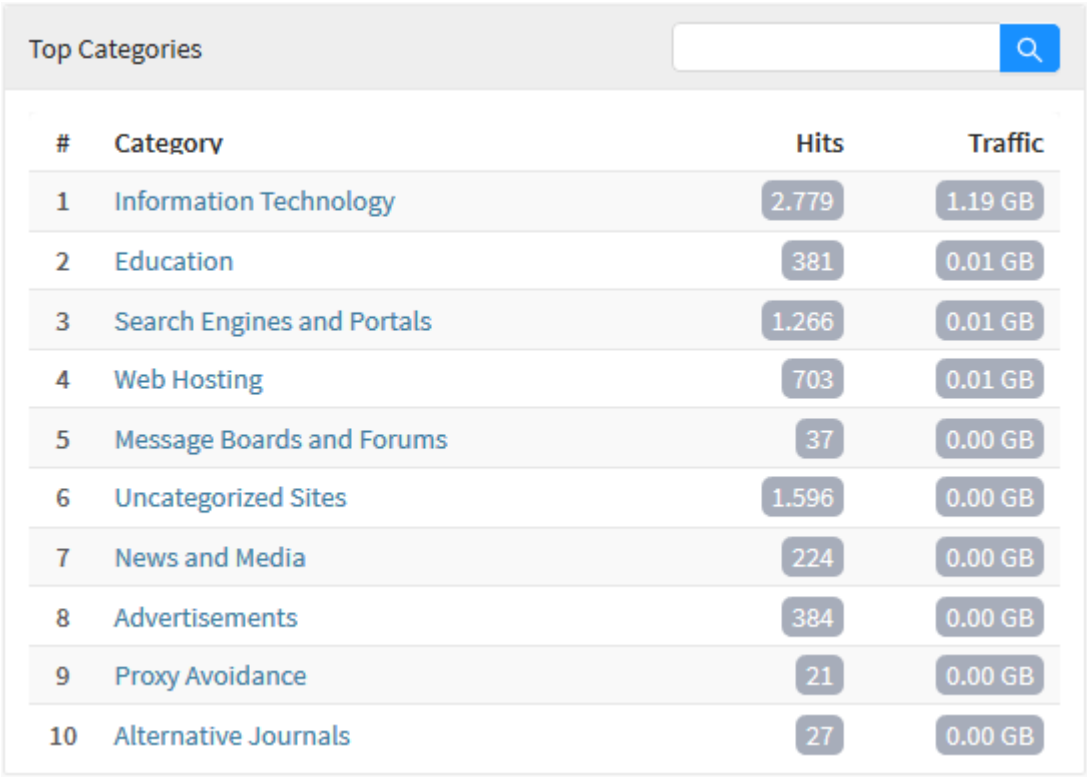


Web Filter – History Profiles – Period Summary

UTM - Web Filter - Top Categories

In the “Top Categories” list, we have a list of the names of the ten categories classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected category.

For more information about the search bar at the top of this graph check this page.



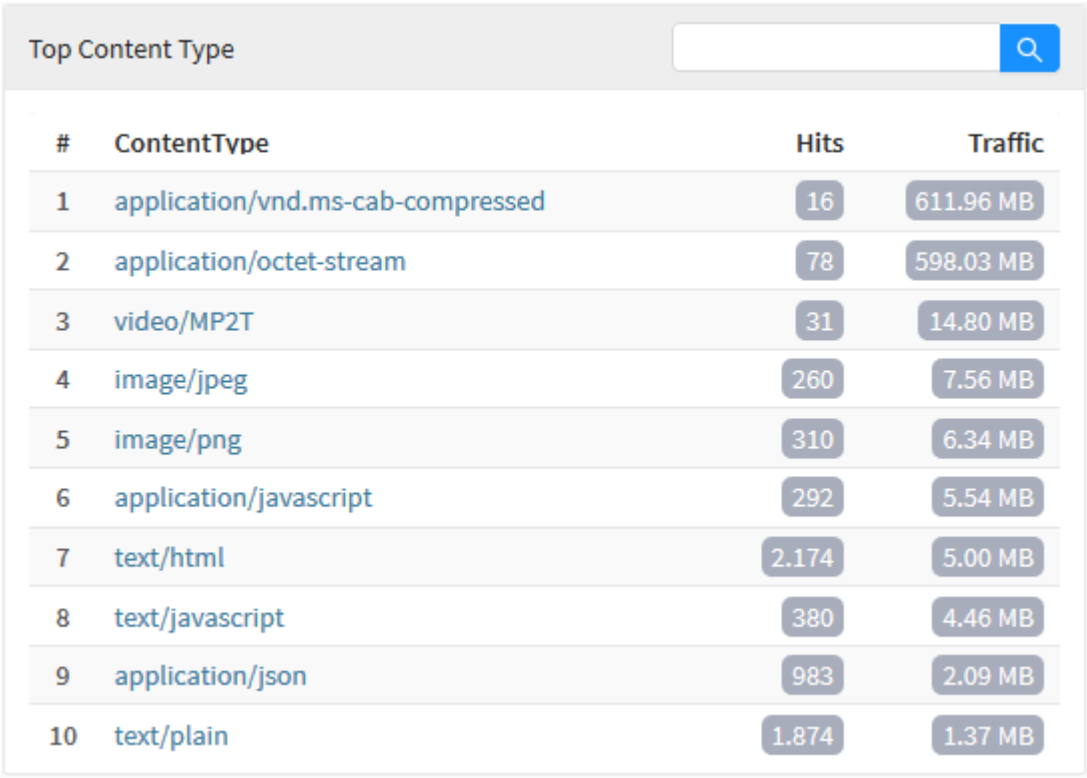
#	Category	Hits	Traffic
1	Information Technology	2.779	1.19 GB
2	Education	381	0.01 GB
3	Search Engines and Portals	1.266	0.01 GB
4	Web Hosting	703	0.01 GB
5	Message Boards and Forums	37	0.00 GB
6	Uncategorized Sites	1.596	0.00 GB
7	News and Media	224	0.00 GB
8	Advertisements	384	0.00 GB
9	Proxy Avoidance	21	0.00 GB
10	Alternative Journals	27	0.00 GB

Web Filter – Top Categories

UTM - Web Filter - Top Content Type

In the “Top Content Type” list, we have a list of the names of the ten most accessed content types classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view regarding these types of content.

For more information about the navigation menu at the top of this graph, check this page.



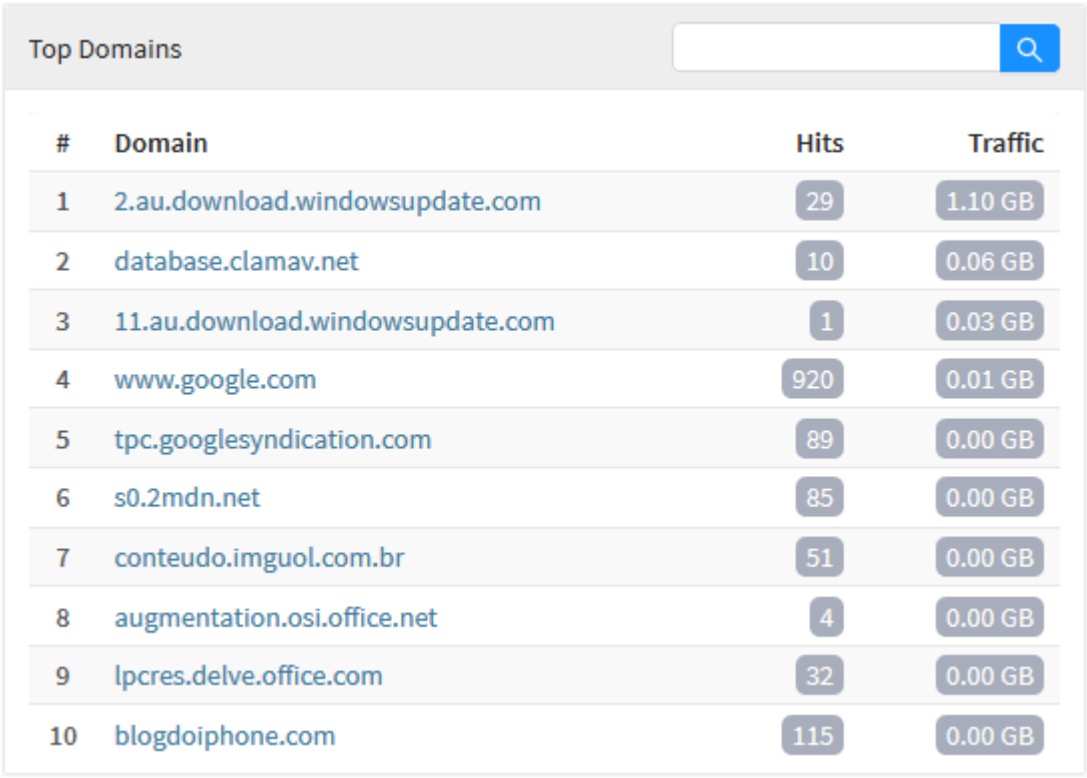
#	ContentType	Hits	Traffic
1	application/vnd.ms-cab-compressed	16	611.96 MB
2	application/octet-stream	78	598.03 MB
3	video/MP2T	31	14.80 MB
4	image/jpeg	260	7.56 MB
5	image/png	310	6.34 MB
6	application/javascript	292	5.54 MB
7	text/html	2.174	5.00 MB
8	text/javascript	380	4.46 MB
9	application/json	983	2.09 MB
10	text/plain	1.874	1.37 MB

Top Content Type

UTM - Web Filter - Top Domains

In the “Top Domains” list, we have a list of the names of the ten domains classified in order of the highest amount of accesses and their respective traffic in Megabytes. Finally, when you click on one of these addresses, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected domain.

For more information about the search bar at the top of this graph check this page.



#	Domain	Hits	Traffic
1	2.au.download.windowsupdate.com	29	1.10 GB
2	database.clamav.net	10	0.06 GB
3	11.au.download.windowsupdate.com	1	0.03 GB
4	www.google.com	920	0.01 GB
5	tpc.googlesyndication.com	89	0.00 GB
6	s0.2mdn.net	85	0.00 GB
7	conteudo.imguol.com.br	51	0.00 GB
8	augmentation.osi.office.net	4	0.00 GB
9	lpcres.delve.office.com	32	0.00 GB
10	blogdoiphone.com	115	0.00 GB

Web Filter – Top Domains

UTM - Web Filter - Top Domains by Time

In the “*Top Domains by Time*”, list, one sees the top ten accessed domains, classified by order of the highest amount of traffic time in a domain.

Top Domains by time

#	Domain	Time
1	https://edge.microsoft.com	58s
2	https://umwatson.events.data.microsoft.com	36s
3	https://www.bing.com	18s
4	http://ctldl.windowsupdate.com	14s
5	http://x1.c.lencr.org	10s
6	https://login.live.com	8s
7	https://slscr.update.microsoft.com	8s
8	https://msedge.api.cdp.microsoft.com	6s
9	https://config.edge.skype.com	5s
10	https://update.googleapis.com	4s

Top Domains by Time

Finally, when clicking in one of these domains ou IPs, one will be redirected to Events using the selected item as a filter, thus creating, a better detailed report enabling a precise view on these contents.

Events

Sessions | Authentication | VPN

web_site:"%https://safebrowsing.googleapis.com%" logtype:"webfilter" date:"today" Query Editor

Date	User	Source	Destination	Device	Service	Log type	Action
2023-01-30 11:10:03	-	192.168.165.102:62...	142.251.129.106:443	eth1 - default	https	webfilter	allow
2023-01-30 11:10:03	-	192.168.165.102:62...	142.251.129.106:443	eth1 - default	https	webfilter	allow
2023-01-30 11:07:24	-	192.168.165.102:61...	142.251.129.106:443	eth1 - default	https	webfilter	allow
2023-01-30 11:07:24	-	192.168.165.102:61...	142.251.129.106:443	eth1 - default	https	webfilter	allow
2023-01-30 10:37:13	-	192.168.165.102:60...	142.251.129.42:443	eth1 - default	https	webfilter	allow
2023-01-30 10:37:13	-	192.168.165.102:60...	142.251.129.42:443	eth1 - default	https	webfilter	allow
2023-01-30 10:07:42	-	192.168.165.102:60...	142.250.218.74:443	eth1 - default	https	webfilter	allow
2023-01-30 10:07:42	-	192.168.165.102:60...	142.250.218.74:443	eth1 - default	https	webfilter	allow
2023-01-30 09:37:23	-	192.168.165.102:60...	216.58.222.10:443	eth1 - default	https	webfilter	allow

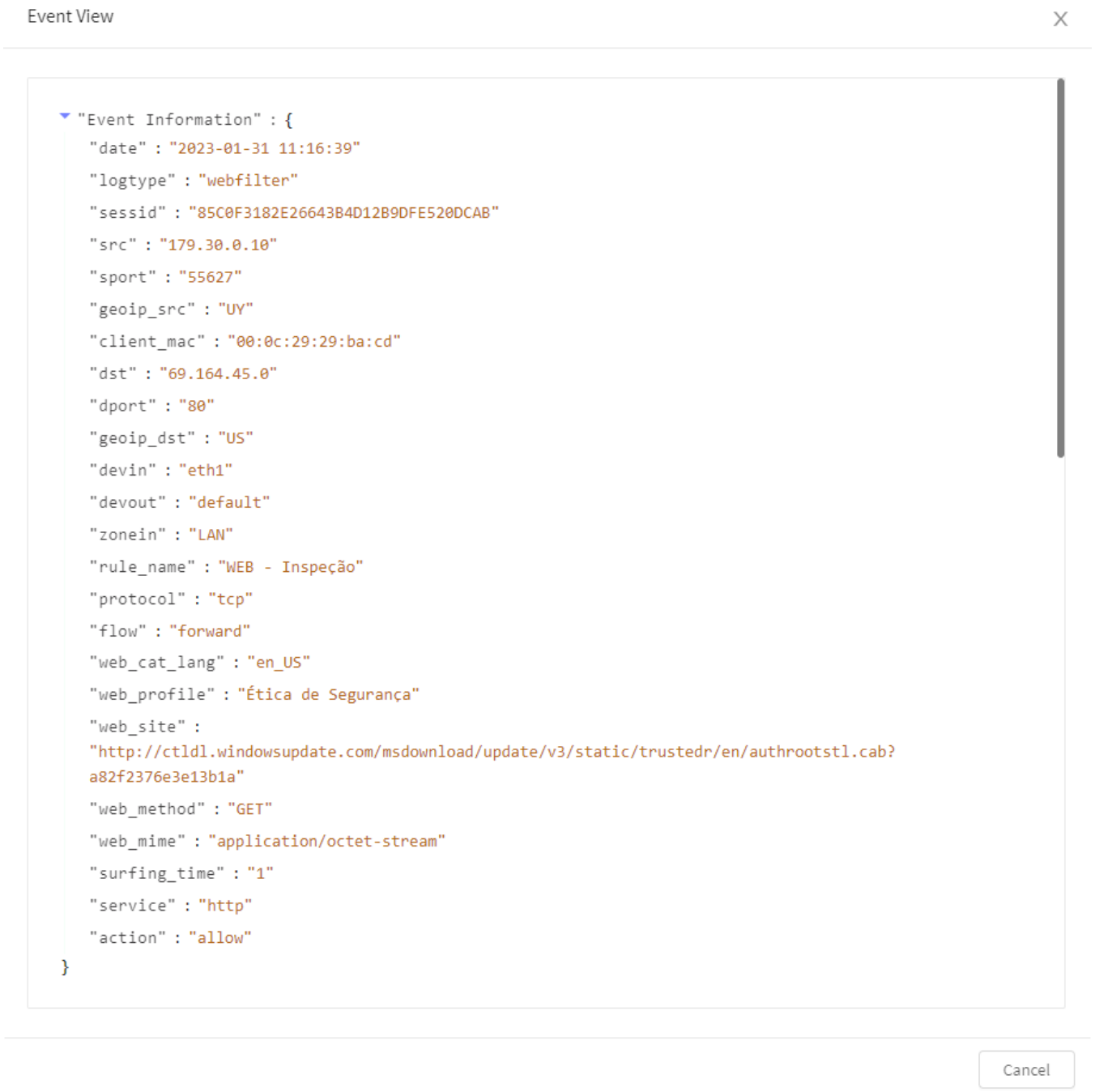
Events - Sessions

Clicking on [or] is possible to verify detailed information in the selected item. Search for *"surfing time"* information to verify the browsing time.

Information

date 2023-01-31 11:16:39	geoip_src UY	devin eth1	flow forward	surfing_time 1
logtype webfilter	client_mac 00:0c:29:29:ba:cd	devout default	web_profile Ética de Segurança	service http
sessid 85C0F3182E26643B4D12B9DFE520DCAB	dst 69.164.45.0	zonein LAN	web_site http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?a82f2376e3e13...	action allow
src 179.30.0.10	dport 80	rule_name WEB - Inspeção	web_method GET	
sport 55627	geoip_dst US	protocol tcp	web_mime application/octet-stream	

Events - Sessions - [ ] Information



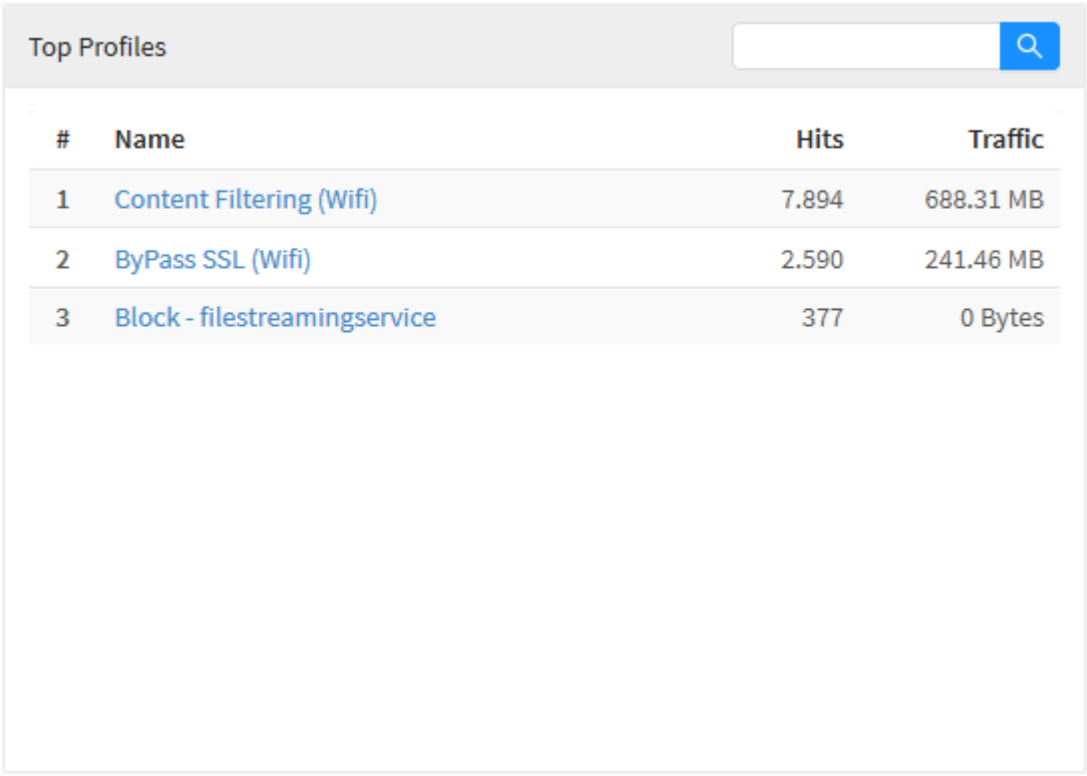
Events - Sessions - [ ] Event View

For additional information about the Analyzer Menu, check this page.

UTM - Web Filter - Top Profiles

In the “Top Profiles” list, we have a list of the ten most used profiles classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when you click on one of these profiles, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected profile.

For more information about the search bar at the top of this graph check this page.



Web Filter – Top Profiles

UTM - Web Filter - Top Users

As with the other “Top Users” lists, in Web Filter we have a list of ten users classified by order of the largest amount of accesses and their respective use in Gigabytes. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

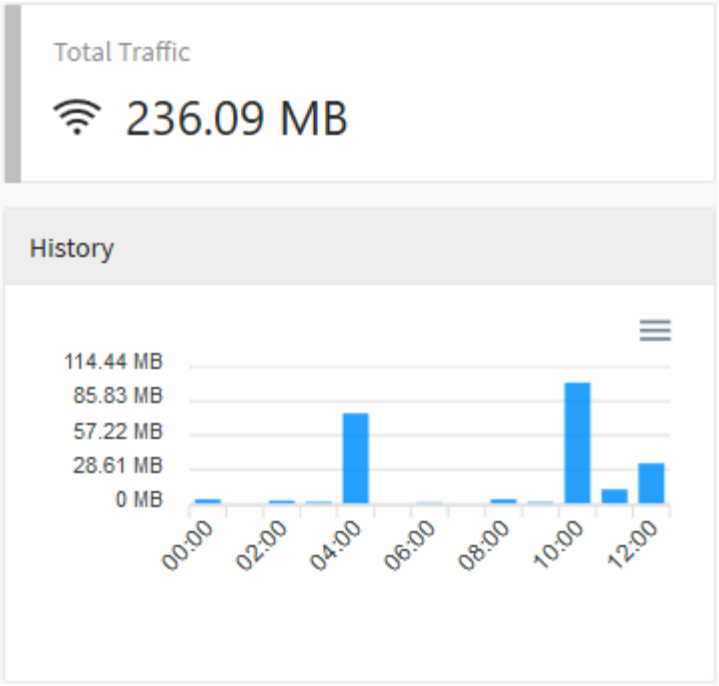
For more information about the search bar at the top of this graph check this page.

#	Name	Hits	Traffic
1	172.32.250.40	762	131.6 MB
2	172.32.250.99	285	98.94 MB
3	doliveira@blockbit.com	1.696	21.28 MB
4	pisantos@blockbit.com	243	20.21 MB
5	172.32.250.46	405	18.68 MB
6	172.32.250.5	553	7.5 MB
7	172.32.250.49	1.461	7.26 MB
8	dsousa@blockbit.com	310	5.43 MB
9	172.32.250.53	67	4.83 MB
10	172.32.250.47	181	4.66 MB

Web Filter – Top Users

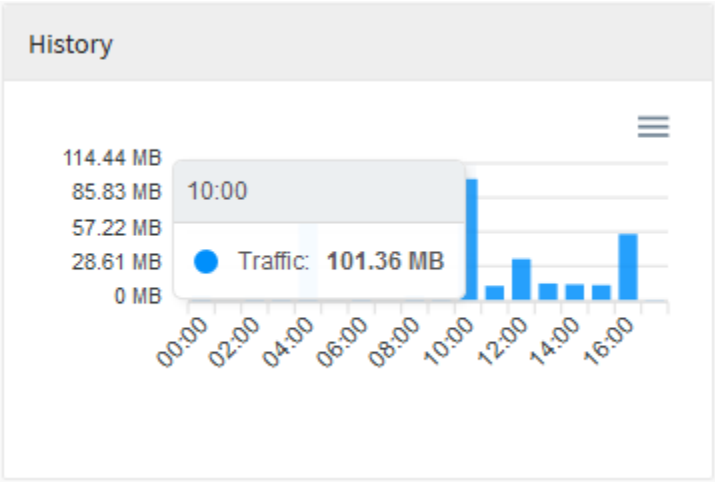
UTM - Web Filter - Total Traffic and History

The “Total Traffic” panel shows the total amount of traffic in Megabytes. Just below, the history is displayed in a bar graph showing the amount of Megabytes trafficked per day.



Web Filter – Total Traffic

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

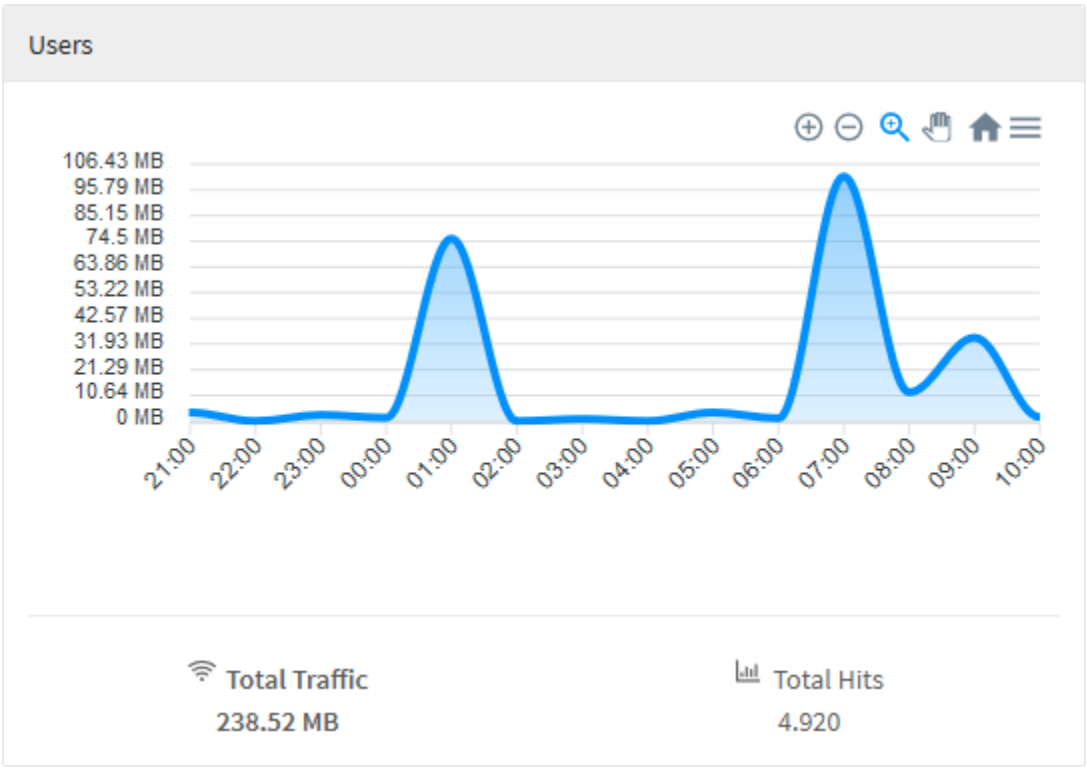


Web Filter – Total Traffic - Period summary

UTM - Web Filter - Users - Total Traffic and Total Hits

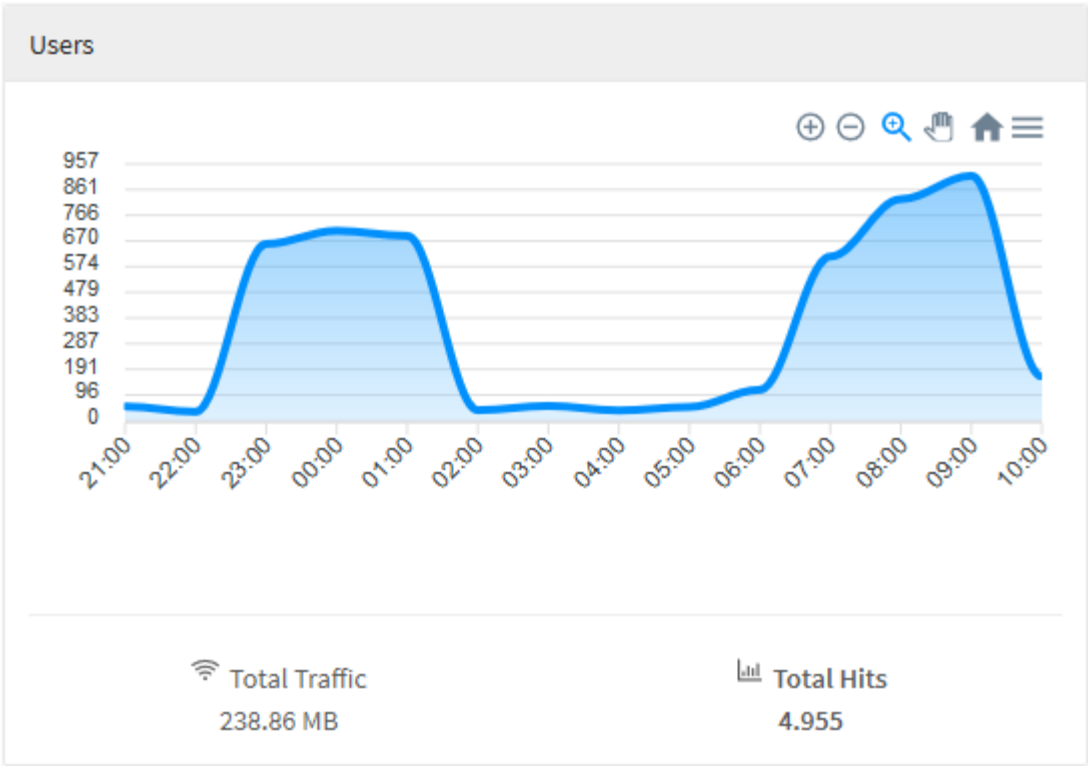
Just below the panels previously described, on the left side of the screen we have the graphic arranged in "Users", which displays information specifically related to the network consumption by users: In it we have "Total Traffic" where the total network traffic is displayed in Megabytes per day and “Total Hits” which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this page.



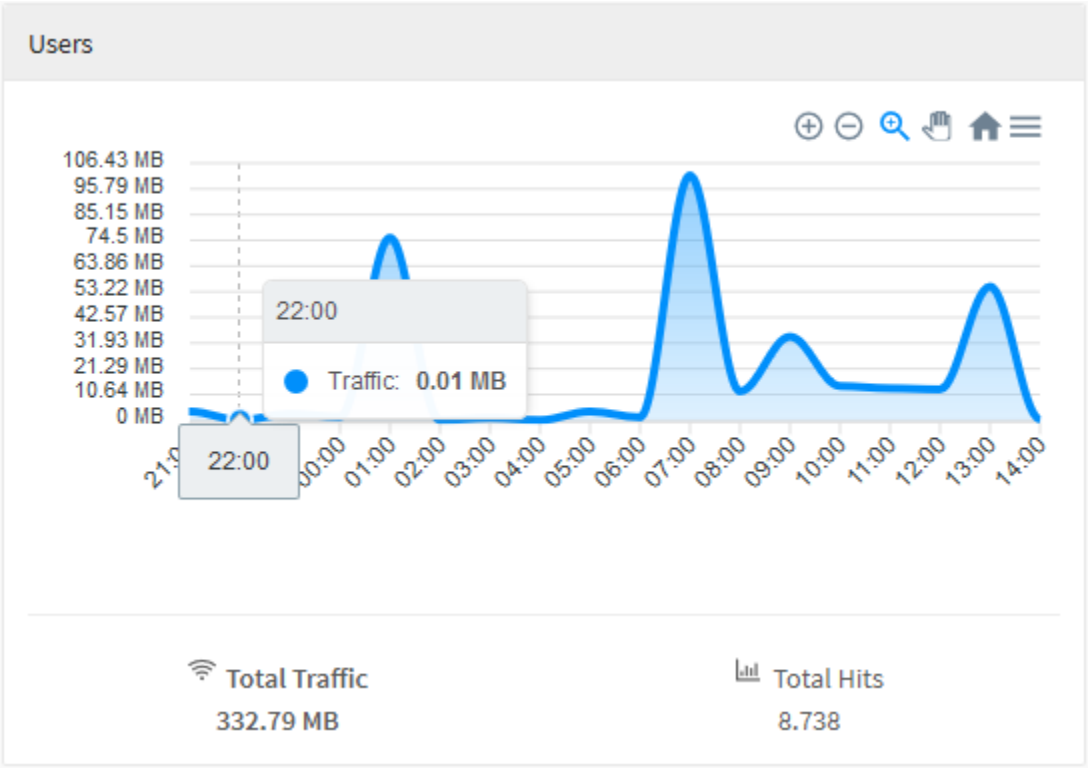
Web Filter – Users – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – Traffic – Total Hits

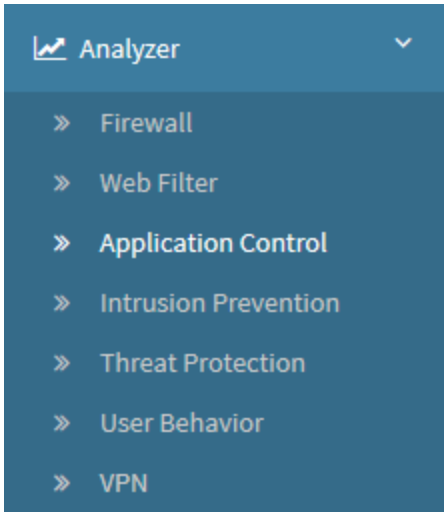
When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



Web Filter – Users – Total Traffic - Period Summary

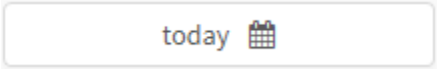
UTM - Application Control

To access the Application Control reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “Application Control” option.



Application Control

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

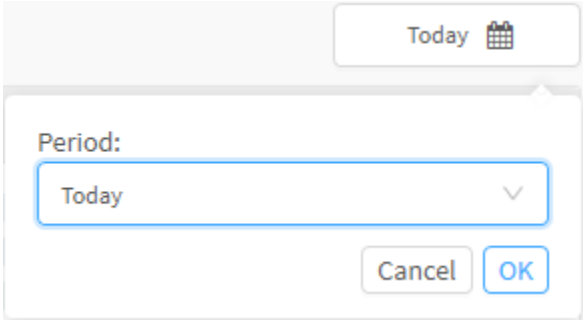


Application Control - Date check box

Its purpose is basically to allow even more accurate filtering of results, the possible options are:

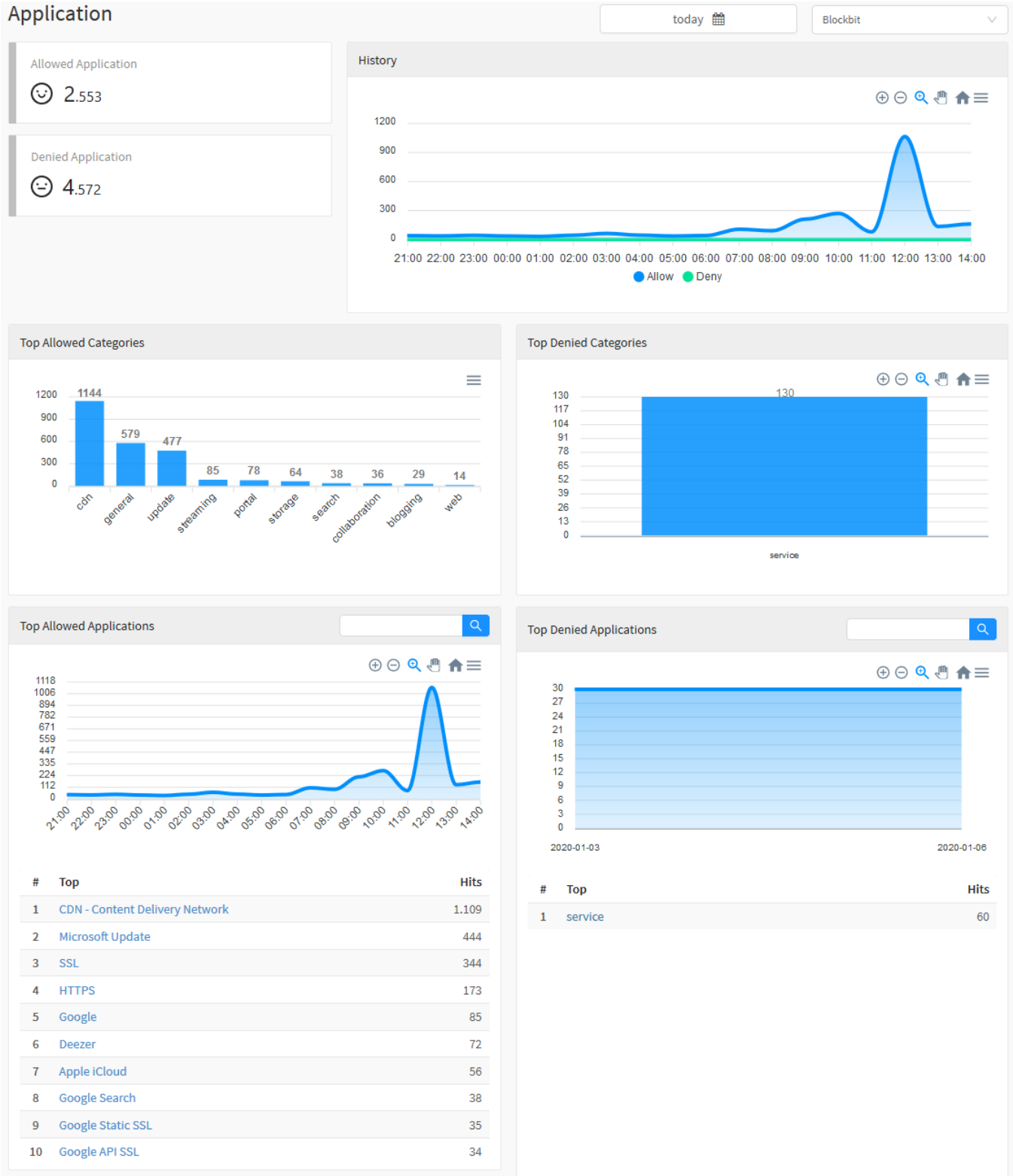
- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



To close this window, click **[** Cancel **]** button or, after selecting the desired date, click **[** OK **]** button;

The screen below will appear:



Analyzer - Application Control

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom;
- **[ ]:** Its function is to remove the zoom;

- []: It serves to make a selection zoom;
- []: Serves to move the graph;
- []: Reset the graph to the starting position;
- []: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

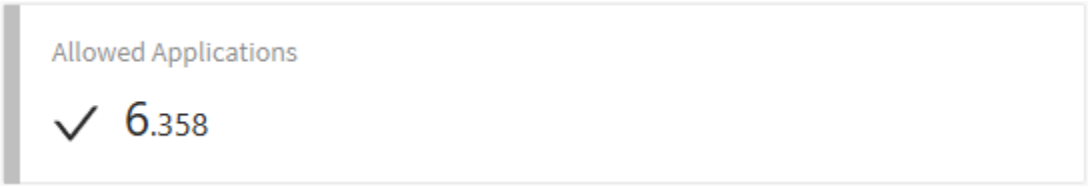
To perform a search, type a term in the search bar and click the search [] button.

Next, we will analyze in detail the components of “Application Control”:

- *Allowed Application*;
- *Denied Application*;
- *History*;
- *Top Allowed Categories*;
- *Top Denied Categories*;
- *Top Allowed Applications*;
- *Top Denied Applications*.

UTM - Application Control - Allowed Applications

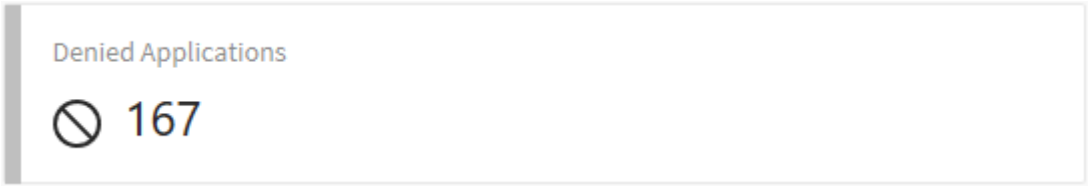
In "Allowed Applications" the total amount of applications to which access has been authorized is displayed.



Application Control – Allowed Application

UTM - Application Control - Denied Applications

In “Denied Applications” is the total of applications to which access has been denied.

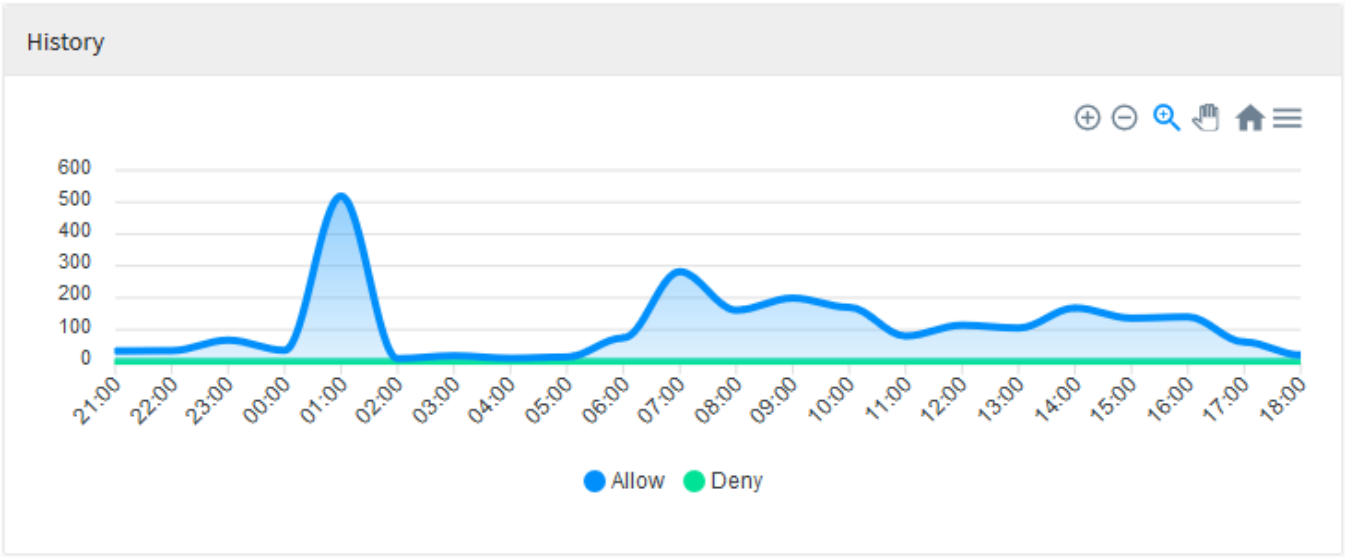


Application Control – Denied Application

UTM - Application Control - History

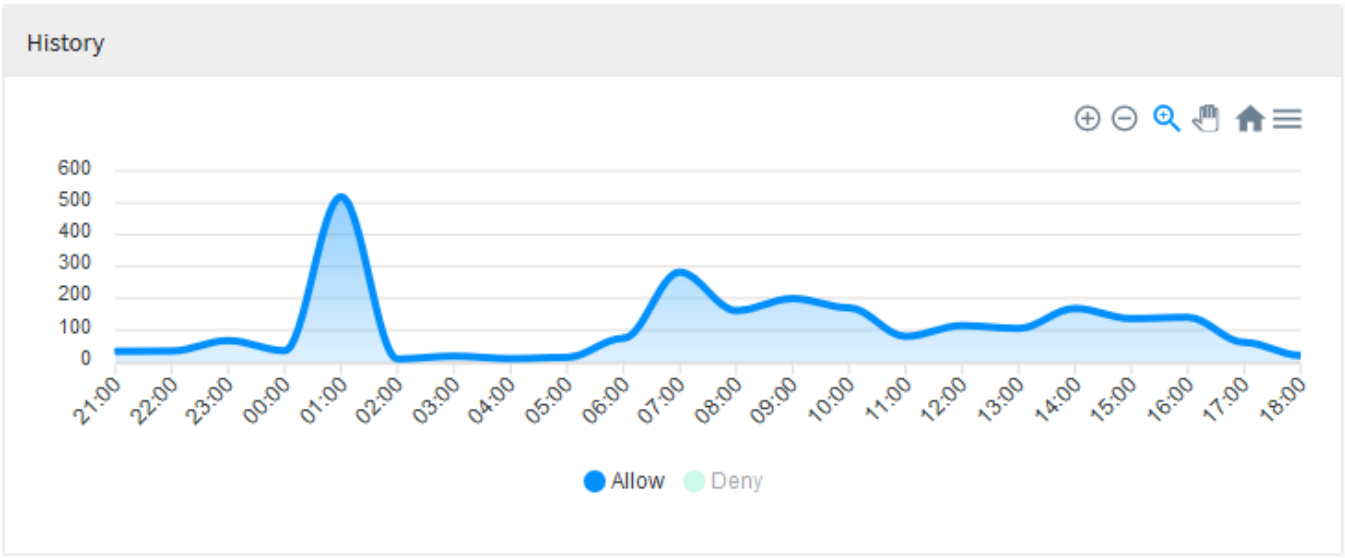
On the right side it is possible to view the “History” graph that displays a history of all applications that have been allowed and denied access, having as reference to their axes the amount of accesses in relation to the previously researched dates. The legend items are interactive and it is possible to change the graph display through them, in order to make the graph display the applications that were allowed and those that were denied by date. In this diagram we have “Allow” where the allowed applications are displayed and “Deny” showing all the applications denied for each of the researched days.

For more information about the navigation menu at the top of this graph, check this page.



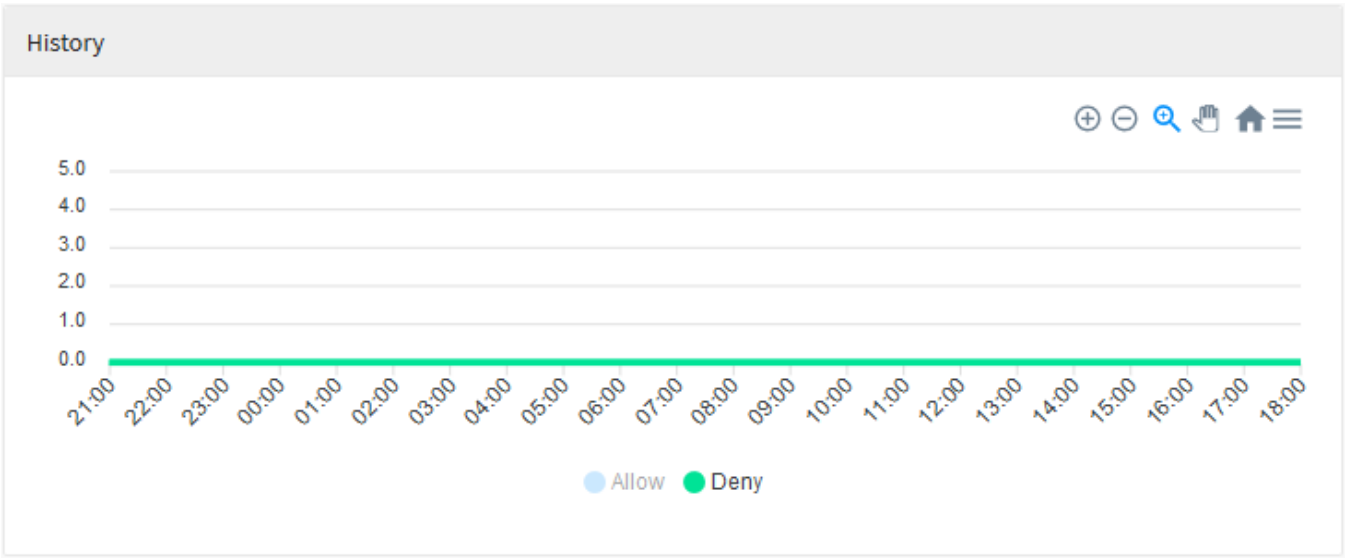
Application Control – History

It is possible to select "Allow", to modify the graph and illustrate the relevant information, as shown below:



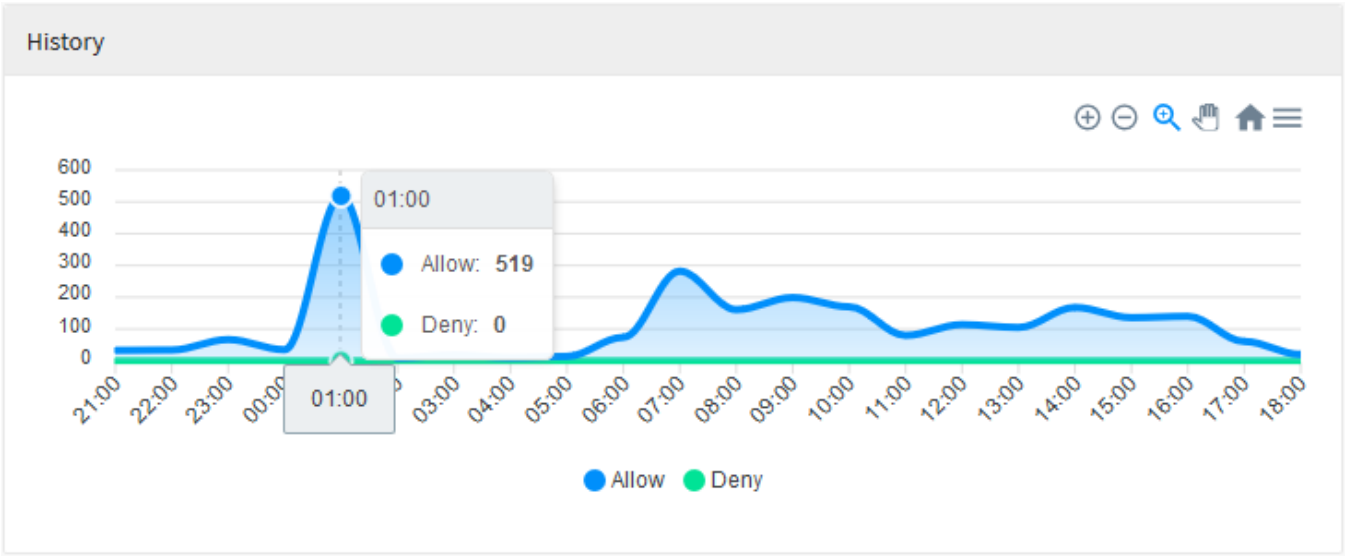
Application Control – History - Allow

You can also click on the "Deny" subtitle to modify the graph, as shown below:



Application Control – History - Deny

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



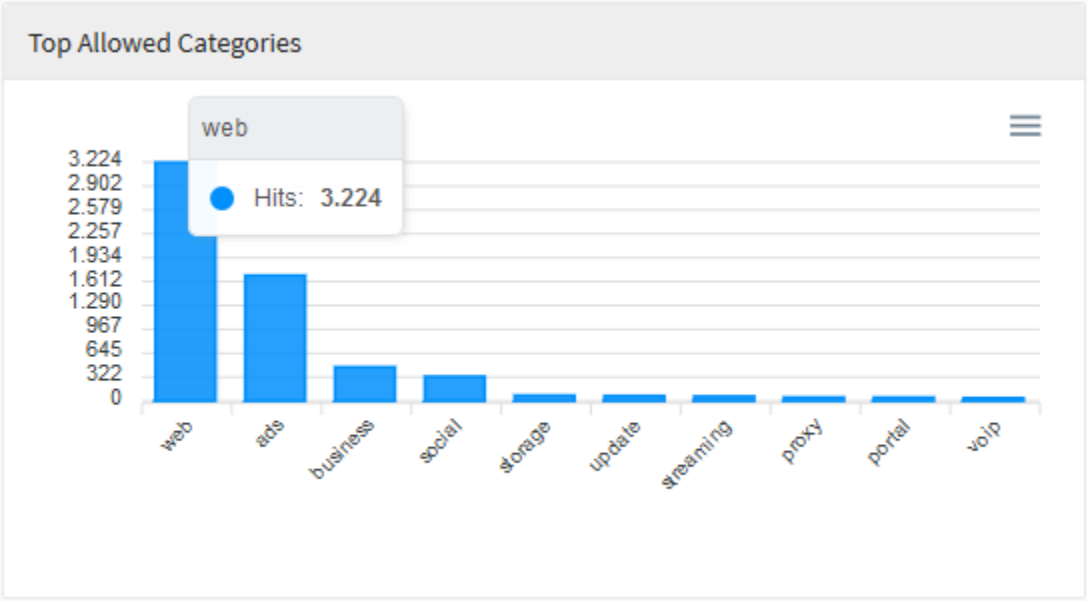
Application Control – History - Period Summary

UTM - Application Control - Top Allowed Categories

In the diagram “Top Allowed Categories” we have a visual representation of the 10 most allowed categories applied in users' accesses, this session serves to represent, in a pragmatic way, the number of pages accessed that apply to each of these categorizations.

When you mouse over the graph, a summary of the period is displayed, as shown in the image below:

For more information about the navigation menu at the top of this graph, check this page.



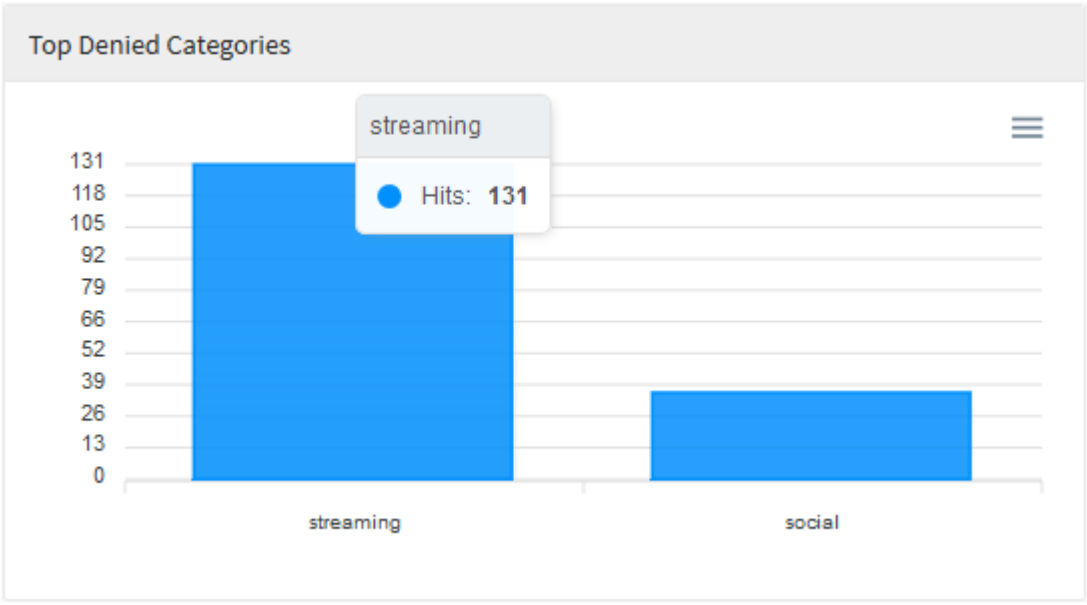
Application Control – Top Allowed Categories

UTM - Application Control - Top Denied Categories

In the diagram “Top Denied Categories” we have a visual representation of the 10 most frequently refused categories used by users, this session serves to represent, in a pragmatic way, the number of pages accessed that fell in each of these categories of refusal.

When hovering the mouse over the graph, a summary of the amount of categories is displayed, as shown in the image below.

For more information about the navigation menu at the top of this graph, check this page.



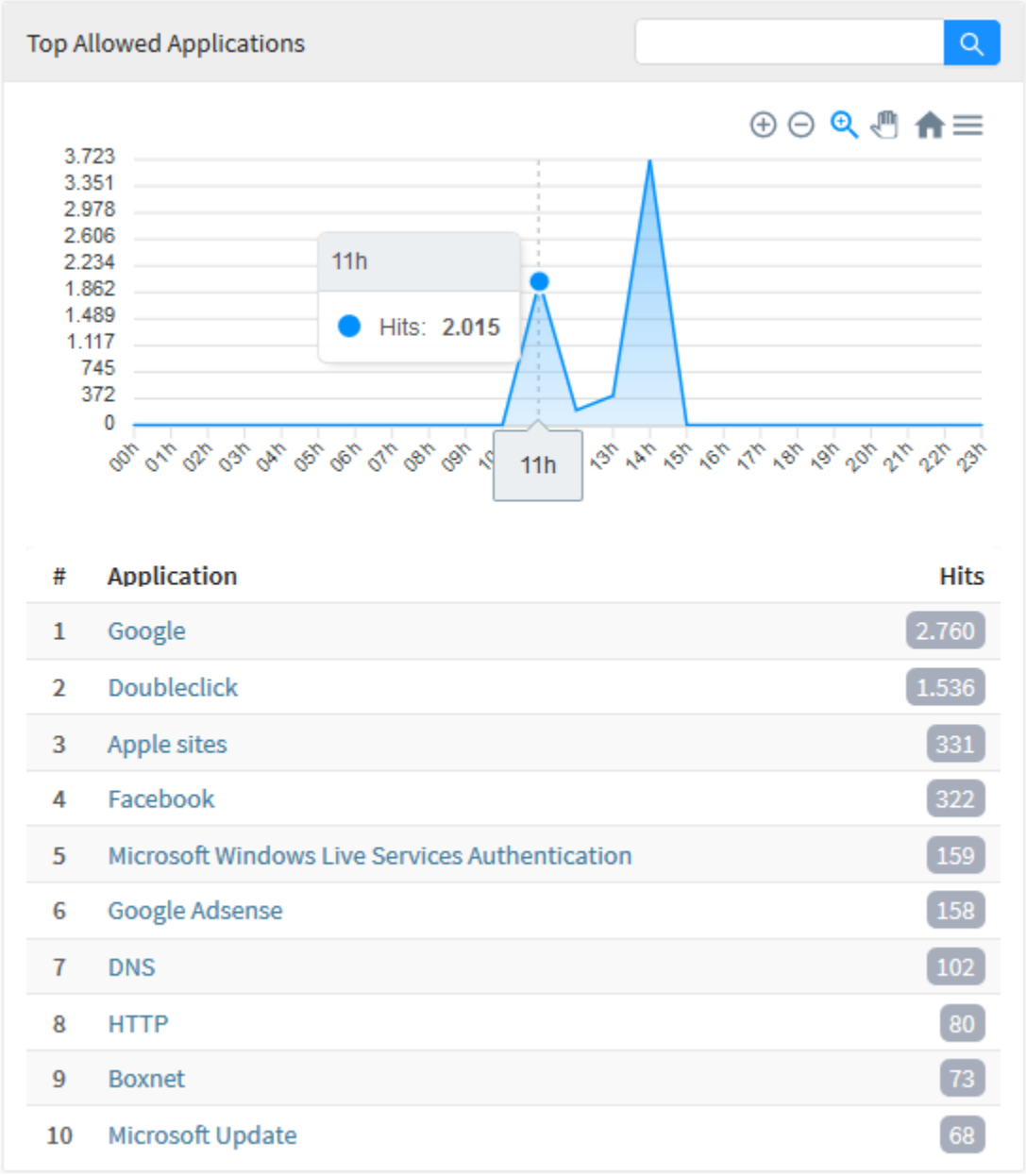
Application Control – Top Denied Categories

UTM - Application Control - Top Allowed Applications

In “Top Allowed Applications” there is a chart representing the ten applications that had their access authorized in relation to the previously specified period of time, below that chart, we have a list of the names of these ten applications classified in order of the highest amount of accesses and their respective categories.

When you mouse over the graph, a summary of the period is displayed, as shown in the image below.

For more information about the navigation menu and the search bar at the top of this graph check this page.



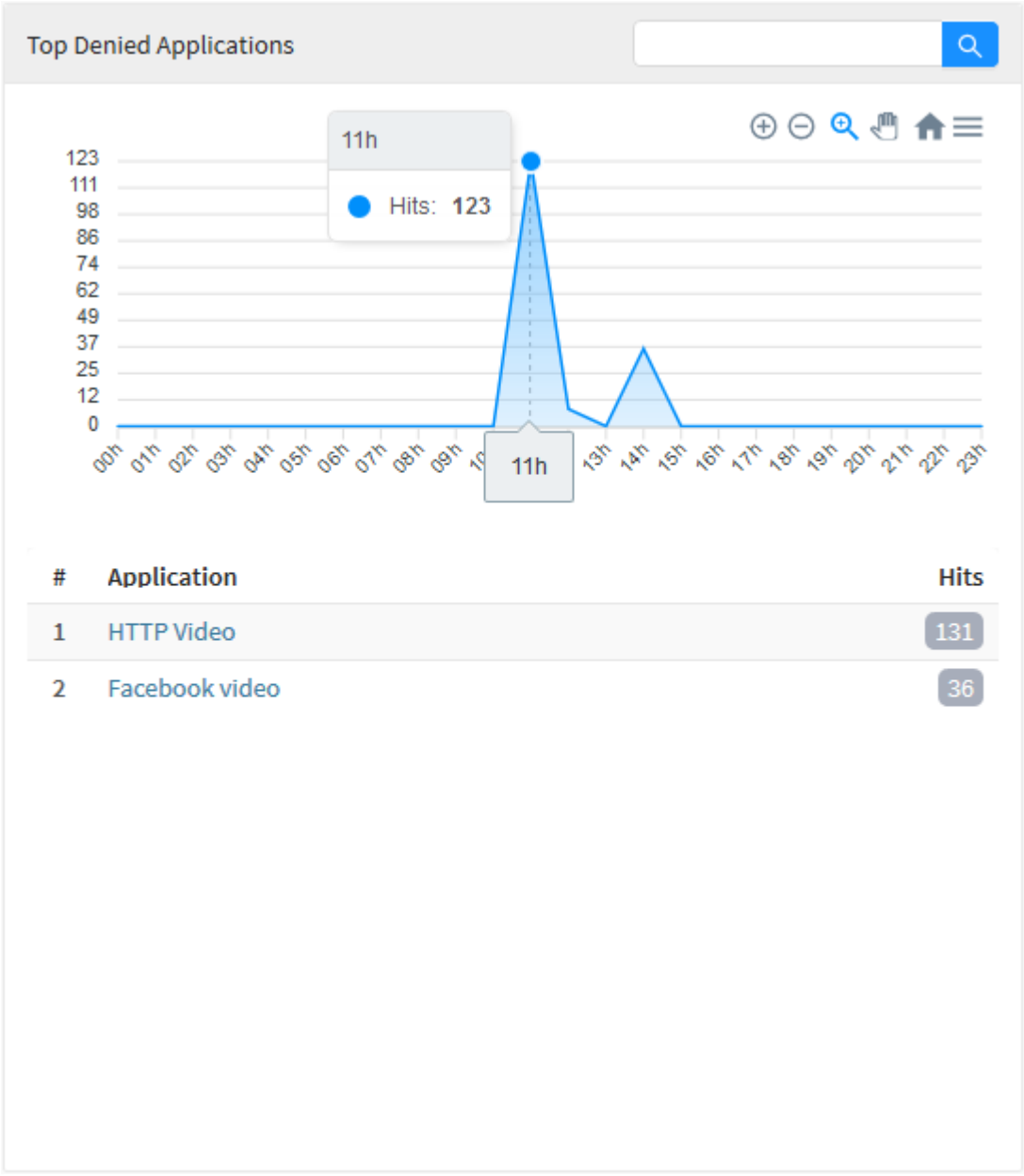
Application Control – Top Allowed Applications

UTM - Application Control - Top Denied Applications

In the panel “Top Denied Applications” we have the exact opposite of the previous session: A graph representing the ten applications that were denied access in relation to the previously specified period of time, below that graph, we have a list of the names of these ten applications classified in order largest amount of accesses and their respective categories.

When you mouse over the graph, a summary of the period is displayed, as shown in the image below.

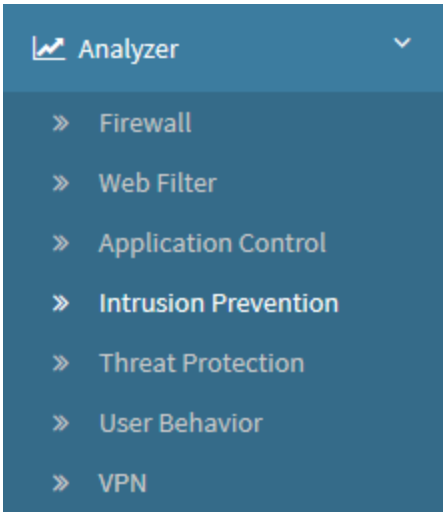
For more information about the navigation menu and the search bar at the top of this graph check this page.



Application Control – Top Denied Applications

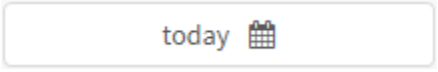
UTM - Intrusion Prevention

To access the Intrusion Prevention reports, click on the “Analysis” icon located on the left side, a dropdown menu will be displayed, select the “Intrusion Prevention” option.



Intrusion Prevention

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

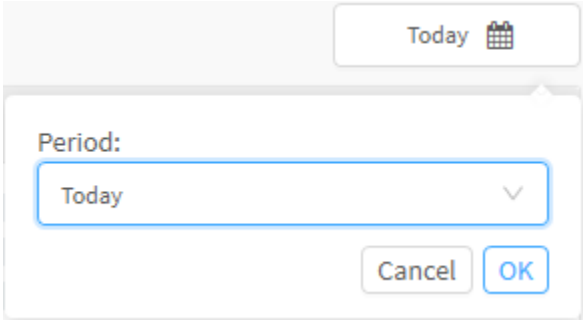


Intrusion Prevention - Selection box

Its purpose is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



To close this window, click **[** Cancel **]** or, after selecting the desired date, click **[** OK **]**;

The screen below will appear:

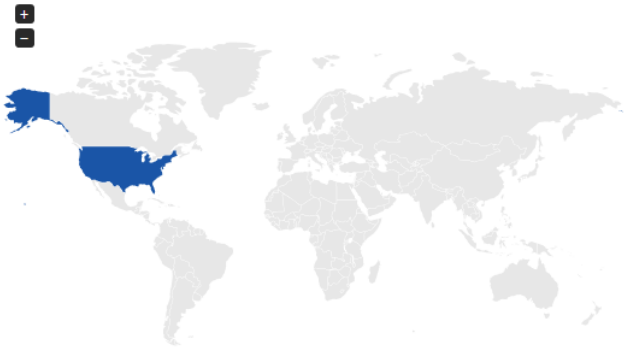
Intrusion Prevention

today | Blockbit

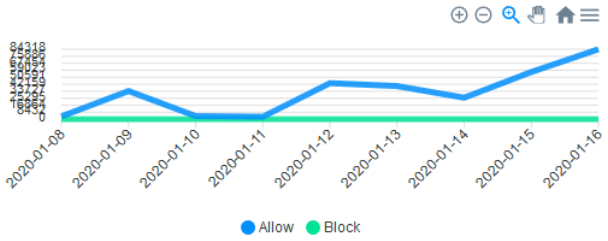
Alerted
✓ 12

Blocked
⊘ 7,000

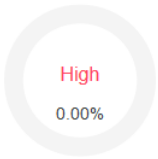
Geolocation

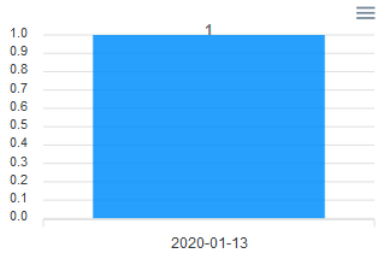


History



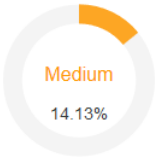
Impact - High

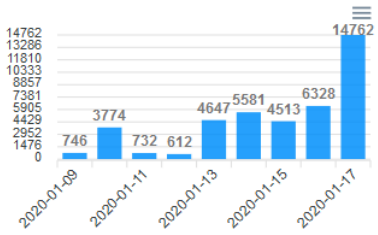




#	Threat	Hits
1	SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt	1

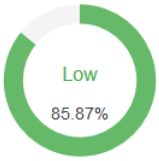
Impact - Medium

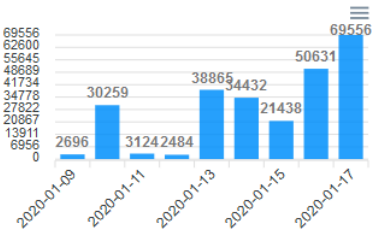




#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	40.993
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	285
3	GPL SNMP request udp	116
4	SERVER-OTHER MRLG fastping echo reply memory corruption attempt	70
5	PROTOCOL-SNMP request udp	65
6	GPL SNMP public access udp	51
7	PROTOCOL-SNMP public access udp	51

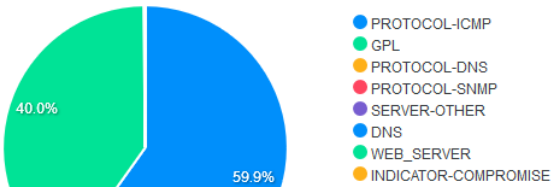
Impact - Low



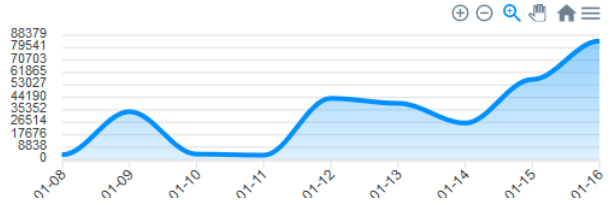


#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	54.896
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	54.874
3	GPL ICMP_INFO PING	41.115
4	PROTOCOL-ICMP PING	40.964
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.811
6	GPL ICMP_INFO Echo Reply	12.550
7	PROTOCOL-ICMP Echo Reply	12.543

Layer 3 Intrusion Protection



Intrusion Classification



Analyzer - Intrusion Prevention

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom;
- **[ ]:** Its function is to remove the zoom;
- **[ ]:** It serves to make a selection zoom;
- **[ ]:** It serves to move the graph;
- **[ ]:** Reset the graph to the starting position;
- **[ ]:** Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the search **[ ]** button.

Next, we will analyze in detail the components of “Intrusion Prevention”:

- *Alerted*, *Blocked* and History;
- *Alerts by Geolocation*;
- *Impact - High*;
- *Impact - Medium*;
- *Impact - Low*;
- *Layer 3 Intrusion Protection*;
- *Intrusion Classification*;
- *Top Source*;
- *Top Destination*.

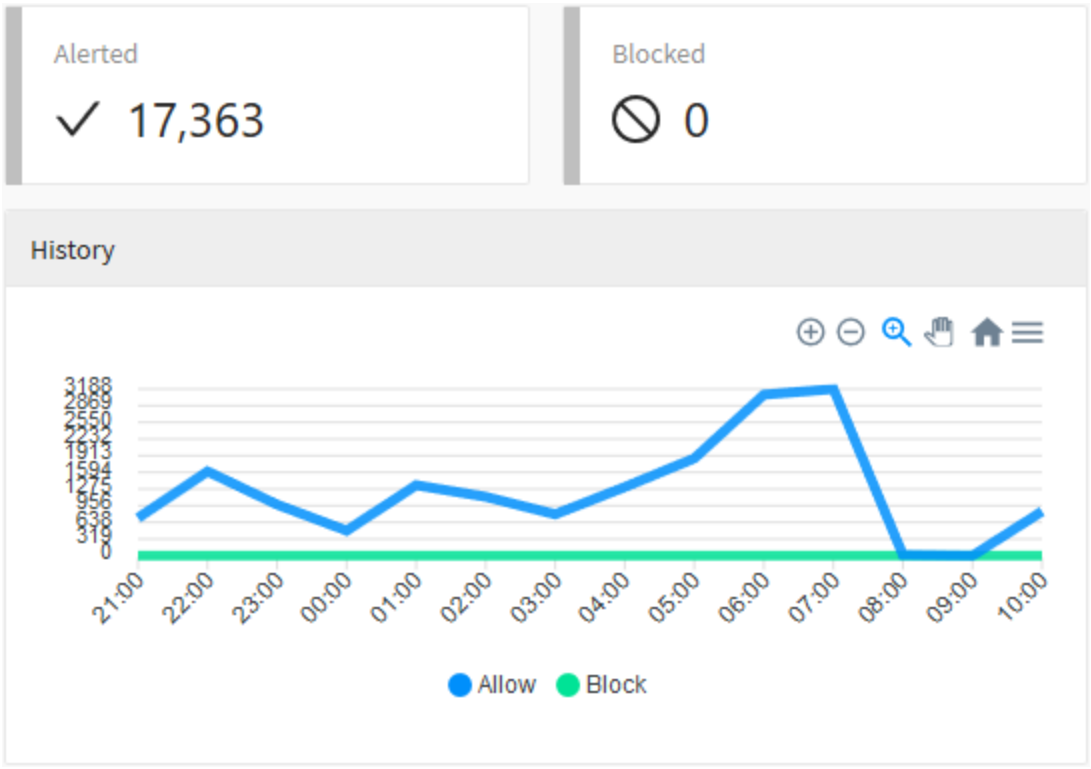
UTM - Intrusion Prevention - Alerted, Blocked and History

The “Alerted” panel displays a total of intrusion alerts.

In “Blocked”, a number is displayed totaling the blocked intrusion attempts.

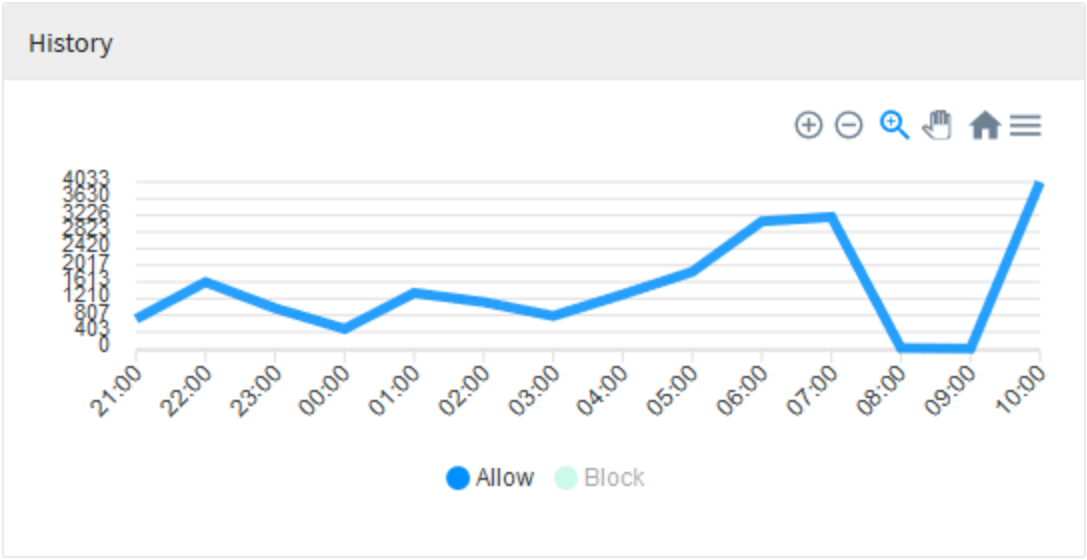
Below, a summary of alerts and blockages is shown in a line graph showing the number of intrusion-related events within the previously selected time period. By selecting one of the captions (“Alerted” or “Blocked”) at the top of the graph, it is possible to determine that only one of these are displayed on the graph.

For more information about the navigation menu at the top of this graph, check this page.



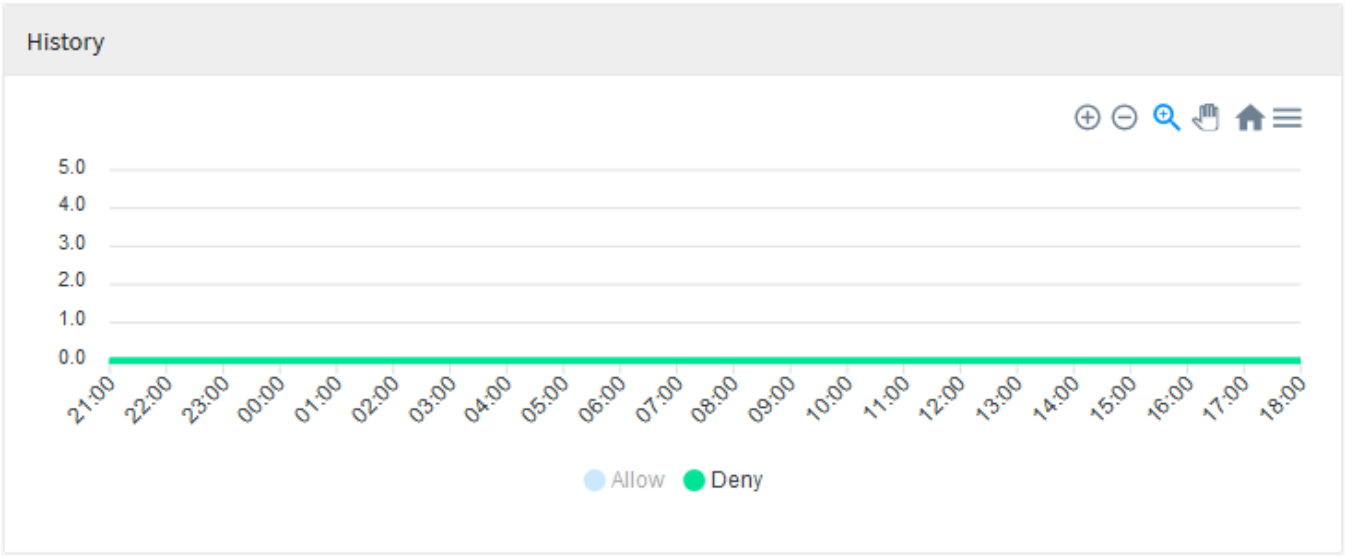
Alerted, *Blocked* and History

It is possible to select "Allow", to modify the graph and illustrate the relevant information, as shown below:



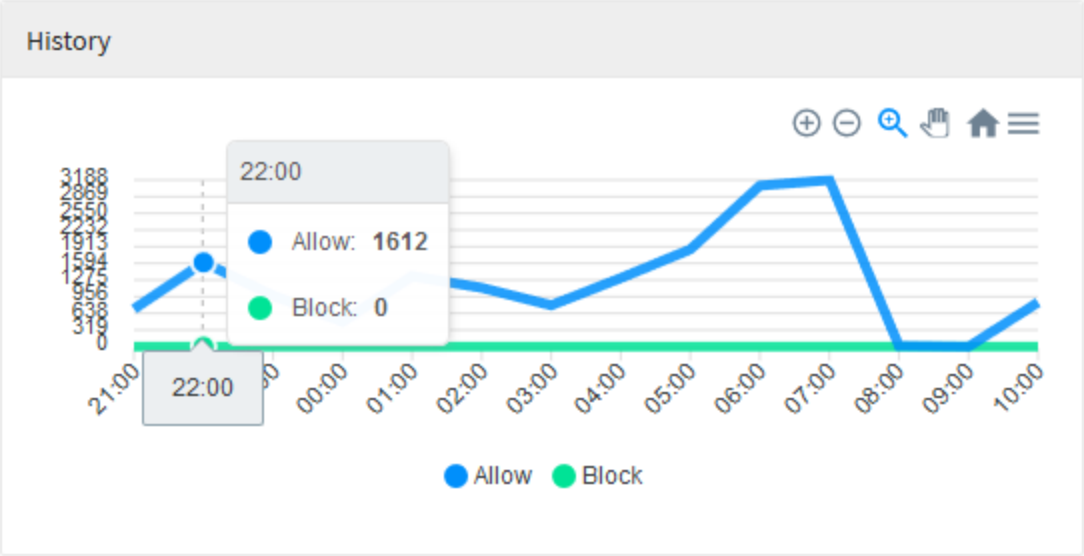
Alerted, Blocked and History - *Allow*

You can also click on the "Deny" legend to modify the graph, as shown below:



Alerted, Blocked and History - *Deny*

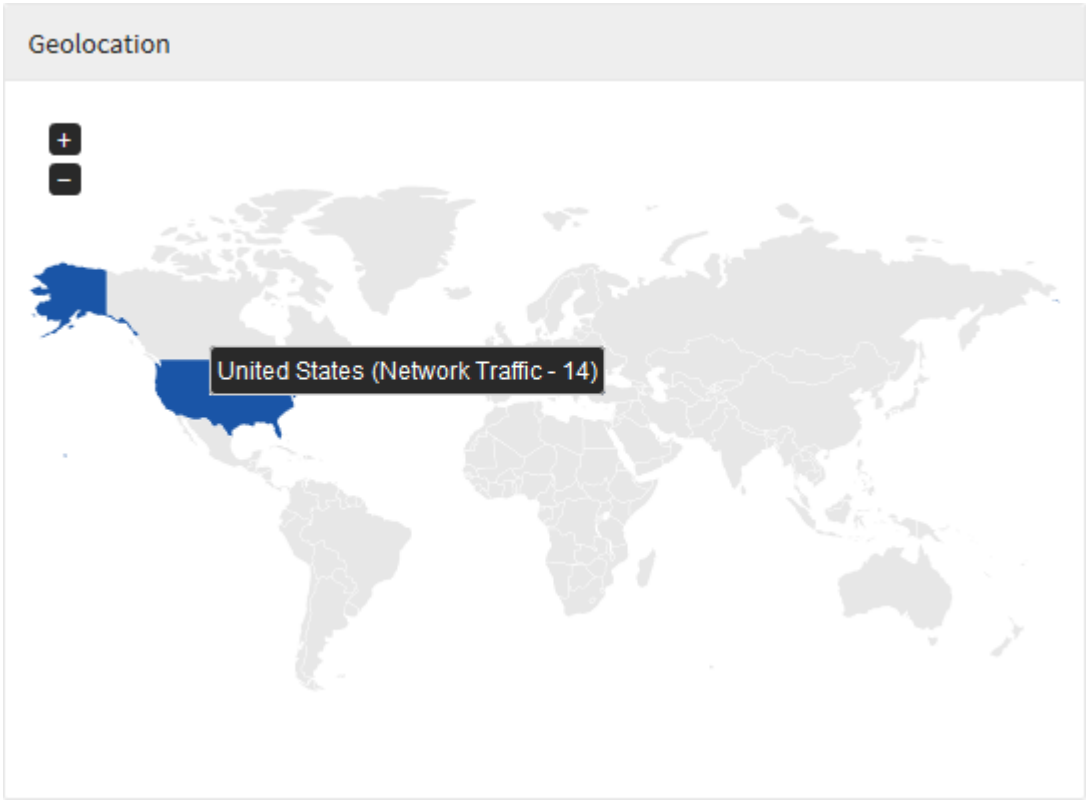
When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



Alerted, *Blocked* and History - Period Summary

UTM - Intrusion Prevention - Alerts by Geolocation

In “Alerts by Geolocation” the origin of the intrusions by geolocation is displayed, the global map demonstrates through a colored legend the amount of accesses made by users. When hovering the mouse over the countries a total number of alerts is displayed, when doing the same with the legend it is possible to view an average, in addition, the country for that value is highlighted on the map.

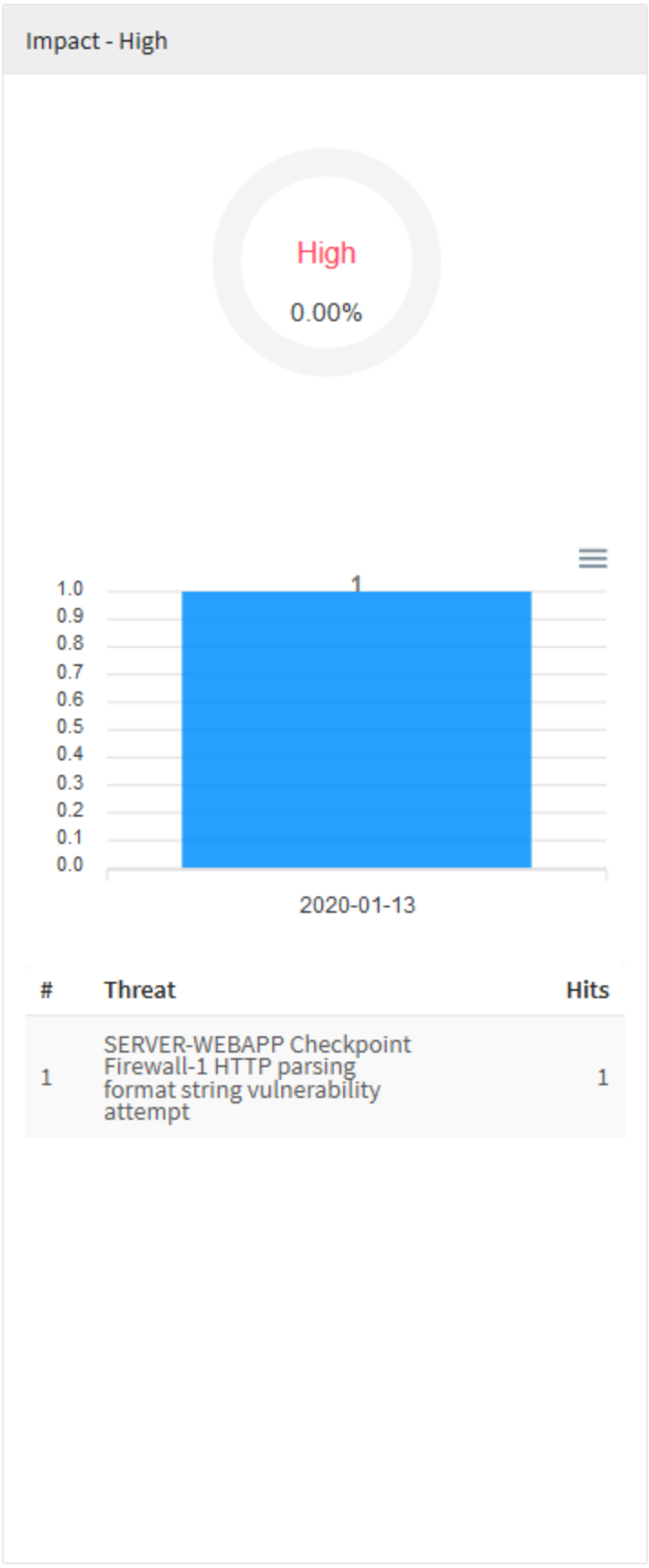


Alerts by Geolocation

UTM - Intrusion Prevention - Impact - High

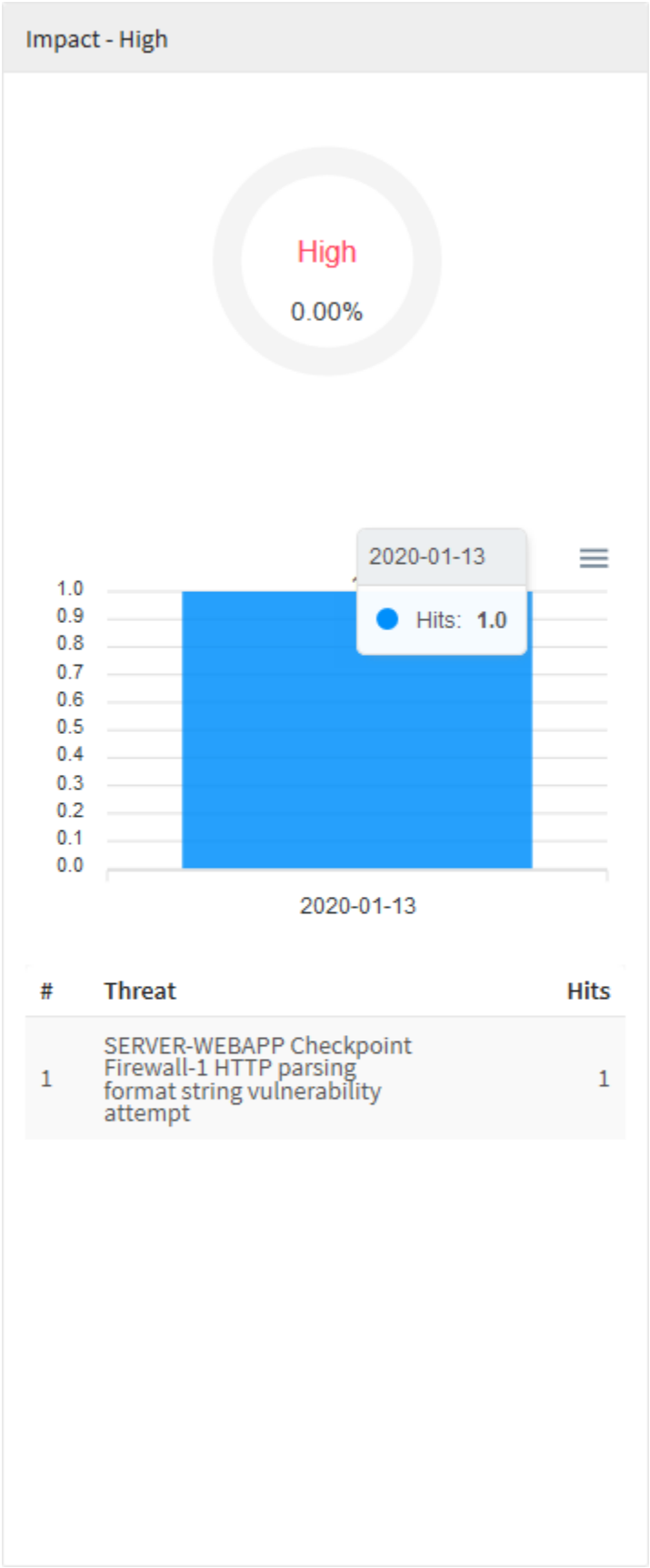
In “Impact - High” we have a donut chart showing the percentage of high impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring high-impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph, check this page.


Impact - High
High
0.00%
1
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
2020-01-13
Threat Hits
1 SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt 1

Impact - High

When you mouse over the graph, a summary of the period is displayed, as shown in the image below:

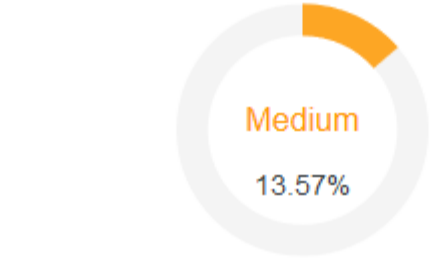


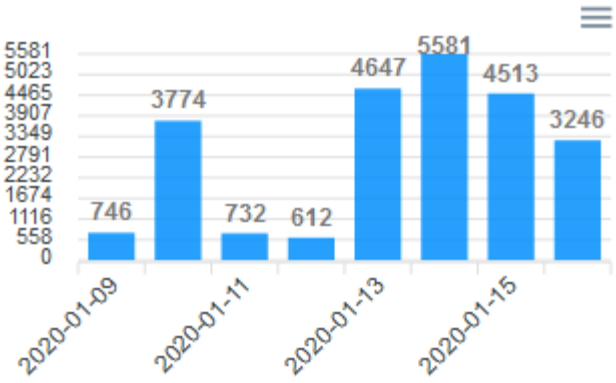
UTM - Intrusion Prevention - Impact - Medium

In “Impact - Medium” we have a donut chart showing the percentage of medium impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring medium impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph, check this page.

Impact - Medium

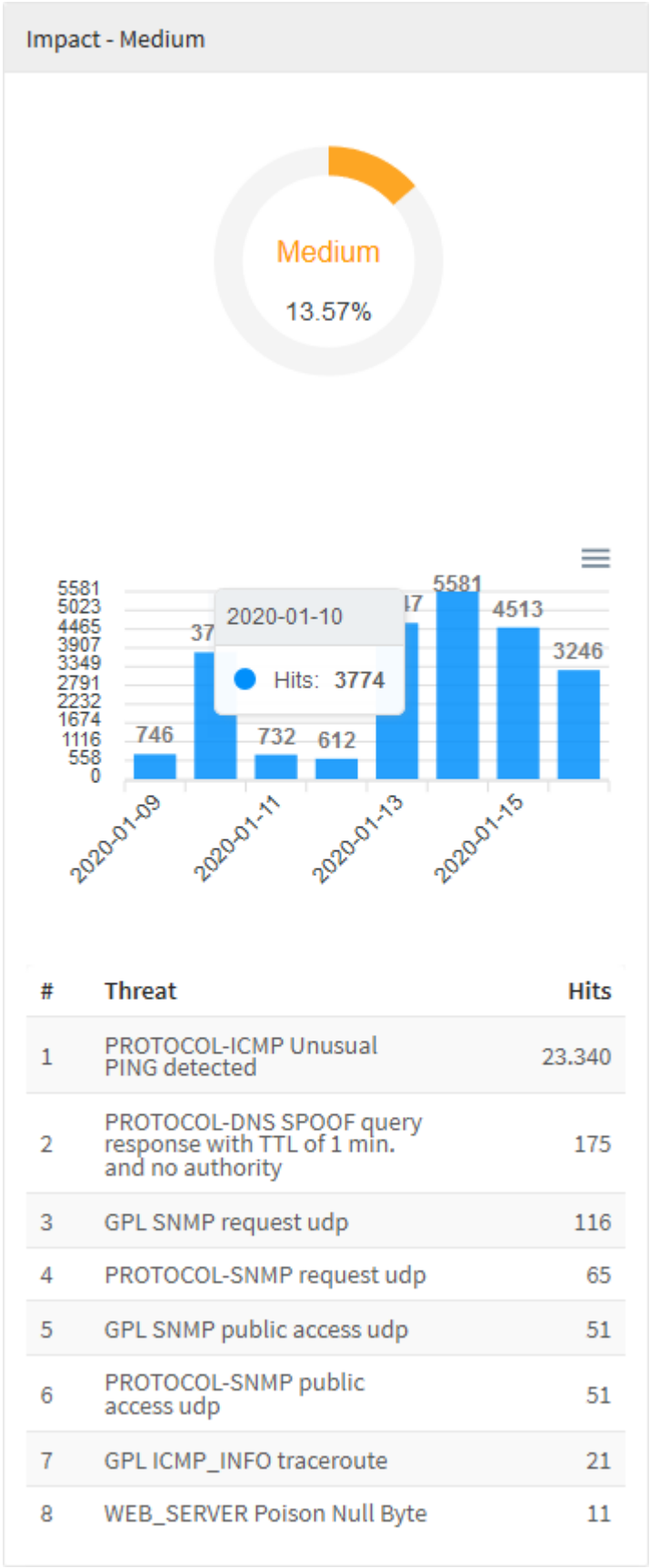




#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

Impact - Medium

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



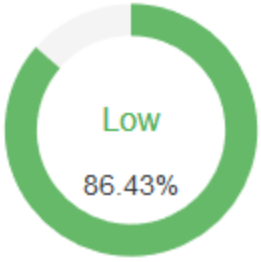
#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

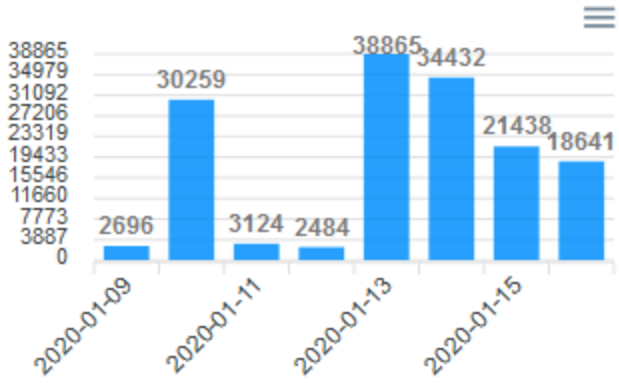
UTM - Intrusion Prevention - Impact - Low

In “Impact - Low” we have a donut chart showing the percentage of low impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring low-impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph, check this page.

Impact - Low

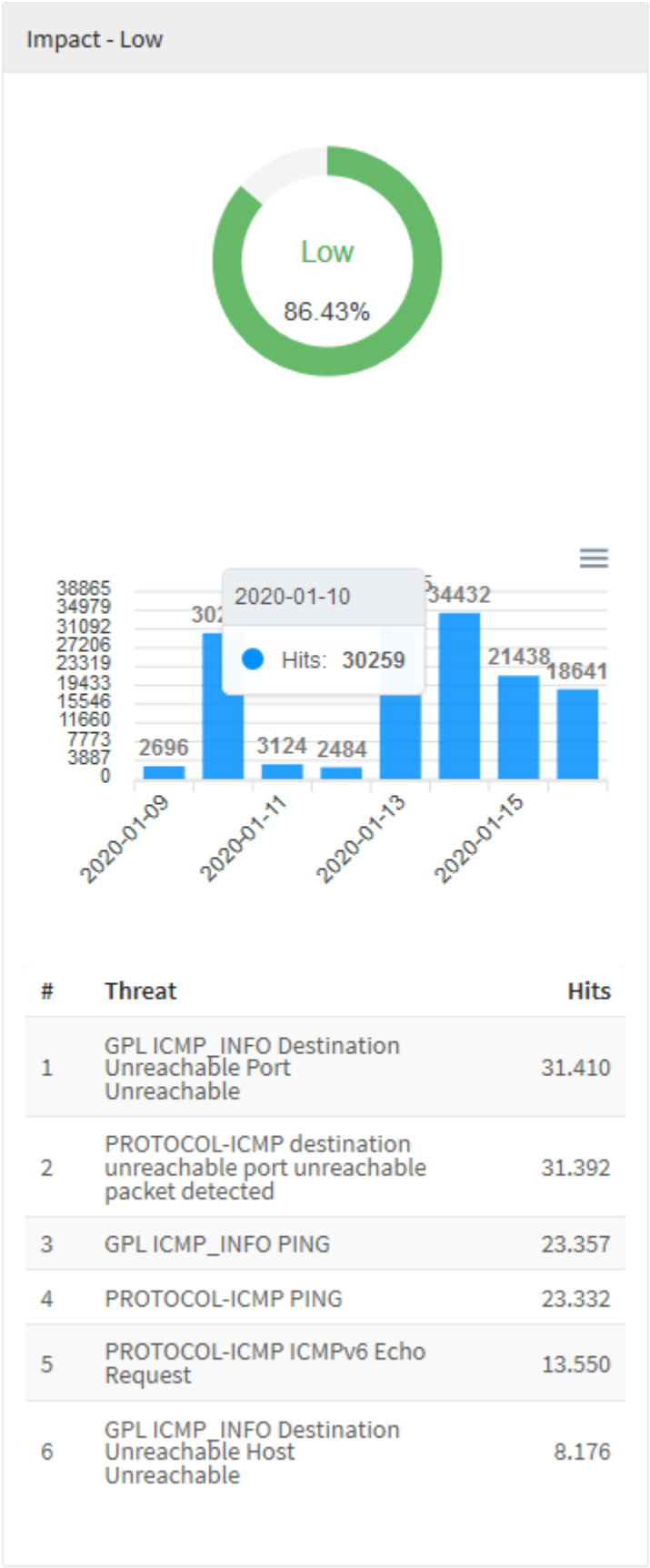




#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

Impact - Low

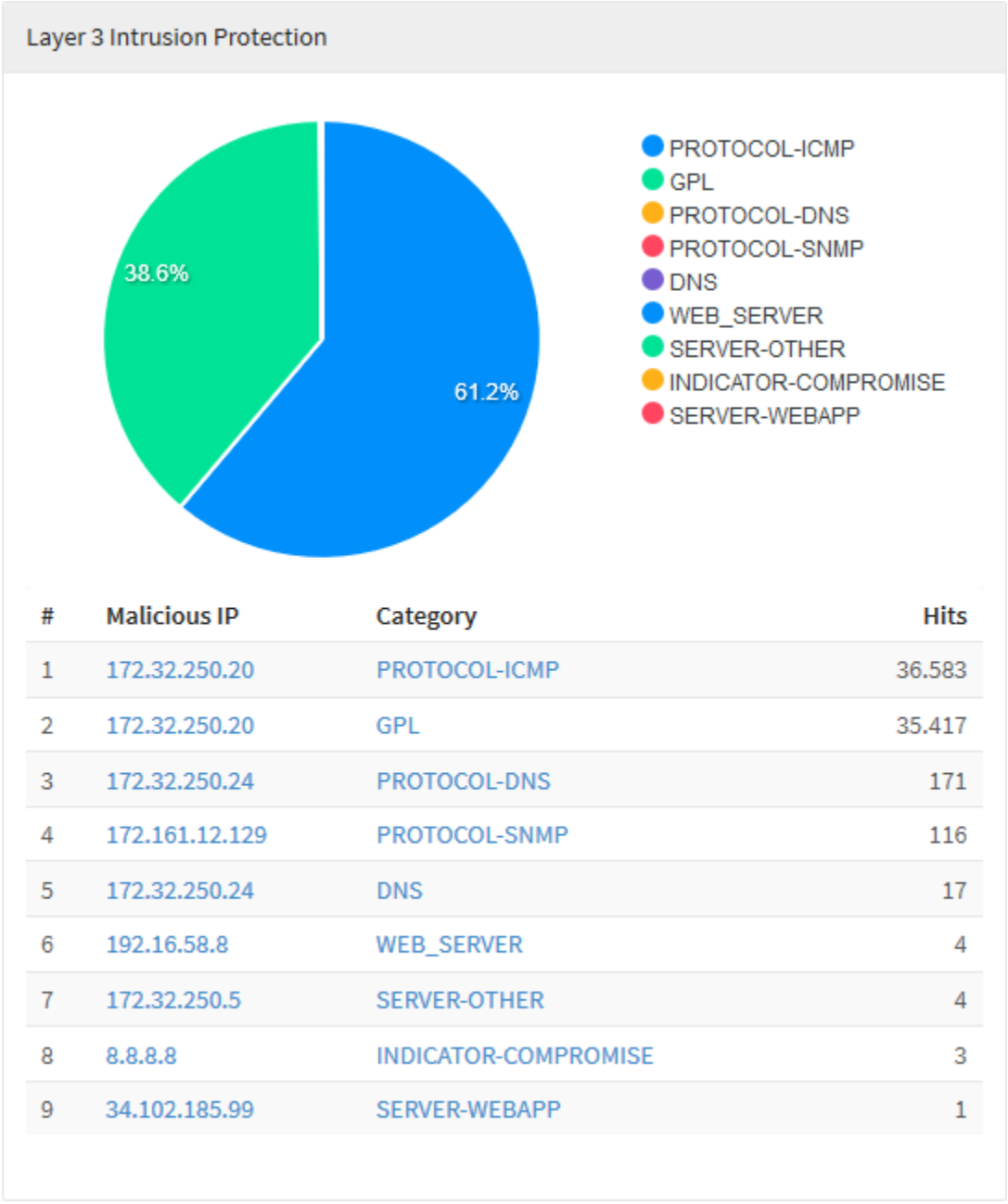
When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

UTM - Intrusion Prevention - Layer 3 Intrusion Protection

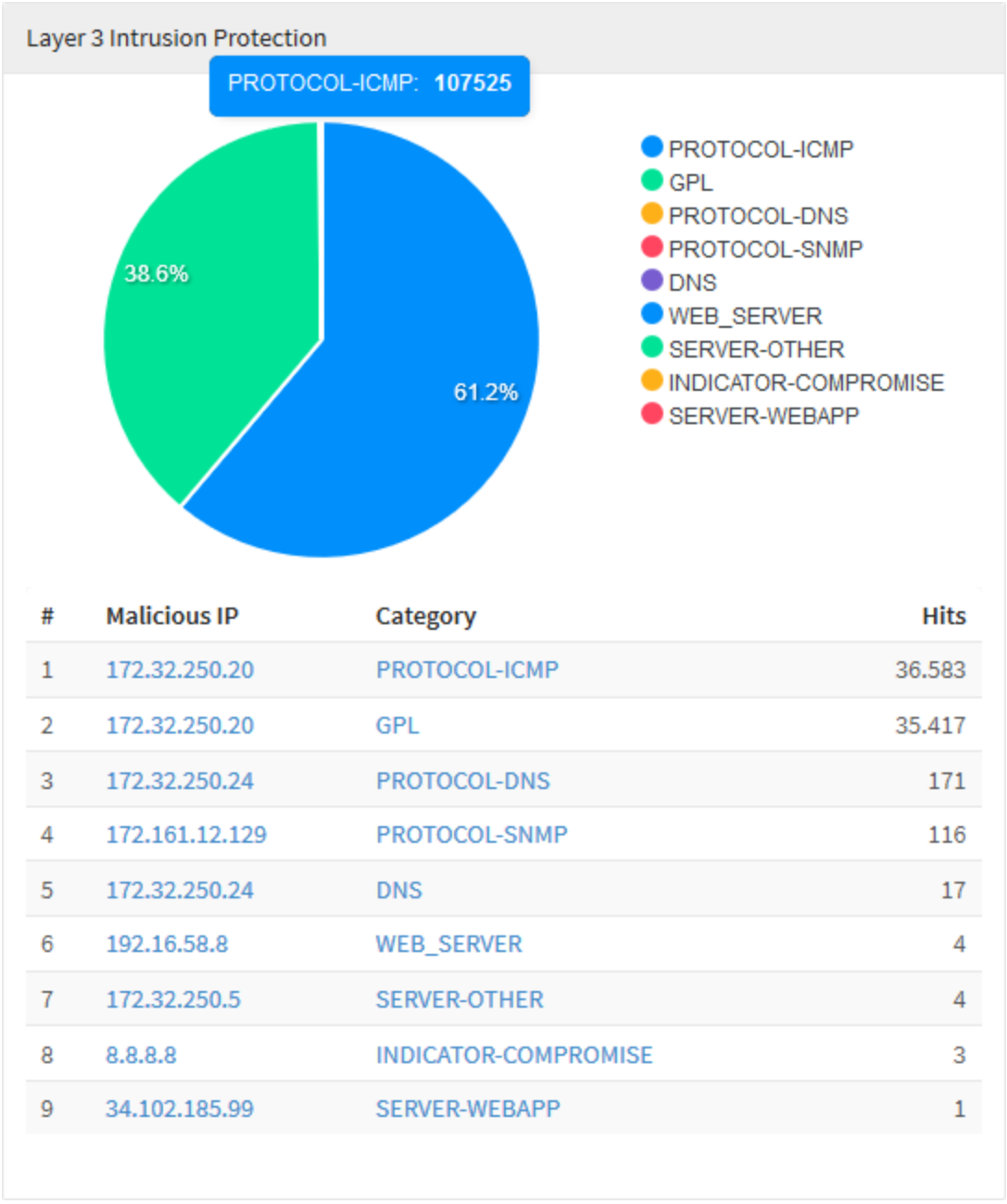
In “Layer 3 Intrusion Protection” we have a graph showing the ten categories of most detected intrusion alerts in layer 3 of the IPS (Intrusion Prevention System). When you click on one of the IPs or one of the categories, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected item. Just below the graph, we have a list of the ten IPs and the most accessed categories in order by the number of accesses.



#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Layer 3 Intrusion Prevention

When you hover your mouse over the graph, it will display a number with the amount of intrusion alerts, as shown in the image below:

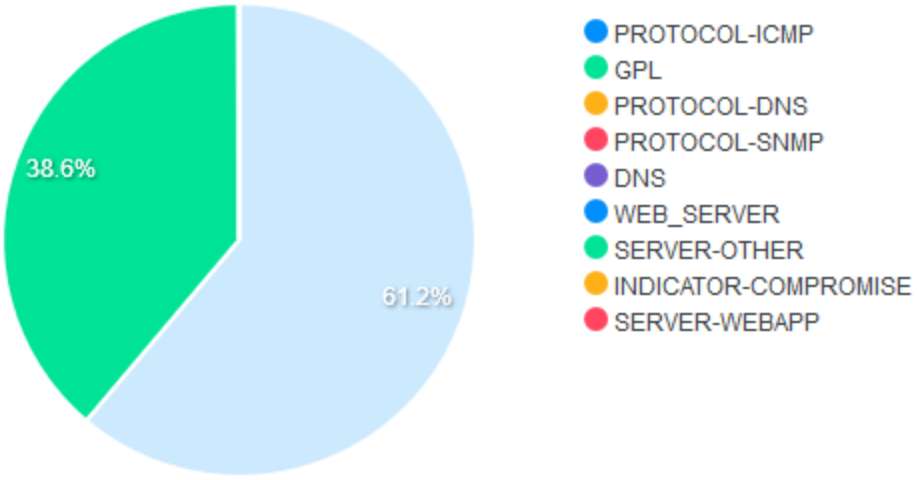


#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Layer 3 Intrusion Prevention - Amount of intrusion alerts

When hovering the mouse over the legend, the graphic will be highlighted, as shown below:

Layer 3 Intrusion Protection



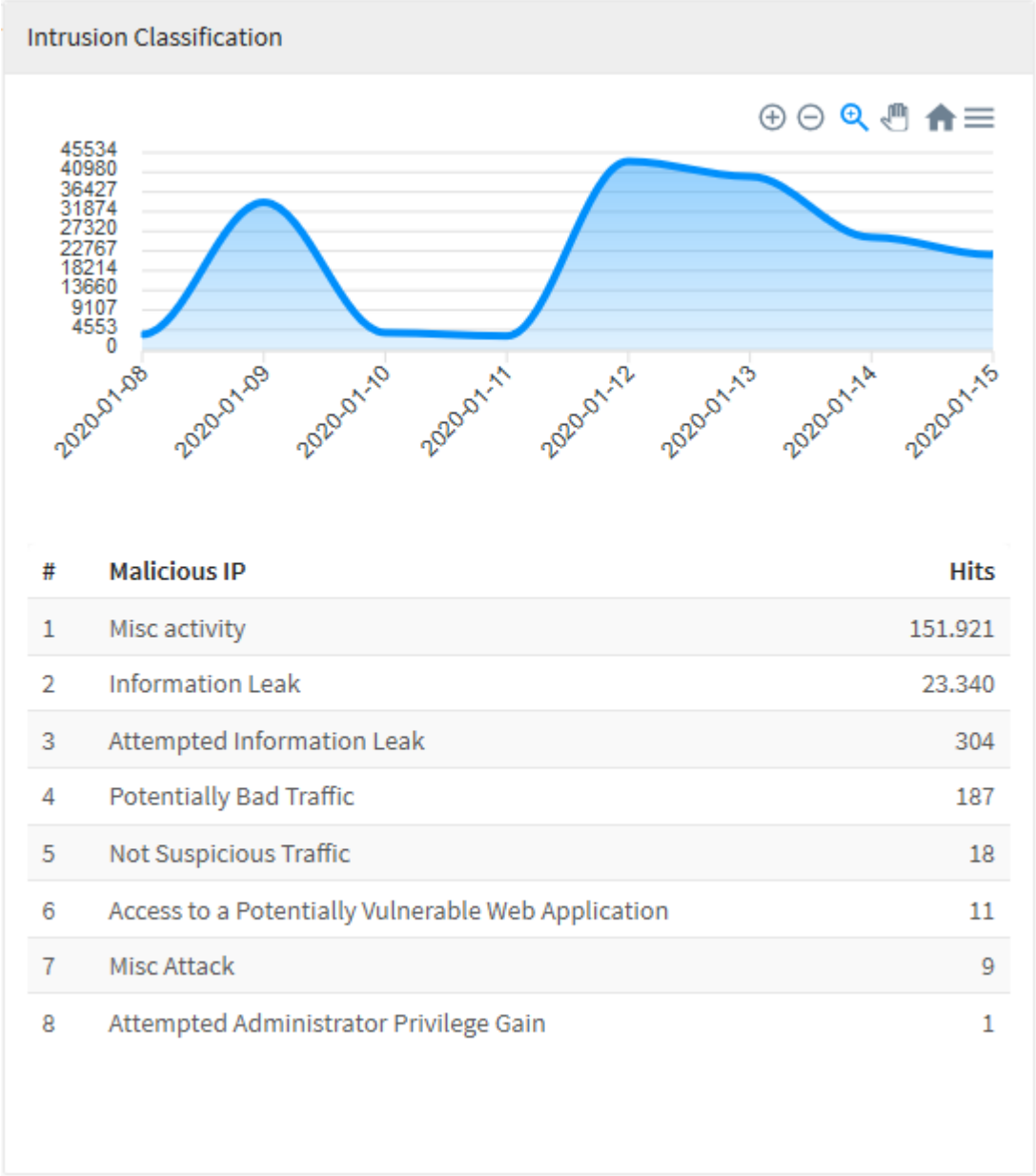
#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Layer 3 Intrusion Prevention - Highlighted graph

UTM - Intrusion Prevention - Intrusion Classification

In “Intrusion Classification” we have a graph representing the ten most recurrent intrusion alert classes in relation to the previously specified time period. Below the graph, we have a listing of the names of the ten classifications in order of highest amount of accesses.

For more information about the navigation menu at the top of this graph, check this page.

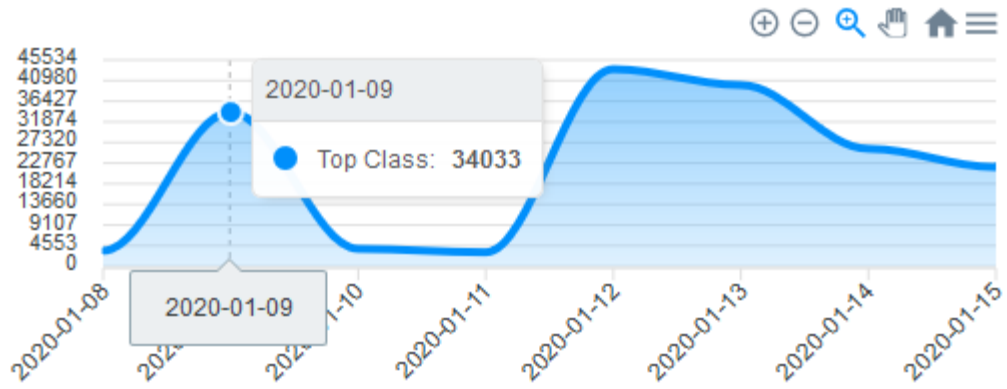


#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

Intrusion Classification

By hovering the mouse over the graph, it will highlight the date and number of accesses of the highest class on this specific day.

Intrusion Classification



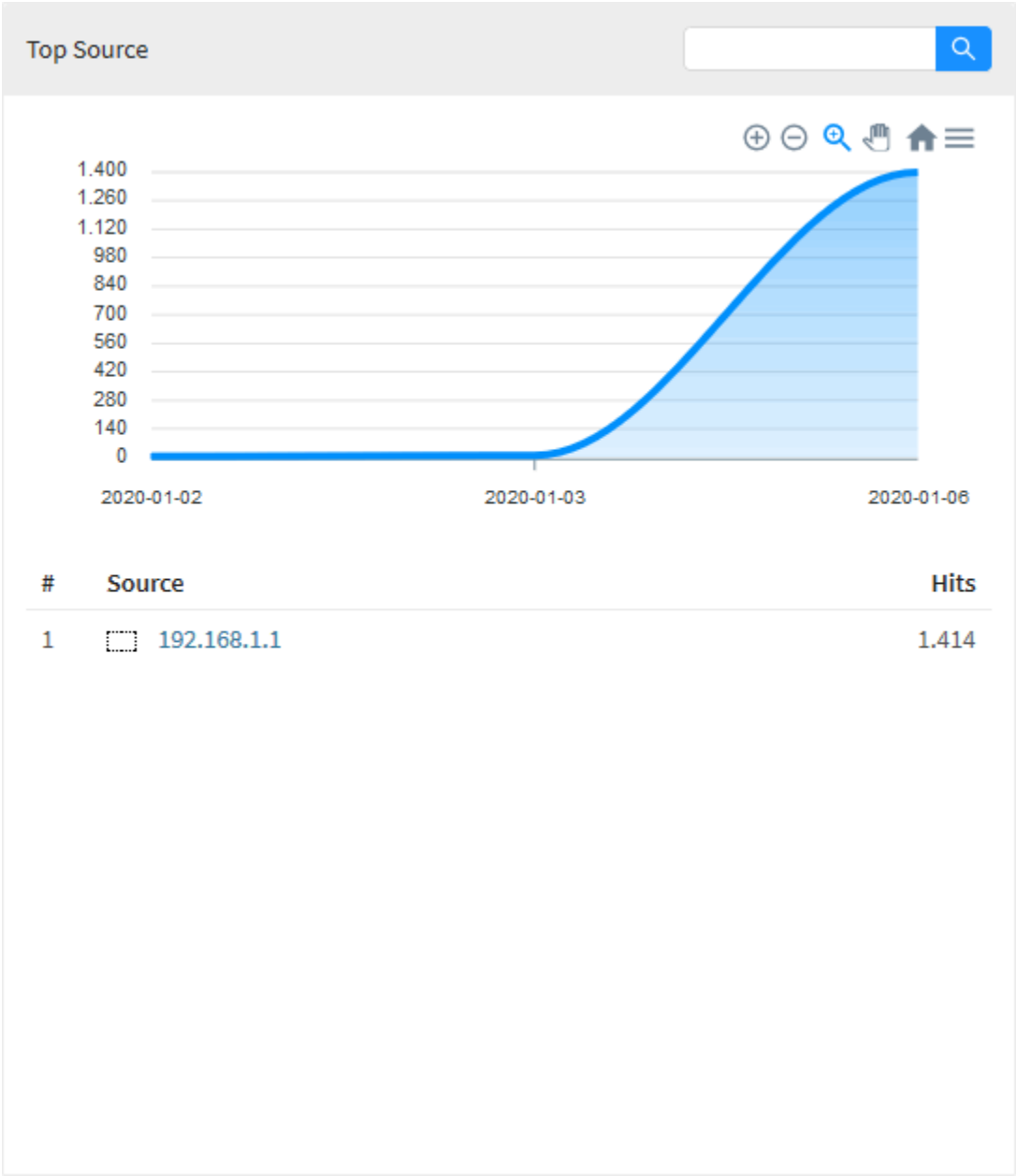
#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

Intrusion Classification - Class summary

UTM - Intrusion Prevention - Top Source

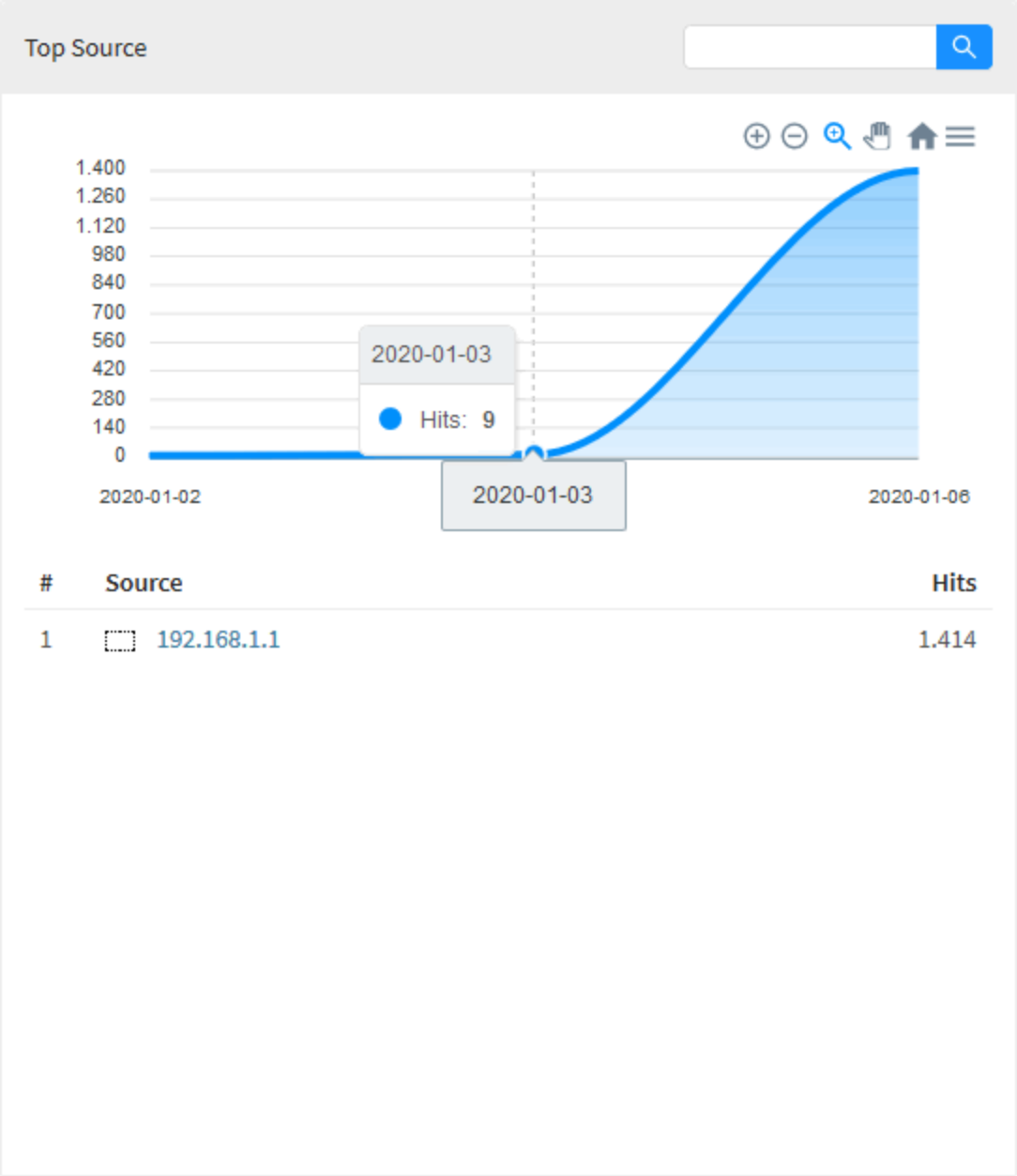
In “Top Source” a line graph is displayed representing the ten most recurrent intrusion alert sources in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten sources previously mentioned, which are classified in order of the highest amount of accesses. When you click on one of the IPs or one of the categories, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected category.

For more information about the navigation menu and the search bar at the top of this graph check this page.



Top Source

When hovering the mouse over the graph, it will highlight the date and the number of accesses of the highest class of this specific day:

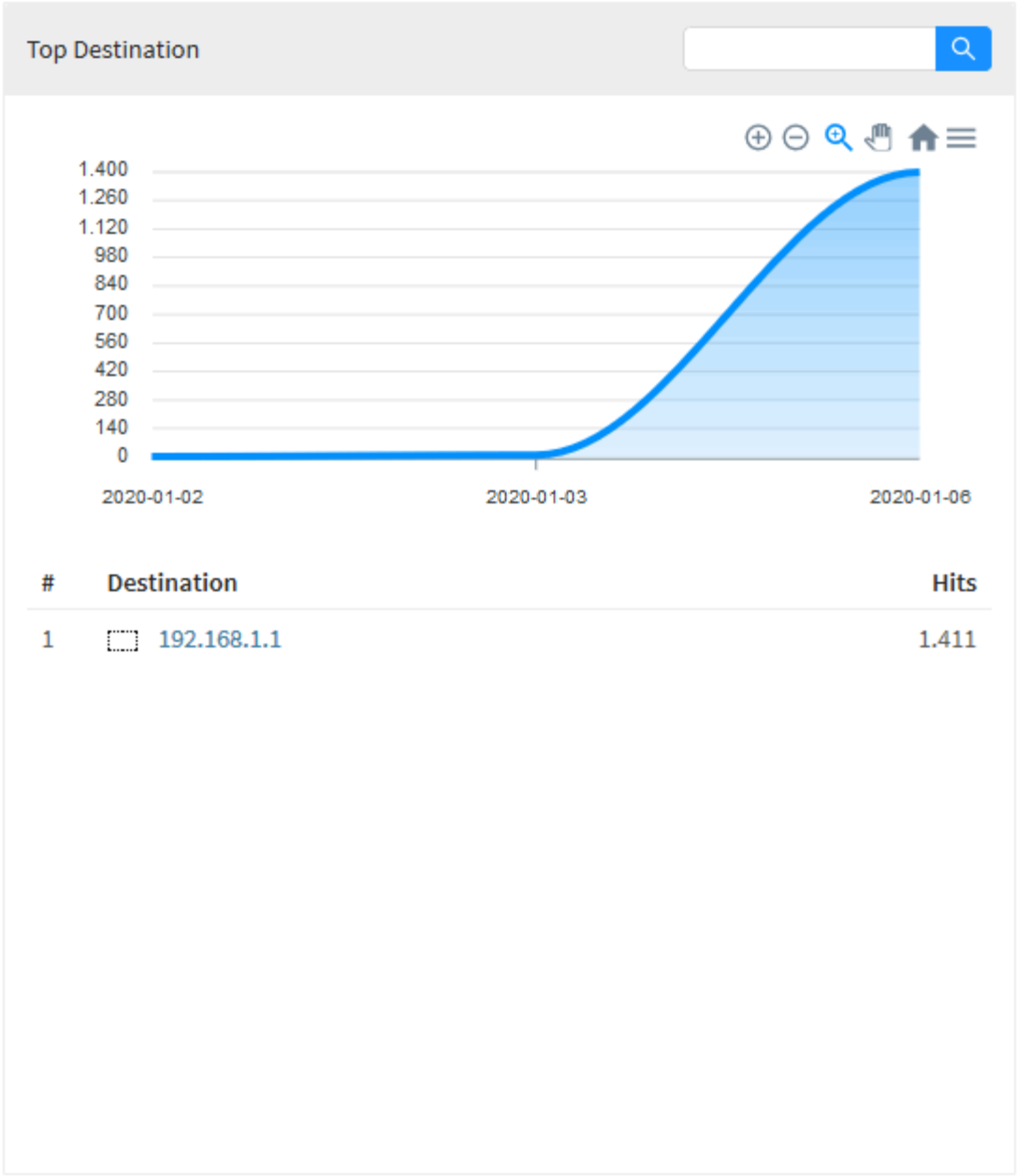


Top Source - Summary

UTM - Intrusion Prevention - Top Destination

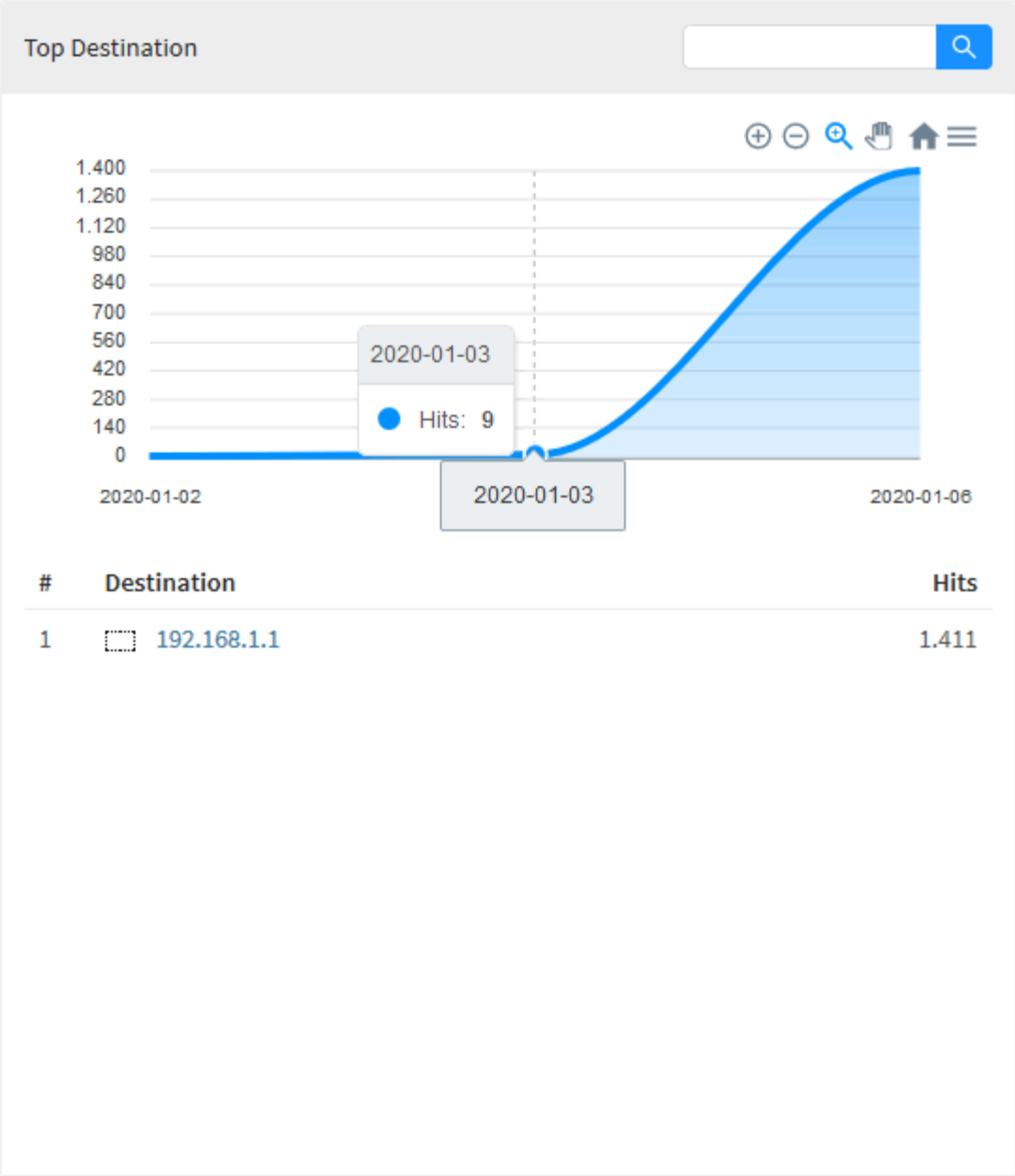
In “Top Destination” there is a line graph showing the ten most recurrent intrusion alert destinations in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of access to these sources generally. Below is a list showing the IPs of the ten destinations with the highest amount of access. When you click on one of the IPs or one of the categories, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected item.

For more information about the navigation menu and the search bar at the top of this graph check this page.



Top Destination

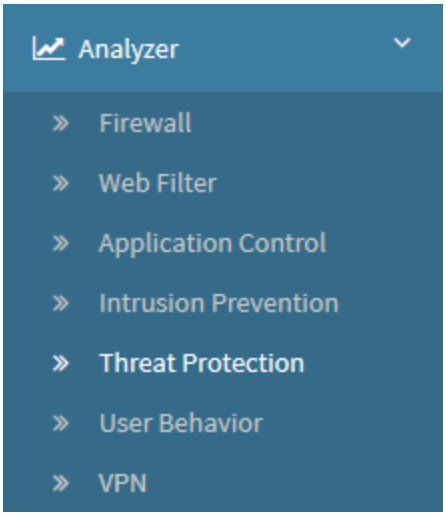
When hovering the mouse over the graph, it will highlight the date and the number of accesses of the highest class of this specific day:



Top Destination - Access Summary

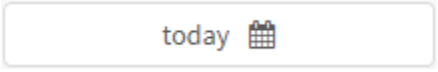
UTM - Threat Protection

To access the Threat Protection reports, click on the “Analysis” icon located on the left side, a dropdown menu will be displayed, select the option “Threat Protection”.



Threat Protection

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

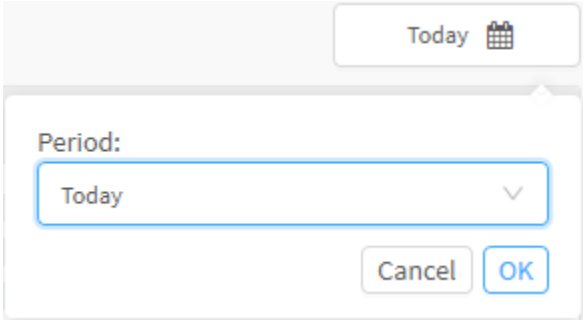


Threat Protection - Selection box

Its purpose is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



To close this window, click **[** Cancel **]** button or, after selecting the desired date, click **[** OK **]**;

The screen below will appear:

Threats

range

Blockbit

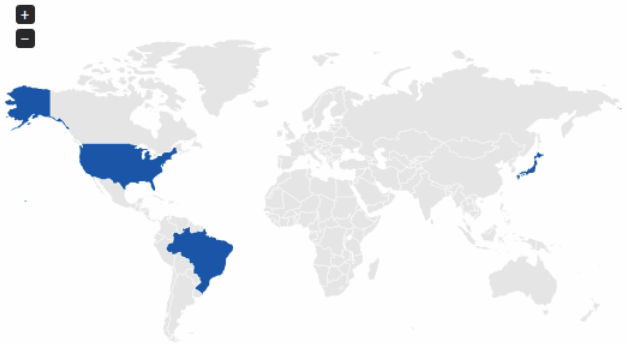
Threats

5,390

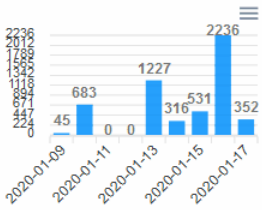
Malwares

2,800

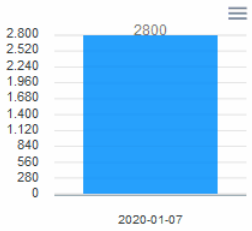
Geolocation



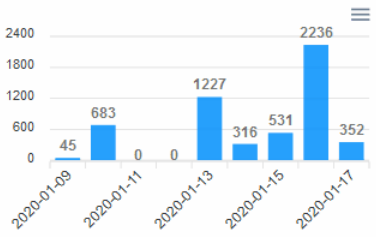
History



History

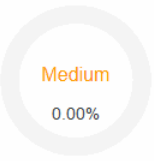


Impact - High



#	Threat	Hits
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	1327
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	1321
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	1235
	PUA-P2P BitTorrent transfer	782
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)	282
	PUA-P2P Bittorrent uTP peer request	248

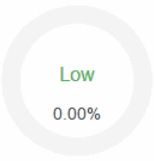
Impact - Medium



#	Threat	Hits

No Data

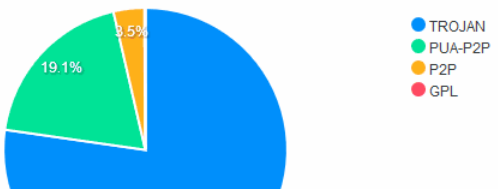
Impact - Low



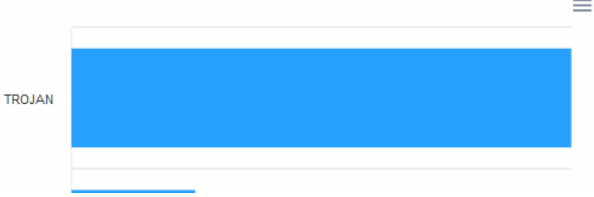
#	Threat	Hits

No Data

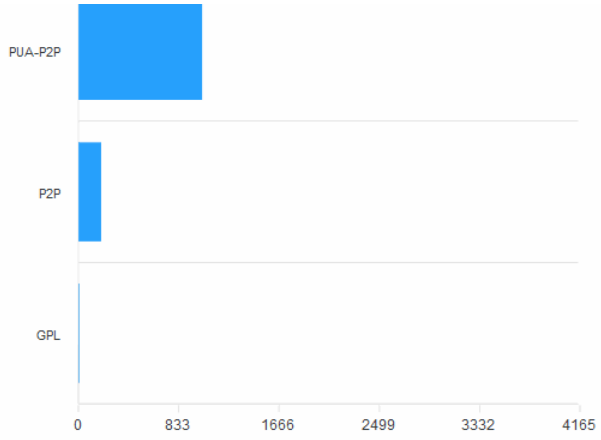
Malicious IP Classification



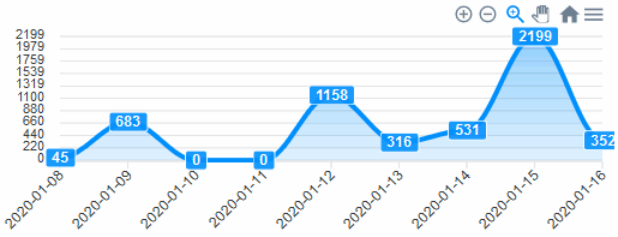
Top Threat Types



#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	970
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	45.234.149.16	TROJAN	110



Top Users by Threats



#	Threat	User	Hits
	lpereira@blockbit.com		3.659
	172.32.250.20		1.387
	172.32.250.27		237
	172.105.76.15		1

Top Users by Malwares

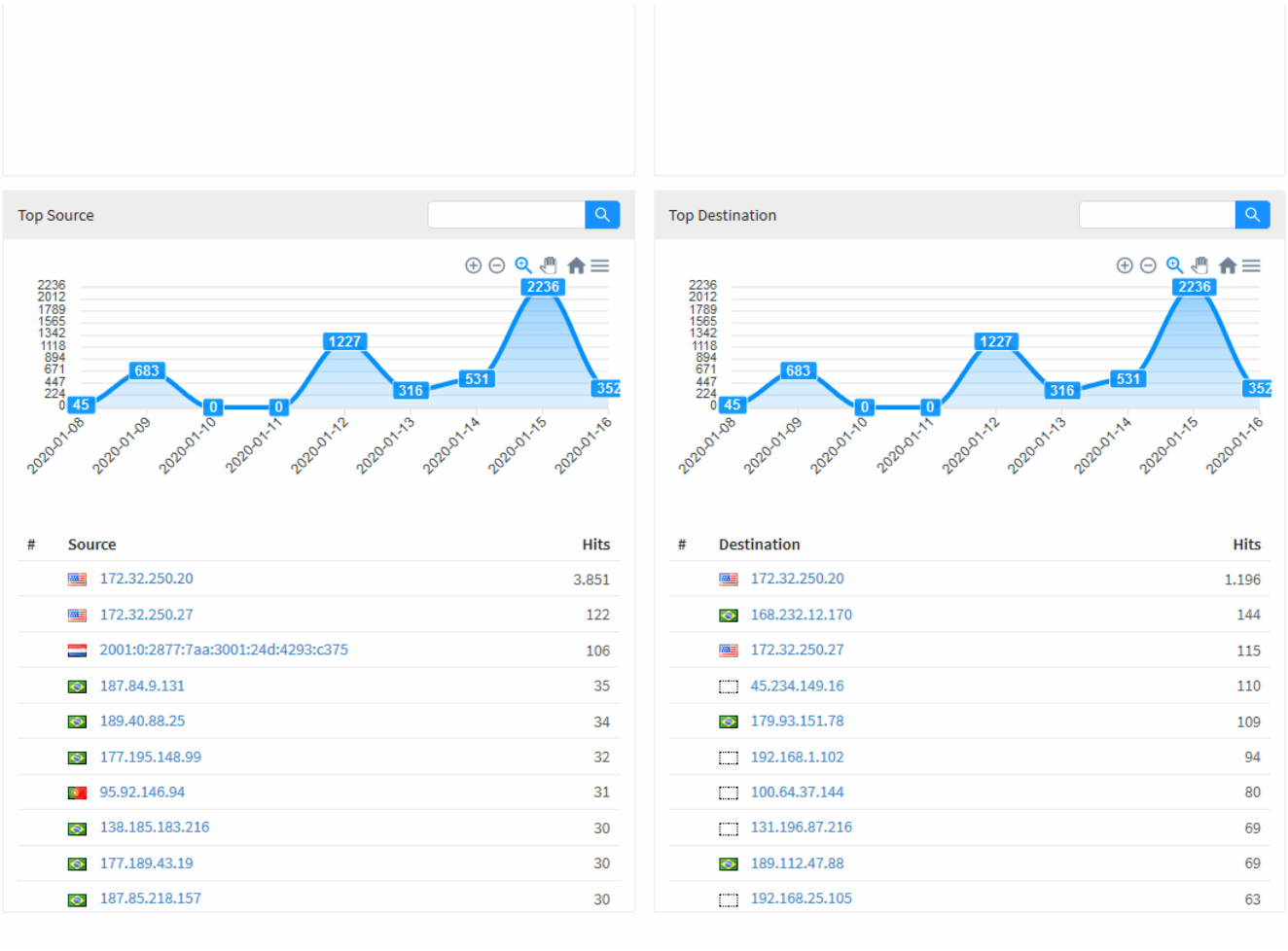
#	Malware	User	Hits
	No Data		

Top Malware

#	Malware	Hits
	No Data	

Top Infected Domains

#	Domain	Hits
	No Data	



Analyzer - Threat Protection

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom in;
- **[ ]:** Its function is to remove the zoom;
- **[ ]:** It serves to make a selection zoom;
- **[ ]:** Serves to move the graph;
- **[ ]:** Reset the graph to the starting position;
- **[ ]:** Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the search **[ ]** button.

Next, we will analyze in detail the components of “Threat Protection”:

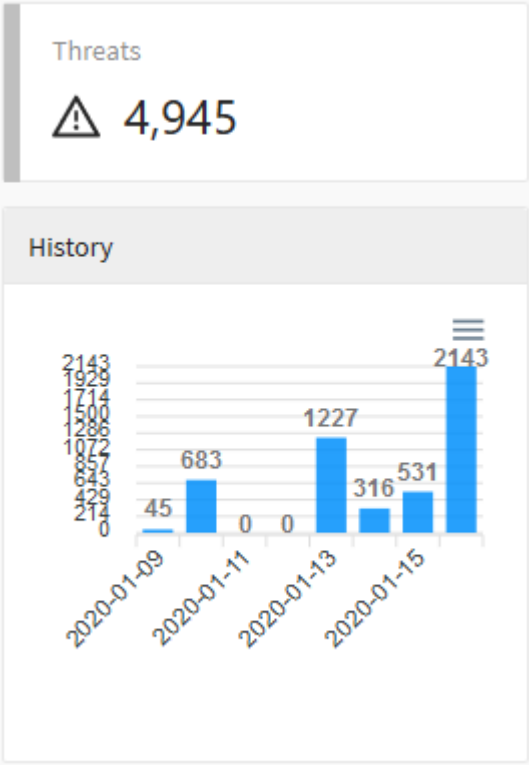
- *Threats* and *History*;
- *Malwares* and *History*;
- *Geolocation*;
- *Impact - High*;
- *Impact - Medium*;
- *Impact - Low*;
- *Malicious IP Classification*;
- *Top Threat Types*;
- *Top Users by Threats*;
- *Top Users by Malware*;

- *Top Malware*;
- *Top Infected Domains*;
- *Top Source*;
- *Top Destination*.

UTM - Threat Protection - Threats and History

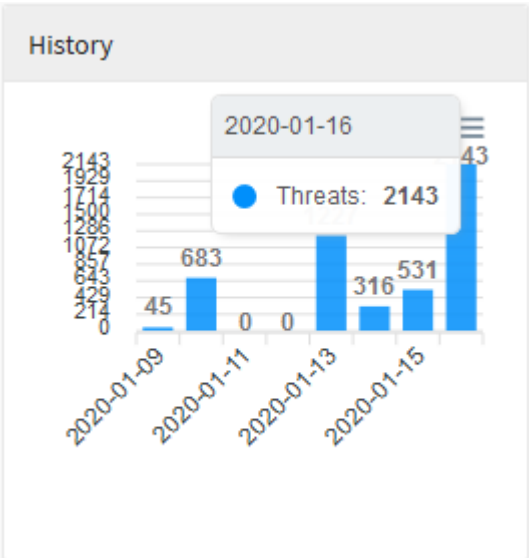
The “Threats” panel displays the total of detected threats. Below, the history is displayed in a linear graph showing the amount of threats detected per day.

For more information about the navigation menu at the top of this graph, check this page.



Threat Protection - *Threats* and *History*

When you hover your mouse over the graph, a summary of the threats for the period is displayed, as shown in the image below:

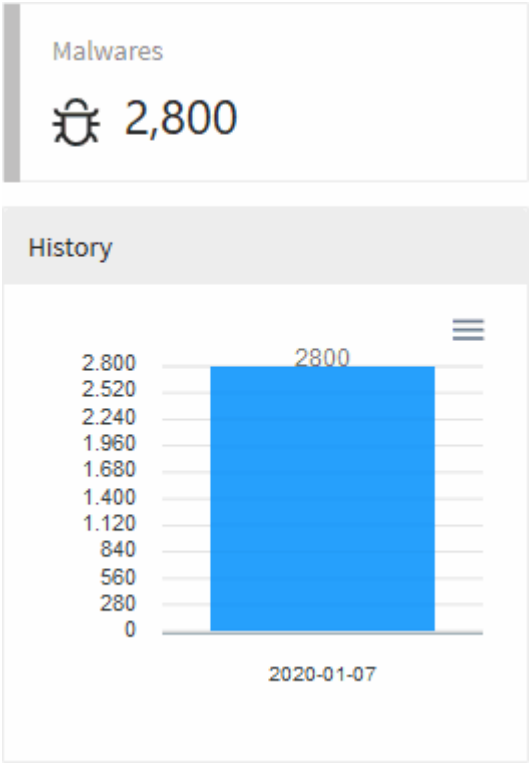


Threat Protection - *History* - Threat Summary

UTM - Threat Protection - Malwares and History

In “Malwares”, a number is displayed totaling the amount of malware detected. Below, the history is displayed in a bar graph showing the amount of threats detected per day.

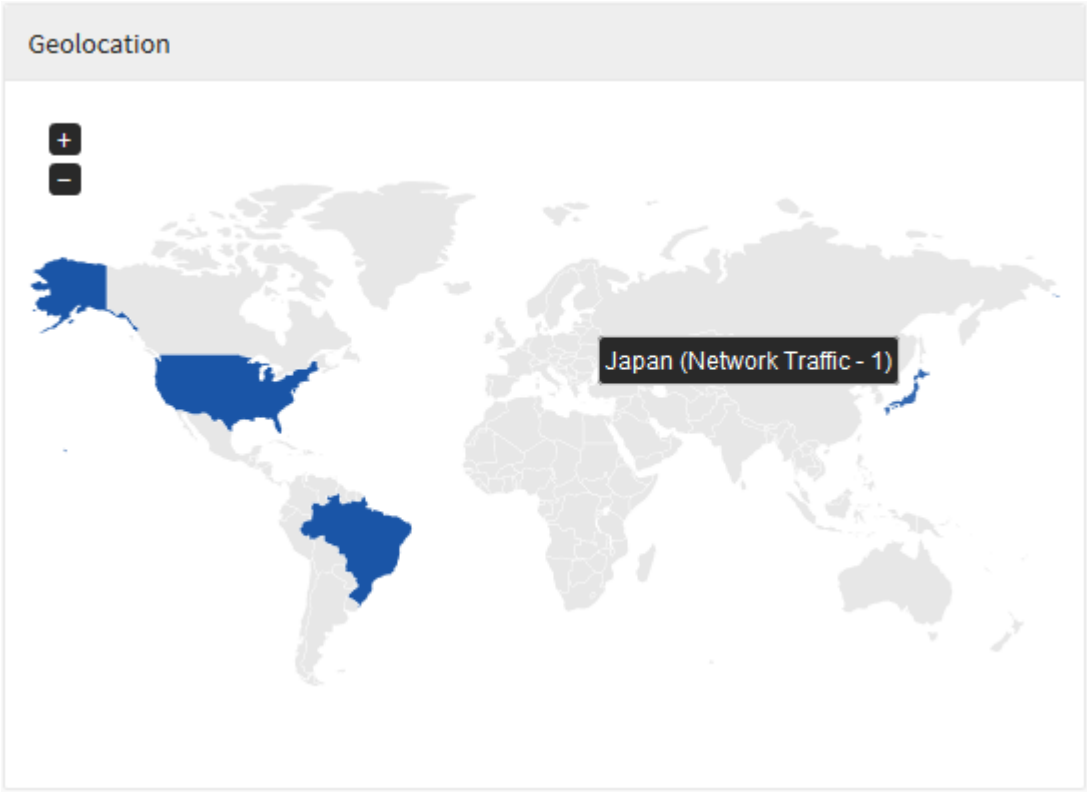
For more information about the navigation menu at the top of this graph, check this page.



Threat Protection - Malware and *History*

UTM - Threat Protection - Geolocation

In “Geolocation” the source of the threats by geolocation is displayed, the global map shows the level of risk through a colored legend. When hovering the mouse over the countries a total number of threats is displayed, when doing the same with the legend it is possible to view an average, in addition, the country for that value is highlighted on the map.

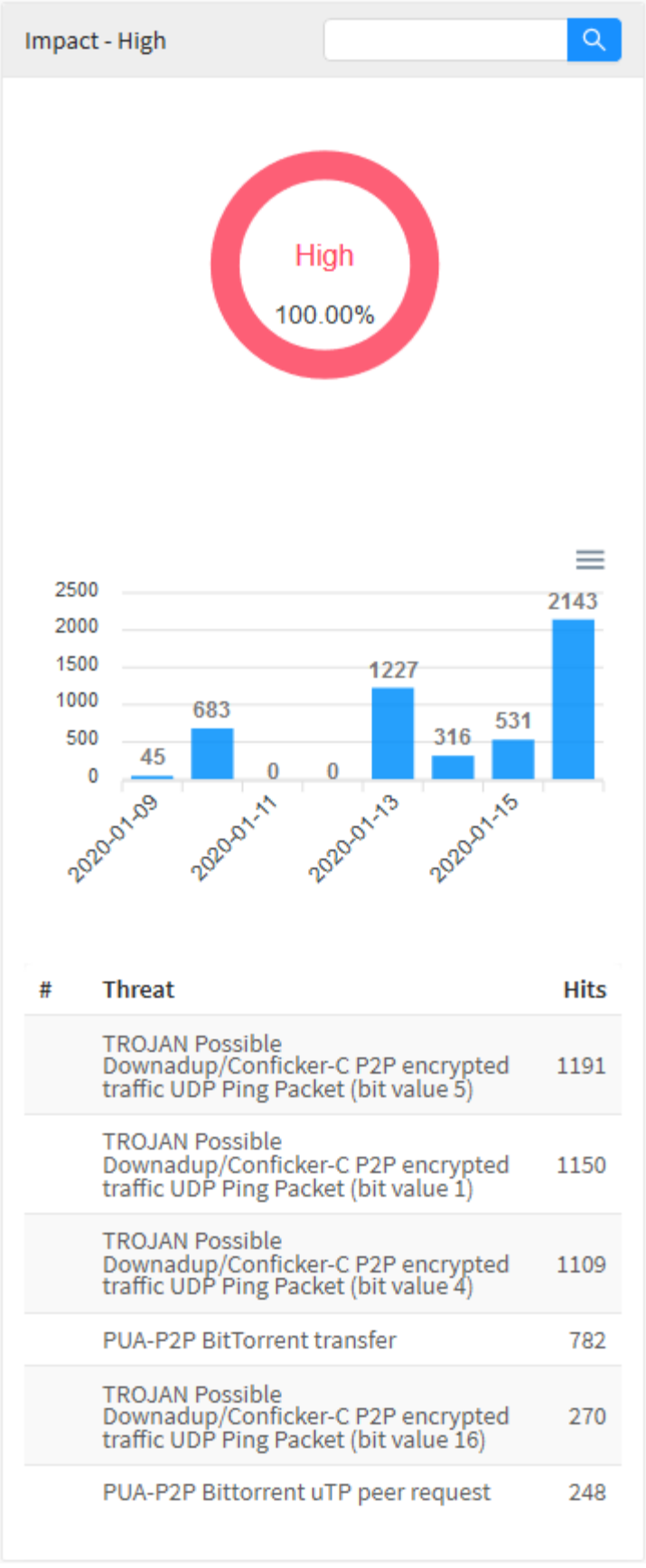


Threat Protection – Geolocation

UTM - Threat Protection - Impact - High

In “Impact - High” we have a donut-shaped chart showing the percentage of high impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring high-impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this page.



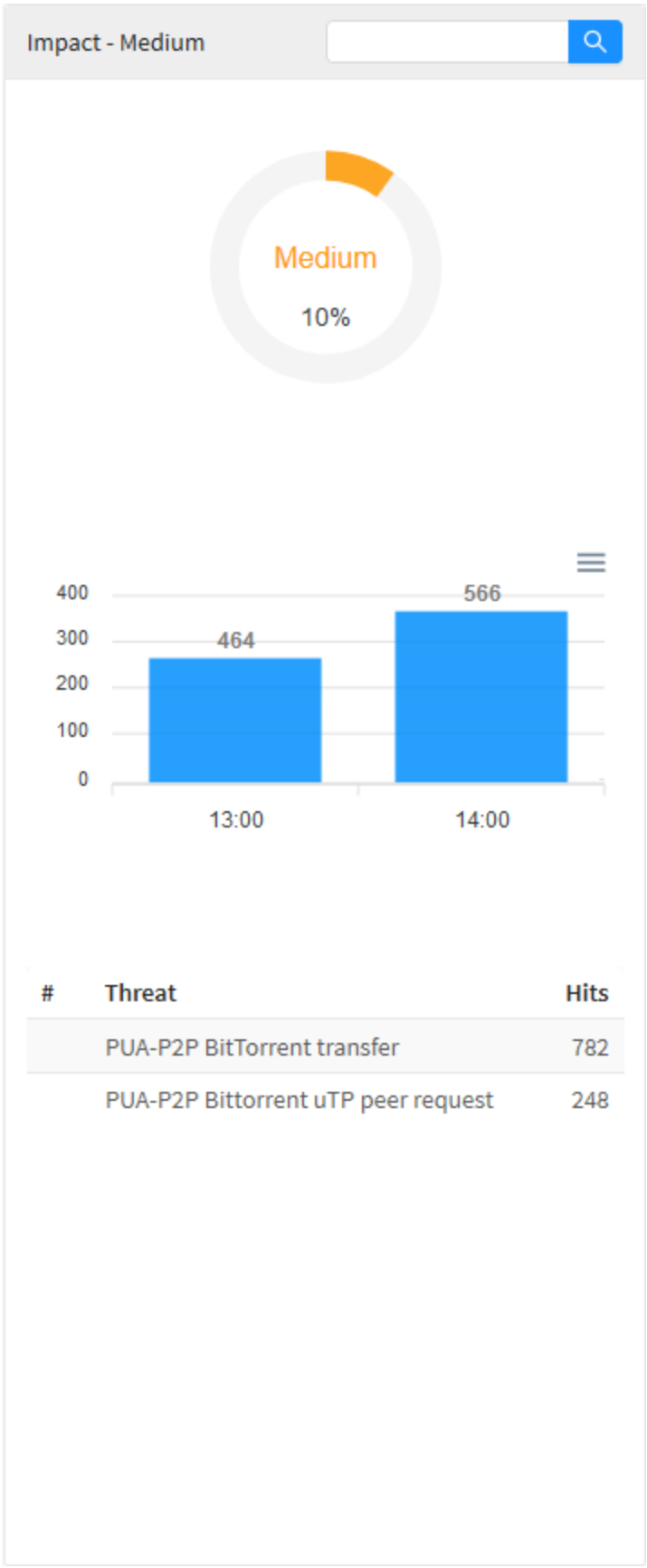
#	Threat	Hits
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	1191
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	1150
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	1109
	PUA-P2P BitTorrent transfer	782
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)	270
	PUA-P2P Bittorrent uTP peer request	248

Threat Protection – Impact High

UTM - Threat Protection - Impact - Medium

In “Impact - Medium” we have a donut-like chart showing the percentage of medium impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring medium impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this page.

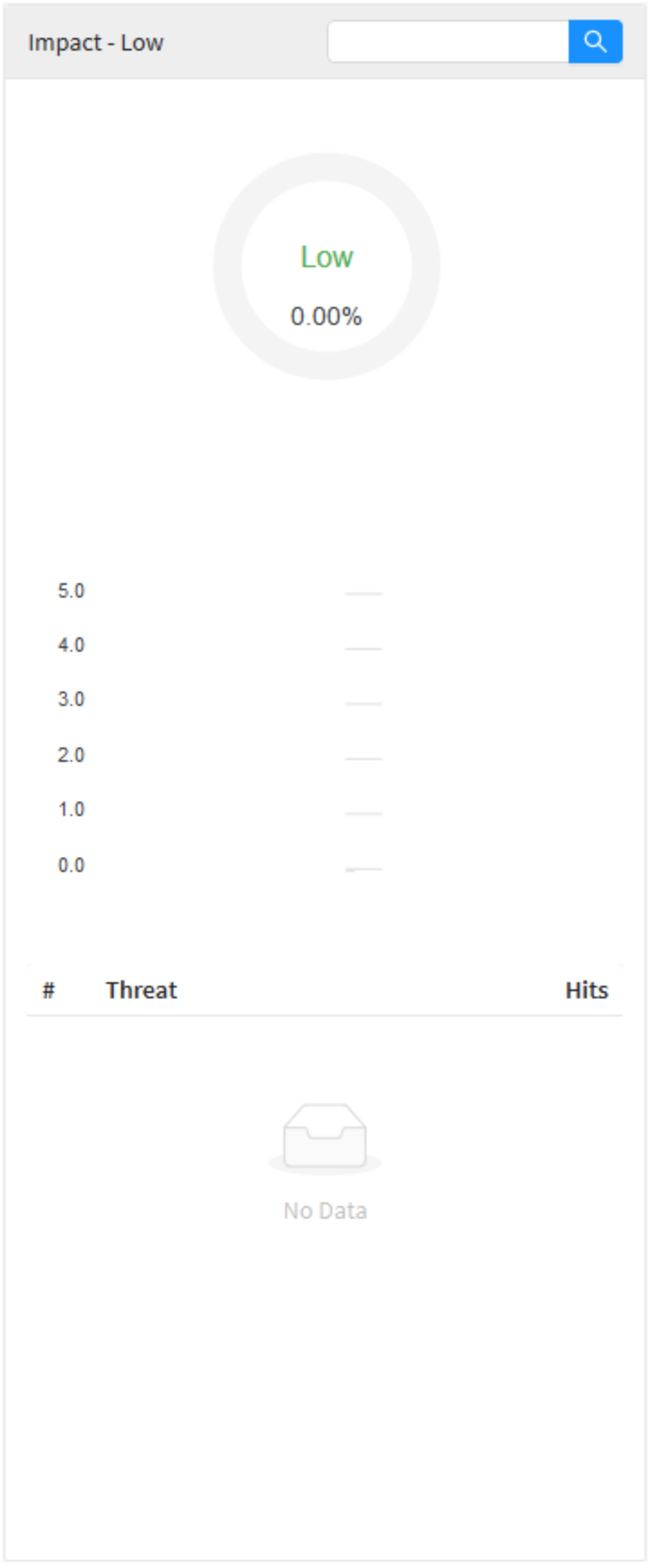


Threat Protection – Impact Medium

UTM - Threat Protection - Impact - Low

In “Impact - Low” we have a donut-shaped chart showing the percentage of low impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring low-impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this page.

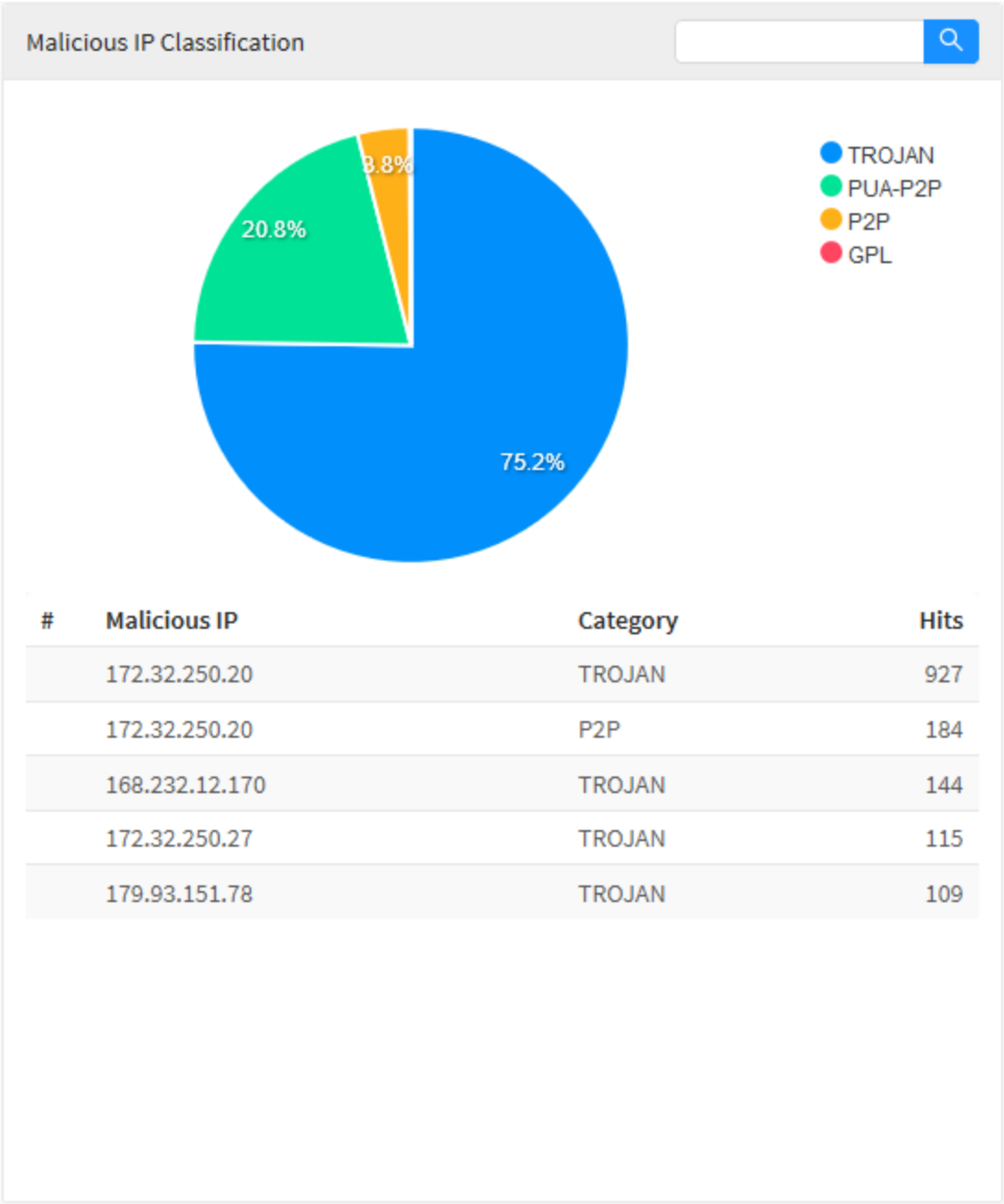


Threat Protection – Impact Low

UTM - Threat Protection - Malicious IP Classification

In “Malicious IP Classification” we have a donut-shaped chart showing the ten most detected categories of Malicious IP alerts on the network, when you hover over each part of the graph or its corresponding text, it will highlight it and display a number with the amount of accesses to this IP category and its corresponding percentage in relation to the other categories. Just below the graph, we have a list of the ten IPs that most accessed these categories ordered by number of accesses.

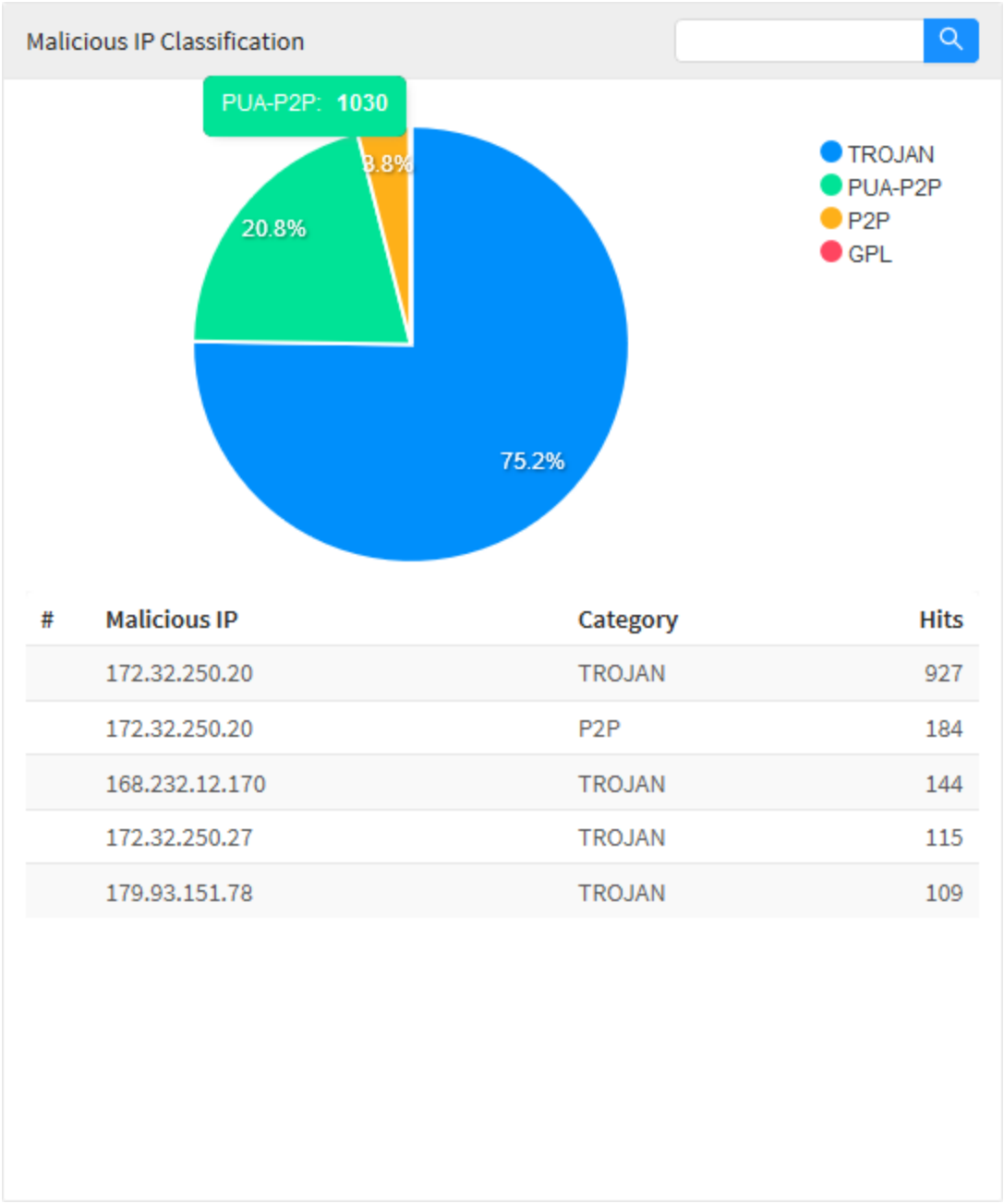
For more information about the navigation menu and the search bar at the top of this graph check this page.



#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	927
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	179.93.151.78	TROJAN	109

Threat Protection – Malicious IP Classification

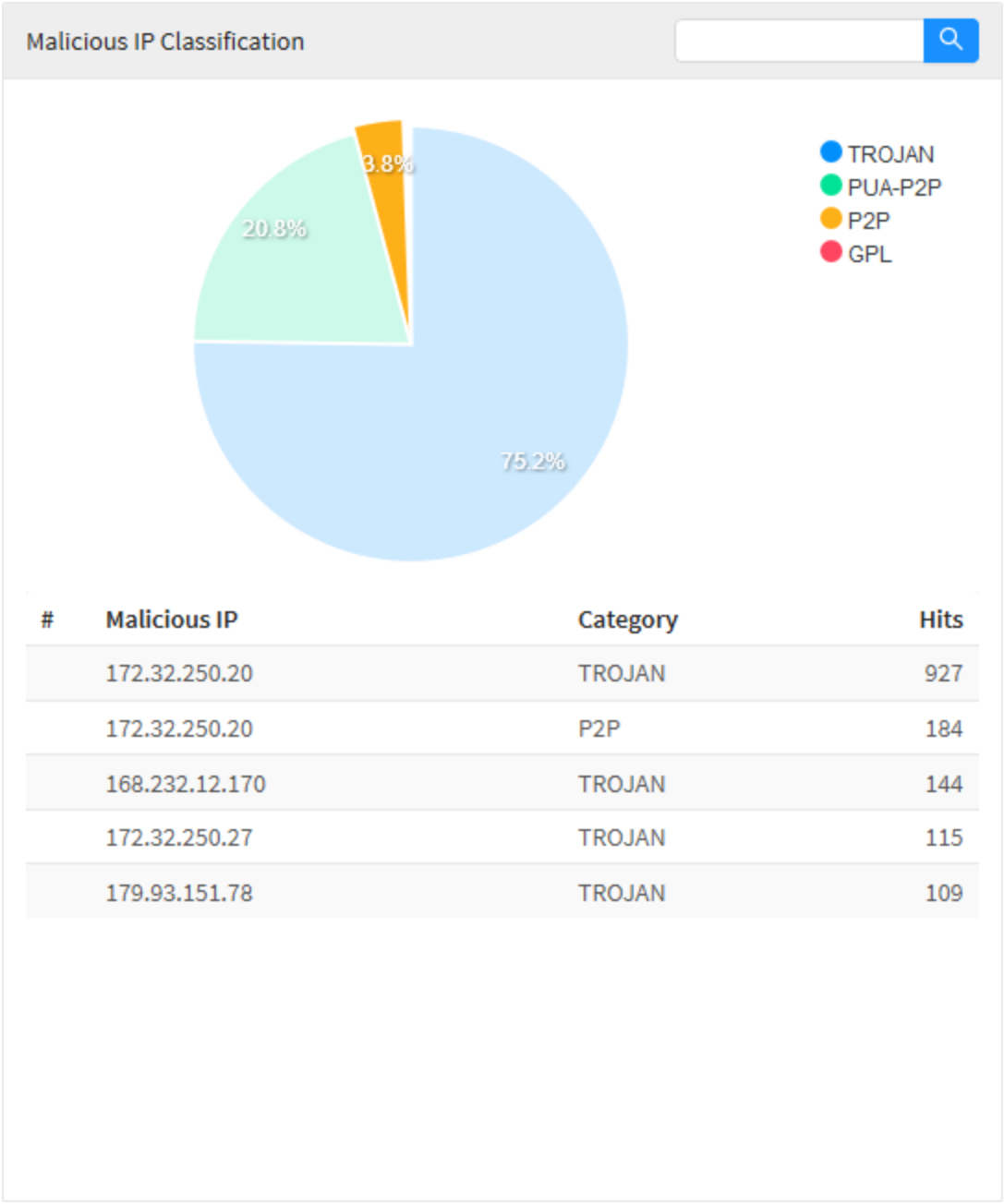
When you hover your mouse over the graph, it will display a number with the amount of malicious IPs, as shown in the image below:



#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	927
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	179.93.151.78	TROJAN	109

Threat Protection – Malicious IP Classification - Summary

When hovering the mouse over the legend, the graphic will be highlighted, as shown below:



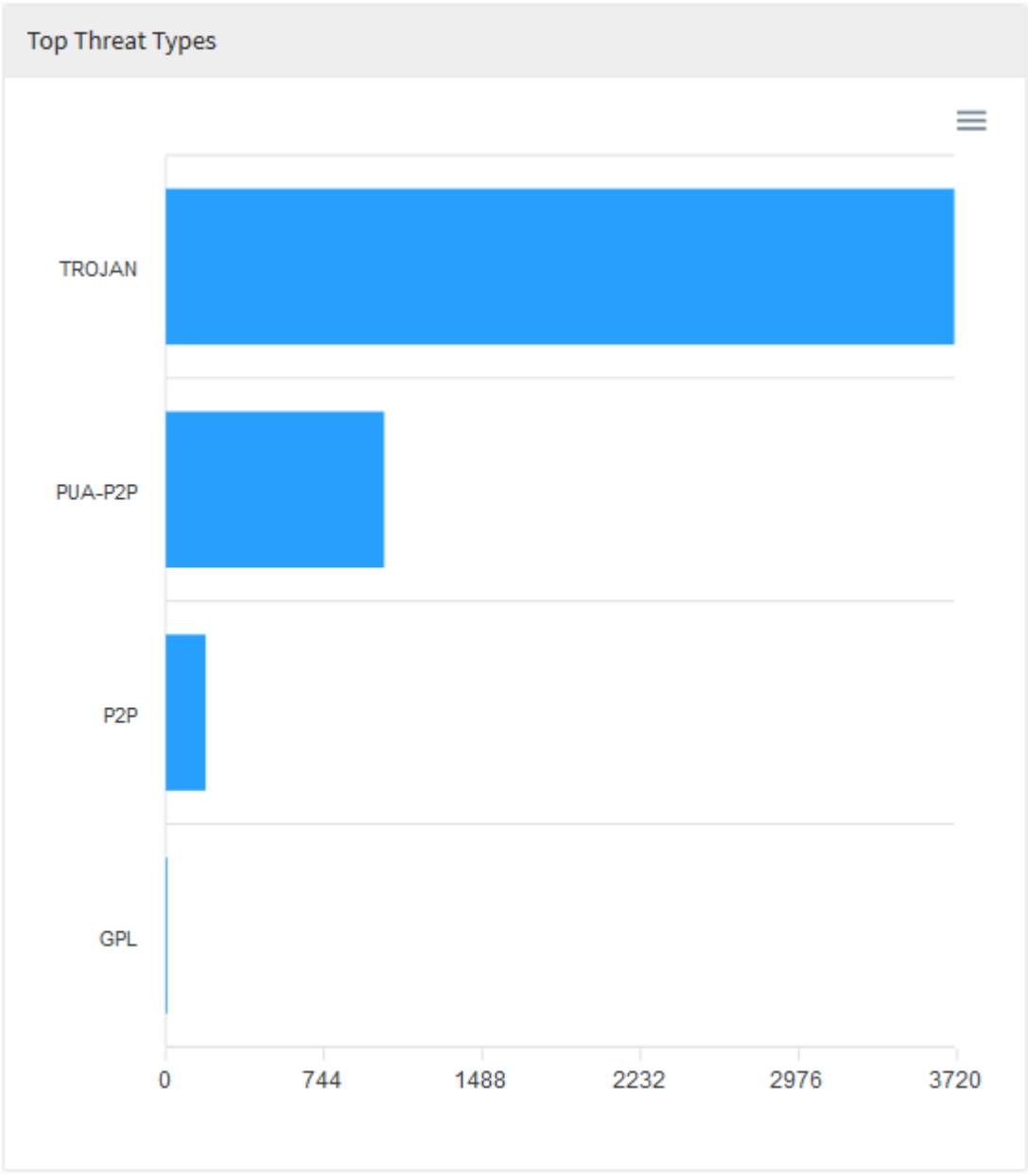
#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	927
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	179.93.151.78	TROJAN	109

Threat Protection – Malicious IP Classification - Summary

UTM - Threat Protection - Top Threat Types

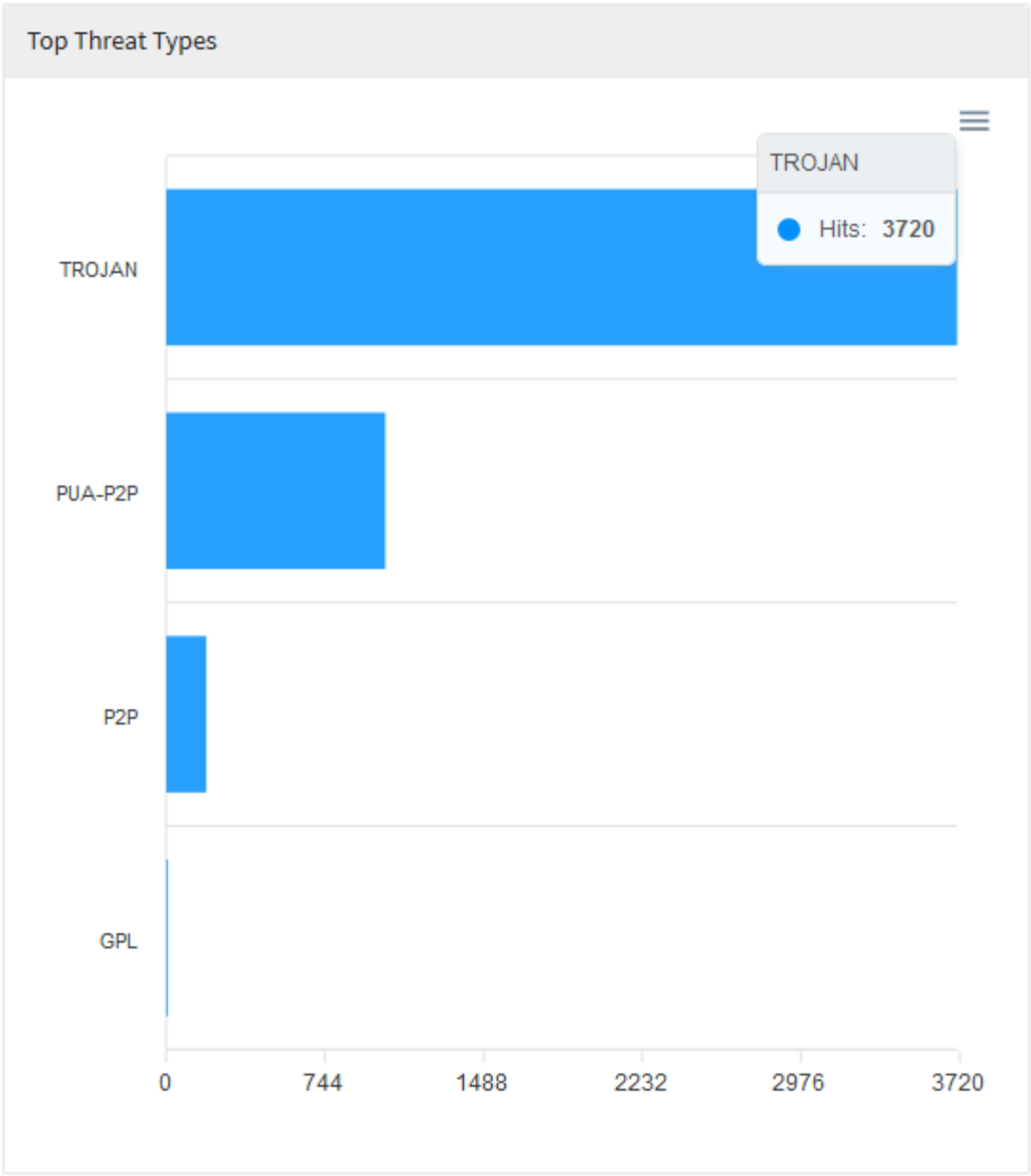
In "Top Threat Types" a bar graph is displayed representing the most recurrent threat types in relation to the number of times they were detected.

For more information about the navigation menu at the top of this graph, check this page.



Threat Protection – Top Threat Types

Hovering the mouse over the graph will show the exact amount of detections:

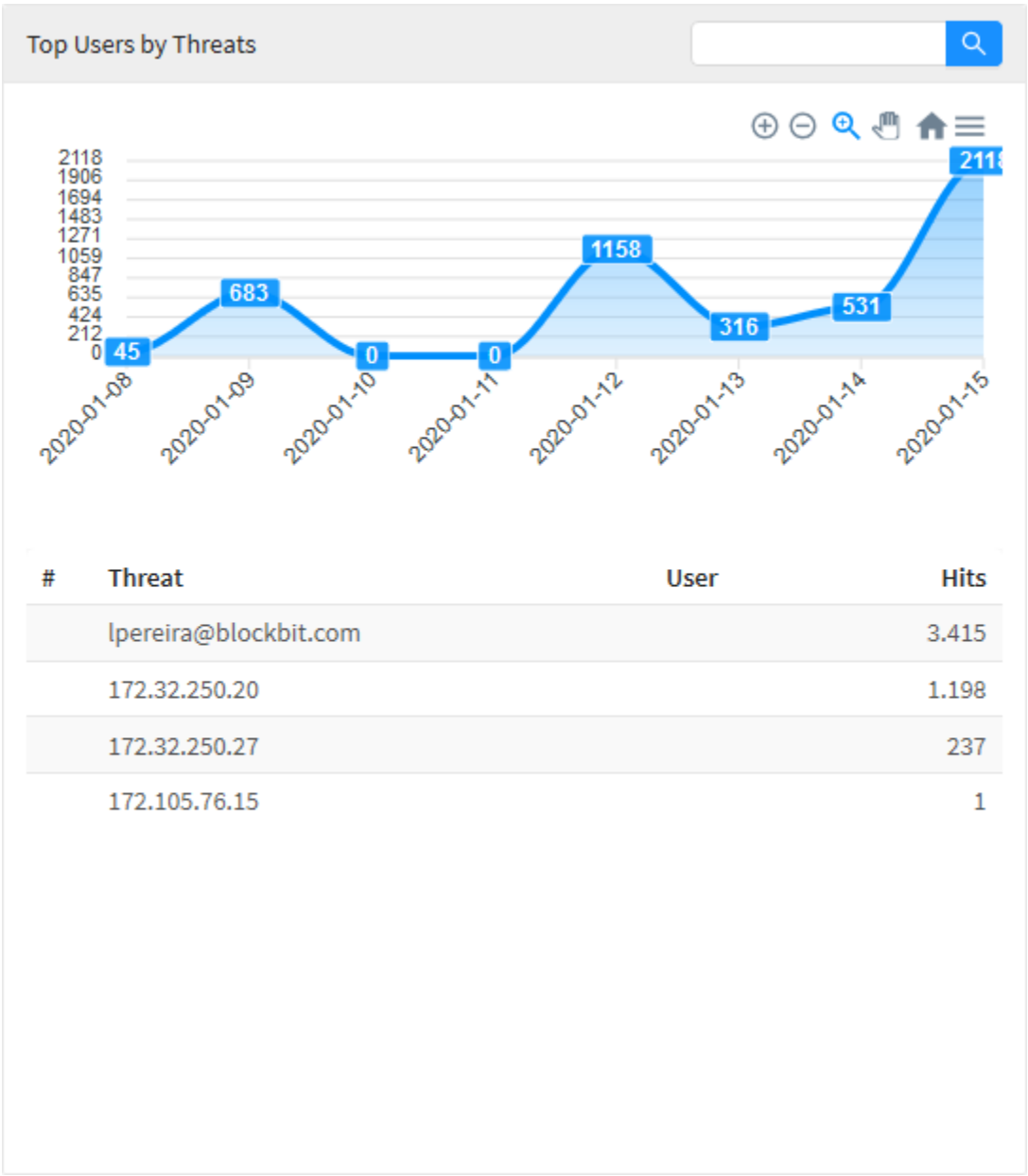


Threat Protection – Top Threat Types - Summary

UTM - Threat Protection - Top Users by Threats

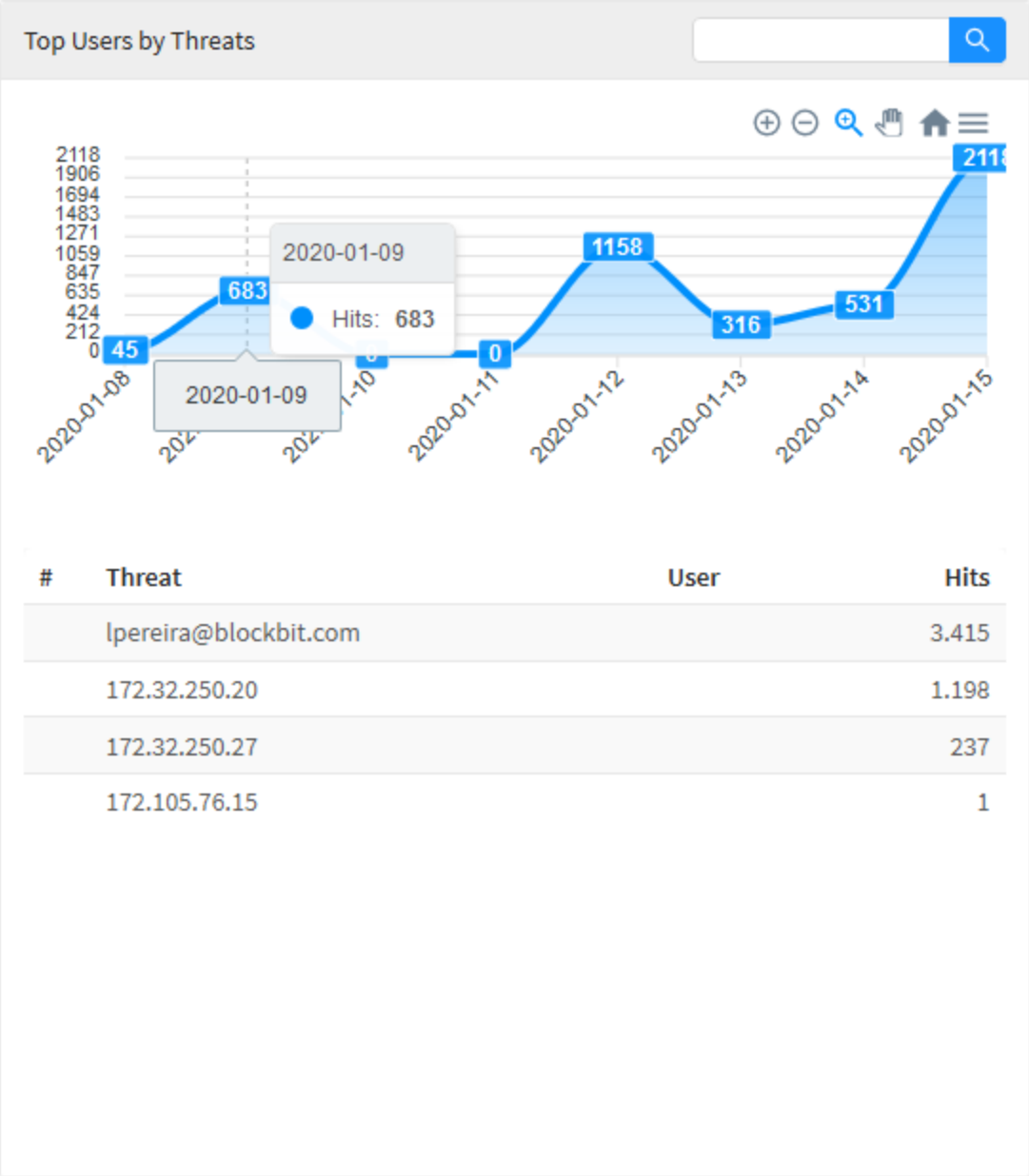
In “Top Users by Threats” we have a line graph showing the amount of threats per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of threats for the selected day. Below the graph, we have a list of the ten users who were most affected by these threats, ordered by the number of accesses.

For more information about the navigation menu and the search bar at the top of this graph check this page.



Threat Protection – Top Users by Threats

When hovering the mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:



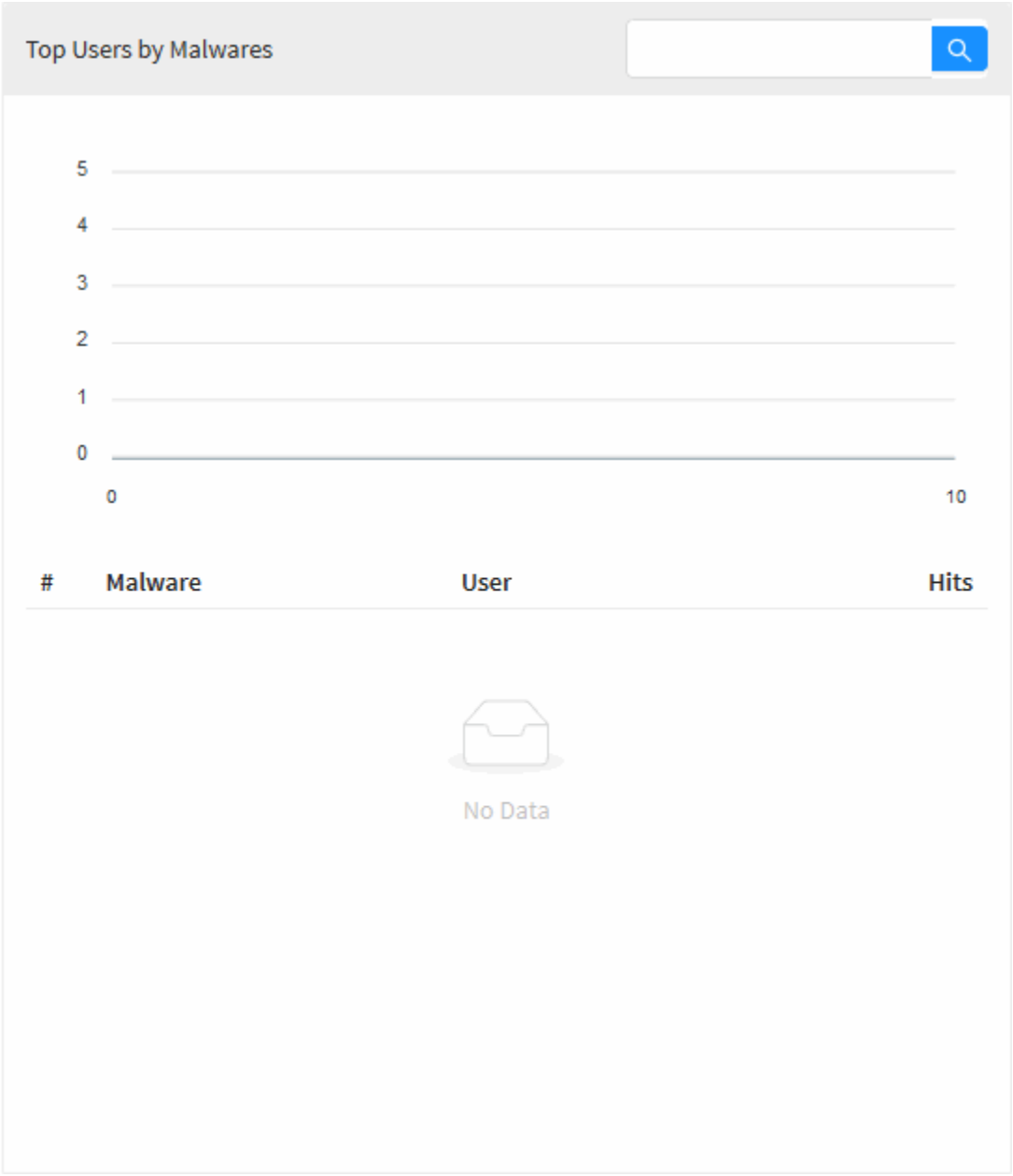
#	Threat	User	Hits
	lpereira@blockbit.com		3.415
	172.32.250.20		1.198
	172.32.250.27		237
	172.105.76.15		1

Threat Protection – Top Users by Threats - Summary

UTM - Threat Protection - Top Users by Malware

In “Top Users by Malware” we have a line graph showing the amount of malware alert per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of threats for the selected day. Just below the graph, we have a list of the ten users who were most affected by malware ordered by the amount of detections. Below the graph, we have a list of the ten users who were most affected by these threats, ordered by the number of accesses. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

For more information about the search bar at the top of this graph check this page.

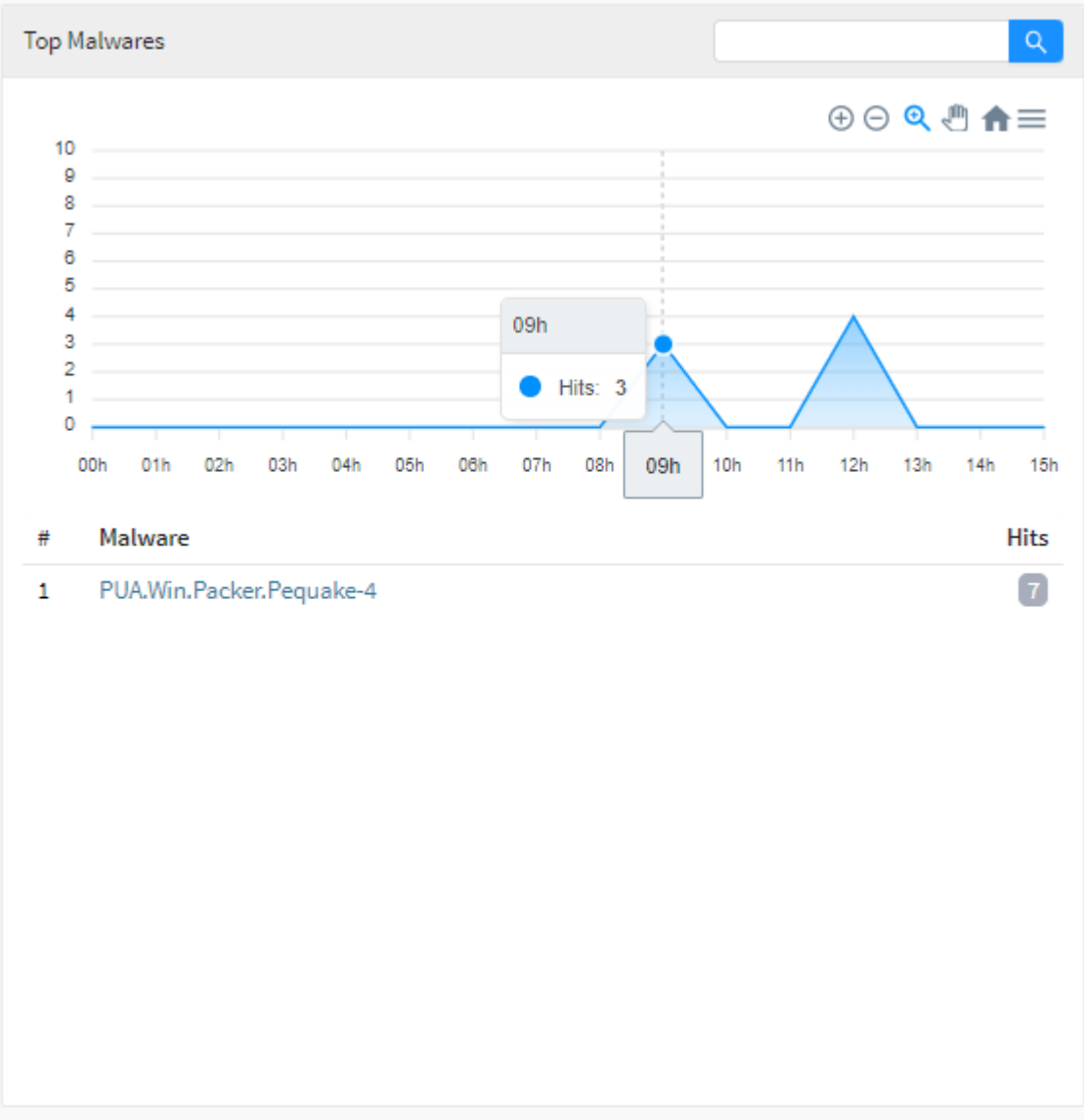


Threat Protection – Top Users by Malware

UTM - Threat Protection - Top Malware

In "Top Malware" we have a line graph showing the amount of malware detected per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of detections for the selected day. Just below the chart, we have a list of the ten most prevalent malware ordered by amount of detections.

For more information about the search bar at the top of this graph check this page.



Threat Protection – Top Malware

UTM - Threat Protection - Top Infected Domains

In “Top Infected Domains” we have a line graph showing the amount of infected domains detected per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of detections for the selected day. Just below the chart, we have a list of the ten most frequent domains ordered by amount of detections.

For more information about the search bar at the top of this graph check this page.

Threat Protection – Top Infected Sites

UTM - Threat Protection - Top Source

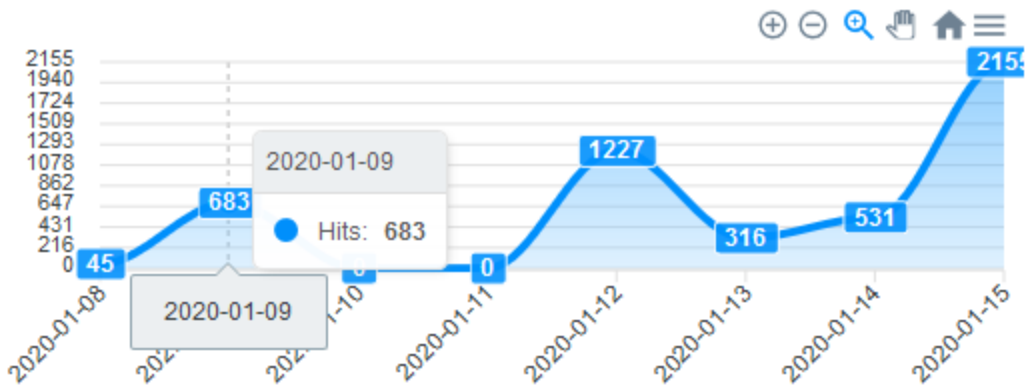
In “Top Source” a line graph is displayed representing the ten most recurrent threat sources in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten sources previously mentioned, which are classified in order of the highest amount of accesses. When you click on one of the IPs or one of the categories, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view regarding the selected threat source.

For more information about the navigation menu and the search bar at the top of this graph check this page.

Threat Protection – Top Source

When you hover your mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:

Top Source



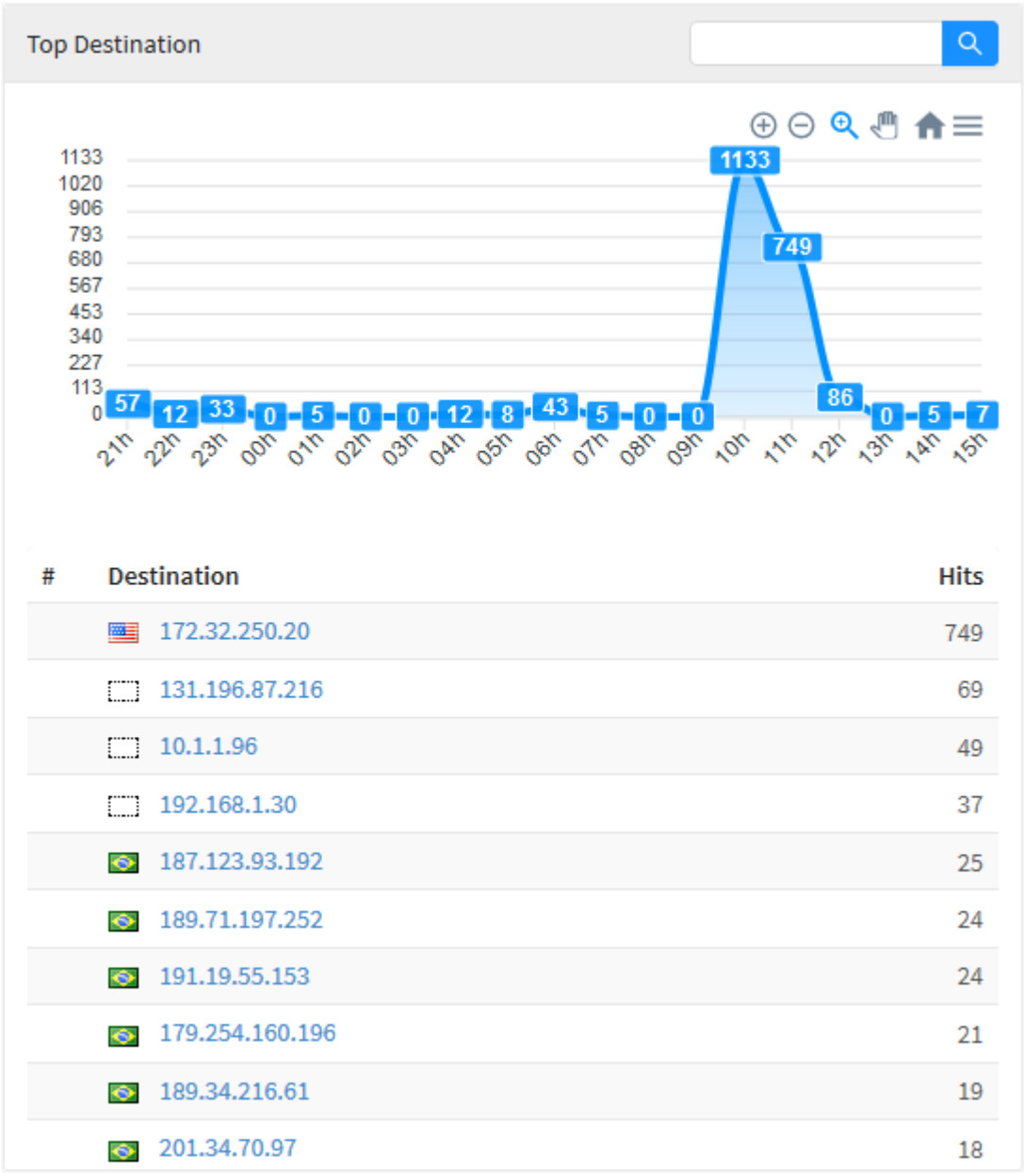
#	Source	Hits
	172.32.250.20	3.461
	172.32.250.27	122
	2001:0:2877:7aa:3001:24d:4293:c375	106
	187.84.9.131	35
	189.40.88.25	34
	177.195.148.99	32
	95.92.146.94	31
	138.185.183.216	30
	177.189.43.19	30
	187.85.218.157	30

Threat Protection – Top Source - Summary

UTM - Threat Protection - Top Destination

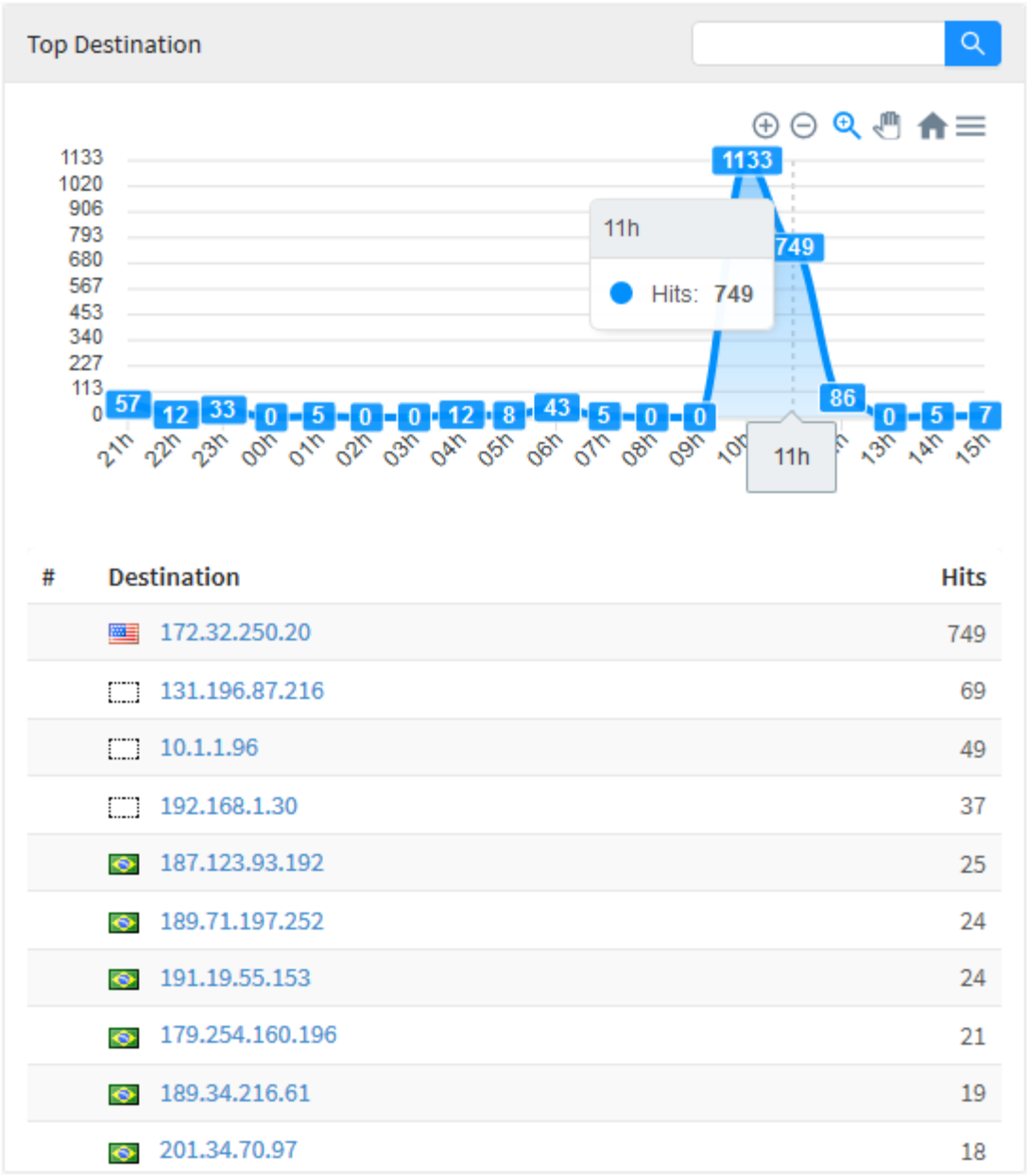
In “Top Destination” a graphic is displayed representing the ten most recurring threat destinations in relation to the previously specified period of time, when hovering over the graphic it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten destinations previously mentioned and these are classified in order of the highest amount of accesses. When clicking on one of the IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected threat source.

For more information about the navigation menu and the search bar at the top of this graph check this page.



Threat Protection – Top Destination

When hovering the mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:

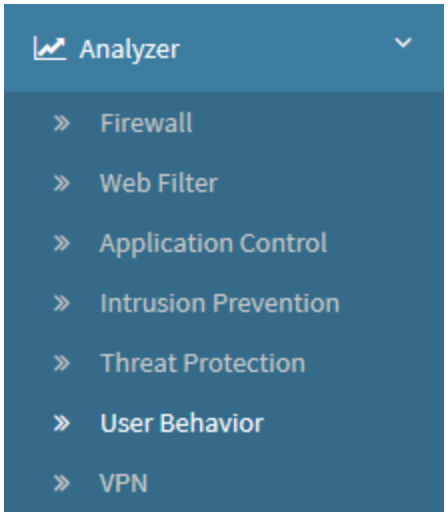


#	Destination	Hits
	172.32.250.20	749
	131.196.87.216	69
	10.1.1.96	49
	192.168.1.30	37
	187.123.93.192	25
	189.71.197.252	24
	191.19.55.153	24
	179.254.160.196	21
	189.34.216.61	19
	201.34.70.97	18

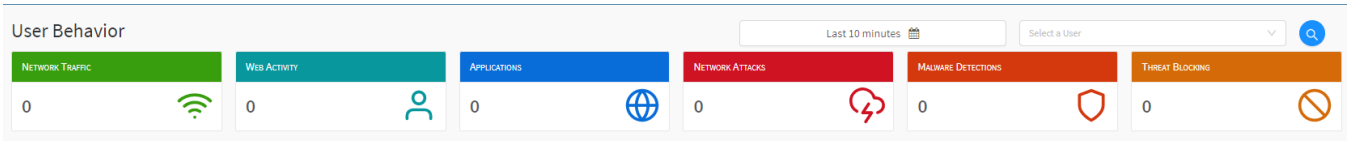
Threat Protection – Top Destination - Summary

UTM - User Behavior

To access the reports available in "User Behavior", click on the "Analysis" icon located on the left side, a dropdown menu will be displayed, select the option "User Behavior".



User Behavior



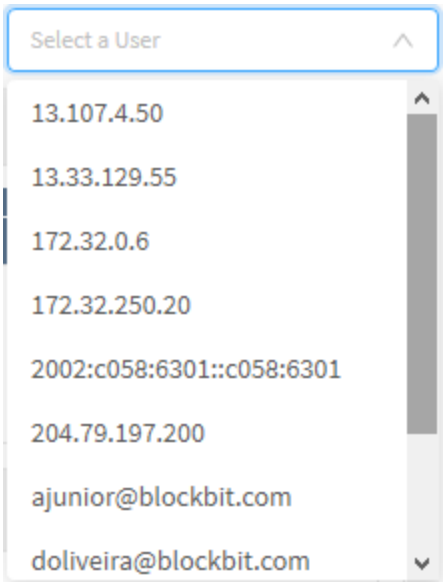
The “User Behavior” report is a summary of the behavior of a given user of a device, informing the user's IP, machine's hostname, the Operational System in use and a general classification of the threats (as placed on "Top 10"), making the extraction of a report from within a specific period of time, possible. The provided reports are a summary of the previously mentioned set of information, but being applied specific to a target user.

To generate a new report, it will be necessary to select the desired device, then the user to be analyzed and finally, to determine a date. Once these three data are selected, the reports will be generated.

Locate the checkbox that is positioned at the top right of the screen, as shown below:

User Behavior - Selection box

In the "Select a User" checkbox, all users of the previously selected device will be listed, select the desired user.

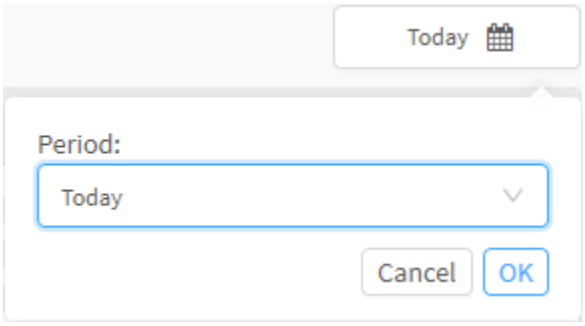


Selecting the user

Finally, the date selection box aims to allow more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



Date Selection

To close this window, click **[** Cancel **]** button or, after selecting the desired date, click **[** OK **]**;

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** Its function is to zoom;
- **[ ]:** Its function is to remove the zoom;

- []: It serves to make a selection zoom;
- []: Serves to move the graph;
- []: Reset the graph to the starting position;
- []: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the [] button.

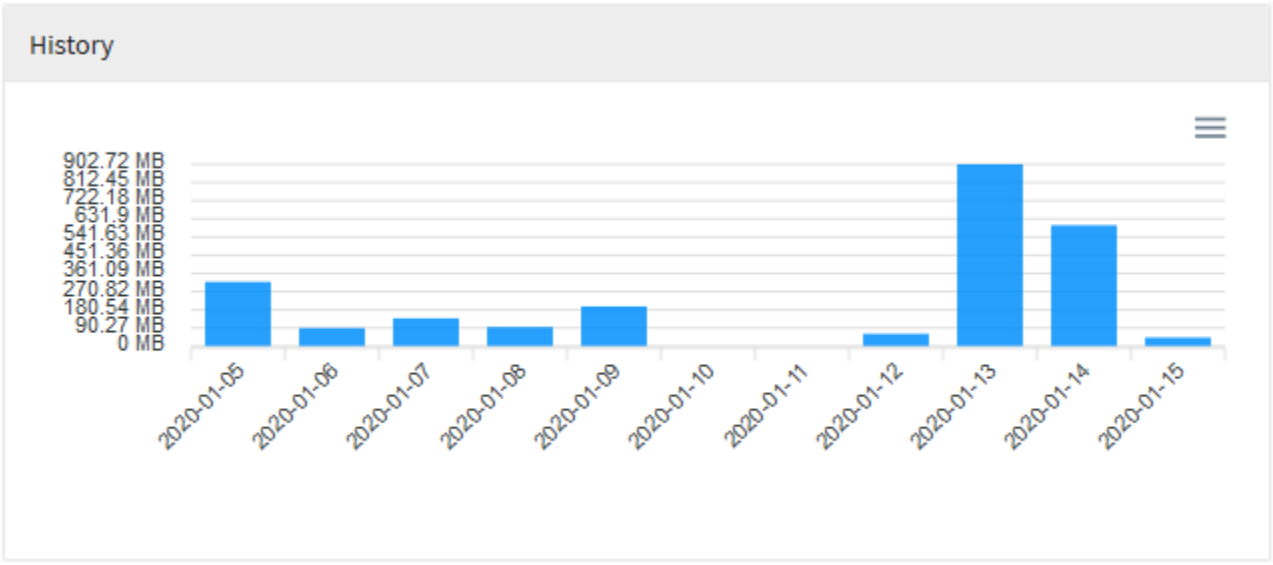
Below, we will analyze each of these reports in detail:

- *History*;
- *Analysis Panel*;
- *Geolocation Information*.

UTM - User Behavior - History

In “History” a vertical bar graph is displayed showing the traffic consumption in Megabytes in relation to the pre-selected days, the arrow in the middle of the graph represents the average consumption of users in general. Hovering over one of the graph's columns displays the exact amount of traffic in Megabytes for each day.

For more information about the navigation menu at the top of this graph, check this page.



User Behavior - History

UTM - User Behavior - Analysis Panel

In “Analysis Panel” we have a summary of several information cited in the reports previously analyzed, but this time, applied specifically to the user in question.

For more information about the navigation menu at the top of this graph, check this page.

Analysis Panel

Network Traffic

Total Traffic

2.37 GB

Top Services

#	Services	Traffic
1	https	1.08 GB
2	admin	548.79 MB
3	ssh	548.9 MB
4	http	4.06 MB
5	rdesktop	221.56 MB

Top Source

#	Source	Traffic
1	172.32.250.20	48.74 KB
2	172.16.13.246	123 Bytes
3	172.16.102.130	81 Bytes
4	192.168.254.252	43 Bytes
5	172.16.12.27	30 Bytes

Top Destination

#	Destination	Hits
1	172.16.13.245	2.916
2	172.16.13.246	2.502
3	172.16.12.171	1.063
4	172.31.0.50	558
5	172.16.13.57	485

Policy Usage

Policy Tags

w SSL

Top Profiles

#	Policies	Hits
1	Default (Allow) (Wifi)	24.647
2	Default (Allow) (Wifi) (Copy)	12.246
3	SMB	5.412
4	FORWARD LOCAL	3.962
5	Content Filtering (Wifi)	3.138

Application Usage

Total Application

1.74 KB

Top Applications

#	Applications	Hits
1	CDN - Content Delivery Network	1.043
2	Microsoft Update	547
3	HTTP	50
4	Google API SSL	48
5	MSN	18

Web Usage

Total Traffic

0

Allowed Sites

0

Denied Sites

0

Top Categories

#	Categories	Hits
1	Information Technology	1.628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination

#	Ip	Hits
1	2.23.98.145	476
2	201.0.217.42	449
3	13.107.4.50	273
4	52.114.142.2	117
5	191.252.51.215	111

THREAT PROTECTION

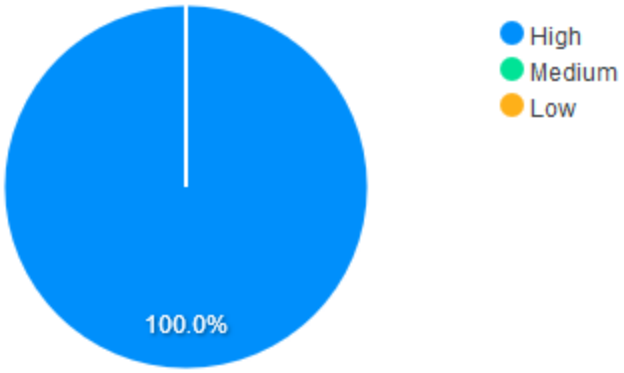
Total Threats

1,198

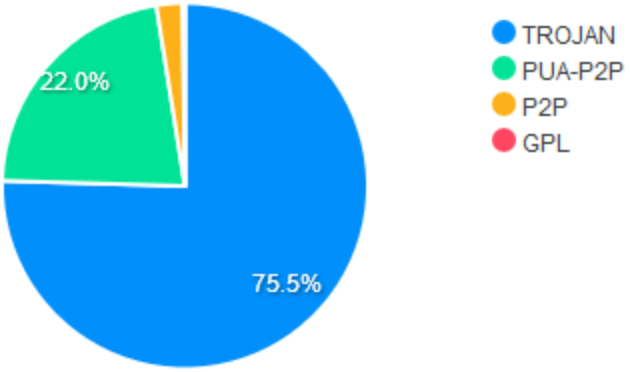
Total Malwares

0

Impacts



Malicious IP Classification



Top Threats

#	Threats	Hits
1	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275

4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

Top Malwares

#	Malwares	Hits

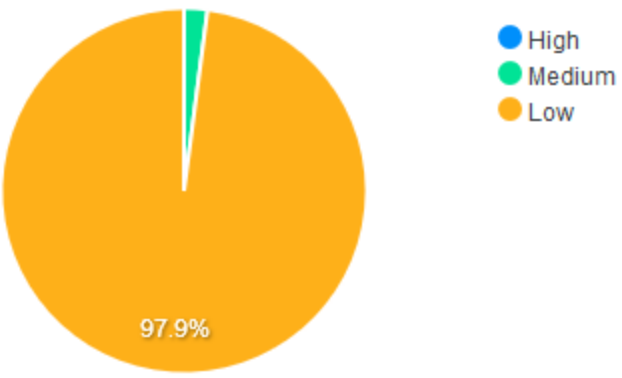
No Data

INTRUSION PREVENTION

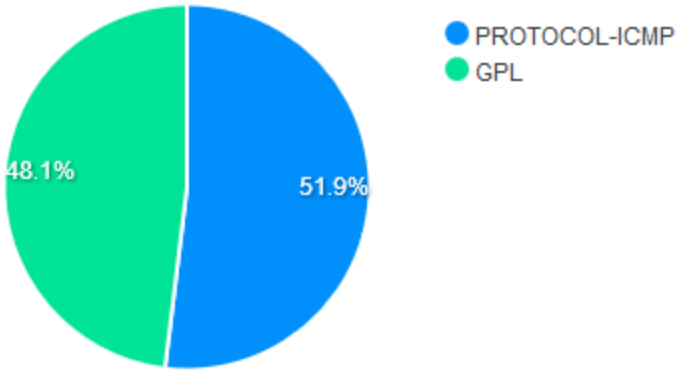
Total Alerts

100,666

Impacts



Intrusion Protection



Top Alerts

#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.511
4	PROTOCOL-ICMP Destination Unreachable Host Unreachable	8.511
5	GPL ICMP_INFO PING	2.081

User Behavior - Analysis Panel

UTM - User Behavior - Analysis Panel - Network Traffic

Below “Network Traffic” we have:

“Total Traffic”, displaying the user's total traffic in Gigabytes, in “Top Services” a list is displayed with the 10 most used services by the user in question, “Top source” shows the largest sources of user access and “Top Destination ”a list of IPs of the destinations most accessed by the user.

Network Traffic

Total Traffic

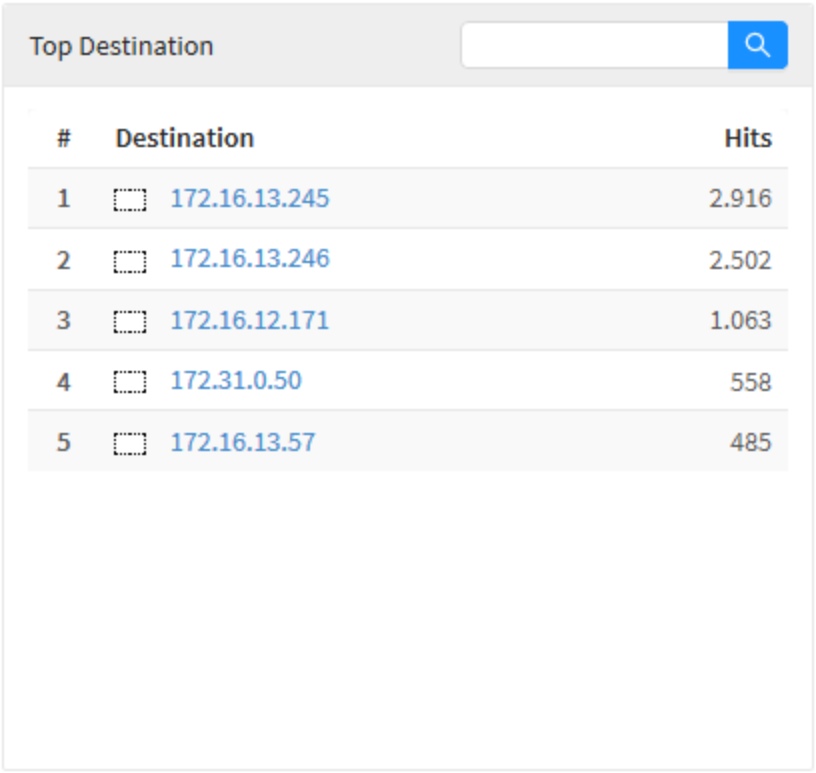
2.37 GB

Top Services

#	Services	Traffic
1	https	1.08 GB
2	admin	548.79 MB
3	ssh	548.9 MB
4	http	4.06 MB
5	rdesktop	221.56 MB

Top Source

#	Source	Traffic
1	172.32.250.20	48.74 KB
2	172.16.13.246	123 Bytes
3	172.16.102.130	81 Bytes
4	192.168.254.252	43 Bytes
5	172.16.12.27	30 Bytes

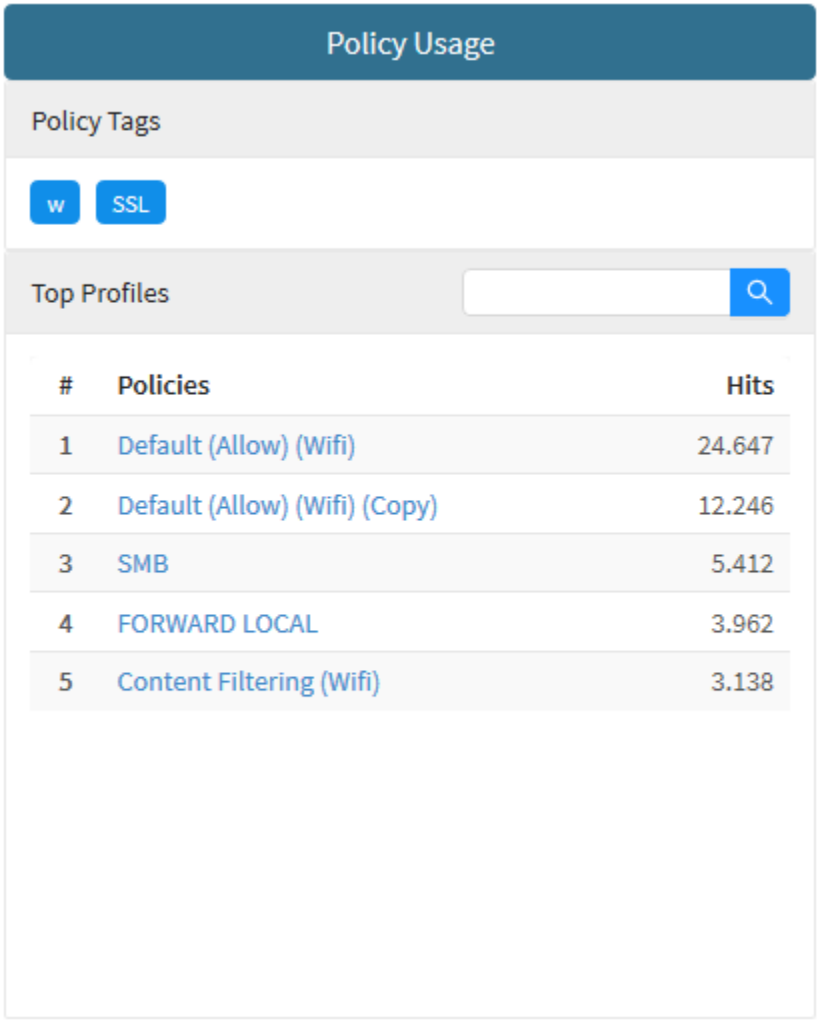


User Behavior - Analysis Panel - Network Traffic

UTM - User Behavior - Analysis Panel - Policy Usage

In “Policy Usage” we have:

“Policy Tags” that shows which Policy Tags were most applied to that user, in “Top Policies” we have the most applied policies for that specific user.

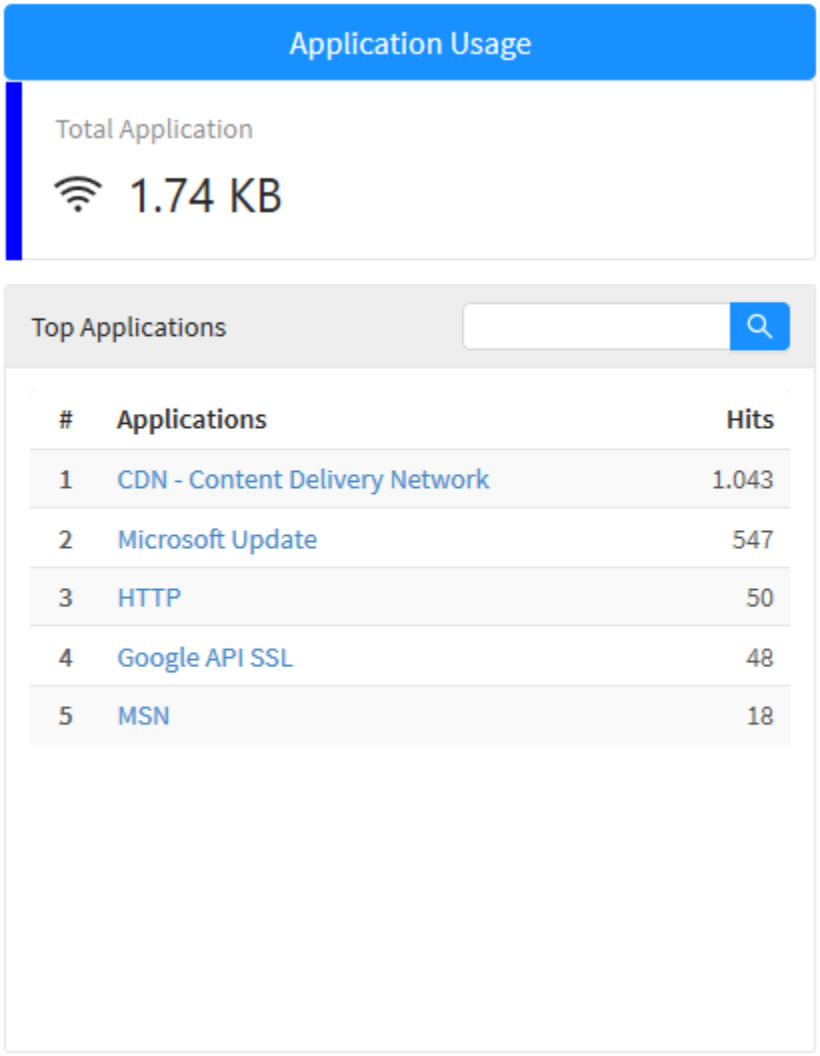


Analysis Panel - Policy Usage

UTM - User Behavior - Analysis Panel - Application Usage

In “Application Usage” we have:

“Total Applications” mentions the total number of applications used by the user and “Total Application” which serves to demonstrate the most used applications by the user and the amount of access made to them.



Analysis Panel - Application Usage

UTM - User Behavior - Analysis Panel - Web Usage

In “Web Usage” we have:

“Total Traffic” showing a total of the user's network traffic, “Allowed Sites” showing the total number of accesses to permitted sites made by the user, “Denied Sites” showing the total accesses to refused sites made by the user, “Top Categories” a list of user accesses by category and finally, in “Top destination” a list of user accesses by destination showing the IP and amount of accesses to it.

Web Usage

Total Traffic

0

Allowed Sites

0

Denied Sites

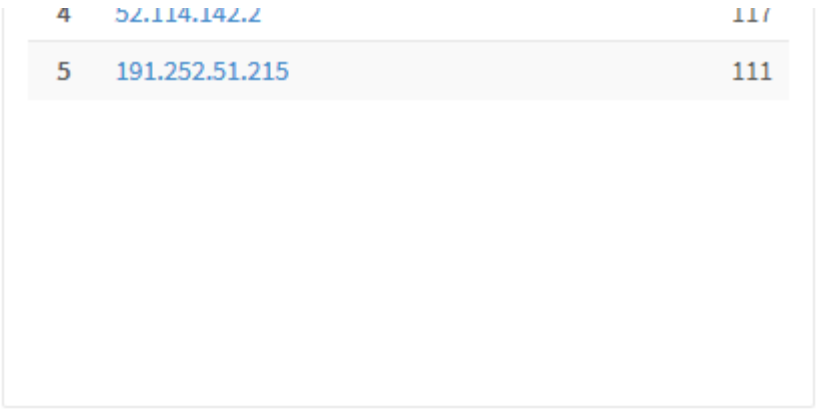
0

Top Categories

#	Categories	Hits
1	Information Technology	1.628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination

#	Ip	Hits
1	2.23.98.145	476
2	201.0.217.42	449
3	13.107.4.50	273



Analysis Panel - Web Usage

UTM - User Behavior - Analysis Panel - Threat Protection

In “Threat Protection” we have:

“Total Threats” showing the total number of threats, “Total Malwares” shows the total number of malware detected on that user, the “Impacts” chart shows the impact levels of the threats previously mentioned, “Malicious IP Classification” displays a chart showing a summary of the classification of malicious IPs accessed by the user, in the “Top Threats” list the 5 most recurring threats to that user are displayed and the amount of accesses made and in “Top Malware” a list of the 5 most detected malware is displayed on the user in question.

THREAT PROTECTION

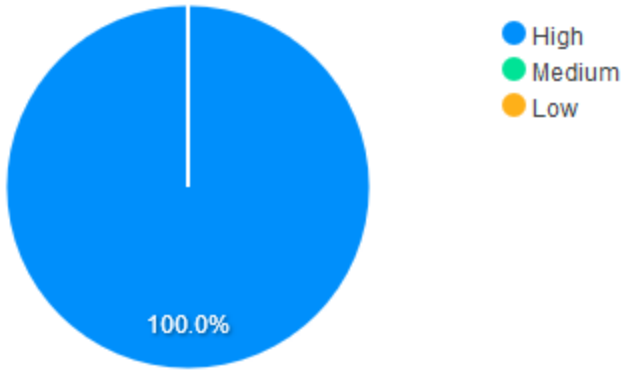
Total Threats

1,198

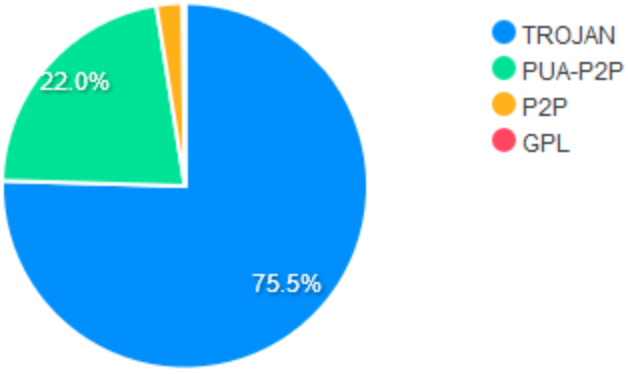
Total Malwares

0

Impacts



Malicious IP Classification



Top Threats

#	Threats	Hits
	TROJAN Possible	

1	Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275
4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

Top Malwares

#	Malwares	Hits

No Data

Analysis Panel - Threat Protection

UTM - User Behavior - Analysis Panel - Intrusion Prevention

In “Intrusion Prevention” we have:

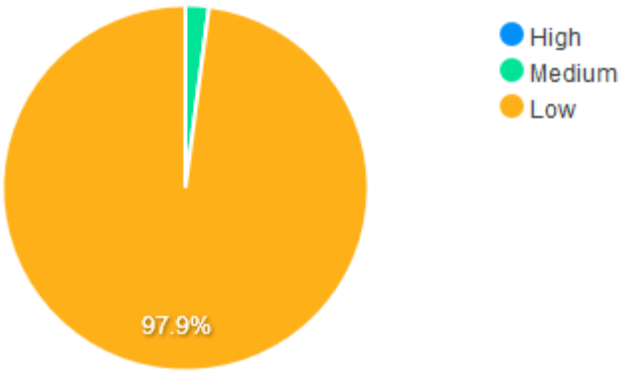
“Total Alerts” showing the total number of alerts for this user, in “Impacts” we have the impact levels of the alerts previously mentioned, “Intrusion Protection” displays a donut chart where it is possible to see the types of intrusions detected by the system and finally, in “Top Alerts” we have a list of the 5 alerts for this user and how many times they occurred.

INTRUSION PREVENTION

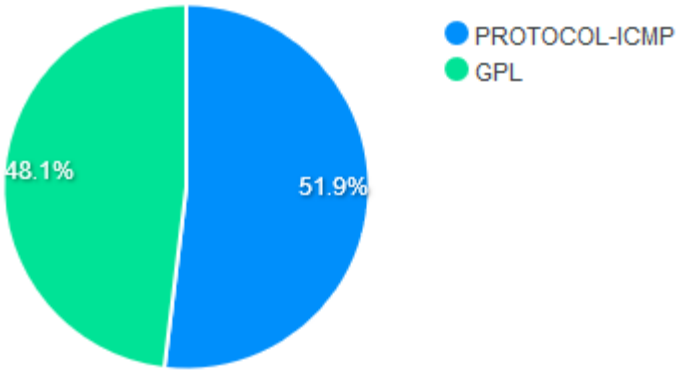
Total Alerts

100,666

Impacts

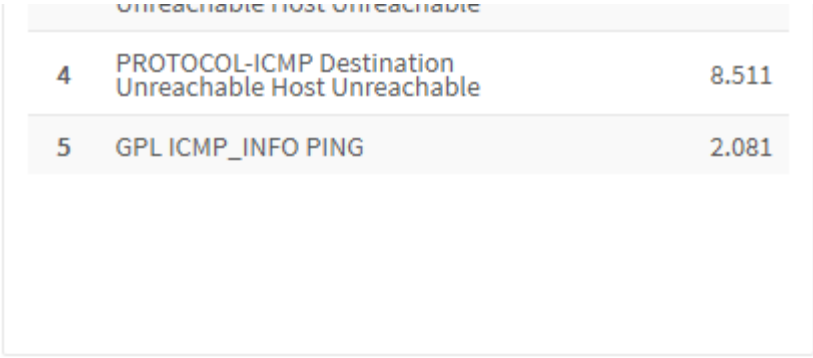


Intrusion Protection



Top Alerts

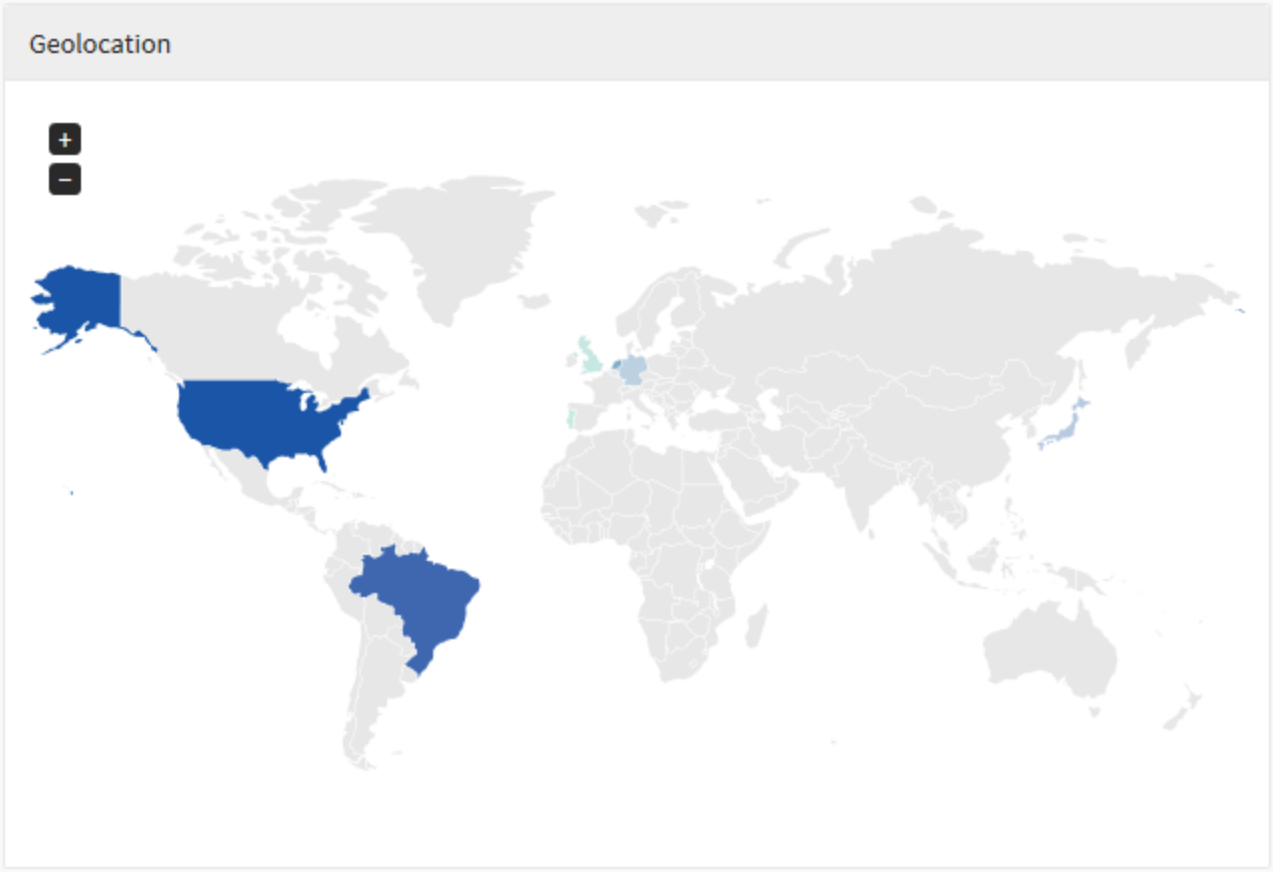
#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.511



Analysis Panel - Intrusion Prevention

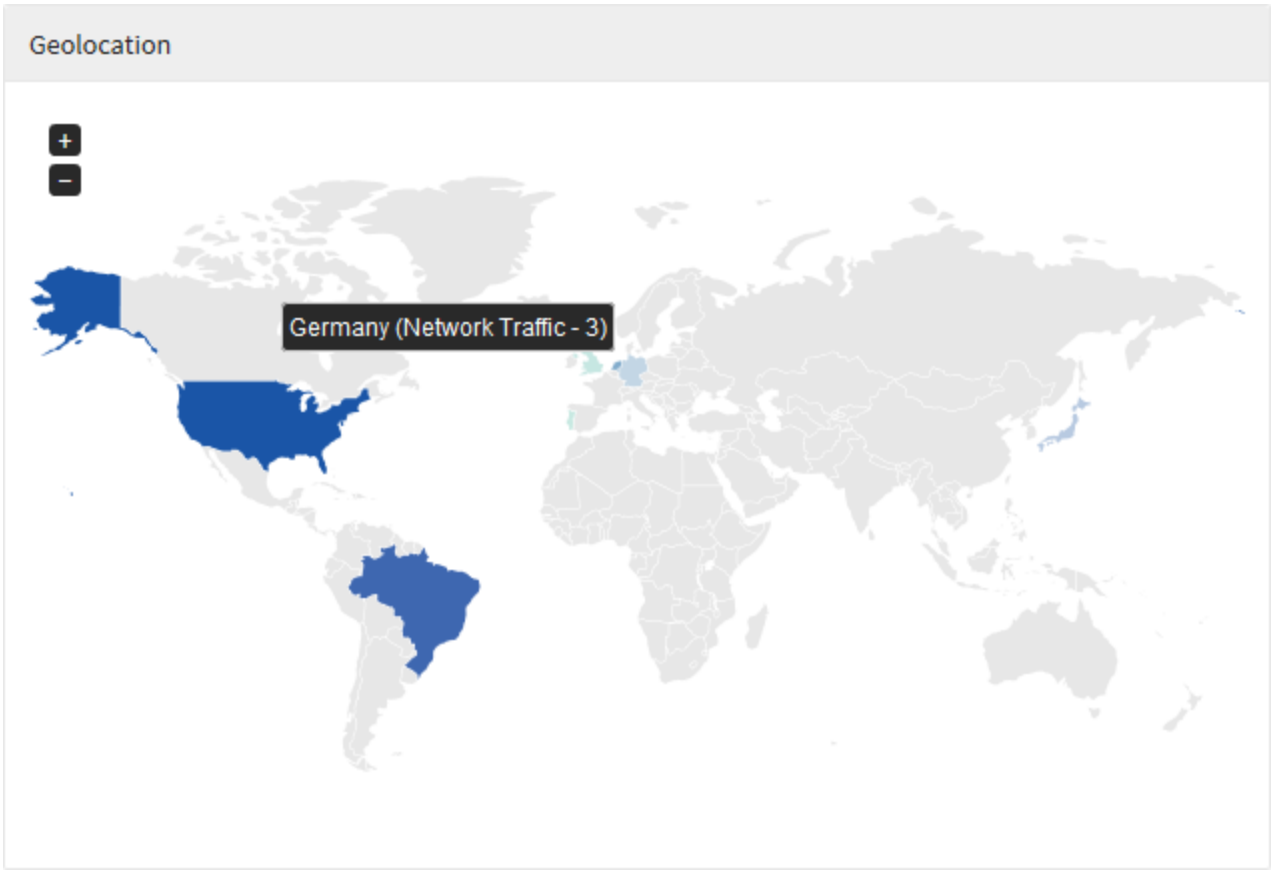
UTM - User Behavior - Geolocation Information

In "Hits by Geolocation" the destination of the connections of that specific user is displayed, the global map shows in a colored legend the amount of access made by users for each country.



User Behavior - Geolocation

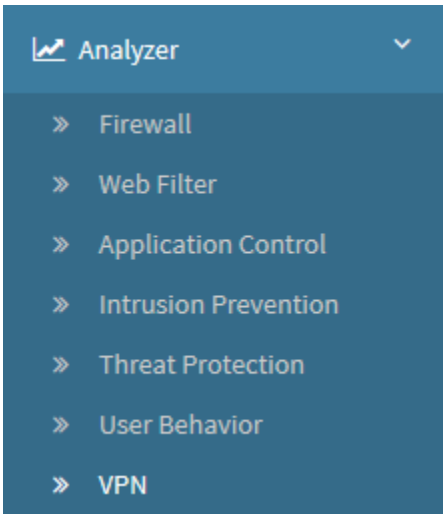
When hovering the mouse over the countries a total number of accesses is displayed, when doing the same with the legend it is possible to view an average, in addition, the country referring to this value is highlighted on the map.



User Behavior - *Geolocation* - Summary of accesses in a country

UTM - VPN

To access the web filter reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “VPN” option.



VPN

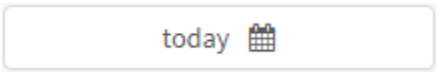
This resource's main function is to provide solid information about the Network's VPNs, enabling a holystic view of the structure, facilitating an integrated management and quick reply in case of any undesired events. In this panel we have the following VPN's statistical reports:

- Traffic on the VPNs;
- Usage by remote users;
- Top 100 most used *Site-to-site* VPNs;
- Top 100 most active remote users.

Besides that, general traffic information of the Top 100 VPNs and Remote users are also displayed:

- VPN connection or user identification;
- Type of the security protocol being used;
- Band consumption (*Bandwidth*);
- Active time (In hours and minutes);
- Amount of packets;
- Traffic.

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:

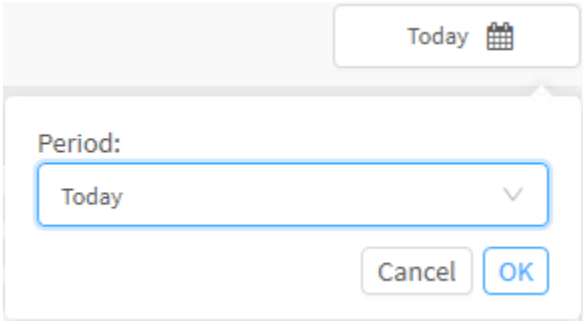


VPN - Date checkbox

Its purpose is basically to allow even more accurate results filtering, the possible options are:

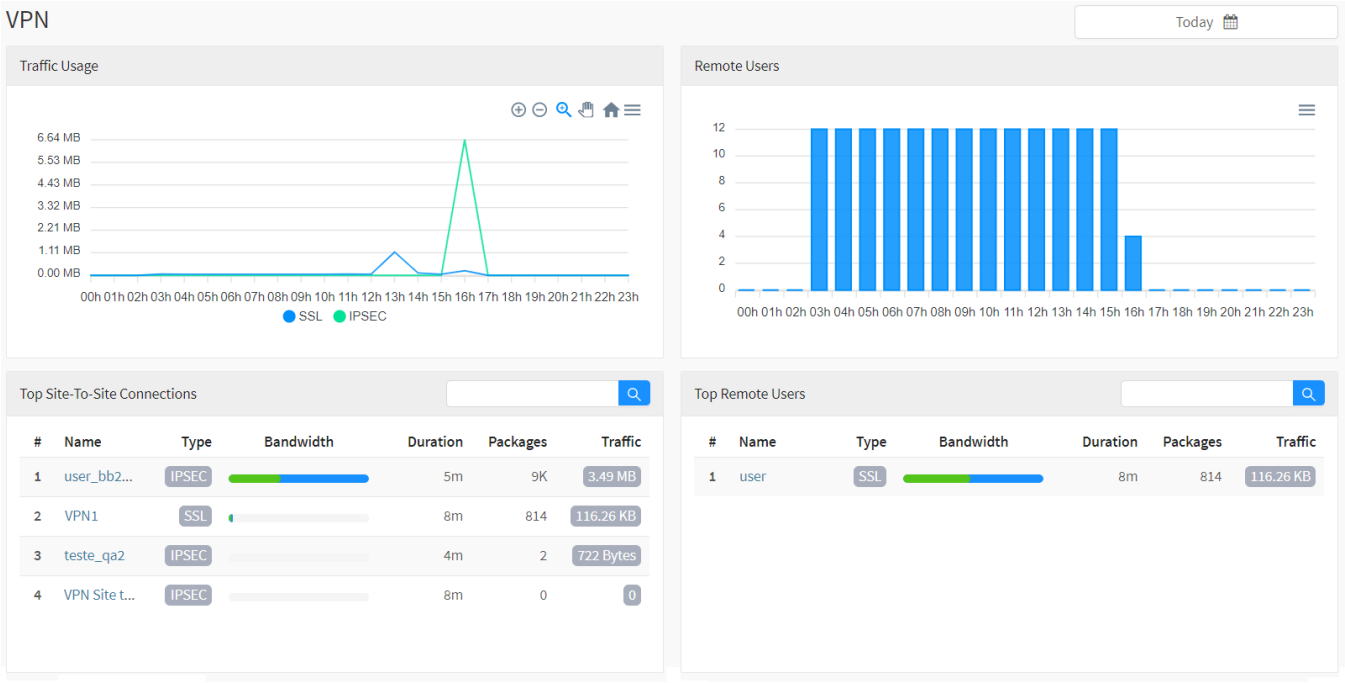
- **By date:** Determines a specific date;
- **By period:** Displays results from a start date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters results from the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays results for this month;
- **Last month:** Displays results for the last month.

Select the desired period:



VPN - Date Selection

To close this window, click **[** Cancel **]** or, after selecting the desired date, click **[** OK **]**;



Analyzer - VPN

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- **[ ]:** It serves to zoom in;
- **[ ]:** Its function is to zoom out;
- **[ ]:** It serves to zoom in a selection;
- **[ ]:** Serves to move the graph;
- **[ ]:** Reset the graph to the starting position;
- **[ ]:** Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

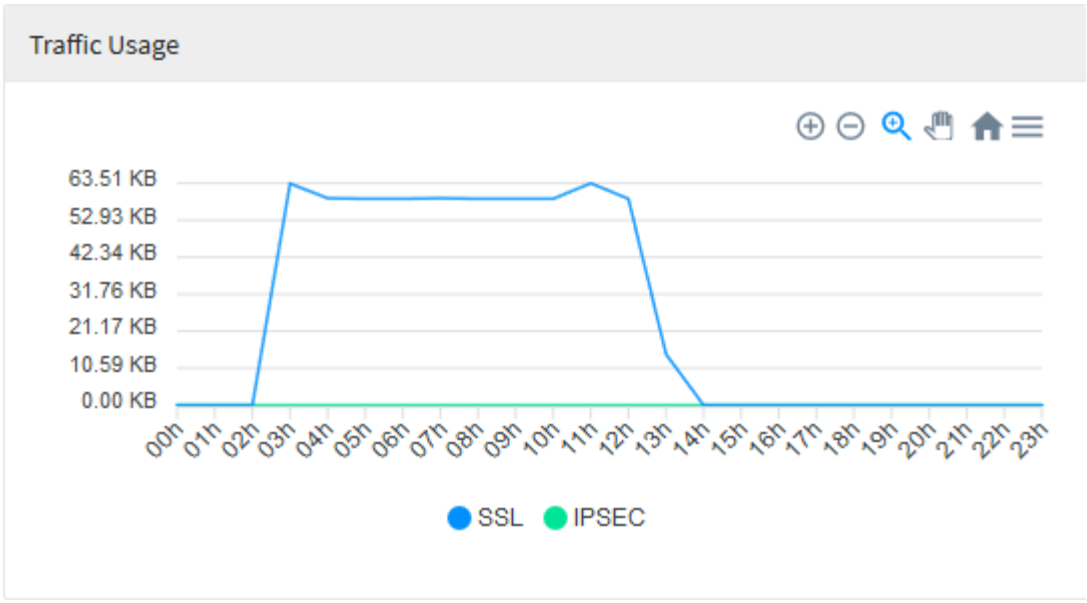
To perform a search, type a term in the search bar and click the **search button [ ]**.

Next, we'll look at each panel on this page.

- *Traffic Usage;*
- *Remote User;*
- *Top Site-to-Site;*
- *Top Remote User.*

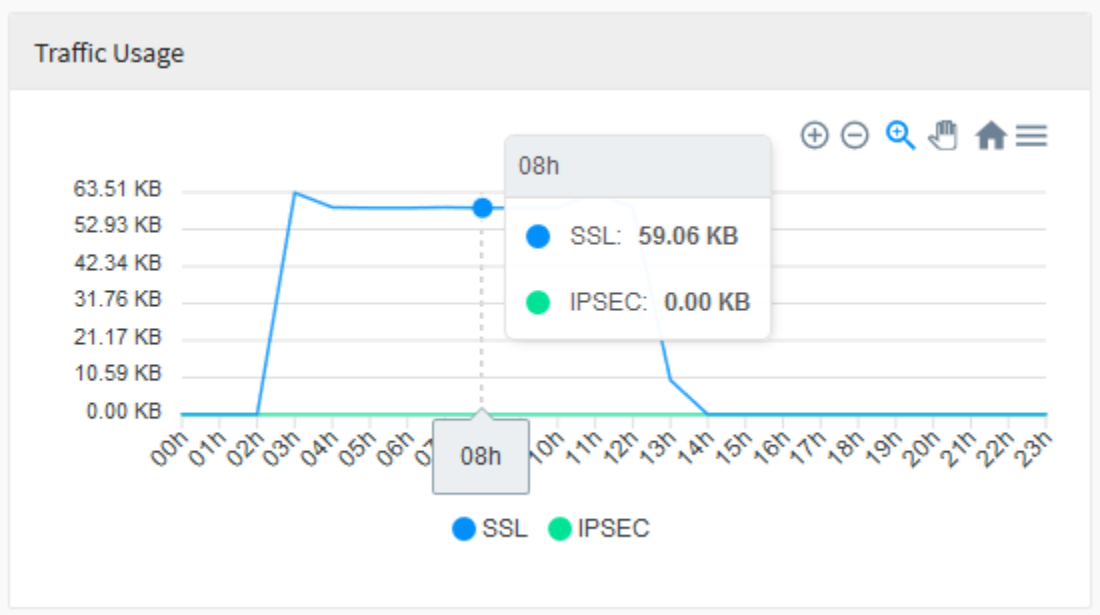
UTM - VPN - Traffic Usage

This panel has the function of showing the traffic consumption on the IPSEC and SSL VPNs. The vertical axis refers to consumption in Megabytes and the horizontal refers to the selected period (which may be hours or days).



Analyzer – VPN - Traffic usage

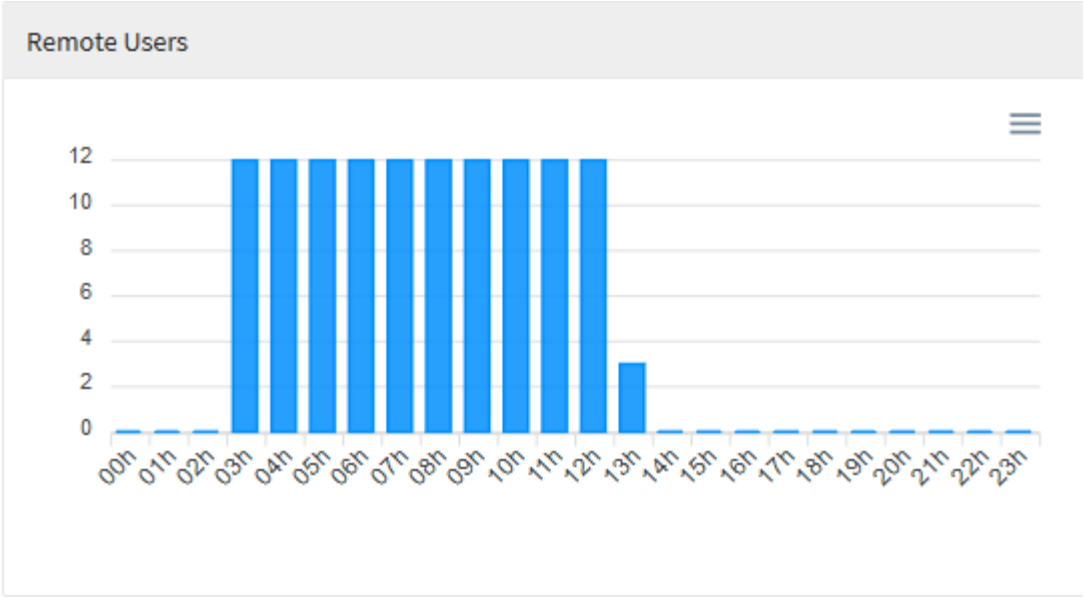
When you mouse over the graph, a summary of all traffic for the period is displayed, as shown in the image below:



Analyzer – VPN - Traffic usage - Details

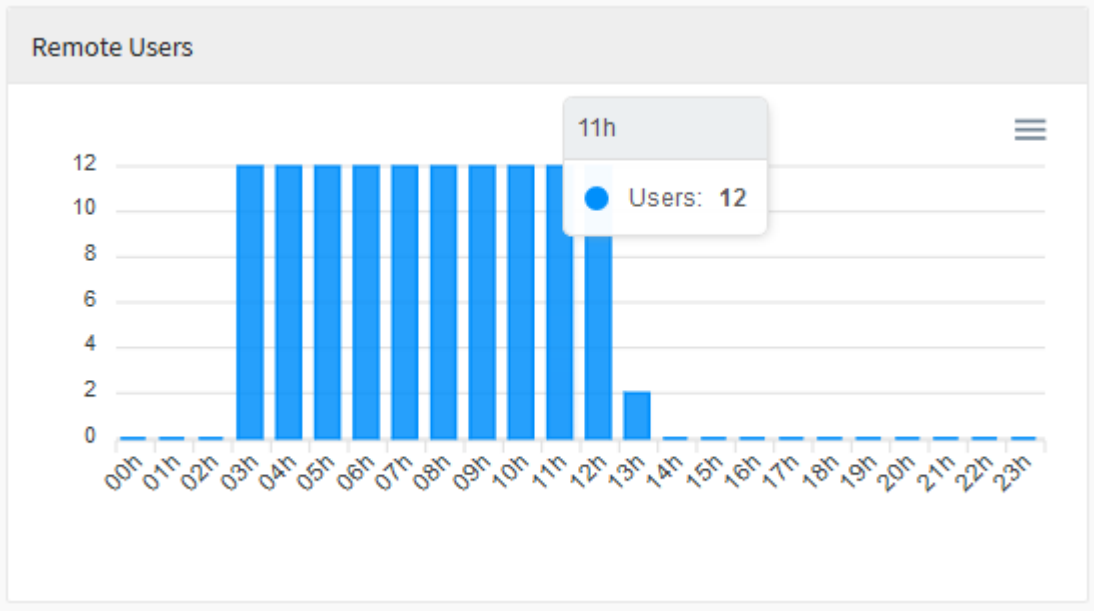
UTM - VPN - Remote User

This panel displays information about remote users. The vertical axis refers to the amount of remote users and the horizontal axis refers to the selected period (which can be hours or days).



Analyzer – VPN - Remote user

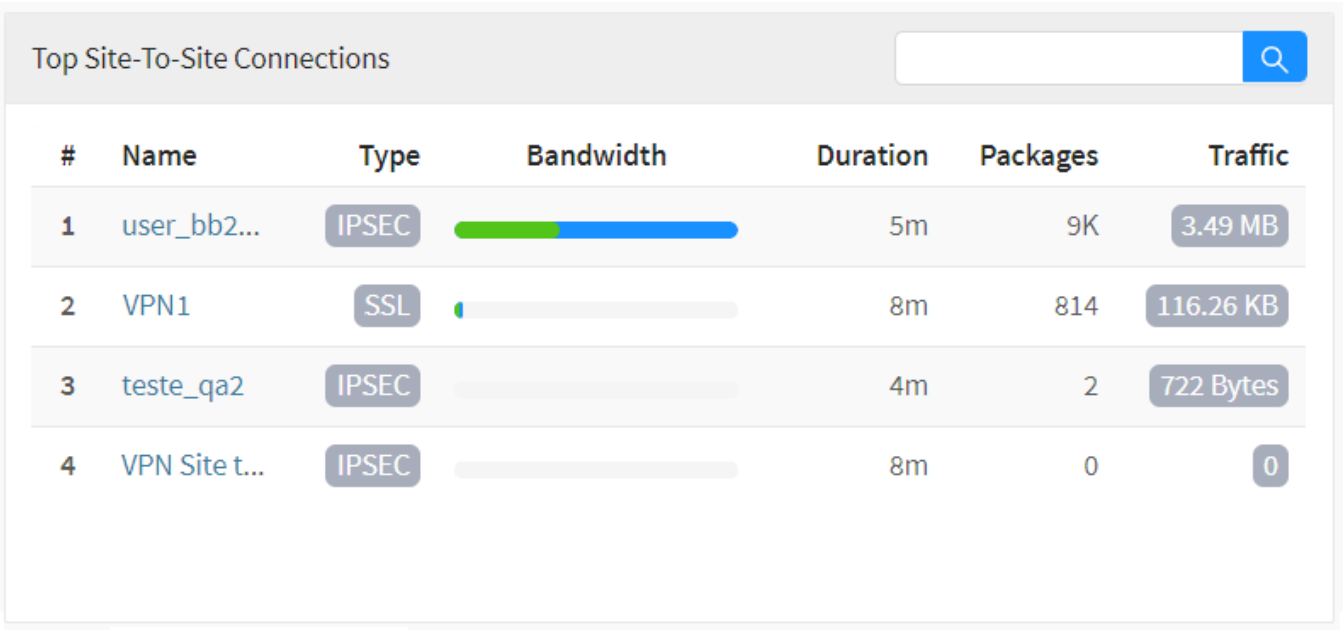
When hovering the mouse over the graph, a summary of all active users in the period is displayed, as shown in the image below:



Analyzer – VPN - Remote user - Details

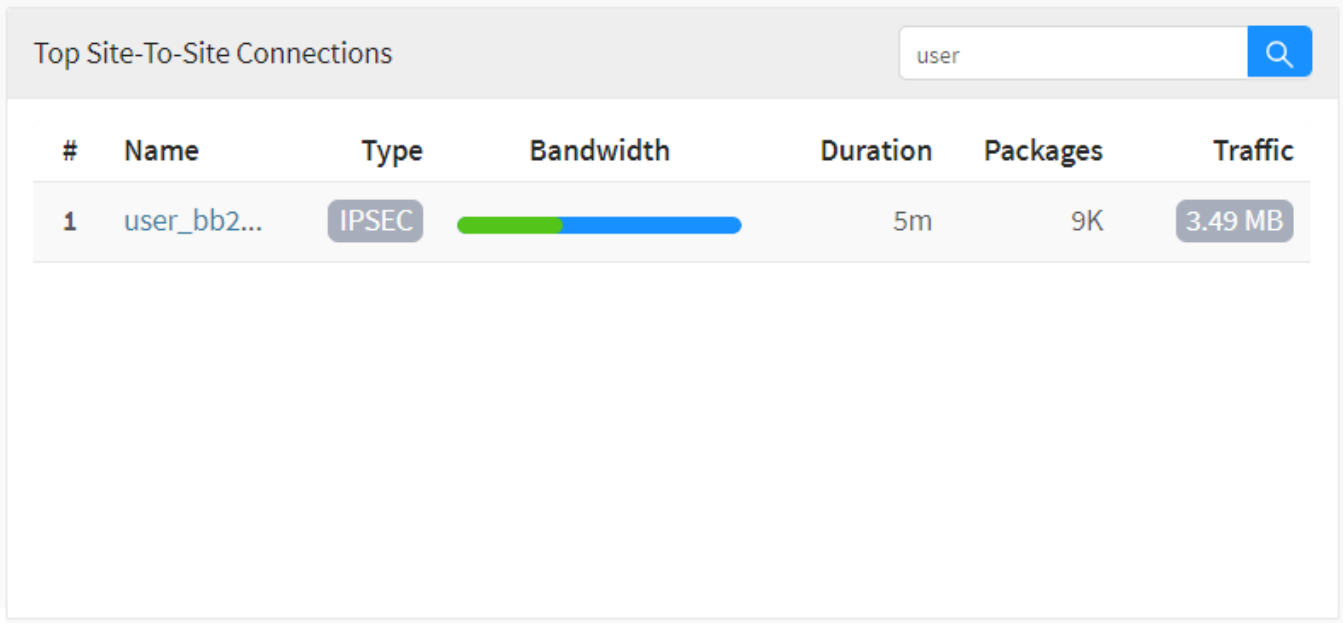
UTM - VPN - Top Site-to-Site Connections

The "Top Site-to-Site Connections" panel has the function of displaying the statistical information regarding the most used Site-to-Site VPN tunnels on the network.



Analyzer – VPN - Top Site-to-Site Connections

For the "Top Site-to-Site" panel to display information regarding a specific VPN, define its name in the search bar and click on **Search [** **]** the system will filter and display the relevant reports according to what was searched.



Analyzer – VPN - Top Site-to-Site Connections Search

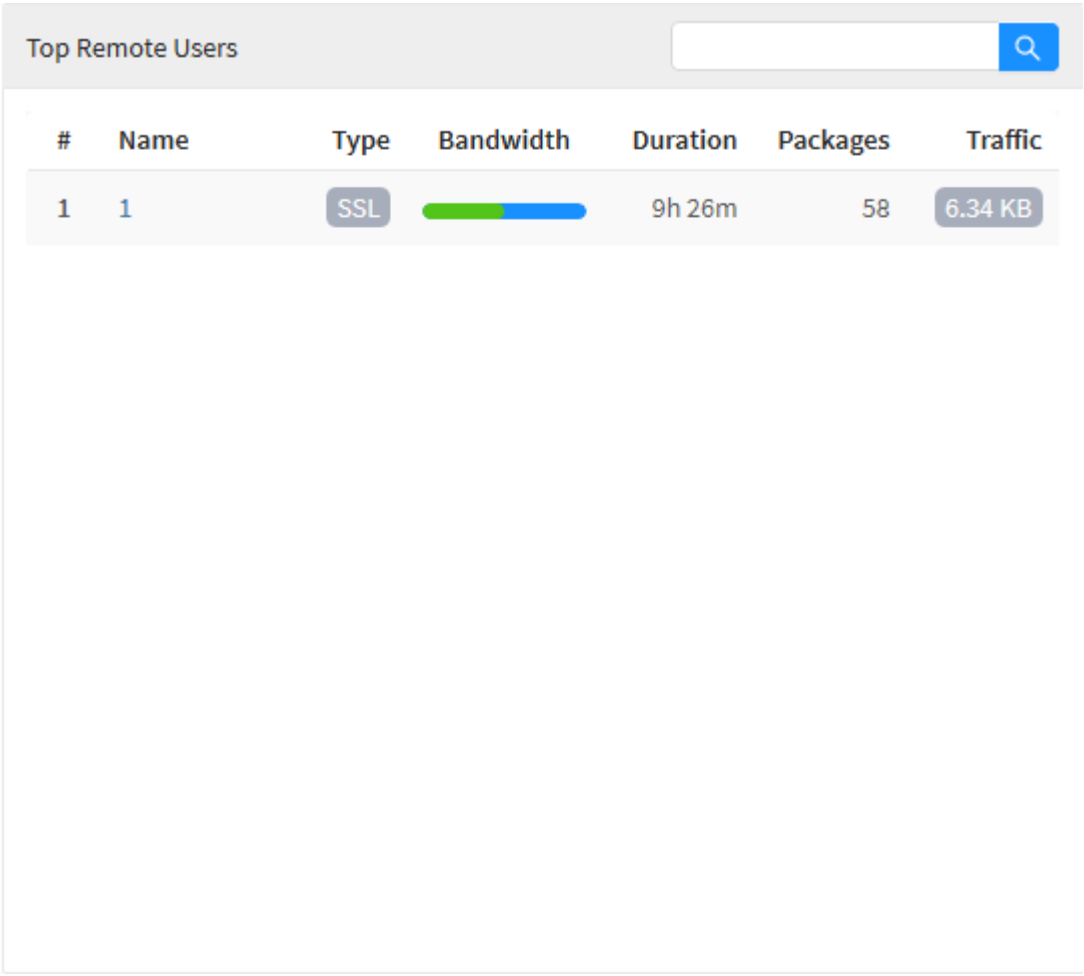
The report is divided into the columns below:

- ***Name*:** VPN tunnel name;

- ***Type*****:** Displays the type of protocol used in the VPN;
- ***Bandwidth*****:** Shows the bandwidth;
- ***Duration*****:** Displays how long the VPN connection has been established. It is displayed in hours and minutes;
- ***Packages*****:** Number of packets trafficked. It is displayed in Kilobytes;
- ***Traffic*****:** Displays the current VPN traffic. It is displayed in Megabytes.

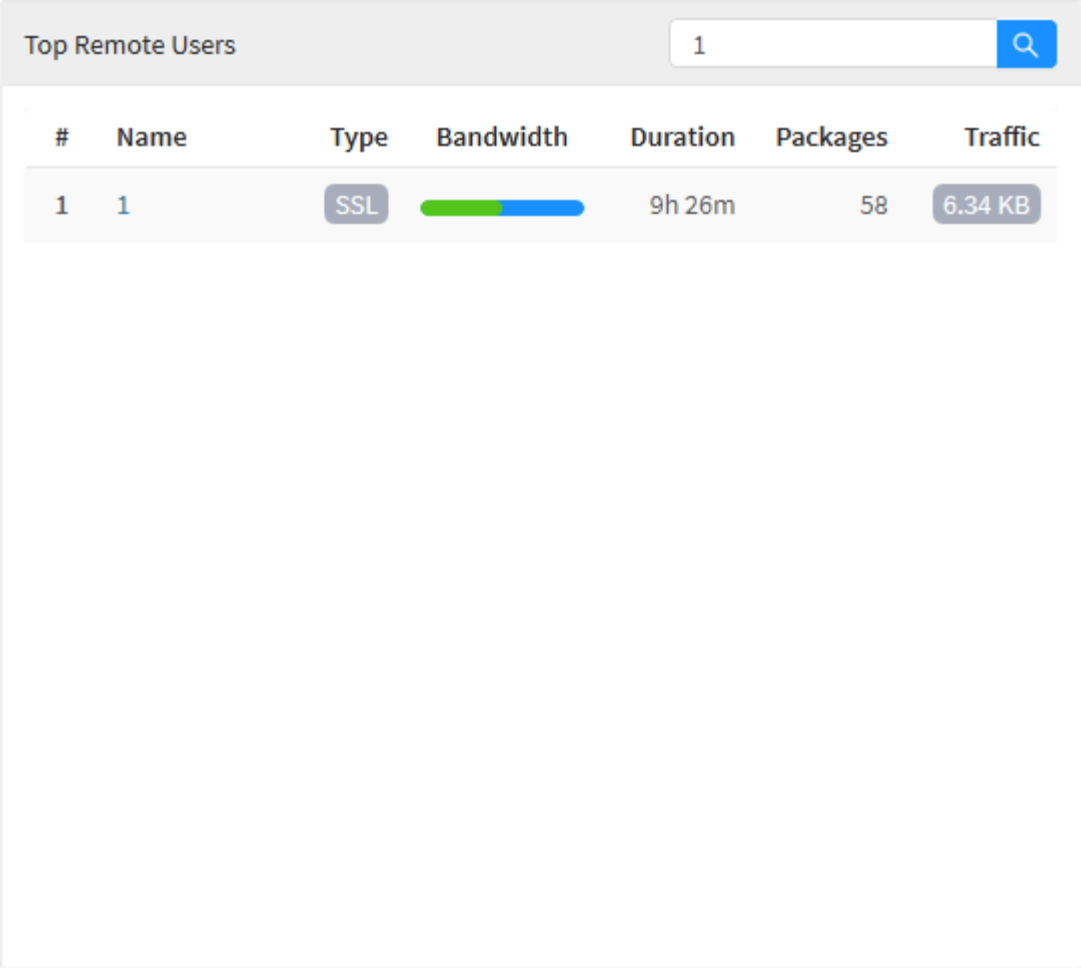
UTM - VPN - Top Remote User

The "Top Remote User" panel displays statistical information regarding remote users.



Analyzer – VPN - Top Remote User

In order for the "Top Remote User" panel to display information regarding a specific remote user, define his name in the search bar and click on Search **[**  **]** the system will filter and display the relevant reports according to what was searched for.



Analyzer – VPN - Top Remote User Search

O relatório é dividido pelas colunas abaixo:

- **Name:** Name of the remote user;
- **Type:** Displays the type of protocol used in the VPN;
- **Bandwidth:** Shows the bandwidth;
- **Duration**: Displays how long the VPN connection is established. It is displayed in hours and minutes;
- **Packages:** Number of packages trafficked. It is displayed in Kilobytes;
- **Traffic:** Displays the current VPN traffic. It is displayed in Megabytes.

UTM - POLICIES

All NGFW service management features, “Web content filter”, “WEB 2 application filter and control”, “SSL interception”, “Deep Inspection”, “Routing”, “QoS control (Traffic Shaping)”, “Traffic guarantee and priority”, “Traffic quota and time control”, “File size control”, “Header and content filters”, “Link balancing”, “Multiple services”, “NAT” and “ Proxy ”, are applied through policies.

The definition of security rules and policies integrates all these resources in the same interactive interface, and it is possible to apply a set of filters in the same policy that make up the integrated resources. The interface allows you to track all policies from TAGs that make it possible to group the rules by purpose, which facilitates filters for policy searches. The tags are added automatically by the system or the administrator can define one.

1. In just one configuration interface, the integration of resources in a single Policy:

- *WEB Category*;
- Application Control;
- Bandwidth control;
- Multiple Services;
- *QoS*;
- Time and Traffic Quota;
- *Choice of link profile*;
- Choice of deep inspection profile;
- Virus and Malware Control.

2. The configuration or activation of services and resources do not imply the creation of a security policy;

3. Security policies are not applied individually to each service.

With the exception of "SD-WAN" and "Firewall" services, which include exclusive rules or policies in the module itself. These do not apply to security policies, but exclusively to the service;

4. The security policies integrate [N] analysis conditions, which interact with the different resources of each service, and all of this in the same security policy.

Which makes managing policies much easier and more dynamic for the administrator;

5. Policies work in layers and their analysis behavior works in "First Match Wins" mode;

6. Security policies are registered in groups and by priority and support reordering.

Through the evaluation of logs and statistical reports, it is possible to reassess priorities and reorder security policies, according to the volume or importance of traffic.
Which consequently, improves server performance;

7. Security policy actions are:

- Allow;
- Deny;
- Reject.

These are the first basic concepts one should know about.

Compliance Policy features

- **Operation method:**
  - *First-match wins*;
  - Priority sorting.

Direct relationship with the Firewall's performance supports multithreaded functionality that makes best use of processors' performance. It allows setting the rules into a specific order, so that the most used policies or rules are placed above the less used ones, resulting in faster analysis.

The definition of rules and policies meet the following specifications and set of filters and conditions for taking action.

Below the list of "Actions" **VERSUS** "Conditions of the rules":

Table 1 - Policy Actions

Actions
Allow
Deny
Reject

VERSUS...

Table 2 - Rules Conditions

Condition by:	Policy conditions:
Server	The same rule can be applied to multiple servers; Configured on the same screen.
Properties	*Name*; *Description*; *Tags*; *Action*; *Policy Group*; *Position*; *Enable traffic logging*; *Time*/*Period*/*Date*.
Connection	***Source*** *Network Zone*; *Network Interface*; *IP Address*; *MAC Address*; ***Destination*** *IP Address*; *Service*. ***Identification*** ***Authenticated*** (*Users*/ *Groups*);
Content	***Web Proxy*** *FTP*; *HTTP*; *HTTPS*; *SSL Inspection*; *Validate SSL certificate*; *SSL Common Name*; *Malware Scanning*; *Explicit Proxy*. ***Web Filter*** *Web Categories*; *Applications*; *URL Filter*; *Browsers*; *HTTP method*; ***Email Protection*** *SMTP*; *POP3*.
Control	***Surfing Control*** *Content-Type Filter*; *HTTP Filter Header*; *Filter*;

	Surfing Quotas *Maximum Time*; *Maximum Traffic*; *Max Download Size*; *Max Upload Size*.
Security	***Deep Inspection*** *Sensor;* ***Threat Blocking*** *Compromised Addresses*; *Geolocation;* ***Packet Filter*** *TTL*; *Package Type*; *Packet Content*; *TCP MSS;*
Routing	***Gateway*** *NAT*; *SD-WAN;* ***QoS*** *Traffic Shaping*; *Flag packets* (*TOS*); *Flag packets* (*DSCP*);

The definitions are identical for IPv4 and IPv6, with changes only in their addresses and some proprietary characteristics of each version of the protocol.

Policies

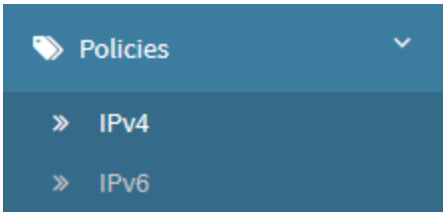
Next, we will analyze both options:

- IPv4;
- IPv6.

IPv4 Policies

This section will demonstrate the process of creating IPv4 policies, in addition to explaining in depth the concepts of how they work at the NGFW.

If it is not already selected, click on the "IPv4" option;



IPv4 option

The “IPv4 Policies” screen will appear, as shown on the following image:

IPv4

This section will delve into:

- Creating policy groups;
- Policy Registration and Removal.

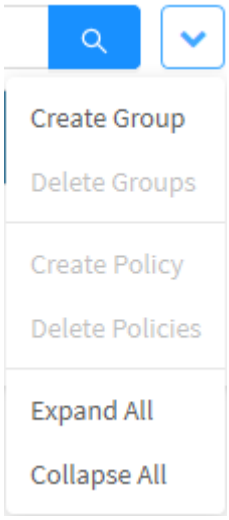
Next, we'll look at each component of this panel.

IPv4 - Actions menu

At the top right of the screen we have the actions menu:

IPv4 - Action menu button.

By clicking on this button the menu below is displayed:



IPv4 - Actions menu

The menu consists of the following options:

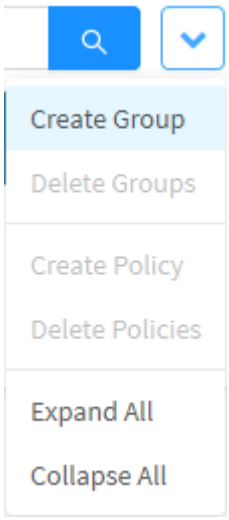
- *Create Group*;
- *Delete Groups*;
- *Create Policy*;
- *Delete Policies*;
- *Expand All* and *Collapse All*;
- Validate Policies.

Next, each action menu option will be detailed.

IPv4 - Actions menu - Create Group

Through the option “Create Group” it is possible to create a new group. To access, click on the **actions menu [**  **]**.

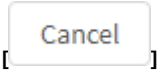
1. Click on the “Create Group” option;



IPv4 - Actions menu - Create Group

2. The “Create Group” screen will be displayed. Add the desired group name:

IPv4 – Create Group

After naming the group, if you want to cancel click on the **[**  **]** button. To finish creating the group, click on the **[**  **]** button.

Group successfully created

The group was successfully created.

Create Group - Examples - Creating Groups

Next, we will exemplify the registration of groups in order to demonstrate the best practices for modeling groups and policies.

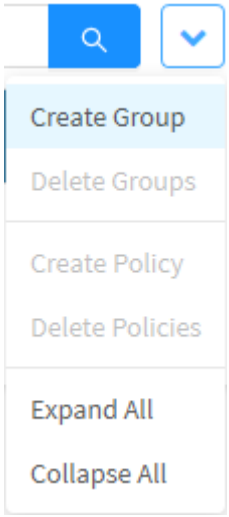
We will carry out the demonstration by creating the following groups:

- *Block;*
- *Forward;*
- *Masking (NAT);*
- *Web Filter.*

Group: Block

Purpose: To define the policies to apply the immediate and definitive “blocking” of specific traffic already known as INAPPROPRIATE. Without the intervention of “proxies”.

To add the policy groups, access the **actions menu [ ]** and select the **[Create Group]** option.

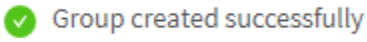


IPv4 - Actions menu - Create Group

To perform this example, create the group, as shown in the following image:

Create Group - Creating the "Block" group

After typing the name, click the button [Save];



Group successfully created

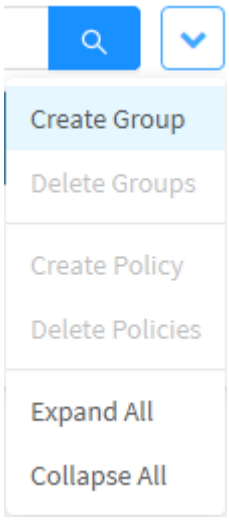
The group has been successfully created.

Grupo: *Forward* (*FW*)

Purpose: To define traffic management policies between internal networks / subnets.

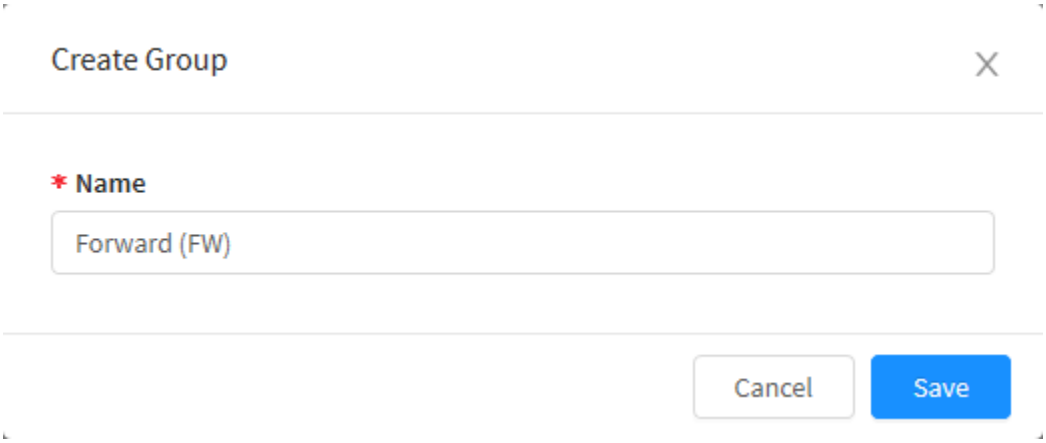
In this group we are going to define policies for “blocking” unauthorized traffic, for detecting and generating “log” and “Greylist” policies, that is, allowing traffic initially classified as “reliable”, however with the condition of “Inspecting” The traffic and validate its legitimacy and apply the disposal of the identified packages with “inappropriate or malicious” content.

To add the policy groups, access the **actions menu [ ]** and select the **[Create Group]** option.

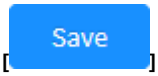


IPv4 - Actions menu - Create Group

To perform this example, create the group, as shown in the following image:



Create Group - Creating the Forward group

After typing the indicated name, click on the **[**  **]** button;

Group successfully created

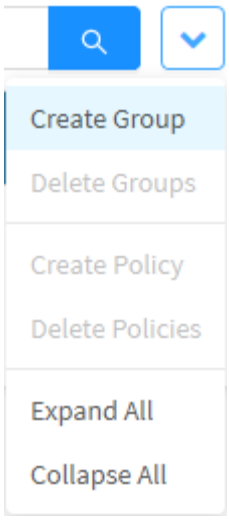
The group has been successfully created.

Group: Masking (NAT)

Purpose: To define traffic management policies for the WAN (Internet) network for specific servers and services without the intervention of a "proxy".

In this group, we will define “Greylist” policies, that is, allow traffic initially classified as “reliable”, for specific servers and services, however with the condition of “Inspecting” traffic and validating its legitimacy and applying the disposal of packages identified as “inappropriate or malicious” content.

To add the policy groups, access the **actions menu [**  **]** and select the **[Create Group]** option.



IPv4 - Actions menu - Create Group

To perform this example, create the group, as shown in the following image:

Create Group - Creating the Masking Group (NAT)

After typing the indicated name, click on the [Save] button;

Group successfully created

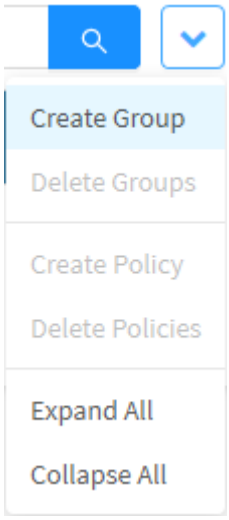
The group has been successfully created.

Group: Web Filter

Purpose: To define the traffic management policies for the WAN (Internet) network via "Proxy".

In this group we are going to define policies to “block” unauthorized traffic, to detect and generate “logs”, “Greylist” policies, that is, to allow traffic initially classified as “reliable”, however with the condition of “Inspecting ”Traffic to validate its legitimacy and enforce the disposal of identified packages with“ inappropriate or malicious ”content.

To add the policy groups, access the **action menu [ ]** and select the **[Create Group]** option.

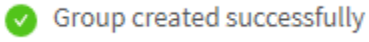


IPv4 - Actions menu - Create Group

To perform this example, create the group, as shown in the following image:

Create Group - Creating the "Web Filter" group

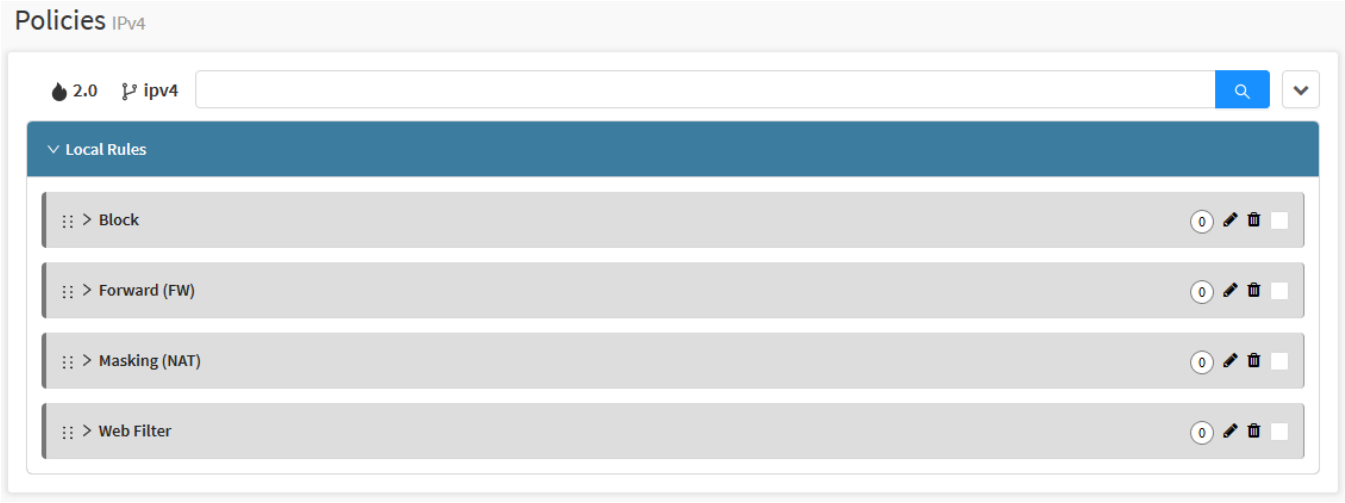
After typing the indicated name, click on the **[Save]** button;



Group successfully created

The group has been successfully created.

This concludes the process of creating the groups that will be used for the example, it will be possible to view them on the IPv4 home page under "Local Rules", as shown on the image below.



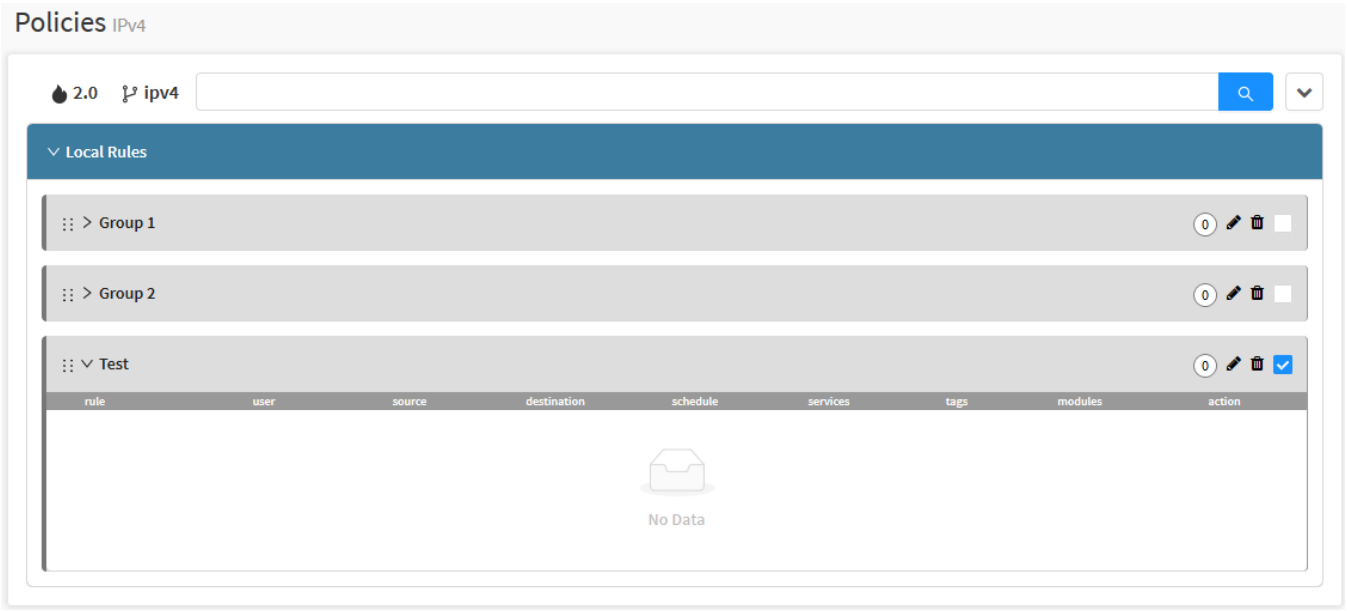
IPv4 – Policy Groups

To see the registration of some basic policies, access *IPv4 Policies - Examples - Policy Creation*.

IPv4 - Actions menu - Delete Groups

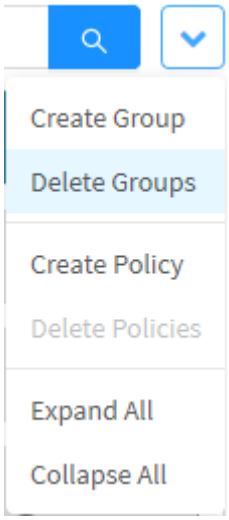
Through the button “Delete Groups” it is possible to delete several groups installed at the same time. To delete from the actions menu, follow these steps:

1. Select which group (s) you want to delete by clicking on the ***checkbox*** **[ ]**, as shown in the image below:



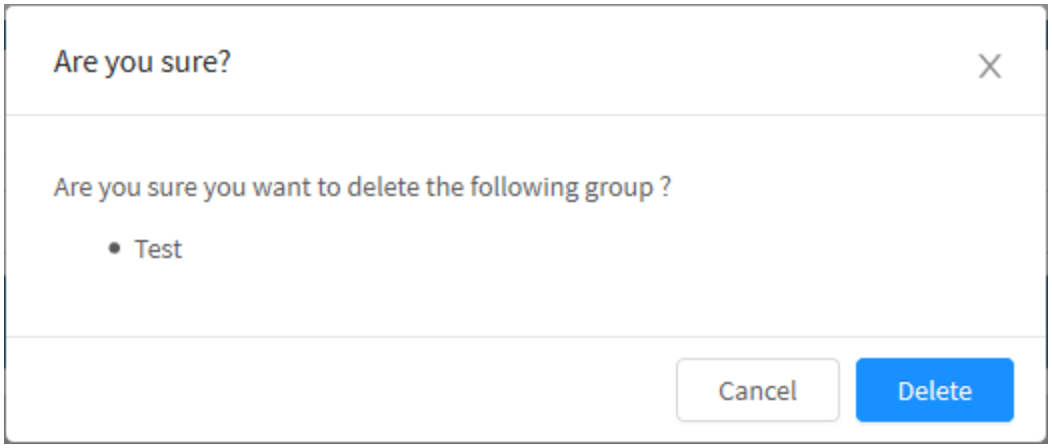
IPv4 – Delete Groups

2. Enter the **actions menu [ ]** and click on the “Delete Groups” button.



IPv4 - Actions menu - Delete Groups

3. The message will appear if you really want to delete the selected packages:



IPv4 – Delete Groups

If you want to cancel click on the **[** Cancel **]** button. To finish, click on the **[** Delete **]** button.

Group successfully deleted

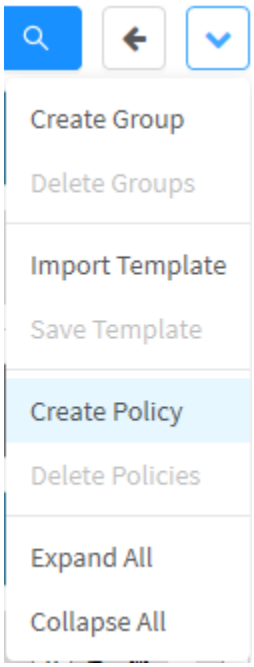
After performing these procedures, the groups will have been successfully deleted.

IPv4 - Actions menu - Create Policy

The “Create Policy” button creates Policies within pre-created and pre-selected Policy groups. In order to do so, it is necessary to have a previously created Policy group (check this page for more information).

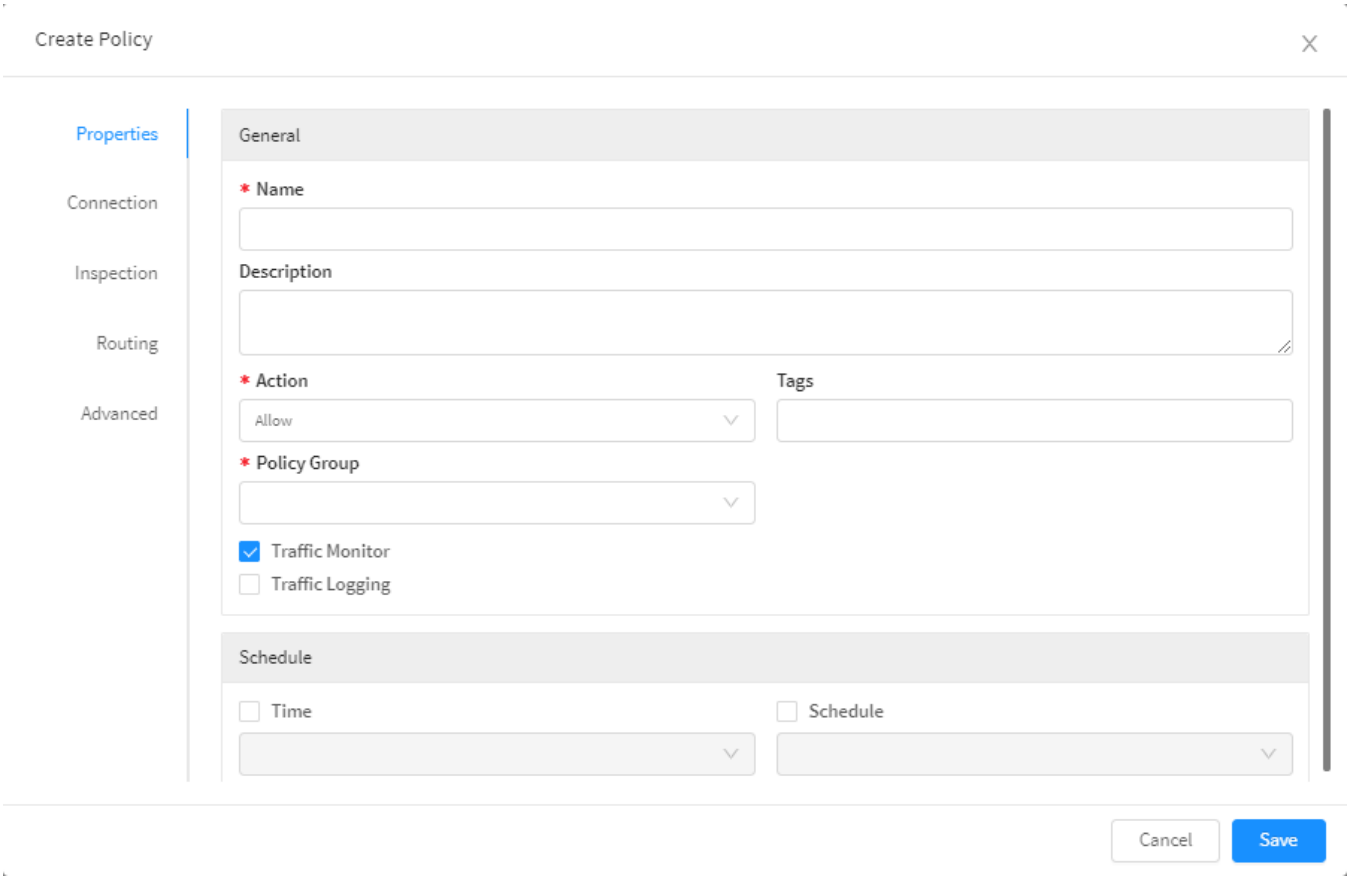
To create a policy, follow these steps:

1. In the actions menu **[**  **]**, click on the “Create Policy” option;



IPv4 - Actions Menu - Create Policy

2. The Policy Form screen will appear;



IPv4 – Policy Form

This window is organized by the following tabs:

- *Properties*;
- *Connection*;
- *Inspection*;
- *Routing;*
- Advanced.

Next we will explain each field in this window.

Create Policy - Properties Tab

In the **[Properties]** tab, it is mandatory to define a name and description for the policy, however tags can be defined as one pleases. Those help in the organization and facilitate the search for policies.

IPv4 - Side Tabs - Properties

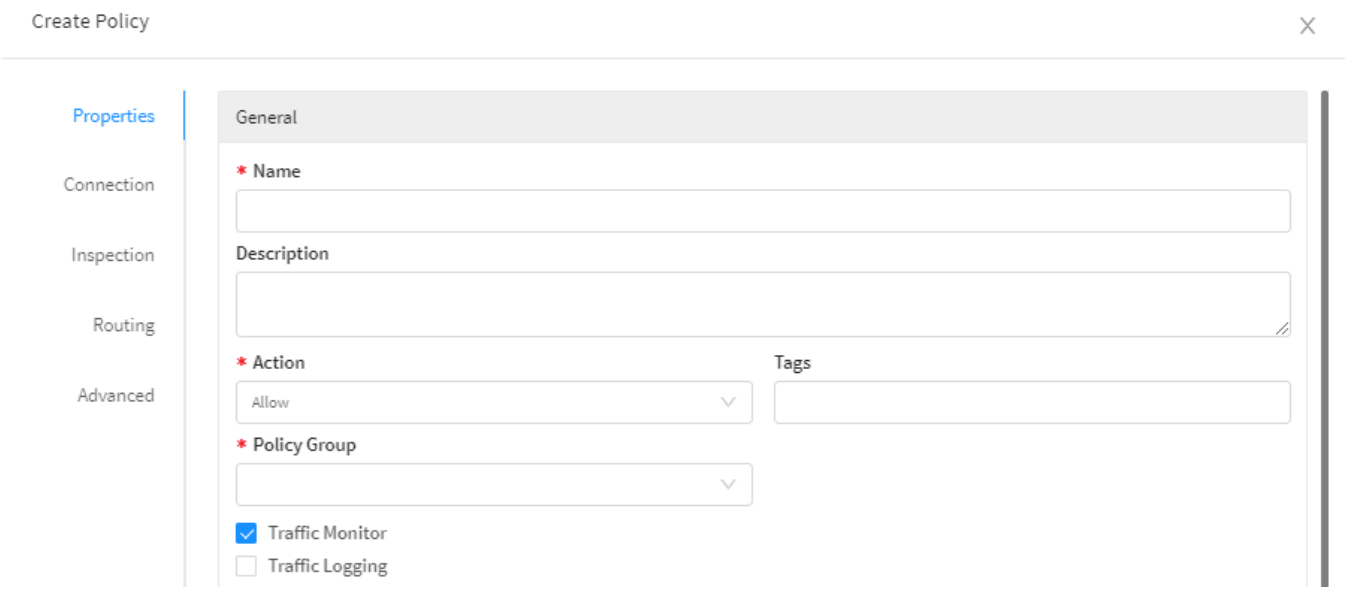
This tab contains the panels:

- *General*;
- *Schedule*.

Next, we will analyze each panel's functions

General

This is a description of each field's function from the form displayed in the **[General]** panel:



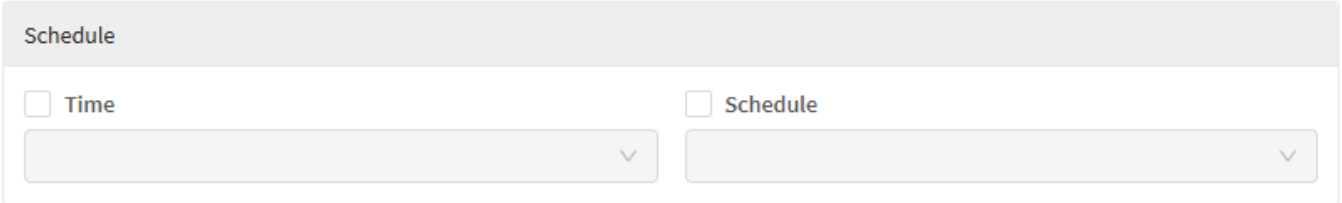
IPv4 – Properties - General

- ***Name*:** Define a name for the policy;
- ***Description*:** Insert a description for the policy;
- ***Action*:** Determines the behavior of the policy, having as possibilities:
  - ***Allow*:** The Allow action grants access and leaves traffic free of blocks;
  - **Deny:** The Deny action blocks traffic but does not inform the source address of the service that is being blocked. That is, in this scenario, for the address of the connection source, it is not possible to know if there is a firewall intercepting the connection or simply if the service is not active;
  - **Reject:** The Reject action notifies the source address that the service has been blocked by a firewall, which sends an ICMP packet indicating that the service is inaccessible.
- ***Tags*:** This option allows you to define Tags, so that the administrator can use them as “Filters” for their searches based on definitions. By default, the system defines a “name” for the Tags by the type of resource being used in the policy;
- ***Policy Group*:** Through this option it is possible to include the selected policy within a group of policies;
- **Traffic Monitor:** When this option is checked[ ], the matching information from the sessions with the created policy, will be collected by the monitoring service.
- ***Traffic Logging[ ]*:** This checkbox, if enabled, provides the option to generate a report for a specific policy. The Traffic Loging options are configured in Settings - System - Logging tab.

If you intend to use Netflow, it must be enabled by the administrator in the system's Traffic Logging settings.

Schedule

On the **[Schedule]** panel, it is possible to define specific schedules for the policies to be enabled or disabled automatically. Here is a description of the functions in every field of the form:



IPv4 – Properties - Schedule

- ***Time[ ]*:** If the checkbox is selected, it determines whether the rule will apply on working days (“Business”), weekends (“Weekend”) or on any other object of the "Time" type that has been previously created;
- ***Schedule[ ]*:** If the checkbox is selected, it determines if the rule will be applied in according to a “Period/Date” object that has been previously created.

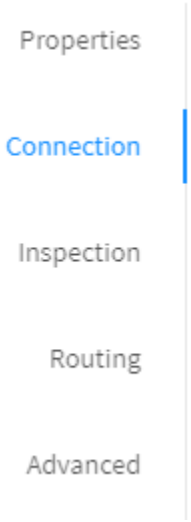
Next we will analyze the contents of the *Connection* tab.

Remaining tabs:

- Inspection;
- Routing;
- Advanced.

Create Policy - Connection tab

The **[Connection]** tab provides several filters to specify the scope of origin and destination, and it is mandatory to choose at least one of them.



IPv4 - Side Tabs - Connection

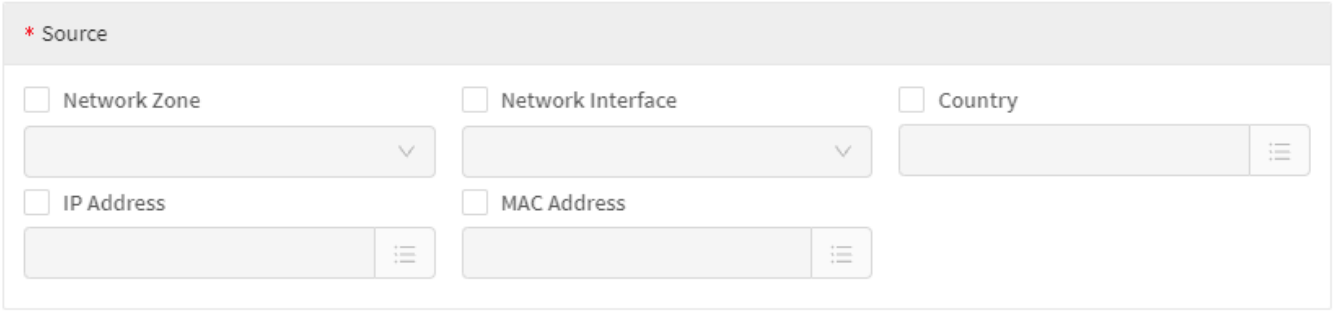
This tab contains the panels:

- *Source*;
- *Destination;*
- *Identification*.

Next, we will analyze each panel's functions:

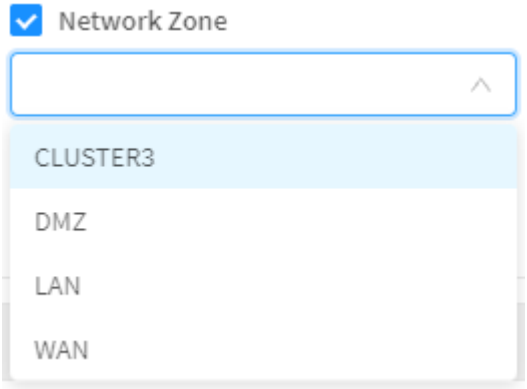
Source

The **[Source]** panel offers several filters to determine the source scope, as already mentioned, it is necessary to select at least one filter. Below is a description of the functions on the form displayed on the **[Source]** panel:



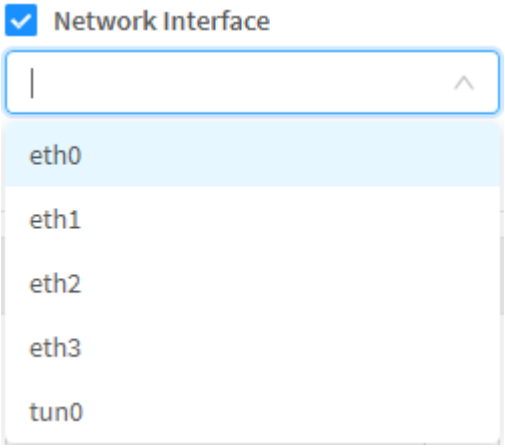
IPv4 – Connection - Source

- ***Network Zone[ ]*:** This field is only available by marking the checkbox. This field allows you to select network interfaces that can be signaled with acronyms such as LAN, WAN and DMZ to facilitate the organization and creation of policies segmenting by network type. The network zones that appear in this menu are created in *Network - Interfaces*;



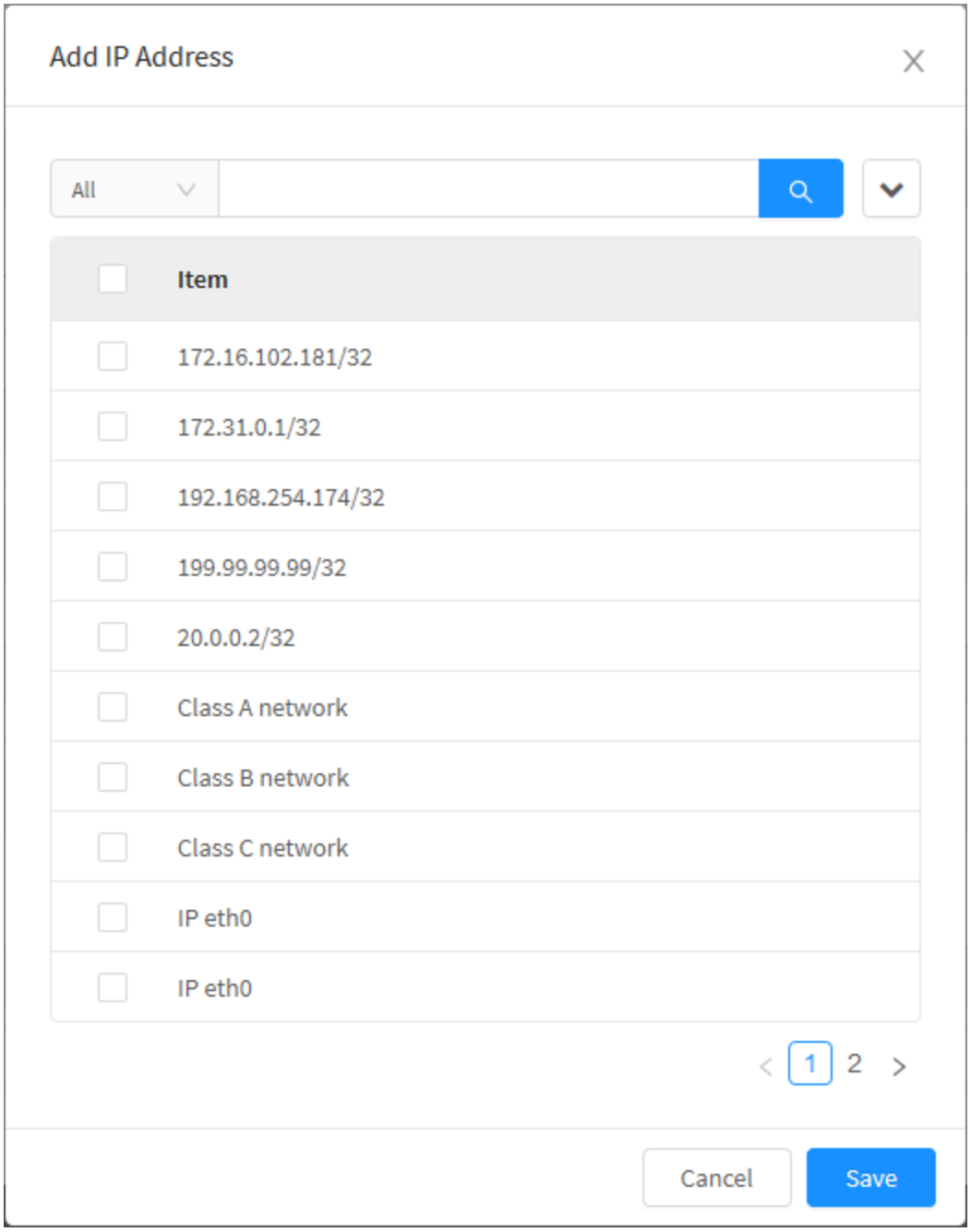
IPv4 – Connection - Source - Network Zone

- ***Network Interface[ ]*:** This field is only available by marking the checkbox. This field allows the selection of a network interface to be used as source filter. The interfaces that appear in this menu are created in *Network - Interfaces;*



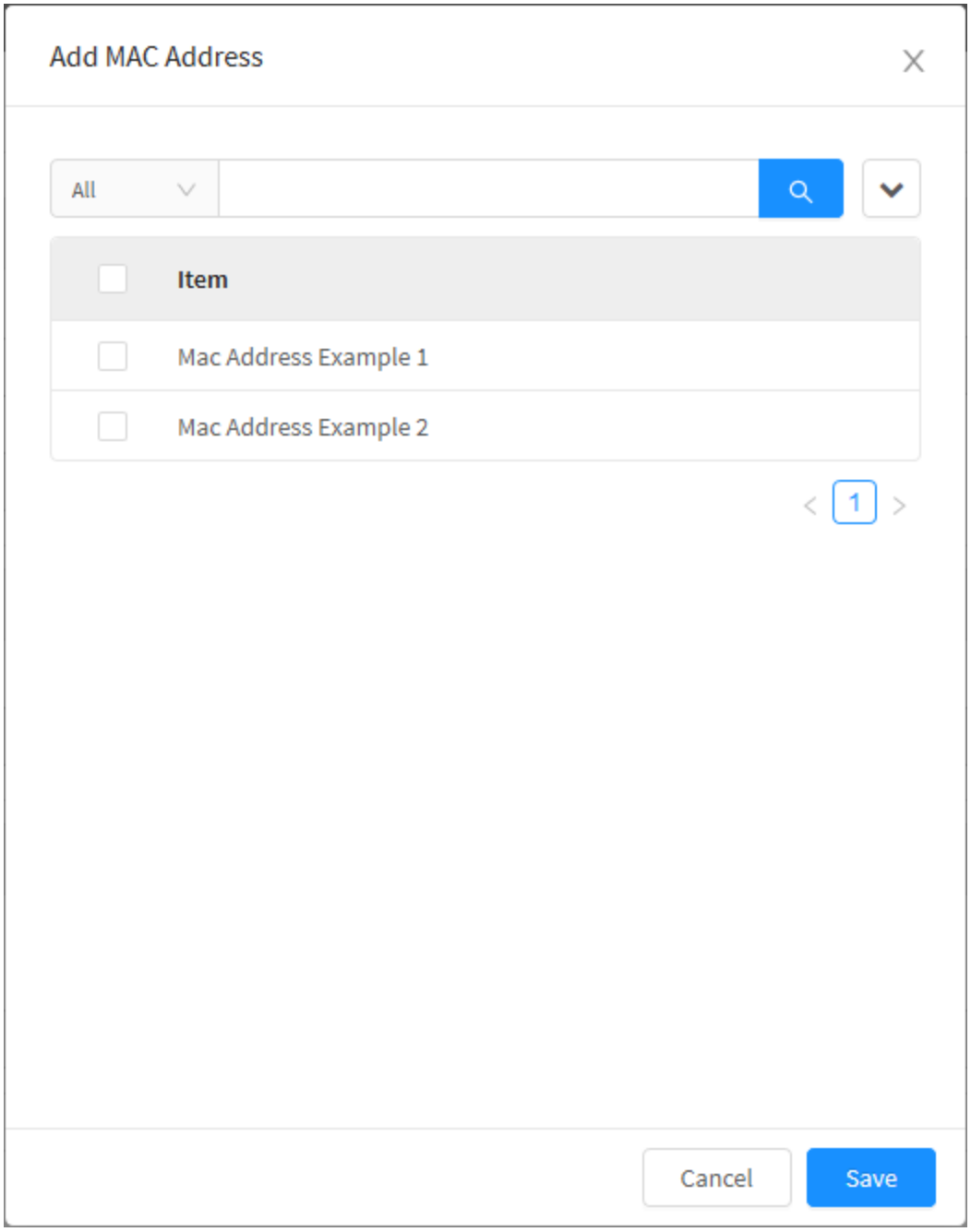
IPv4 – Connection - Source - Network Interface

- ***IP Address[ ]*:** This field is only available by marking the checkbox. This field allows the selection of IP Address Objects (IPs, networks or sets) to be used as a source filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more address objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



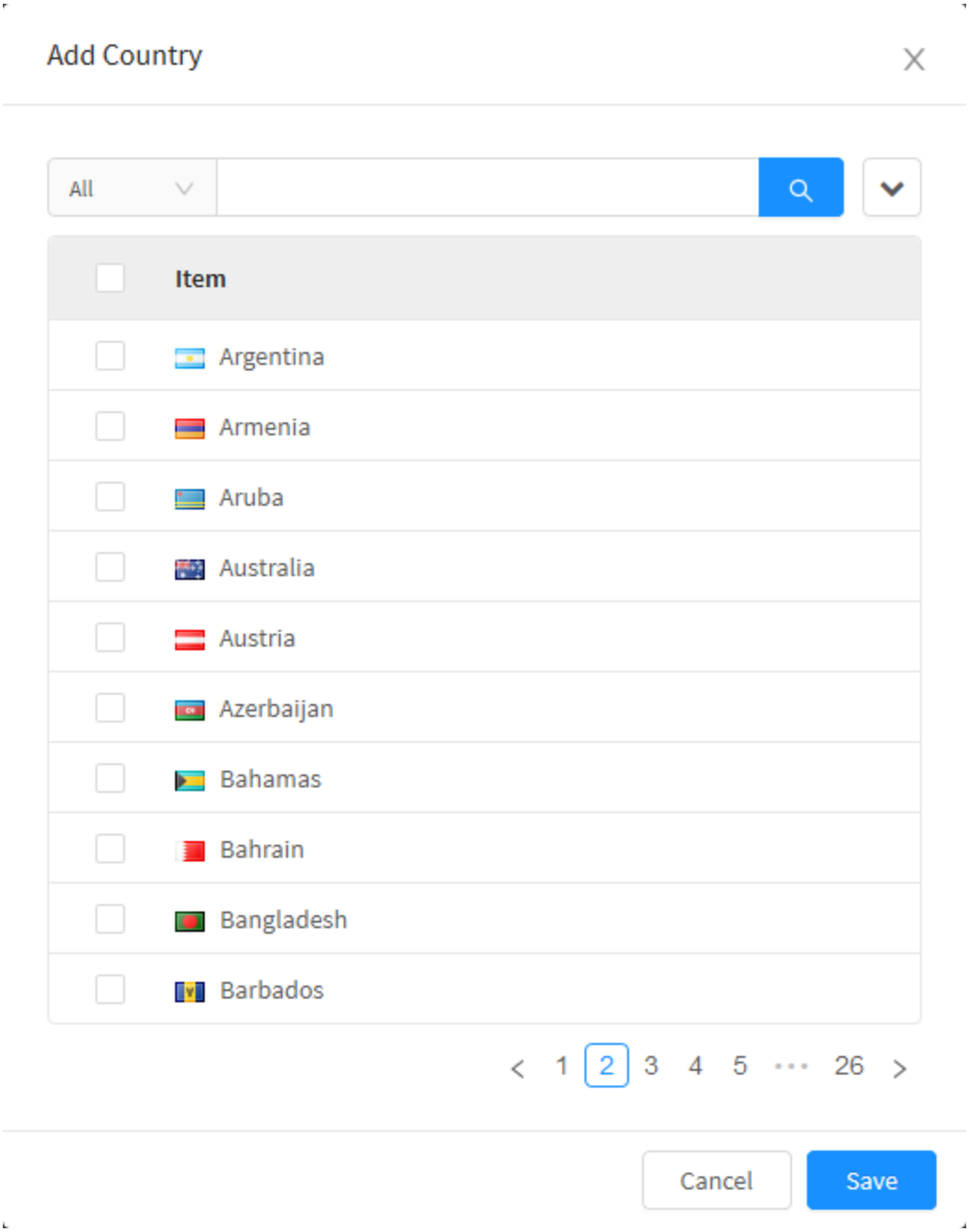
IPv4 – Connection - Source - IP Address

- ***MAC Address[ ]*:** This field is only available by marking the checkbox. This field allows to select Mac Address Address Object (s) to be used as source filter. When clicking on the **[ ]** button, the screen below will be displayed to select one or more MAC address objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



IPv4 – Connection - Source - Mac Address

- ***Country[ ]*: This field is only available by marking the checkbox. This field allows you to select *Countries* to be used as a source filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more countries that will compose the rule.



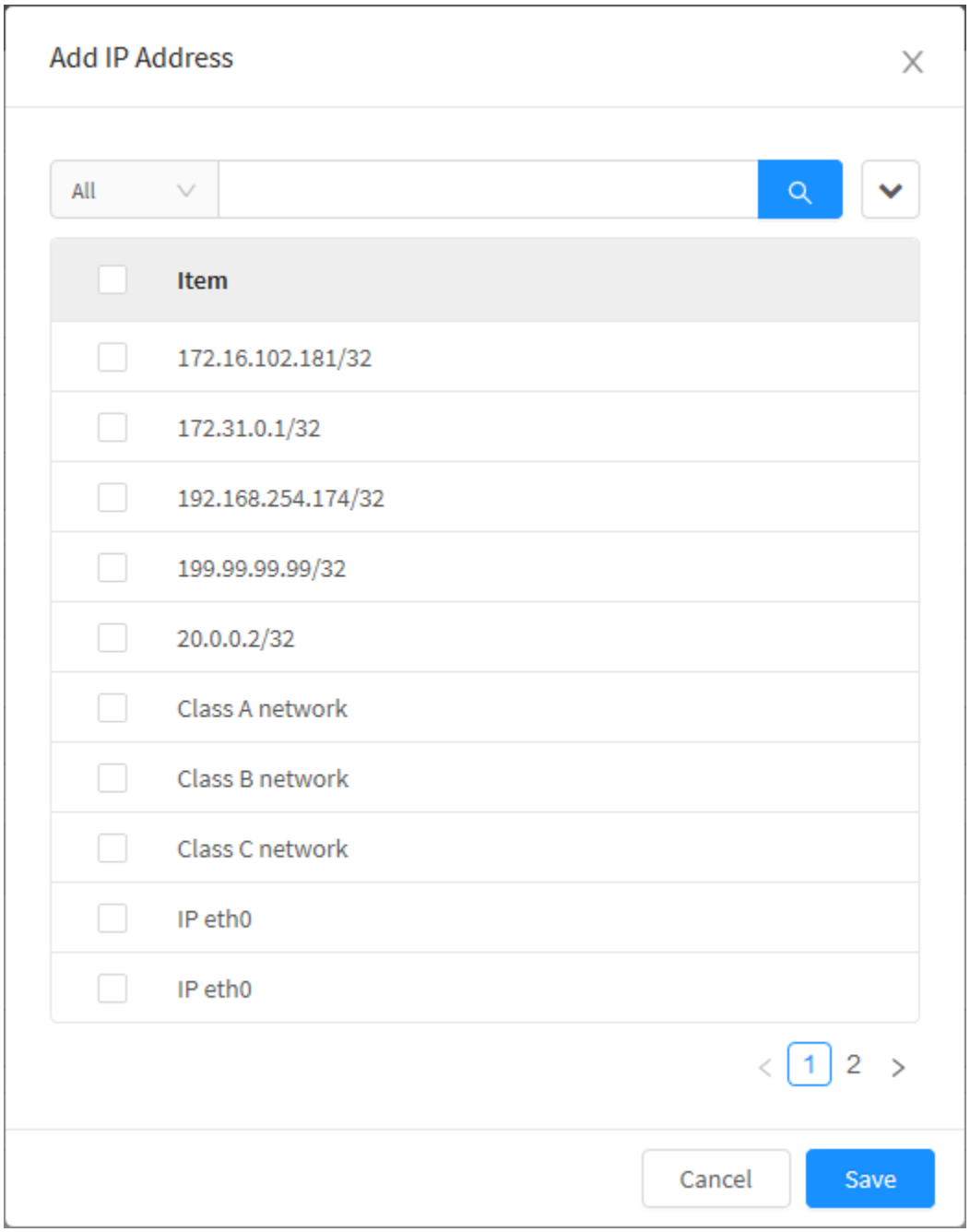
IPv4 – Connection - Source - Country

Destination

The **[Destination]** panel provides several filters to specify the scope of the destination, being mandatory to choose at least one filter. Below is a description of each of the functions on the form displayed on the **[*Destination*]** panel:

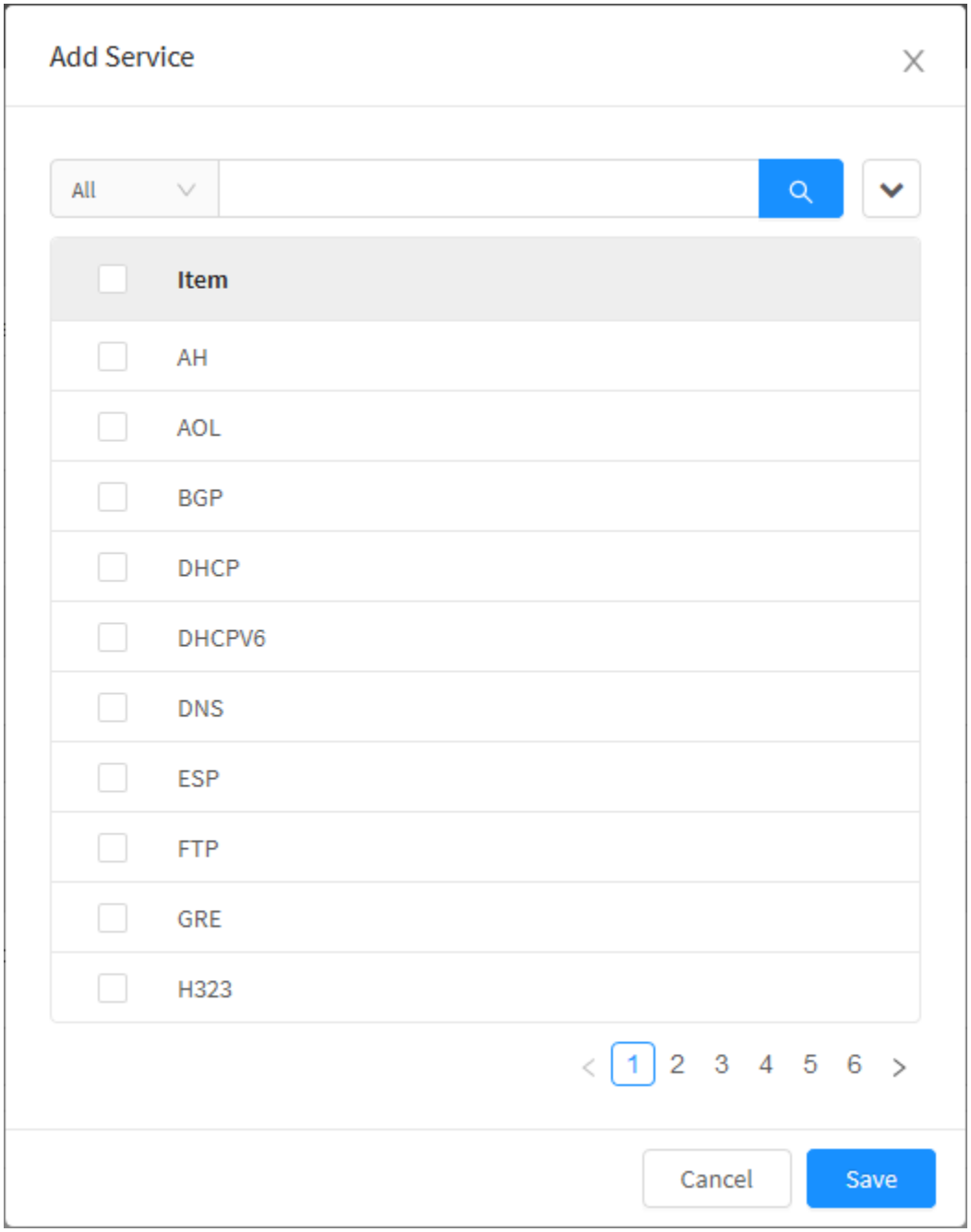
IPv4 – Connection - Destination

- ***IP Address[ ]*:** This field is only available by checking the checkbox. This field allows you to select IP Address Objects (IPs, networks or sets) to be used as a destination filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more IP address object (s) that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



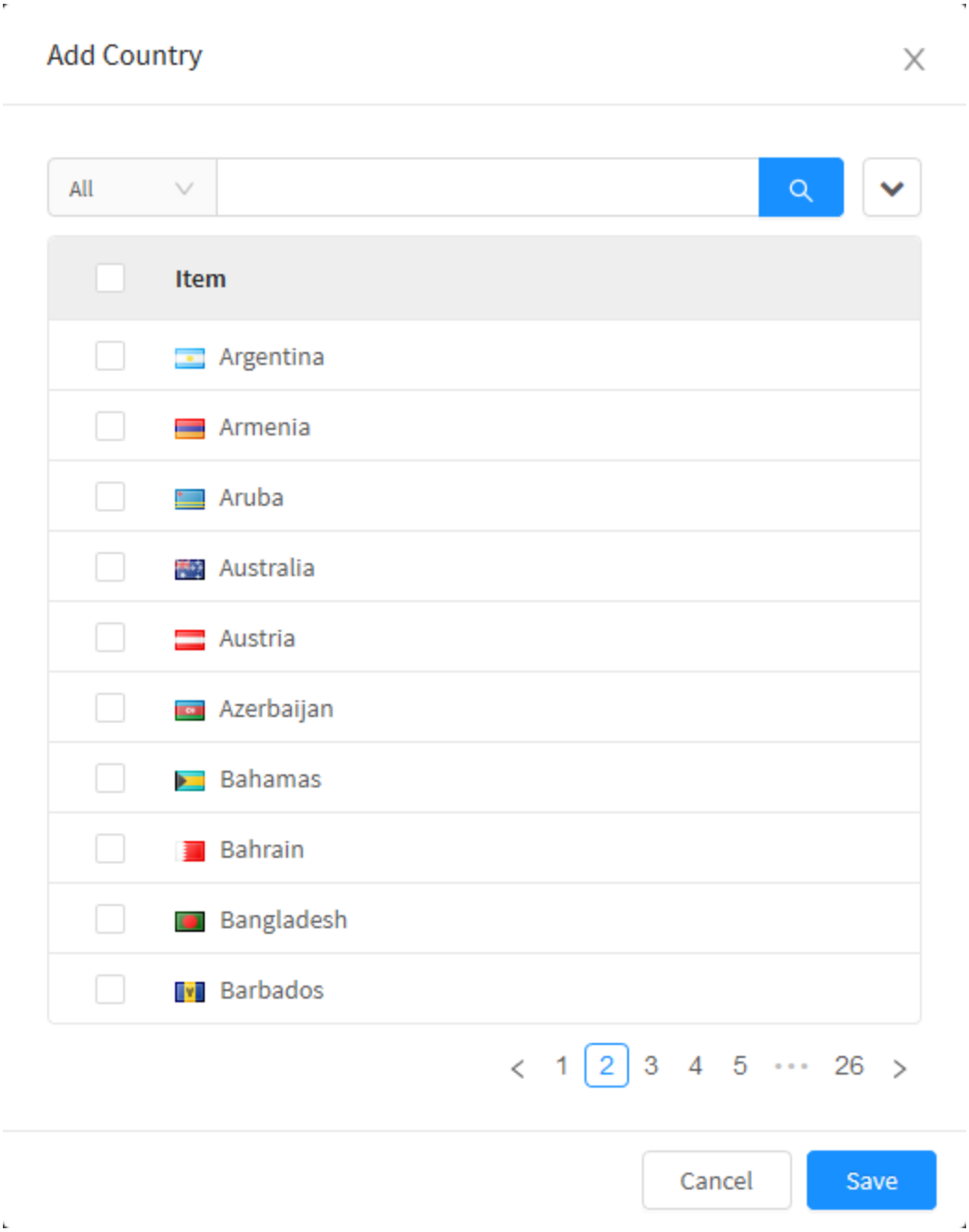
IPv4 – Connection - Destination - IP Address

- ***Service[ ]*:** This field is only available by checking the checkbox. This field allows you to select Service object (s) (protocols and ports) used as the destination filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more service objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



IPv4 – Connection - Destination - Service

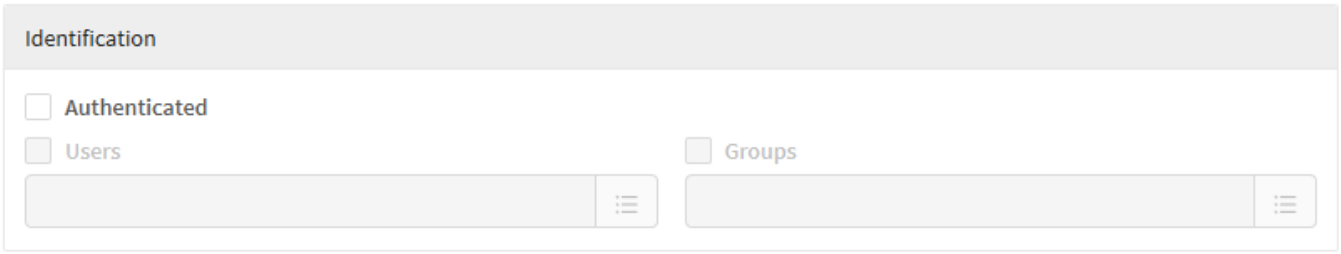
- ***Country[ ]*:** This field is only available by marking the checkbox. This field allows you to select Countries to be used as a destination filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more countries that will be part of the rule.



IPv4 – Connection - Destination - Country

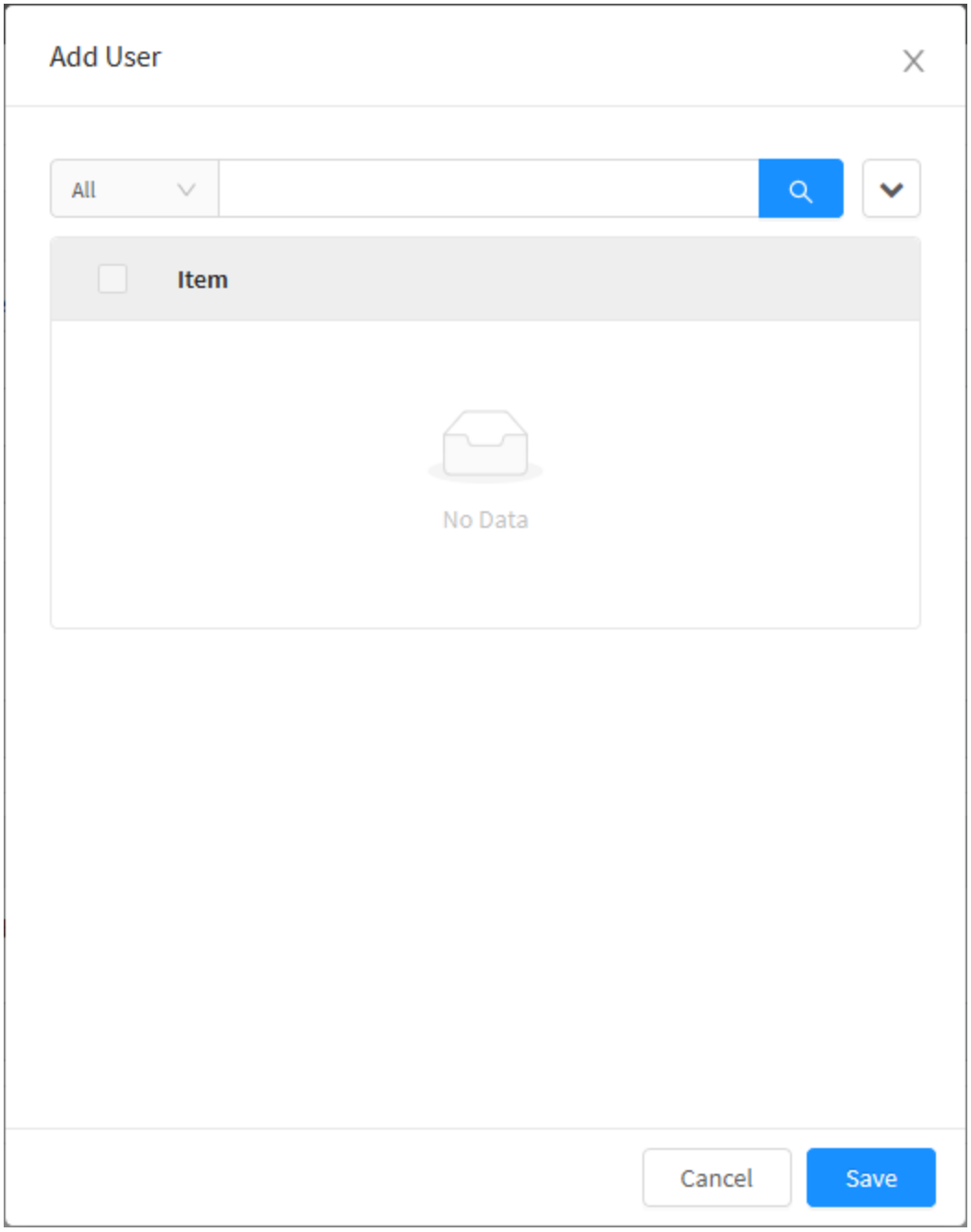
Identification

The **[Identification]** panel allows you to enable the authentication feature for the policy. Below is a description of every single field displayed in the **[Identification]** panel:



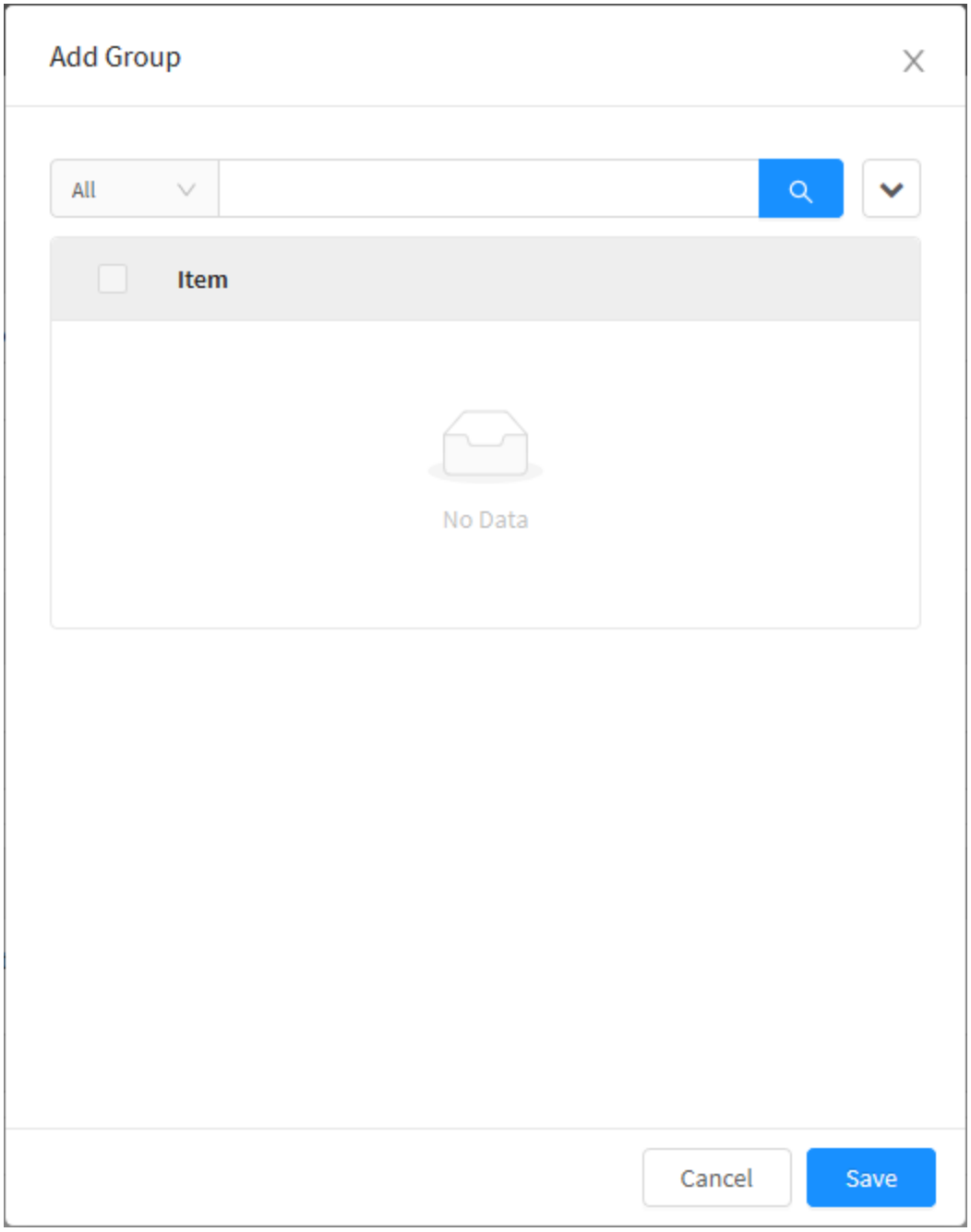
IPv4 Policies – *Connection - Identification*

- ***Authenticated[ ]*:** If enabled, this checkbox determines whether the policy requires authentication;
- ***Users[ ]*:** This field is only available by checking the checkbox and the *Authenticated* option. Allows you to specify users over whom the policy will be applied. When clicking on the **[ ] button**, the screen below will be displayed to select one or more users that will be affected by the rule;



IPv4 – Connection - Destination - Users

- ***Groups[ ]*:** This field is only available by checking the checkbox and the Authenticated option. Allows you to specify the group(s) to which the policy applies. When clicking on **[ ]**, the screen below will be displayed to select one or more groups that will compose the rule.



IPv4 – Connection - Destination - Groups

This feature requires web policies with the "Authentication" mode enabled so that they are redirected to the login page. When enabling the Explicit Proxy option, there are two authentication options; Basic, which generates an authentication pop-up, and the Captive Portal option, which will redirect to the authentication portal.

If the Explicit Proxy option is not activated, that is, if it is a Transparent Proxy, then the authentication will automatically be performed in the authentication portal (Captive Portal).

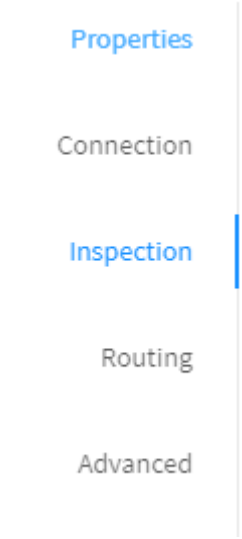
For additional information, check Proxy HTTP.

Next, we will analyze the *Inspection* tab.

- Routing;
- Advanced.

Create Policy - Inspection tab

In the **[Inspection]** tab, it is possible to select several resources to inspect the traffic affected by the policy.



IPv4 - Side Tabs - Inspection

This tab contains the panel

- *Inspection*;

Next, we'll look at it.

Inspection

Below is a description of the fields displayed in the **[Inspection]** panel:

- ***SSL Inspection[ ]:*** This field is only available by enabling the checkbox. This field allows the interception of SSL traffic allowing the inspection of its content. The options that appear in this menu are created in Proxy - SSL Inspection;
- ***Intrusion Prevention* [ ]:** This field is only available by enabling the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in Services - Intrusion Prevention;
- ***Threat Protection* [ ]:** This field is only available by checking the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in Services - Threat Protection;
- ***Application Control* [ ]:** This field is only available by checking the checkbox. This field allows you to select a profile to apply access control to applications. The profiles displayed in this menu are created in Services - Application Control;

  If an Application Control is added to a policy, the Web Filter is enabled in that policy, even if a Web Filter itself has not been selected.

- ***Web Filter* [ ]:** This field is only available by checking the checkbox. This field allows you to select a profile to perform content filtering. The profiles displayed in this menu are created in Services - Web Filter.

Next we will analyze the content of the *Routing* tab.

- Advanced.

Create Policy - Routing tab

In the **[Routing]** tab, you can set up NAT, SD-WAN profiles, QoS and Application Routing. We will analyze the function of each field in this tab.

The routing based on politics (*Policy-based Routing*) consists on a technique that forwards packages based on policies or filters. The network managers are able to apply policies in a selective way, based on specific parameters, such as origin and destination IP address origin or destination port, traffic type, access list, protocols, packets size, or other parameters and then route packets in routes predefined by the user. The main goal of routing based on policies is to make the network as agile as possible.

IPv4 - Side Tabs - Routing

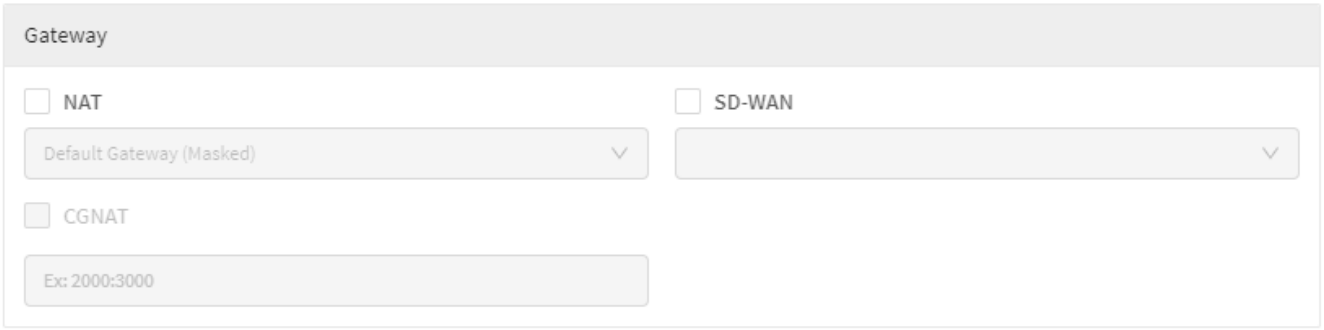
This tab contains the panels:

- *Gateway*;
- *QoS;*
- *Application Routing*.

Next, we will analyze the function of each of the panel's field.

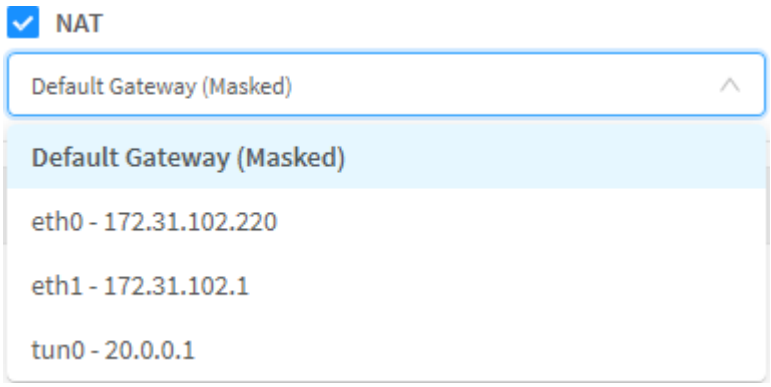
Gateway

Below is a description of the function of each form field displayed on the **[Gateway]** panel:



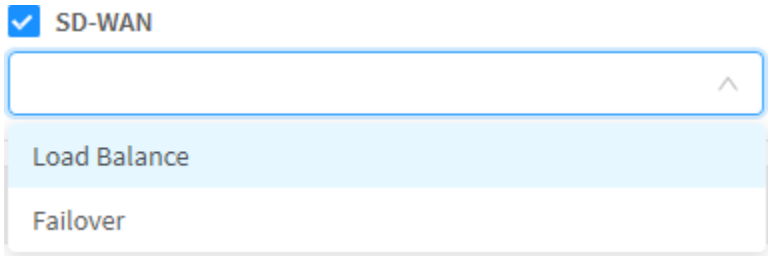
IPv4 – Routing - Gateway

- ***NAT[ ]*:** Allows you to activate NAT and choose the address for source translation, by default the IP of the Default Gateway link is configured;



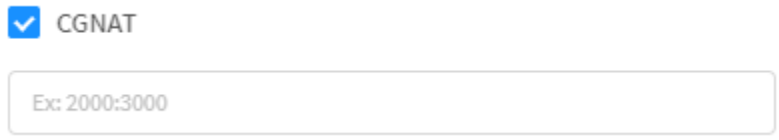
IPv4 – Routing - Gateway - NAT

- ***SD-WAN[ ]*:** It allows configuring the use of SD-WAN in the policy, being able to choose profile that apply to the policy;



IPv4 – Routing - Gateway - SD-WAN

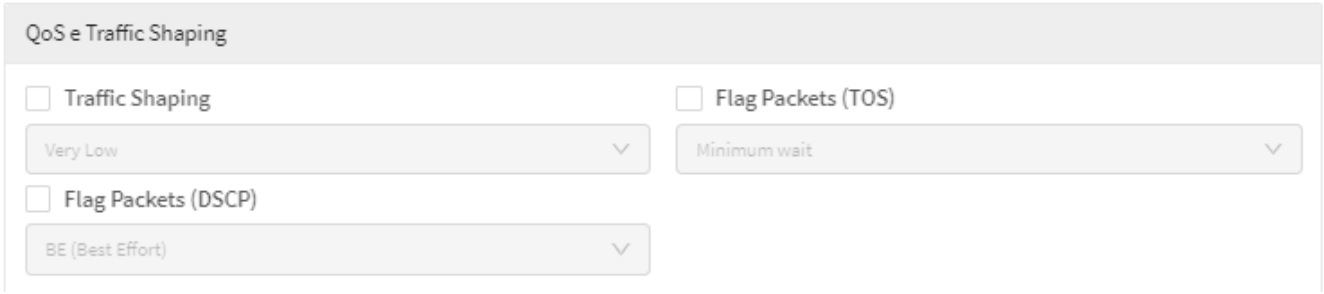
- ***CGNAT [ ]*:** It allows to set up the use of CGNAT in the policy. It is a NAT solution in a provider-level, where the same IP address can be assigned to different hosts at the same time, with different traffic ports. In order to use CGNAT, available ports must start from port 2000 (TCP and UDP).



IPv4 - Routing - Gateway - CGNAT

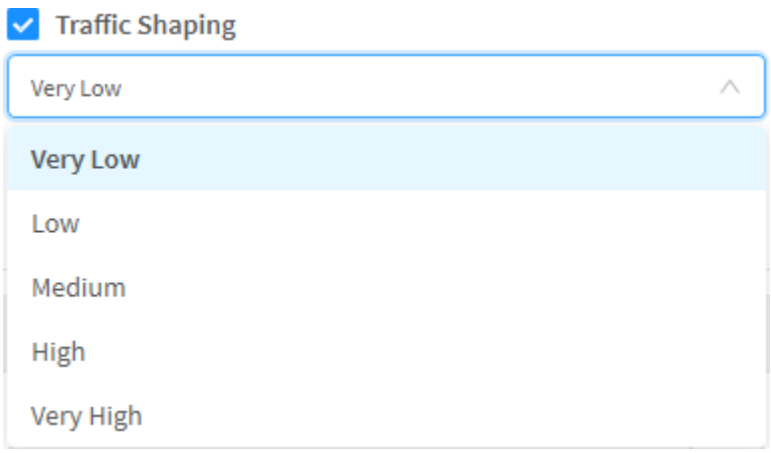
QoS

Below is a description of the function of each field displayed in the **[QoS]** panel:



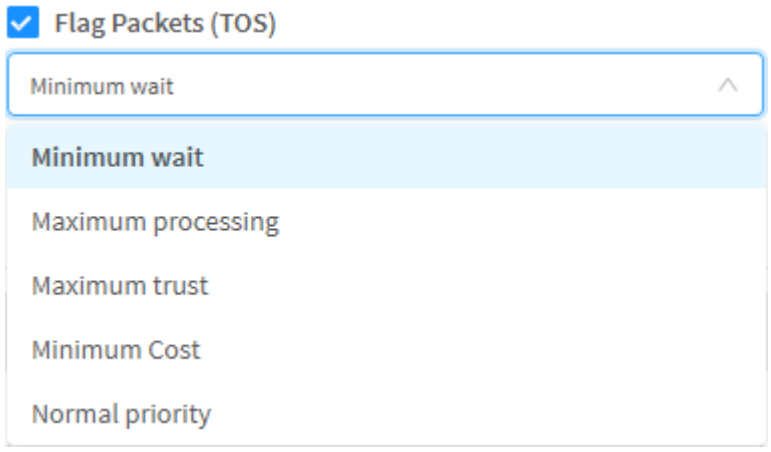
IPv4 – Routing - QoS

- ***Traffic Shaping[ ]:*** *It activates and selects the traffic priority, the values can be adjusted in* ***Settings Network Traffic Shaping;***



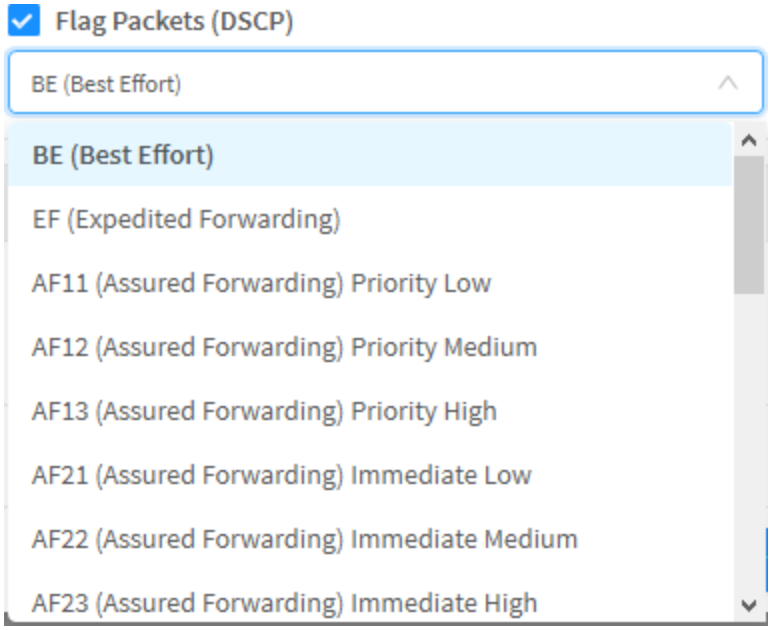
IPv4 – Routing - QoS - Traffic Shaping

- **Flag packets (*TOS*)[ ]:** Activating allows the package to be marked according to the options: Minimum wait, Maximum processing, Maximum reliability, Minimum cost and normal priority;



IPv4 – Routing - QoS - Flag packets (TOS)

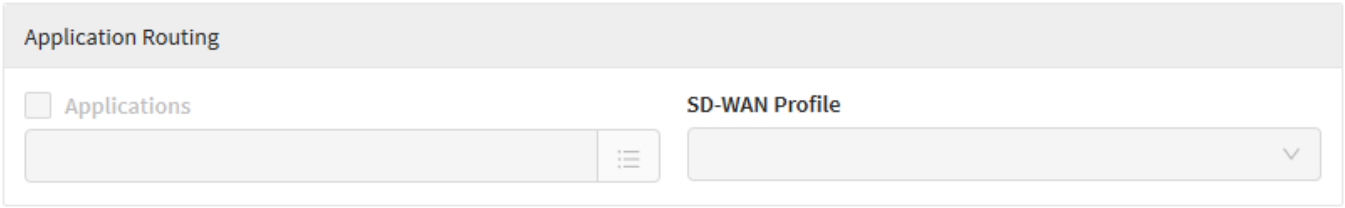
- ***Flag packets (DSCP)[ ]:*** Activating allows the package to be marked according to the options.



IPv4 – Routing - QoS - Flag packets (DSCP)

Application Routing

*The **[Application Routing]** panel is used to apply route balancing in certain applications, it is necessary to select at least one SD-WAN profile and activate the SSL Inspection*. Below is a description of the fields in the **[Application Routing]** panel:

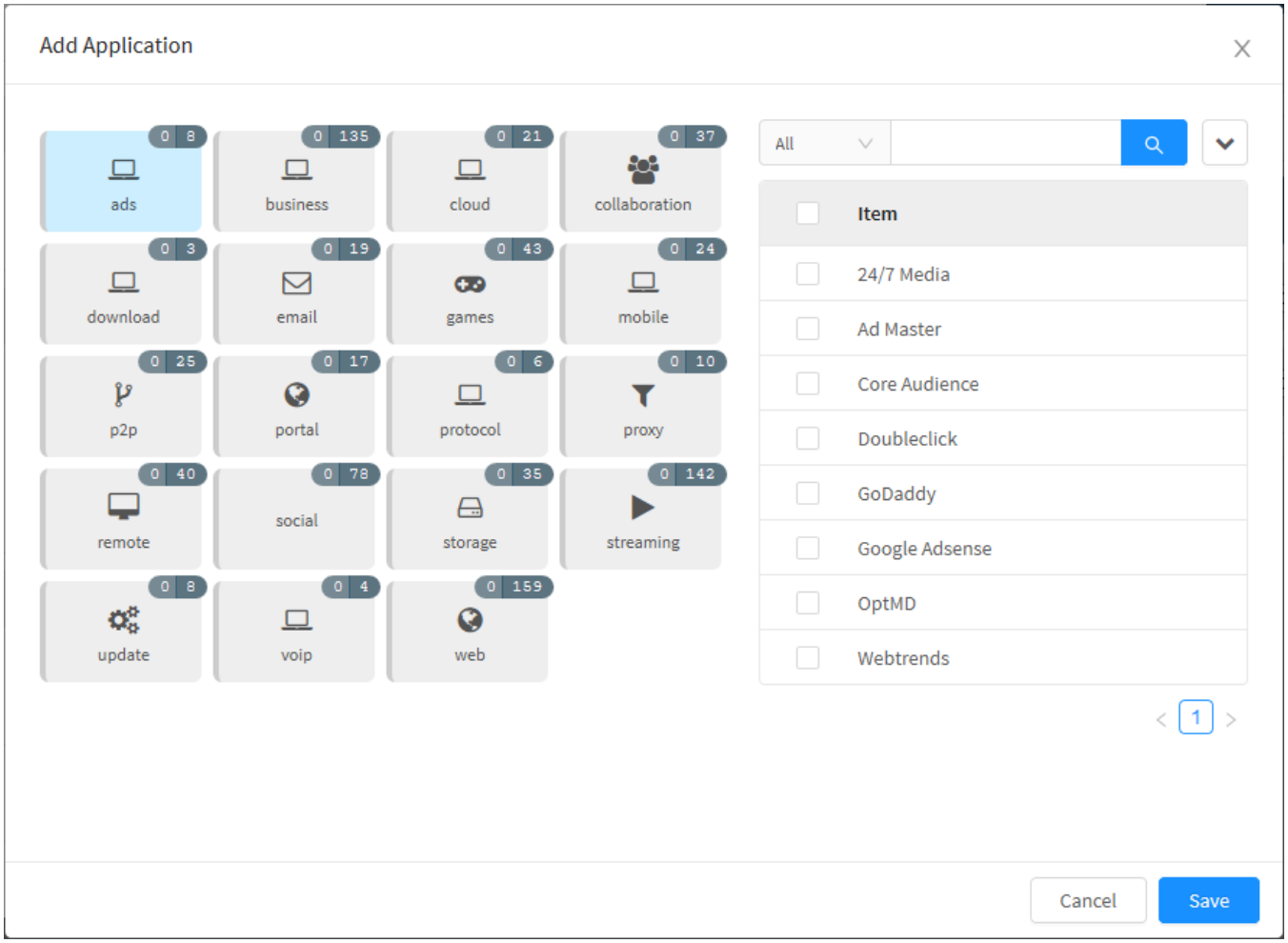


IPv4 – Routing - QoS - Application Routing

For the options in this panel to be available for editing, it is necessary to activate the SSL Inspection in the *Inspection* tab.

When applying application routing, traffic will follow a different path regardless of what was defined in the original connection's gateway.

- ***Applications[ ]:*** This field is only available by checking the checkbox. This field allows you to select applications so that requests received through the SD-WAN profile that is selected in the field below are routed, so that it is possible to obtain greater control over the consumption and bandwidth consumption of the selected applications. When clicking on the **[ ] button**, the screen below will be displayed to select one or more IP address objects that will compose the rule;



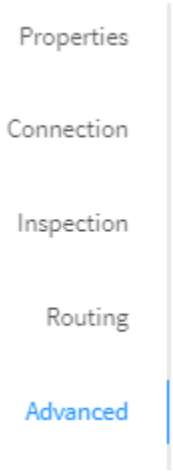
IPv4 – Routing - QoS - Application Routing - Applications

- ***SD-WAN Profile:*** This is a mandatory field. It is used to determine which SD-WAN profile will be used to balance the routes used by the selected applications. The profiles displayed on this menu are created in Services - SD-WAN.

Finally, we will analyze the Advanced tab.

Create Policy - Advanced tab

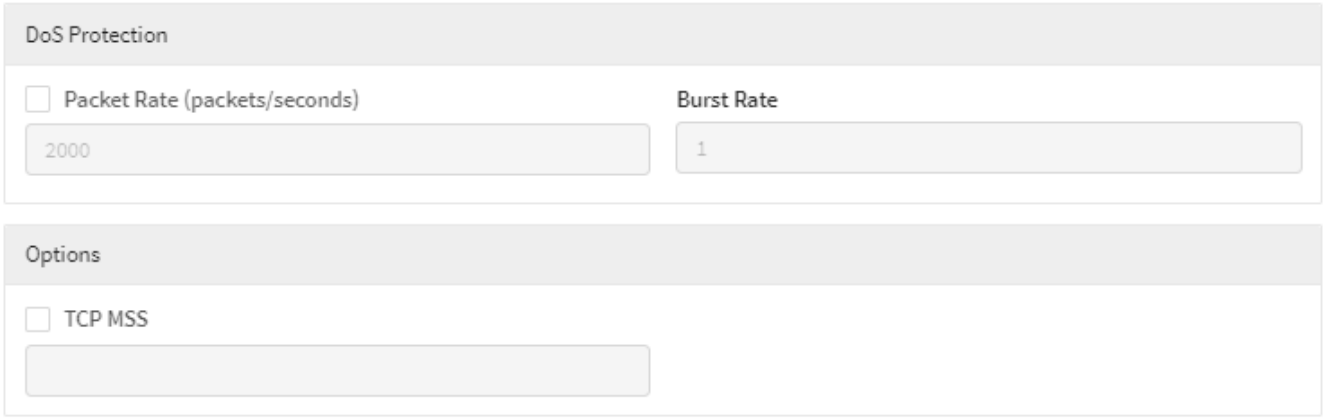
In the **Advanced** tab, it's possible to set the limits of the packages per second in a connection.



IPv4 - Side Tabs - Advanced

Advanced

Here is a description of the fields on the Advanced form:



IPv4 – Advanced

DoS Protection: With the DoS Protection box checked [☑] it's possible to limit the maximum quantity of packages per second in the Firewall, avoiding distributed attacks or traffic anomalies caused by possible malwares in the network.

- ***Packet Rate****:* The *Packet Rate* option sets up the *Firewall* in order to limit the connections to a maximum amount of packages per second.
- ***Burst Rate***: The *Burst Rate* option sets up the *Firewall* initially in order to allow a maximum quantity of packages per second without validating the Packet Rate to make the traffic control flexible in ocasional traffic peaks.

Options:

- ***TCP* MSS *[☑]*:** Allows the definition of a value that specifies the major quantity of data, in bytes, that a computer or communication device can receive in a single *TCP* segment.

This concludes the analysis of each panel. Next, we will analyze some examples of creating IPv4 policies.

Examples - Creating Policies

Next, we will exemplify the registration of some examples of policies as a way to demonstrate good practices. The model presented aims to guide the modeling of groups and policies based on the fundamental concept of ordering and treating policies, vis-a-vis “First match Wins”.

We will carry out the demonstration by creating the following policies:

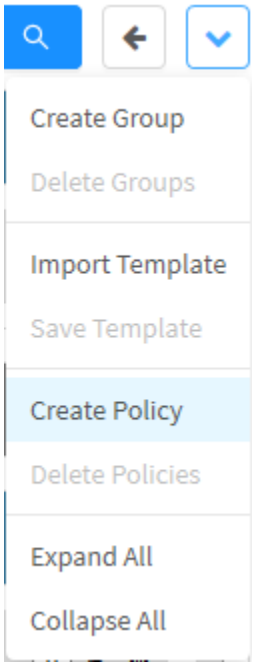
- Example 1 - Proxy Navigation Policy with ATP-enabled Deep Inspection;
- Example 2 - WEB Content Filter Policy - Blocking unproductive categories;
- Example 3 - Application Filter Policy - Blocking WEB 2 applications;
- Example 4 - NAT Policy - For MS Windows AD Server >> with destination >> Base UPDATE WSUS - without authentication and with IPS inspection;
- Example 5 - NAT policy for all protocols with DPI and Proxy.

Example 1 - Navigation Policy via ATP-enabled Proxy

Policy definition:

- ***[Properties]:*** *Web Navigation Users, Action: Allow; Enable traffic logging; Policy Group = Web Filter;*
- ***[Conditions]:*** *Zone = LAN, Authenticated, Services (HTTP; HTTPS);*
- ***[Inspection]:*** *SSL Inspection, Threat Protection and Web Filter;*
- ***[Routing]:*** *Medium Priority (Reservation 50% link) and TAG = Maintain the tags generated by the system.*

To add a security policy, in the **actions menu [ ]**, click on the “Create Policy” option;



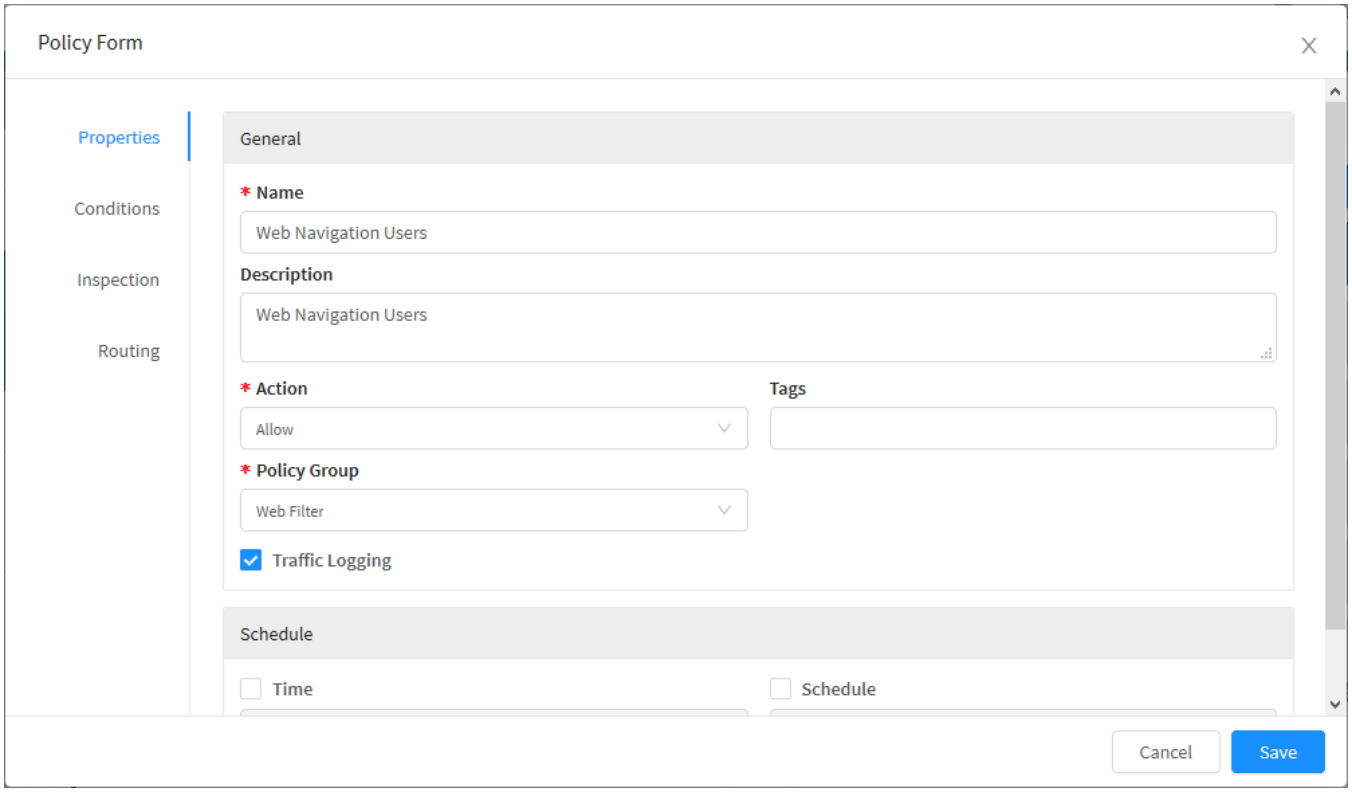
IPv4 - Actions Menu - Create Policy

Configure each tab according to the settings shown below.

Properties

- In the **[Properties]** tab, under **Name**, name it as: “Web Navigation Users”;
- In **Description**, type “Web Navigation Users”;
- In **Action** select the option “Allow”;
- In **Policy Group** select “Web Filter”;
- Select the ***Traffic Logging[ ]*** checkbox .

You will have set options just like the result illustrated by the image below:



Create Policy – Ex. 1 – *Properties*

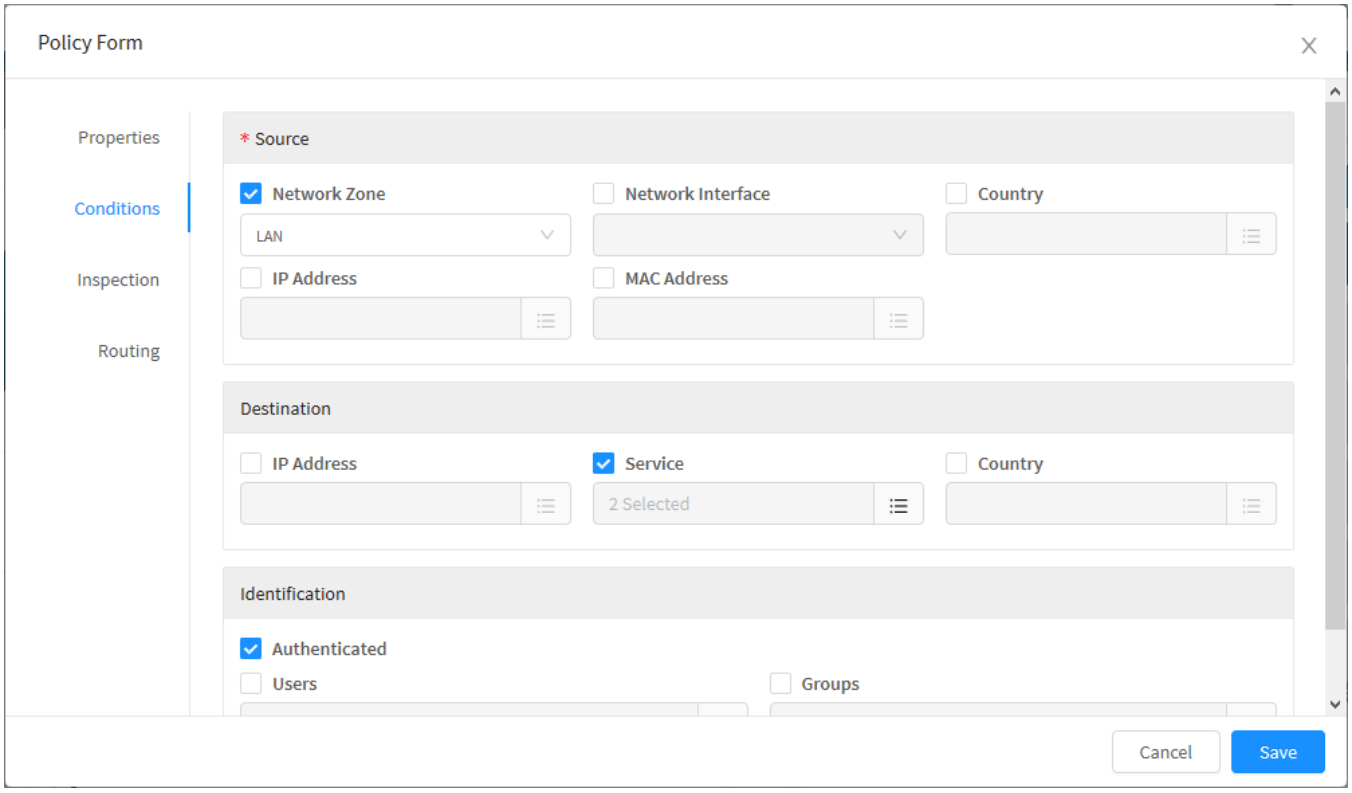
Select the next tab, **[Conditions]**.

Conditions

- In the **[Conditions]** tab, in **Network Zone** select: “LAN”;
- In **Service** select HTTP and HTTPS;
- Check the ***Authenticated [ ]*** checkbox.

You will have set options up just like the result illustrated by the image below:

When selecting HTTP and HTTPS services, speed up simply by typing "HTTP" in the search field, by default only HTTP and HTTPS services will appear, then just select both.



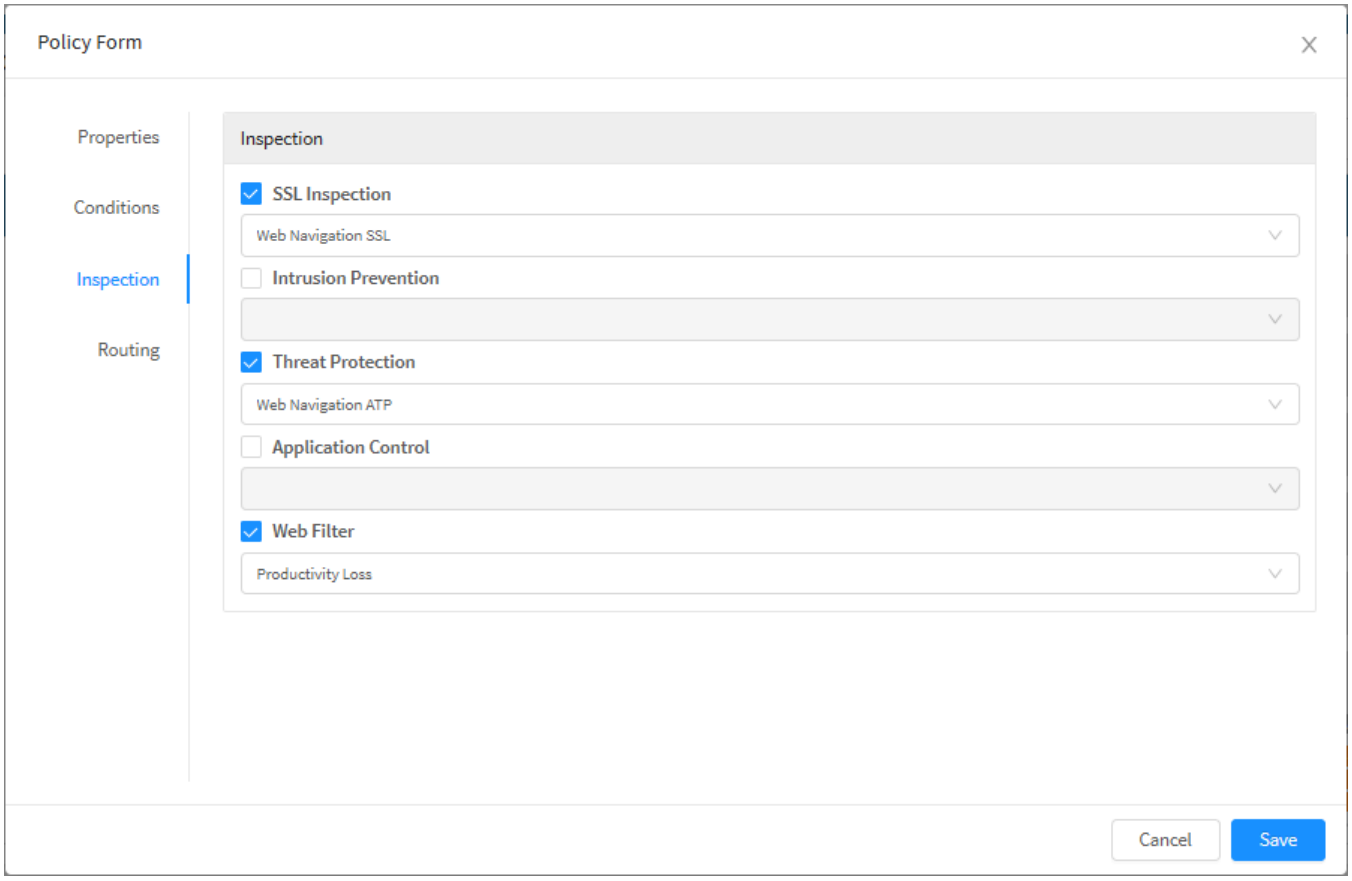
Create Policy – Ex. 1 – *Conditions*

Select the next tab, **[*Inspection*]**.

Inspection

- *On the **[Inspection]** tab, check the **SSL Inspection [ ]** checkbox and add a profile that inspects **HTTPS** (For more information, check this page);*
- *Select the **Threat Protection [ ]** checkbox and add the profile with the desired malware checks and blocks (For more information, check this page);*
- *Select the **Web Filter [ ]** checkbox and add the profile with the categories you want to filter (For more information, check this page);*

You will have arrived at the result illustrated by the image below:



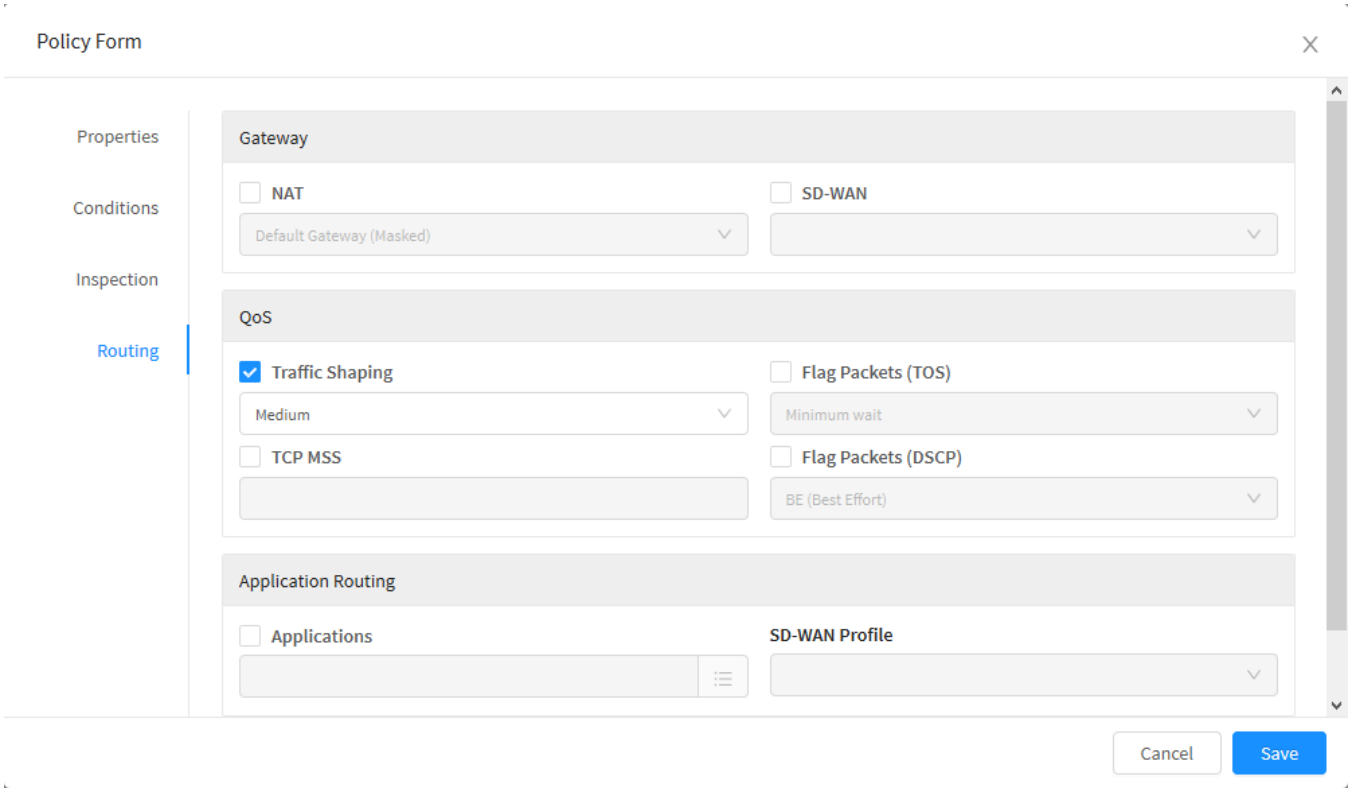
Create Policy – Ex. 1 – *Inspection*

Select the next tab, **[Routing]**.

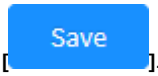
Routing

- On the **[Routing]** tab, select the ***Traffic Shaping [ ]*** checkbox and select the **Medium** option.

You will have arrived at the result illustrated by the image below:

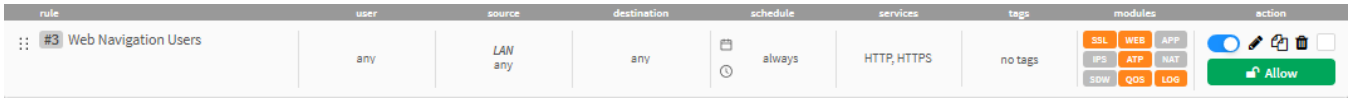


Add Policy – Ex. 1 – *Routing*

After configuring each tab according to the definition of the applied policy, click on **[**  **]**.

Policy successfully saved

The screen illustrated in the following image will be displayed:



Add Policy – Web Navigation Users

After saving, for the policy to take effect it will be necessary to access the **command queue [**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

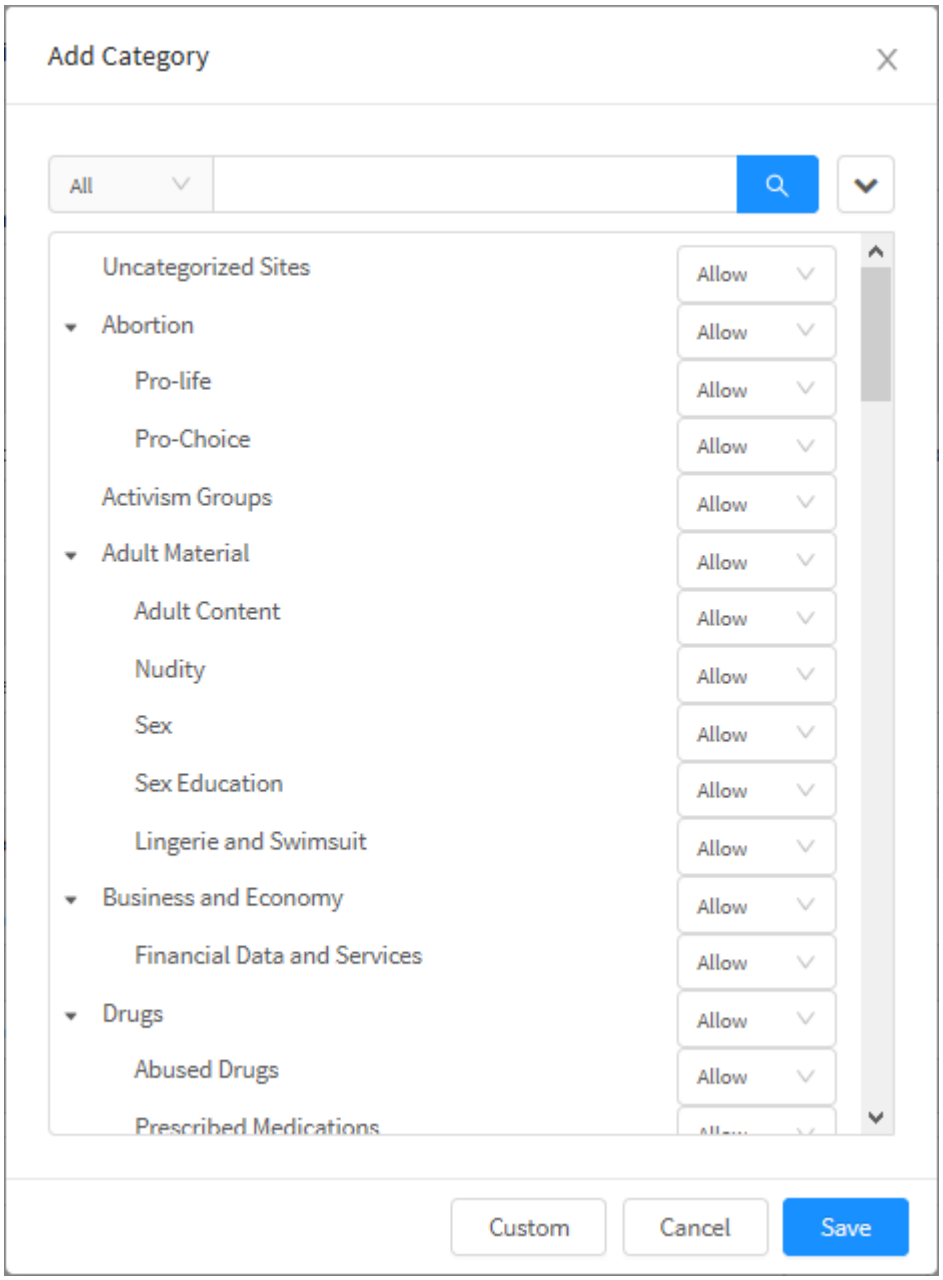
After performing these procedures, the policy will have been successfully configured.

In example 1 we defined and add a policy for web access with inspection, however, without restrictions or any type of filter.

Example 2 - Web Content Filter Policy - Blocking unproductive categories

We are going to add a policy by applying a content filter, we are going to define the parameters for this policy and consider the filter to URLs that are understood as “Unproductive” categories.

To define this list of categories, it is interesting to consult them first in *Diagnostics - Category Lookup*, or even browse the profiles in *Services - Web Filter* in Web Categories, click on **[ ]** in order to identify the categories that match this type of classification.



Services - Web Filter – Web Categories

List of categories identified as *unproductive*.

- Entertainment;
- *MP3*;
- Gambling and betting;

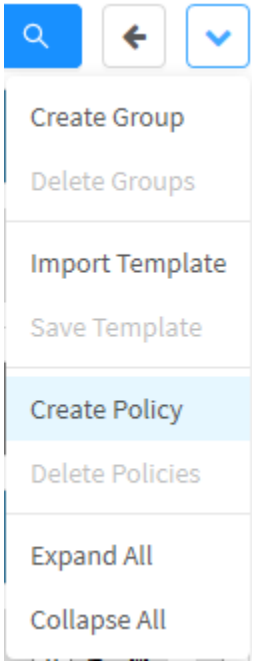
- Games;
- Bandwidth management;
- *Internet radio and TV*;
- Streaming media;
- Society and lifestyles;
- Personal ads and dating;
- *Personal Web Sites*;
- Sports;
- Tourism.

Below is a summary of what will be configured in the rule:

- **[*Properties*]:** *Productivity Loss, Enable traffic logging; Policy Group=Web Filter; TAG = Block;*
- **[Conditions]:** IP network zone = "LAN"; Services (HTTP; HTTPS); Authenticated;
- ***[Inspection]:*** *SSL Inspection and Web Filter;*
- **[Routing]:** No controls.

To add a security policy follow the steps:

To add a security policy, in the **action menu [**  **]**, click on the “Create Policy” option;



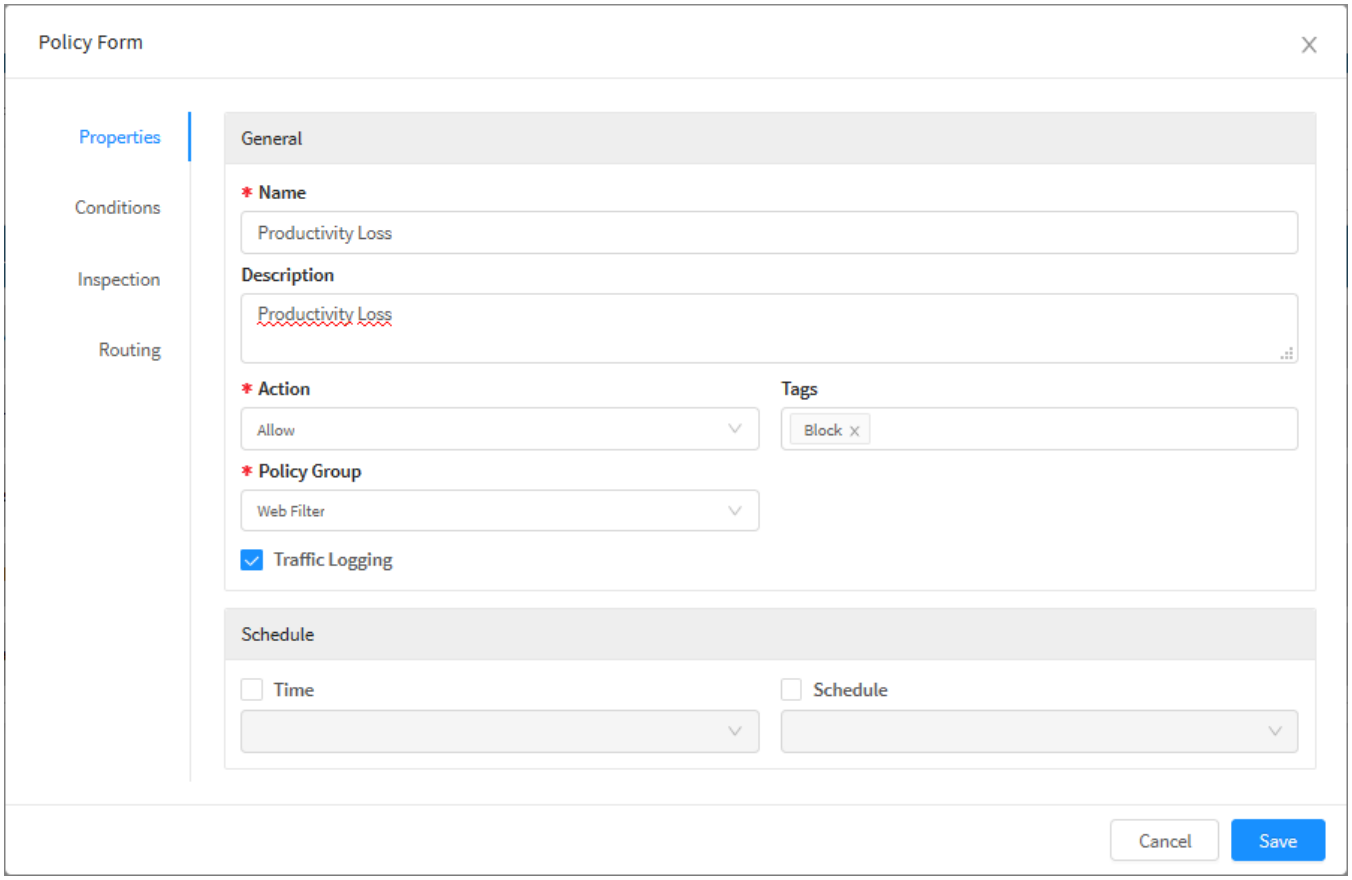
IPv4 - Actions Menu - Create Policy

Configure each tab according to the settings shown below.

Properties

- In the **[Properties]** tab, in **Name**, name it as: “Productivity Loss”;
- In **Description** type “Productivity Loss”;
- In **Action** leave the option "Allow", you will make the block through the profile of Web Filter;
- In **Policy Group** select “Web Filter”;
- In **Tags** type “Block”;
- Select the Traffic Logging checkbox ***Traffic Logging [***  ***]***.

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 2 – *Properties*

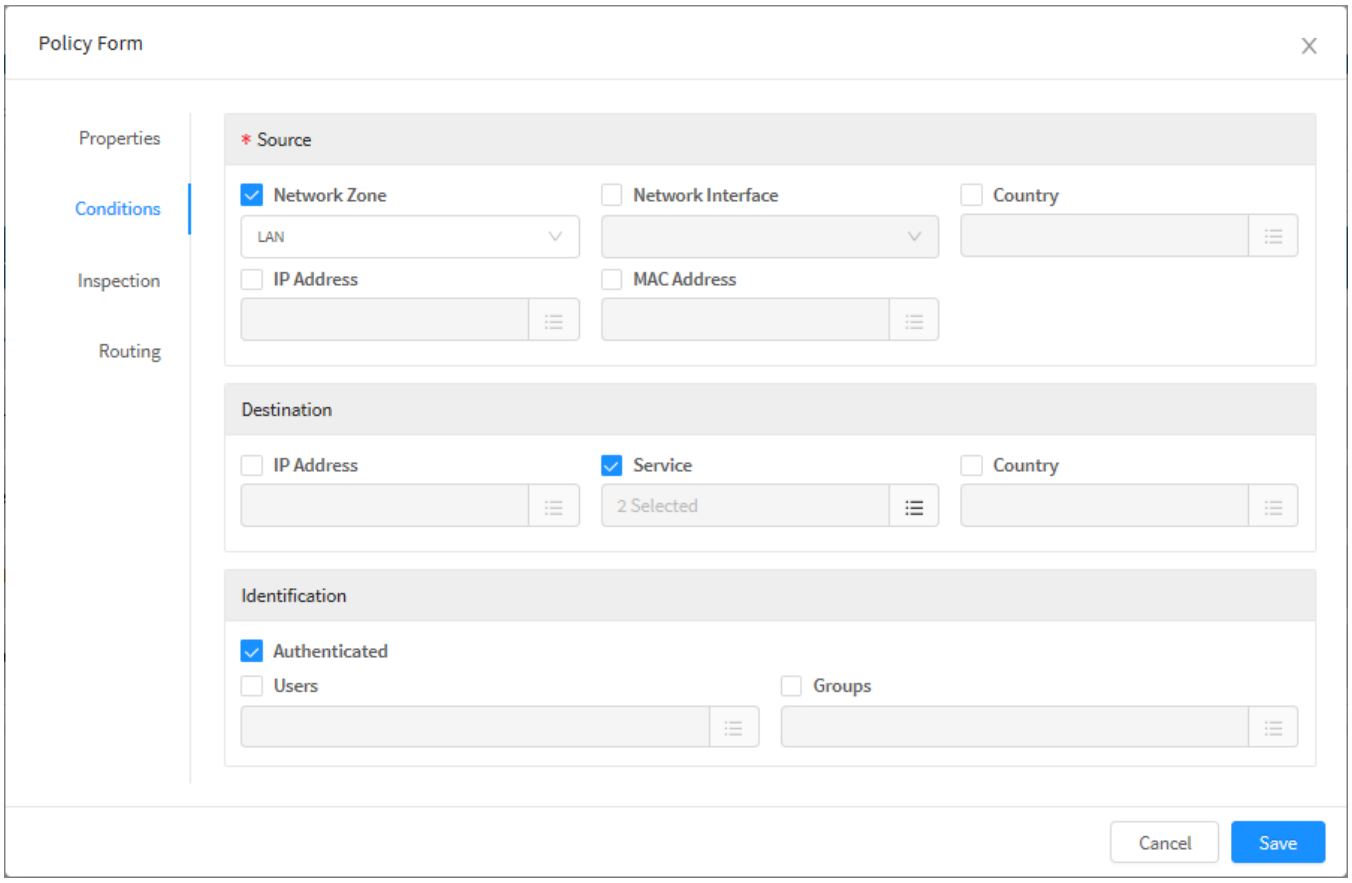
Select the next tab, **[Conditions]**.

Conditions

- In the **[Conditions]** tab, in **Network Zone** select: “LAN”;
- In **Service** select HTTP and HTTPS services;
- Select the ***Authenticated [ ]*** checkbox.

You will have arrived at the result illustrated by the image below:

When selecting HTTP and HTTPS services, speed up simply by typing "HTTP" in the search field, by default only HTTP and HTTPS services will appear, then just select both.



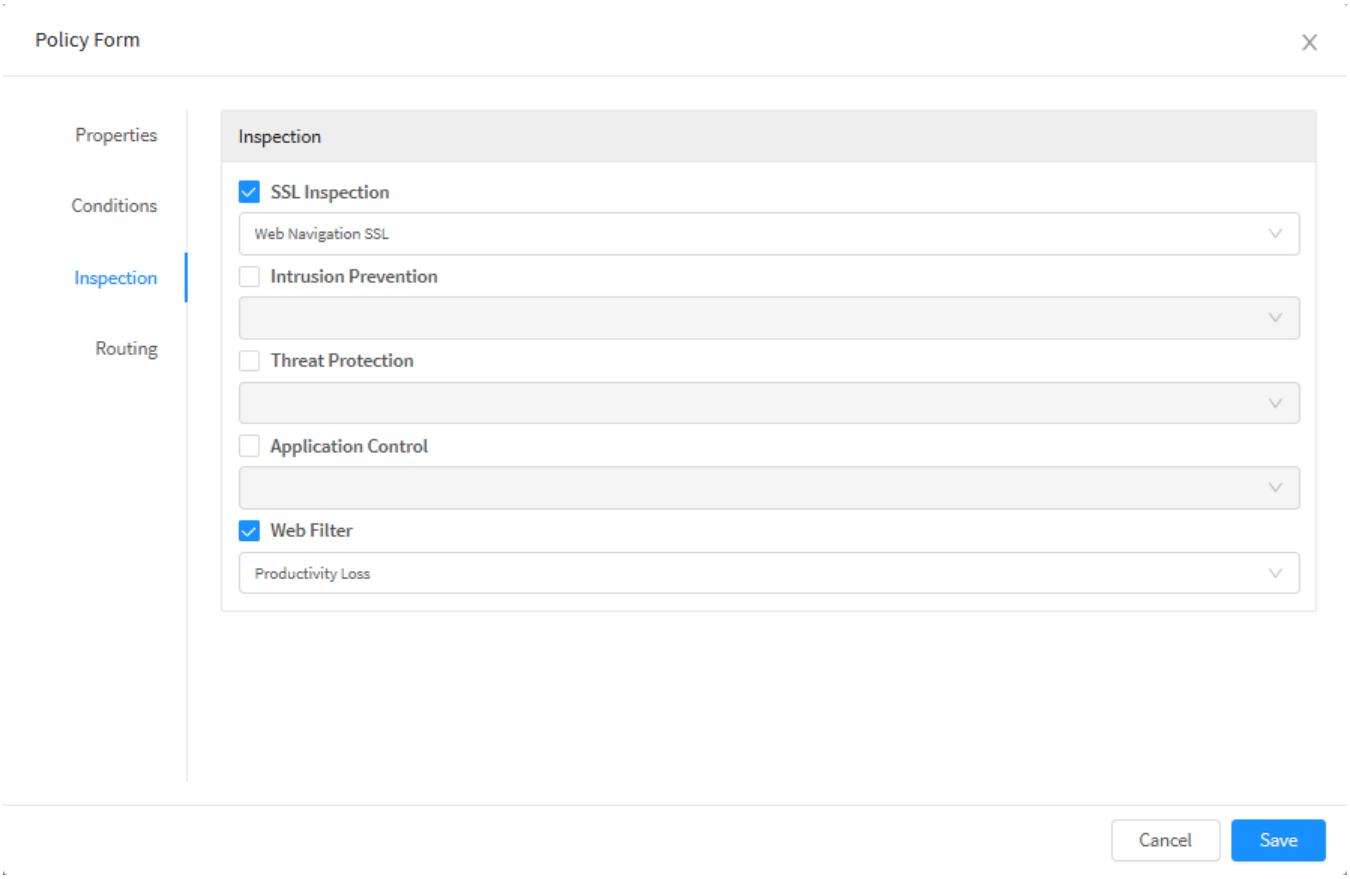
Create Policy – Ex. 2 – *Conditions*

Select the next tab, **[Inspection]**.

Inspection

- On the **[Inspection]** tab, check the ***SSL Inspection [✓]*** checkbox and add a profile that inspects **HTTPS** (For for more information, check this page);
- Select the ***Web Filter [✓]*** checkbox and select the profile related to the *unproductive* categories (For more information, check this page);

You will have set options up just like the result illustrated by the image below:

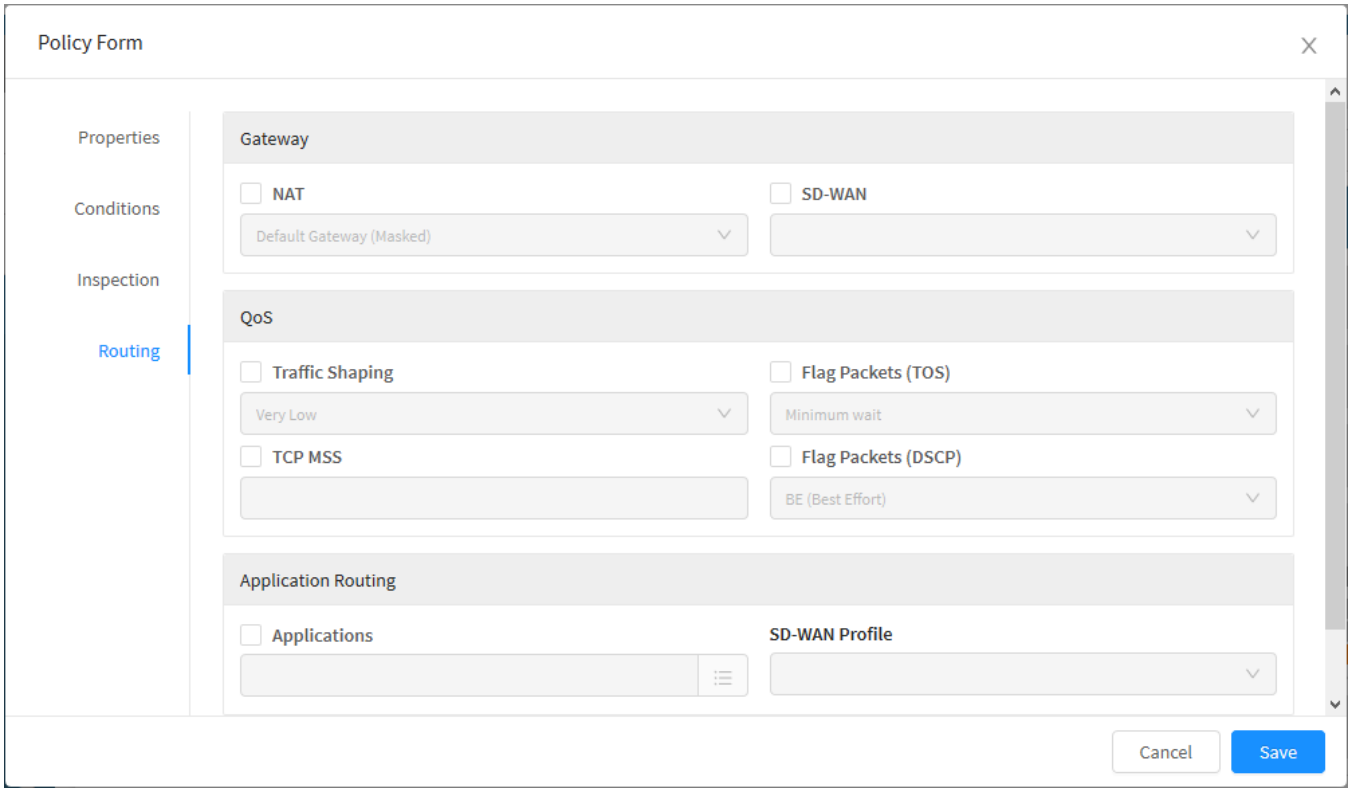


Create Policy – Ex. 2 – *Inspection*

Select the next tab, **[Routing]**.

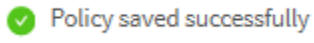
Routing

In the **[Routing]** tab, no control will be activated, as exemplified by the following image:



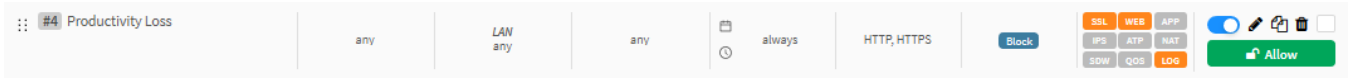
Create Policy – Ex. 2 – *Routing*

After configuring each tab according to the definition of the applied policy, click on [Save].



Policy successfully saved

The screen illustrated in the following image will be displayed:



Create Policy – Productivity Loss

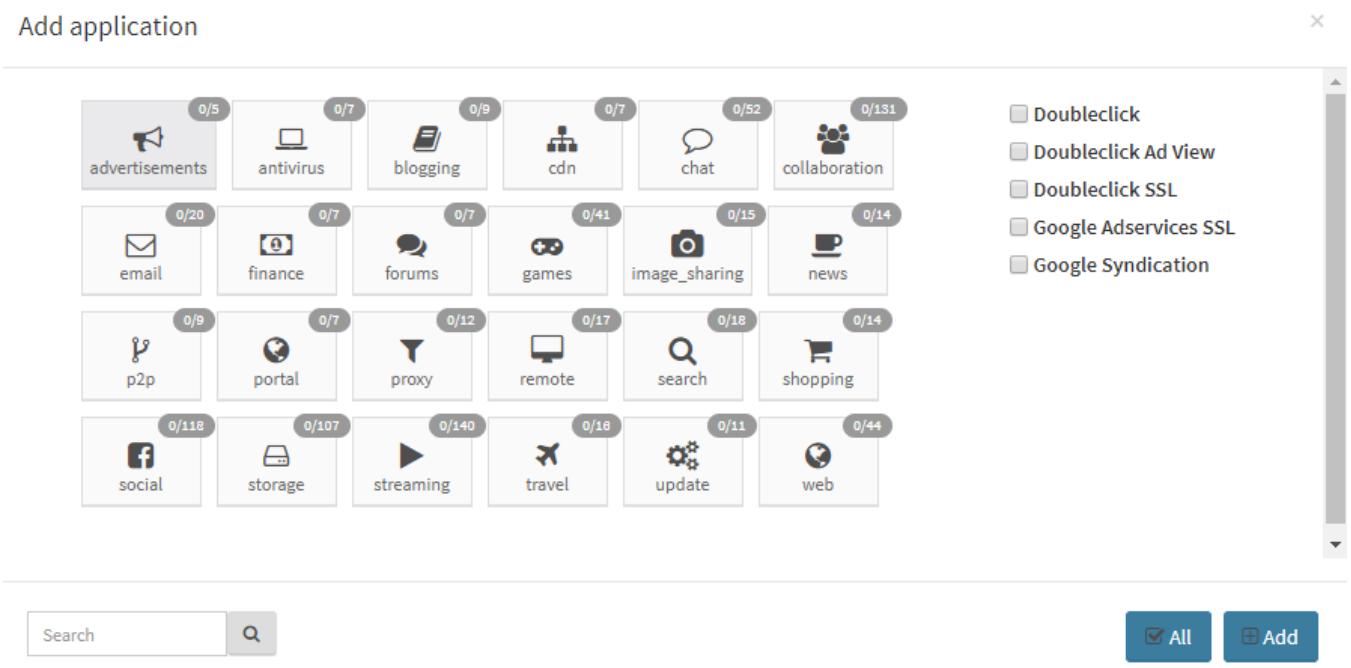
After saving, for the policy to take effect it will be necessary to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures, the policy will have been successfully configured.

In example 2, we define and add a blocking policy for some categories of unproductive content sites.

Example 3 - Application Filter Policy - Blocking cloud application control

Let's add a policy by applying application filters. We will consider filtering on *Urls* or *websites* that run applications that understand the actions of unproductiveness and security risk. Let's see the list of applications that we can filter in the localized Services - Application Control profiles, in Applications click on **[ ]**, this panel aims to identify cloud applications that fit this type of classification.



Application Control – Add application

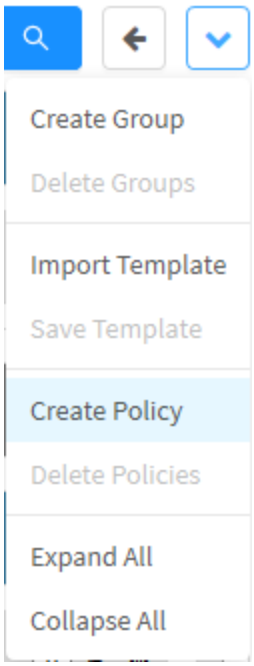
List of applications identified as unproductive or security risk.

- *Baidu Movies*;
- *CDN – Content Delivery Network* (messengers);
- *Dropbox*;
- *Facebook* (all);
- *Google Drive*;
- *Google Drive Upload*;
- *Google Mail*;
- *Google Photos* / *Google + Photos*;
- *One Drive*;
- *Skype Call Start*;
- *Skype Call End*.

Here is a summary of what will be configured in the rule:

- **[*Properties*]:** *WEB – APP Block, Action: Allow; TAG = Block;*
- **[Conditions]:** Zone = *LAN, Authenticated;*
- **[Inspection]:** *SSL Inspection, Application Control and Web Filter;*
- **[*Routing*]:** No controls.

To add a security policy, in the action menu **[ ]**, click on the “Create Policy option” ;



IPv4 - Actions Menu - *Create Policy*

Configure each tab according to the settings shown below.

Properties

In the **[Properties]** tab, in **Name**, name it as: “WEB - APP Block”;

In **Description** type “WEB - APP Block”;

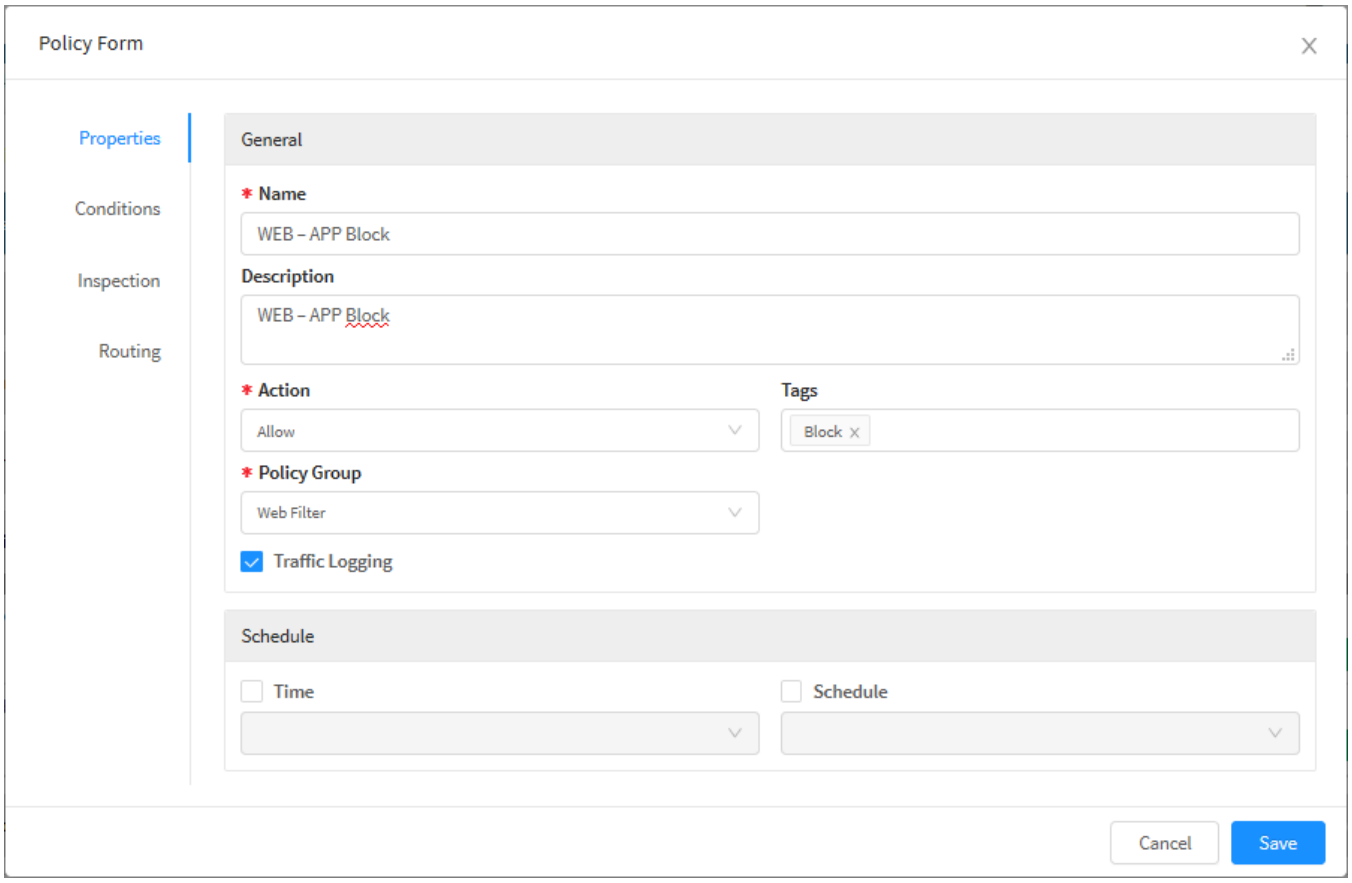
In **Action** leave the option "Allow", you will make the block through the profiles of Web Filter and Application Control;

In **Policy Group** select “Web Filter”;

In **Tags** type “Block”;

Select the ***Traffic Logging[ ]*** checkbox.

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 3 – *Properties*

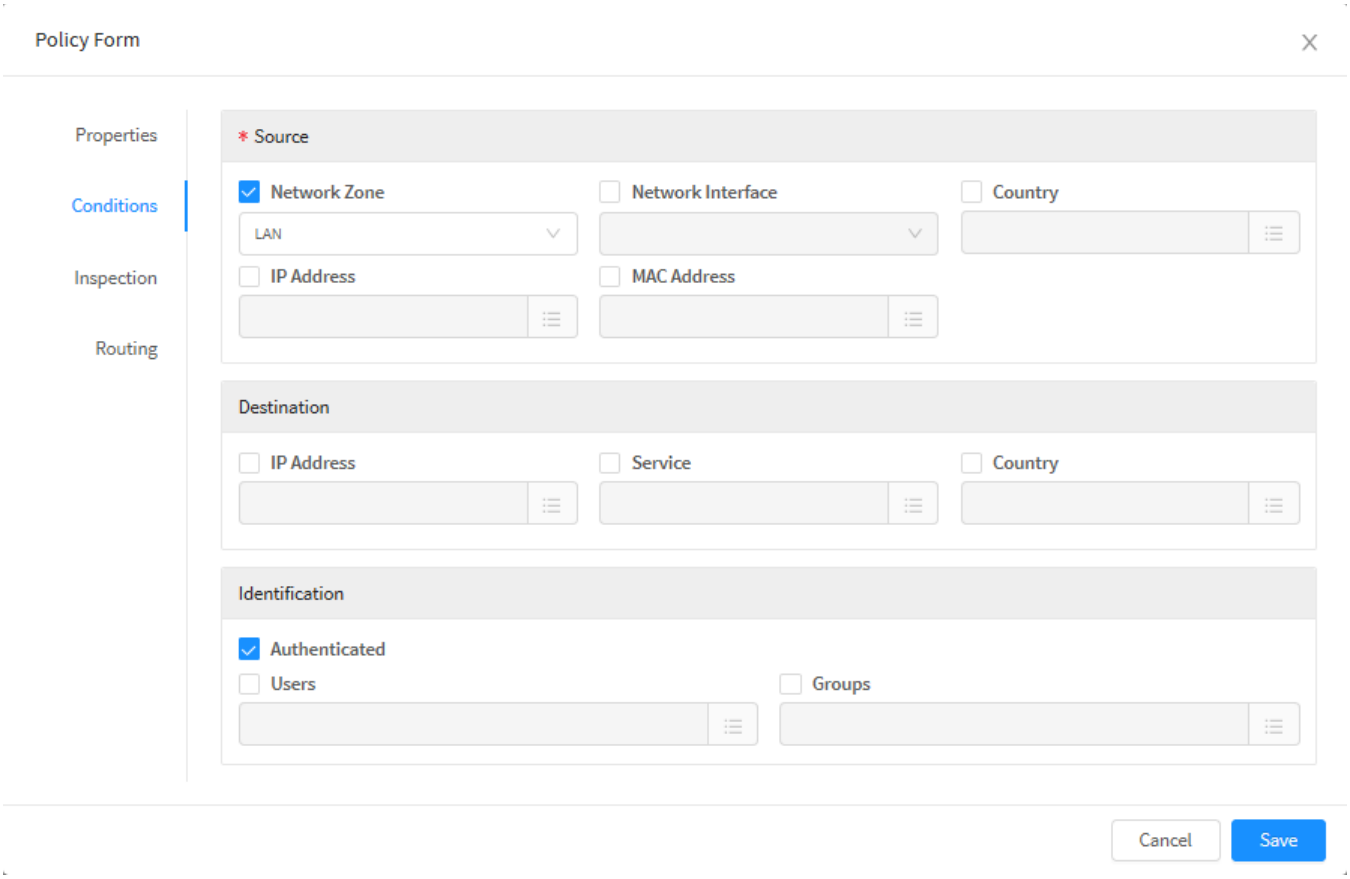
Select the next tab, **[Conditions]**.

Conditions

In the **[Conditions]** tab, in **Network Zone** select the option: “LAN”;

In **Identification** select the checkbox ***Authenticated[ ]***;

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 3 – *Conditions*

Select the next tab, **[Inspection]**.

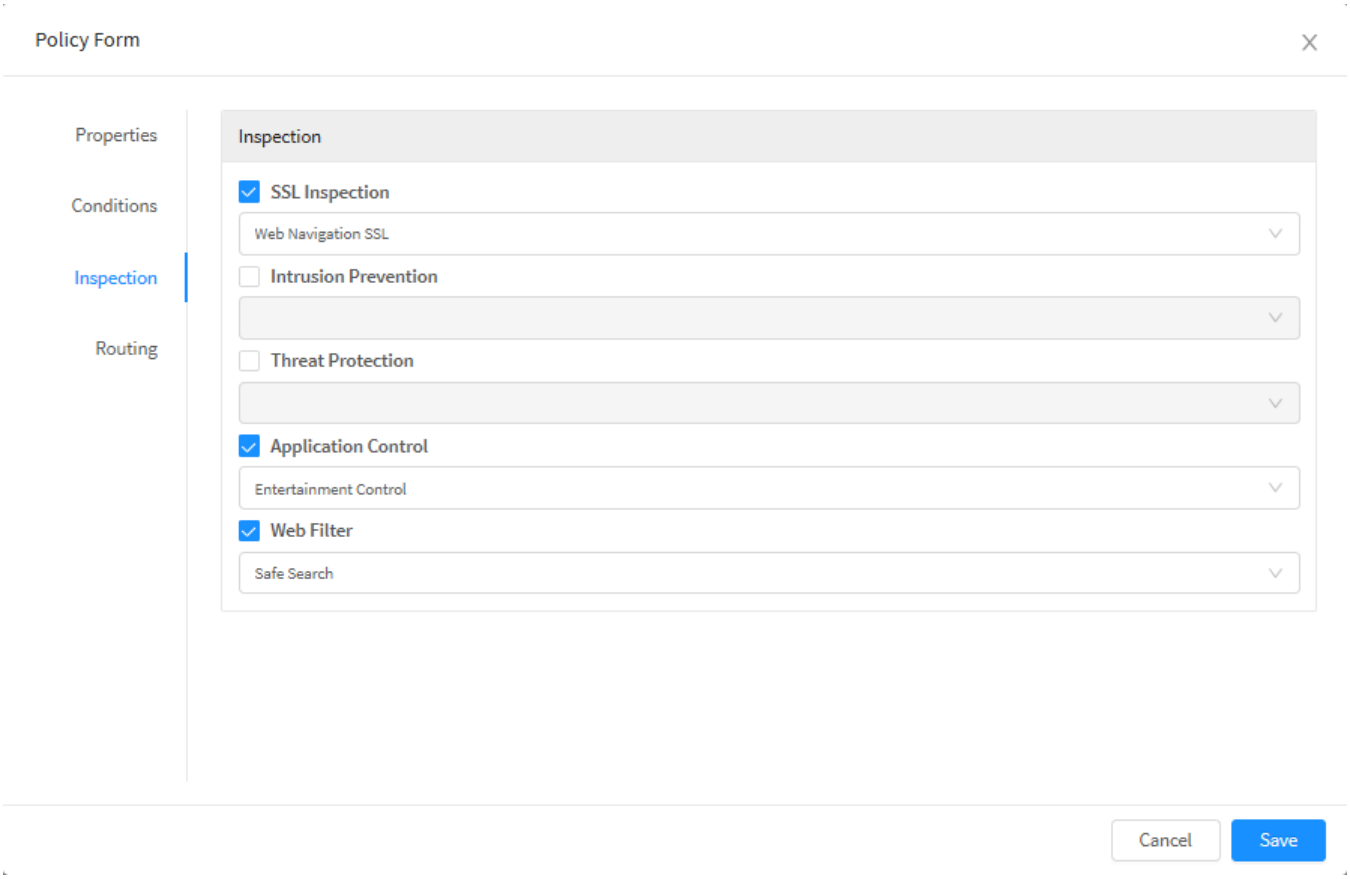
Inspection

On the **[Inspection]** tab, check the ***SSL Inspection[ ]*** checkbox and add a profile that inspects ***HTTPS*** (For more information, check this page);

Select the ***Application Control[ ]*** checkbox and select the profile related to all *unproductive* or *risky application categories* (For more information, check this page);

Select the ***Web Filter[ ]*** checkbox and select the profile related to the *unproductivity* or *risk categories* (For more information, check this page);

You will have arrived at the result illustrated by the image below:

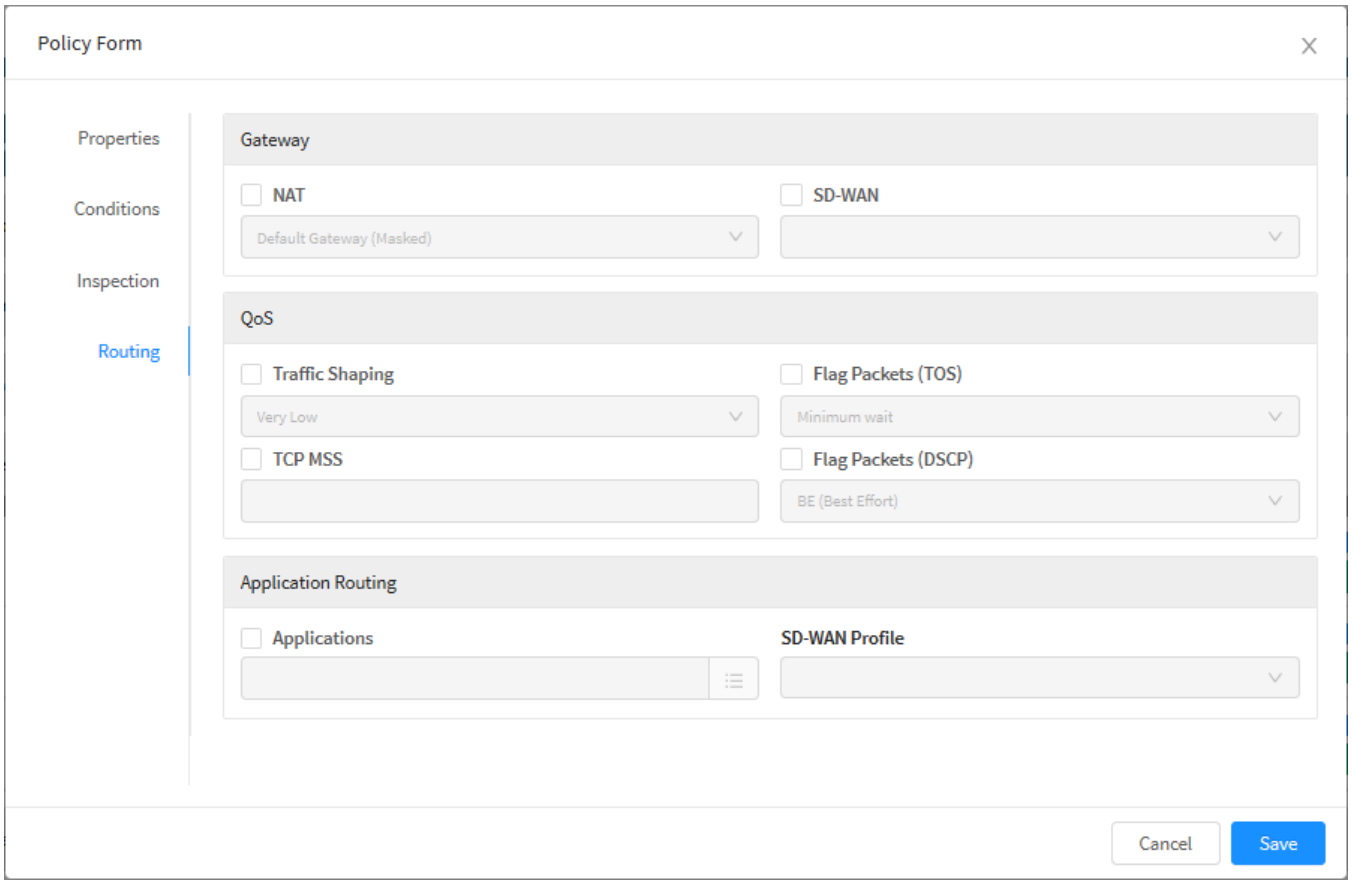


Create Policy – Ex. 3 – *Inspection*

Select the next tab, **[Routing]**.

Routing

In the **[Routing]** tab, no control will be activated, as exemplified by the following image:

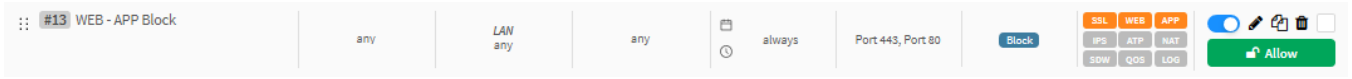


Create Policy – Ex. 3 – *Routing*

After configuring each tab according to the definition of the applied policy, click on **[** Save **]**.

Policy successfully saved

The screen shown on the following image will be displayed:



Create Policy – WEB - APP Block

After saving, for the policy to take effect it will be necessary to access the command queue **[** **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures, the policy will have been successfully configured.

In example 3 we defined and added a “categories and apps” blocking policy for inappropriate or unproductive content.

Example 4 - NAT Policy - For MS Windows AD Server destined for UPDATE WSUS Base - Without authentication and with IPS inspection

We will add a policy applying “NAT (Network Address Translation)” for different services. Let's consider the example:

Windows server masking for the WSUS service. In order to allow automatic UPDATE without requiring authentication.

Link to MS documentation - How to set up a network connection for MS WSUS

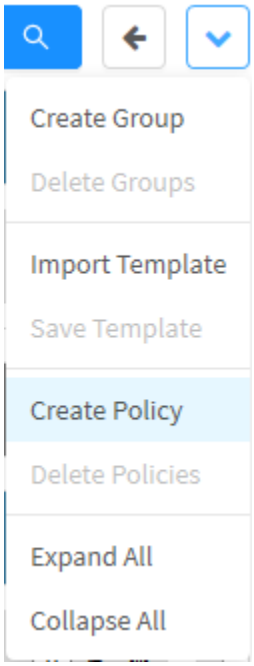
https://technet.microsoft.com/en-us/library/cc708602(v=ws.10).aspx

For specific cases, first define and configure the objects that will be used in the policy.

Below is a summary of what will be configured in the rule:

- **[*Properties*]:** *NAT: MS-WSUS Servers, Action: Allow; TAG = NAT;*
- **[Conditions]:** Zone = *WAN;*
- **[Inspection]:** *Intrusion Prevention;*
- **[*Routing*]:** Enable *[Nat]; SD-WAN*= Performance *BB; Traffic Shaping= Very high.*

To add a security policy, in the action menu **[ ]**, click on the “Create Policy” option;



IPv4 - Actions Menu - *Create Policy*

Configure each tab according to the settings shown below.

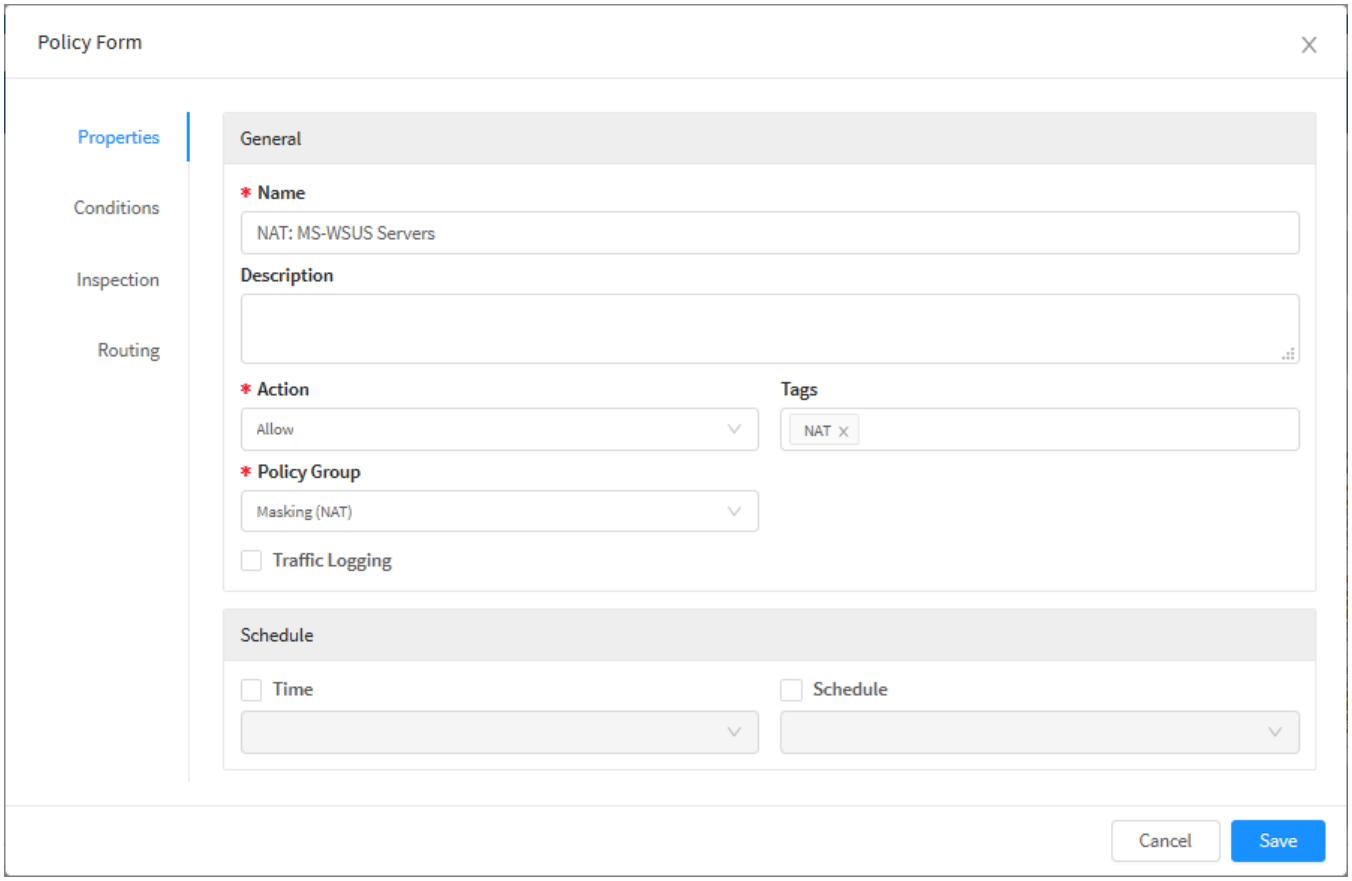
Properties

In the **[Properties]** tab, in **Name**, name it as: “NAT: MS-WSUS Servers”;

In **Tags** include “NAT”;

In **Policy Group** select “Masking (NAT)”;

You will have arrived at the result illustrated by the image below:



Add Policy – Ex. 4 – *Properties*

Select the next tab, **[Conditions]**.

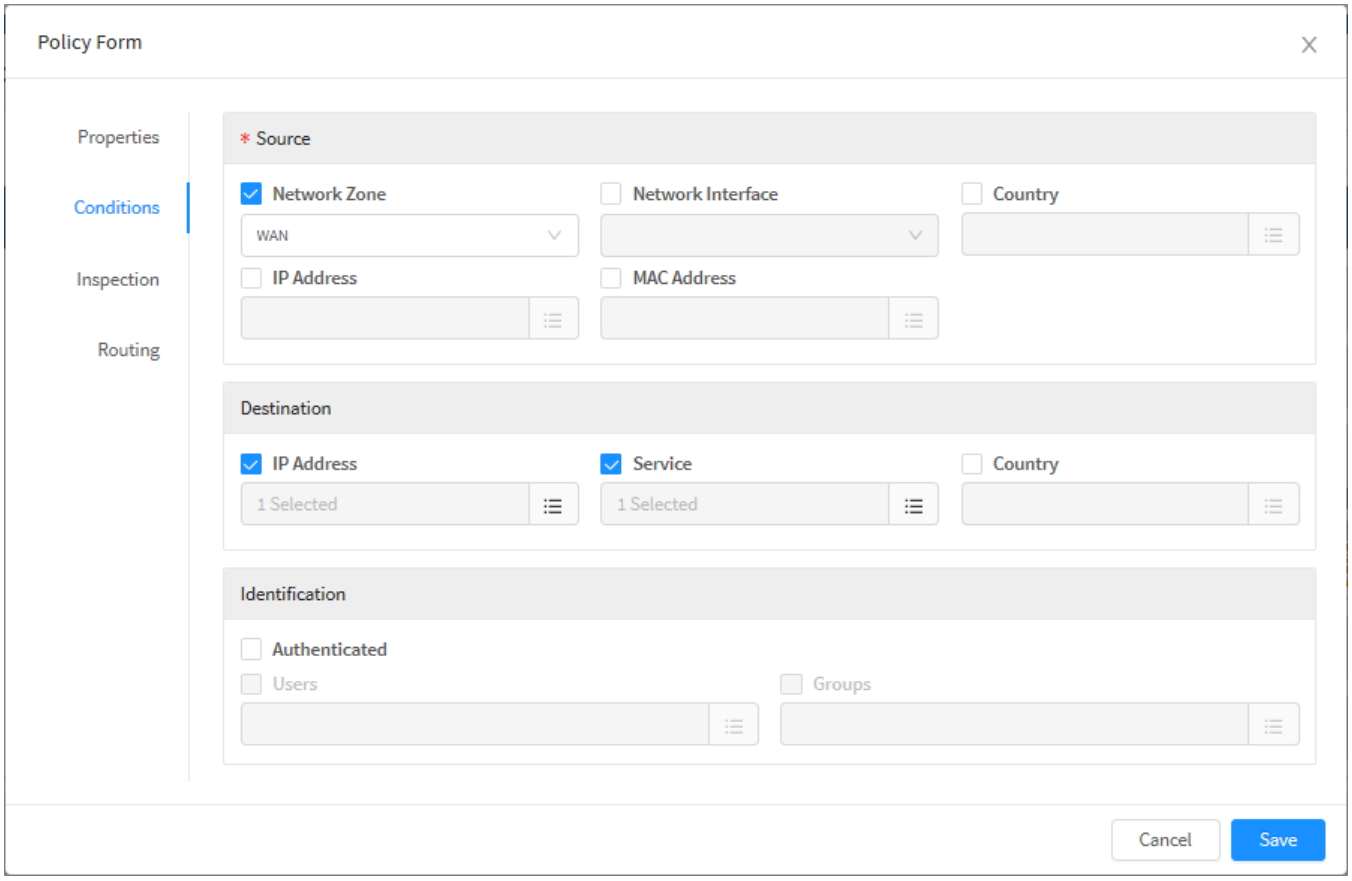
Conditions

In the **[Conditions]** tab, in Network Zone select "WAN";

IP Address select: “Server Windows AD / LDAP” (If it is necessary to add a new one, check this page);

In Service select “Services UPDATE MS WSUS” (If it is necessary to add a new one, check this page);

You will have arrived at the result illustrated by the image below:



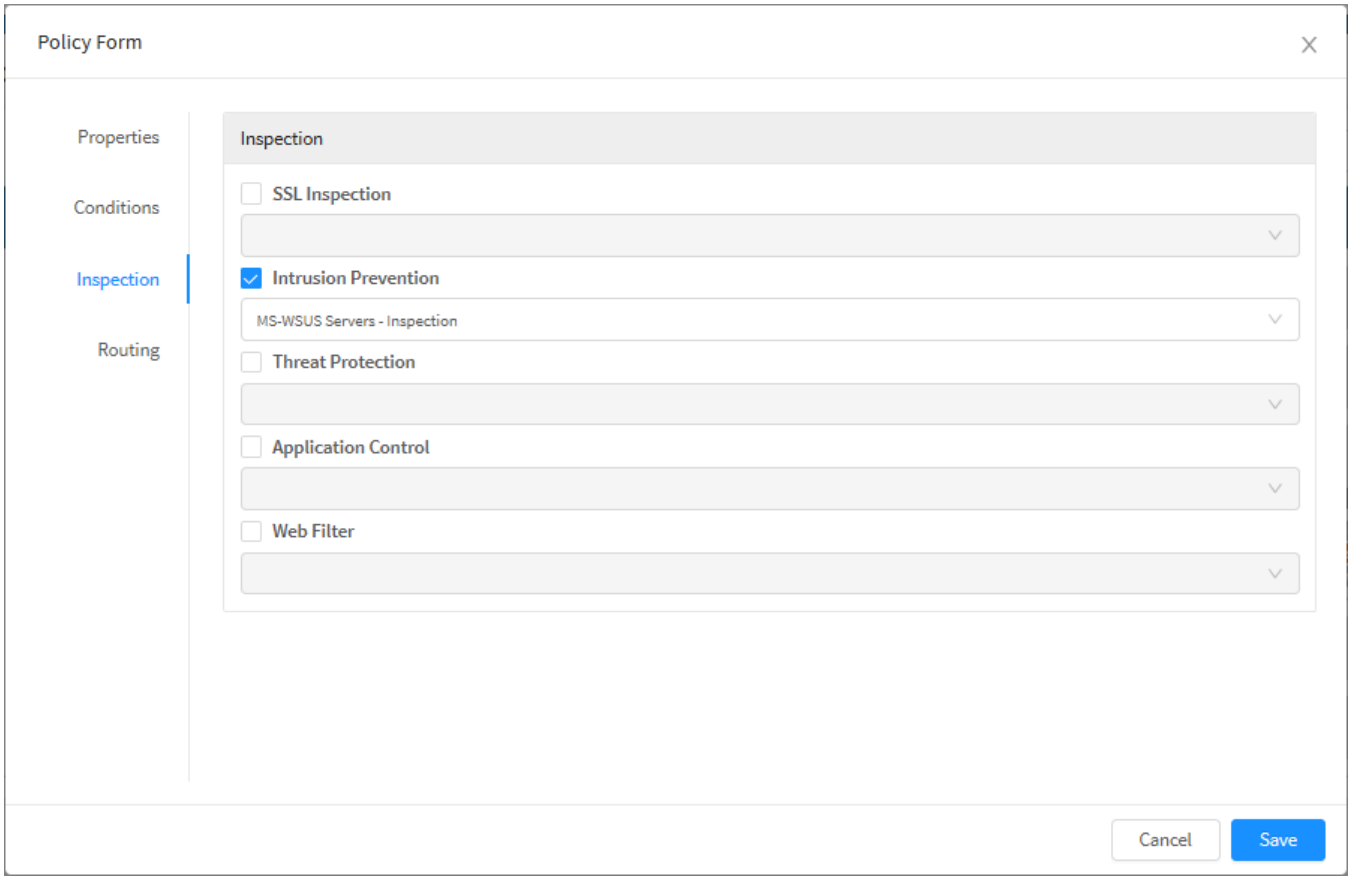
Create Policy – Ex. 4 – *Conditions*

Select the next tab, **[Inspection]**.

Inspection

In the **[Inspection]** tab, enable the check box for ***Intrusion Prevention*** **[ ]** and select a profile to perform Deep Inspection (For more information, check the *Services - Intrusion Prevention*);

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 4 – *Inspection*

Select the next tab, **[Routing]**.

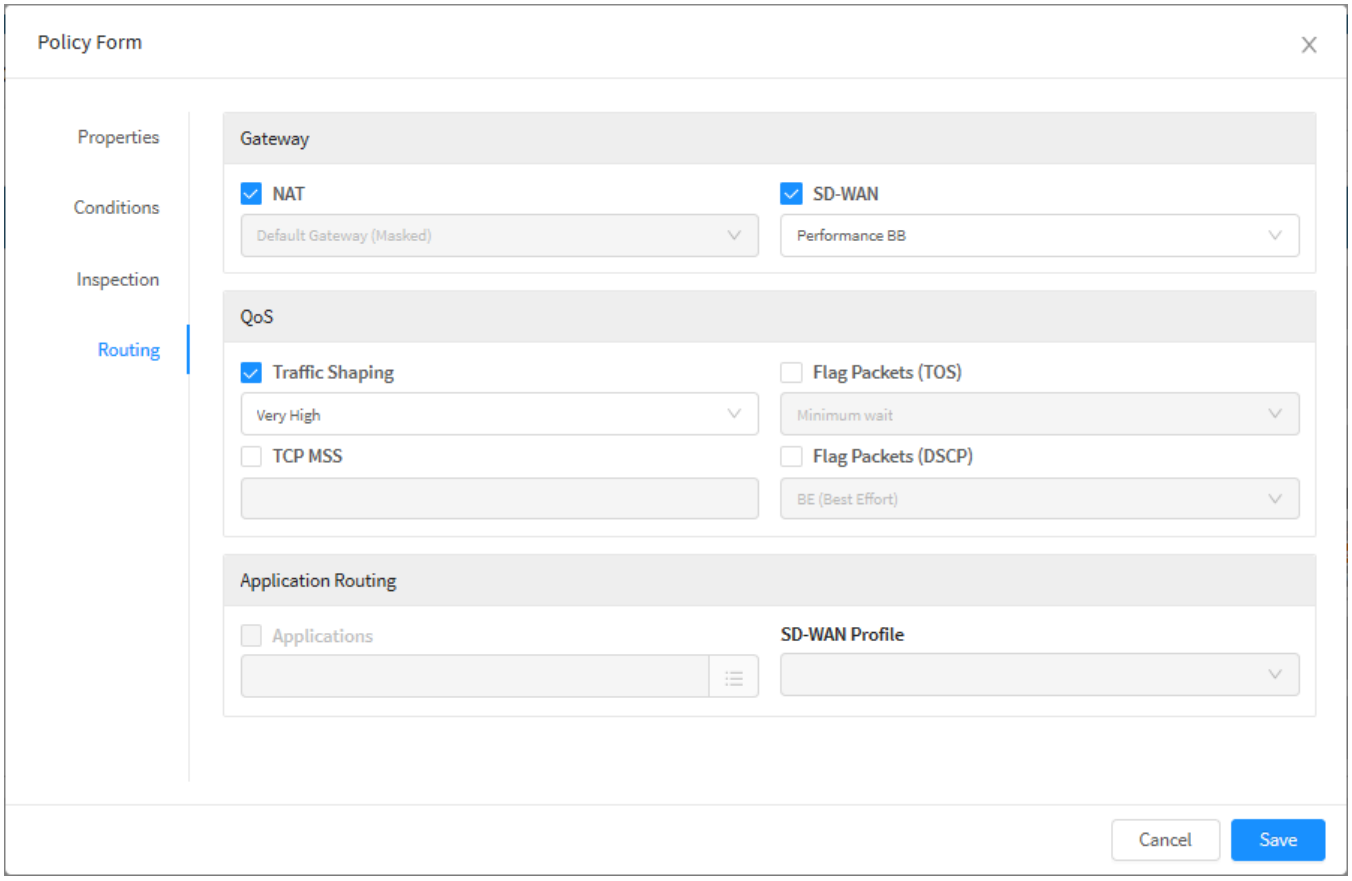
Routing

On the **[Routing]** tab, check the ***NAT[☑]*** checkbox;

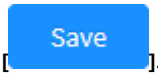
Check the ***SD-WAN*[☑]** checkbox and select the “Performance BB” option;

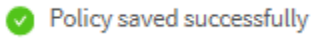
In **Traffic Shaping** select the option “Very High”;

You will have arrived at the result illustrated by the image below:



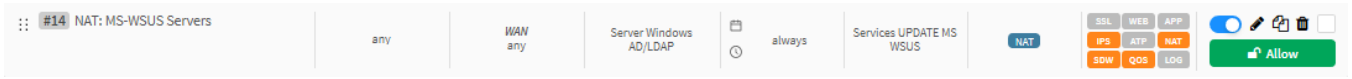
Create Policy – Ex. 4 – *Routing*

After configuring each tab according to the definition of the applied policy, click on **[**  **]**.



Policy successfully saved

The screen shown in the following image will be displayed:



Create Policy – Ex. 4 – *NAT: MS-WSUS Servers*.

After saving, for the policy to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures, the policy will have been successfully configured.

Observe the need to order / reorder policies.

In this case, we will not need to reorder.

The policies are well defined, the NAT rule of the Windows AD / LDAP server is very specific considering “Origin / Destination”, including the service ports.

The access policies and WEB filters with inspection and ordered in a way that apply the blocks first, then the permission.

In this way "not in conflict" with other policies, meeting the specifications of the presented policy model and the considerations and "Important Tips" mentioned in the previous chapter.

Ex.: Objeto endereço “Servidores Wsus” ver lista de endereços na documentação em nota;

Service object “Service UPDATE MS WSUS”. See list of ports in the documentation in note.

In example 4 we defined a redirection policy to update without requiring authentication.

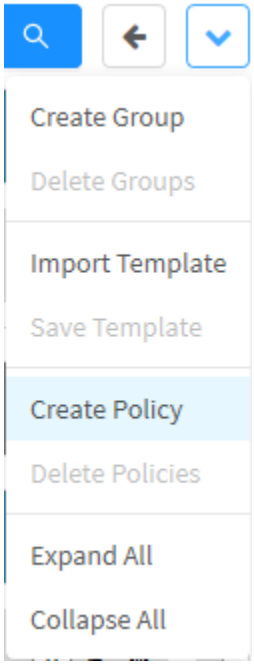
Example 5 - NAT policy for all protocols with IPS and Proxy

In this example we will configure a policy that encompasses all protocols for users authenticated with ATP and Proxy inspection for the HTTP and HTTPS navigation ports with SSL Inspection.

Below is a summary of what will be configured in the rule:

- **[*Properties*]:** *Allow all with IPS + PROXY*, *TAG = IPS, NAT, PROXY;*
- **[*Conditions*]:** Network zone *"LAN", Authenticated;*
- **[*Inspection*]:** *SSL Inspection, Intrusion Prevention;*
- **[*Routing*]:** *Enable [Nat], QOS: Medium Priority* (*Reserve 50% link*).

To add a security policy, in the action menu **[**  **]**, click on the "Create Policy" option;



IPv4 - Actions Menu - *Create Policy*

Configure each tab according to the settings shown below.

Properties

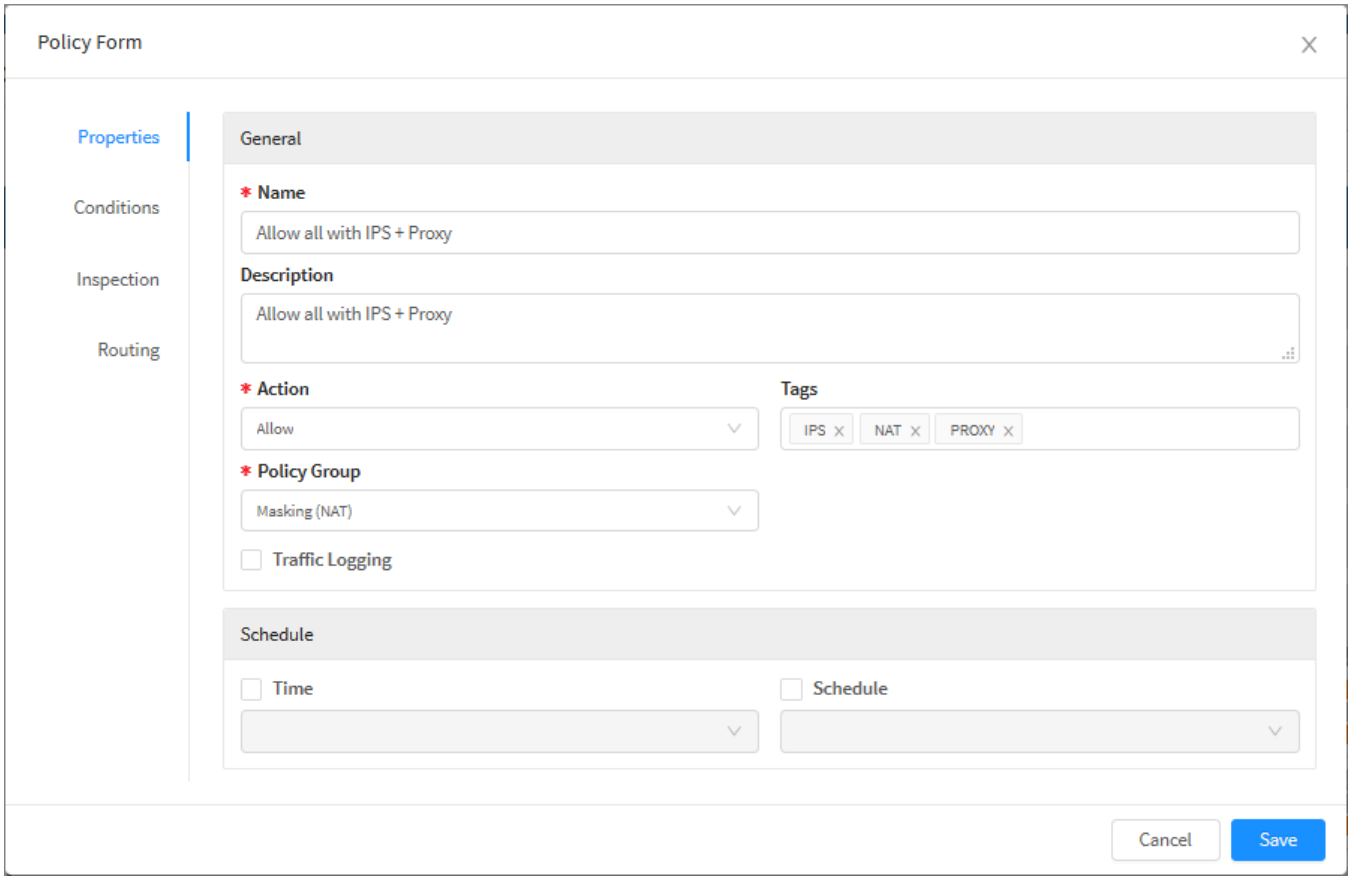
In the **[Properties]** tab, in **Name** set it as: "Allow all with IPS + Proxy";

In **Description** type "Allow all with IPS + Proxy";

In ***Tags*** include "IPS", "NAT" and "PROXY";

In ***Policy Group*** select "Masking (NAT)";

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 5 – *Properties*

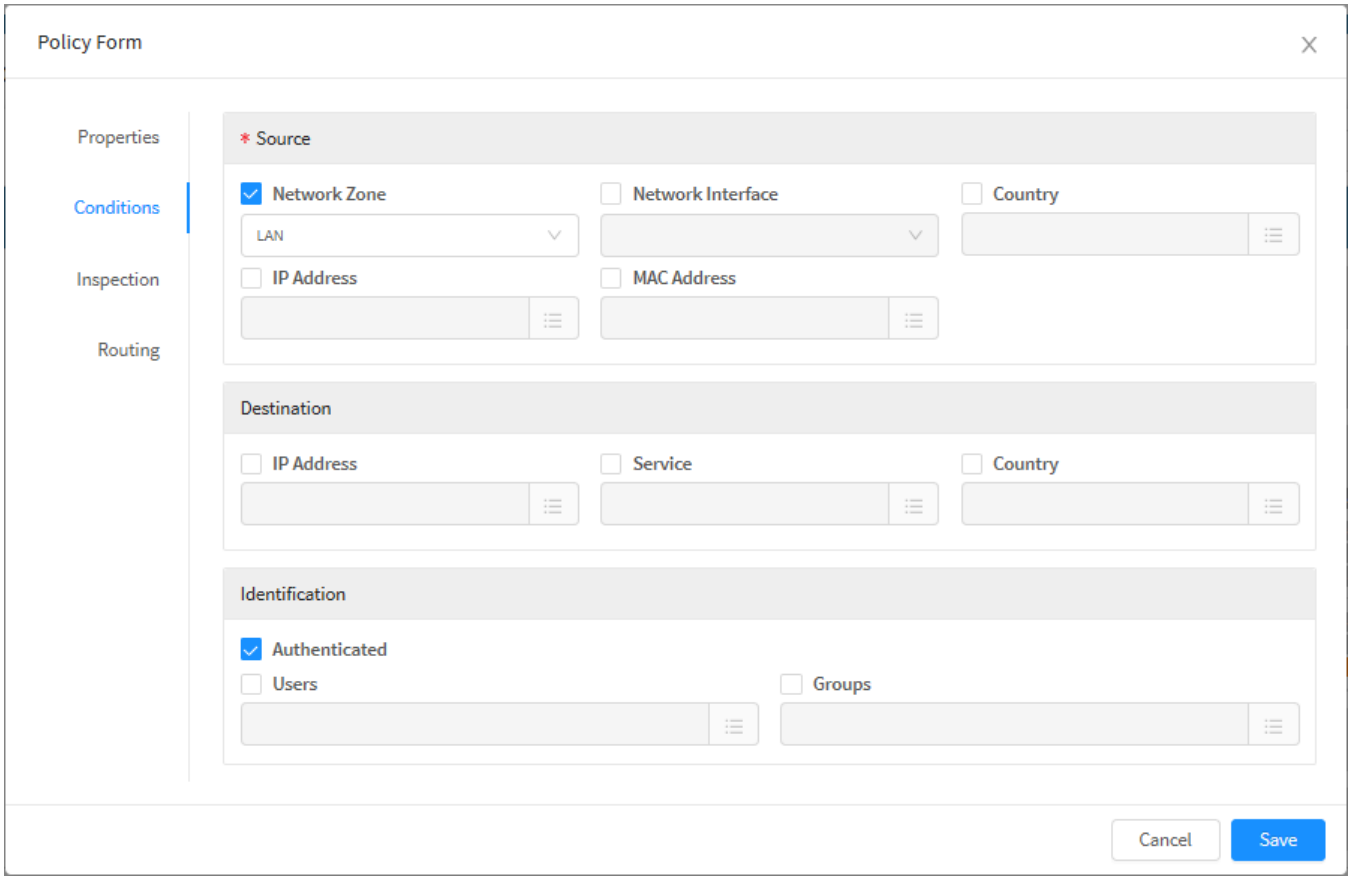
Select the next tab: **[Conditions]**.

Conditions

In the **[Conditions]** tab, in **Network Zone** select: “LAN”;

Select the **Authenticated** checkbox.

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 5 – *Conditions*

Select the next tab: **[Inspection]**.

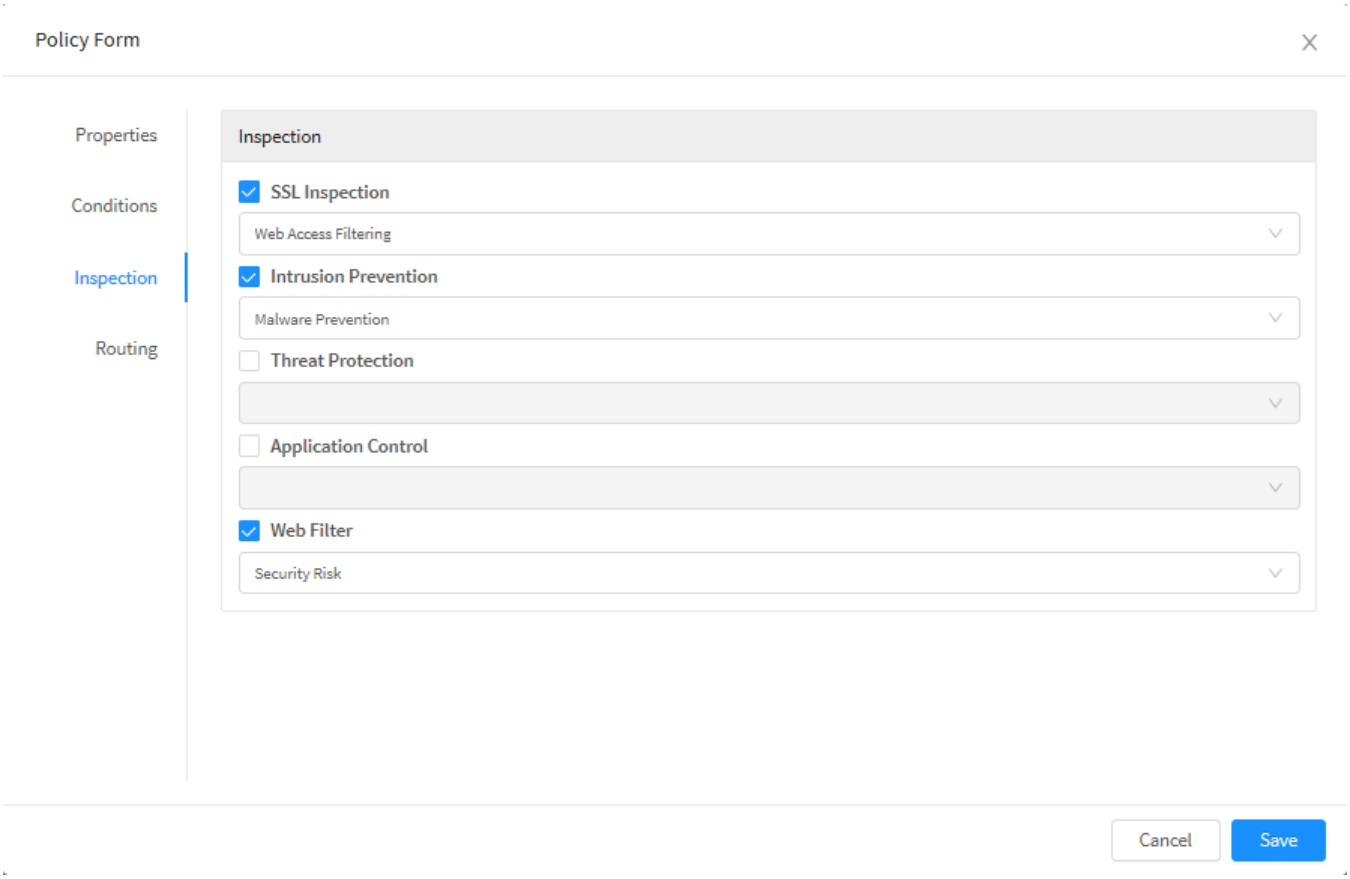
Inspection

In the **[Inspection]** tab, enable the ***SSL Inspection [✓]*** checkbox and select a profile to inspect ***SMTP, POP3, FTP***, ***HTTP***, ***HTTPS*** and ***SSL*** (For more information, check the Proxy - SSL Inspection section);

Enable the ***Intrusion Prevention [✓]*** check box and select the desired inspection profile (For more information, check this *page*);

Select the ***Web Filter [✓]*** checkbox and select the desired profile (For more information, check this page);

You will have arrived at the result illustrated by the image below:



Create Policy – Ex. 5 – *Inspection*

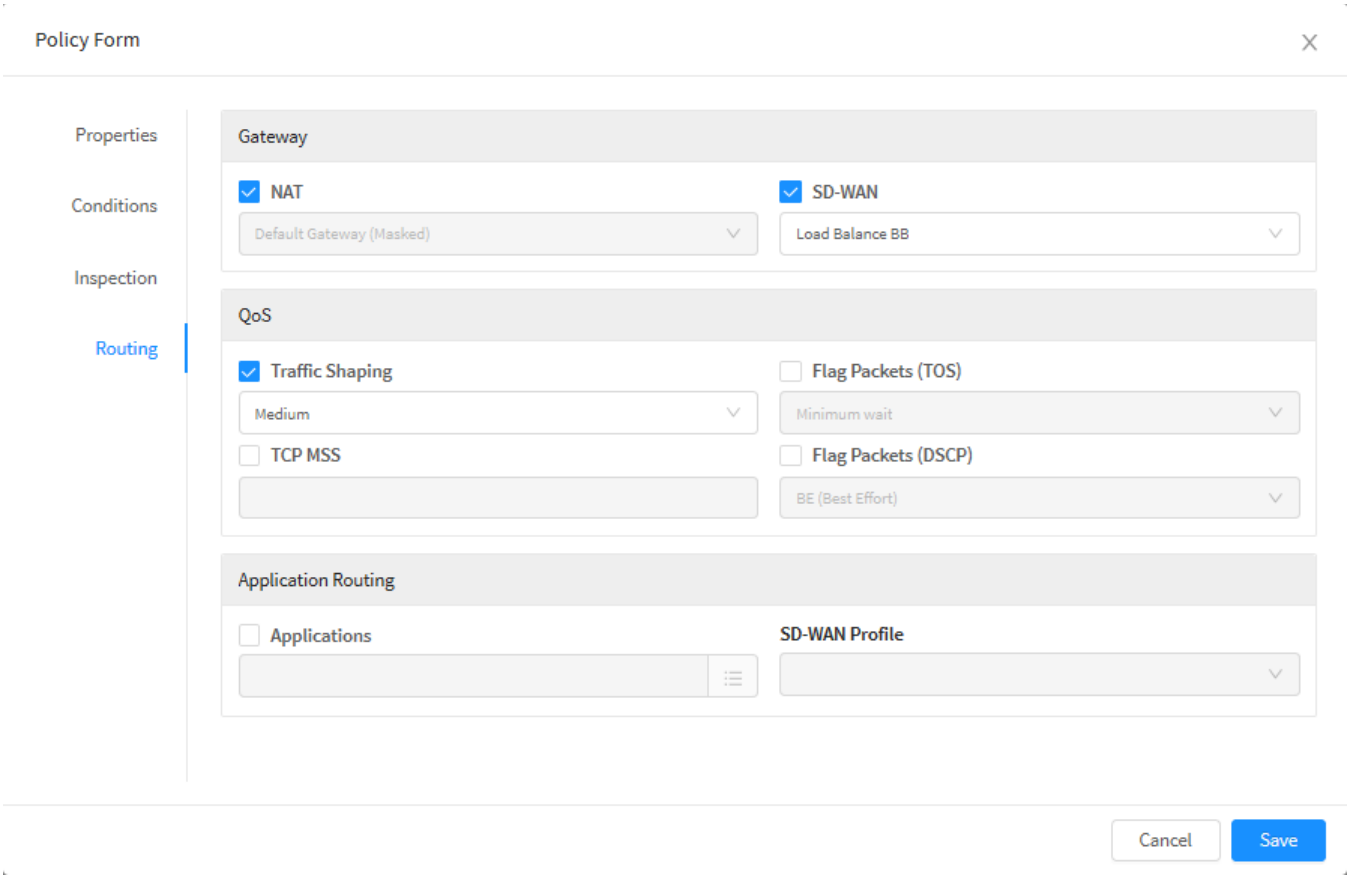
Select the next tab: **[Routing]**.

Routing

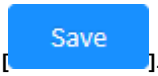
On the **[*Routing*]** tab, select the **Nat** check box;

Check the **SD-WAN** checkbox and select the option “Load Balance BB”;

In **Traffic Shaping** select the option “Medium”;

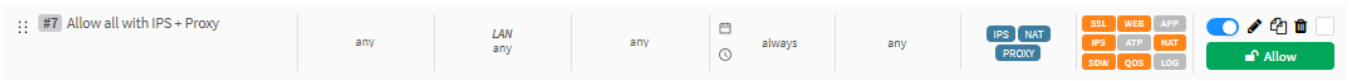


Create Policy – Ex. 5 – *Routing*

After configuring each tab according to the definition of the applied policy, click on **[**  **]**.

Policy successfully saved

The screen shown in the following image will be displayed:



Create Policy – Ex. 5 – *Allow all with IPS + PROXY*

After saving, for the policy to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made . For more information on the command queue access the page: UTM - Command queue.

After performing these procedures, the policy will have been successfully configured.

Ready! Now just apply some tests.

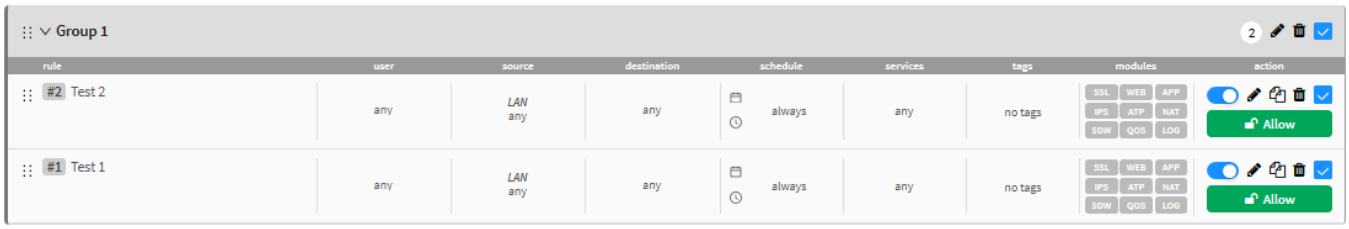
To do so, use a properly configured workstation and browse the WEB.

Then check the Traffic logs on the Dashboard.

IPv4 - Actions Menu - Delete Policies

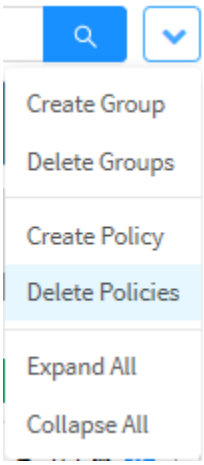
The “Delete Policies” button deletes the selected Policies. To delete, follow the steps:

1. Select the Policy(ies) to be deleted by checking the checkbox. In selected packages the checkbox will change from gray to blue **[ ]**. Ex.: *Test 1* and *T est 2*;



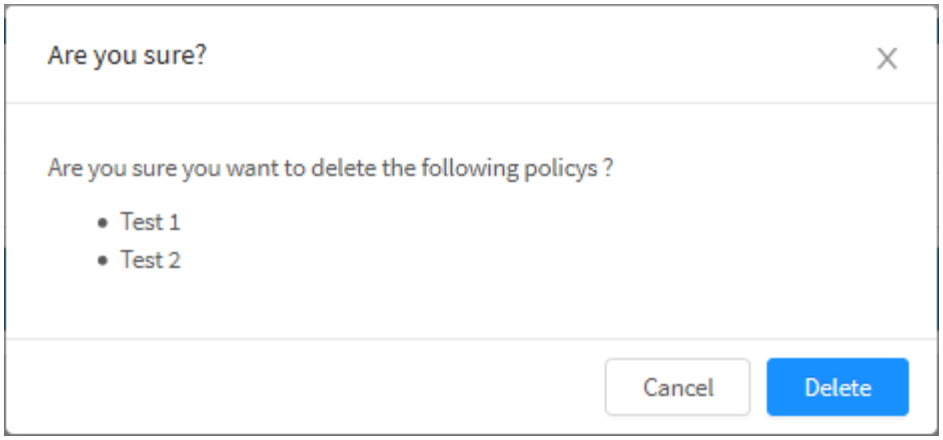
Policies selected to be deleted

2. In the actions menu **[ ]**, click on the option “Delete Policies”;



Policies IPv4 - Actions Menu - *Delete Policies*

3. The screen will appear asking if you want to delete the items:



Policies IPv4 - Deletion confirmation message

If you wish to cancel, click on the **[** Cancel **]** button. To finish, click on the **[** Delete **]** button.

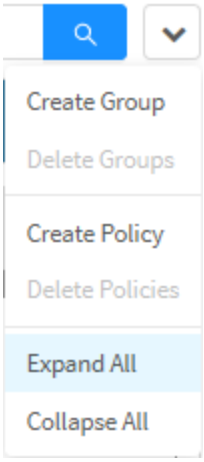
Policy successfully deleted

The chosen Policies have been successfully removed.

IPv4 - Actions menu - Expand All and Collapse All

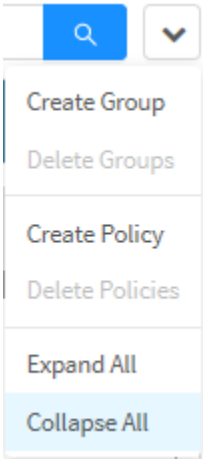
The “Expand All” button is intended to expand the policy group. To expand the policy group, follow these steps:

1. In the action menu, click on the “Expand All” option to expand the expanded policy groups;



Policies IPv4 – Actions menu - Expand All

2. By clicking on “Collapse All” in the action menu, all options shall be collapsed.

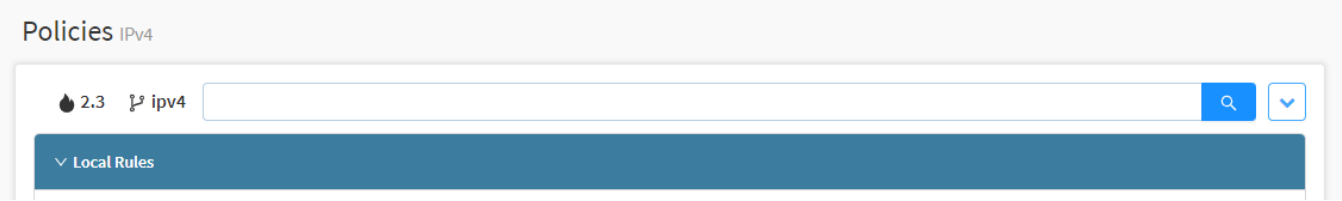


Policies IPv4 – Actions menu – *Collapse All*

IPv4 - Actions menu - Validate Policies

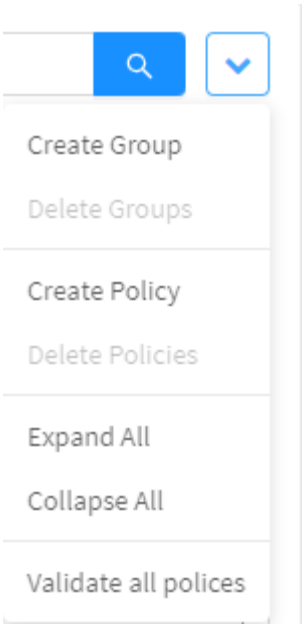
The "Validate Policies" button verifies the existence of redundant Policies, in duplicity, or in obscurement (overlapping).

In the IPv4 Policies main menu, click the options button[ ], and the Validate Policies option will be available:



IPv4 Policies – Main Menu

1. In the actions menu, click the "Validate Policies" option in order to have the system check for conflicts and redundancies among current Policies;



IPv4 Policies action menu – Validate all policies

When running the validation process, it's important to check the notifications at the upper right corner of the screen, to check the result. Right after, we must refresh the page, by clicking the refresh button of your internet browser.

The Policies validation will provide you with one of the following Policies' statuses:

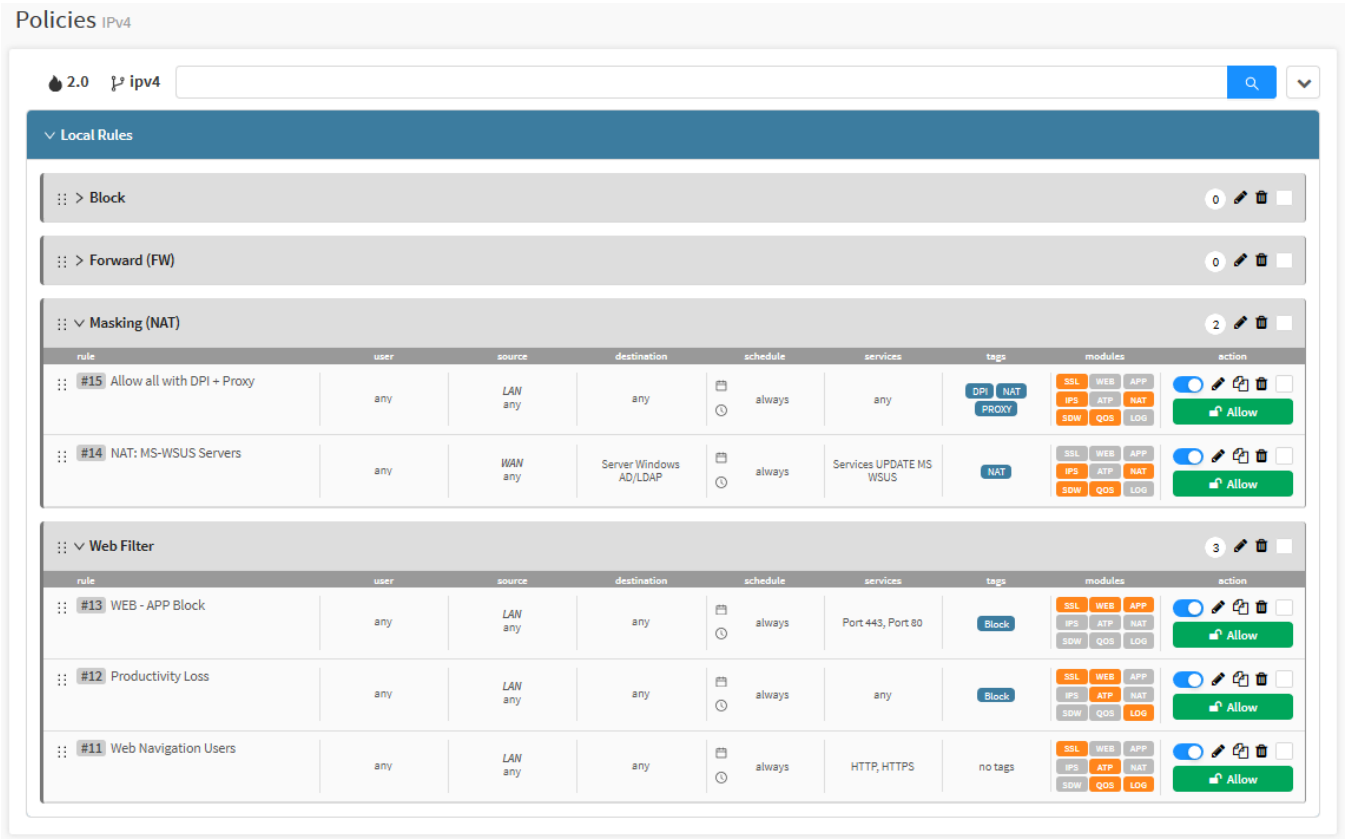
- ***Same parameters with different actions:*** In case two Policies nominate the same origin and the same destination, but the actions contradict each other. For instance, allow internet browsing action set in a Policy and deny internet browsing action in the other for the same origin and the same destination;
- ***Duplicity:*** Occurs when two Policies comprehend the same actions, origin and destination;
- ***Obscurement:*** Occurs when a Policy overlaps another in terms of action, therefore, the requested action has already been taken by a previous Policy.

Keep in mind that the Policies prioritization is top-down in the Firewall.

So we were able to analyze the available options on the IPv4 Policies' main menu.

IPv4 - Columns

The IPv4 Policies screen displays more detailed information on the policies created:



IPv4 – Policies

The top of the Policy panel contains:

- **Package Name:** Displays the name of the registered Policy Package;
- **System Version[ ]:** Displays the version in which the Policy Package was created. It is extremely important to create Policy Packages of the same version as the NGFW, otherwise the package will not be compatible;
- **IP[ ]:** Represents the type of IP used in the Policy Packages created. Ex.: "IPv4";
- **Search Bar:** It makes it possible to locate specific items, by clicking on some column fields within the policy group to serve as a filter in a more specific search, for more information check this page.
- **Actions Menu [ ]:** Features the following set of contextual options:
  - Create Group;
  - Delete Groups;
  - Create Policy;
  - Delete Policies;
  - Expand All and Collapse All.
- **Pre Rules:** If a GSM is linked to this NGFW, it represents all the policy groups that were put in place before the local NGFW policies, so they have priority over the policies created in the NGFW itself;
- **Local Rules:** Represents the rules of the policy groups created in the NGFW itself;
- **Post Rules:** All policy groups that will be created will take effect only after local NGFW policies, so they will have lower priority and will be installed below existing policy groups at the NGFW.

It is important to remember that the policies are ordered by "Priority", and they are applied considering the "First Match Wins" method.

Therefore, the policies positioned above have priority over those below, since their application (prioritization) is top-down.

Each policy group contains the following buttons:

- [ ] Clicking and dragging moves the group order and allows you to rearrange the priority according to which group is above (First Match Wins);
- [ ] Expands to display the policies created in the group;
- [0] Reports how many policies there are in the group;
- [ ] Allows you to edit the settings added in the Create Group option of the actions menu;
- [ ] Delete the group;
- [ ] Select the group to interact with the action menu.

The columns within each policy group are divided into:

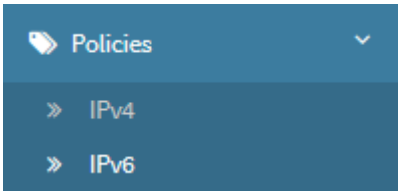
- **Move [ ]:** Clicking and dragging moves the order of the policy and allows you to rearrange the priority according to which policy is above (First Match Wins);
- **Id [#8]:** Displays the policy identification number, you can click it to serve as a filter in the search field;
- **Rule:** Displays the policy name;
- **User:** Determines which users are affected by the policy, you can click on this field to serve as a filter in the search field;
- **Source:** Displays if the source of this rule will be the Network zone, IP address, network interface, Mac Address or any of these, you can click on this field to serve as a filter in the search field;
- **Destination:** Determines the destination of the rule, the IP address or service, you can click on this field to serve as a filter in the search field;
- **Schedule:** Displays if the rule depends on a period of time or schedule, you can click on this field to serve as a filter in the search field;
- **Services:** Displays the services that the rule affects, you can click on this field to serve as a filter in the search field;
- **Tags:** Displays the tags that have been added to this rule, you can click on this field to serve as a filter in the search field;
- **Modules:** Determines which NGFW modules the rule will interact with, you can click on this field to serve as a filter in the search field;
- **Action:** Displays some contextual buttons and what action the rule takes.
  - **Enabled[ ]** or **Disabled[ ]:** Using this selector, enables or disables the rule;
  - **Edit[ ]:** Allows you to edit the settings added in the Create Policy option of the actions menu;
  - **Clone[ ]:** Copies policy, note that when using this option, the copied policy will use the same name as the original policy, but it will add a number on the front (for example, if I copy the policy "Test" the copy will be called "Test (1)") and it will be automatically below the original policy, therefore, taking into account "First Match Wins", it is important to move the policy according to the desired priority;
  - **Delete[ ]:** Removes the policy;
  - **Select[ ]:** Allows the selection of policies in order to interact with the actions menu;
  - **Action:** Determines the behavior of the policy in question, having as possibilities:
    - [Allow]: As the name says, this option is meant to grant access;
    - [Deny]: Access is denied;
    - [Reject]: Access is denied, but a rejection message is displayed to the user.

Next, we'll review IPv6 policies.

IPv6 Policies

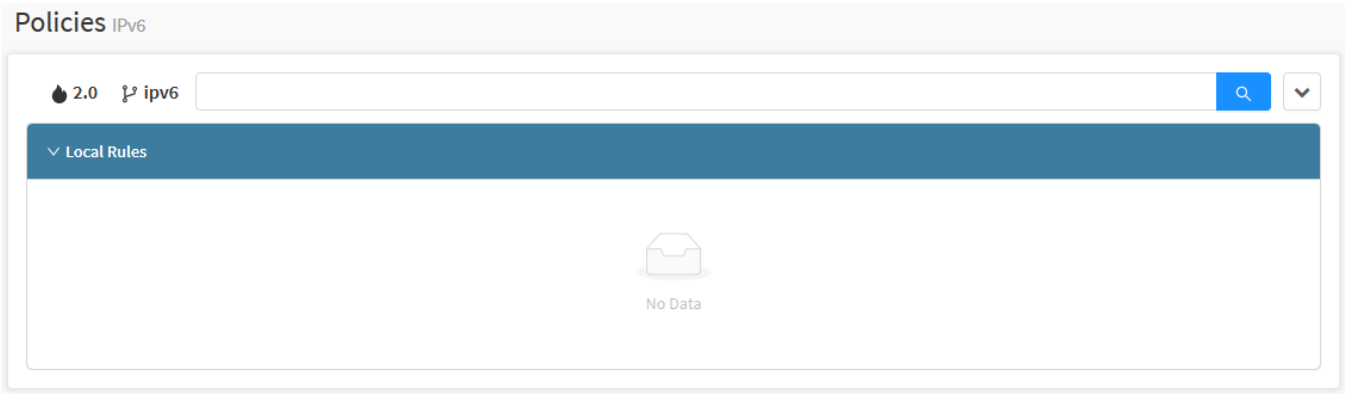
This section will analyze each component of the IPv6 policy creation interface. The definitions are identical for IPv4 and IPv6, undergoing changes only in their addresses and some proprietary characteristics to each version of the protocol.

Click on the "IPv6" option;



IPv6 menu

The “IPv6 Policies” screen will appear:



IPv6 Policies Section

This section will delve into:

- Creating policy groups;
- Policy Registration and Removal.

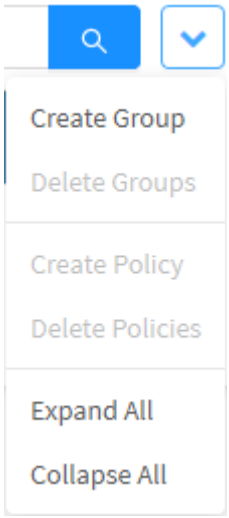
Next, we'll look at each component of this panel.

IPv6 - Actions Menu

At the top right of the screen we have the actions menu:

IPv6 – Actions menu button

By clicking on this button the menu below is displayed:



IPv6 – Actions Menu

The menu consists of the following options:

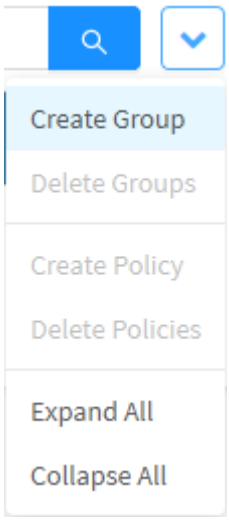
- *Create Group*;
- *Delete Groups*;
- *Create Policy*;
- *Delete Policies*;
- *Expand All* and *Collapse All*.

Next, each action menu option will be detailed.

IPv6 - Actions Menu - Create Group

Through the “Create Group” option it is possible to create a new group. To access it, click on the **actions menu [ ]**.

1. Click on the “Create Group” option;



IPv6 - Actions menu - *Create Group*

2. The “Create Group” screen will be displayed. Add the desired group name:

IPv6 – Create Group

After naming the group, if you want to cancel click on the [Cancel] button. To finish creating the group, click the [Save] button.

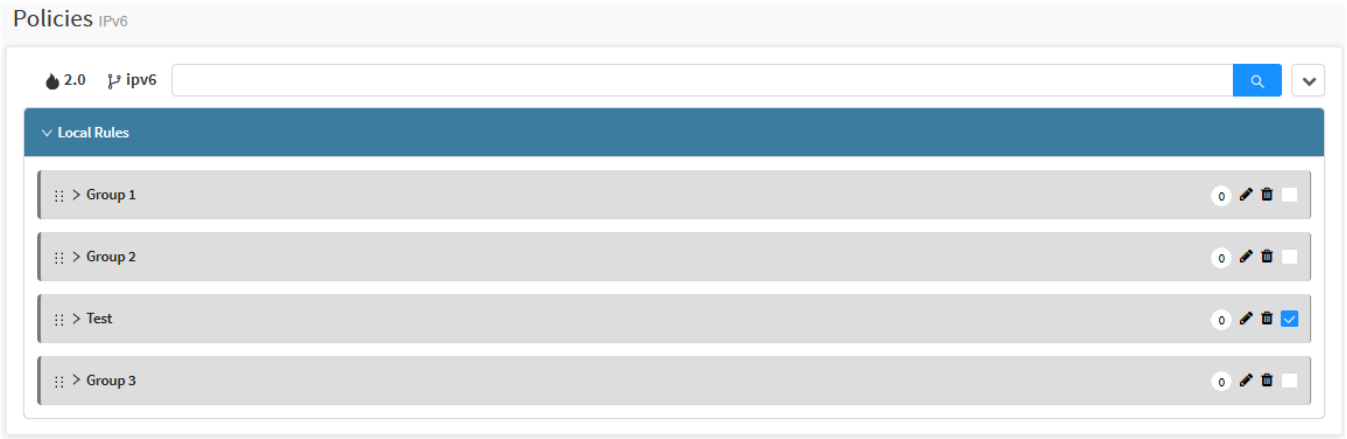
Group successfully created

The group was created successfully.

IPv6 - Actions Menu - Delete Groups

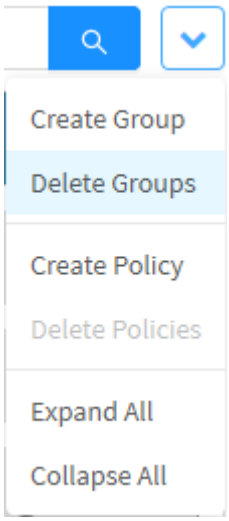
Through the “Delete Groups” button it is possible to delete several installed groups at the same time. To delete them from the actions menu, follow these steps:

1. Select which group(s) you want to delete by clicking on the checkbox **[ ]**, as shown on the image below:



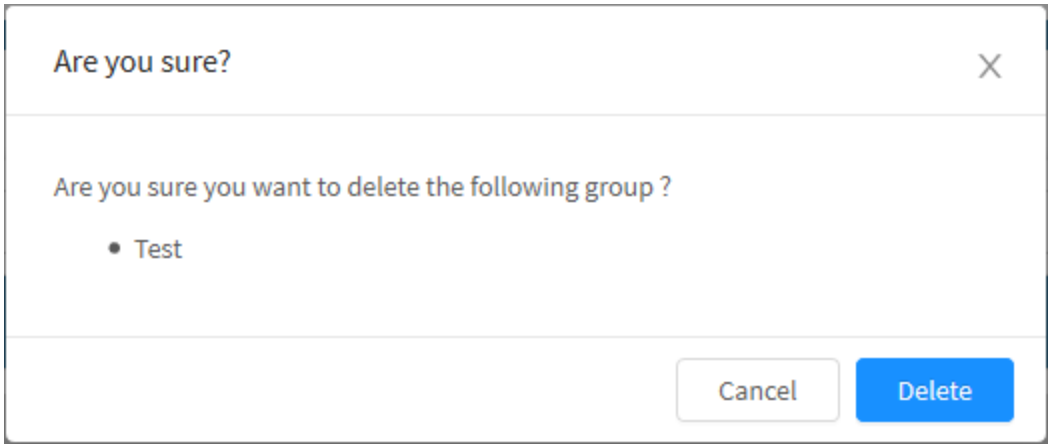
IPv6 – Delete Groups

2. Enter the actions menu **[ ]** and click on the “Delete Groups” button.



IPv6 – Actions Menu - *Delete Groups*

3. The message will appear if you really want to delete the selected packages:



IPv6 – Delete Groups

If you want to cancel click on the [Cancel] button. To finish, click on the [Delete] button.

Group successfully deleted

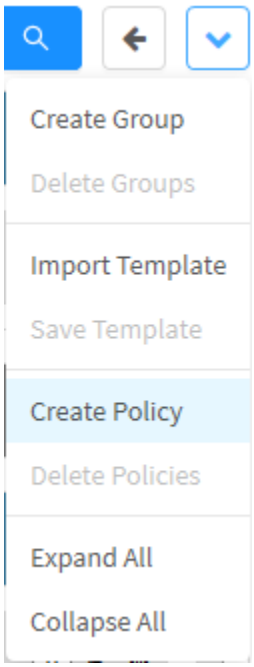
After performing these procedures, the groups will have been successfully deleted.

IPv6 - Actions Menu - Create Policy

The “Create Policy” button creates Policies within a selected Policy group. To do so, it is necessary to have created a group (check this page for more information).

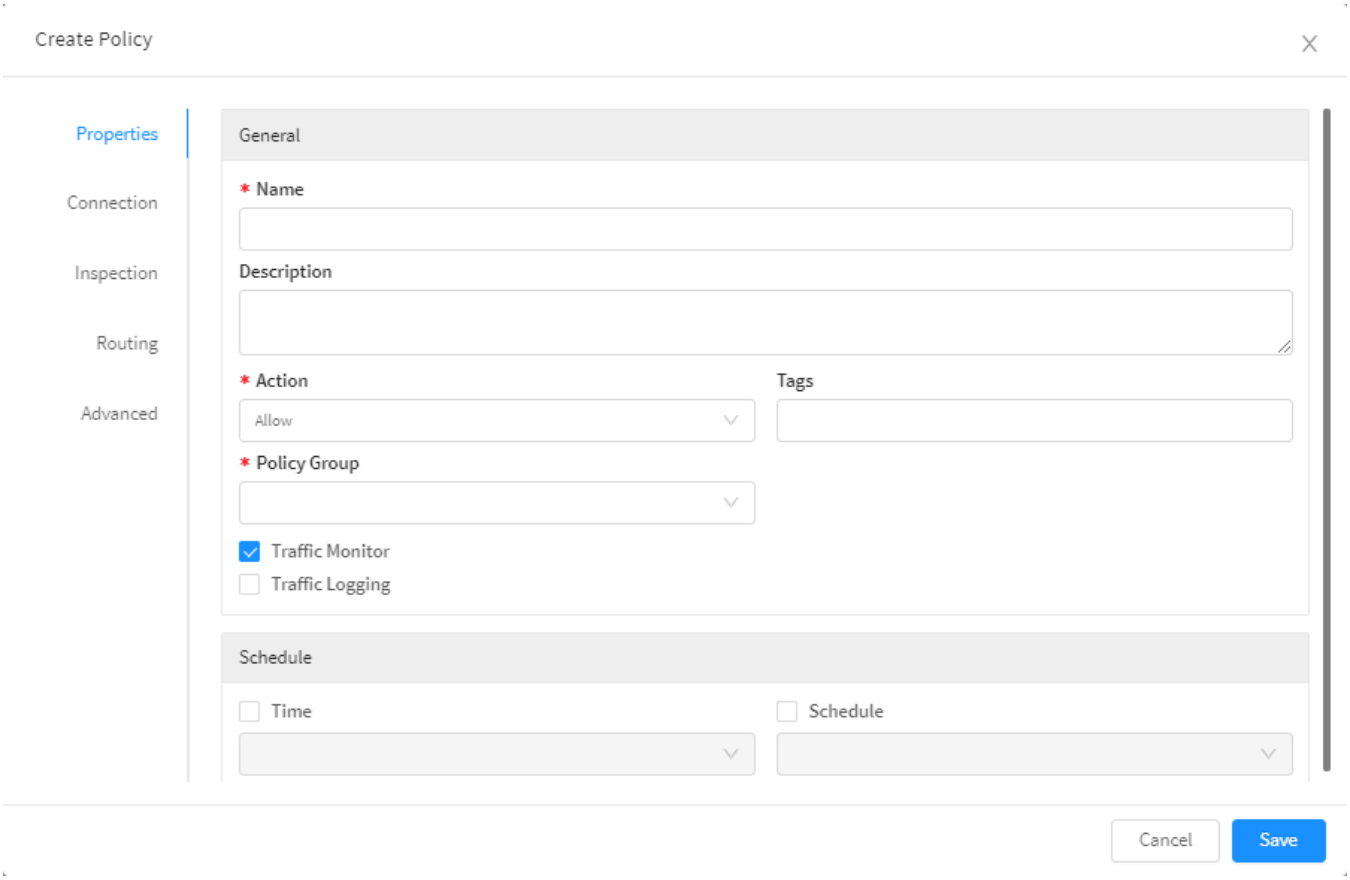
To create a Policy, follow the steps:

1. In the actions menu **[**  **]**, click on the option “Create Policy”;



IPv6 - Actions Menu - *Create Policy*

2. The Policy Form screen will appear;



IPv6 – Policy Form

This screen is organized by the following tabs:

- *Properties*;
- *Conditions*;
- *Inspection*;
- *Routing*.

Next, we will explain each field.

IPv6 - Create Policy - Properties tab

In the **[Properties]** tab, it is mandatory to define a name and description for the Policy and optionally define Tags that help in the organization and facilitate future searches for Policies.

IPv6 - Side Tabs - *Properties*

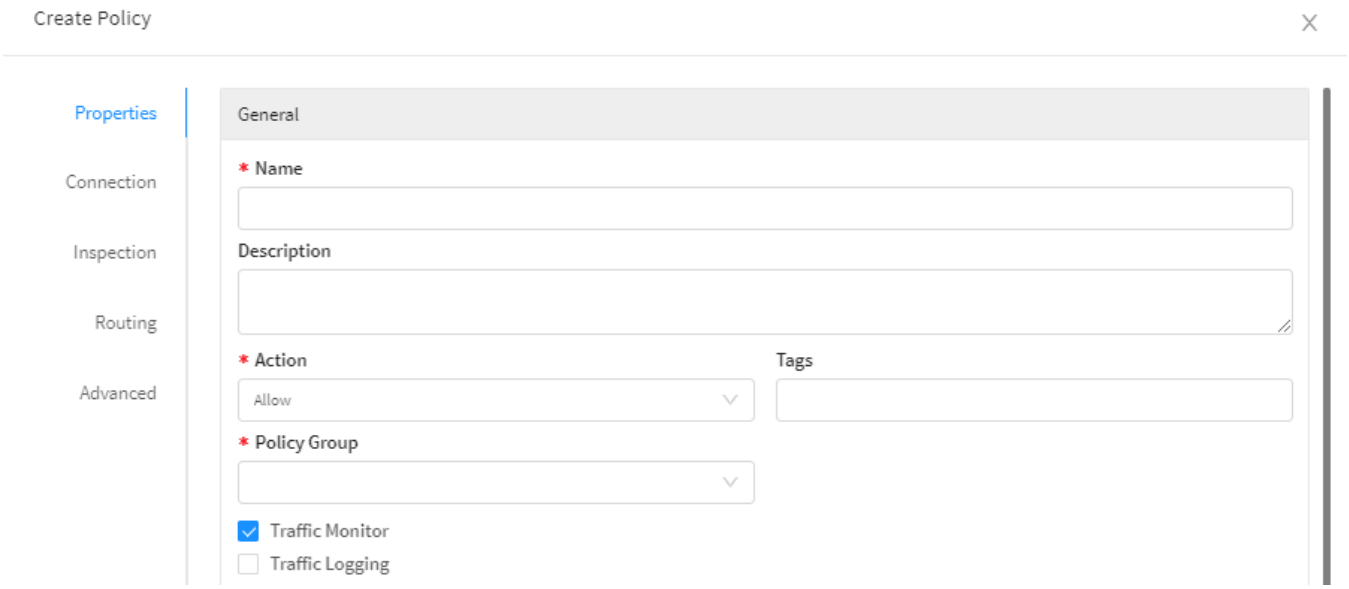
This tab contains the panels:

- *General*;
- *Schedule*.

Next, we will analyze the function of each panel field.

General

*Below is a description of the function of each field on the form displayed in the **[General]** panel:*

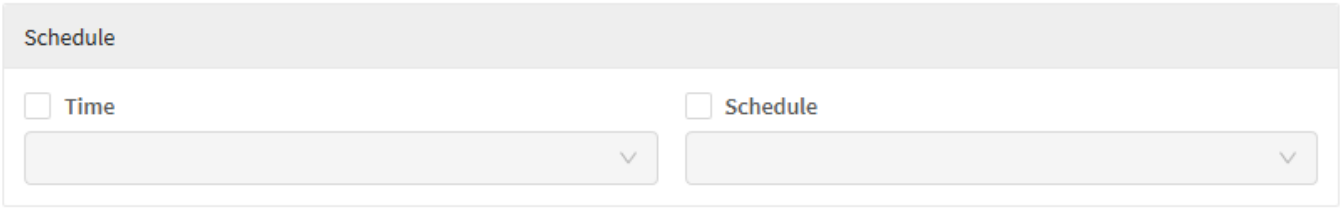


IPv6 – Properties - General

- ***Name*:** Define name for the Policy;
- ***Description*:** Define description for the Policy;
- ***Action*:** Determines the behavior of the Policy in question, with the following possibilities:
  - ***Allow*:** As the name suggests, the Allow action grants access and leaves traffic free of blockages;
  - **Deny:** The Deny action blocks traffic but does not inform the source address of the service is being blocked. That is, in this scenario, for the address of the connection source, it is not possible to know if there is a firewall intercepting the connection or simply the service is not active;
  - **Reject:** The Reject action notifies the source address that the service has been blocked by a firewall, which sends an ICMP packet indicating that the service is inaccessible.
- ***Tags*:** This option allows you to define Tags so that the administrator is able to use them as a “Filter” for his searches based on his definitions. By default, the system defines a name for Tags by type of resource being used in the Policy (enabled);
- ***Policy Group*:** Through this option it is possible to include a Policy in a group of Policies;
- **Traffic Monitor:** When this option is checked[ ], the matching information from the sessions with the created Policy, will be collected by the monitoring service.
- ***Traffic Logging[ ]*:** This check box, if enabled, provides the option to generate the report for a particular Policy.

Schedule

We'll see the functions of each field displayed on the **[Schedule]** panel in detail:



IPv6 – Properties - Schedule

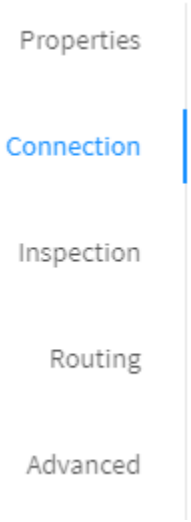
- ***Time[ ]*:** If the checkbox is selected, it determines whether the rule will apply on working days (“Business”), weekends (“Weekend”) or on any other object of the "Time" type that has been previously created;
- ***Schedule[ ]*:** If the checkbox is selected, it allows to determine if the rule will apply in relation to a “Period / Date” object that has been previously created.

Next, we will analyze the contents of the Connection tab.

- Inspection;
- Routing;
- Advanced.

IPv6 - Create Policy - Connection tab

The **[Connection]** tab provides several filters to specify the scope of origin and destination, and it is mandatory to choose at least one of them.



IPv6 - Side Tabs - *Connection*

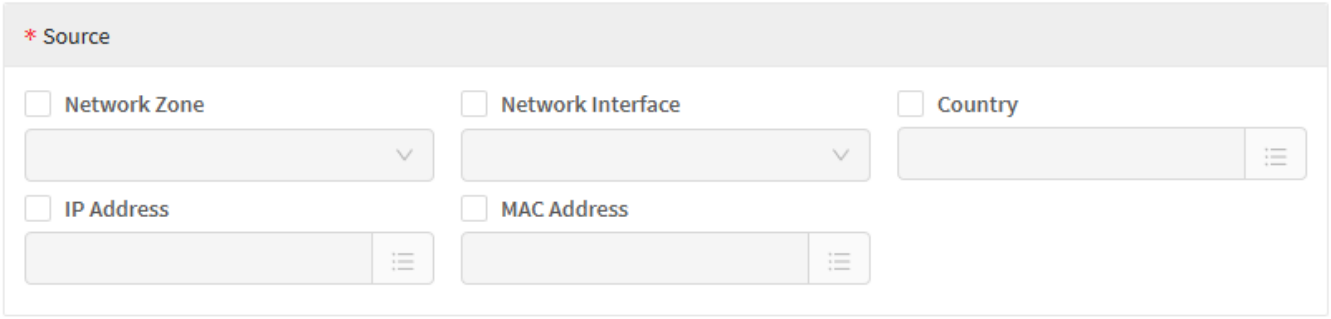
This tab contains the panels:

- *Source*;
- *Destination;*
- *Identification*.

Next, we will analyze the functions available on the Source panel.

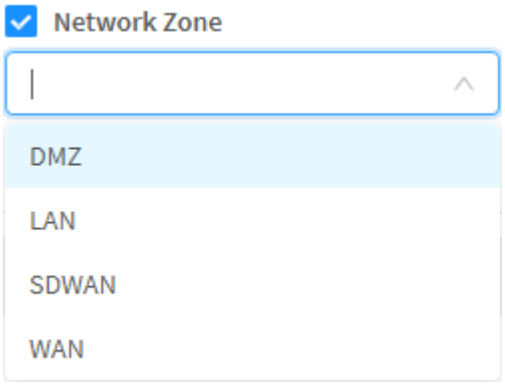
Source

The **[Source]** panel offers several filters to determine the source scope, as already mentioned, it is necessary to select at least one filter. Below is a description of the function of each field on the form displayed in the **[Source]** panel:



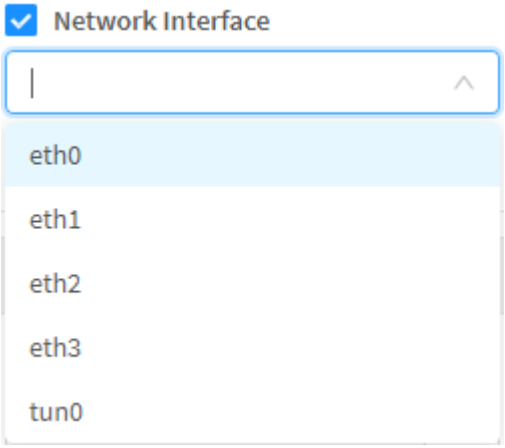
IPv6 – Connection - Source

- ***Network Zone[ ]*:** This field is only available by checking the checkbox. This field allows you to select network interfaces that can be signaled with acronyms such as LAN, WAN and DMZ to facilitate the organization and creation of policies by segmenting by network type. The network zones that appear in this menu are created in *Network - Interfaces*;



IPv6 – Connection - Source - Network Zone

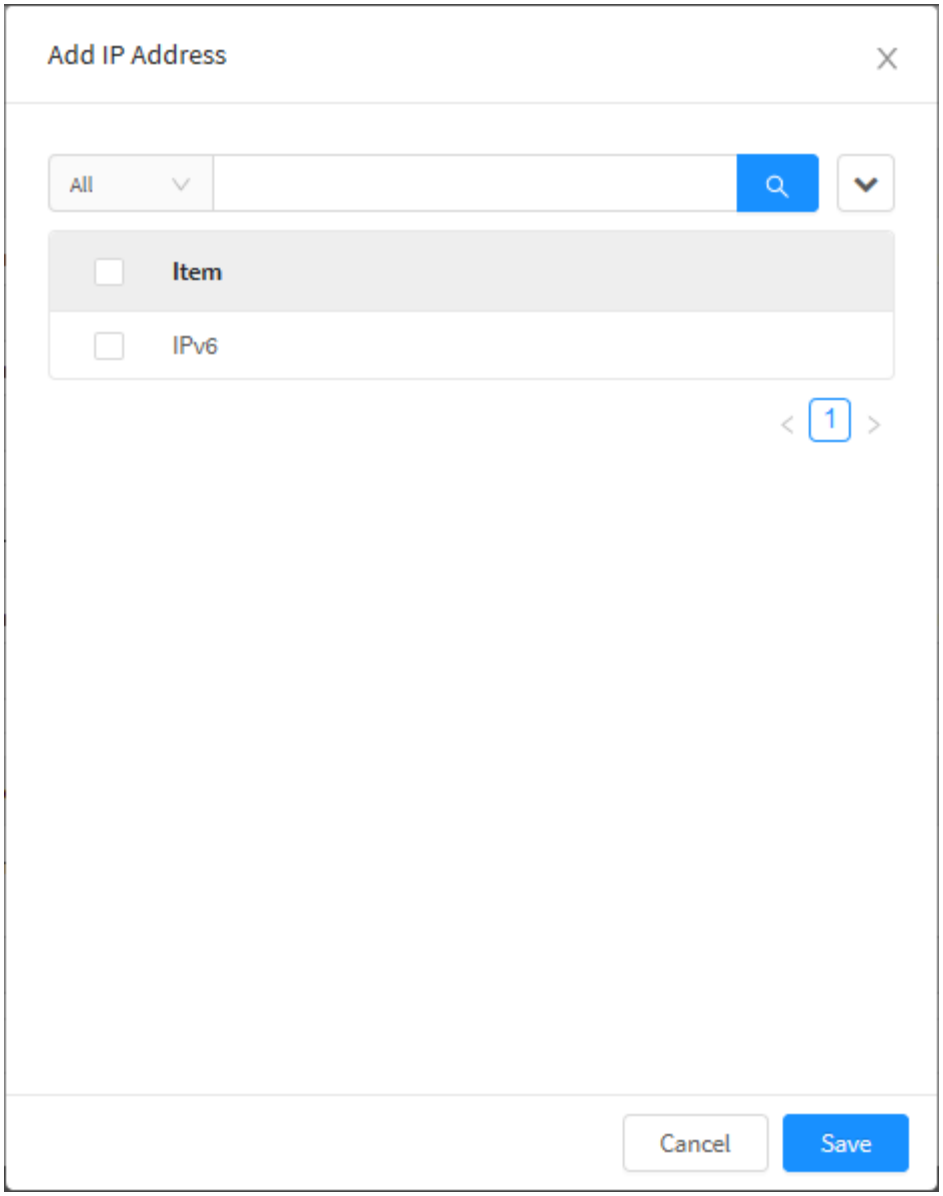
- ***Network Interface[ ]*:** This field is only available by checking the checkbox. This field allows to select network interface to be used as source filter. The interfaces that appear in this menu are created in *Network - Interfaces;*



IPv6 – Connection - Source - Network Interface

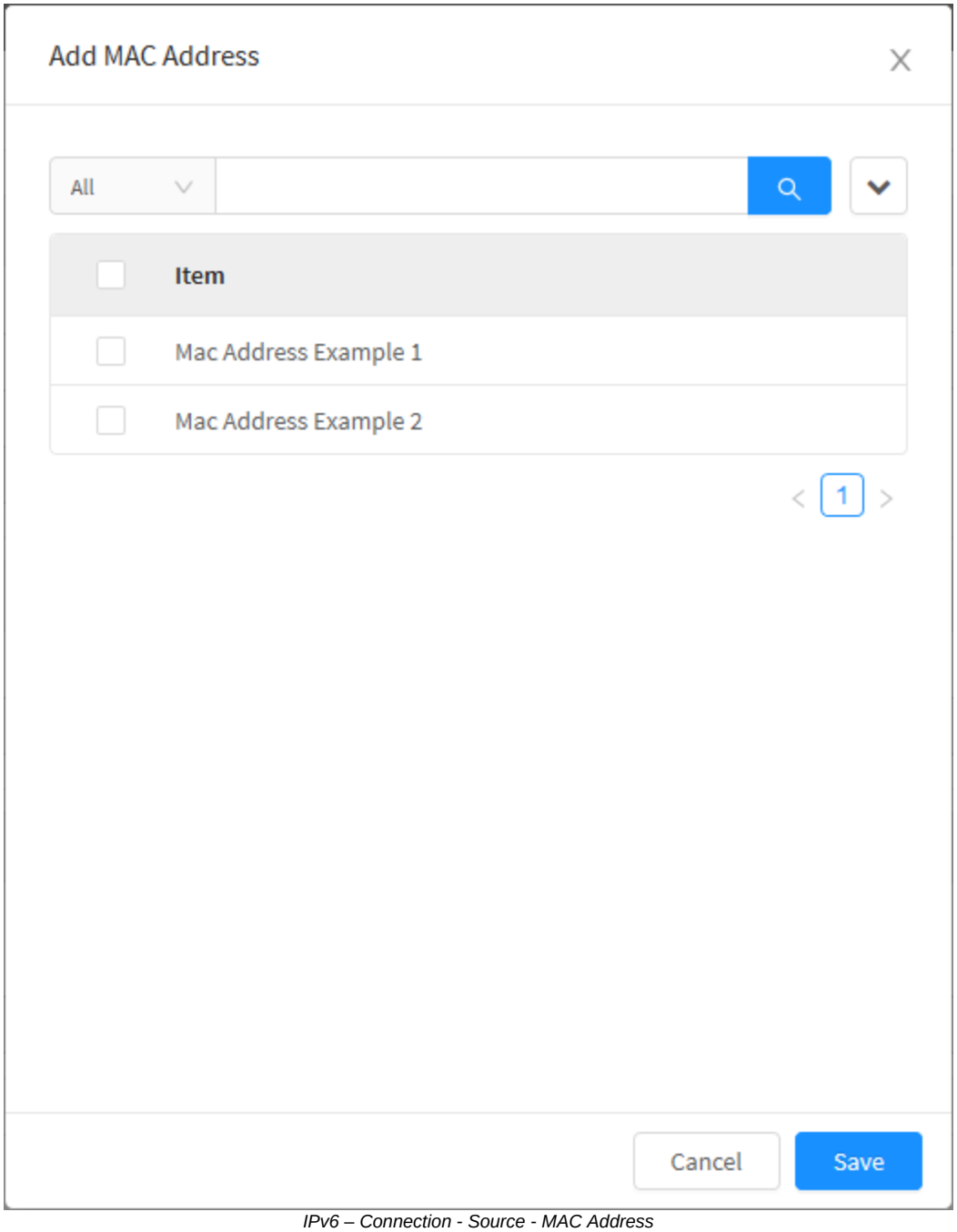
- ***IP Address[ ]*:** This field is only available by checking the checkbox. This field allows you to select IPv6 Address Object(s) (IPs, networks or sets) to be used as a source filter.
- When clicking on the button **[ ]**, the screen below will be displayed to select one or more address objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;

This list is populated specifically by IPv6 address objects. Make sure to select the correct option in "Type" when creating a new address object.



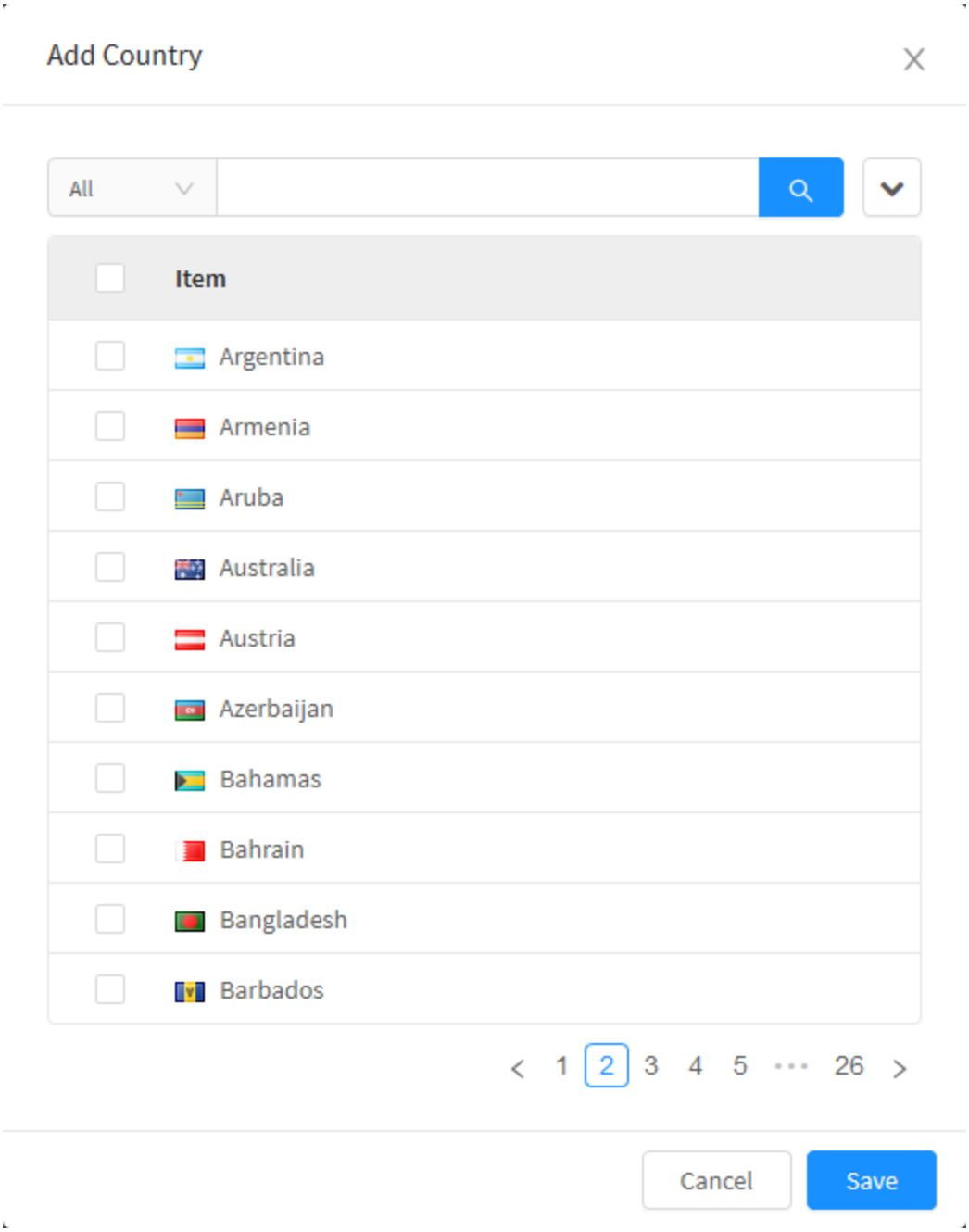
IPv6 – Connection - Source - IP Address

- ***MAC Address[ ]*:** This field is only available by checking the checkbox. This field allows to select Mac Address Address Object (s) to be used as source filter. By clicking on the button **[ ]**, the screen below will be displayed to select one or more MAC Address objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



IPv6 – Connection - Source - MAC Address

- ***Country[ ]*:** This field is only available by checking the checkbox. This field allows you to select *Countries* to be used as a source filter. When clicking on the button **[ ]**, the screen below will be displayed to select one or more countries that will compose the rule.



IPv6 – Connection - Source - Country

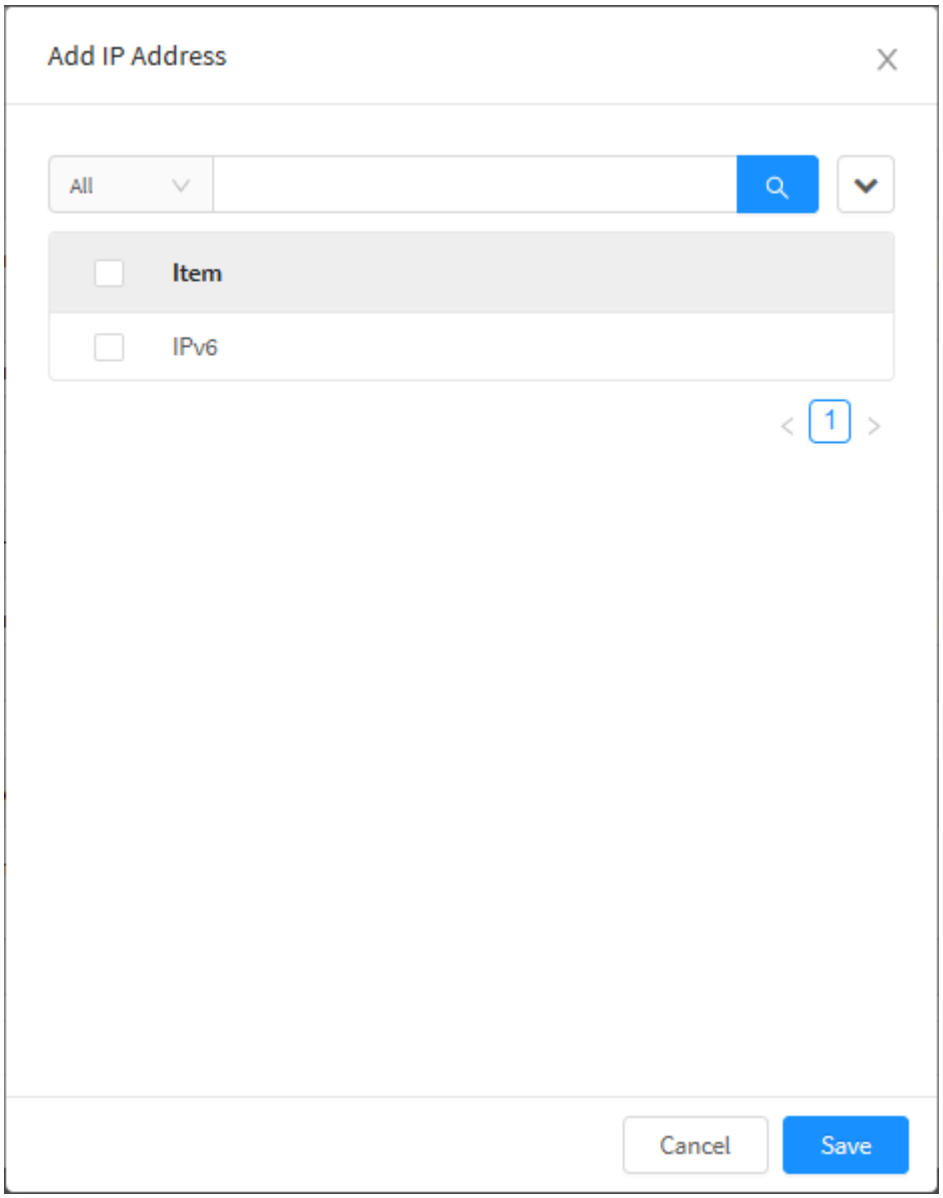
Destination

The **[Destination]** panel provides several filters to specify the scope of destination, and it is mandatory to choose at least one filter. Below is a description of the function of each form field displayed in the **[Destination]** panel:

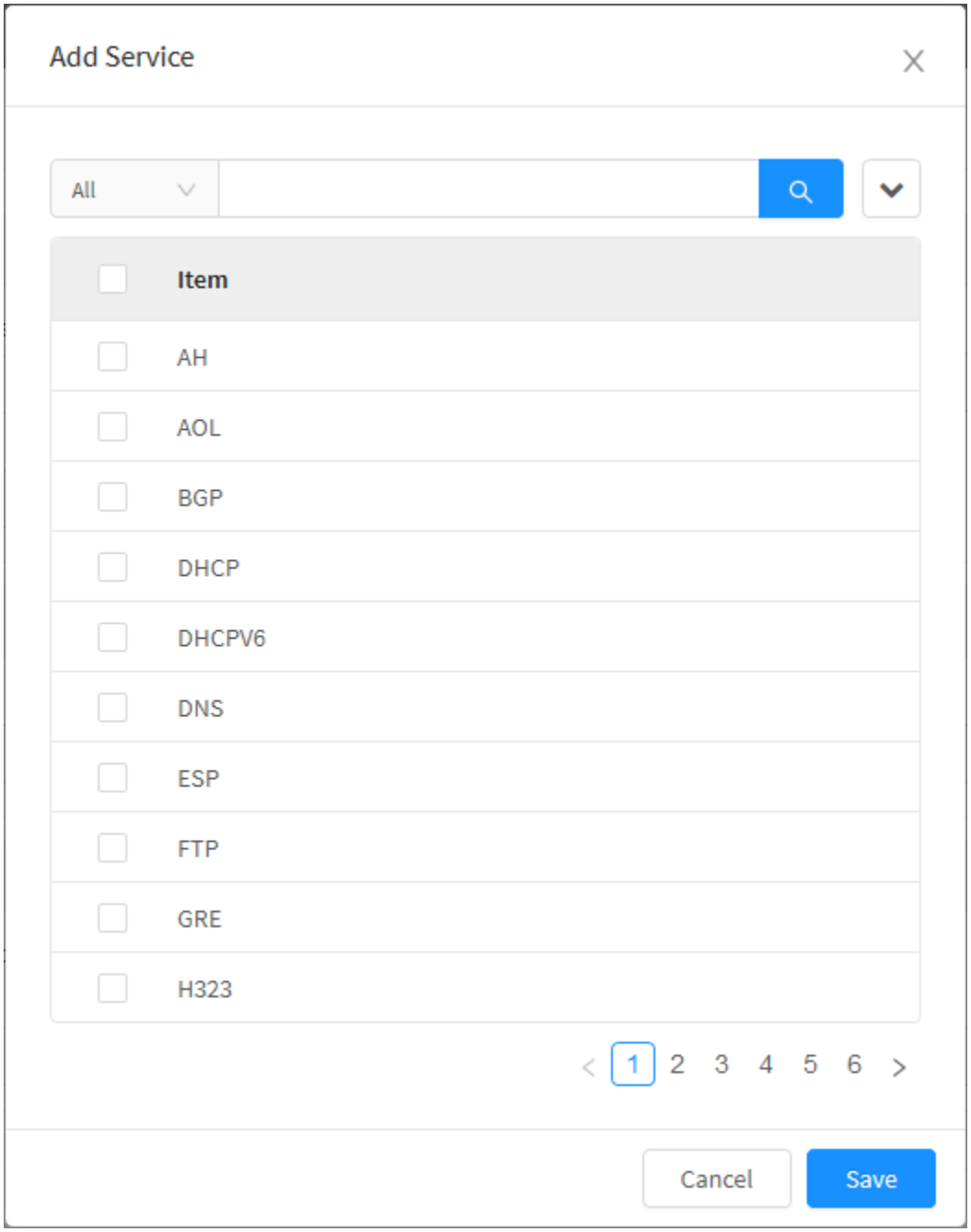
IPv6 – Connection - Destination

- ***IP Address[ ]*:** This field is only available by checking the checkbox. This field allows you to select IPv6 Address Object(s) (IPs, networks or sets) to be used as a destination filter. When clicking on the **[ ] button**, the screen below will be displayed to select one or more IP address object that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;

This list is populated specifically by IPv6 address objects. Make sure to select the correct option in "Type" when creating a new address object.

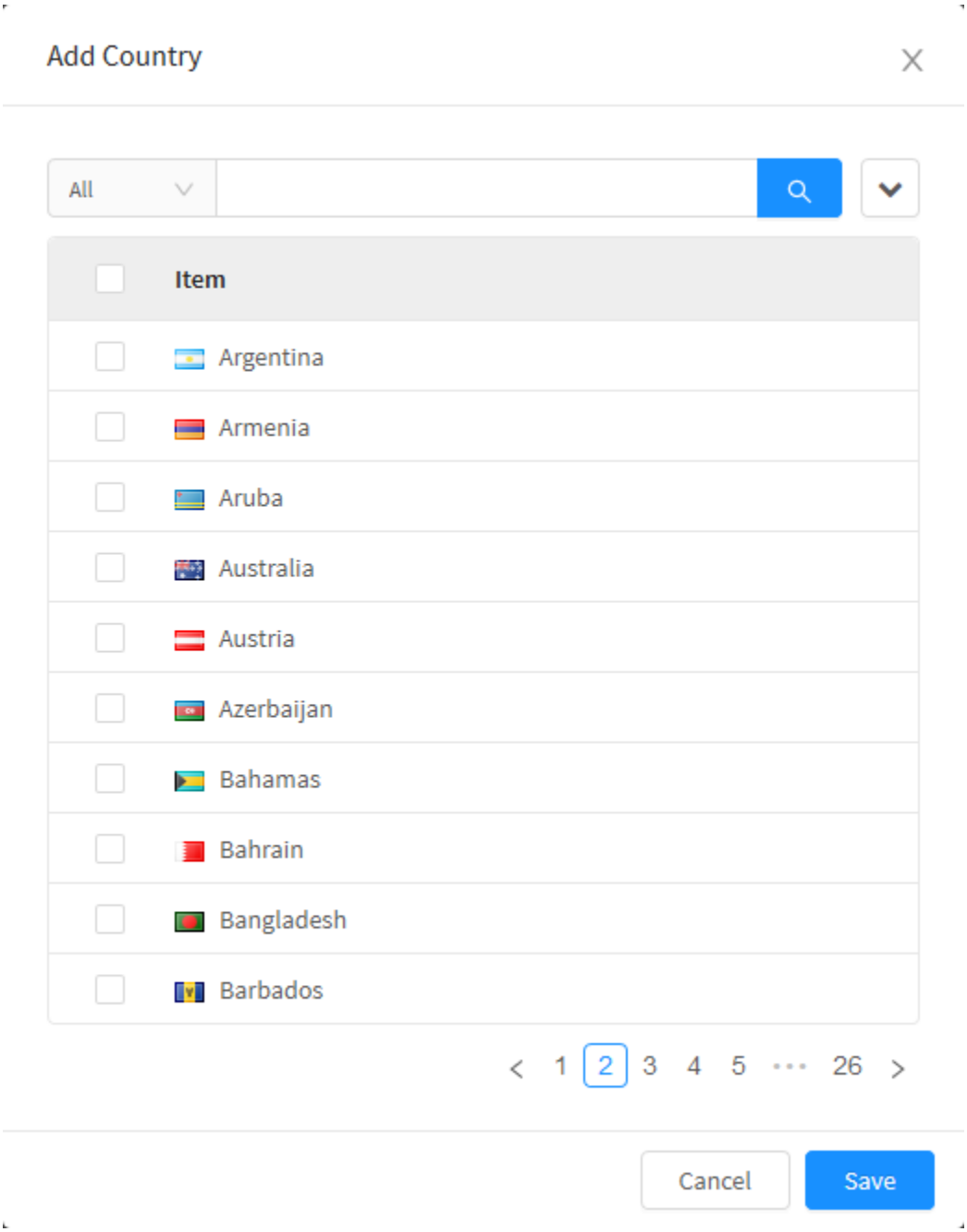


- ***Service[ ]*: This field is only available by checking the checkbox. This field allows you to select Service object(s) (protocols and ports) used as the destination filter. When clicking on the [ ] button, the screen below will be displayed to select one or more service objects that will compose the rule. The addresses that appear in this menu are created in *Settings - Objects*;



IPv6 – Connection - Destination - Service

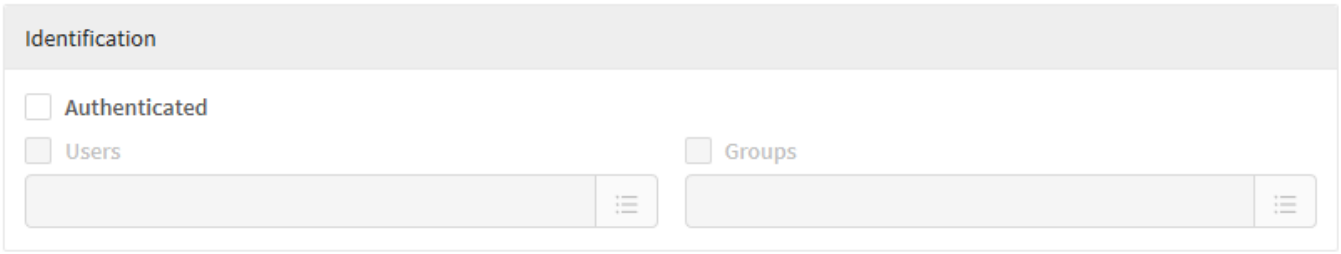
- ***Country[ ]*: This field is only available by checking the checkbox. This field allows you to select *Countries* to be used as a destination filter. When clicking on the [ ] button, the screen below will be displayed to select one or more countries that will compose the rule.



IPv6 – Connection - Destination - Country

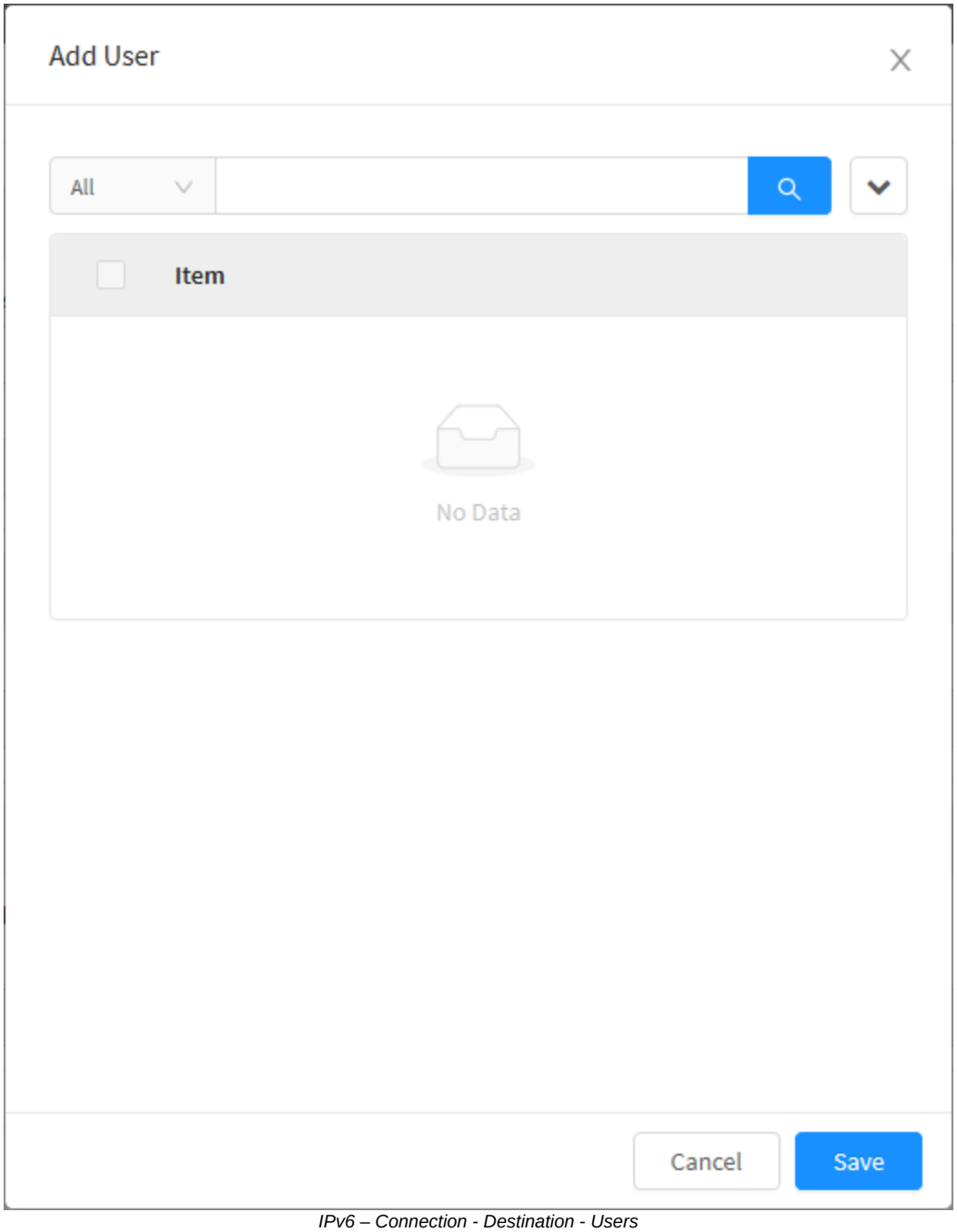
Identification

The **[Identification]** panel allows you to enable the authentication feature for the policy. Below is a description of the function of each field on the form displayed in the **[Identification]** panel:



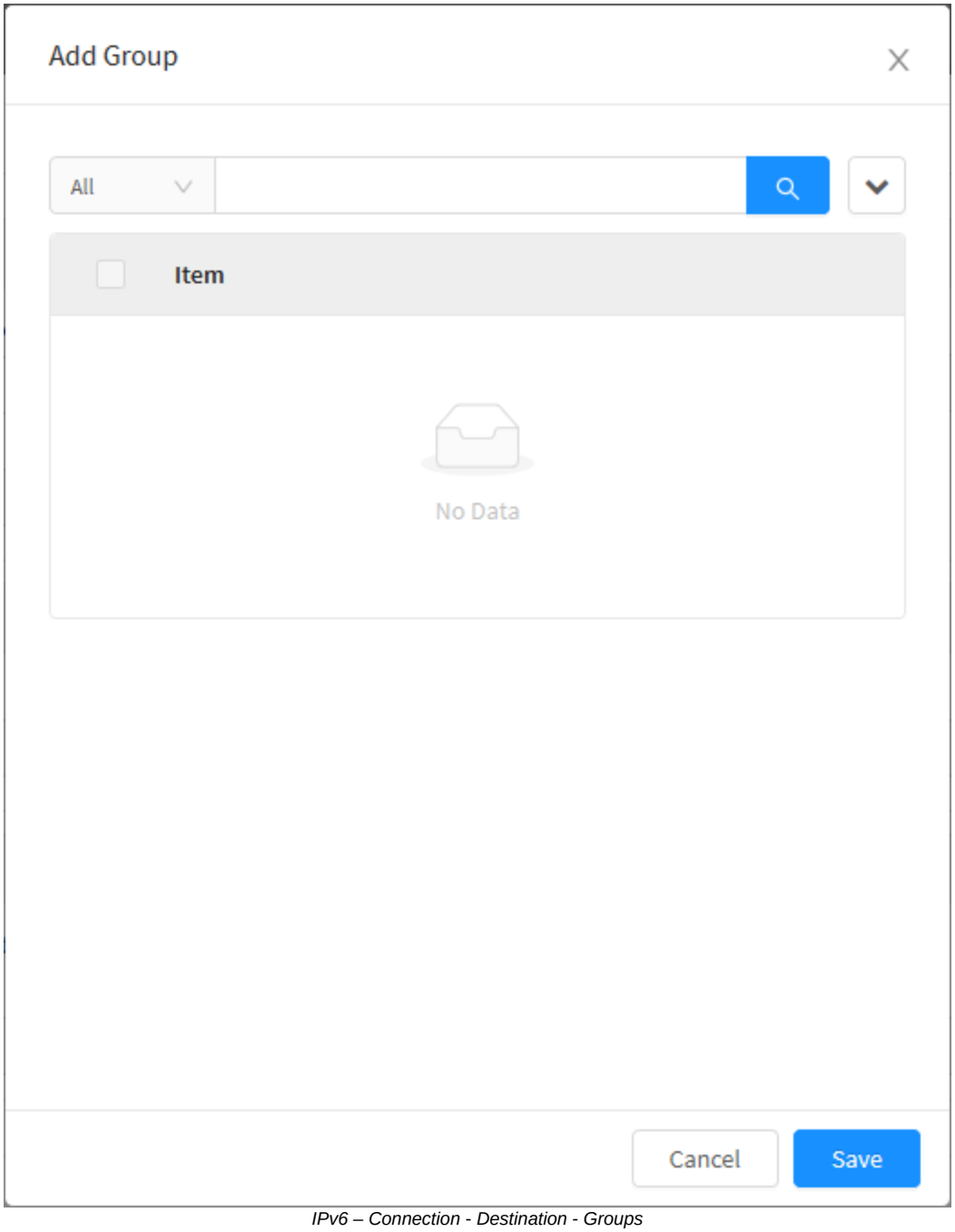
Policies IPv6 – Connection - Identification

- ***Authenticated[ ]*:** If enabled, this check box determines whether the policy requires authentication;
- ***Users[ ]*:** This field is only available by checking the checkbox and the Authenticated option. Allows you to specify the user (s) to which the policy will be applied. When clicking on the **[ ] button**, the screen below will be displayed to select one or more users that will compose the rule;



IPv6 – Connection - Destination - Users

- ***Groups[ ]*:** This field is only available by checking the checkbox and the Authenticated option. Allows you to specify the group(s) to which the policy applies. When clicking on **[ ]**, the screen below will be displayed to select one or more groups that will compose the rule.



IPv6 – Connection - Destination - Groups

Next, we will analyze the contents of the Inspection tab.

- Routing;
- Advanced.

IPv6 - Create Policy - Inspection tab

In the **[Inspection]** tab, it is possible to select several resources to inspect the traffic affected by the policy.

IPv6 - Side Tabs - *Inspection*

This tab contains the panel

- *Inspection*;

Next, we'll look at it.

Inspection

Below is a description of the function of each field on the form displayed in the **[Inspection]** panel:

IPv6 – Inspection - Inspection

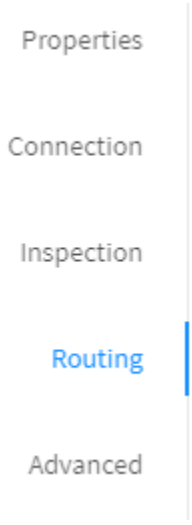
- ***SSL Inspection*** [☑]***:*** *This field is only available by checking the checkbox. This field allows the interception of SSL traffic allowing the inspection of its content. The options that appear in this menu are created in Proxy - SSL Inspection*;
- ***Intrusion Prevention*** [☑]**:** *This field is only available by checking the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in Services - Intrusion Prevention*;
- ***Threat Protection*** [☑]**:** This field is only available by checking the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in Services - Threat Protection;
- ***Application Control*** [☑]**:** This field is only available by checking the checkbox. This field allows you to select a profile to apply access control to applications. The profiles displayed in this menu are created in Services - Application Control;
- ***Web Filter*** [☑]**:** This field is only available by checking the checkbox. This field allows you to select a profile to perform content filtering. The profiles displayed in this menu are created in Services - Web Filter.

Next we will analyze the content of the *Routing* tab.

- Advanced.

IPv6 - Create Policy - Routing tab

In the **[Routing]** tab, you configure the NAT, SD-WAN profile, QoS, among others that will be detailed below. Next, we will analyze the function of each field of the forms.



IPv6 - Side tabs - *Routing*

This tab contains the panels:

- *Gateway*;
- *QoS*.

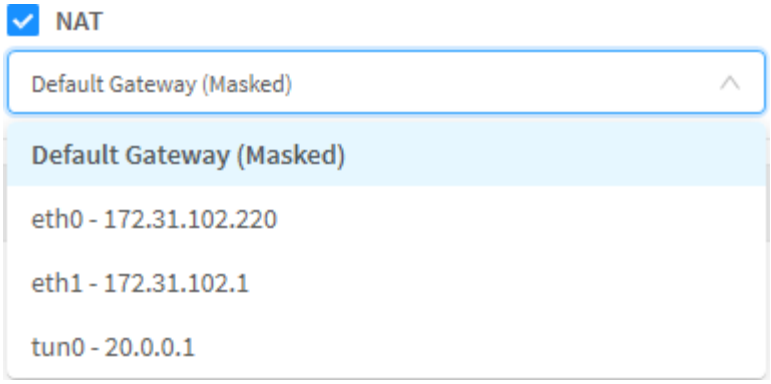
Next, we will analyze the function of each panel field.

Gateway

Below is a description of the function of each form field displayed on the **[Gateway]** panel:

IPv6 – Routing - Gateway

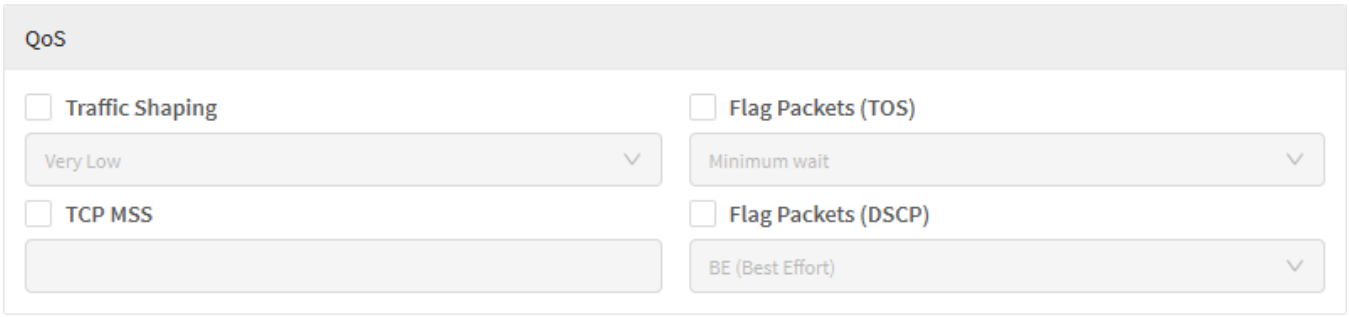
- ***NAT[ ]*:** Allows you to activate NAT and choose the address for source translation, by default the IP of the Default Gateway link is configured;



IPv6 – Routing - Gateway - NAT

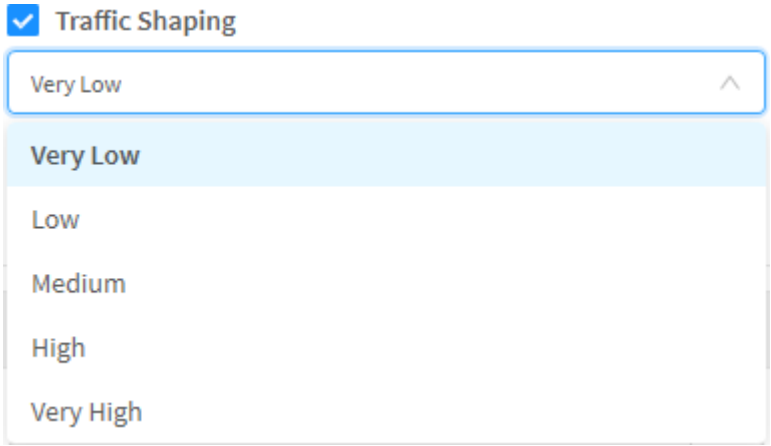
QoS

Below is a description of the function of each form field displayed in the **[QoS]** panel:



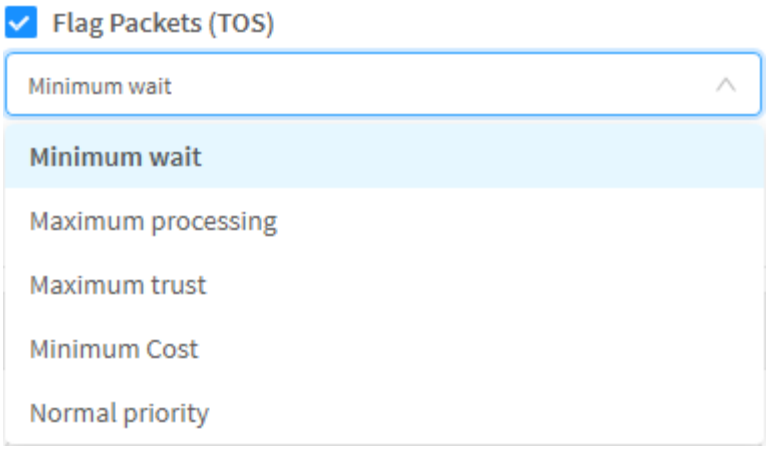
IPv6 – Routing - QoS

- ***Traffic Shaping[ ]:*** *It allows to activate and select the traffic priority, the values can be adjusted in* ***System Network Traffic Shaping;***



IPv6 – Routing - QoS - Traffic Shaping

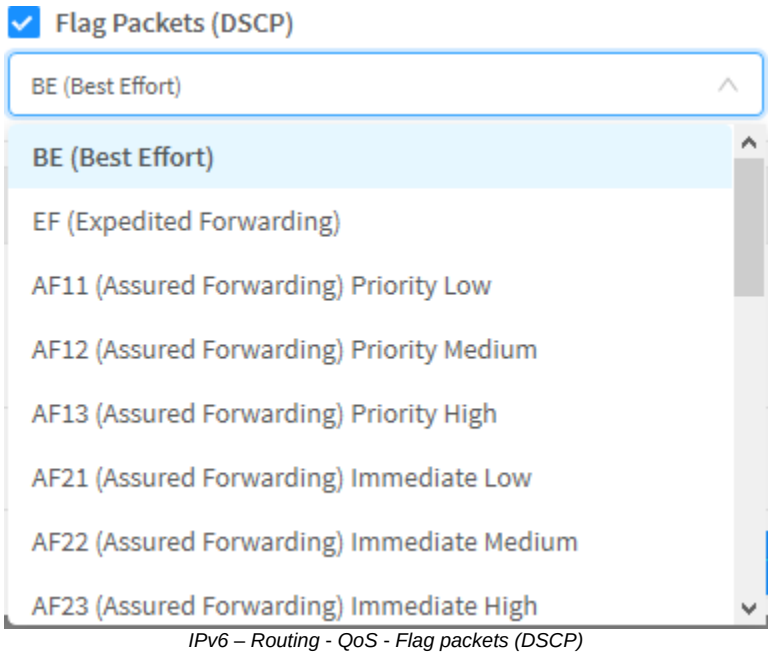
- **Flag packets (*TOS*)[ ]:** Activating allows the package to be marked according to the options: Minimum wait, Maximum processing, Maximum reliability, Minimum cost and normal priority;



IPv6 – Routing - QoS - Flag packets (TOS)

- ***TCP* MSS [ ]:** Allows you to define a value that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive on a single TCP segment;

- ***Flag packets* (*DSCP*)[ ]:** Activating allows the package to be marked according to the options.



IPv6 – Routing - QoS - Flag packets (DSCP)

Finally, we will analyze the Advanced tab.

IPv6 - Create Policy - Advanced tab

In the **Advanced** tab, it's possible to set the parameters' limits of the packages per second in a connection.

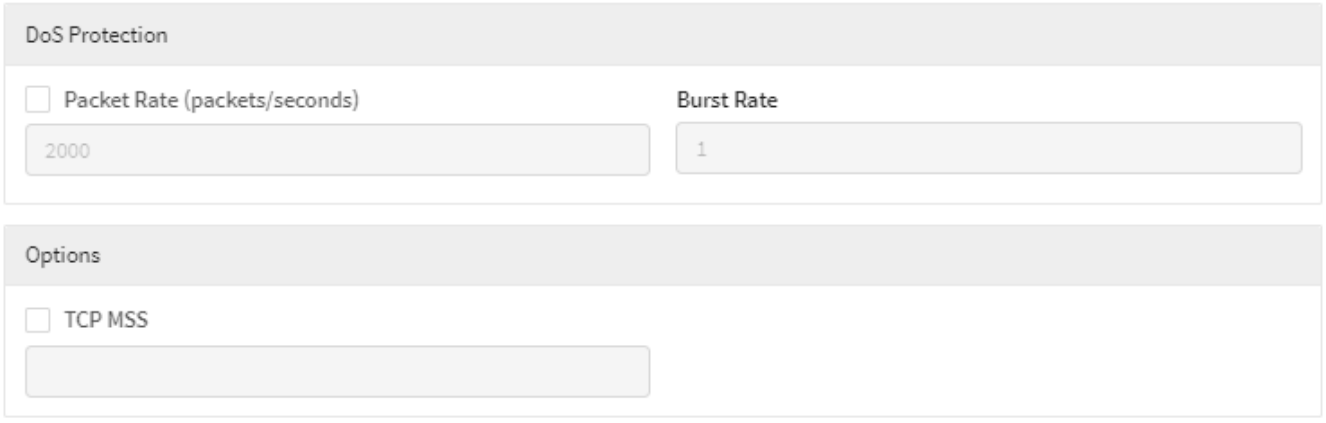
IPv6 - Side Tabs - *Advanced*

This tab contains the following panel:

- *Inspection*;

Advanced

We'll look at a description of the functions of the fields available on the Advanced form:



IPv6 – Inspection - Advanced

DoS Protection: With the DoS Protection box checked [☑] it's possible to limit the maximum quantity of packages per second in the Firewall, avoiding distributed attacks or traffic anomalies caused by possible malwares in the network.

- ***Packet Rate****:* The *Packet Rate* option sets up the *Firewall* in order to limit the connections to a maximum amount of packages per second.
- ***Burst Rate***: The *Burst Rate* option sets up the *Firewall* initially in order to allow a maximum quantity of packages per second without validating the Packet Rate, as to make the traffic control flexible in ocasional traffic peaks.

Options:

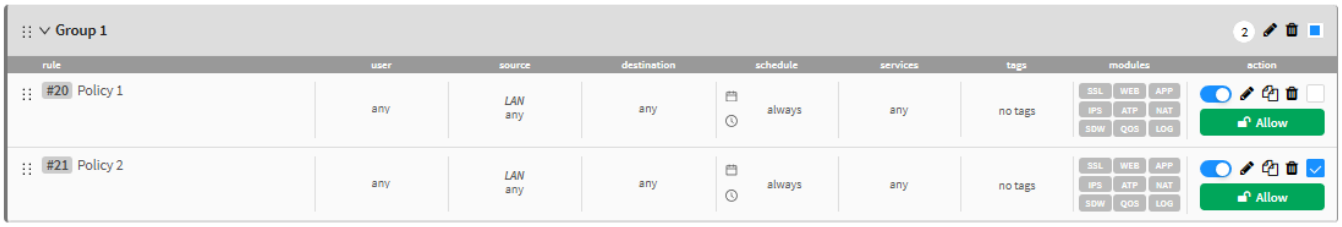
- ***TCP* MSS [☑]:** Allows the definition of a value that specifies the major quantity of data, in bytes, that a computer or communication device can receive in a single *TCP* segment.

This concludes the analysis of each window pane.

IPv6 - Actions Menu - Delete Policies

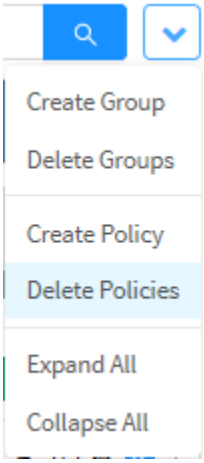
The “Delete Policies” button removes the selected Policies. To delete, follow the steps:

1. Select the Policy(ies) to be deleted. To select them, simply click on the checkbox. On the selected packages the checkbox will change from gray to blue **[ ]**. Ex.: *Policy 1* and *Policy 2*;



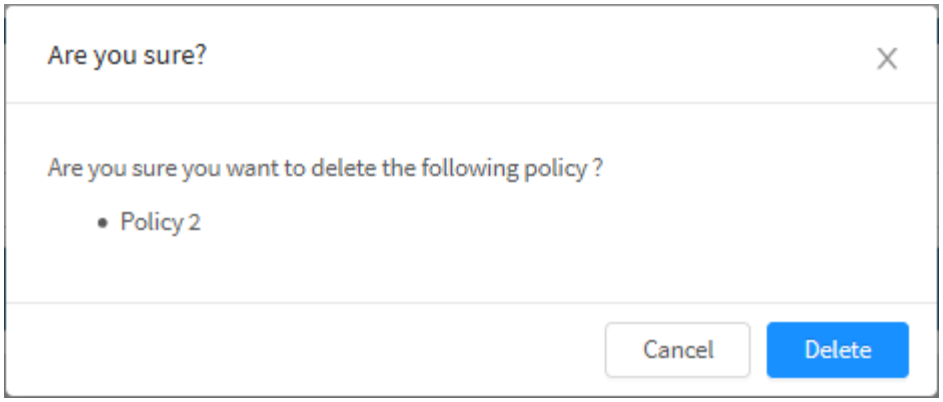
Policies selected to be deleted

2. In the actions menu **[ ]**, click on the option “Delete Policies”;



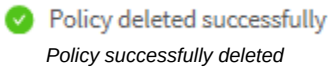
Policies IPv6 - Actions Menu - *Delete Policies*

3. The screen will appear asking if you want to delete the items:



Policies IPv6 - Deletion confirmation message

If you wish to cancel, click on the **[** Cancel **]** button. To finish, click on the **[** Delete **]** button.



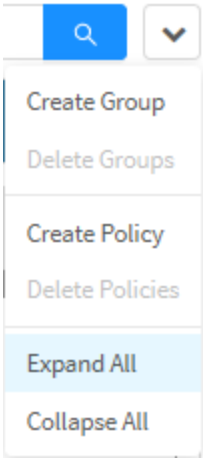
Policy successfully deleted

Policies have been successfully removed.

IPv6 - Actions Menu - Expand All and Collapse All

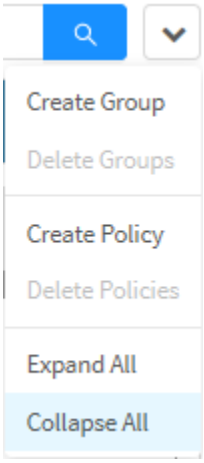
The “Expand All” button is intended to show more information on the policy group. To expand it, follow these steps:

1. In the action menu, click on the “Expand All” option to expand the expanded policy groups;



Policies IPv4 – Actions Menu – *Expand All*

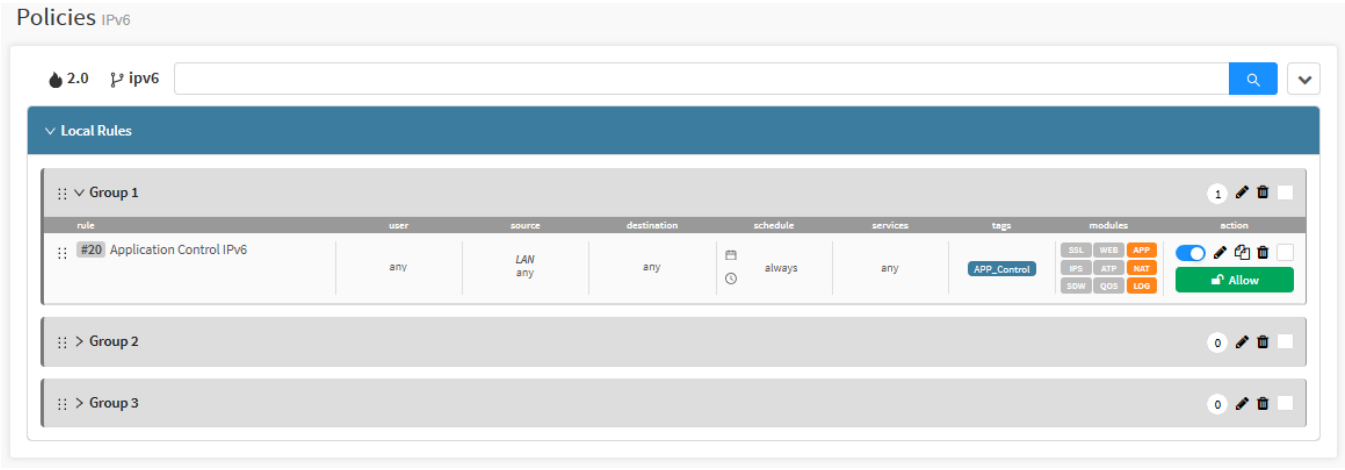
2. By clicking on “Collapse All” in the action menu, the opposite is the case.



Policies IPv4 – Actions Menu – *Collapse All*

IPv6 - Columns

The IPv6 Policies screen displays more detailed information on the created policies.



IPv6 – Policies

The top of the Policy panel contains:

- **Package Name:** Displays the name of the registered Policy Package;
- **System Version[ ]:** Displays the version in which the Policy Package was created. It is extremely important to create Policy Packages of the same version as the NGFW's, otherwise the package will not be compatible;
- **IP[ ]:** Represents the type of IP used in the created Policy Packages. Ex .: “IPv6”;
- **Search Bar:** Its function is to make it possible to locate specific items, it is possible to click on some column fields within the policy group to serve as a filter in a more specific search, for more information check this page.
- **Actions Menu [ ]:** Features the following set of contextual options:
  - *Create Group*;
  - *Delete Groups*;
  - *Create Policy*;
  - *Delete Policies*;
  - *Expand All* and *Collapse All*.
- **Pre Rules:** If a GSM is linked to this NGFW, it represents all the policy groups that were put in place before the local NGFW policies, so they have priority over the policies created in the NGFW itself;
- **Local Rules:** Represents the rules of the policy groups created in the NGFW itself;
- **Post Rules:** All policy groups that will be created will take effect only after local NGFW policies, so they will have lower priority and will be installed below existing policy groups at the NGFW.

It is important to remember that the policies are ordered by “Priority”, and they are applied considering the “First Match Wins” method.

Therefore, the policies located above have priority while those below have a lower priority.

Each policy group contains the following buttons:

- [ ] Clicking and dragging moves the group order and allows you to rearrange the priority according to which group is above (First Match Wins);
- [ ] Expands to display the policies created in the group;
- [ ] Reports how many policies there are in the group;
- [ ] Allows you to edit the settings added in the *Create Group* option of the actions menu;
- [ ] Delete the group;
- [ ] Select the group to interact with the action menu.

The columns within each policy group are divided into:

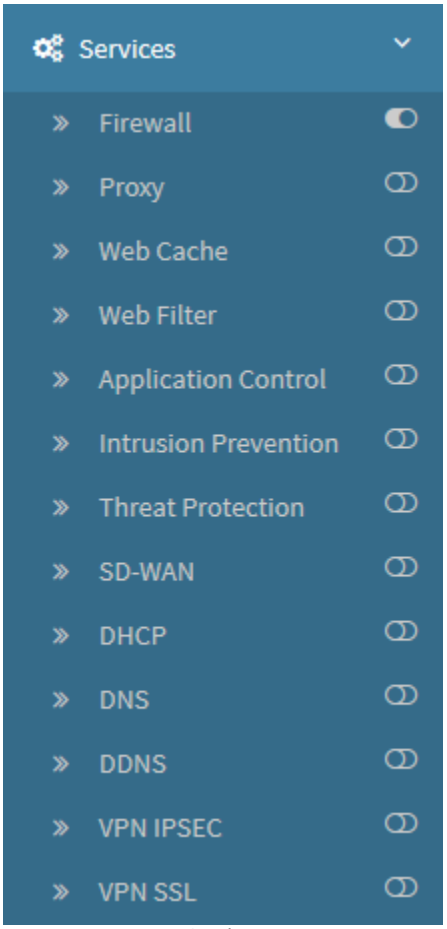
- ***Move*** **[**  **]:** Clicking and dragging moves the order of the policy and allows you to rearrange the priority according to which policy is above (First Match Wins);
- ***Id*** **[**  **]:** Displays the policy identification number, you can click it to serve as a filter in the search field;
- ***Rule*****:** Displays the policy name;
- ***User*****:** Determines which users are affected by the policy, you can click on this field to serve as a filter in the search field;
- ***Source*****:** Displays if the source of this rule will be the Network zone, IP address, network interface, Mac Address or any of these, you can click on this field to serve as a filter on the search field;
- ***Destination*****:** Determines the destination of the rule, the IP address or service, you can click on this field to serve as a filter in the search field;
- ***Schedule*****:** Displays if the rule depends on a period of time or schedule, you can click on this field to serve as a filter in the search field;
- ***Services*****:** Displays the services that the rule affects, you can click on this field to serve as a filter in the search field;
- ***Tags*****:** Displays the tags that have been added to this rule, you can click on this field to serve as a filter in the search field;
- ***Modules*****:** Determines which NGFW modules the rule will interact with, you can click on this field to serve as a filter in the search field;
- ***Action*****:** Displays some contextual buttons and what action the rule takes.
  - ***Enabled*****[**  **]** or **Disabled[**  **]:** Using this selector, enables or disables the rule;
  - ***Edit*****[**  **]:** Allows you to edit the settings added in the *Create Policy* option of the actions menu;
  - ***Clone*****[**  **]:** Copies a policy. Note that when using this option, the copied policy will use the same name as the original, but it will add a number on the front of the new one (for example, if I copy the policy "Test" the copy will be called "Test (1)") and it will be automatically set below the original policy, therefore, taking into account "First Match Wins", it is important to move the policy according to the desired priority;
  - ***Delete*****[**  **]:** Removes the policy;
  - ***Select*****[**  **]:** Allows the selection of policies in order to interact with the actions menu;
  - ***Action*****:** Determines the behavior of the policy in question, having as possibilities:
    - **[**  **]:** This option grants access;
    - **[**  **]:** Access is denied;
    - **[**  **]:** Access is denied, but a rejection message is displayed to the user.

This concludes the analysis of IPv6 policies.

UTM - SERVICES

Through the Services item it is possible to manage all the services available in the BLOCKBIT NGFW.

Activate a service using the [ ] button, to disable a service use the [ ] button.



Services

Contains the options:

- ***Firewall***;
- ***Proxy***;
- ***Web Cache***;
- ***Web Filter***;
- ***Application Control***;
- ***Intrusion Prevention***;
- ***Threat Protection***;
- ***SD-WAN***;
- ***DHCP***;
- ***DNS***;
- ***DDNS***;
- ***VPN IPSEC***;
- ***VPN SSL***.

UTM - Services - Firewall

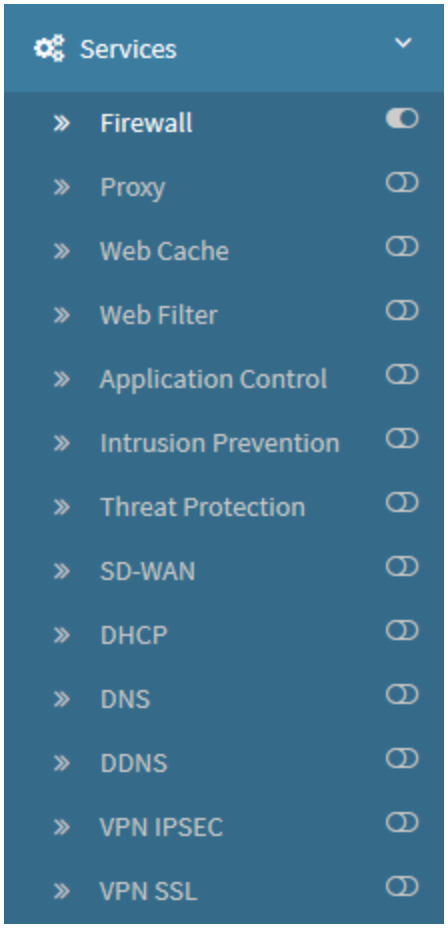
The Blockbit NGFW enables protection for internal network segments or for external environments, such as edge perimeters, data centers, hybrid networks and cloud applications. It was designed to protect your organization's confidential information through security controls used to prevent the intrusion of malicious programs on the network.

These controls contain permissions to access services and ports, which by default are configured to prohibit all security parameters and connections, integrated with security policies, SSL interception, packet filters and NAT.

The Firewall operates in "Stateful" mode and has tools that parameterize the "Security Levels" and "Control of connections", in addition to the "Packet Filters" and "Redirection - DNAT" policies.

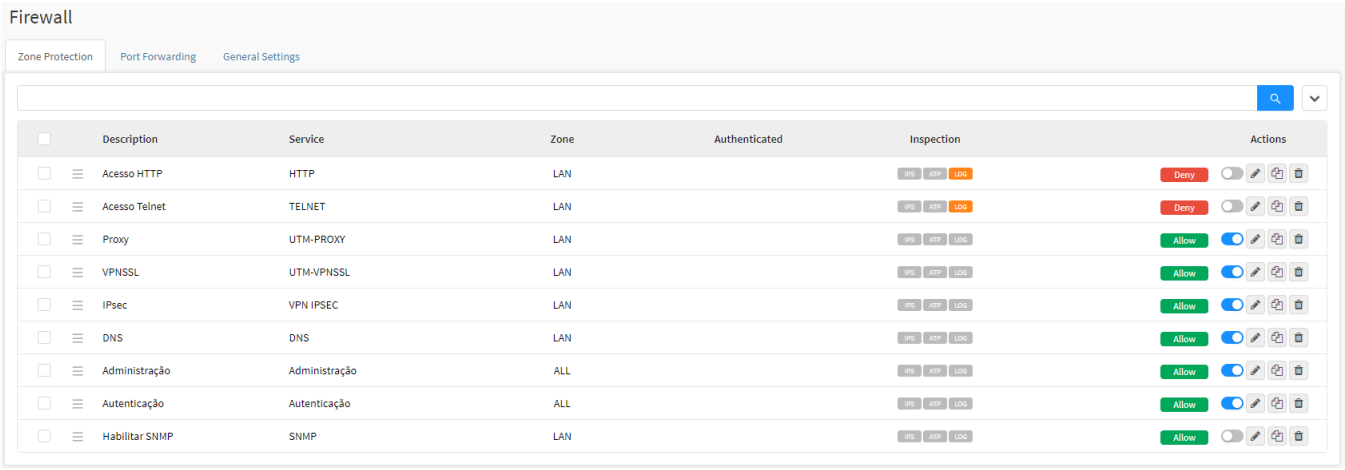
The service is pre-configured to allow access to local Blockbit NGFW services.

To access this screen, just select the option “Firewall”.



Services - Firewall

The screen below will appear:



Firewall - Settings

The Firewall screen has the following tabs:

- *Zone Protection*;
- *Port Forwarding*;
- *General Settings*.

Next we will analyze the components of the Zone Protection tab.

UTM - Firewall - Zone Protection

Through this tab, it is possible to configure entry policies for Blockbit NGFW local ports and services when it requires a specific access policy.

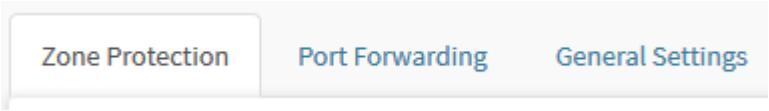
By default, Zone Protection policies are characterized by an access profile, a "network zone" and the "Actions" for handling the packet that even allow "Inspecting" traffic from **[Inbound]**.

Zone Protection policies deal with “Inbound” packets by conditional analysis that includes: “Network zone”, “Source IP”, “Destination IP”, with addressing support [IPv4/IPv6], “time” and “ Authentication by users and groups ”, are registered by“ Priority ”and support“ Reordering ”.

Entry policies of the “Zone Protection” type significantly increase the degree of security in accessing the services of the Blockbit NGFW device.

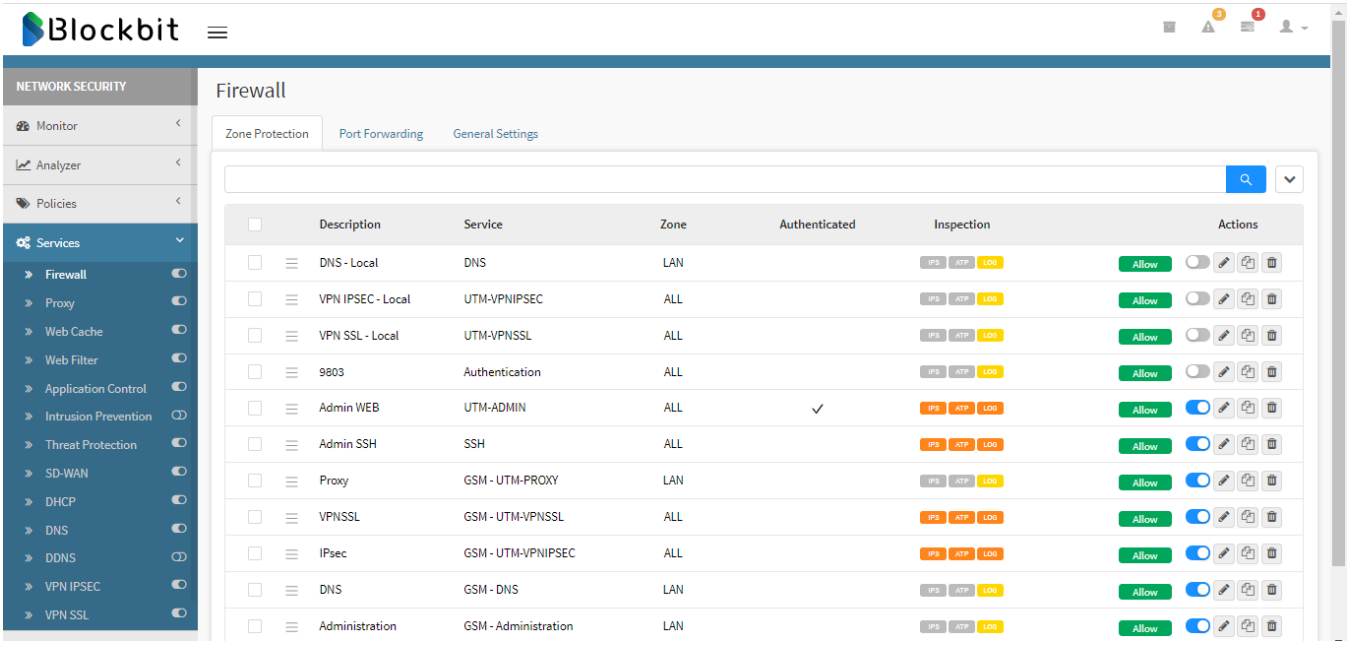
To open the "Zone Protection" screen, simply select the "Firewall" option in the vertical menu on the left.

If the tab is not selected, click on "Zone Protection".



Zone Protection tab

The “Zone Protection” screen will appear, as shown by the image below:



Zone Protection

The Zone Protection area has a search bar that allows the location of objects and contant inside these objects.

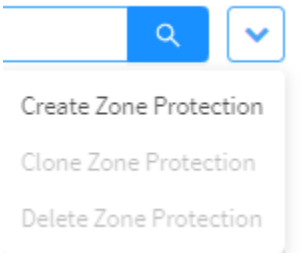
This session will cover:

- Creation, Editing and Removal of Zone Protection firewall policy;
- Activation and Deactivation;
- Examples of registration.

Next, we'll look at the functions located at the top of this panel.

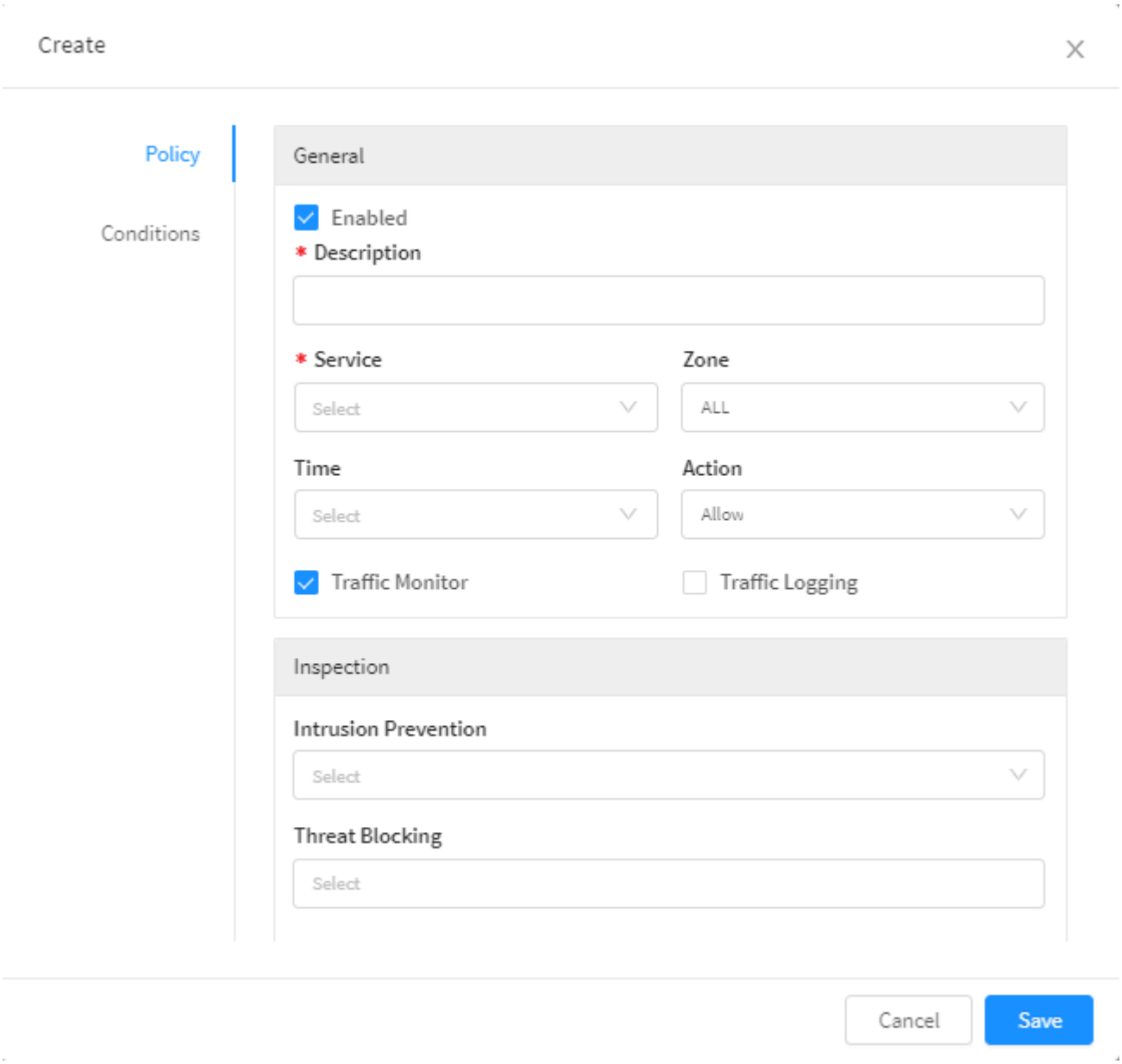
UTM - Zone Protection - Create button

To create a specific Firewall - Zone Protection Policy, click the button located at the upper right:



Zone Protection - Create Button

When clicking this button the window below is displayed:



Zone Protection - Create Button - Window

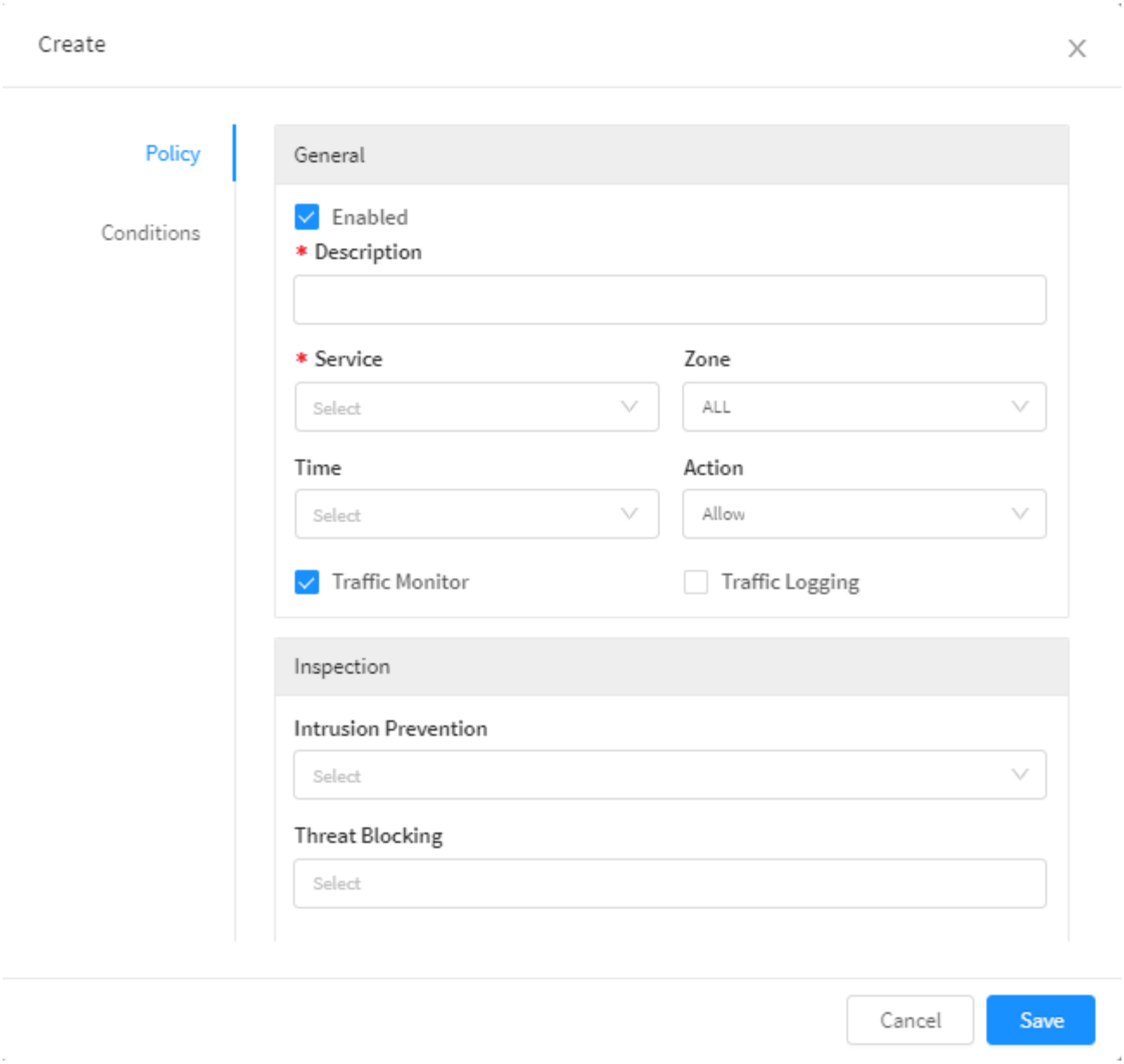
The menu consists of the sessions:

- *Policy*;
- *Conditions*.

Below we will analyze each of these sessions in detail.

Policy

In "Policy" we configure all options related to how the Zone Protection policy will work:



Zone Protection – Policy

- ***Enabled*[ ]: Determines whether the status is **on [ ]** or **off [ ]**;
- ***Description*: Defines a description for identification;
- ***Service*: It determines the service that will be used in the creation of the policy, the services that appear in this field are created in *Objects - Services*;
- ***Zone*: Determines the type of interface grouping that will be used. These groupings are created in *Network - Interfaces*;
- **Time:** Determines the time in which the policy will be applied, the items that appear in this field are created in *Objects* - Time;
- ***Action*:** Defines the action to be taken, which can be:
  - ***Allow*;**
  - ***Deny*;**
  - ***Reject*.**
- **Traffic Monitor:** When checking the*Traffic Monitor box*[ ], the information that match the located policy will be collected by the monitoring service and sent to the real-time summarizing service (Reporter).
- **Traffic Logging:** When checking the *Traffic Logging box*[ ], Logs reffering to the information collected by the monitoring service will be generated.
- ***Intrusion Prevention*:** With the checkbox checked, it determines which IPS will be used, in addition activates the drop-down list, which allows the selection of which profile will be used. The profiles that appear are created in *Services - Intrusion Prevention*;
- ***Threat Blocking*:** By activating this checkbox, all listed threats (as a tag) will be blocked in the text field. If tags are added without activating the checkbox, it will be activated automatically when saving.

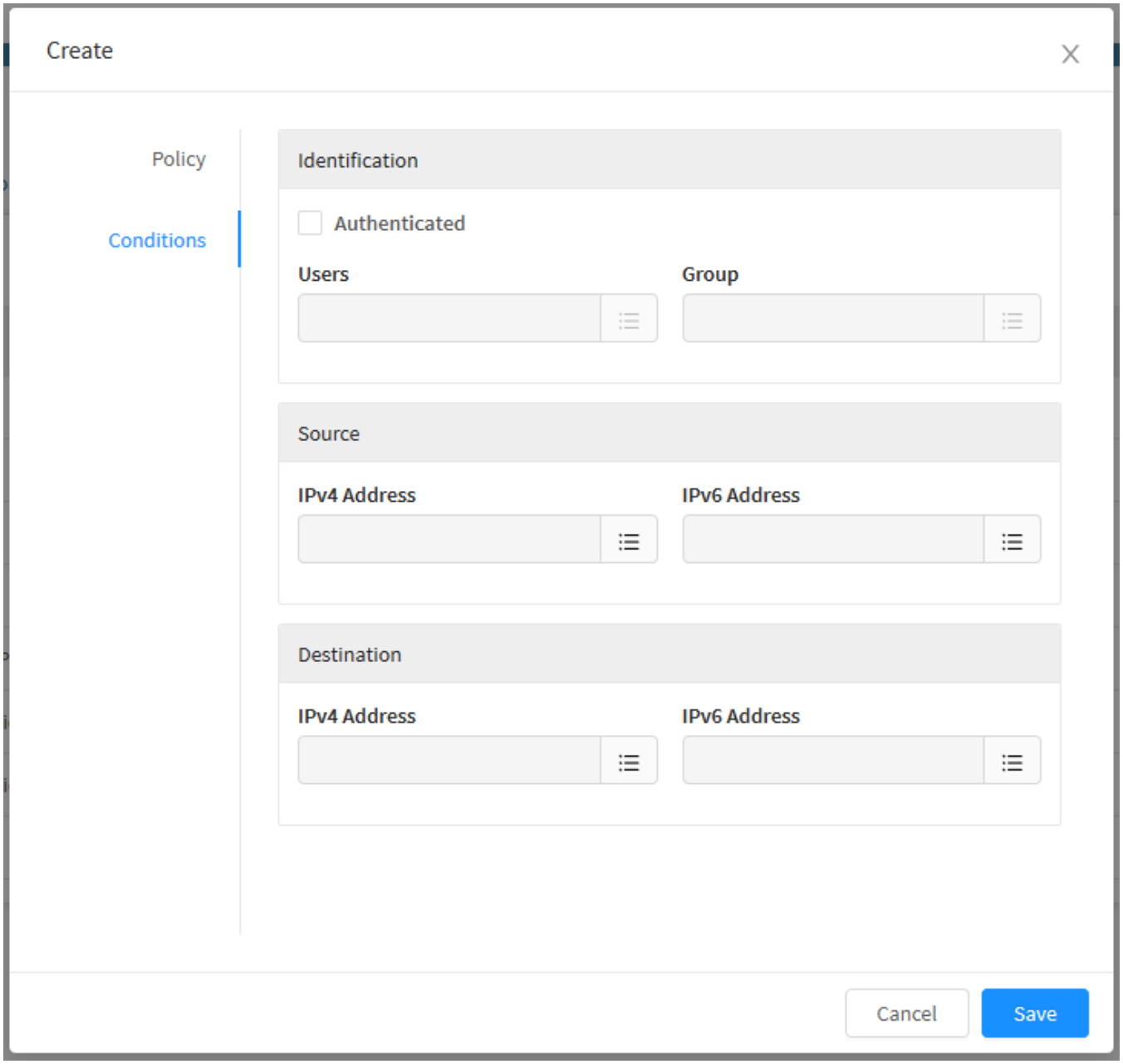
This concludes the configuration, if no "condition" is needed, save the changes by clicking [Save], if you want to close this window, click [ ] to cancel all settings and return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

If there is a need to configure "condition", check the section below.

Conditions

In "Conditions" we configure all the conditions on how Zone Protection will work:



Zone Protection – Conditions

- ***Authenticated[ ]:*** This check box determines whether the policy requires authentication (if enabled) or not (if disabled). In addition, by enabling this checkbox, the Users and Groups fields are available for editing;
- ***Users*:** Click **[ ]** and select all users to whom the policy will apply. The users that appear in this window are created in Settings - Authentication - Users tab;
- ***Groups*:** Click **[ ]** and select all user groups to which the policy will apply. The user groups that appear in this window are created in Settings - Authentication - Users tab - Groups – Add Group;
- ***IPv4 Source IP*:** Click **[ ]** and select all source IPv4 addresses to which the policy will be applied. The IPv4 addresses that appear in this window are created in Objects - Addresses;
- ***IPv6 Source IP*:** Click **[ ]** and select all source IPv6 addresses to which the policy will be applied. The IPv6 addresses that appear in this window are created in Objects - Addresses;
- ***Destination IPv4*:** Click **[ ]** and select all destination IPv4 addresses to which the policy will be applied. The IPv4 addresses that appear in this window are created in Objects - Addresses;
- ***Destination IPv6*:** Click **[ ]** and select all destination IPv4 addresses to which the policy will be applied. The IPv4 addresses that appear in this window are created in Objects - Addresses;

To save changes, click **[** Save **]**, otherwise, click **[ ]** to cancel all settings and return to the previous screen.

After saving, you will need to access the **command queue [** 1 **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

To better illustrate the procedures listed above, next, we will look at some examples:

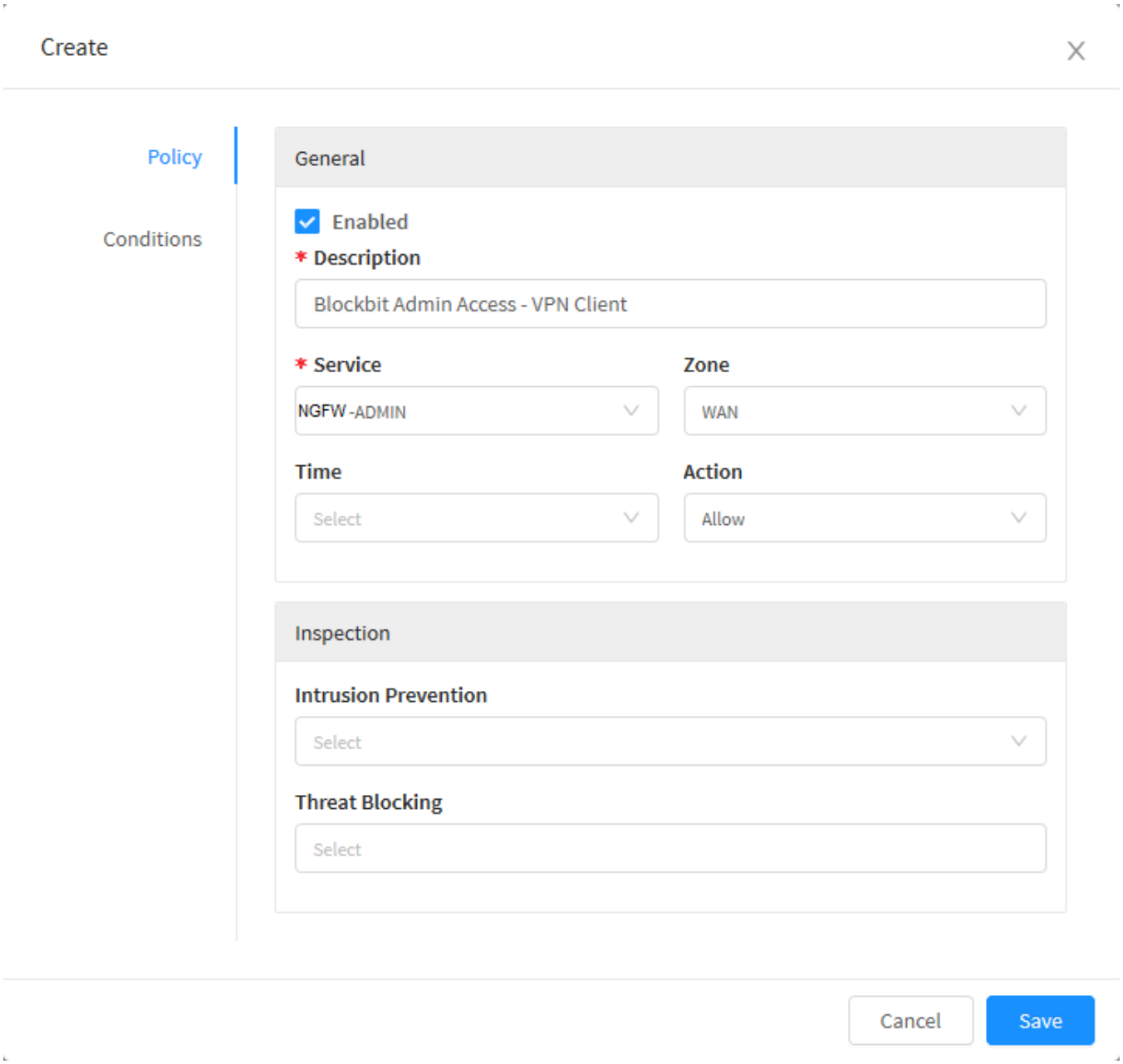
- Example 1 - Web interface access - Blockbit UTM (VPN Client);
- Example 2 - SSH remote access - over the WAN “Internet” - (Blockbit support).

UTM - Example 1 - Web interface access - Blockbit UTM (VPN Client)

Here is a demonstration of how to create a policy to allow access to the “Firewall” administration interface, through the VPN Client Network:

In this example we will add a “Permission” policy for the Blockbit Admin [98/TCP] port. Only for users who are members of the Support group and authenticated.

Policy



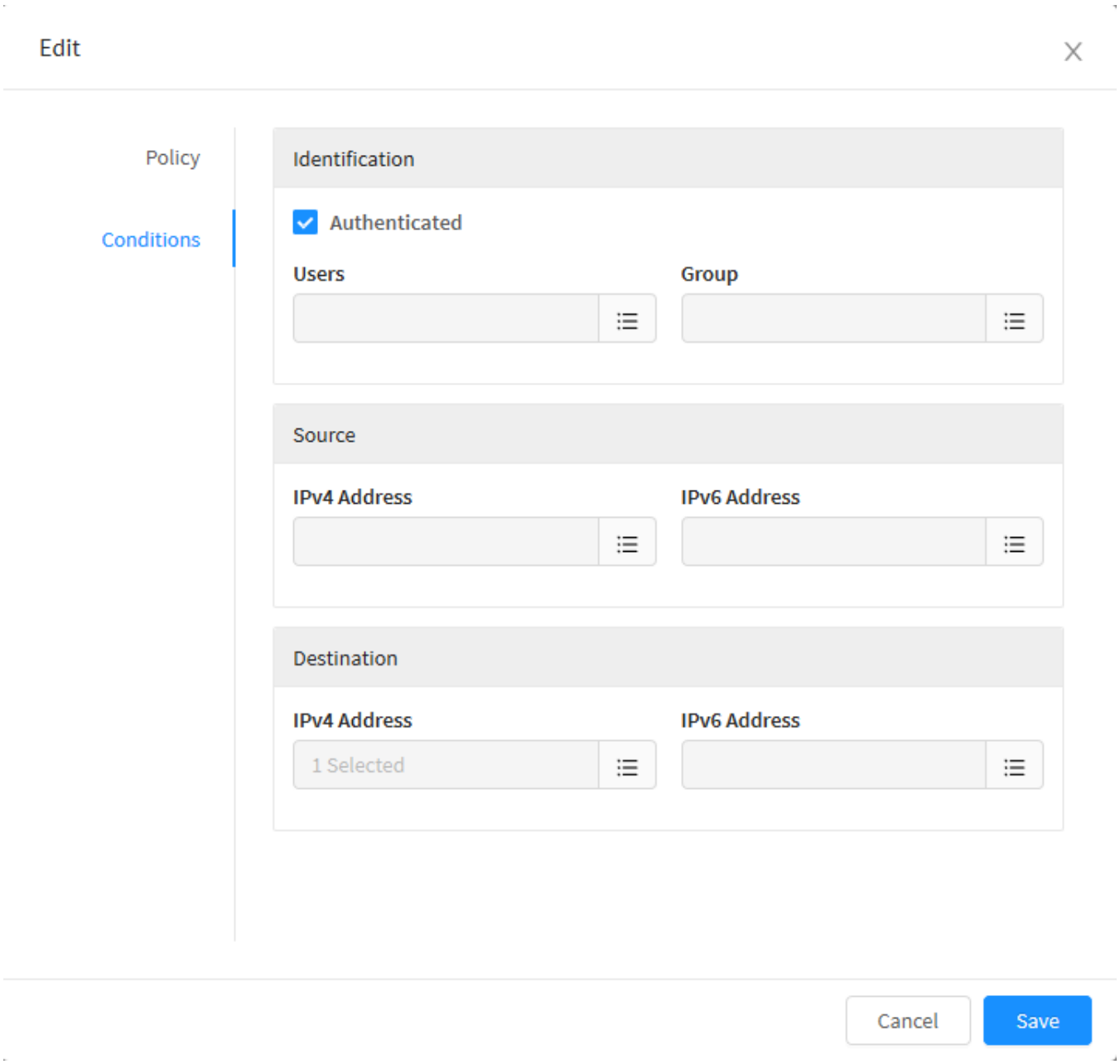
Zone Protection - Access interface admin for VPN client - Policy

Specifically complete the following fields:

- ***Enabled*** **[ ]:** Enable this checkbox;
- ***Zone***: Select “WAN”;
- ***Action*****:** Select “Allow”;
- ***Service*****:** Inform and select from the “NGFW-ADMIN” list;
- **Descrição:** "Blockbit Admin Access - VPN Client".

Next, we will analyze the settings that are needed in "Conditions".

Conditions



Zone Protection - Access interface admin for VPN client - Conditions

Specifically complete the following fields:

- **Authenticated [ ]:** Enable to require authentication;
- **IPv4 source IP:** Select the source IPv4 “192.168.31.0”. If necessary, add the address object, for more information see this page.

Finally, click **[Save]**, otherwise, click **[ ]** to cancel all settings and return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

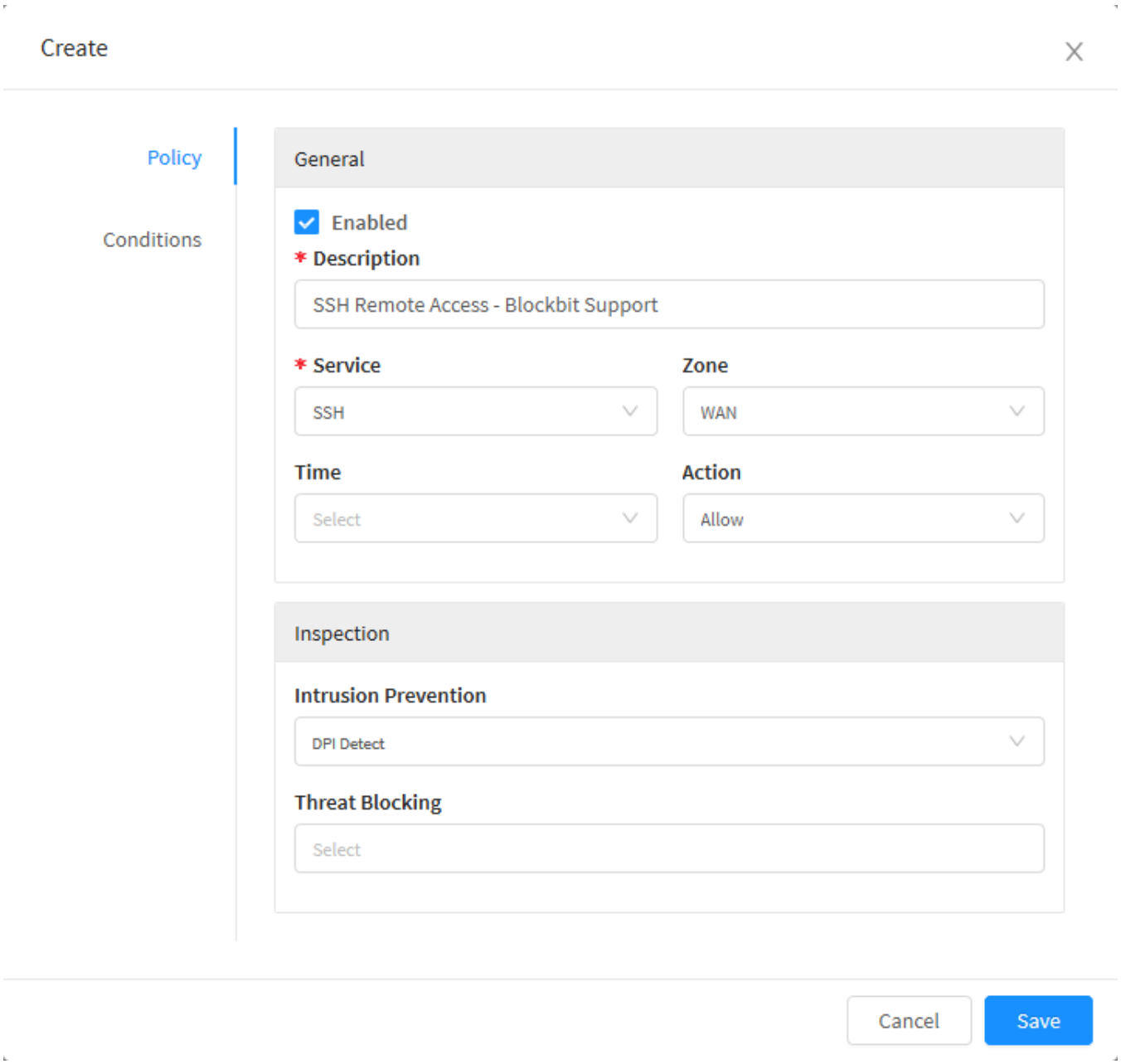
This concludes example 1.

UTM - Example 2 - SSH remote access - over the WAN “Internet” - (Blockbit support)

Here is a demonstration on how to create a policy that allows remote access to the SSH console over the internet.

In this example we will add a “Permission - with IPS inspection” policy for the SSH port [22/TCP]. Only for the source IP of the Blockbit support.

Policy



Zone Protection - SSH Remote Access – Policy

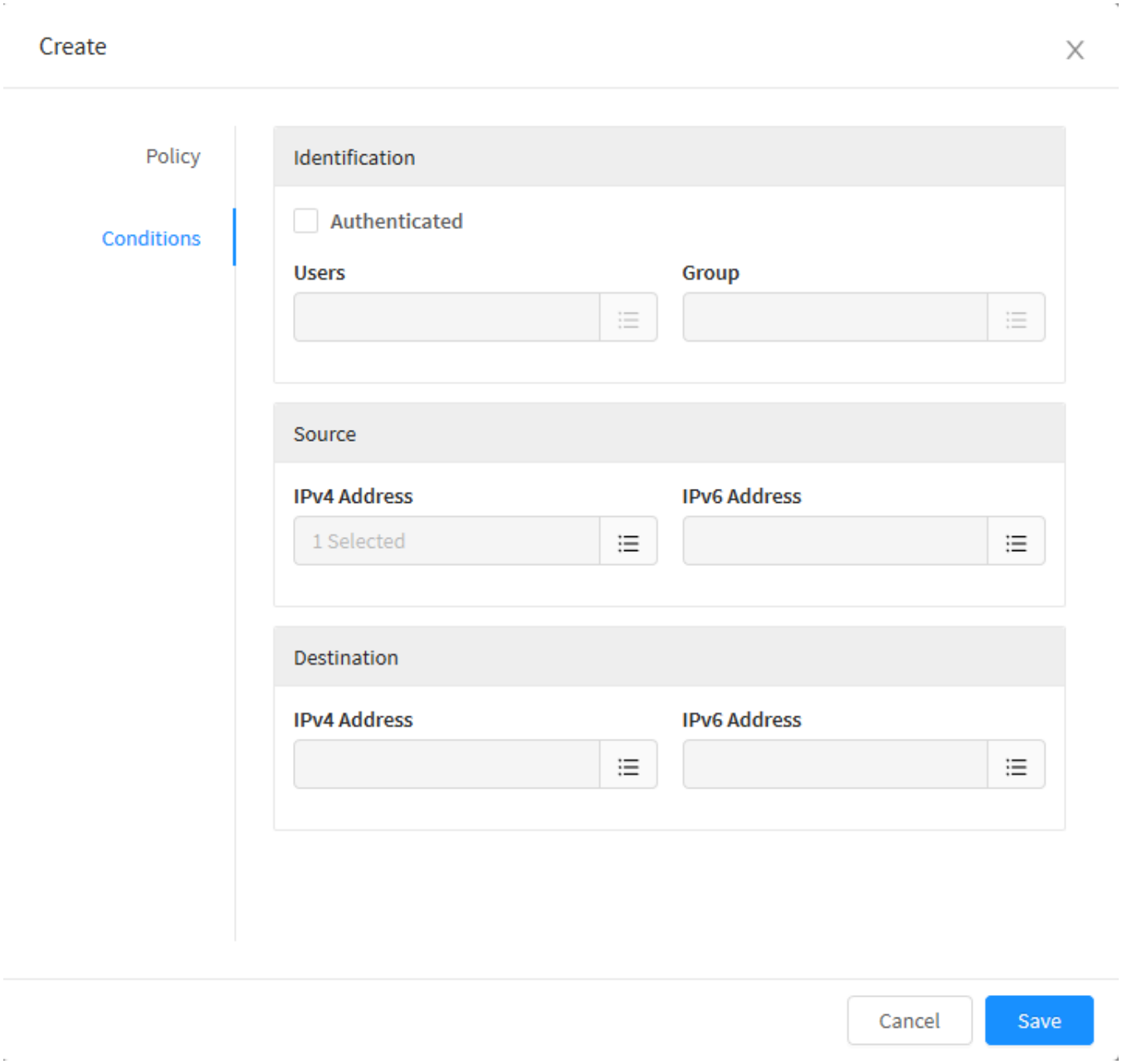
Specifically complete the following fields:

- ***Enabled*** **[ ]:** Enable this checkbox;

- ***Zone***: Select "WAN";
- ***Action*****:** Select "Allow";
- ***Service*****:** Inform and select from the “SSH” list;
- **Intrusion Prevention[ ]**: Check the checkbox and select the desired IPS, for more information check the Intrusion Prevention page;
- ***Description*****:** “SSH Remote Access - Blockbit Support”.

Next, we will analyze the settings that are needed in "Conditions".

Conditions

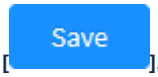


Zone Protection - SSH Remote Access - Conditions

Specifically complete the following fields:

- **Source IPv4:** Select from the list the IP that you want to give remote access to the SSH console over the internet, in this example we will use the “Blockbit Support” network object, for more information on how to create them, check this page.

The entry settings for Blockbit NGFW services in the [Zone Protection] item are intended to improve security levels in accessing firewall services and resources.

Finally, click **[** 

], otherwise, click **[ ]** to cancel all settings and return to the previous screen.

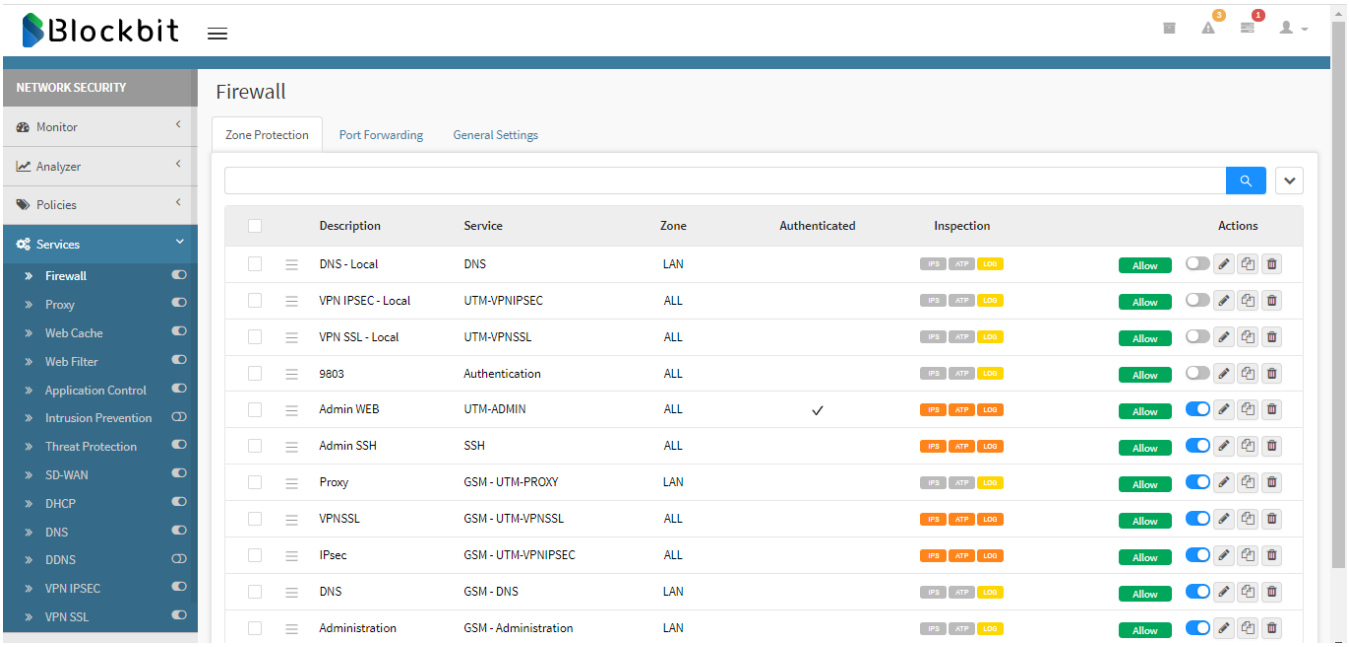
After saving, you will need to access the **command queue [** 

] and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

This concludes example 2.

UTM - Zone Protection - Columns

Next, we will explain each column of the Zone Protection tab:



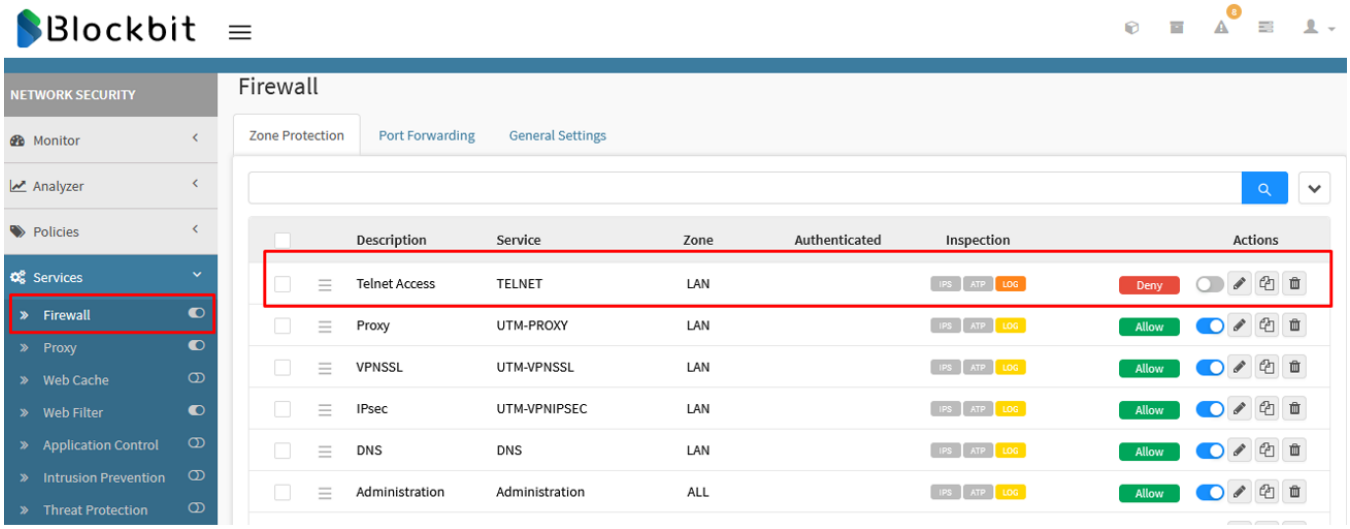
Zone Protection

- ***Select*** **[ ]:** Allows you to select a Firewall policy;
- ***Move[ ]:*** Allows you to move the Firewall policy and determine its priority, the topmost rule will have higher priority;
- ***Description:*** Displays the description of the policy that was added in *Zone Protection* - Add button;
- ***Service:*** Determines which service is used by the Firewall policy;
- ***Zone*****:** Displays the zone registered in Zone Protection - Add button, by default, can be LAN, WAN or DMZ
- ***Action:*** *Displays what action the policy will take*: **[** Allow **]**, **[** Deny **]** or **[** Reject **]**;
- ***Authenticated*****:** Determines whether authentication is required or not, if required, this icon **[ ]** will be displayed;
- ***Inspection*****:** Displays if the policy has enabled Intrusion Prevention **[** IPS **]**, Threat Blocking **[** ATP **]** or Log **[** LOG **]**;
- ***Actions Menu*****:** It provides the following essential actions:
  - ***Enable*****[ ]*****/Disable*****[ ]:** Allows you to enable or disable a Firewall policy;
  - ***Edit*****[ ]:** Allows you to edit the settings of the interface added in *Zone Protection* - Add button;
  - ***Delete*****[ ]:** Allows you to remove one of the items.
  - ***Clone*** **[ ]:** Allows you to clone an item.

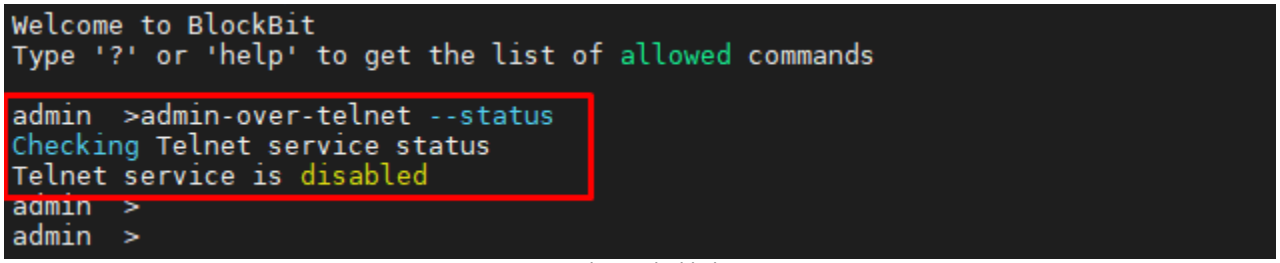
UTM - Zone Protection - Services Column

The Services column is configured along the creation of a Zone Protection Profile. In this section, we will analyze the enabling process of the SSH (Secure Shell) via Telnet service, in specific:

It is important to note that this service is disabled by factory default:

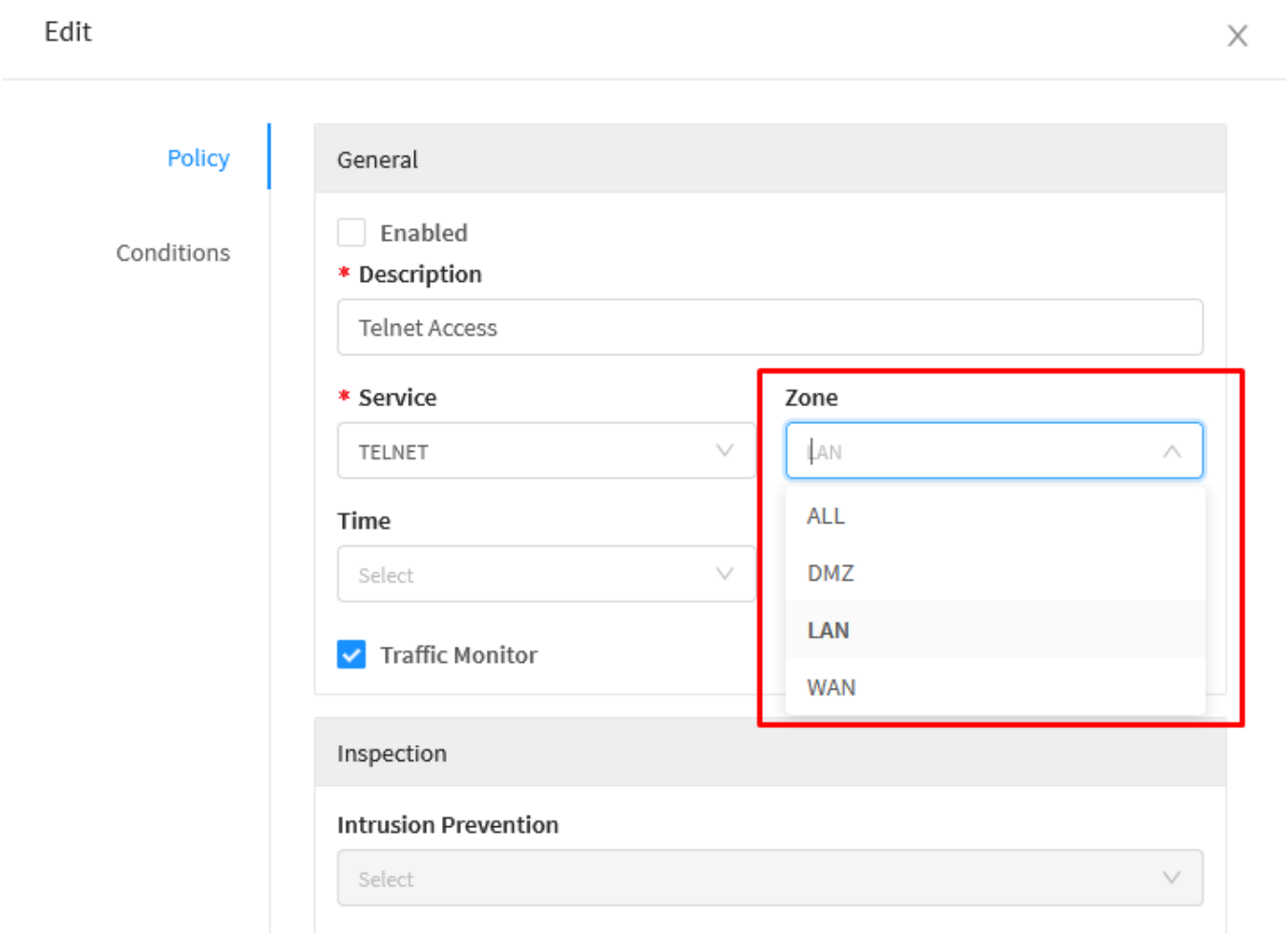


Firewall - Zone Protection

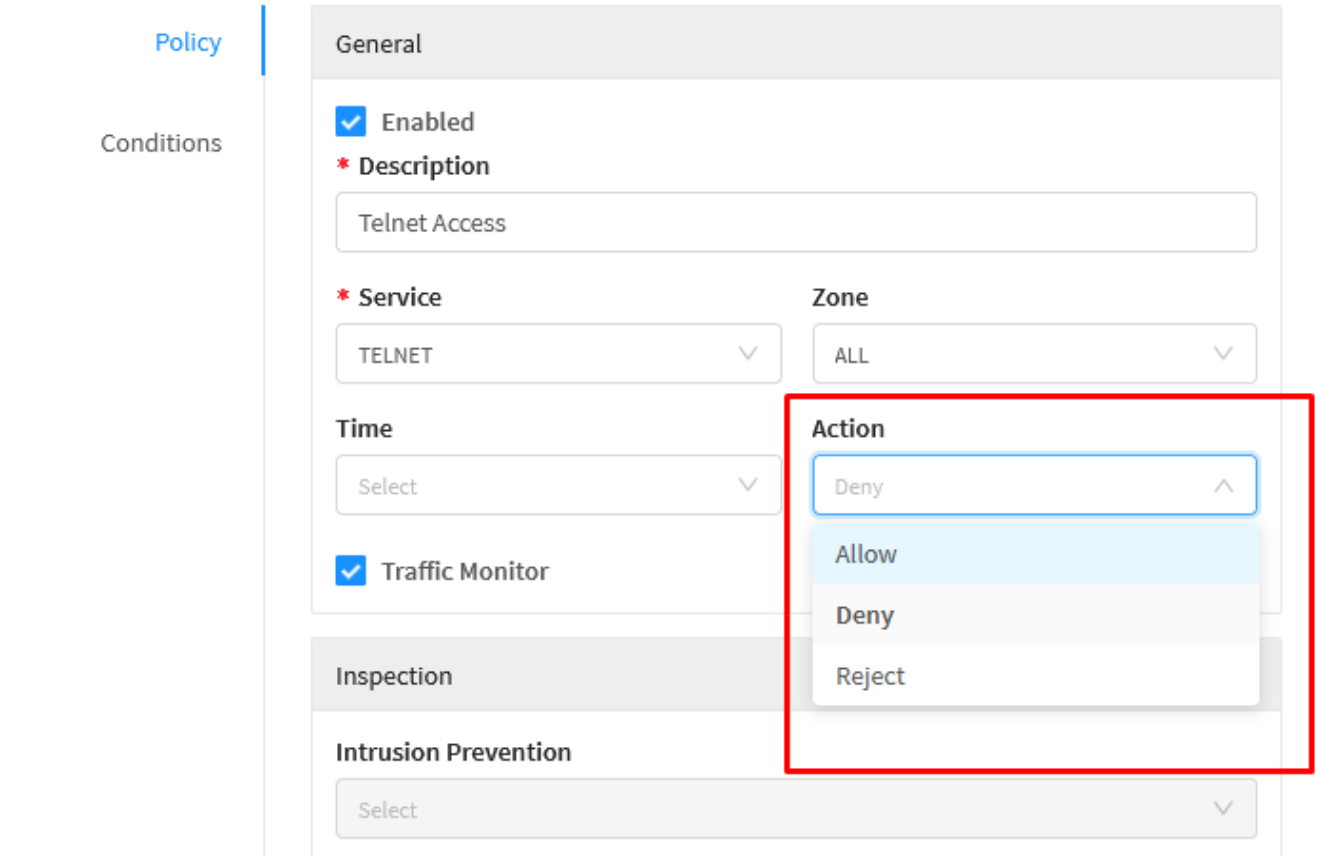


Telnet - Disabled

Firstly, we must create a rule in Zone Protection, to do that click in [ ] and in the *create option. Next, we must select the Zone and Action:*

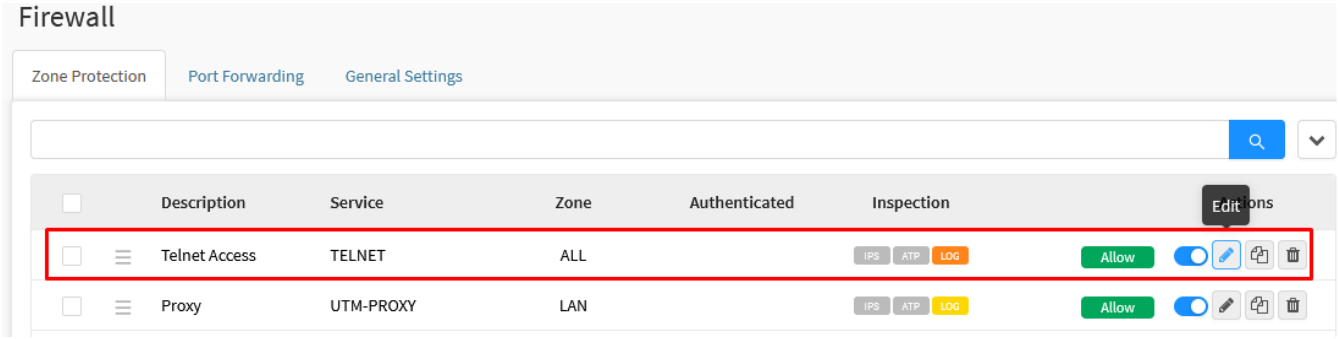


Zone Protection - Create - Zone



Zone Protection - Create - Action

After its creation, the rule will be displayed on the main screen:



Zone Protection - Telnet Rule

Bellow we can check the commands that can be used to manage the function:

```
admin  >
admin  >
admin  >admin-over-telnet
Usage: admin-over-telnet <enable|disable|status>

--enable: Enables service
--disable: Disables service
--status: Check service status

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

admin  >
```

CLI Interface - Telnet Management Commands

By using the "admin-over-telnet --enable" we can enable the Telnet service over the 23 port:

```
admin  >
admin  >admin-over-telnet --enable
Success Telnet service, enabled and started
admin  >
```

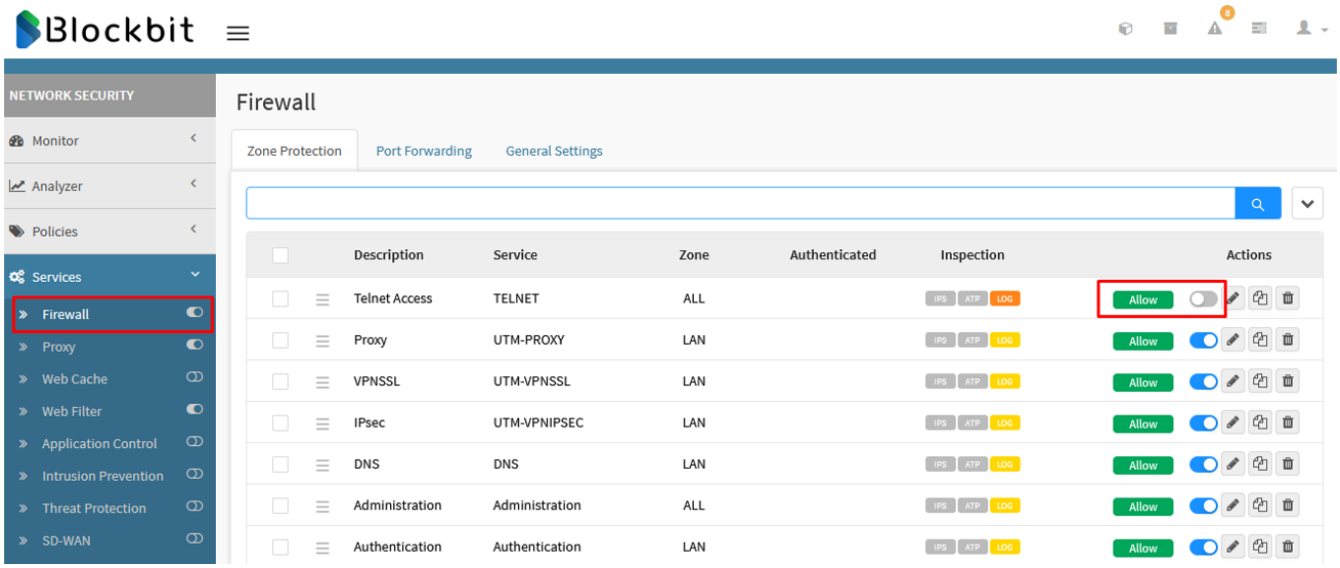
Enabling Telnet

To disable it, we must use the "*admin-over-telnet --disable*" command:

```
admin  >
admin  >admin-over-telnet --disable
Telnet disabled with success
admin  >
```

Disabling Telnet

The rule with the enabled service will then be visible on the main screen:

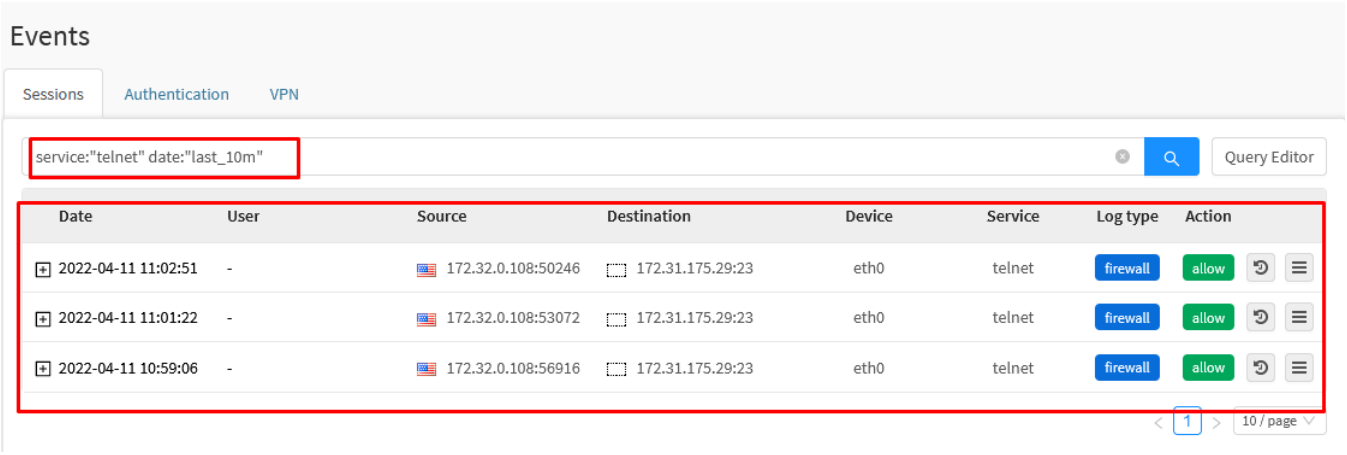


The rules with the Telnet service enabled can also be seen in Security Events:

Date	User	Source	Destination	Device	Service	Log type	Action
2022-04-11 11:02:51	-	172.32.0.108:50246	172.31.175.29:23	eth0	telnet	firewall	allow
2022-04-11 11:01:25	-	192.168.29.10:55926	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2022-04-11 11:01:22	-	172.32.0.108:53072	172.31.175.29:23	eth0	telnet	firewall	allow
2022-04-11 11:00:50	-	192.168.29.10:55926	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2022-04-11 10:59:06	-	172.32.0.108:56916	172.31.175.29:23	eth0	telnet	firewall	allow

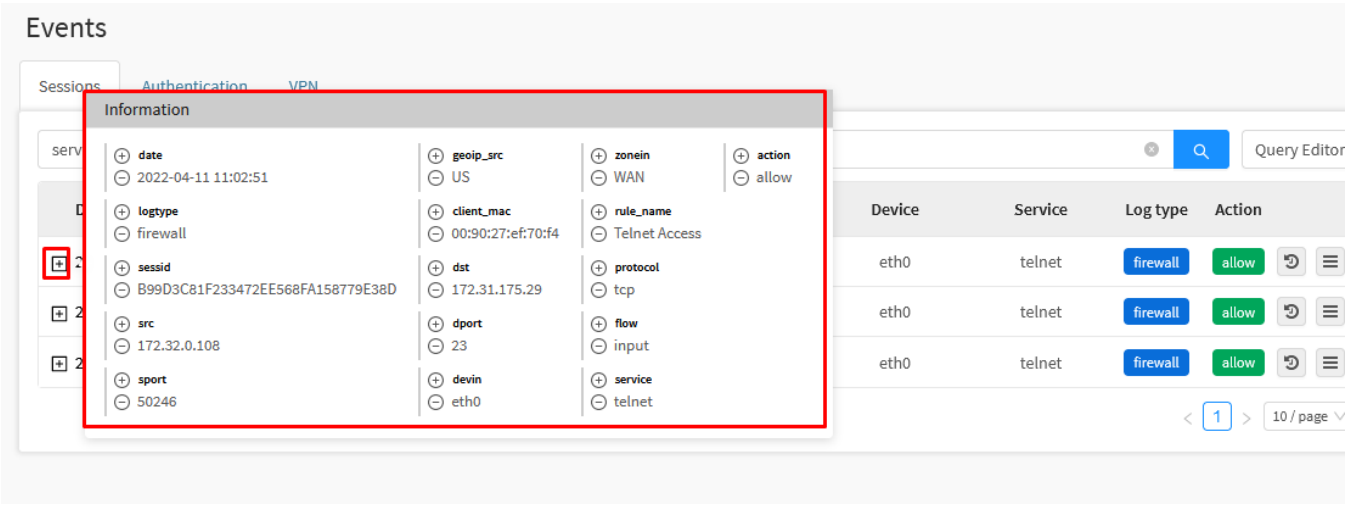
Telnet Enabled

By using the Query editor we can also search for the rule with active Telnet Service:



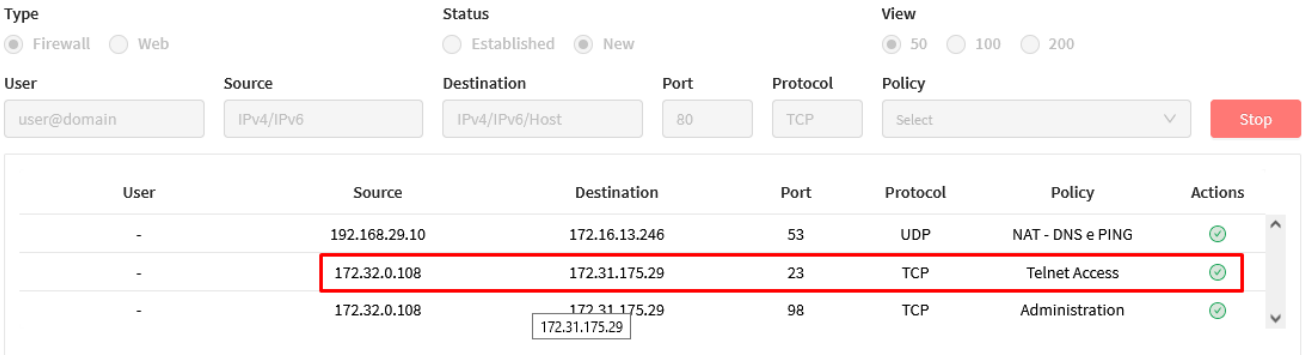
Security Events - Query Editor

By clicking the plus [⊞] button, we can check more information on the rule:



Query Editor - More information

In live Sessions we can also see the rule working:

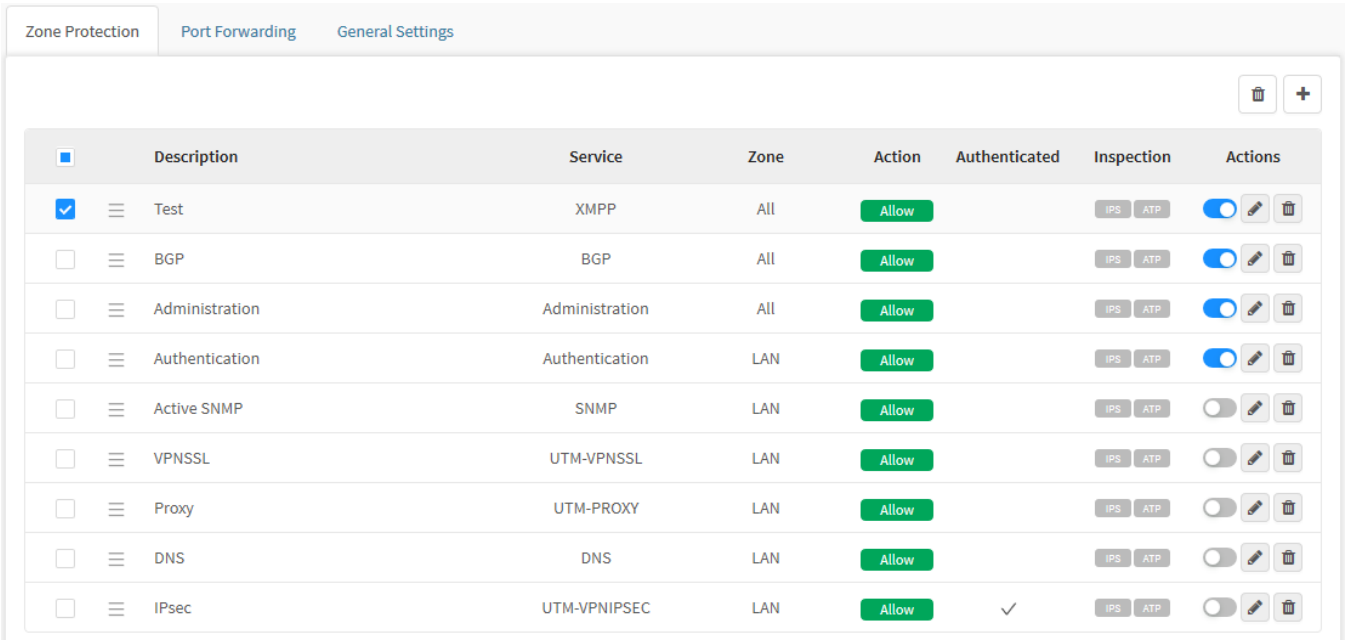


And so we could enable and verify the Telnet Service working.

UTM - Zone Protection - Remove

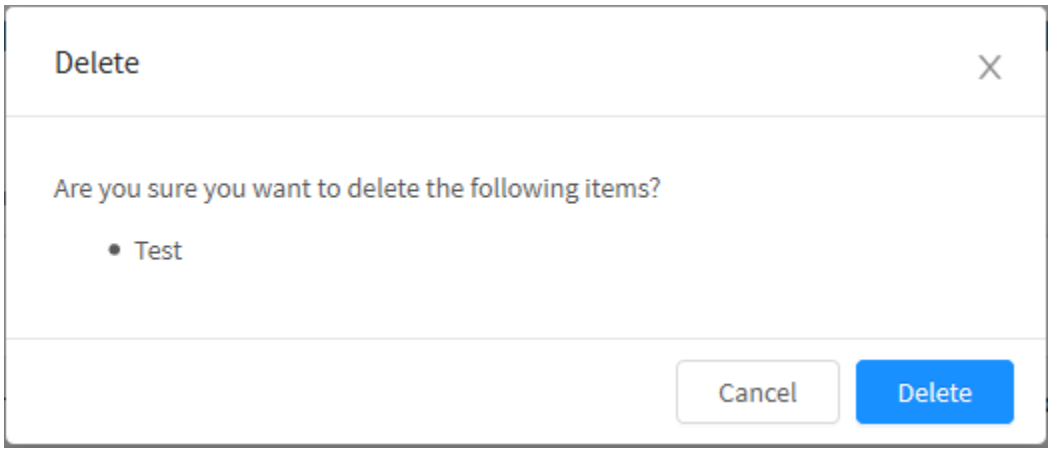
Through this button it is possible to delete several items at the same time. Follow the example below:

1. Select the items you want to delete by clicking on the **selection [ ]** icon;

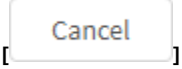
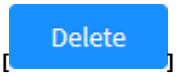


Zone Protection - Selection for deletion

2. Click on the **[ ]** button, a screen will appear asking if you want to delete the selected item:



Zone Protection - Remove items

If you want to cancel, click the **[**  **]** button. To complete the item removal, click the **[**  **]** button.

The item has been successfully deleted.

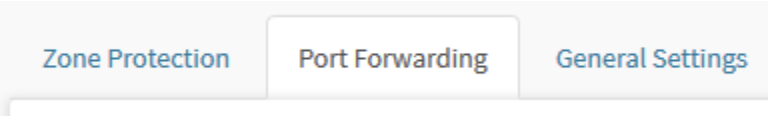
UTM - Firewall - Port Forwarding

The Port Forwarding allows a particular port to be determined for specific IP addresses on a LAN. This makes it possible, for example, to connect to another appliance or service through a private network, regardless of whether the appliance is behind a router.

The service is made up of packet filter rules with the option of address translation, making it possible to modify the destination address of client machines. Through its resources, it is possible to route traffic between the buses and configure DNAT masking, the latter being especially useful in redirecting ports.

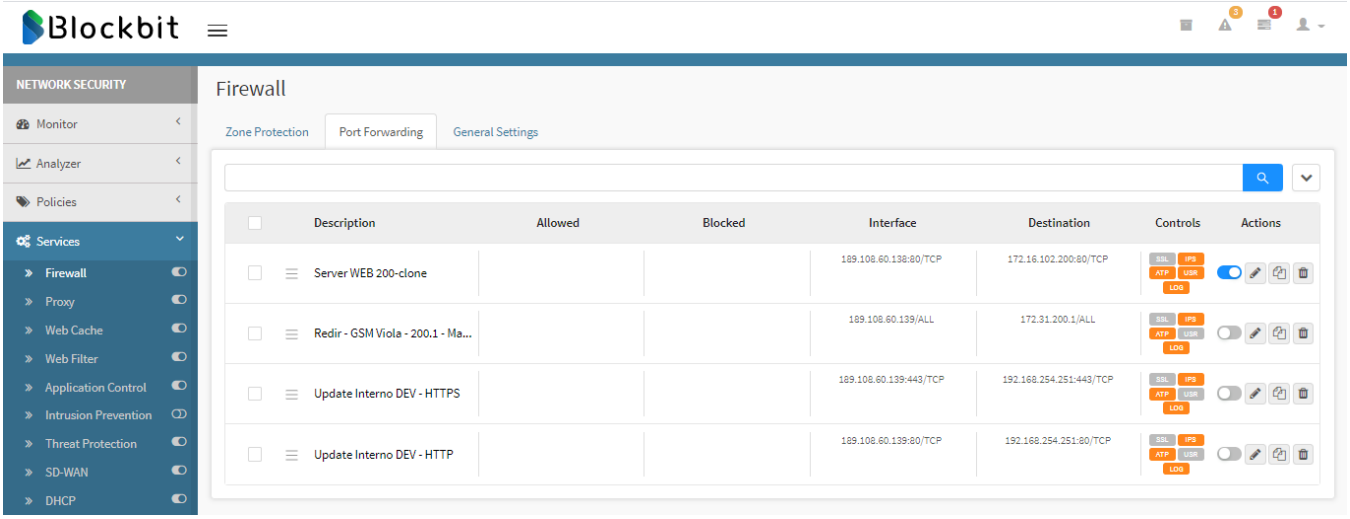
Port Forwarding rules are loaded from top to bottom, so the rules at the top of the table have priority over the ones below (being possible until they overlap the settings of the bottom rules).

To open the screen, click on the “Port Forwarding” tab.



Port Forwarding Tab

The screen below will appear:



Port Forwarding

The Port Forwarding tab has a search bar that allows the search for objects and content included in these objects.

The Clone button [ ] allows the replication of policies individually.

This session will cover:

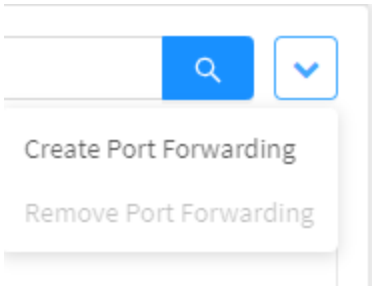
- Create, Editing and Removal of redirection policies;
- Activation and Deactivation of policies;
- Examples of redirect policies
- Column details on this screen.

Next, we will analyze the functions located at the top of this screen.

UTM - Port Forwarding - Create Button

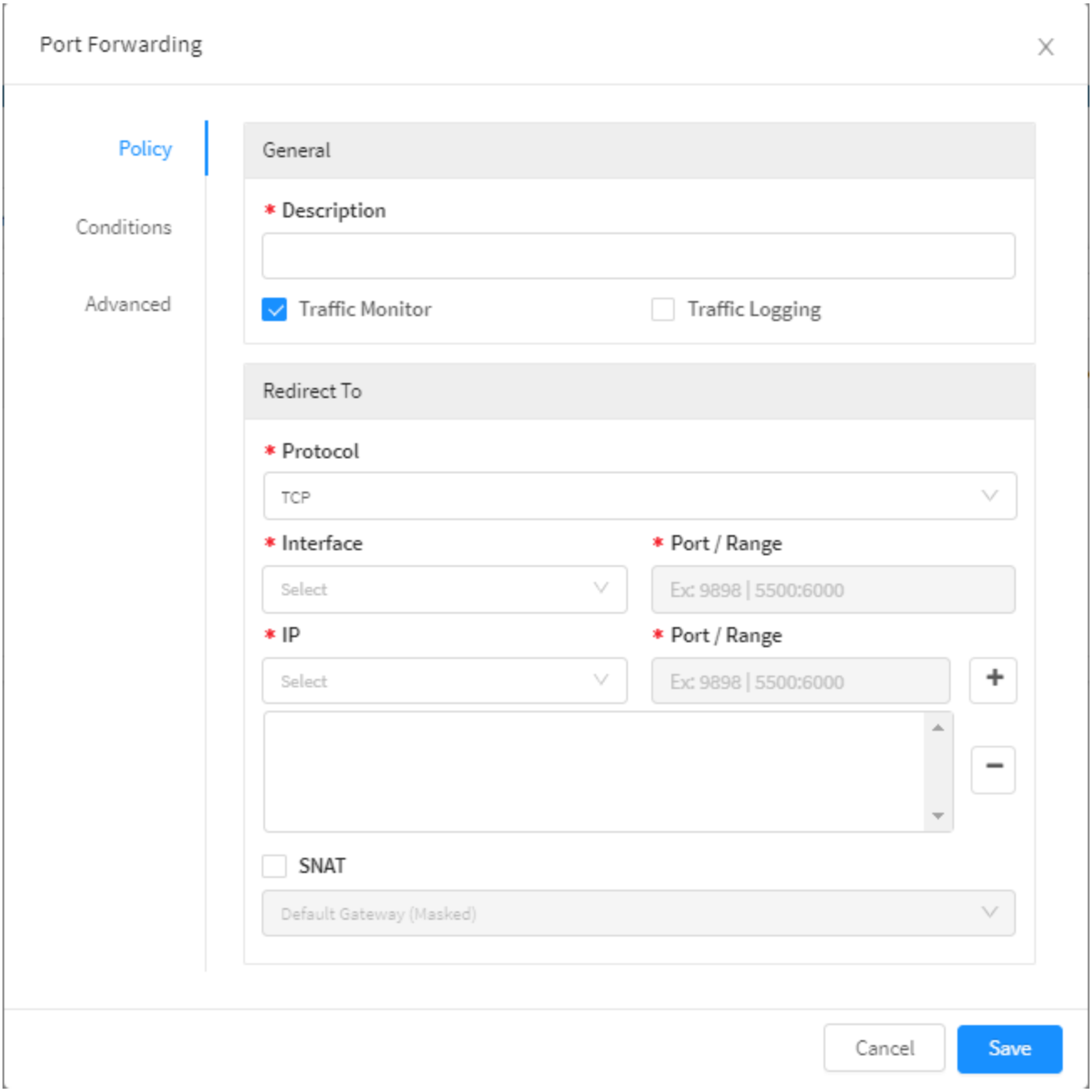
Through this window it is possible to create a Port Forwarding and configure the permissions of masking and redirection of traffic between the buses.

To create a Port Forwarding, click on the button located at the top right:



Port Forwarding – Create Button

By clicking on this button the window below is displayed:



Port Forwarding - Creating a new Port Forwarding

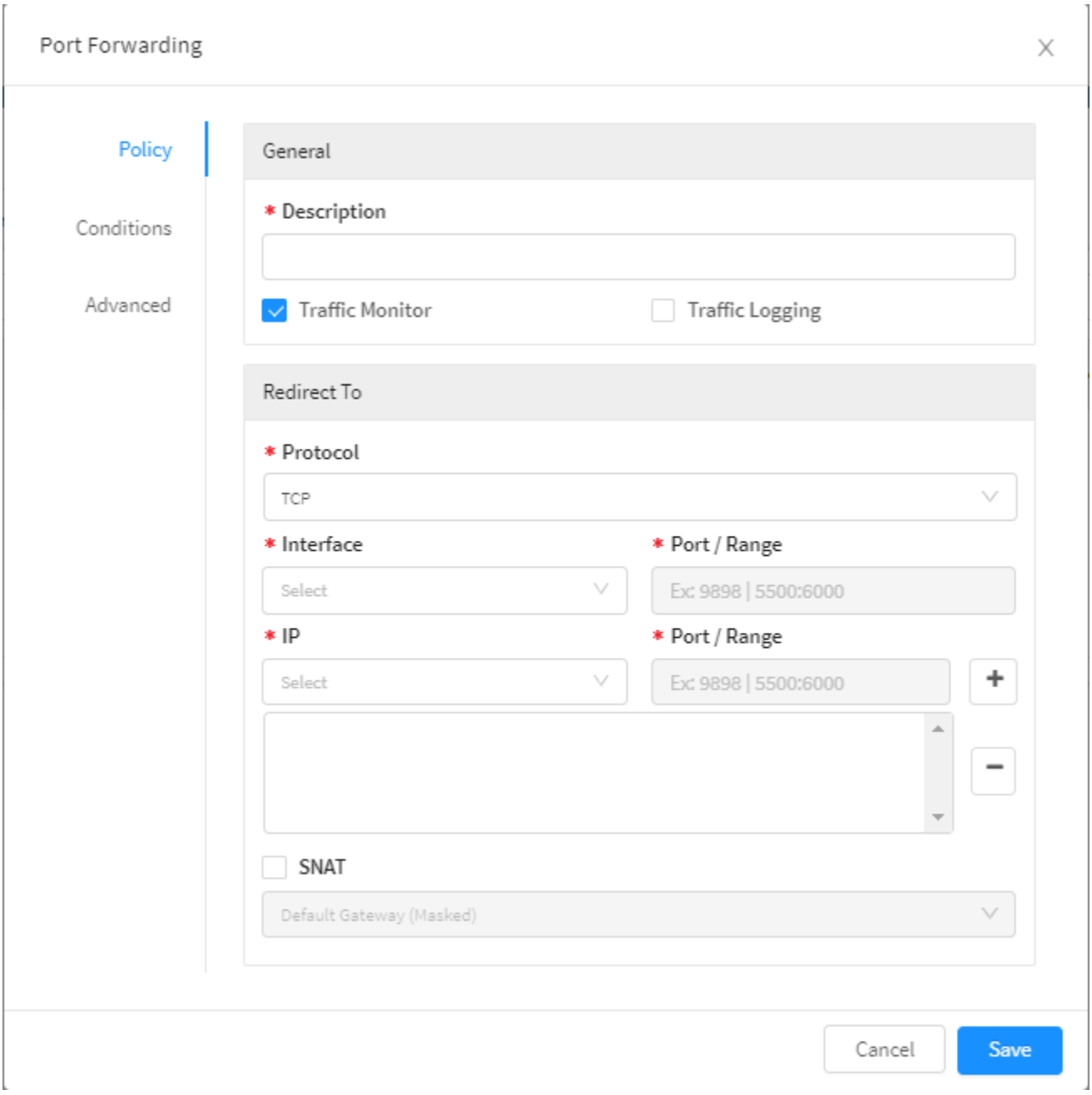
The menu consists of several sessions and panels:

- *Policy*;
  - *General*;
  - *Redirect to*.
- *Conditions*;
  - *Authentication*;
  - *Sources*;
  - *Schedule*.
- *Advanced*;
  - *DoS Protection*.

Below we will analyze each of these sessions in detail.

Policy

In "Policy" we configure all options related to the policy of how Port Forwarding will act:



Port Forwarding - Policy

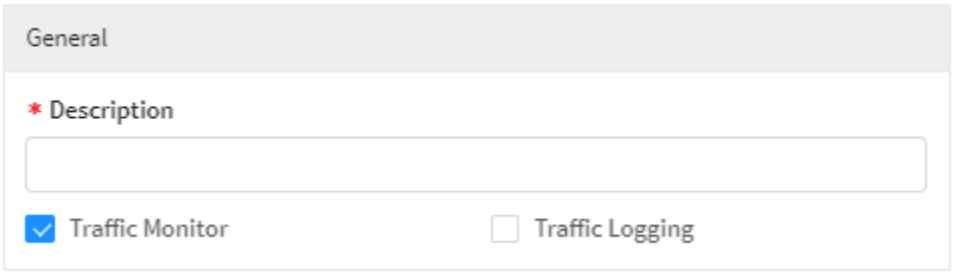
This tab is composed of the panels:

- *General;*
- *Redirect to.*

We will start by detailing the General panel.

General

This panel contains only the field for adding the policy description.



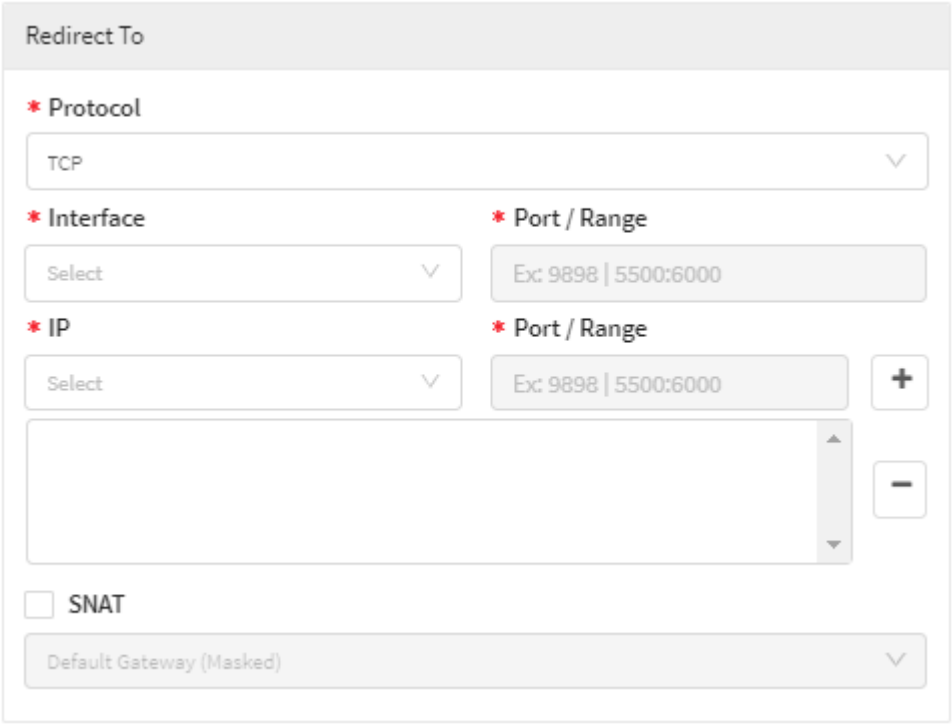
Policy - General

- **Description:** Defines a description for identification;
- **Traffic Monitor:** With the Traffic Monitor checked [ ], data on the information traffic on the sessions assgined to the *Port Forwarding* will be collected;
- **Traffic Logging:** With the Traffic Logging checked[ ], logs reffering to the information traffic on the sessions assigned to the Port Forwarding will be generated.

Next we will detail the panel Redirect to.

Redirect To

This panel contains the resources for configuring the redirection of the Port Forwarding policy



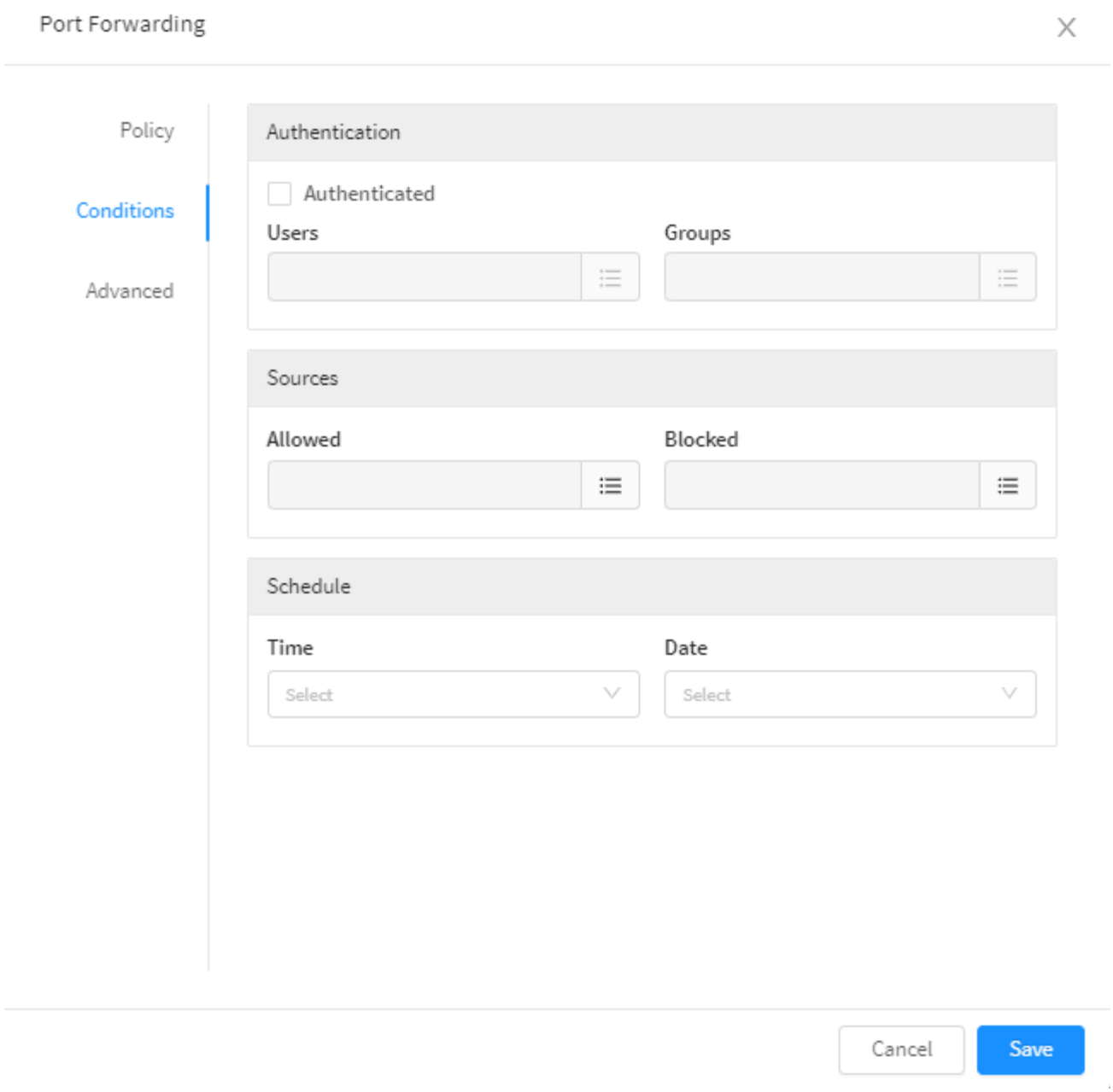
Policy - Redirect to

- **Protocol:** Defines which protocol will be used;
- ***Interface***: Determines which network interface will be used. The interfaces that appear in this menu are configured in *Network - Interfaces*;
- **Port /*Range*:** Defines the port to be used and its range. *For this field to be enabled it is necessary to add an interface in the previous field*;
- ***IP***: Determines the IP addresses that will be used in the redirection and their respective ports, note that for them to be displayed in this list, they must be of the "unique IP" type. Click the **[ ]** button to add the address to the list, if you want to remove an address, select it from the list and click **[ ]**. For more information on how to add a "unique IP" address object, see this page.
- **Port /*Range*:** Defines the port that will be used by the redirect IP and its respective range. For this field to be enabled it is necessary to add an IP in the previous field;
- **SNAT[ ]:** If the check box is enabled, it allows the selection of a gateway to perform NAT. For this, it is possible to select the default Gateway or an interface. The interfaces that appear in this menu are configured in *Network - Interfaces*;

Next we will detail the components of the "Conditions" side tab.

Conditions

In "Conditions" we configure all the conditions on how port forwarding will work:



Port Forwarding - Conditions

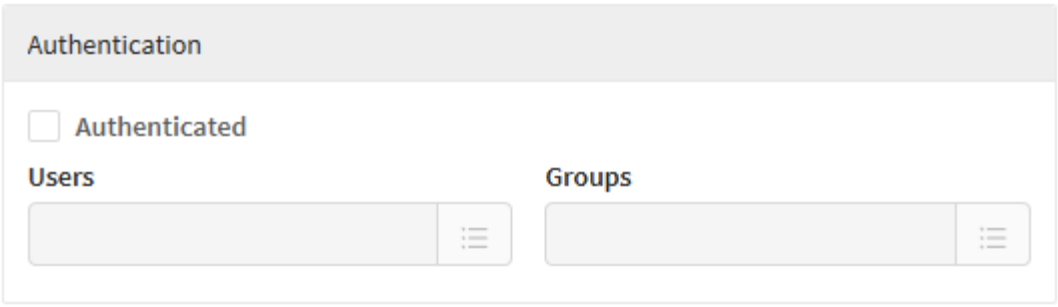
This tab is composed of the panels:

- *Authentication;*
- *Sources;*
- *Schedule.*

We'll start by detailing the Authentication panel.

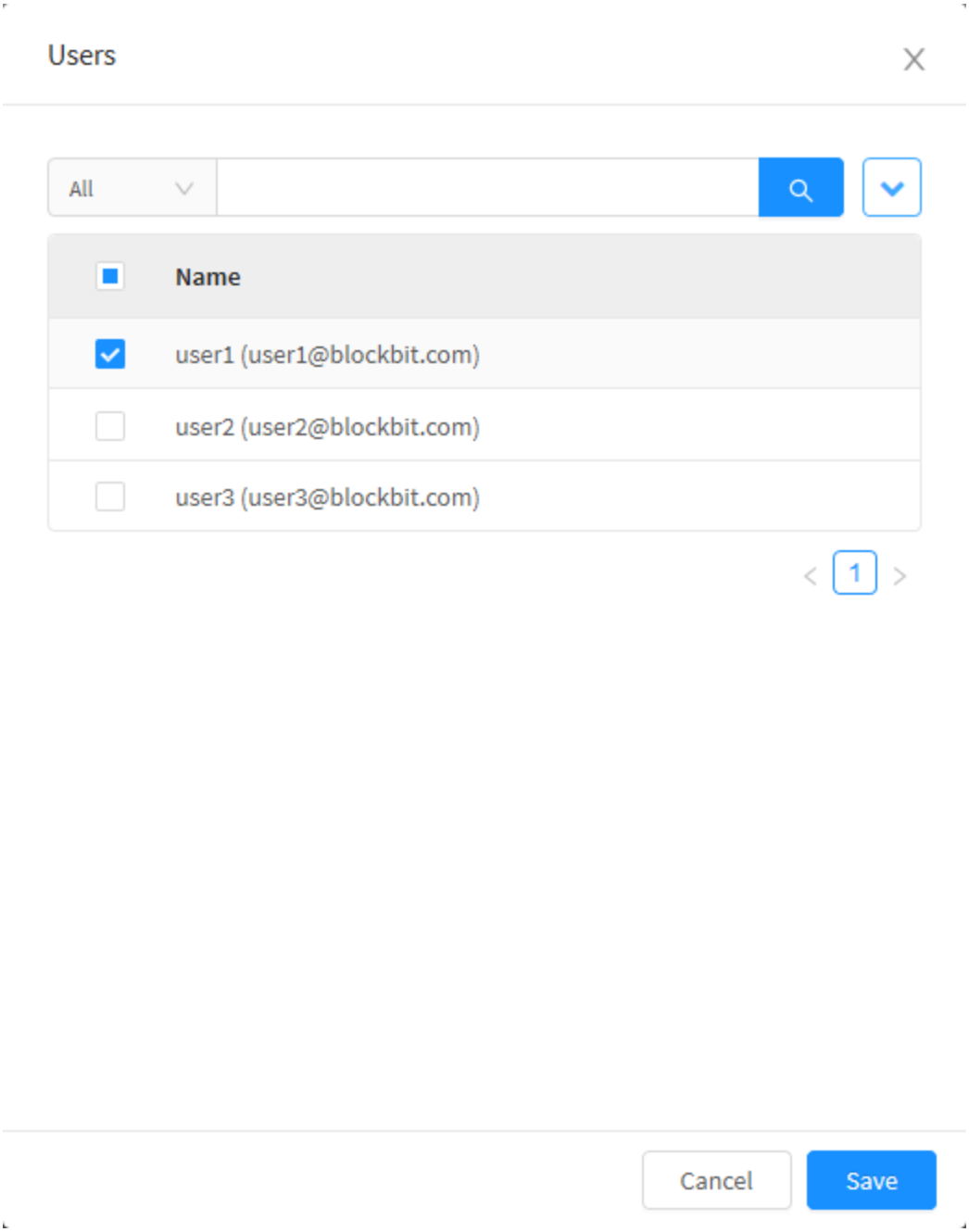
Authentication

In this panel are located the resources that allow conditioning the activation of Port Forward by authentication.



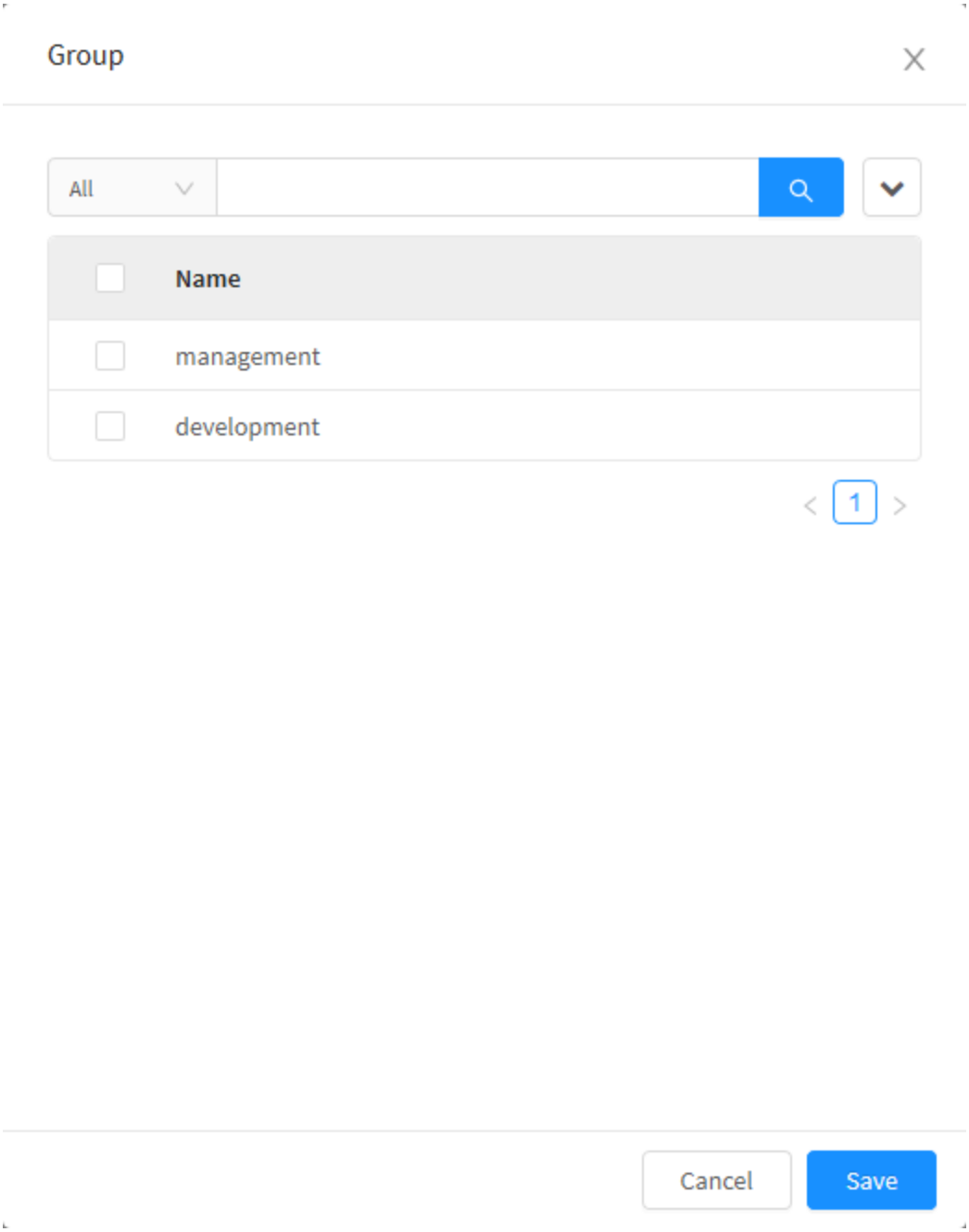
Conditions - Authentication

- ***Authenticated[ ]:*** This check box determines whether port forwarding will require authentication (if enabled) or not (if disabled). In addition, by enabling this check box, the Users and Groups fields are available for editing:
  - ***Users*:** With the **authenticated** checkbox checked, click **[ ]** to determine which users port forwarding will be applied to, as shown in the image below. When you have finished selecting, click **[Save]** otherwise, click **[Cancel]** to cancel;



Authentication - Users

- ***Groups*:** With the **authenticated** checkbox checked, click **[** **]** to determine which user groups port forwarding will be applied to, as shown in the image below. When you have finished selecting, click **[** **]** otherwise, click **[** **]** to cancel;

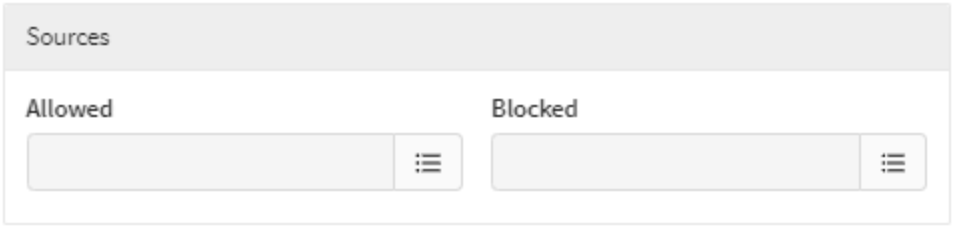


Authentication - Group

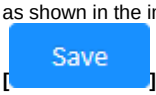
Next, we will detail the Sources panel.

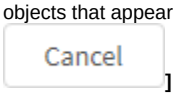
Sources

In this panel are located the resources that allow conditioning the activation of Port Forward according to the origin of the traffic.

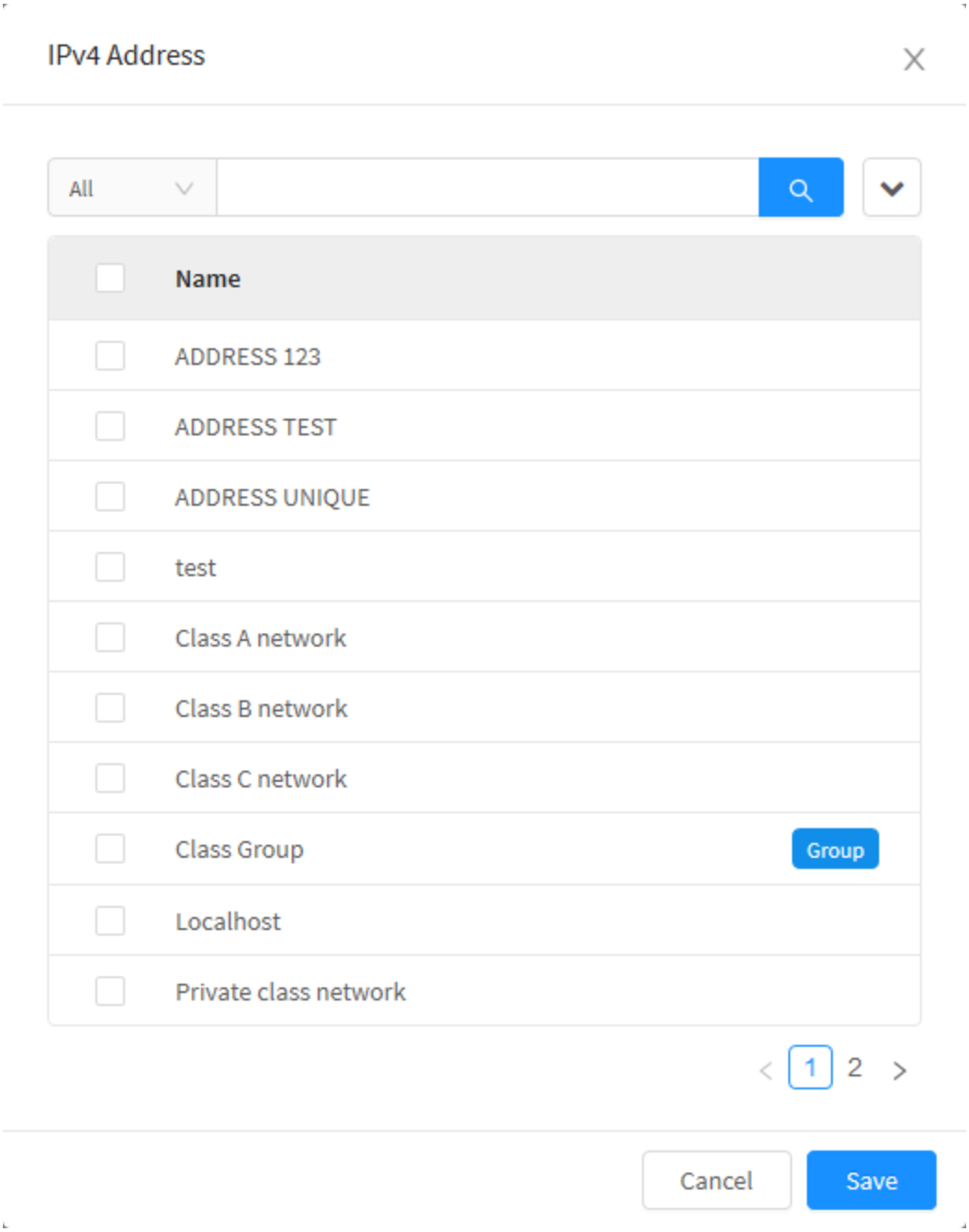


Conditions - Sources

- ***Allowed:*** Click **[**  **]** to determine which source addresses and IPs will be allowed by port forwarding, as shown in the image below. The objects that appear in the list are created in *Objects - Addresses*. When you have finished selecting, click **[** 

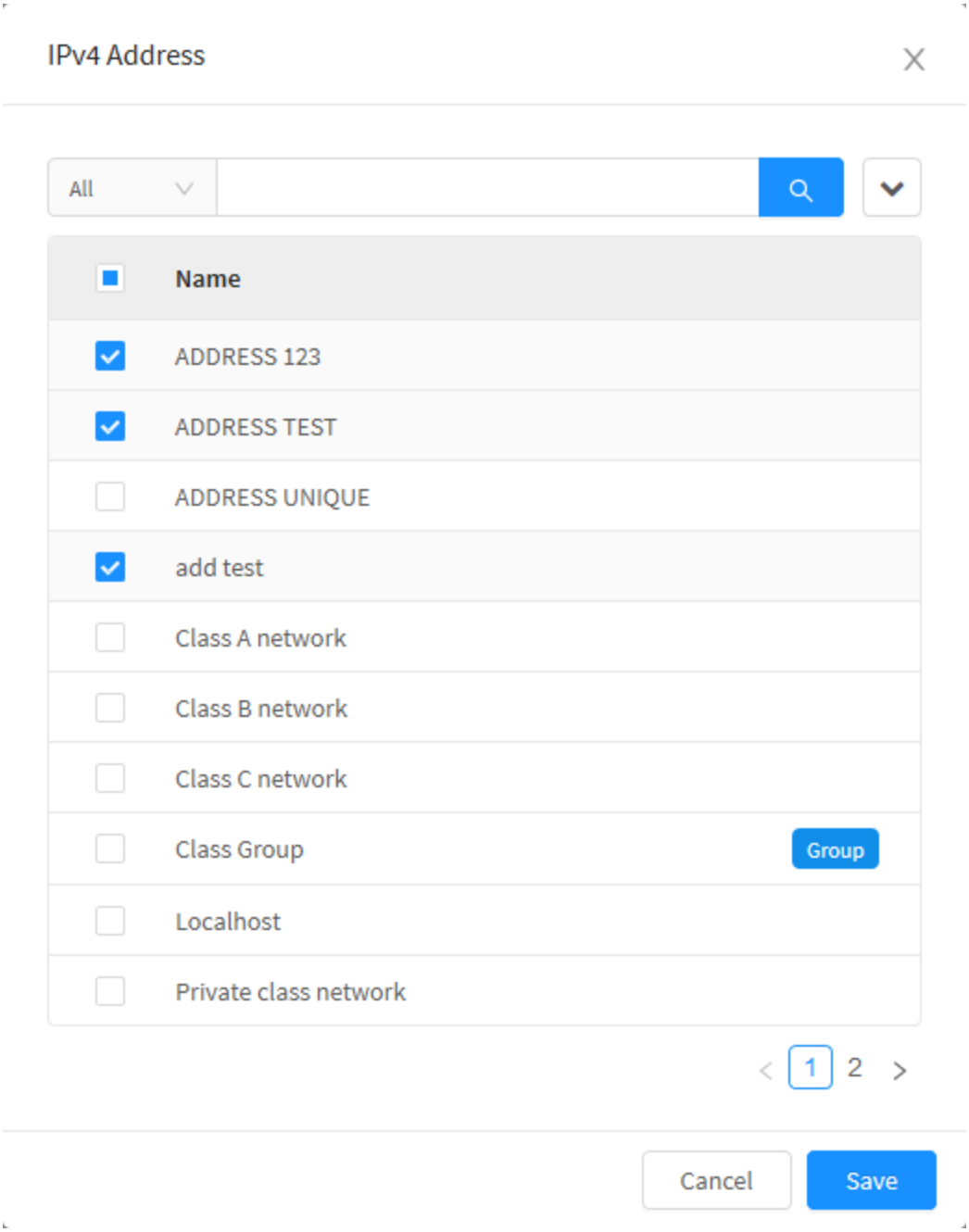
] otherwise, click **[** 

] to cancel;



Allowed sources

- ***Blocked:*** Click on **[** **]** to determine which source addresses and IPs will be blocked by port forwarding, as shown in the image below. The objects that appear in the list are created in *Objects - Addresses*. When you have finished selecting, click **[** **]** otherwise, click **[** **]** to cancel;

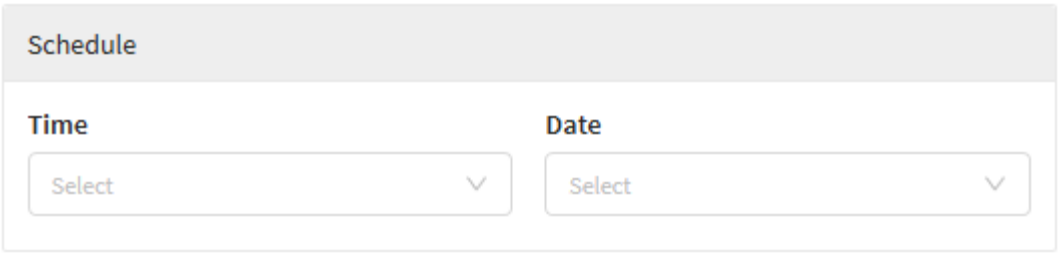


Blocked Sources

Next, we will detail the Schedule panel.

Schedule

In this panel are located the resources that allow you to control the activation of Port Forward in a specific period.



Condition - Schedule

- ***Time:*** Determines that port forwarding will be applied only according to the selected "Time" type object. The objects that appear in the list are created in *Objects - Times*;
- ***Date:*** Determines that port forwarding will be applied only according to the selected "Schedule" object. The objects that appear in the list are created in *Objects - Schedules*;

Next, we will detail the Inspection tab.

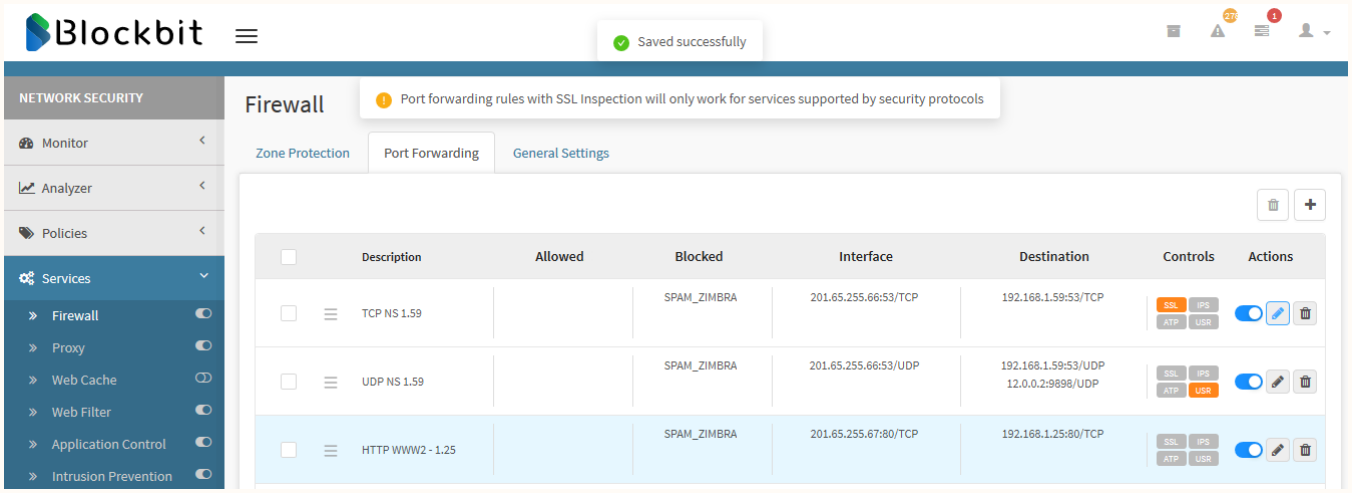
Advanced

In "Advanced" we configure which inspections will be applied in port forwarding:

Port Forwarding - Inspection

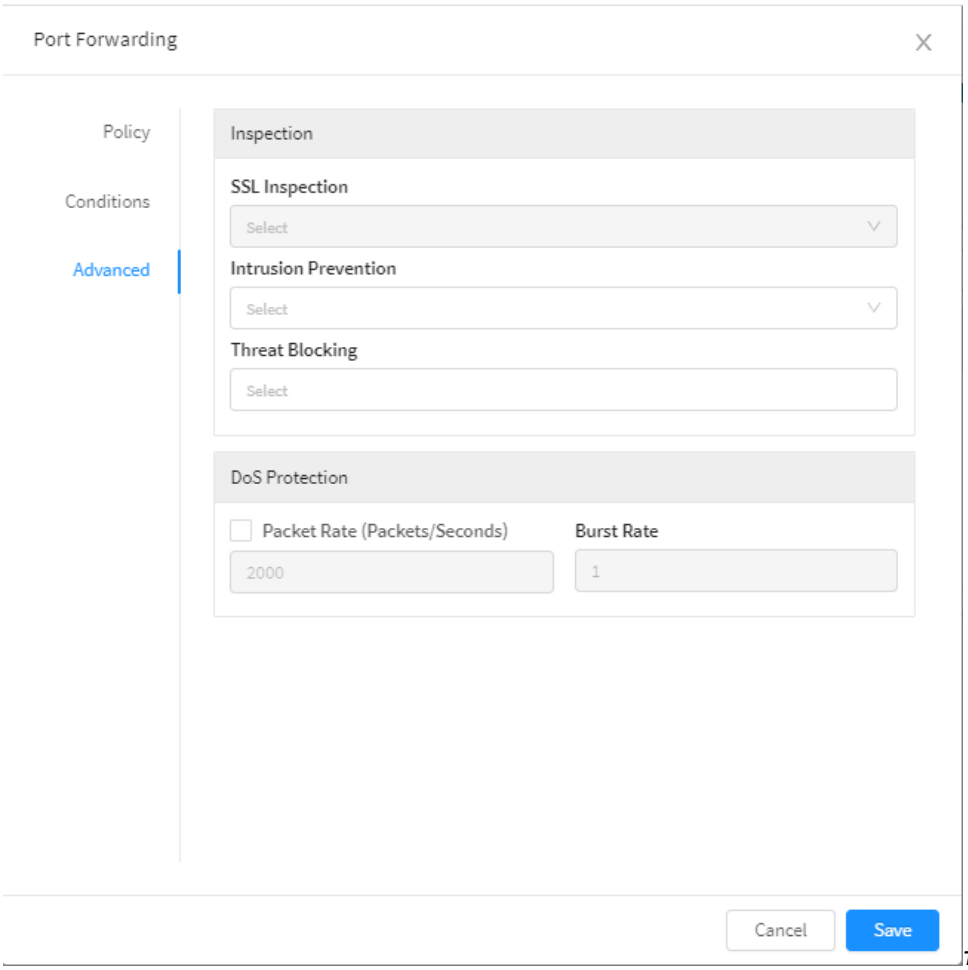
- ***SSL Inspection:*** Allows you to select a service certificate and apply SSL Inspection in Port Forwarding.
  The certificates that appear in the list are created in Settings > Certificates > Services.

WARNING: When using an SSL Inspection profile, port forwarding will only work on secure traffic, for example, when protocols are used: *HTTPS*, *POPS*, *IMAPS*, *SMTPS and other types of encryption*. Note that when creating a port forwarding in this way, the following alert message will be displayed:



Alerta - Redirection rules with SSL inspection will only work for services where the security protocol is supported

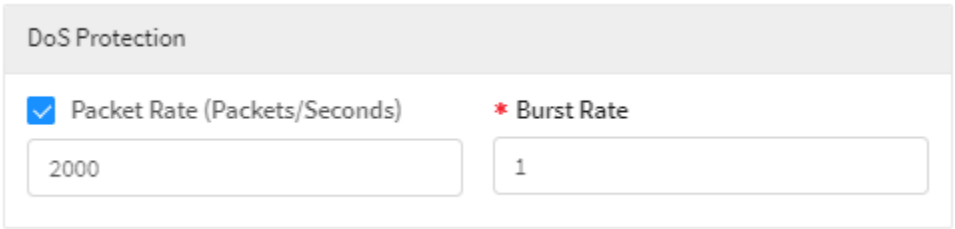
- ***Intrusion Prevention:*** Allows you to select a profile and apply Intrusion Prevention in port forwarding. *The profiles that appear in the list are created in* NGFW - Services - Intrusion Prevention;



- ***Threat Blocking:*** Enables protection against selected threats. Each option is added as a tag, if you want to remove any option click on **[** **]** or select it again in the menu . To clear this field, just click on **[** **]**. You have the options below:
  - *Abuse*;
  - *Anonymizers*;
  - *Attacks*;
  - *Malware*;
  - *Reputation*;
  - *Spam*.

DoS Protection

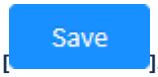
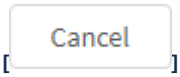
This panel contains the DoS Protection controls:



Port Forwarding - DoS Protection Settings.

- ***DoS Protection:*** With the DoS Protection box checked [ ] It's possible to limit the maximum quantity of packets per second in the *Firewall*, avoiding distributed attacks or traffic anomalies caused by possible network *malwares* in the network.
  - ***Packet Rate:*** The *Packet Rate* option sets up the *Firewall* in order to limit the connections to a maximum amount of packets per second.

- ***Burst Rate:*** The *Burst Rate* option sets up the *Firewall* initially to allow a maximum amount of packets per second without validating the packet rate, allowing the flexibilization of traffic control for occasional peaks.

To save changes, click **[**  **]**, otherwise, click **[** **]** or **[**  **]** to cancel all settings and return to the previous screen.

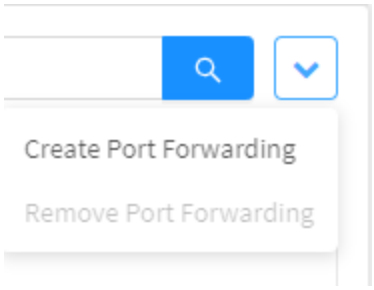
After saving, you will need to access the **command queue [**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command Queue.

To better illustrate the procedures listed above, we will look at some examples.

Port Forwarding - Create Port Forwarding

Through this window it is possible to create a Port Forwarding and configure the permissions of masking and redirecting of traffic between the buses.

To create a Port Forwarding, click on the button located at the top right:



Port Forwarding – Create Button

The window below will be displayed:

Port Forwarding

Policy

Conditions

Advanced

General

* Description

Traffic Monitor

Traffic Logging

Source

Interface

Source Protocol + Port / Range

* Protocol

TCP

* Port / Range

Ex: 9898 | 5500:6000

Redirect To

* IP

Select

* Port / Range

Ex: 9898 | 5500:6000

SNAT

Default Gateway (Masked)

Cancel

Save

The menu consists of several sessions and panels:

- *Policy;*
  - *General;*
  - *Source*
  - *Source Protocol + Port/Range*
  - *Redirect to.*
- *Conditions;*
  - *Authentication;*
  - *Sources;*
  - *Schedule.*
- *Advanced;*
  - Inspection
  - *DoS Protection.*

Below we will analyze each of these sessions in detail.

Policy

In "Policy" we configure all options related to the policy of how Port Forwarding will act:

Port Forwarding

Policy

Conditions

Advanced

General

* Description

Traffic Monitor

Traffic Logging

Source

Interface

Source Protocol + Port / Range

* Protocol

TCP

* Port / Range

Ex: 9898 | 5500:6000

Redirect To

* IP

Select

* Port / Range

Ex: 9898 | 5500:6000

SNAT

Default Gateway (Masked)

Cancel

Save

Port Forwarding - Policy

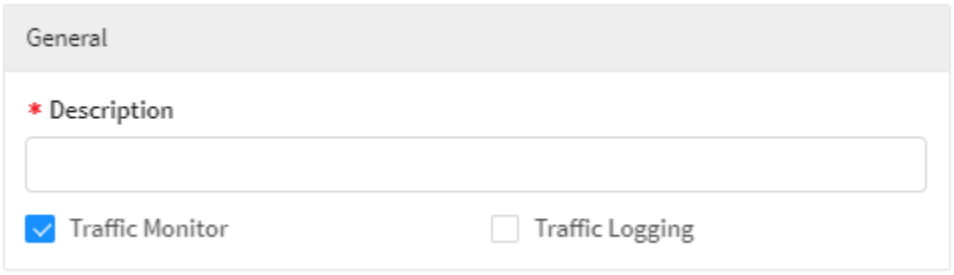
This tab is composed of the panels:

- *General;*
- *Source;*
- *Source Protocol + Port/Range*
- *Redirect to.*

We will start by detailing the General panel.

General

This panel contains only the field for adding the policy description.

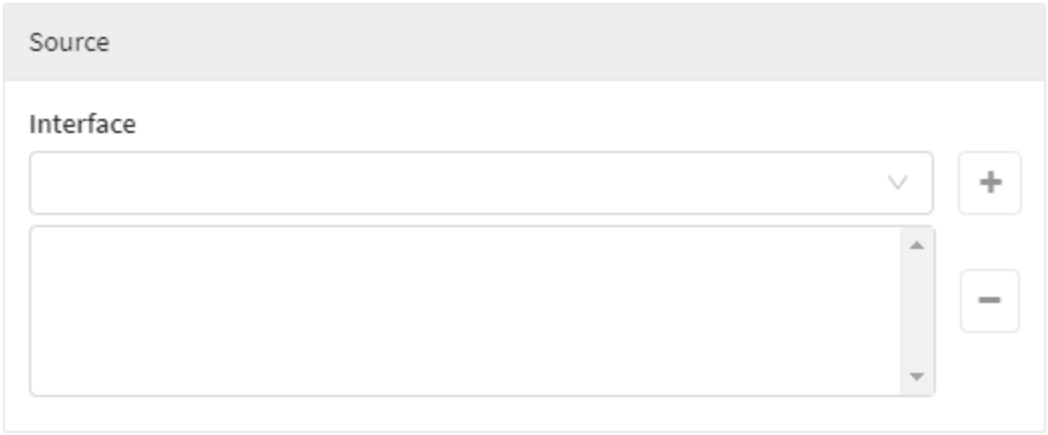


Port Forwarding - Policy - General

- **Description:** Defines a description for identification;
- **Traffic Monitor:** With the Traffic Monitor checked [ ], data on the information traffic on the sessions assgined to the *Port Forwarding* will be collected*;*
- **Traffic Logging:** With the Traffic Logging checked[ ], logs reffering to the information traffic on the sessions assigned to the Port Forwarding will be generated.

Next we will detail the panel 'Source'.

Source

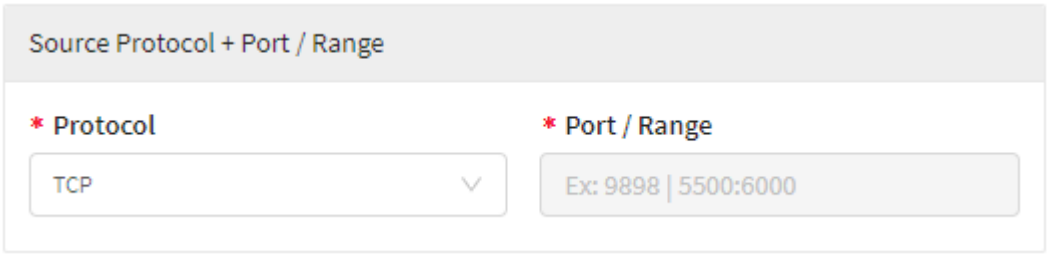


Port Forwarding - Policy - Source

- ***Interface***: Determines which network interfaces will be used. It is possible to add more than one interface. The interfaces that appear in this menu are configured in *Network Interfaces*;

Next we will detail the panel 'Source Protocol + Port/Range'.

Source Protocol + Port/Range



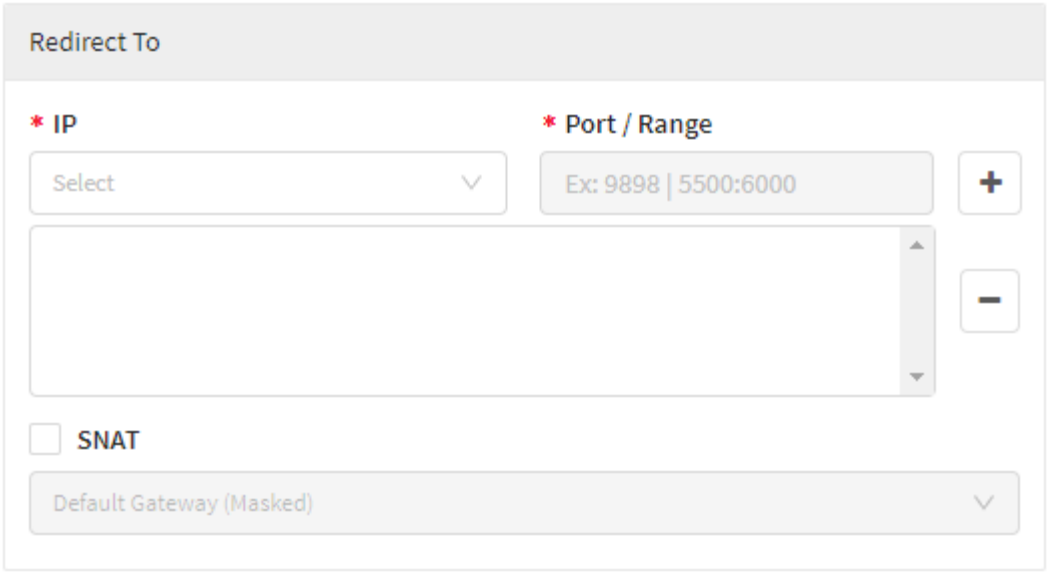
Port Forwarding - Policy - Source Protocol + Port/Range

- **Protocol:** Defines which protocol will be used;
- **Port /*Range*:** Defines the port to be used and its range*. For this field to be enabled it is necessary to add an interface in the previous field*;

Next we will detail the panel 'Redirect to'.

Redirect To

This panel contains the resources for configuring the redirection of the Port Forwarding policy



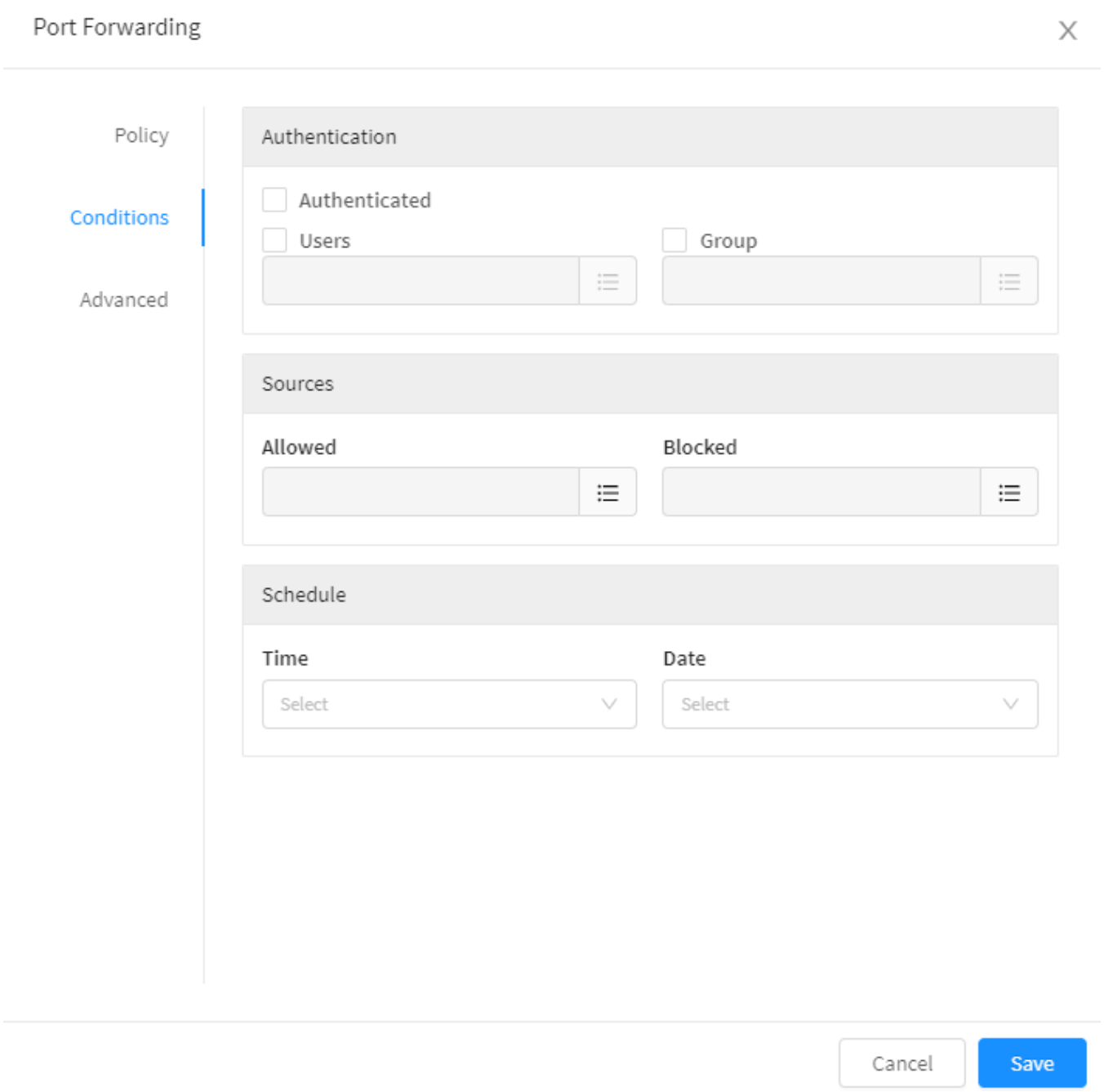
Port Forwarding - Policy - Redirect to

- ***IP***: Determines the IP addresses that will be used in the redirection and their respective ports, note that for them to be displayed in this list, they must be of the "unique IP" type. Click the **[ ]** button to add the address to the list, if you want to remove an address, select it from the list and click **[ ]**. For more information on how to add a "unique IP" address object, see this page.
- **Port /*Range*:** Defines the port that will be used by the redirect IP and its respective range. For this field to be enabled it is necessary to add an IP in the previous field;
- **SNAT[ ]:** If the check box is enabled, it allows the selection of a gateway to perform NAT. For this, it is possible to select the default Gateway or an interface. The interfaces that appear in this menu are configured in *Network - Interfaces*;

Next we will detail the components of the "Conditions" side tab.

Conditions

In "Conditions" we configure all the conditions on how port forwarding will work:



Port Forwarding - Conditions

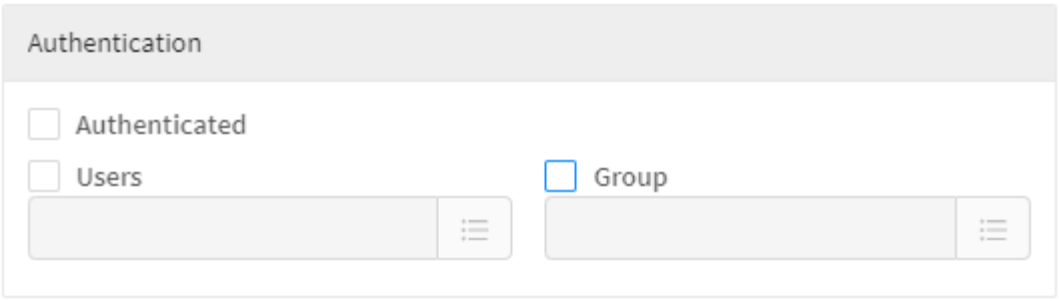
This tab is composed of the panels:

- *Authentication;*
- *Sources;*
- *Schedule.*

We'll start by detailing the Authentication panel.

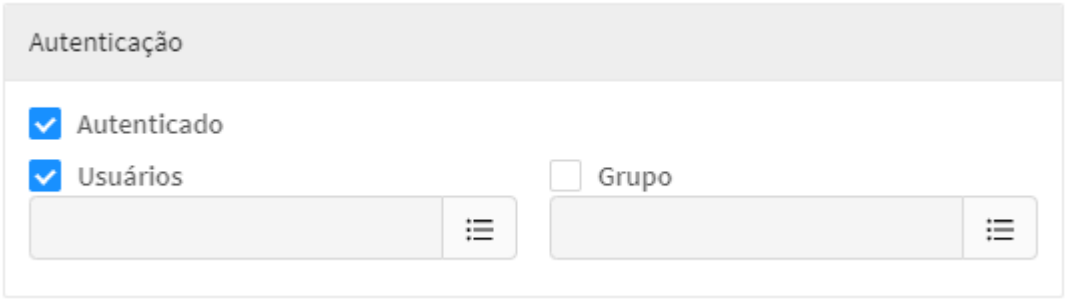
Authentication

In this panel are located the resources that allow conditioning the activation of Port Forward by authentication.

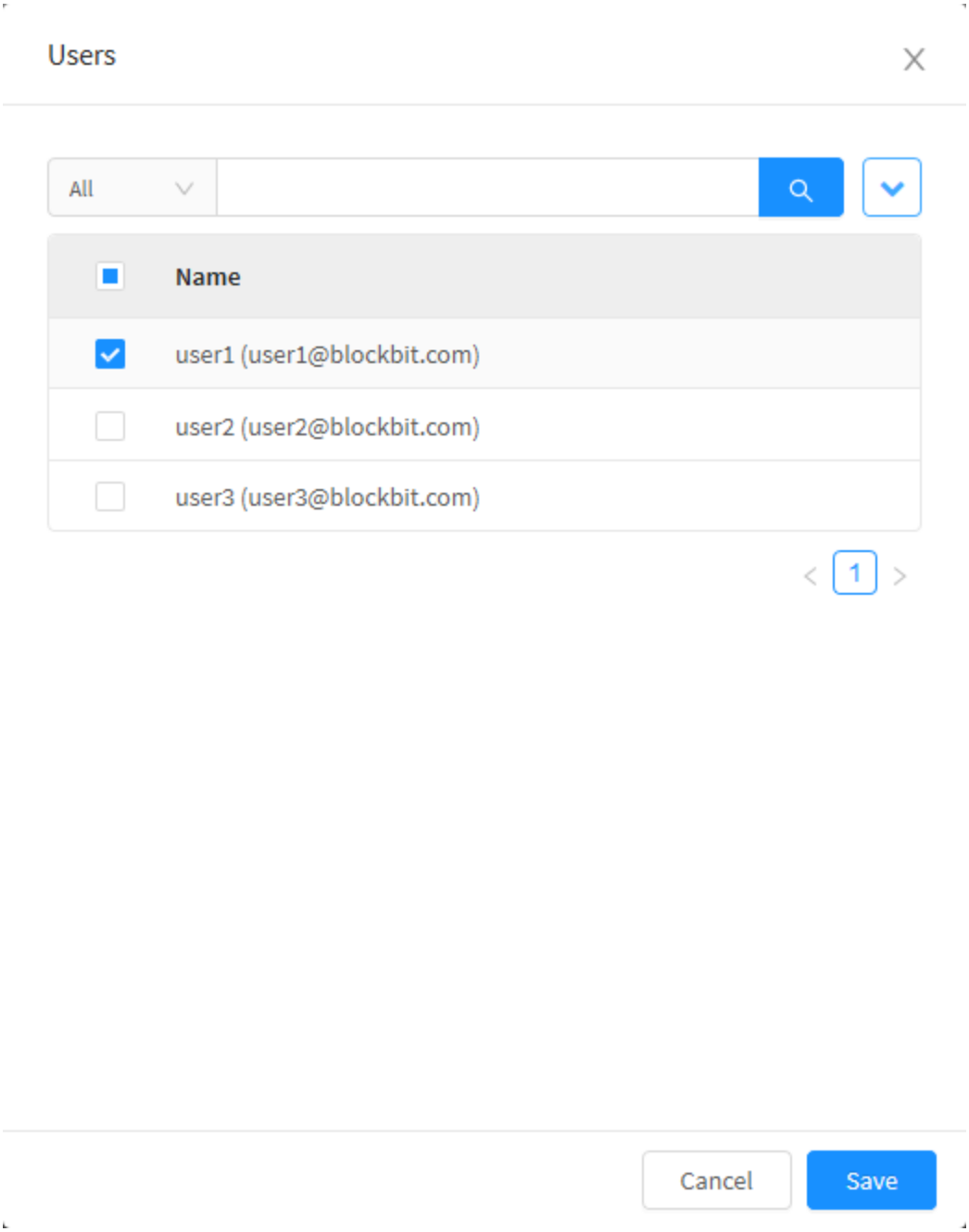


Conditions - Authentication

- ***Authenticated[ ]:*** This check box determines whether port forwarding will require authentication (if enabled) or not (if disabled). In addition, by enabling this check box, the Users and Groups fields are available for editing:
    - ***Users*:** With the **authenticated** checkbox checked, click **[ ]** to determine which users port forwarding will be applied to, as shown in the image below. When you have finished selecting, click **[ ]** otherwise, click **[ ]** to cancel;

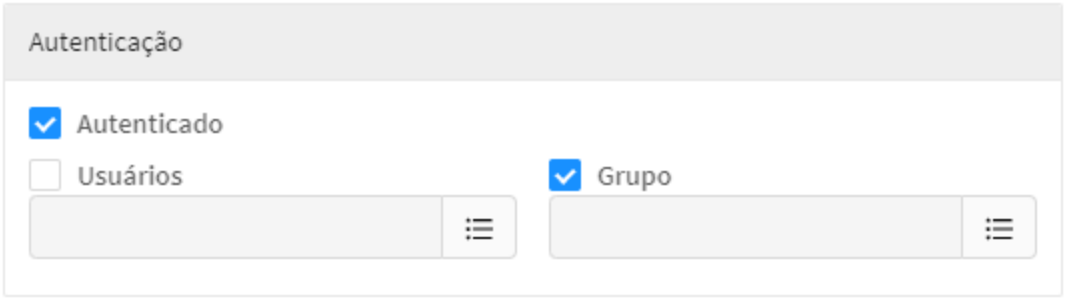


User option selection

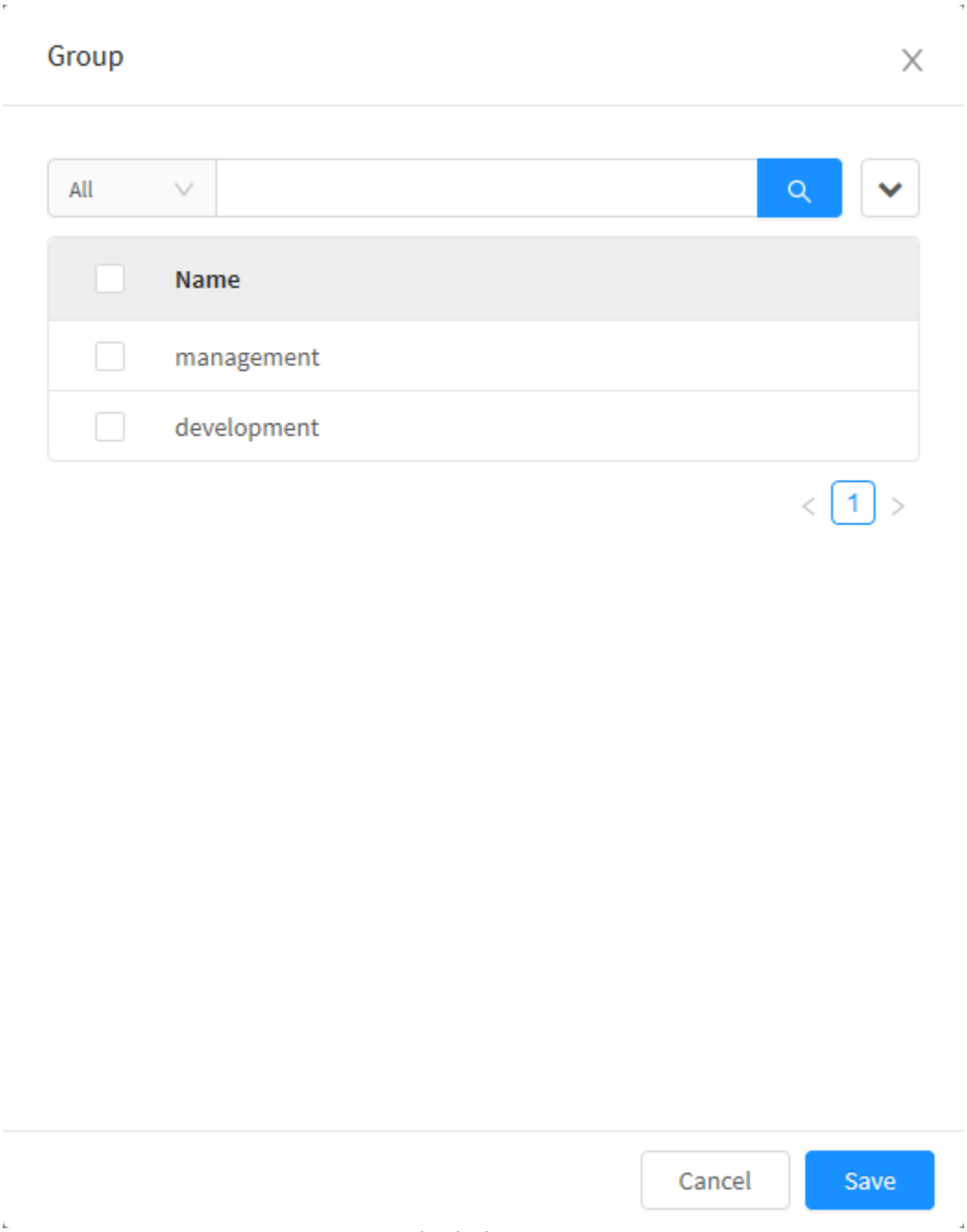


Authentication - Users

- ***Groups*:** With the **authenticated** checkbox checked, click **[** **]** to determine which user groups port forwarding will be applied to, as shown in the image below. When you have finished selecting, click **[** **]** otherwise, click **[** **]** to cancel;



Group option selection

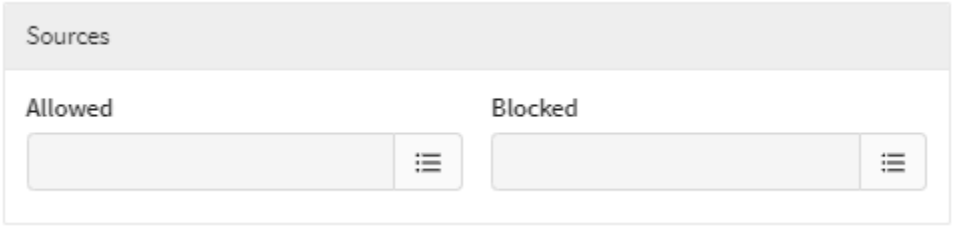


Authentication - Group

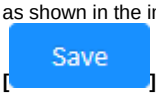
Next, we will detail the Sources panel.

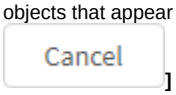
Sources

In this panel are located the resources that allow conditioning the activation of Port Forward according to the origin of the traffic.

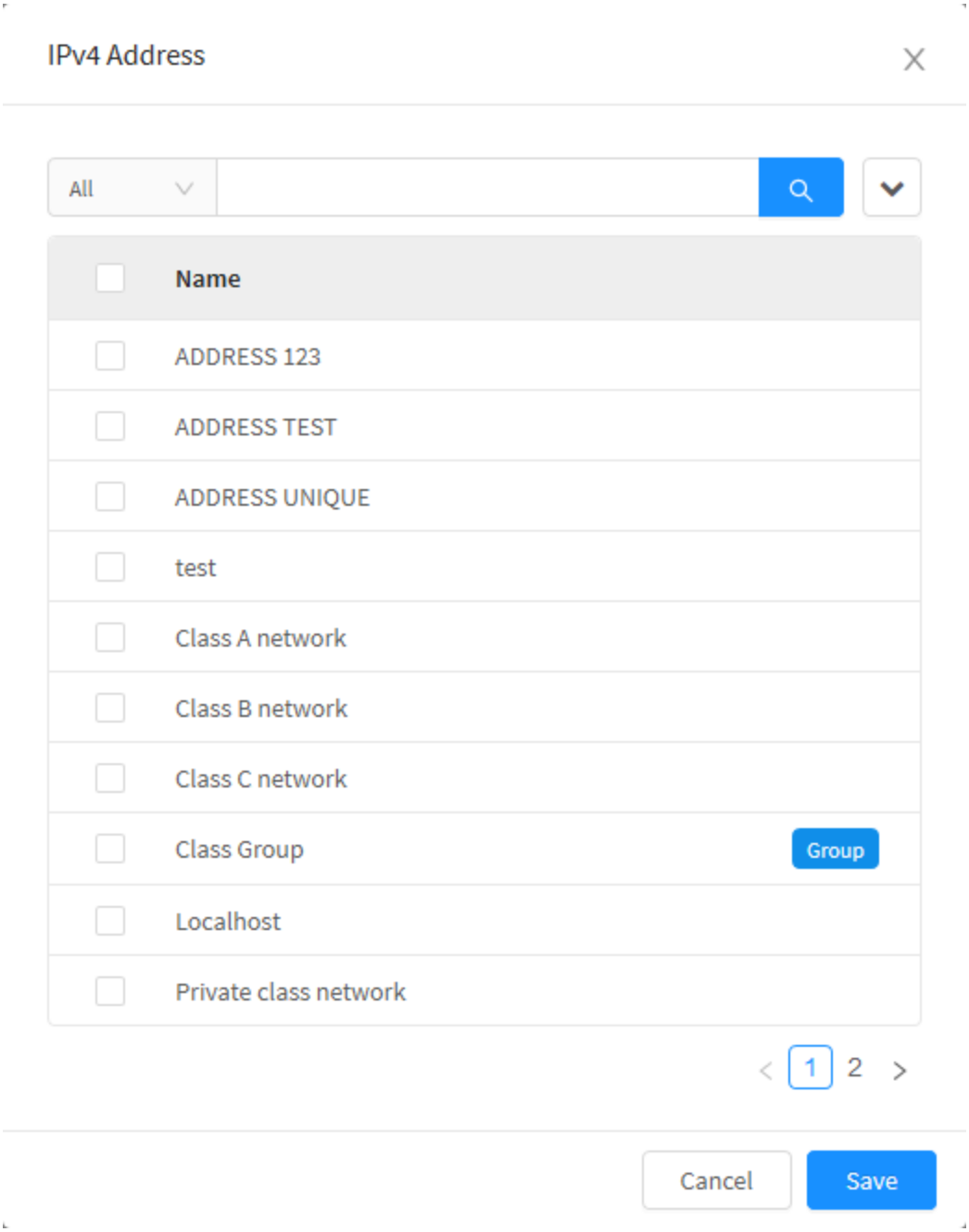


Conditions - Sources

- ***Allowed:*** Click **[**  **]** to determine which source addresses and IPs will be allowed by port forwarding, as shown in the image below. The objects that appear in the list are created in *Objects - Addresses*. When you have finished selecting, click **[** 

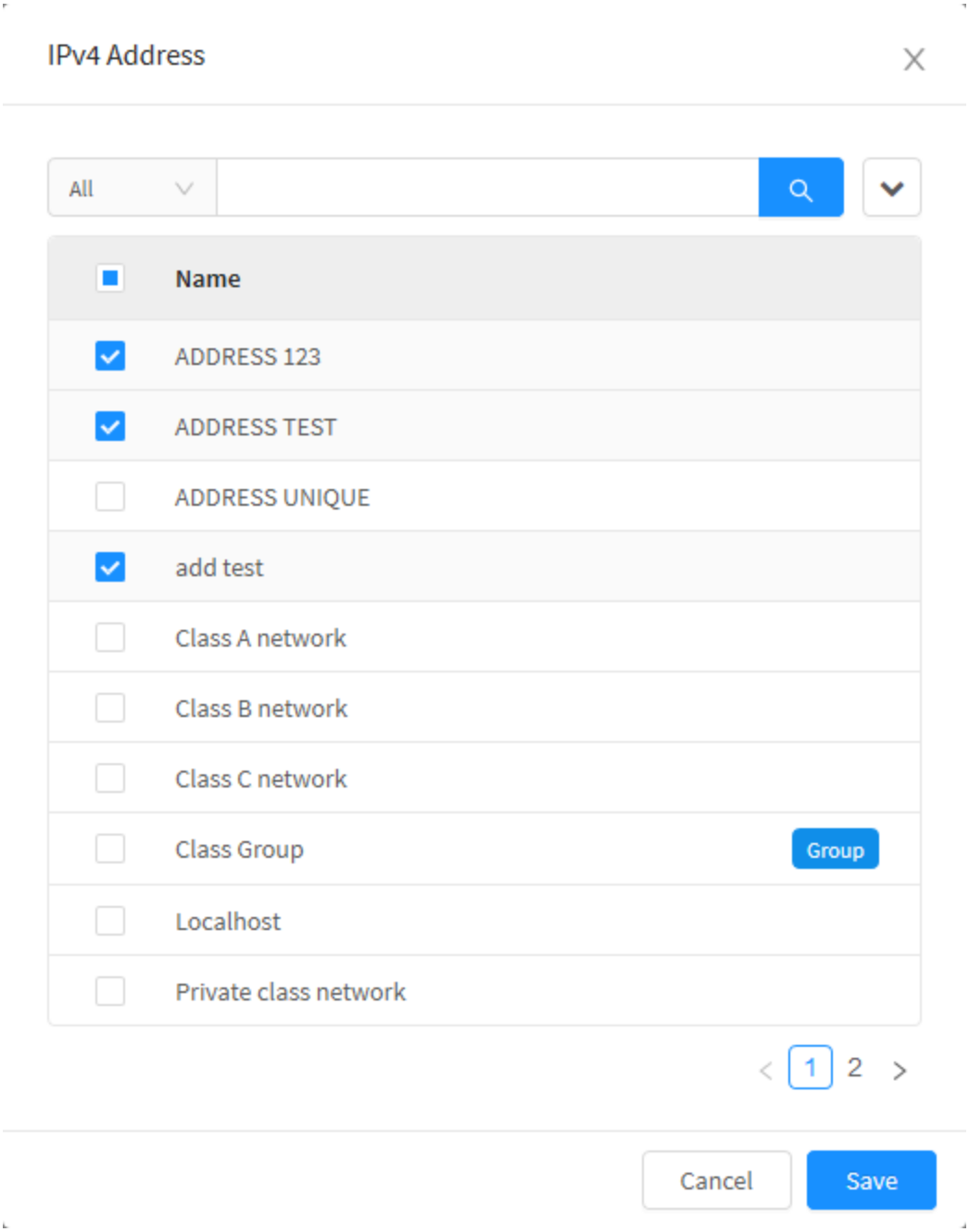
] otherwise, click **[** 

] to cancel;



Allowed sources

- ***Blocked:*** Click on **[** **]** to determine which source addresses and IPs will be blocked by port forwarding, as shown in the image below. The objects that appear in the list are created in *Objects - Addresses*. When you have finished selecting, click **[** **]** otherwise, click **[** **]** to cancel;

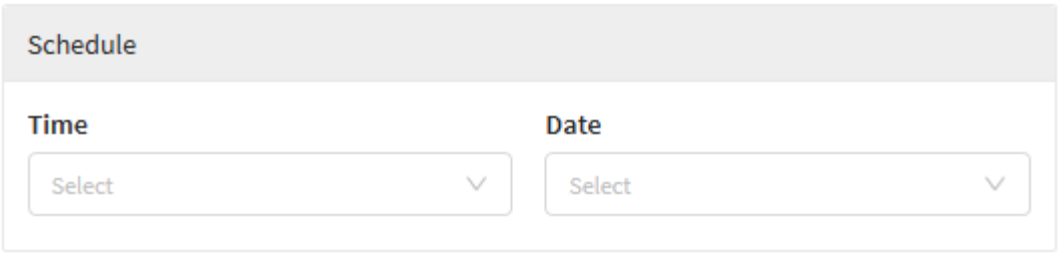


Sources - Blockeds

Next, we will detail the Schedule panel.

Schedule

In this panel are located the resources that allow you to control the activation of Port Forward in a specific period.



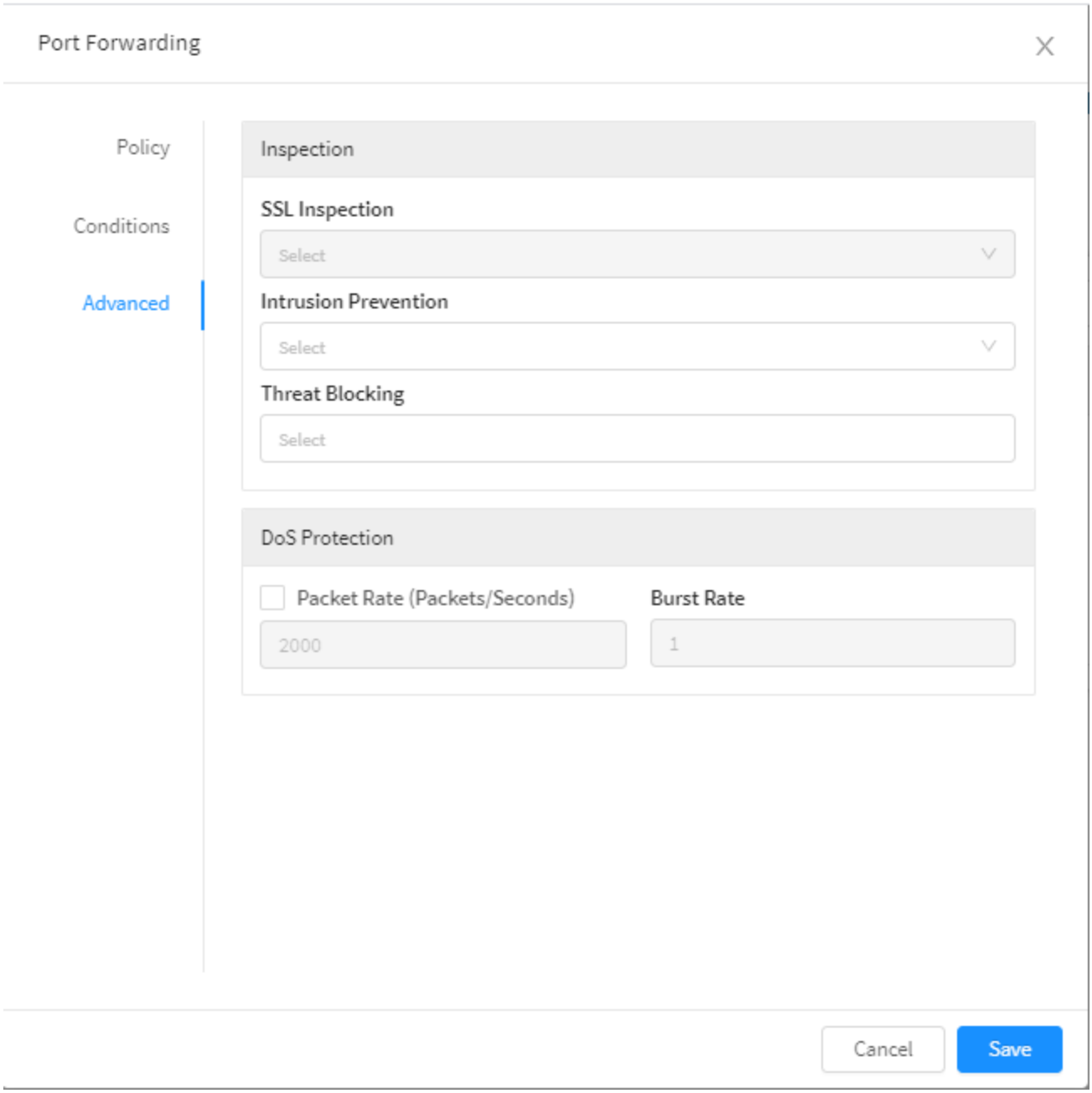
Condition - Schedule

- ***Time:*** Determines that port forwarding will be applied only according to the selected "Time" type object. The objects that appear in the list are created in *Objects - Times*;
- ***Date:*** Determines that port forwarding will be applied only according to the selected "Schedule" object. The objects that appear in the list are created in *Objects - Schedules*;

Next, we will detail the Inspection tab.

Advanced

In "Advanced" we configure which inspections will be applied in port forwarding:



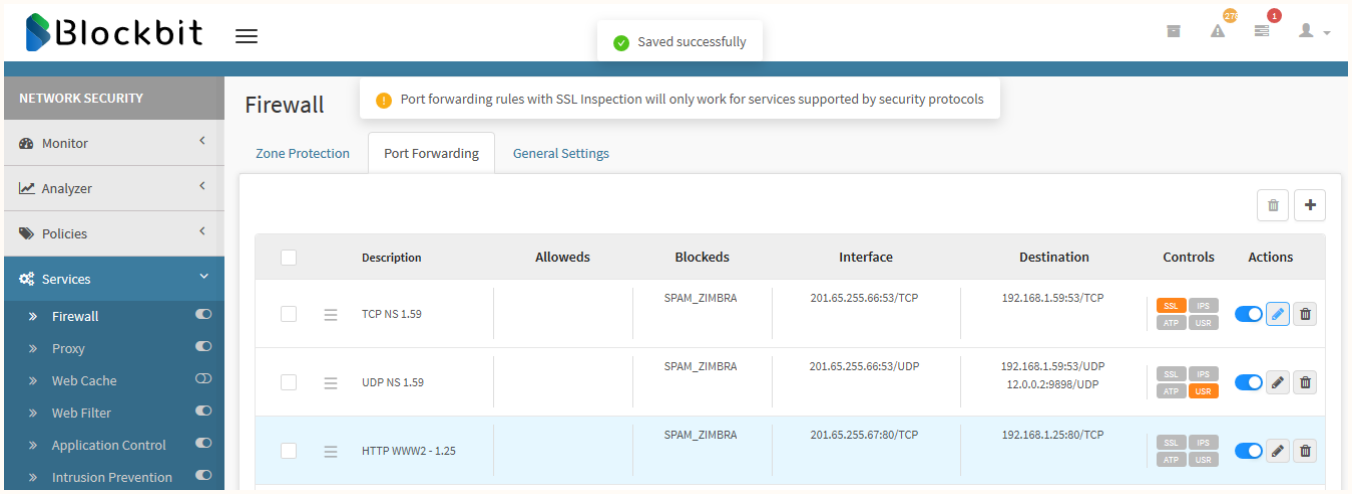
Port Forwarding - Inspection

SSL Inspection

- ***SSL Inspection:*** Allows you to select a profile and apply SSL Inspection in Port Forwarding. *The profiles that appear in the list are created in* SSL Inspection - SSL Profile;

Advanced - SSL Inspection

WARNING: When using an SSL Inspection profile, port forwarding will only work on secure traffic, for example, when protocols are used: *HTTPS*, *POPS*, *IMAPS*, *SMTPS and other types of encryption*. Note that when creating a port forwarding in this way, the following alert message will be displayed:

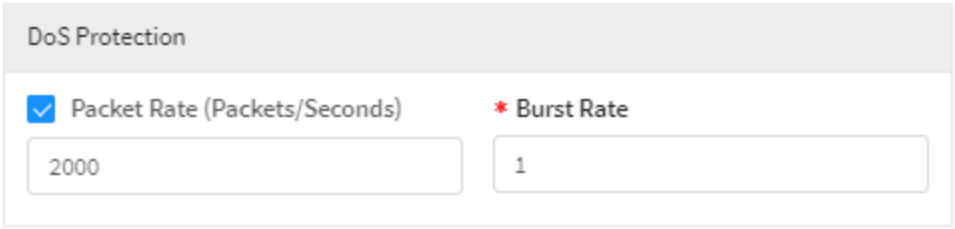


Alerta - Redirection rules with SSL inspection will only work for services where the security protocol is supported

- ***Intrusion Prevention:*** Allows you to select a profile and apply Intrusion Prevention in port forwarding. *The profiles that appear in the list are created in* NGFW - Services - Intrusion Prevention;
- ***Threat Blocking:*** Enables protection against selected threats. Each option is added as a tag, if you want to remove any option click on **[** **]** or select it again in the menu . To clear this field, just click on **[** **]**. You have the options below:
  - *Abuse*;
  - *Anonymizers*;
  - *Attacks*;
  - *Malware*;
  - *Reputation*;
  - *Spam*.

DoS Protection

This panel contains the DoS Protection controls:



Port Forwarding - DoS Protection Settings.

- ***DoS Protection:*** With the DoS Protection box checked [ ] It's possible to limit the maximum quantity of packets per second in the *Firewall*, avoiding distributed attacks or traffic anomalies caused by possible network *malwares* in the network.
  - ***Packet Rate:*** The *Packet Rate* option sets up the *Firewall* in order to limit the connections to a maximum amount of packets per second.
  - ***Burst Rate:*** The *Burst Rate* option sets up the *Firewall* initially to allow a maximum amount of packets per second without validating the packet rate, allowing the flexibilization of traffic control for occasional peaks.

To save changes, click **[** Save **]**, otherwise, click **[ ]** or **[** Cancel **]** to cancel all settings and return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command Queue.

To better illustrate the procedures listed above, we will look at some examples.

Port Forwarding - Examples

Below let's exemplify how to create Port Forwarding policies.

 This feature configures the “Forwarding” policies with allowed traffic, based on the Source/Destination IP addresses and Ports defined in the respective DNAT policy.

 Some details will not be considered in this example, if you want more information, see this page.

Example I - Port Forwarding 1:1

When accessing the configuration form, we will fill in the fields according to the specifications defined in the example policy.

- **Description**: Policy identification name;
- **Source**: Desired input interface;
- **Source Protocol + Port/Range**: Desired source protocol and port
- **Redirect to**: Desired IP address and port;

Port Forwarding

Policy

Conditions

Advanced

General

* Description

1:1

Traffic Monitor

Traffic Logging

Source

Interface

Select

eth0 - 172.31.150.44

Source Protocol + Port / Range

* Protocol

TCP

* Port / Range

21

Redirect To

IP

Select

Port / Range

Ex: 9898 | 5500:6000

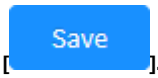
10.40.150.100 - 443

SNAT

Default Gateway (Masked)

Cancel

Save

After filling in the fields click on **[**  **].**

After saving the policy, it will be necessary to access the **command queue [**  **]** and appply the changes done. For more information about the command queue access: UTM - Command Queue.

After completing these steps the policy will have been successfully configured.

Example II - Port Forwarding N:1

When accessing the configuration form, we will fill in the fields according to the specifications defined in the example policy.

- **Description**: Policy identification name;
- **Source**: Desired input interface;
- **Source Protocol + Port/Range**: Desired source protocol and port
- **Redirect to**: Desired IP address and port;

Port Forwarding

Policy

Conditions

Advanced

General

* Description

N:1

Traffic Monitor

Traffic Logging

Source

Interface

Select

eth0 - 172.31.150.44
eth1 - 10.40.150.44

Source Protocol + Port / Range

* Protocol

TCP

* Port / Range

21

Redirect To

IP

Select

Port / Range

Ex: 9898 | 5500:6000

10.40.150.100 - 443

SNAT

Default Gateway (Masked)

Cancel

Save

Port Forwarding - Policy 2

After filling in the fields click on **[** Save **].**

After saving the policy, it will be necessary to access the **command queue [**  **]** and appply the changes done. For more information about the command queue access: UTM - Command Queue.

After completing these steps the policy will have been successfully configured, and, thus, it will be possible to redirect traffic from port X, on different Blockbit's inputs/interfaces, to N hosts of the internal network.

Example III: Port Forwarding N:N

When accessing the configuration form, we will fill in the fields according to the specifications defined in the example policy.

- **Description**: Policy identification name;
- **Source**: Desired input interface;
- **Source Protocol + Port/Range**: Desired source protocol and port
- **Redirect to**: Desired IP address and port;

Port Forwarding

Policy

Conditions

Advanced

General

* Description

N:N

Traffic Monitor

Traffic Logging

Source

Interface

Select

eth0 - 172.31.150.44
eth1 - 10.40.150.44

Source Protocol + Port / Range

* Protocol

TCP

* Port / Range

21

Redirect To

IP

Select

Port / Range

Ex: 9898 | 5500:6000

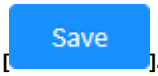
10.40.150.100 - 443
10.40.150.42 - 80

SNAT

Default Gateway (Masked)

Cancel

Save

After filling in the fields click on **[**  **].**

When 2 or more destinations are configured, the rule created will obey the "first match wins" pattern, that is, the first IP configured as a destination will be the main one, and if it is unavailable, the redirection will be done by the other configured IPs.

After saving the policy, it will be necessary to access the **command queue [**  **]** and appply the changes done. For more information about the command queue access: UTM - Command Queue.

After completing these steps the policy will have been successfully configured, and, thus, it will be possible to redirect traffic from port X, on different Blockbit's inputs/interfaces, to N hosts of the internal network.

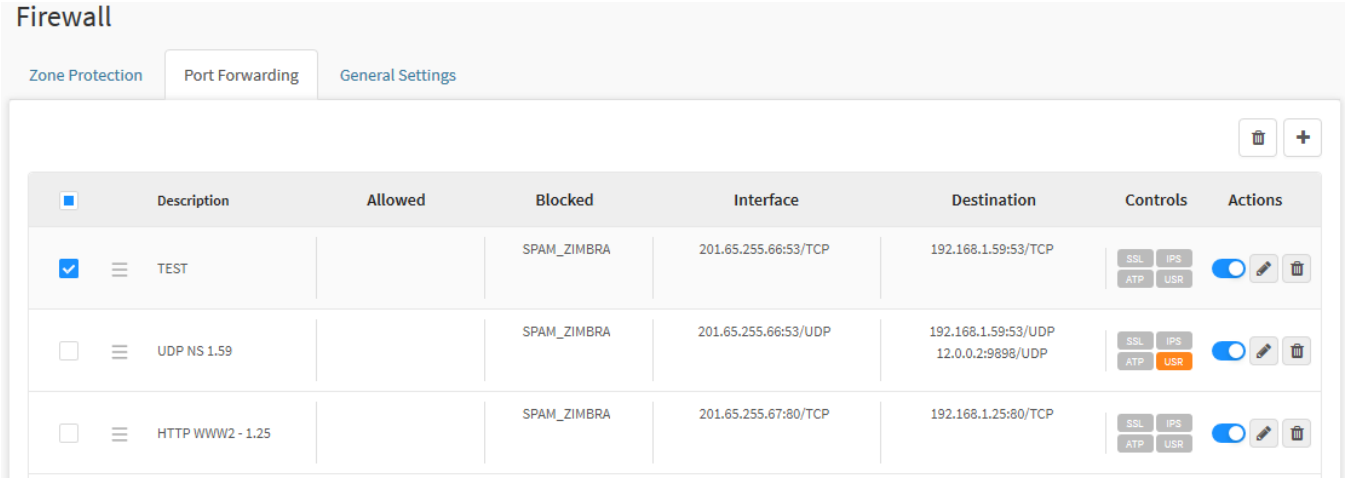
After completing the configuration and saving the policy, do not forget to enable the new policy, to do so, click **enable [**  **]**.

Exemplification concluded, next we will detail the Removal Button.

UTM - Port Forwarding - Removal button

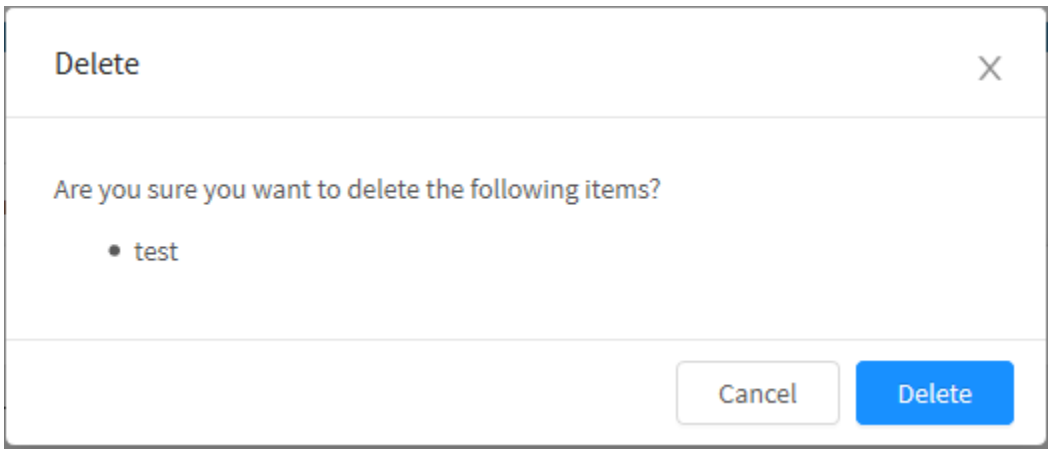
Through the removal button it is possible to delete several items at the same time. Follow the steps below:

1. Select the items you want to delete by clicking the **checkbox[ ]**;

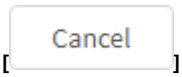
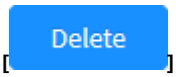


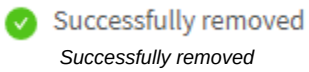
Port Forwarding - Selection for deletion

2. Click the **remove button [ ]** and a screen will ask if you want to delete the selected item:



Port Forwarding - Remove itens

If you want to cancel click on the **[**  **]** button. To complete the deletion click on the **[**  **]** button.



Successfully removed

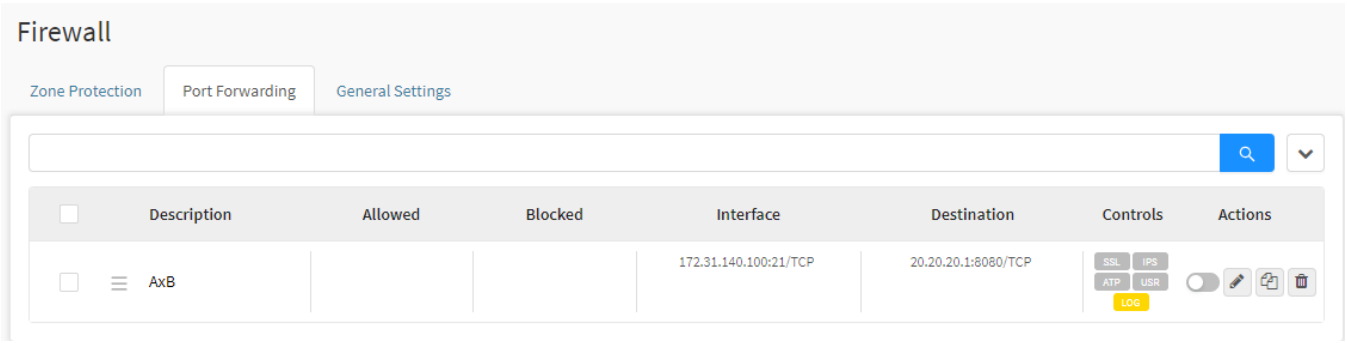
The item was successfully deleted.

Below we will detail the contents of the columns.

Port Forwarding - Delete Port Forwarding

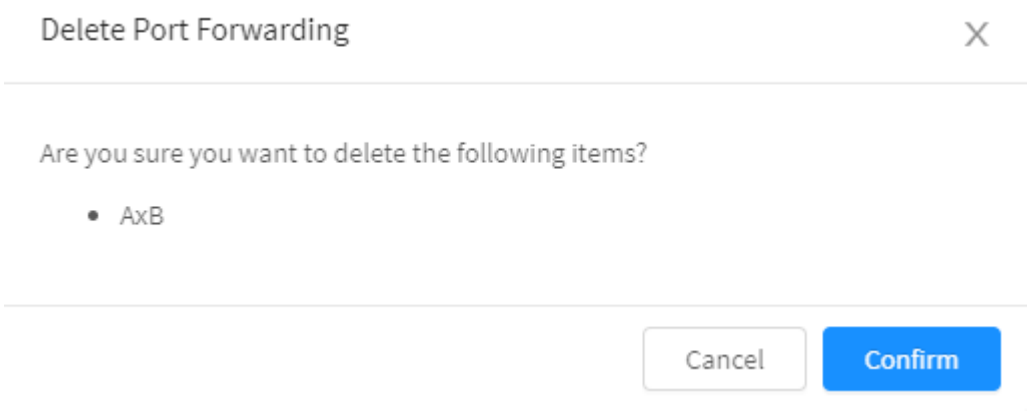
Through the delete buttom is possible to delete several itens all at once. Follow the next steps:

1. Select the itens to be deleted using the **Selection [ ]** option;



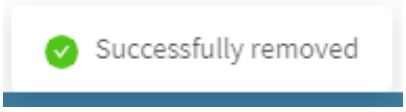
Port Forwarding - Seleção para deleção

2. Click on the **Delete [ ]** and a confirmation window will be opened:



Port Forwarding - Delete Item

If you do not want to delete the item, click on **[**  **]**. To confirm the deletion, click on **[**  **]**.



Successfully Removed

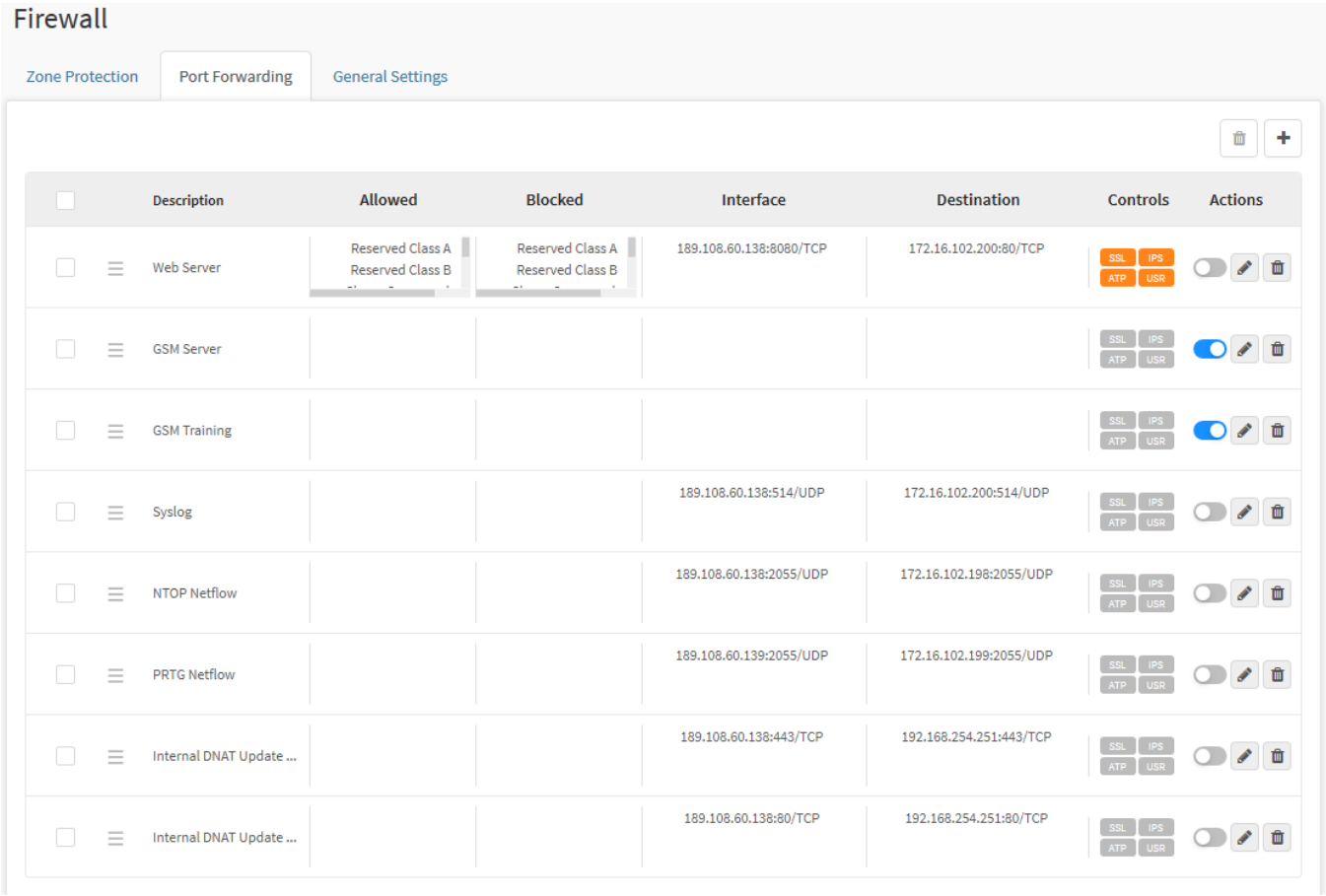
The item was successfully deleted.

Next we will detail the columns content.

UTM - Port Forwarding - Columns

Below we will explain each column of the Port Forwarding tab:

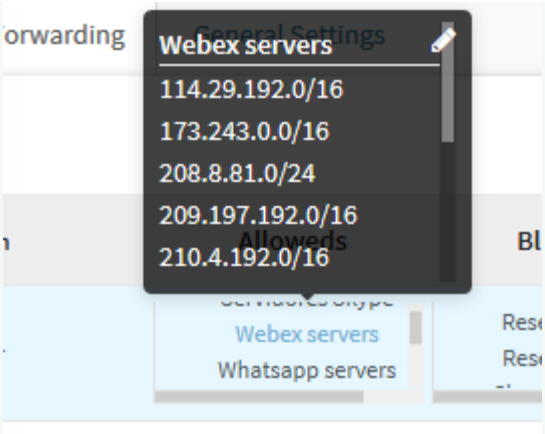
Port Forwarding rules are loaded from top to bottom, so the rules at the top of the table have priority over those below (being possible until they overlap the settings of the low rules).



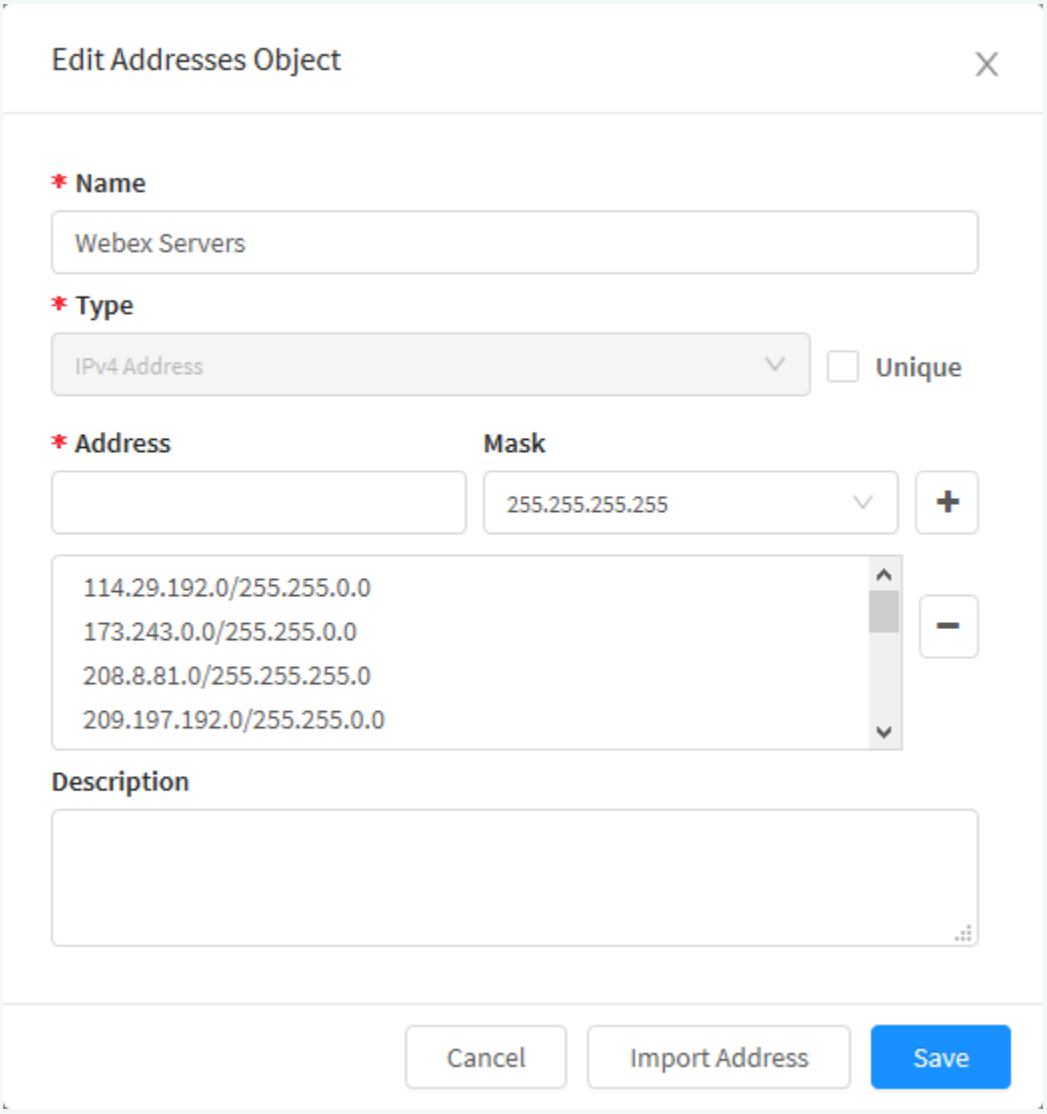
Port Forwarding

- ***Select [ ]:*** Allows you to select a Port Forwarding policy*;*
- ***Move[ ]:*** Allows you to move the Port Forwarding policy;
- **Description:** Displays the description of Port Forwarding for identification;
- ***Allowed:*** Displays allowed address objects that have been configured in *Port Forwarding* - Addition Button;
- ***Blocked:*** Displays blocked address type objects that have been configured in *Port Forwarding - Add Button*;

In the **Allowed** and **Blocked** columns it is possible to view more details by hovering over the address objects, a list with all the IPs that are part of the object will be displayed, as follows:



In addition, by clicking on the [ ] button displayed in this window, it is possible to edit the address object, as shown below:



- ***Interface:*** Determines the IP and the type of interface that Port Forwarding is using;
- ***Destination:*** Displays the destination IP address determined in *Port Forwarding* - Addition Button;

- **Controls:** Displays whether Port Forwarding has been configured to perform SSL Inspection[SSL], *Intrusion Prevention*[IPS], *Threat Blocking*[ATP] and/or *user authentication*[USR];
- ***Actions*:** Provides the following essential actions:
  - ***Enable***[]/***Disable***[]**:** Allows you to enable or disable a Port Forwarding policy;
  - ***Edit***[]**:** It allows to edit the settings of the interface added in *Port Forwarding - Addition Button*;
  - ***Delete***[]**:** Allows you to remove one of the items, it is equivalent to Port Forwarding - Removal button.

 When too much data is entered, exceeding the limit of the table cells and / or in the object details window (mentioned above), scroll bars will appear to facilitate navigation.

For more information on port forwarding, visit this page.

UTM - Firewall - General Settings

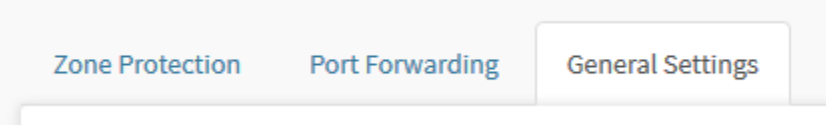
Through this tab it is possible to enable and configure the entry policies for the local ports and services of the Blockbit NGFW.

In addition, this tab allows you to configure the security parameters and firewall connection controls.

The item “Security Parameters” defines the basic security settings and the parameters of the connection controls responsible for maintaining the state information of all connections and Firewall sessions.

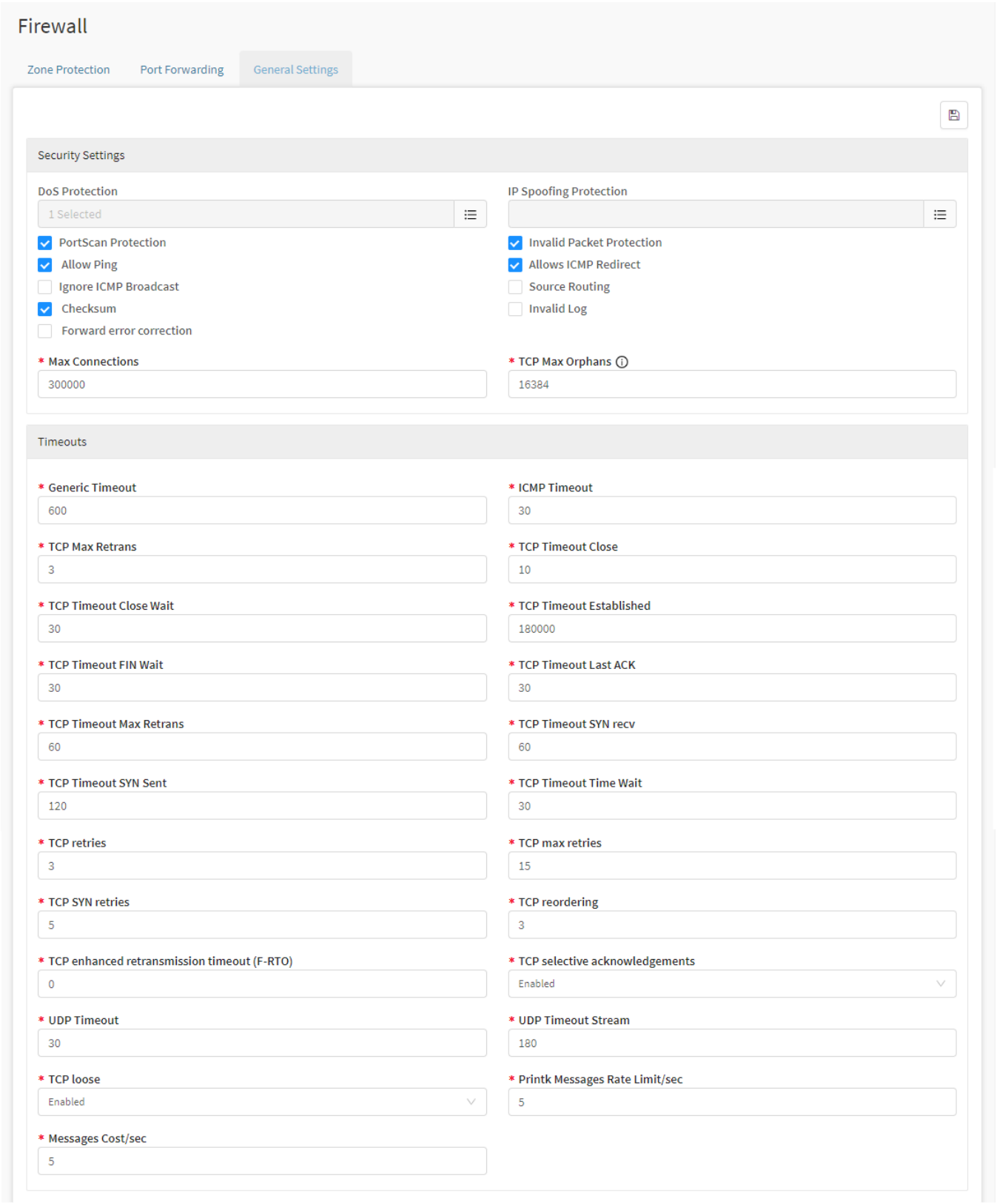
The pre-configured resources referring to the items of the “Connection Settings” of this interface refer to the connection control parameters, changing these values directly implies the performance result of the server.

To access, click on "General Settings".



General Settings tab

The “General Settings” screen will appear, as shown by the image below:



General Settings

The "General Settings" screen is made up of the following panels and features:

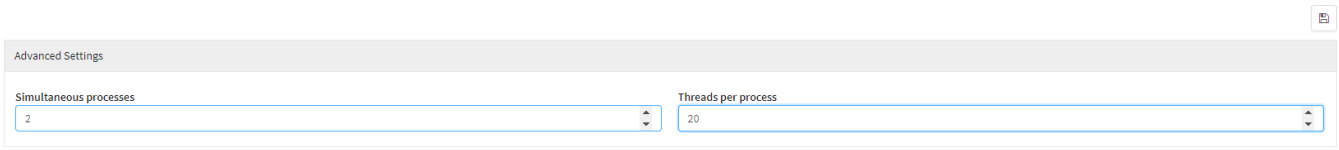
- Advanced Settings;
- *Security Settings;*
  - *DoS Protection;*

    - *IP Spoofing Protection;*
    - *PortScan Protection;*
    - *Invalid Packet Protection;*
    - *Allow Ping;*
    - *Allow ICMP Redirect;*
    - *Ignore ICMP Broadcast;*
    - *Source Routing;*
    - *Checksum;*
    - *Invalid Log;*
    - *Forward Error Correction;*
    - *Max Connections;*
    - *TCP Max Orphans.*
- *Timeouts;*
    - *Generic Timeout;*
    - *ICMP timeout;*
    - *Max Connections;*
    - *TCP Loose;*
    - *TCP Max Retrans;*
    - *TCP Timeout Close;*
    - *TCP Timeout Close Wait;*
    - *TCP Timeout Established;*
    - *Timeout TCP FIN Wait;*
    - *TCP Timeout Last ACK;*
    - *TCP Timeout Max Retrans;*
    - *TCP Timeout SYN Recv;*
    - *TCP Timeout SYN Sent;*
    - *TCP Timeout Time Wait;*
    - TCP Retries;
    - TCP Max Retries;
    - TCP SYN Retries;
    - TCP Reordering;
    - TCP Enhanced Retransmission Timeout (F-RTO);
    - TCP Selective Acknowledgements;
    - *UDP Timeout;*
    - *UDP Timeout Stream.*

Below we will detail each component of the panels:

Advanced Settings

Allows the configuration of the number of simultaneous processes and threads per process:



General Settings - Advanced options

Simultaneous Processes: Allows the selection of the number of simultaneous processes in the *Firewall* (Minimum of 2 and maximum of 8). It's important to remember that the values may vary for each appliance model, for they rely on the number of CPU Cores available.

To check the number of CPUs available in your appliance, use the lscpu commando on the terminal interface, then confirm the value on the CPUs field.

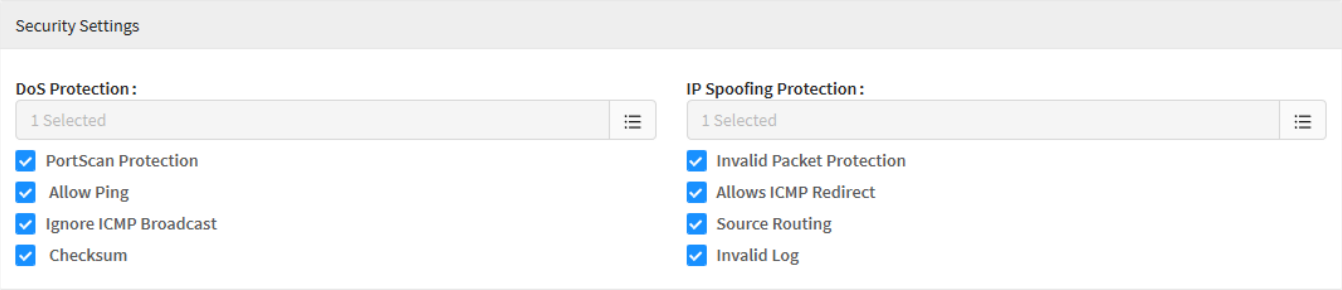
Threads per Process: Allows the selection of the number of threads per process in the *Firewall* (Minimum of 20 and Maximum of 40).

This configuration will cause the Firewall service to be reloaded by the system, which can cause some intermitence.

After selecting the target number, click save [] to record your changes.

Security Settings

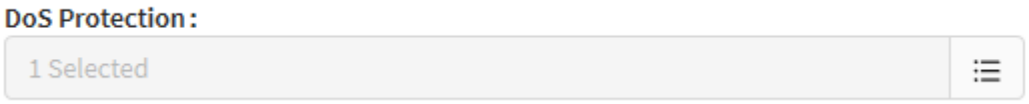
It serves to detail some of the configuration items of the security parameters.



General Settings - Security Settings

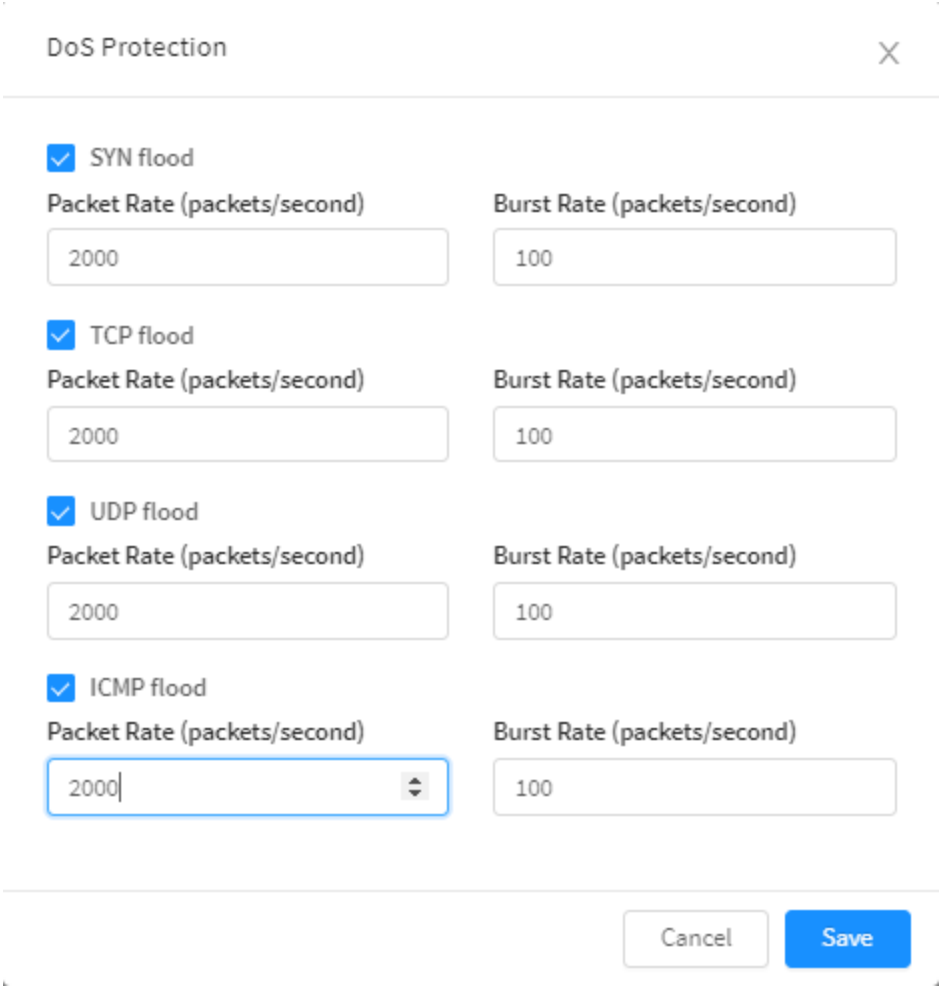
DoS Protection

This feature allows the blocking of denial of service counter attacks (also known as Denial of Service - DoS), it is an attempt to make system resources unavailable to its users. This is not an invasion of the system, but its invalidation due to overload, the supported techniques are: SYN Flood, TCP Flood, UDP Flood and ICMP Flood.



Dos Protection

When clicking on the **[** **]** button, the screen below will be displayed:

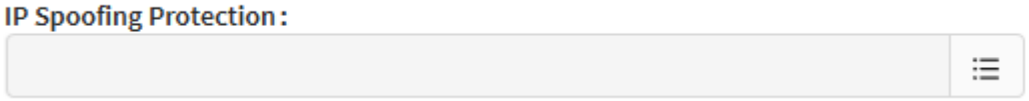


Dos Protection - Window

- ***SYN Flood limit (per second):*** *Determines the limit of incoming packets to prevent SYN Flood attacks*. The minimum value is 100 and the default value is 2000*;*
- ***SYN Burst:*** *The minimum value is 1 and the default value is 100;*
- ***TCP Flood limit (per second):*** *Determines the TCP access limit in order to prevent TCP Flood attacks. The minimum value is 100 and the default value is 2000;*
- ***TCP Burst:*** *The minimum value is 1 and the default value is 100;*
- ***UDP Flood limit (per second):*** *Determines the UDP access limit in order to prevent UDP Flood attacks. The minimum value is 100 and the default value is 2000;*
- ***UDP Burst:*** *The minimum value is 1 and the default value is 100;*
- ***ICMP Flood limit (per second):*** *Determines the ICMP access limit in order to prevent ICMP Flood attacks. The minimum value is 100 and the default value is 2000;*
- ***ICMP Burst:*** *The minimum value is 1 and the default value is 100.*

IP Spoofing Protection

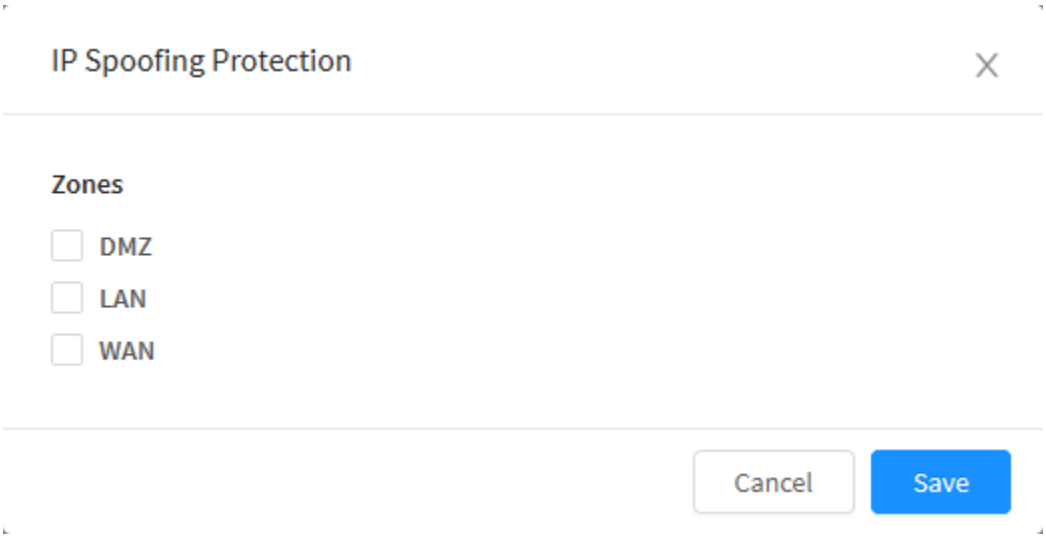
This feature enables the protection of IP Spoofing in the desired network zone.



IP Spoofing protection.

Zones with [IP Spoofing Protection] do not allow the use of SD-WAN.

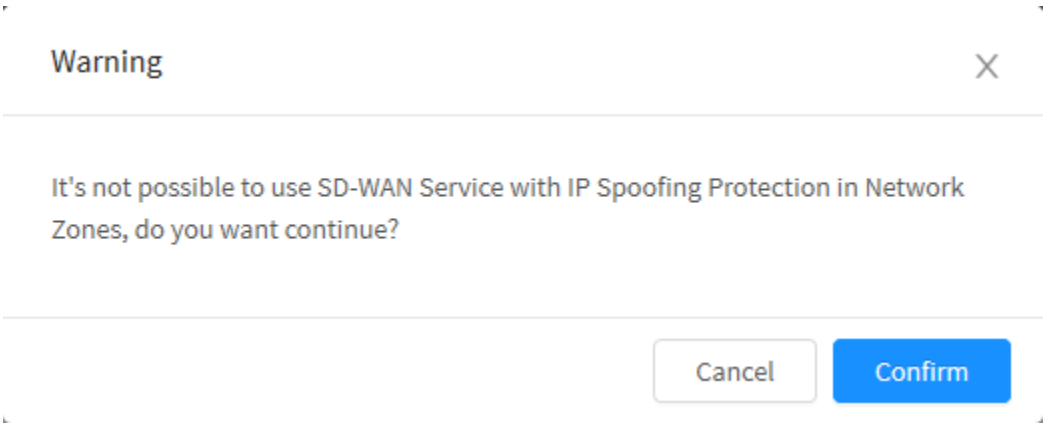
When clicking on the **[ ]** button, the screen below will be displayed:



IP Spoofing protection Zones

This feature enables the protection of IP Spoofing in the desired network zone.

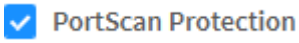
This option can cause problems with the SD-WAN service



Alert: SD-WAN and IP Spoofing Protection problems.

PortScan Protection

This feature allows application identification and blocking in order to map TCP and UDP ports. PortScan applications try to identify the status of the ports, whether they are closed, listening or open. Port scanners are often used by malicious people to identify open doors, exploit vulnerabilities and plan intrusions. **Recommendation**: Ex: *"[Enable]"*.



PortScan Protection

Invalid Packet Protection

Invalid packets are those that do not respect the TCP state diagram (handshake). Recommendation: Ex: "*[Enable]". The firewall service discards packets that are considered invalid*.

Invalid Packet Protection

Allow Ping

This feature allows all PING requests (Echo Request and Echo Reply) to be answered through any network interface on the system. Recommendation: Ex: *"[Disable]".*

Allow Ping

Allow ICMP Redirect

This feature is a message type used by routers to notify hosts on the same network segment, that there is a better path (route) to a given destination. Recommendation: Ex: *"[Disable]".*

Allows ICMP Redirect

This item comes with a standard [Enabled] for identifying numerous ill-defined network structures.

Ignore ICMP Broadcast

This feature ignores ICMP Broadcast traffic, used to make servers unwittingly participate in DOS attacks, sending large amounts of pings exponentially increasing NETBIOS network traffic and making real services unavailable.

Recommendation: Ex: *"[Enable]" Ignore ICMP Broadcast.*

Ignore ICMP Broadcast

Source Routing

This feature allows you to apply routing tests behind the firewall, allow the sender of the packet to specify the path to and from the packet. Recommendation: Ex: *"[Disabled]".*

Source Routing

Source Routing consists in a protocol mechanism that allows the transportation of information by an IP packet. Information like addresses lists, informing the router the path that the packet must follow. It also counts with an option to save leaps as the route is run. The route register, which lists the addresses, provides the destination with a return path, back to the origin. Which allows the origin (sender host) to specify the route, in a vague or strict manner, ignoring some or every routers' routing sheets. It also allows a user to redirect the network traffic for malicious ends. Therefore, the *Source Routing* must be disabled.

The *Source Routing* option makes that the network interfaces accept packets with a *Strict Source Route* (SSR) or *Loose Source Routing* (LSR) options set. The source routed packets acceptation is controlled by the kernel settings. Therefore, to issue the packet's discard command along the SSR or LSR options set, the checkbox must be kept disabled.

Checksum

Packages with bad checksums are in an invalid state. With this option enabled, such packets will not be considered for connection tracking in session tracking.

Checksum

Invalid Log

Enables package logs with INVALID state.

Invalid Log

Forward Error Correction

Consists in an error control method in data transmission. During a session of data transmition from a source to a destination, usually the data is recognized without error, even if part of the data is lost. With this option on, the data packets are received twice and accepted only with validation at least in a single instance.

FEC - Forward error correction

Max Connections

Maximum number of connection.

Max connections

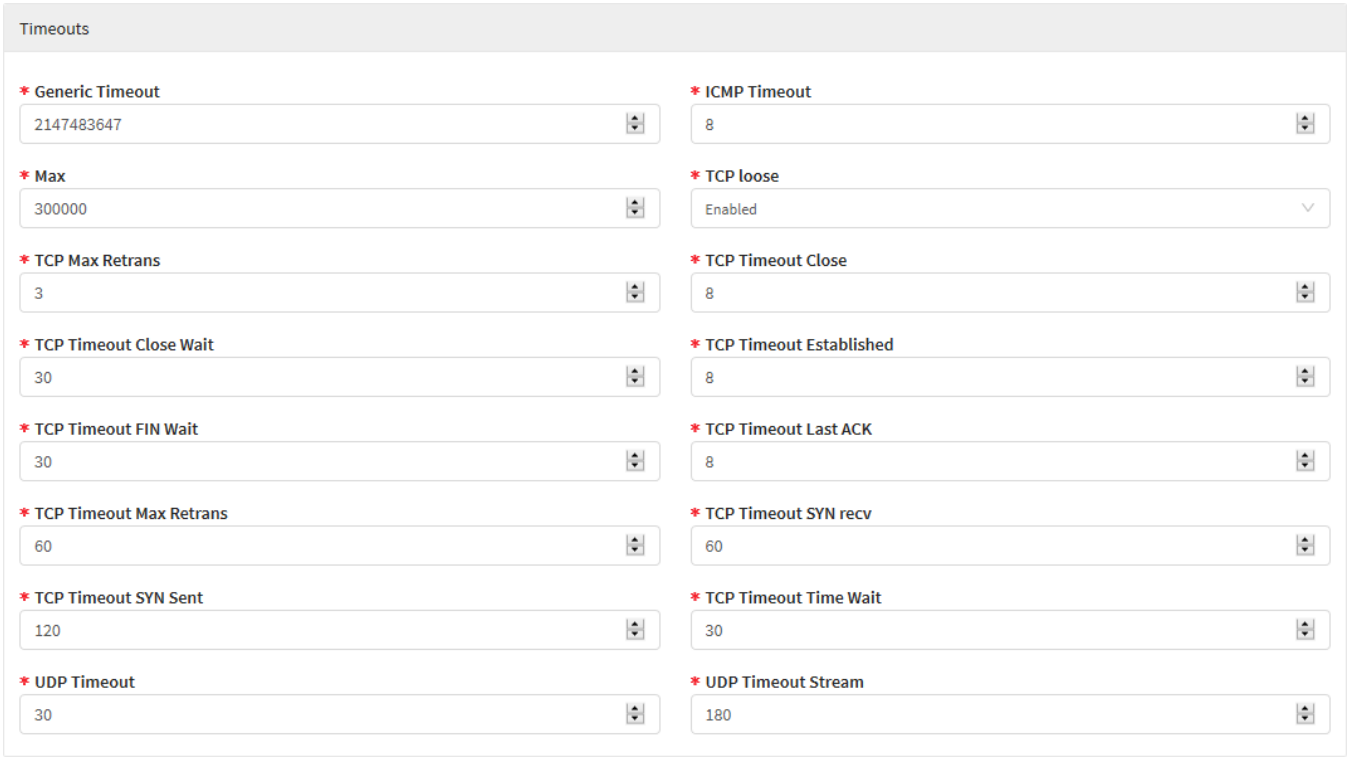
TCP Max Orphans

Maximum number of TCP sockets not associated to processes or services, that are run by the OS in the user space. In case this mumber is exceeded the connections are immediately reset.

TCP Max Connections

Timeouts

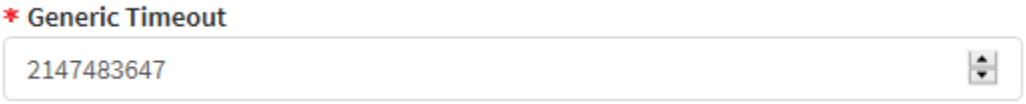
The other preconfigured resources referring to the items of the “Connection settings” of this interface refer to the parameters of the “Session Track”, the change of these values directly implies the performance result of the server.



General Settings - Timeout

Generic Timeout

This parameter is used to inform the session tracking of the generic timeout in seconds if it is not possible to determine the protocol used or to use more specific values. Any flow or packet that enters the firewall that cannot be fully identified as any other type of protocol will receive a generic timeout defined in this parameter. The minimum value is 0 and the default value is 600 seconds.



Generic Timeout

ICMP Timeout

Used to set the timeout in seconds for ICMP packets that will result in return traffic. In other words, include ECHO REQUEST and REPLY, TIMESTAMP REQUEST and REPLY, INFORMATION REQUEST and REPLY and ADDRESS MASK REQUEST and REPLY. Once an order is placed, there must be a return package, and that is when the ICMP timeout is counted. An ICMP response is usually quite fast, unless a very slow connection is used. The minimum value is 0 and the default value is 30.

ICMP Timeout

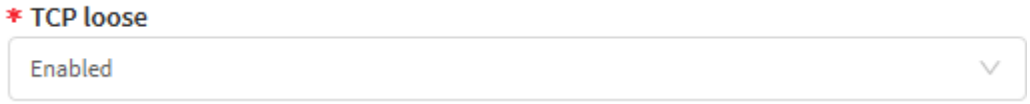
Max Connections

Maximum size of the session tracking table, that is, of connections established simultaneously. The default value is 300,000 seconds.

Max Connections

TCP Loose

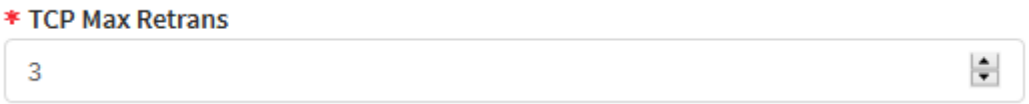
Enables / Disables the survey of new connection entries already established in the session tracking table. The minimum value is 0 and the default value is 1 (enabled), to disable, set the value to 0.



TCP Loose

TCP Max Retrans

Defines the maximum number of TCP packets that can be retransmitted without receiving an acceptable ACK from the destination. The minimum value is 0 and the default value is 3.



TCP max retrans

TCP Timeout Close

Sets the default timeout value in seconds for TCP connections in the CLOSE state, to be removed from the session tracking table. The minimum value is 0 and the default is 10 seconds.

TCP timeout close

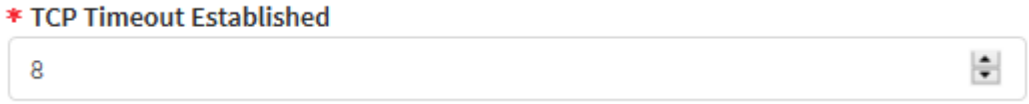
TCP Timeout Close Wait

Defines the default timeout value in seconds for TCP connections with CLOSE-WAIT status, to be removed from the session tracking table. The minimum value is 0 and the default is 30 seconds.

TCP timeour close wait

TCP Timeout Established

Sets the timeout in seconds for established TCP connections, to be removed from the session tracking table. The minimum value is 0 and the default value is 180000 seconds (equivalent to 2.08 days).



TCP timeout established

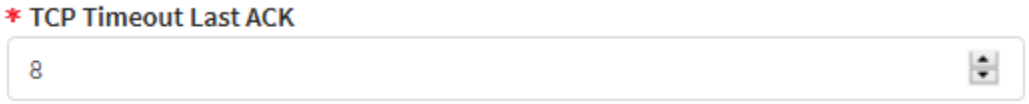
TCP Timeout FIN Wait

Sets the timeout in seconds for TCP connections with FIN-WAIT-1 and FIN-WAIT-2 status, to be removed from the session tracking table. The minimum value is 0 and the default value is 30 seconds.

Timeout TCP FIN wait

TCP Timeout Last ACK

Sets the timeout in seconds for TCP connections with LAST-ACK status, to be removed from the session tracking table. The minimum value is 0 and the default value is 30 seconds.



TCP timeout last ACK

TCP Timeout Max Retrans

Defines the timeout in seconds for TCP connections that reach the maximum number of retransmissions defined in the "TCP max retrans" option without receiving an acceptable ACK from the destinations. The minimum value is 0 and the default value is 300 seconds.

TCP timeout max retrans

TCP Timeout SYN Recv

Sets the timeout in seconds for TCP connections with the SYN RECV status, to be removed from the session tracking table. The minimum value is 0 and the default value is 60 seconds.

TCP timeout SYN recv

TCP Timeout SYN Sent

Sets the timeout in seconds for TCP connections with the SYN SENT state, to be removed from the session tracking table. The minimum value is 0 and the default value is 120 seconds.

TCP timeout SYN sent

TCP Timeout Time Wait

Sets the timeout in seconds for TCP connections with TIME WAIT status, to be removed from the session tracking table. The minimum value is 0 and the default value is 60 seconds.

TCP timeout time wait

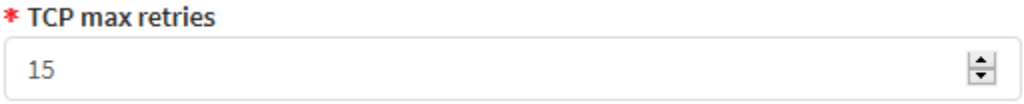
TCP Retries

Defines how many times to try to retransmit TCP packets over an established connection. When this limit is exceeded, before each new retransmission the network layer will have its route updated. The default value is 3.

TCP retries

TCP Max Retries

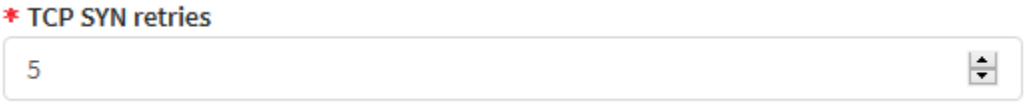
Defines the maximum number of times that TCP packets will be retransmitted before interrupting this process. The default value is 15 (approximately 13 to 30 minutes).



TCP max retries

TCP SYN Retries

Determines at most how many times the initial SYNs will be retransmitted in an active TCP connection attempt. The default value is 5 (equivalent to about 180 seconds) and the maximum value is 255.

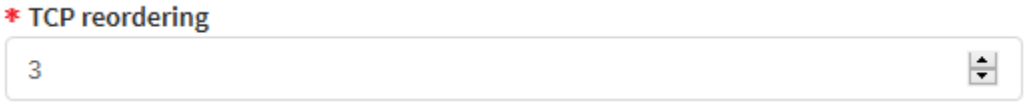


TCP SYN retries

TCP Reordering

This value defines the maximum limit for reordering to be carried out on packets in a TCP stream without the protocol assuming that these packets are lost and their initialization performance is reduced. The default value is 3.

WARNING: Do not change this value without being completely sure what you are doing. It acts by detecting the reordering of the packets and serves to minimize retransmissions (necessary or not) caused by the reordering of the connection packets.



TCP reordering

TCP Enhanced Retransmission Timeout (F-RTO)

F-RTO stands for Forward Retransmission TimeOut, it is an algorithm whose function is to detect and improve the time limit in illegitimate retransmission using the TCP and SCTP protocol (flow control).

For more details regarding this feature, refer to RFC 4138.

TCP enhanced retransmission timeout (F-RTO)

TCP Selective Acknowledgements

This field allows you to enable or disable the TCP Selective Acknowledgements (SACK) feature. This functionality works by sending the sender a report of everything that was successfully received so that all data packets and segments that have been lost can be sent again by the sender, guaranteeing the integrity of the data packets and limiting the amount of retransmissions. By default, this field is enabled.

For more details regarding this feature, see the RFC 2018.

TCP selective acknowledgements

UDP Timeout

This feature defines the maximum time that a connection remains active in an idle state, that is, without any traffic. Once the configured timeout is reached, the system removes all UDP protocol connections, which are in idle state with the configured timeout exceeded. The minimum value is 0 and the default value is 30 seconds.

UDP timeout

UDP Timeout Stream

Sets the timeout in seconds for UDP STREAM (ASSURED) connections. The minimum value is 0 and the default value is 180 seconds.

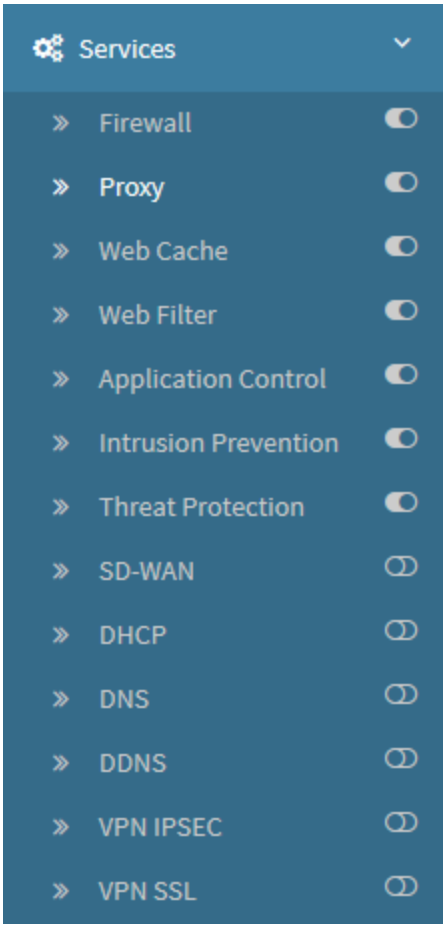
UDP timeout stream

NGFW - Services - Proxy

The "Proxy" screen has the function of configuring the operation of the system's proxies and also how the SSL inspection will act.

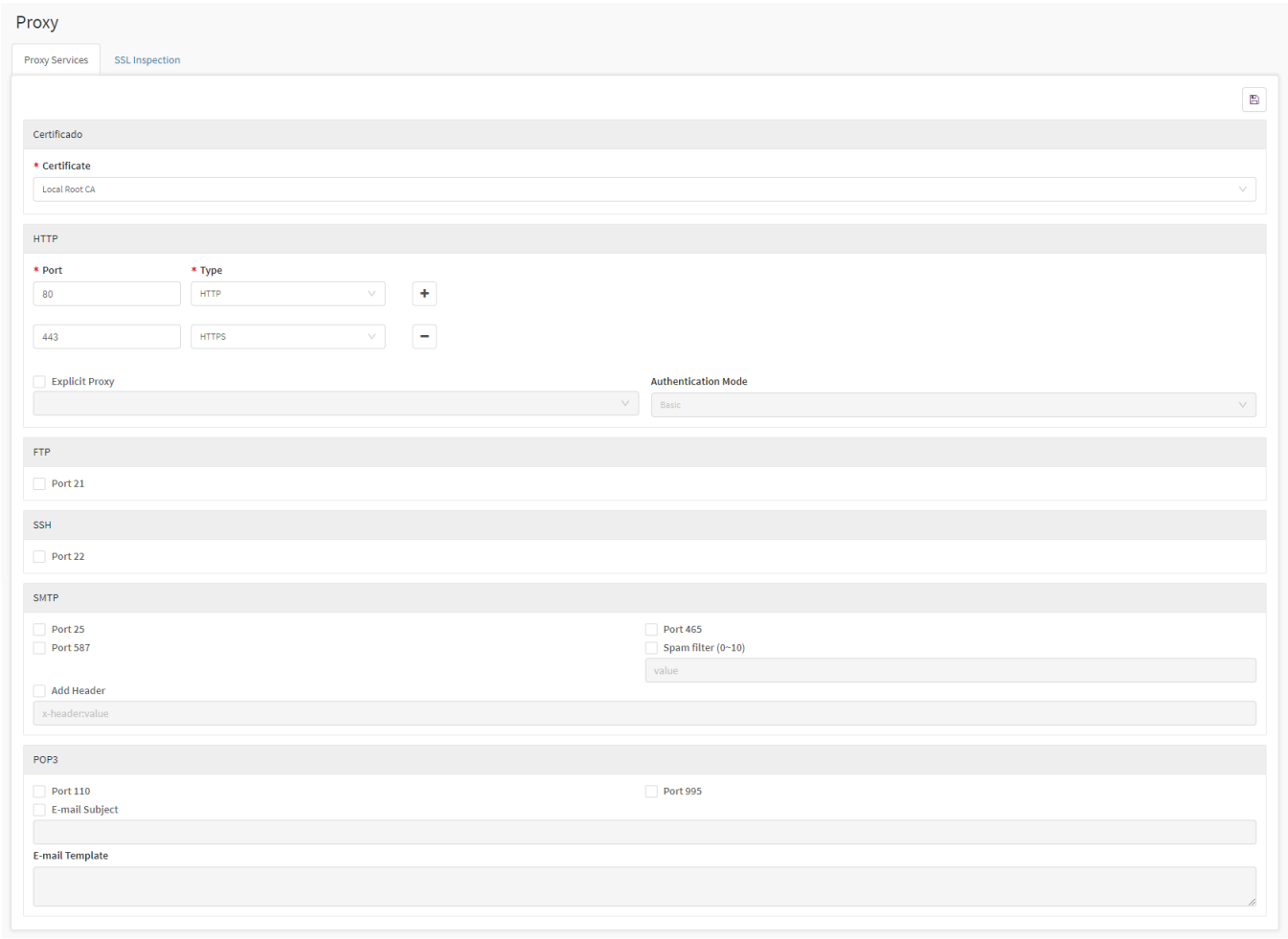
In the following pages we will analyze it in more detail.

To access this screen, just select the “Proxy” option.



Services - Proxy

The screen below will appear:



Proxy Services - Settings

The screen has the following options:

- *Proxy Services*;
- *SSH Proxy*;
- *SSL Inspection*.

Next we will analyze the components of the Proxy Service tab.

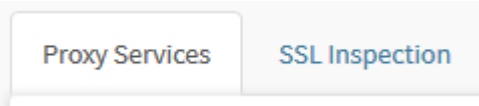
NGFW - Proxy - Proxy Services

We will address the aspects of network security through the analysis of the *Proxies*, which are connections/network traffic interception services.

Proxies are systems or applications that act as intermediaries for client requests that request resources from other servers. A client application connects to a "Proxy" server, requesting some service, e.g. "a connection", "a web page", "a file", or "other resources" from other servers. The Proxy forwards this request to the remote server (usually on the public network), and returns its response to the internal client (local network host).

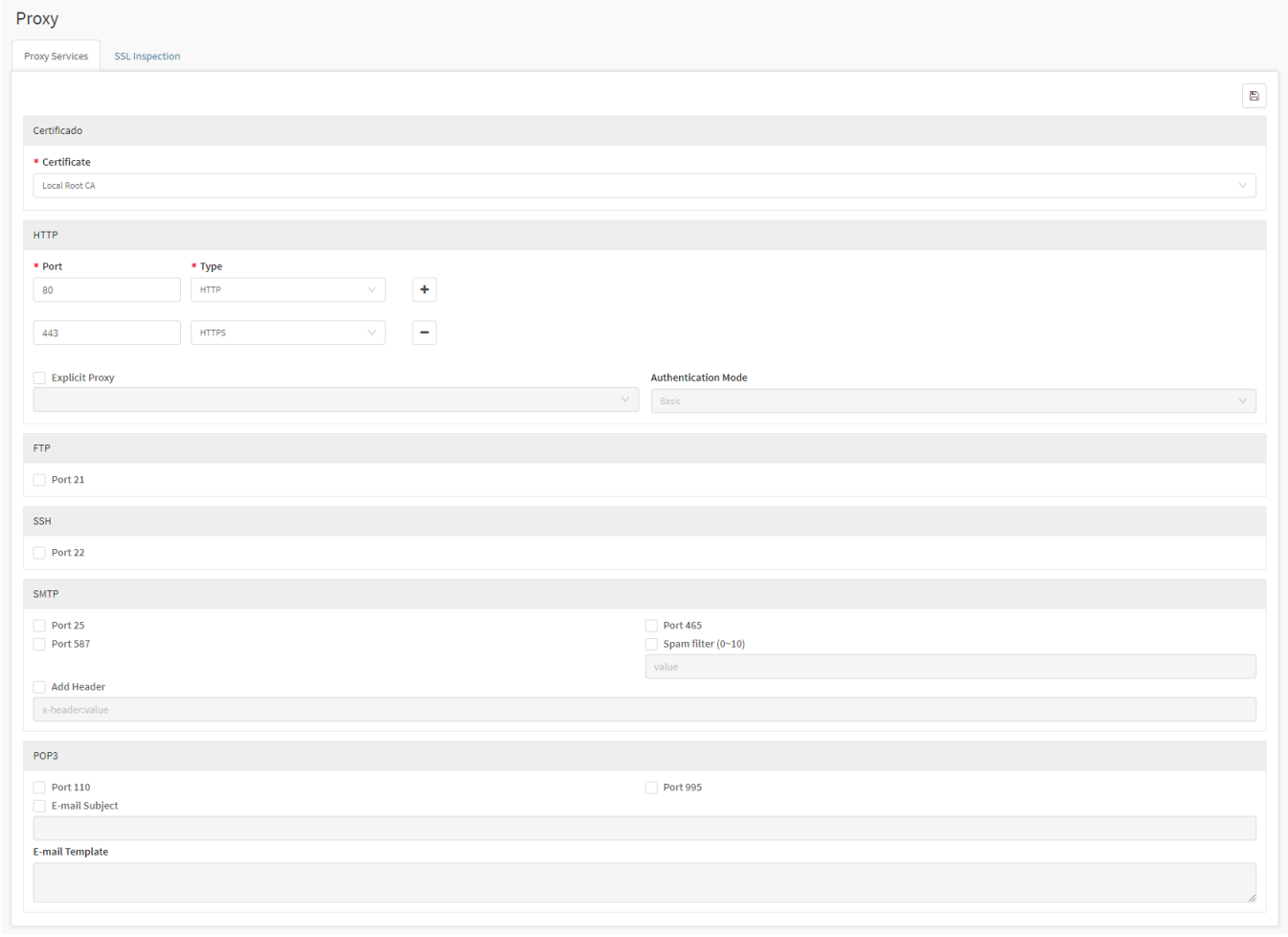
Most of the time, Proxies are used by all clients in a subnet and due to their strategic position, they usually implement a cache system for some services. In addition, as Proxies work with application data, a different Proxy is required for each service.

To configure and enable Proxy services, if it is not already selected, click on the tab, as shown below:



Proxy Services tab

The screen below will be displayed:



Services – Proxy Services

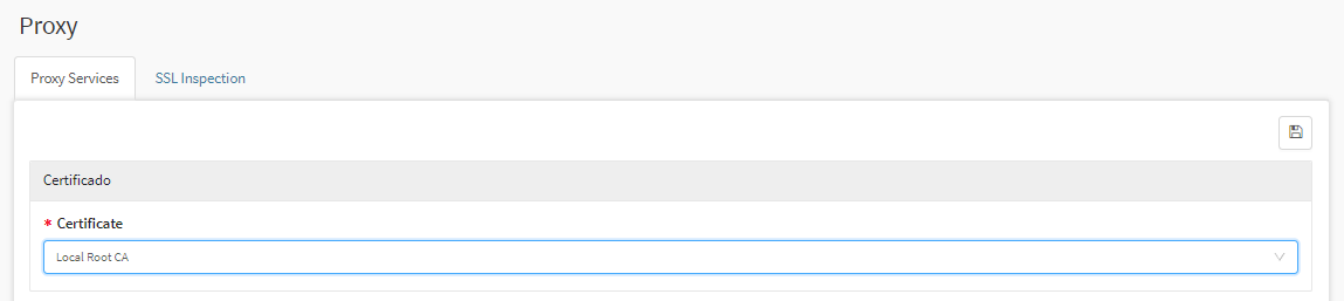
The Blockbit NGFW, includes security services through active Proxies, the supported protocols and services are:

- Root Certificates;
- *HTTP*;
- *FTP*;
- SSH;
- *SMTP*;
- *POP3*.

Next we will analyze each panel on this screen.

Root Certificates

The *certificates* field is used for the selection of remote authority certificates (CA) to be used in the Proxy service.



Proxy - Certificates overview

The CAs presented in this selection field are remote certificates and must be imported in Settings Certificates Authority tab.

For more details on how to import them, click here.

HTTP Proxy

The HTTP Proxy feature is provided integrated by the Web Cache service, which consists of offering Internet access for users of a network or subnet who do not have direct access to the public network, among its various functionalities, in a simple way , safe and efficient.

In addition, it also contributes to controlling the unrestricted use of web services and reducing bandwidth consumption, since it has “Web caching” mechanisms and integration with the “Web Filter” service with access control through “Content” filters and “Applications”, and the “Antimalware” service for compromised file filters, through security policies that restrict users' browsing.

The Blockbit NGFW Proxy modes:

- **Transparent**

In this mode of operation the proxy is configured to allow Https traffic only under SSL interception, which requires the import and installation of the CA (Certification Authority) for all devices on the network.

To allow SSL traffic in by-pass mode, it is necessary to configure it with an “SSL COMMON NAME” filter for exception in security policies.

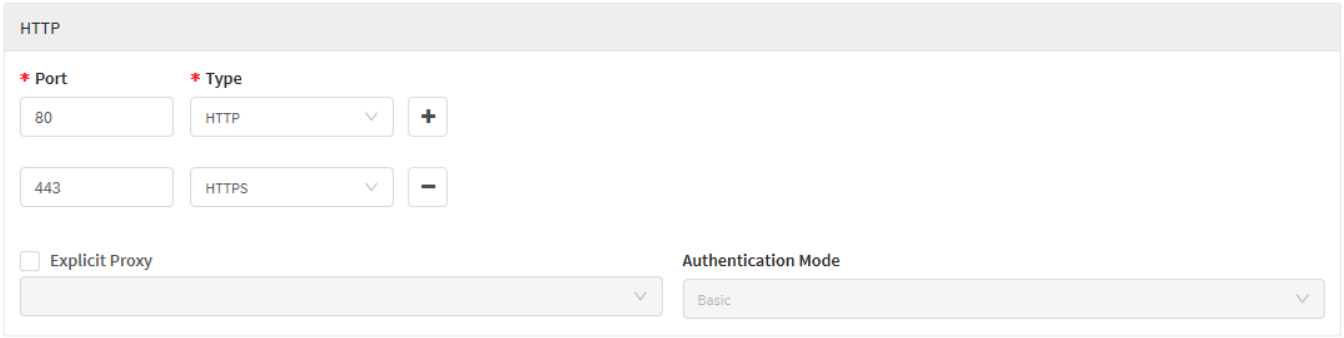
- **Explicit**

To access the proxy in explicit mode, it is necessary to configure the WEB browser of the network devices to access the proxy in configured mode.

This access mode requires the configuration of a security policy with permission to access WEB services in Explicit Proxy mode.

Configuration

For HTTP Proxy configuration, review the considerations below. In this panel you are able to configure the supported ports:



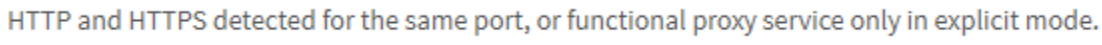
HTTP Proxy

The service is pre-configured to allow access to the standard web services “HTTP (port 80) and HTTPS (port 443)”. The service ports are configurable with support for “HTTP and HTTPS versions 1.0 and 1.1” protocols.

To add a new port, click the **[**  **]** button. If you want to remove a door click on the **[**  **]** button.

In **Port,** type in the desired port, in **Type** it is possible to select the protocol to be used in the proxy, there are 3 options for the checkboxes:

- ***HTTP*:** In this mode the port will use the HTTP protocol;
- ***HTTPS*:** In this mode the port will use the HTTPS protocol;
- ***HTTP/HTTPS*:** If this mode is activated, both the HTTP and HTTPS protocols will be applied to the same port, however, this mode will cause the proxy to work only in explicit mode, therefore, all rules used in the transparent proxy will be ignored. For this reason, the system message illustrated below is displayed when selecting this option:



HTTP/HTTPS Proxy

Attention: If HTTP/HTTPS mode is activated on any port, all proxy rules used in transparent mode will be switched OFF. To reactivate, it is necessary to STOP using HTTP / HTTPS mode on any ports.

- ***Explicit Proxy*[ ]:** By checking this checkbox, the proxy in explicit mode will be activated and the port setting field and authentication mode will be available. In the proxy service port definition field, by default, the system will use the "NGFW-PROXY" service object with TCP port 128;
- ***Authentication Mode*:** Allows you to select the type of authentication to be performed, the options are:
  - **Basic:** If this option is selected, a pop-up requesting authentication will be displayed in the browser;
  - ***Captive Portal:*** If this option is selected, authentication will be performed through the captive portal, for more information on this, see this page;

If the Explicit Proxy option is not activated, that is, if it is a Transparent Proxy, then the authentication will automatically be performed in the authentication portal (Captive Portal).

To save all changes, click **[ ]**.

After saving, for the proxy to take action it will be necessary to access the command queue **[ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

Next we'll review the *FTP proxy*.

FTP Proxy

In this section we will cover the FTP Proxy service, an application integrated with the Blockbit NGFW meant to inspect file transfer traffic between local networks and the public network (Internet) under the FTP protocol in a secure way.

Its basic function is to enable the administrator through the “Security Policies” to handle packets and file transfers through the traffic of FTP ports “20 and 21 / TCP”.

Configuration

For FTP Proxy configuration, review the considerations below:

Proxy FTP

- **[ ] Port 21:** By enabling this check box, the connection port to the Remote FTP servers (21 / TCP) is activated.

Support:

- Mode: **[Active *FTP*]**.

The functioning of the FTP Proxy requires the configuration of a “Security Policy” with the Web Proxy content filter enabled for the FTP protocol.

To save all changes, click **[ ]**.

After saving, for the proxy to take action it will be necessary to access the command queue and apply the changes made. For more information on the command queue, access the following page: UTM - Command queue.

If it is necessary to integrate the Malware Scanning filter through FTP Proxy traffic, it will be necessary to enable and configure the *Threat Protection service.*

Its operation depends on the configuration of profiles by “Security Policies”.

Next, we'll look at *SMTP* features.

SSH Proxy

In this section we will cover the SSH Proxy service, and how to set it up on the NGFW.

In an SSH Proxy configuration, the firewall resides between a client and a server. SSH Proxy enables the firewall to decrypt inbound and outbound SSH connections and ensures that attackers don’t use SSH to tunnel unwanted applications and content. SSH decryption does not require certificates and the firewall automatically generates the key used for SSH decryption when the Firewall boots up. During the boot process, the Firewall checks if there is an existing key. If not, it generates a key. The firewall uses this key to decrypt SSH sessions for all virtual systems configured on the Firewall and all SSH v2 sessions.

SSH allows tunneling, which can hide malicious traffic from decryption. The Firewall can’t decrypt traffic inside an SSH tunnel. You can block all SSH tunnel traffic by configuring a Security policy rule for the application ssh-tunnel with the Action set to Deny (along with a Security policy rule to allow traffic from the ssh application).

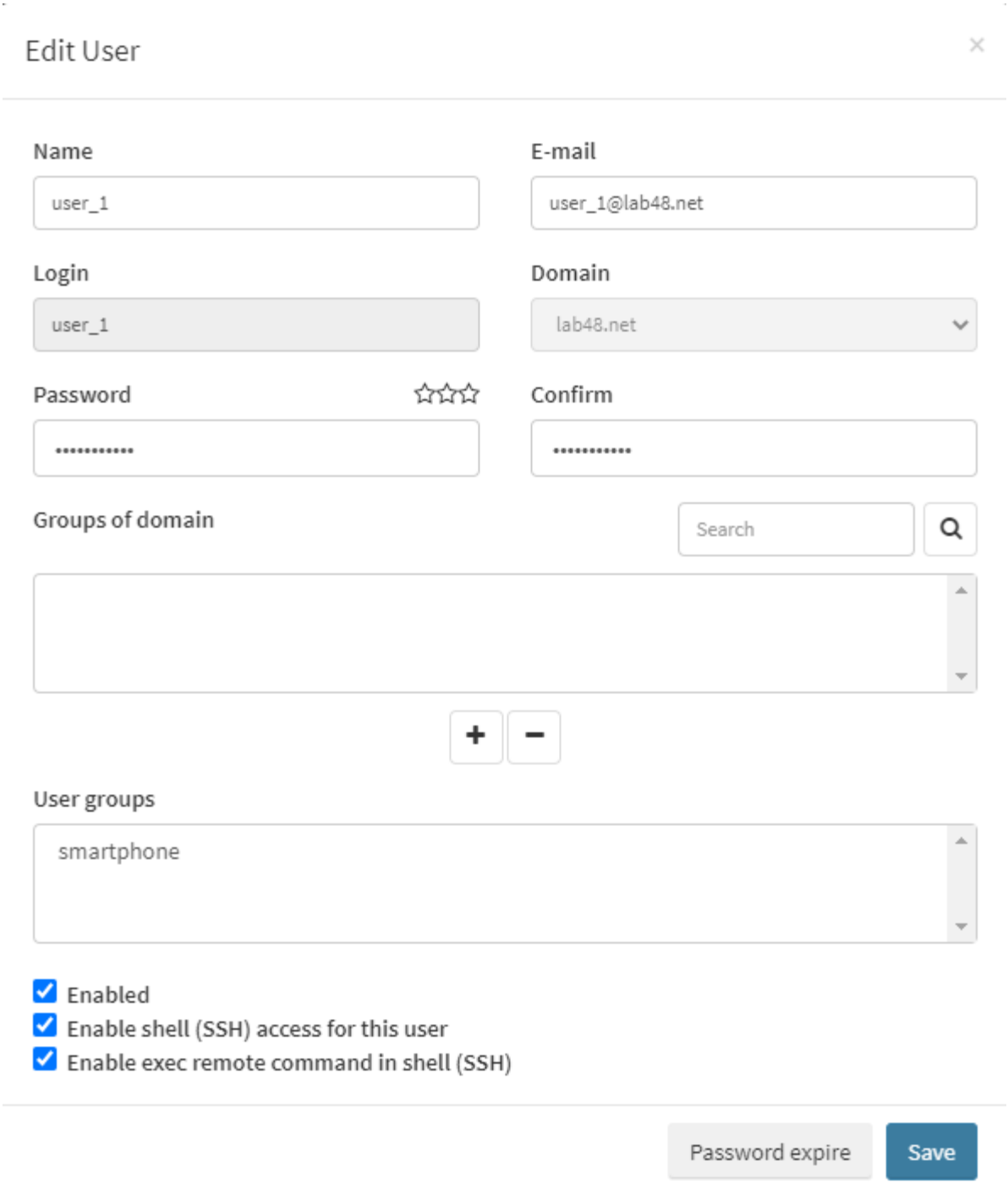
Limit SSH use to administrators who need to manage network devices, log all SSH traffic, and consider configuring Multi-Factor Authentication to help ensure that only legitimate users can use SSH to access devices, which reduces the attack surface.

Configuring the SSH Proxy

On the NGFWs main menu, we must access Services Proxy Proxy Services. In this section we will find the option to enable port 22, initialy we shall mark this option, enabling it:

Proxy services - SSH

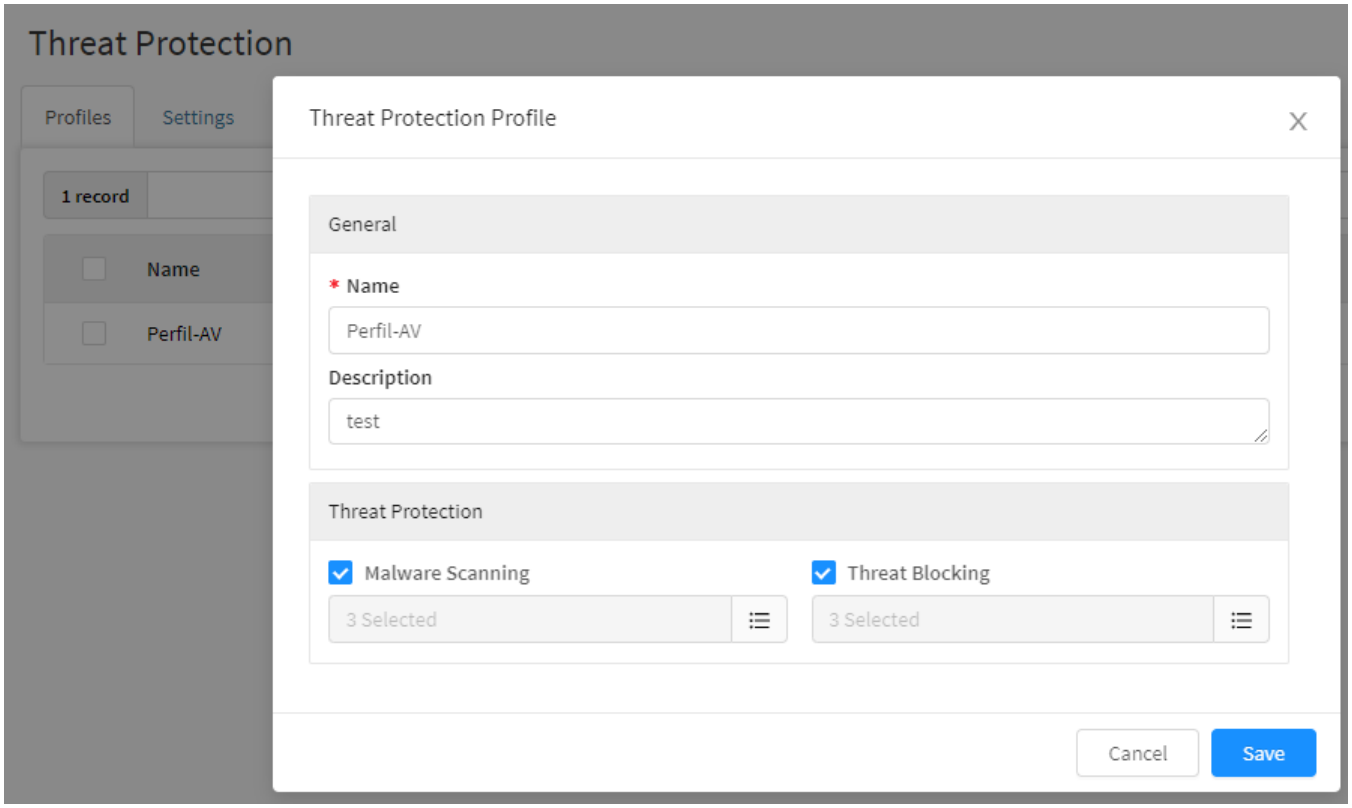
Next, we must access Settings Authentication Users, on this next section we are able to create a new user or edit a preexisting one. The "Allow access to shell (SSH)" and "Allows running remote commands on the secure shell (SSH)" options have to be marked:



User's permissions

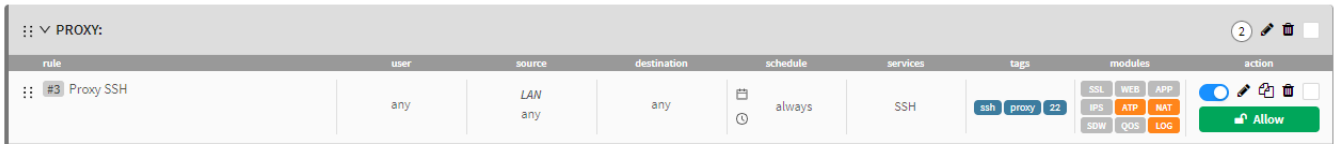
It's important to highlight the fact that this setting is only valid for local users, and remote logins **do not** have this option.

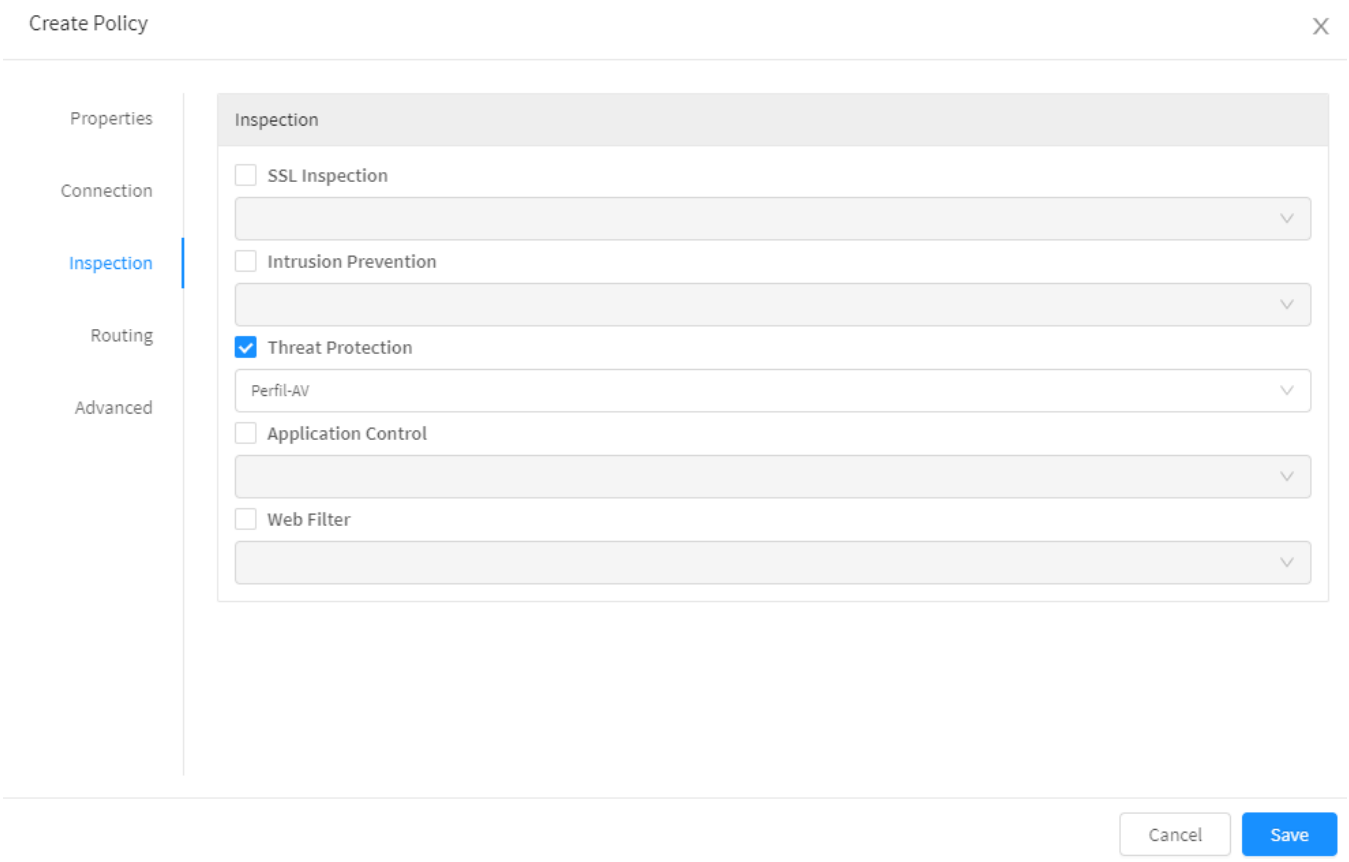
On the sequence, we must go to Services Threat Protection Profiles and set a Threat Protection profile up, enabling the "Malware verification" and "Threats block" options while we do so:



Threat Protection profile set up

Next, we must create an inspection Policy on Policies IPv4 Create Policy, and mark the Threat Protection option, as well as select the Threat Protection profile we have created just a few steps ago:





Policy creation with Threat Protection on

By having finished the settings, we must now initiate an SSH connection normally (from the user to the destination). On the destination, the user must insert the user and IP address of the destination SSH as follows on the example: # ssh root@eizure.com). The user and password we must use are those we have registered on the "Authentication" step with the SSH enabled.

At this point, the NGFW will intercept the connection, and the security verification will be run, normally. In case there is any notification indicating the "fingerprint" exchange, it must be ignored because it signals that the SSH is being connected to the Proxy.

On the next screen we must use the login and password from the user we are using, however it still isn't the SSH data:

```
\*********************************
\* Welcome do Block-bit SSH-Proxy *
\*********************************

 You must login to NGFW first to access 172.16.12.100

 Username:
 Password:
```

SSH Proxy - user validation

After the NGFW's tests with the SSH server on the final destination, these information will be displayed on screen, along with the option to continue the connection:

```
weslei@venon2:~$ ssh administrator@172.23.21.185
********************************
* Welcome to Block-bit SSH-Proxy *
********************************

 You must login to NGFW first to access 172.23.21.185

Login: user_1
Password:
Starting Auditing....
CLIENT
# general
(gen) banner: SSH-2.0-OpenSSH_8.2p1
(gen) software: OpenSSH 8.2p1

# security
(cve) CVE-2021-36368 -- (CVSSv2: 3.7) trivial authentication attack to bypass FIDO tokens and SSH-ASKPASS
(cve) CVE-2021-28041 -- (CVSSv2: 7.1) double free via ssh-agent
(cve) CVE-2020-14145 -- (CVSSv2: 5.9) information leak via algorithm negotiation
(cve) CVE-2020-12062 -- (CVSSv2: 7.5) arbitrary files overwrite via scp

SERVER
# general
(gen) banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
(gen) software: OpenSSH 8.9p1
(gen) compatibility: OpenSSH 8.5+, Dropbear SSH 2018.76+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256                     -- [info] available since OpenSSH 7.4, Dropbear SSH 2018.76
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp256                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521                    -- [fail] using weak elliptic curves
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) sntrup761x25519-sha512@openssh.com    -- [info] available since OpenSSH 8.5
(kex) diffie-hellman-group-exchange-sha256 (2048-bit) -- [info] available since OpenSSH 4.4
(kex) diffie-hellman-group16-sha512         -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(kex) diffie-hellman-group18-sha512         -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group14-sha256         -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73

# host-key algorithms
(key) rsa-sha2-512 (3072-bit)               -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256 (3072-bit)               -- [info] available since OpenSSH 7.2
(key) ecdsa-sha2-nistp256                   -- [fail] using weak elliptic curves
                                            `- [warn] using weak random number generator could reveal the key
```

Vulnerability analysis results

And so we have finished configuring the SSH Proxy.

```
# fingerprints
(fin) ssh-ed25519: SHA256:VHmMgfOtd8rdNth0D2Zf9W+YRTYyjpQk8Y8uSaS2c9A
(fin) ssh-rsa: SHA256:J1RwOIvN1xS+tZVBy60idfXMUL3diCja4H/3XKdaP/U

# algorithm recommendations (for OpenSSH 8.9)
(rec) -ecdh-sha2-nistp256                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                   -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521                   -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256                  -- key algorithm to remove
(rec) -hmac-sha1                            -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com            -- mac algorithm to remove
(rec) -hmac-sha2-256                        -- mac algorithm to remove
(rec) -hmac-sha2-512                        -- mac algorithm to remove
(rec) -umac-128@openssh.com                 -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com              -- mac algorithm to remove
(rec) -umac-64@openssh.com                  -- mac algorithm to remove

Continue(y/N):
y
The authenticity of host '172.23.21.185 (172.23.21.185)' can't be established.
ECDSA key fingerprint is SHA256:nvkWoDCDznPWm3XO19twocOKYOfAux2xB7Op0V6jtrQ.
ECDSA key fingerprint is MD5:ed:f5:63:69:3c:fd:4e:41:02:4d:8a:3d:b9:e7:49:21.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.23.21.185' (ECDSA) to the list of known hosts.
administrator@172.23.21.185's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Feb 14 10:47:29 AM -03 2023

  System load:  0.4716796875      Processes:               249
  Usage of /:   10.5% of 78.19GB  Users logged in:         0
  Memory usage: 42%               IPv4 address for ens160: 172.23.21.185
  Swap usage:   77%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Mon Feb 13 15:29:26 2023 from 172.31.150.48
administrator@mail:~$
```

SMTP Proxy

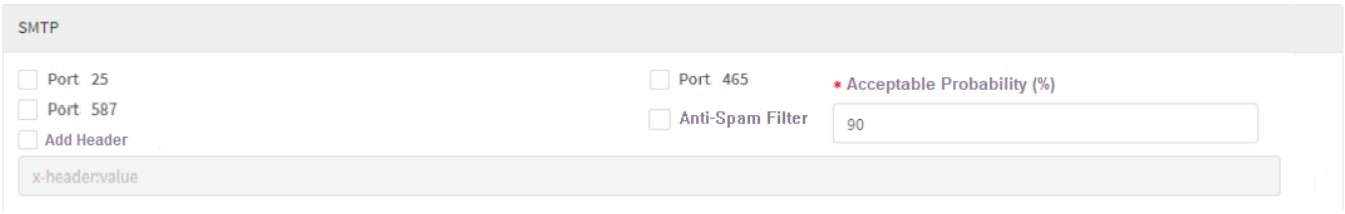
In this section we will cover the SMTP Proxy service, an application integrated with the Blockbit NGFW with the purpose of inspecting the traffic of e-mails between “Client-Server” and “Server-Server” under the SMTP protocol in a secure way.

Its basic function is to enable the administrator through “Security Policies” to handle packets and file transfers through the traffic of SMTP ports, “[25, 465, 587 / TCP]”.

If the traffic is SSL, when enabling SMTP and POP3 proxies it will be necessary to enable an SSL Inspection profile in the IPv4 or IPv6 traffic release policy, for more information on how to create IPv4 policies see this page, for IPv6 see this page.

Configuration

For configuring the SMTP Proxy, review the considerations below:



SMTP Proxy

- **[ ] Port 25:** Enabling the default connection port for Remote SMTP servers. [SMTP - 25/TCP] port. For SMTP port 25 connections it usually applies to connections between SMTP servers;
- **[ ] Port 465:** Enabling the SMTPS port to connect to the SMTP servers over SSL/TLS Remote. [SMTPS - 465/TCP] port. Client-server SSL /TLS traffic requires the source to have a digital certificate that is known to the remote SMTP server;
- **[ ] Port 587:** Enabling the SMTP Submission port to connect to the Remote SMTP servers. [SMTP Sub 587/TCP] port.
- ***[ ] Anti-Spam Filter:*** It is a Spam-Filter function that utilizes a variety of techniques such as DNS filtering and threat classification by punctuation, that analyzes e-mails' content according to the strictness level attributed by the manager. It looks for excess of HTML content and even the domain of the sender's server. Assign a level of acceptability after activating the filter to moderate the level of analysis.

SMTP Submission Traffic requires client-server authentication in the SMTP protocol, which makes it difficult to misuse e-mail accounts or “zombie” machine stations, a method widely used by spammers.

Use this port for client-server connections via email clients. Ex.: “Thunderbird and Outlook”.

- **[ ] Add Header:** This field includes a “Signaling” feature that returns “Informative” content to the user regarding the treatment applied to the E-mail sent in the header of the respective E-mail. Ex .: “x-header: E-mail Infected with viruses.”.

SMTP Proxy - Add Header

The functioning of the SMTP Proxy requires the configuration of a “Security Policy” with the Email Protection content filter enabled for the SMTP protocol

To save all changes, click **[**  **]**.

After saving, for the proxy to take action it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: NGFW - Command queue.

 If it is necessary to integrate the Malware Scanning filter through SMTP Proxy traffic, it will be necessary to enable and configure the Threat Protection service.

Its operation depends on the configuration of profiles by “Security Policies”

Next, we'll look at *POP3* features.

POP Proxy

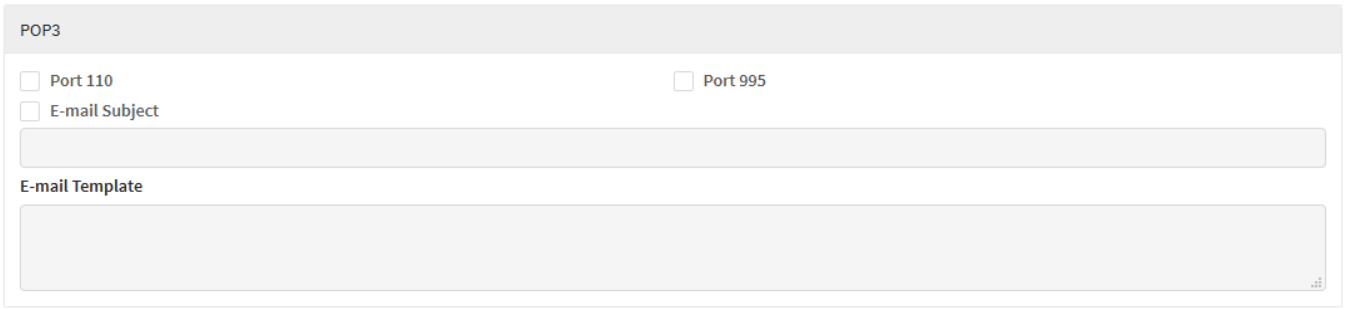
In this section we will cover the POP Proxy service, an application integrated with the Blockbit NGFW in order to inspect the traffic of E-mails between “Client-Server” under the POP protocol in a secure way

Its basic function is to enable the administrator through the "Security Policies" to handle packets and file transfers through the traffic of POP ports, "[110, 995/TCP]"

If the traffic is SSL, when enabling SMTP and POP3 proxies it will be necessary to enable an SSL Inspection profile in the IPv4 or IPv6 traffic release policy, for more information on how to create IPv4 policies see this page, for IPv6 see this page.

Configuration

For configuring the POP Proxy, review the considerations below:



POP3 Proxy

- **[ ] Port 110:** Enabling the default connection port for Remote POP servers. Port [POP3 - 110/TCP];
- **[ ] Port 995:** Enabling the POP3S port connecting to POP3 servers over Remote SSL/TLS. Port [POP3S - 995/TCP]. This feature increases security on POP3 client-server traffic. SSL/TLS traffic requires the source to have a digital certificate that is known to the remote POP server;

Use this port for client-server connections via email clients. Eg: “Thunderbird and Outlook”.

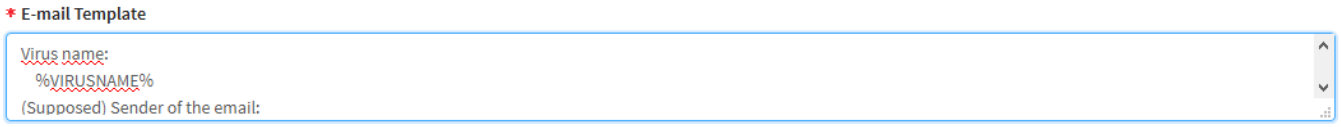
- **[ ] Email Subject:** This field includes a "Signaling" feature that returns a notification E-mail of the type "Mailer Postmaster" to the user regarding the treatment applied to the e-mail received by the POP proxy from the remote POP server;

POP3 Proxy – E-mail Subject

- **E-mail Template:** This field includes the “Body Content” of the **notification email** “sent” to the end user's local mailbox for each email identified as “Infected”. The values of the highlighted fields below correspond to the variable data returned by the “Antimalware” treatment.

```
Virus name:
    %VIRUSNAME%
(Supposed) Sender of the email:
    %MAILFROM%
Sent To:
    %MAILTO%
```

```
On Date:
    %MAILDATE%
Subject:
    %SUBJECT%
Connection data:
    %PROTOCOL% from %CLIENTIP%:%CLIENTPORT% to %SERVERIP%:%SERVERPORT%
```



POP3 Proxy - E-mail Template

The functioning of the POP Proxy requires the configuration of a “Security Policy” with the Email Protection content filter enabled for the POP protocol.

To save all changes, click **[** **]**.

After saving, for the proxy to take action it will be necessary to access the command queue **[** **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

If it is necessary to integrate the Malware Scanning filter through POP Proxy traffic, it will be necessary to enable and configure the Threat Protection service.

Its operation depends on the configuration of profiles by “Security Policies”.

This concludes the analysis of the proxies.

Proxy - SSL Inspection

SSL Inspection works by intercepting SSL traffic and inspecting encrypted content, using this feature it is possible to select the content to be inspected through compliance policies

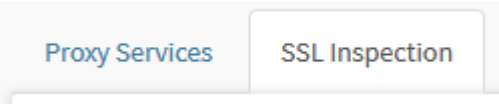
This feature basically acts according to the following steps:

1. Acting Initially, encrypted HTTPS communications are captured between client and server;
2. In order to maintain security, an SSL connection is created;
3. The inspection itself is carried out in a safe way allowing to filter unsafe and unwanted content;
4. Finally, after re-encrypting the information, a new SSL connection is created to continue the communication that was intercepted.

The SSL Inspection profile limit is half the number of CPUs on the appliance.

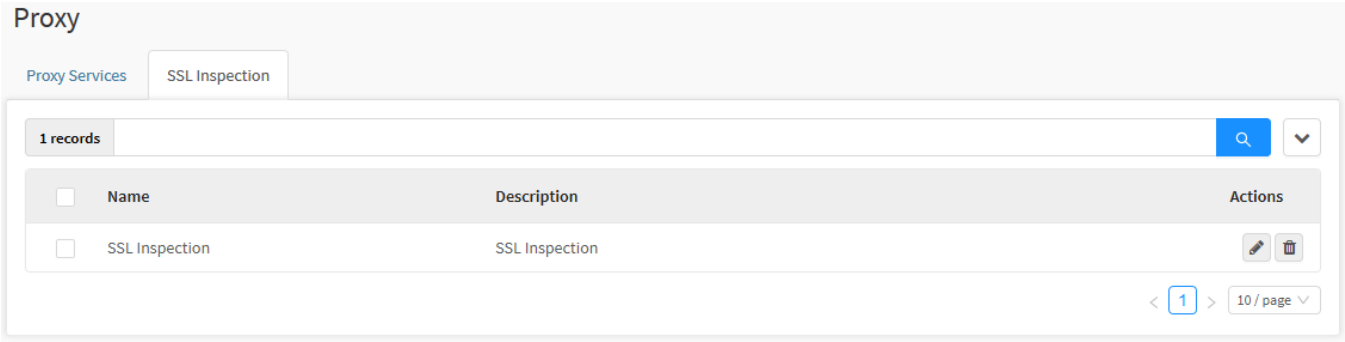
For example: An appliance with 32 CPUs will have a limit of 16 profiles.

Click on the “SSL Inspection” tab.



SSL Inspection tab

The “SSL Inspection” screen will appear. It consists of the columns “Name”, “Description”, “Mode”, “Version” and “Actions”. In addition, at the top right of the screen is the search bar and the actions menu.



Proxy – SSL Inspection

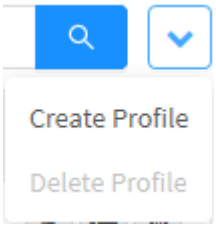
Next, the actions menu will be analyzed and later we will delve into the content of the SSL Inspection panel columns

Proxy - SSL Inspection - Actions Menu

At the top right of the screen we have the actions menu:

SSL Inspection – Actions Menu Button

By clicking on this button the menu below is displayed:



SSL Inspection – Actions Menu

The menu consists of the following options:

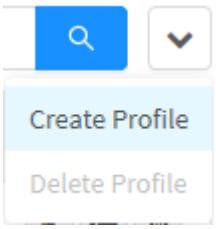
- Create Profile;
- Delete Profile.

Below, each action menu option will be detailed.

Proxy - SSL Inspection - Actions Menu - Create Profile

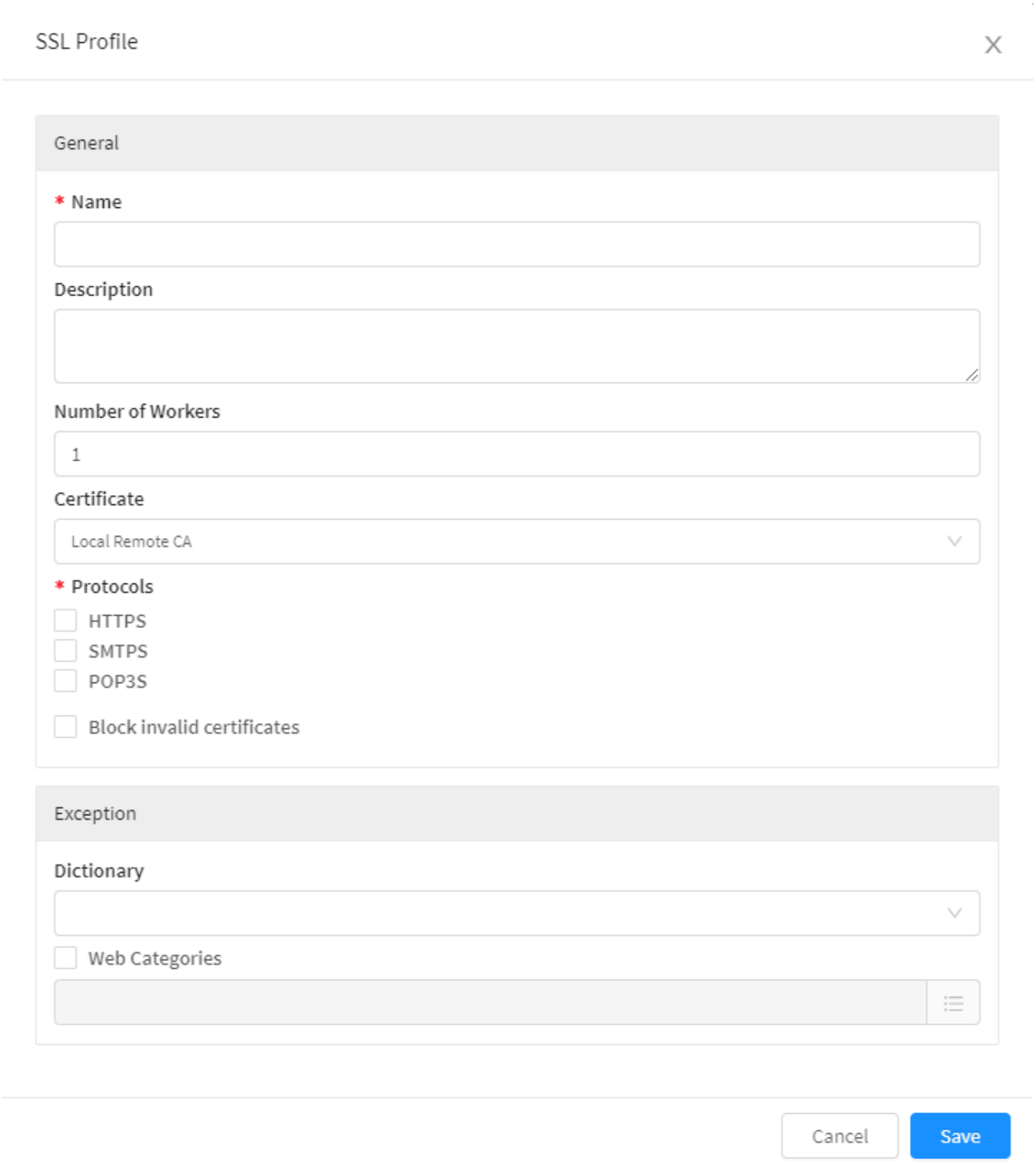
Through the “Create Profile” option, it's possible to create a new SSL Inspection profile. To access, click on the **actions menu [ ]**.

1. Click on the “Create Profile” option;



SSL Inspection - Create Profile

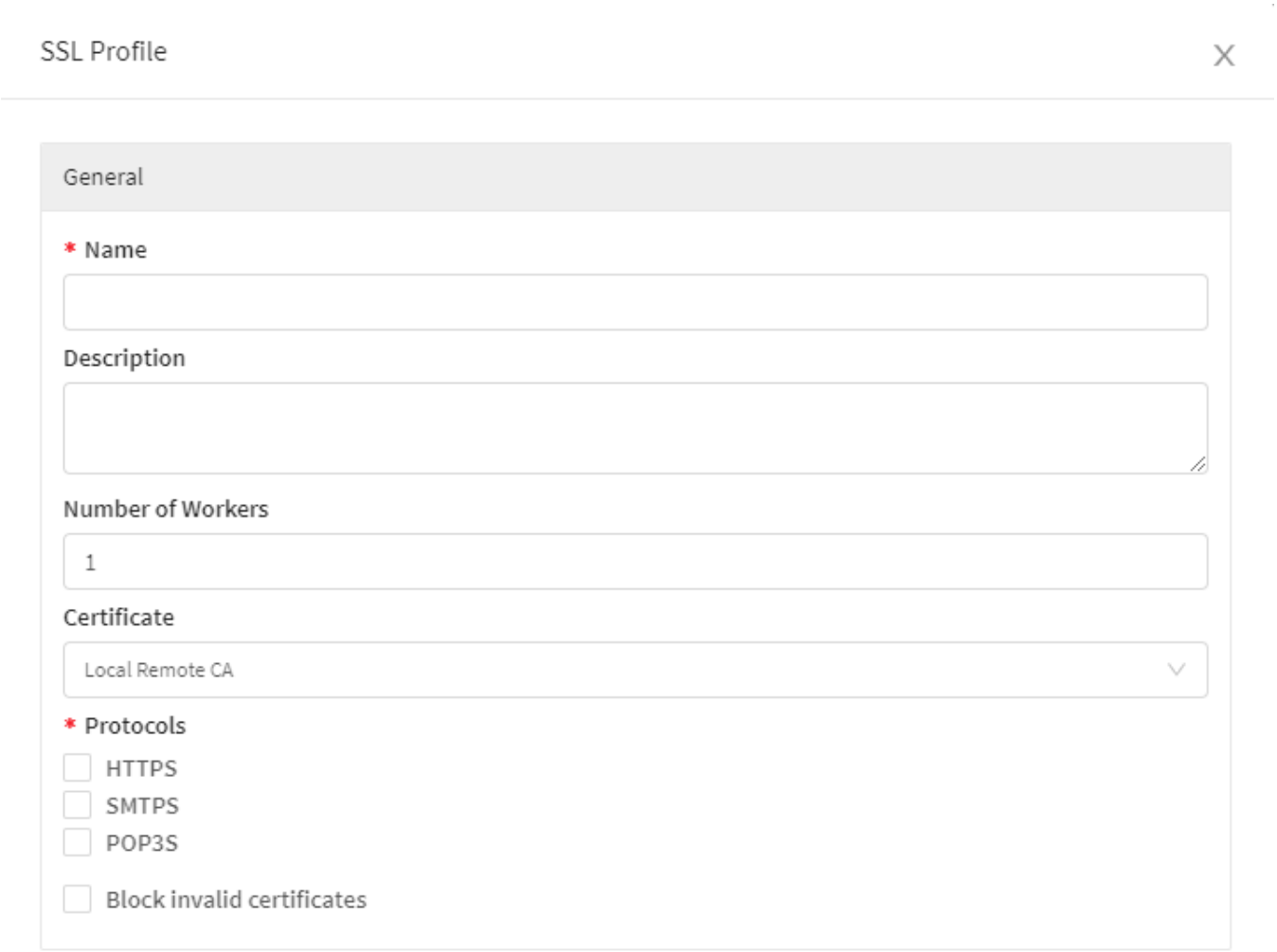
2. The “SSL Profile” screen will be displayed:



SSL Inspection - SSL Profile

General

In this panel the general configurations of the SSL profile are made.



SSL Inspection - SSL Profile - General

- ***Name:*** *Define a name for the profile*. Ex.: *SSL Inspection*;
- ***Description*****:** Set a description for the profile. Ex.: *SSL Inspection;*
- **Number of Workers:** Allows the definition of the number of *workers* (processes) by Inspection profile, limited to the number of CPUs detected automaticaly by the system.
- ***Certificates***: Allows the selection of the CA certificate, that will be used by the Proxy services; It's a mandatory field and in case it's left empty, the certificate that wil be used by the proxy is the one defined by standard in the "Proxy Services" tab;
- ***Protocols:*** Determines in protocols the SSL Inspection will be applied. The available options are: HTTPS, SMTPS and POP3S.
- ***Block Invalid certificates[ ]*****:** If this checkbox has been checked, every time the SSL inspection detects an invalid certificate, a block will be made;

The CA certificate used in the SSL Inspection profile has priority over the one selected in the "Proxy Services" tab.

Exception

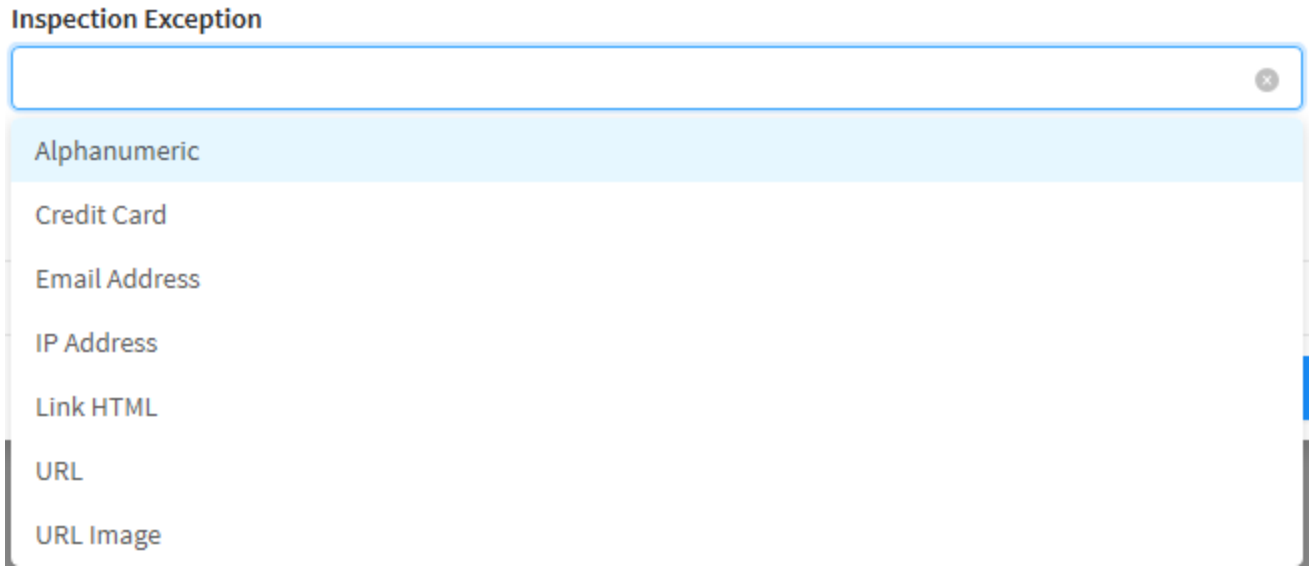
In this panel the SSL profile exceptions are configured.

SSL Inspection - SSL Profile - Exception

- **Dictionary:** Select predefined items as exception for the SSL Profile.
- **Web Categories:** When checking the Web Categories box[ ], it will be possible to select among the available categories, which ones will be marked as exceptions for the SSL Profile.

If an object or a category is added to the SSL exceptions, the packet will not go through the Proxy and Flow-based Inspection Engine modes, from the new Blockbit packet inspection flow, that is, the packet will be forwarded to the Egress Filtering (NAT, IPSec Compression, Traffic Shapping, Routing, etc.).

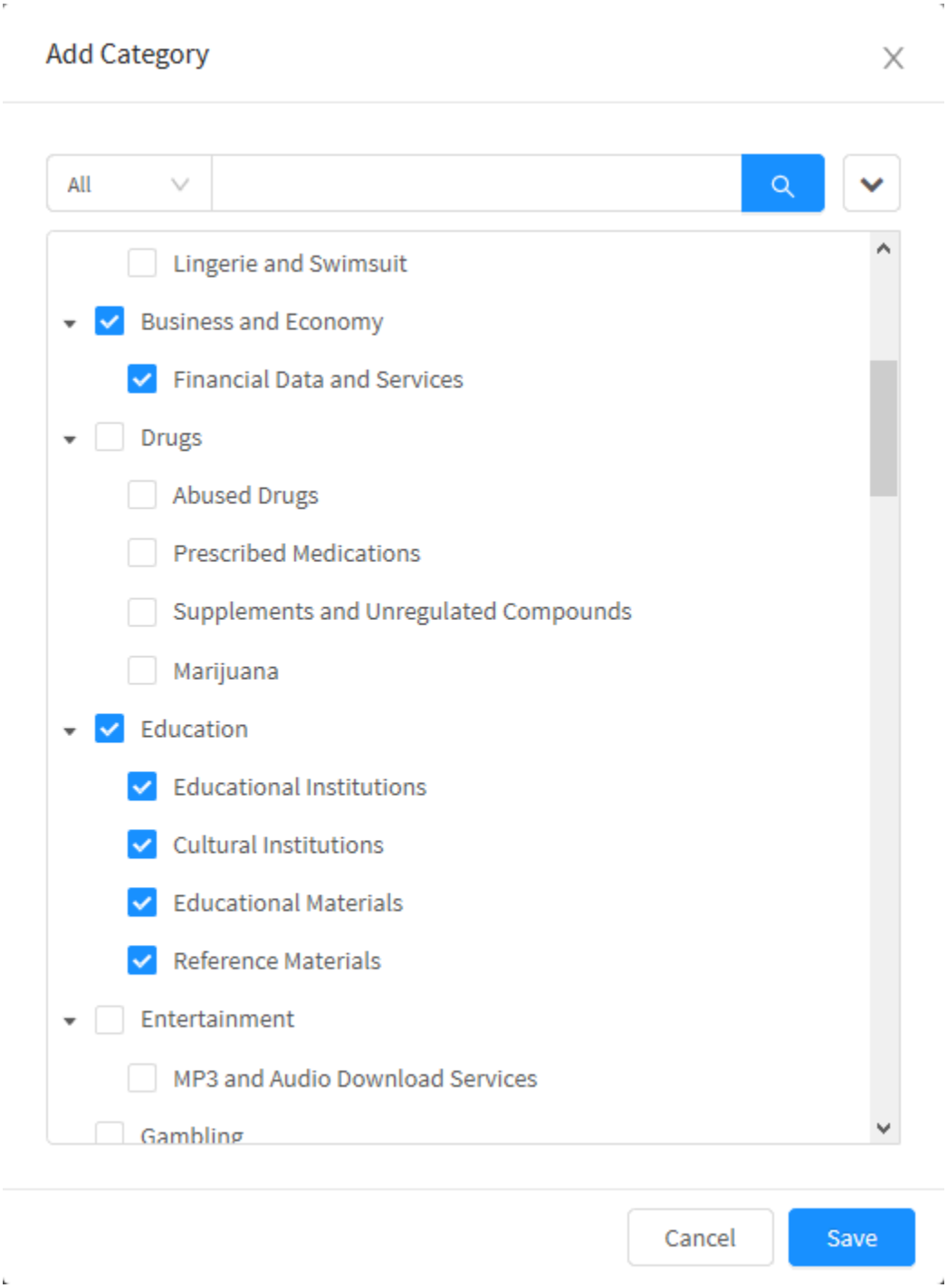
To see the package inspection flow, see the NGFW architecture.



SSL Exception

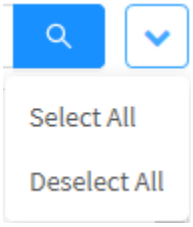
This feature meets the cases of specific conditions of Applications and Services that do not read the system certificates, nor does it have the option to import the certificate in its application, very common cases for services and applications of "Banks, financial institutions and Government", and it is very useful for cases that want to allow the bypass traffic of these services and applications for the entire network;

- ***Web Categories*:** This field follows the same logic as the Inspection Exception field, in Web Categories it is possible to select Web categories to apply “Exception” filters. To select the categories, click on the **[ ]** button, choose the desired categories by checking the checkboxes **[ ]** that will be considered as an exception, as shown below:



SSL Inspection - Add Category

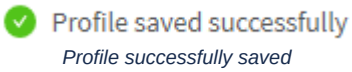
If it is necessary to make a configuration on all items, just select the desired option in the action menu **[ ]**:



SSL Inspection - Add Category - Actions menu

To exit this panel, click the [Cancel] button or click the [Save] button to finish adding the categories.

Finally, if you want to cancel the configuration, click the [Cancel] button. To finish creating the profile click on the [Save] button.



Profile successfully saved

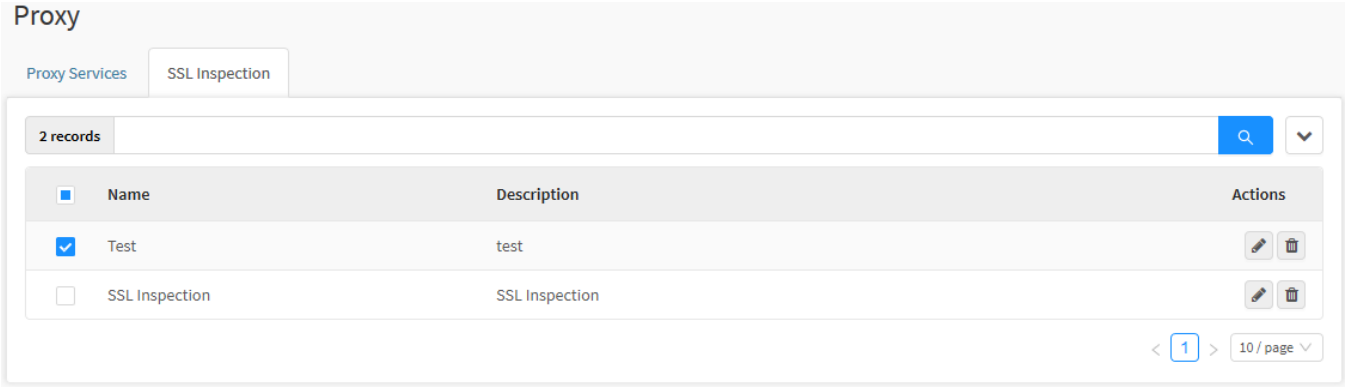
Profile was created successfully.

Next, we will analyze the process of deleting a profile.

Proxy - SSL Inspection - Action Menu - Delete Profile

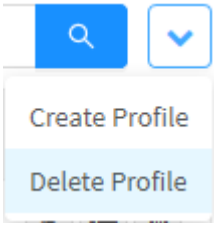
Through the button “Delete Profile” it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Eg: Test;



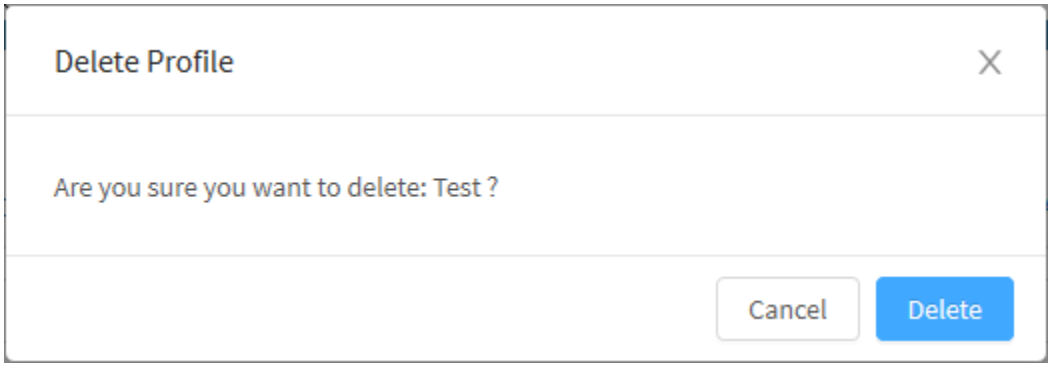
SSL Inspection – Selection of Profiles to delete

2. Enter the actions menu [ ] and click on the option “Delete Profile” .



SSL Inspection – Delete Profile.

3. The notification message will appear asking if you really want to delete the selected Profiles:



SSL Inspection – Message if you want to delete the profiles

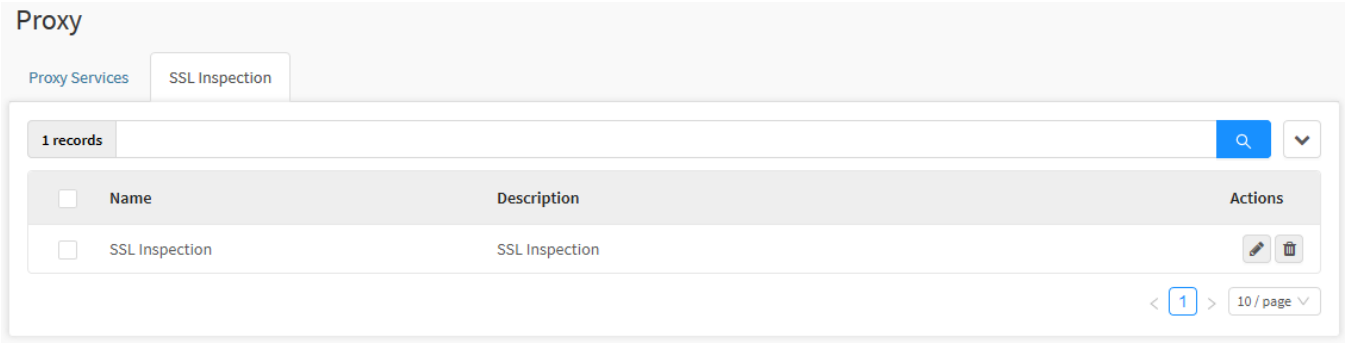
If you want to cancel, click the [Cancel] button. To finish, click the [Delete] button.

Profile successfully deleted

After performing these procedures, the profiles will have been successfully deleted.

Proxy - SSL Inspection - Columns

Below we will explain each column of the SSL Inspection tab:



Profiles – SSL Inspection

We will explain each column below:

- **Checkbox[ ]:** Select profile.
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- ***Actions*:** The “Actions” column consists of several buttons:
    - ***Edit* [ ]:** Allows you to edit the profile settings added in the *Create Profile* option of the actions menu;
    - ***Delete* [ ]:** Deletes the profile, is the equivalent of the *Delete Profile* option in the actions menu.

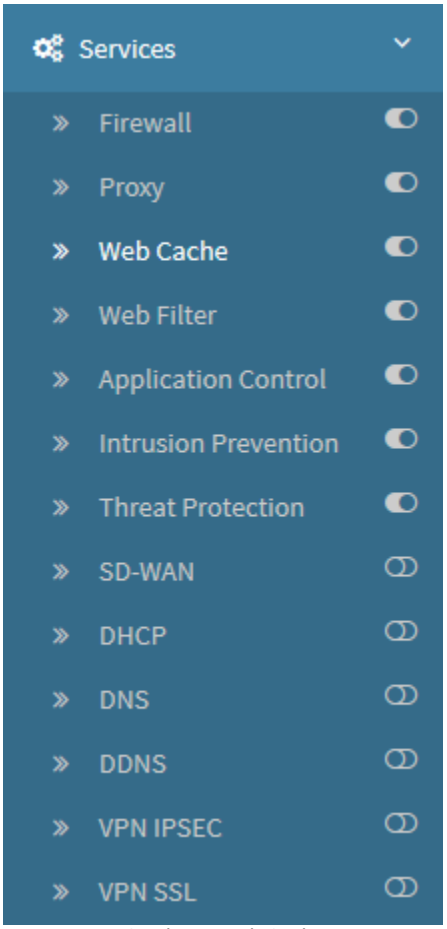
UTM - Services - Web Cache

The "Web Cache" mechanism consists of minimizing the costs of accessing the Web, reducing latency in this type of access is a very important issue, especially when considering that more than 60% of the current internet traffic is generated in the accesses web (HTTP and HTTPS).

The cache system locally stores objects (HTMLS pages, images and files) from the internet, this feature significantly improves the quality of the service offered to users.

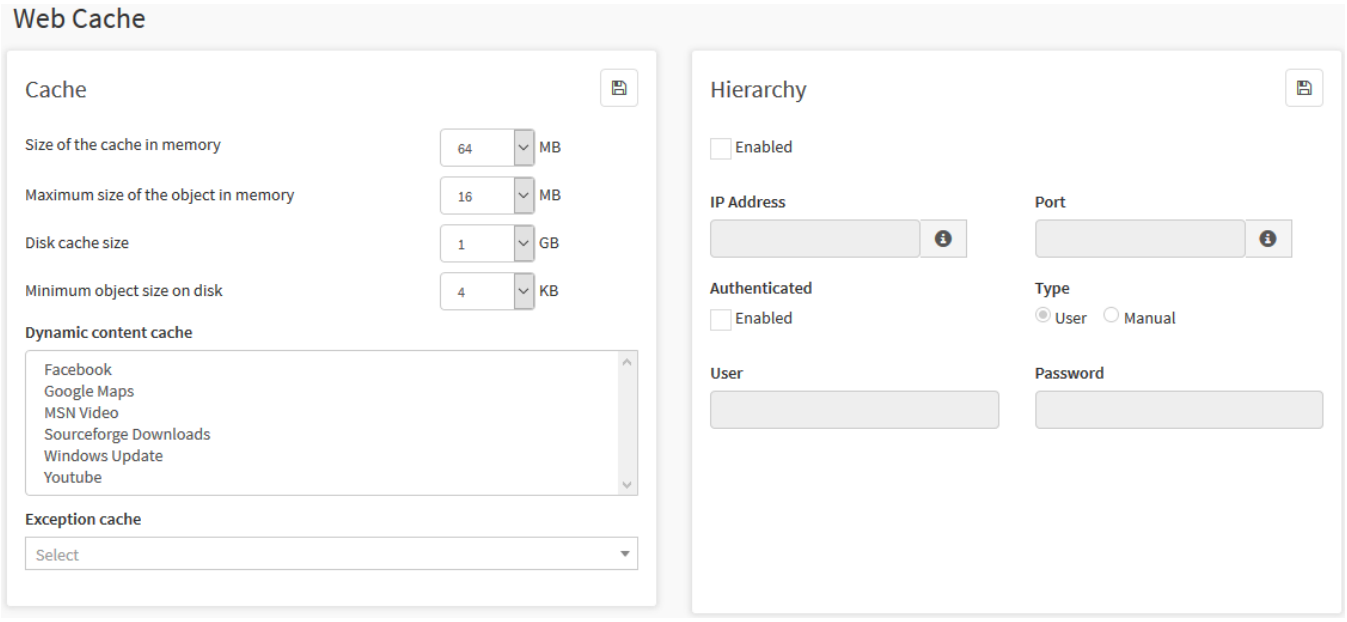
The configuration of the Web Cache service is defined by the configuration of the cache controls and also has the feature of redirecting traffic to a hierarchical proxy.

To access this screen, just select the option “Web Cache”.



Services - Web Cache

The screen below will appear:



Web Cache

The Web Cache screen comprises the following panels:

- *Cache;*
- *Hierarchy*.

Next, we'll look at the components of the Cache panel.

Web Cache - Cache

In the [Cache] table we have the management and control features of the cache service that stores the documents returned from the requested WEB servers on a local basis, this way it is possible to reuse access to these documents without the need to establish a new connection with the remote server.

Memory and disk cache configuration

Maximum and minimum size of the files referring to the Web accesses that will be saved / loaded into memory when the 1st (first) access for immediate delivery to users when requested again.

Dynamic content cache

There are contents that are made available by the WEB servers in a dynamic and distributed way, they are called CDN (Content Delivery Network). This feature uses technology that responds to the user's request for web servers closest to their geographic location.

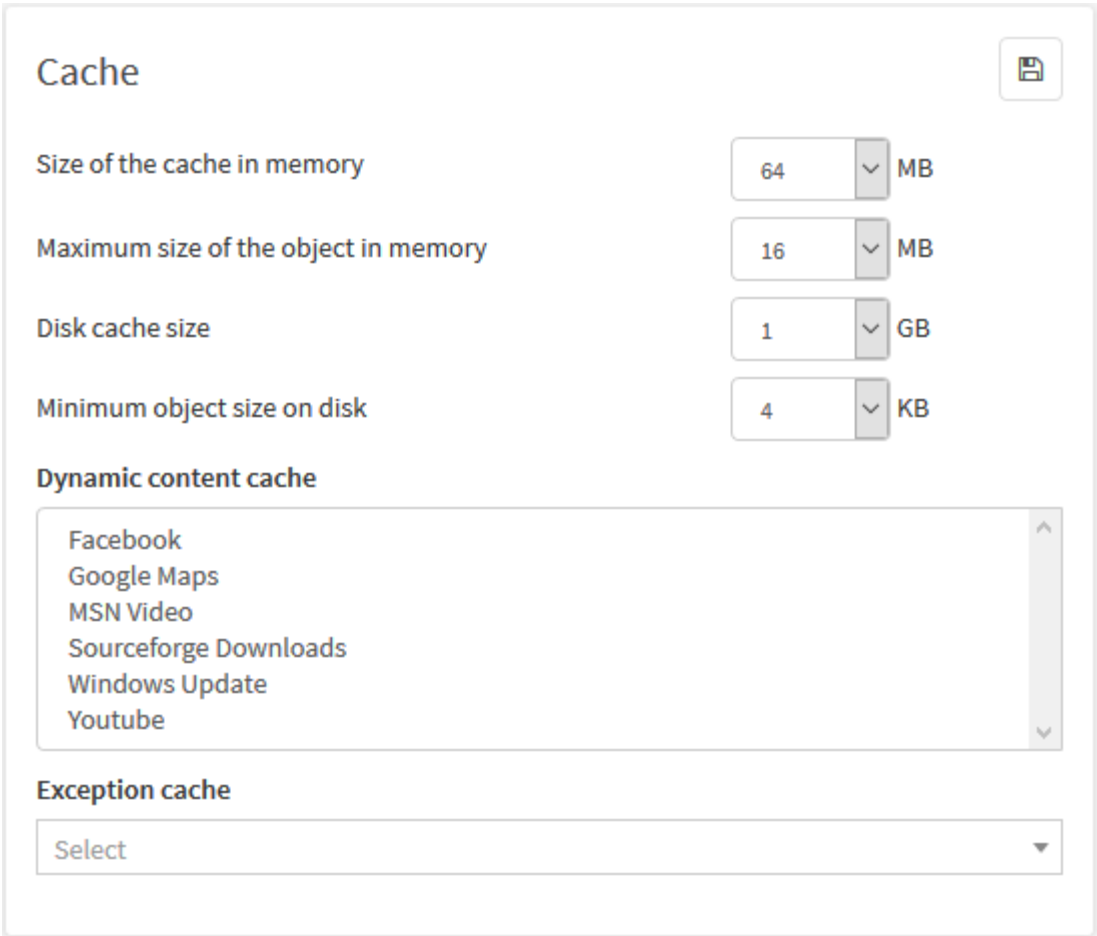
Normally the response to the request is answered dynamically where each server in the stack of servers close to the request responds to fragments of the requested content.

List of supported dynamic content web services:

- *Facebook;*
- *Google Maps;*
- *MSN Video;*
- *Sourceforge Downloads;*
- *Windows Update, Youtube.*

The Blockbit NGFW has a proxy feature capable of concatenating these fragments of the requested content and saving cache even from different sources.

Cache exception, configurable by regular expressions.



Web Cache Settings

*To save all changes, click **[ ]**.*

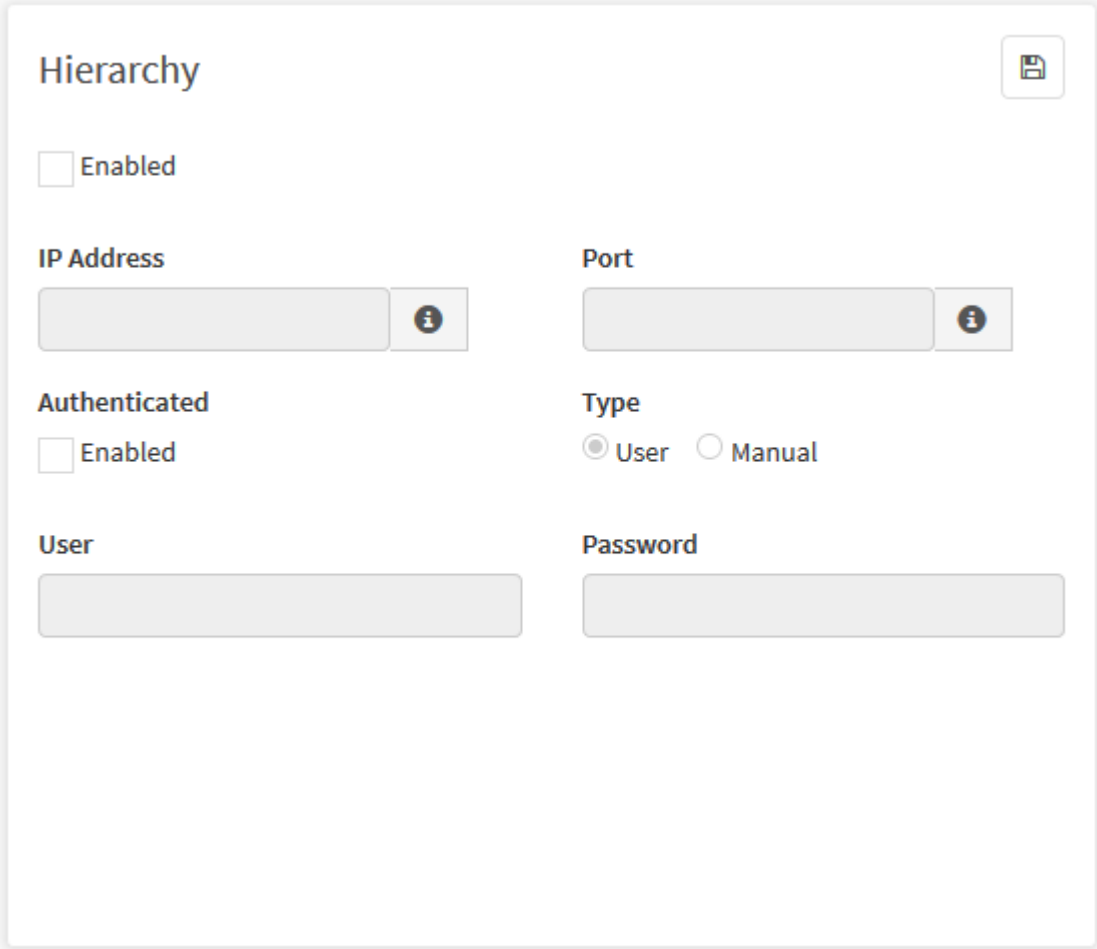
After saving, for the changes to take effect it will be necessary to access the command queue **[ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures, the Cache settings will have been successfully configured.

Web Cache - Hierarchy

In the **[Hierarchy]** box we have the Proxy traffic redirection configuration feature. A hierarchical Proxy model, which acts on the “Proxy Parent” model.

Some structures with subnets require that the traffic of each subnet, even if already managed through a proxy server, redirects its traffic to a hierarchical proxy server, either to apply connection filters by proxy hierarchy or just for consultation in a local cache server before redirecting internet access.



Web Cache - Hierarchy

- ***Enabled[ ]*:** Enables the hierarchical proxy service;
  - ***IPAddress*:** Sets the IP of the remote proxy service;
  - ***Port*:** Defines the port on which the remote proxy service is running.
- ***Authenticated[ ]*:** Defines whether the service will be authenticated or not;
- ***Type*:** Defines whether the type will be per user or manual, as detailed below:
  - ***User*:** The **User authentication method** requests authentication directly from the end user, through “basic” authentication via browser;
  - ***Manual*:** The **Manual authentication method** requests “master” authentication directly to the Proxy, when selecting this option the User and Password fields will be enabled.
- ***User*:** If manual authentication is selected, this field will be enabled, enter the user who will be used to authenticate;
- ***Password:*** *If manual authentication is selected, this field will be enabled, enter the password that will be used to authenticate.*

Some Proxies even though they act as exclusive Parent Proxies to receive redirection, require authentication.

To save all changes, click **[ ]**.

After saving, for the settings to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

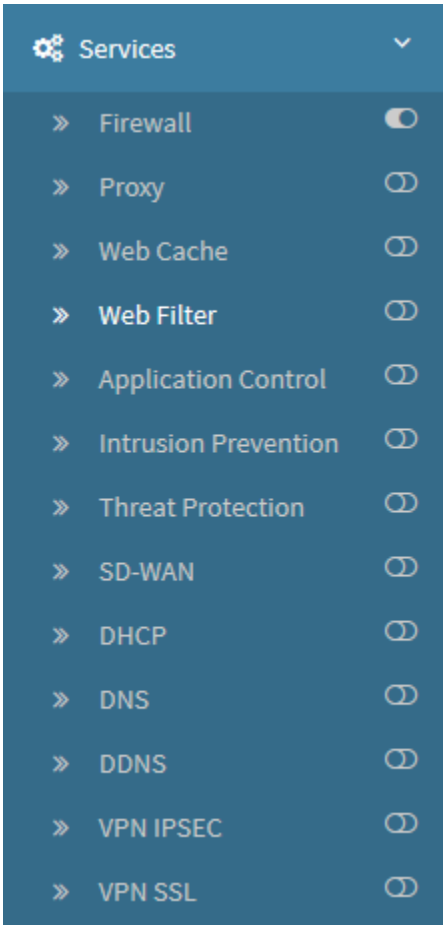
UTM - Services - Web Filter

The Web Filter acts as a second layer to filter users' browsing. It is responsible for the content filter and can only be used when HTTP/HTTPS Web access requests are forwarded by a Proxy server, before requesting data from the remote server, it redirects some information from the request (url, user and IP address for the Web Filter service).

Based on the information sent by the HTTP Proxy, the Web Filter service searches for a filter by category to which it applies, through the “Security Policies”. Depending on how the policies are configured, the Web Filter responds to the proxy if the request was allowed or blocked.

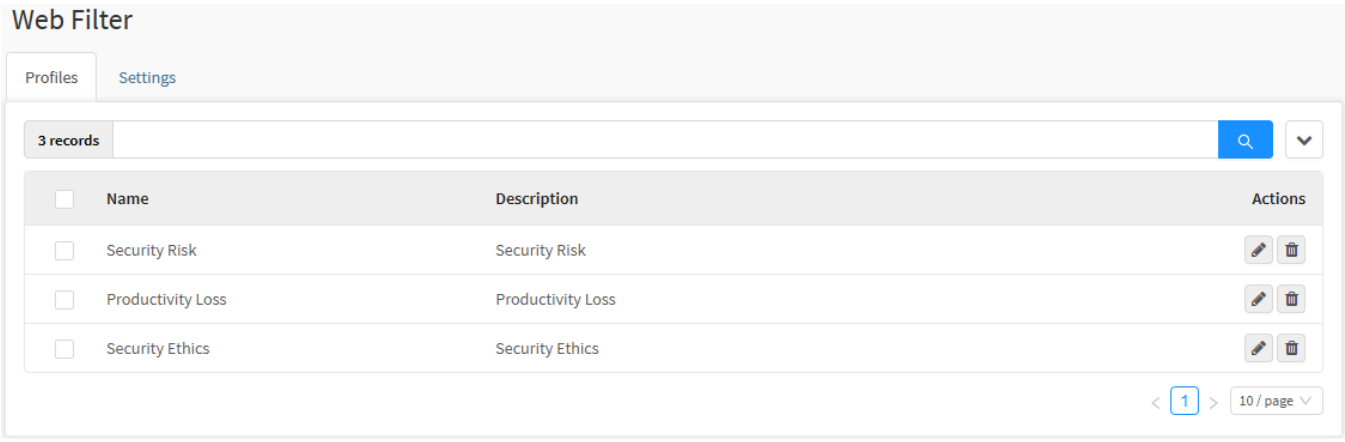
In this item we can manage the resource through the "Update" of the base of URLS of categories, define the "Blocking Message", apply "Login controls by domain for Google services" and also enable the integration of the secure search service "Safe" Search ”for the main web search engines,“ Google, Yahoo and Bing ”.

To access this screen, just select the option “Web Filter”.



Services - Web Filter

The screen below will appear:



Web Filter

The NGFW provides 3 different types of Web Filter by default*:*

- *Security Risk;*
- *Productivity Loss;*
- *Security Ethics.*

The Web Filter screen has the following tabs:

- *Profiles;*
- *Settings*.

Next we will analyze the components of the *Profiles* tab

Web Filter - Profiles

The system allows the application of several content filter profiles in the same connection context (Source, Destination, User). That is, when detecting a policy where a specific type of HTTP or HTTPS traffic is applicable, the system considers the URL in the policy's search parameters (Lookup).

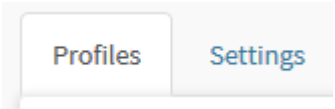
In Content Filter profiles it is possible to Allow, Block and Disable categories. A policy that has a Web Filter enabled takes into account only the URLs whose categories have been allowed or blocked in the Profile, if the URL is disabled, the service will move on to the next policy where the HTTP connection context matches, if there is no policy that applies, the URL will be blocked, the same is true for web-type applications if the application control is active.

This table shows the behavior if the request matches Web Filter and Application Control categories:

Application Control	Web Filter Category	Behavior
Without inspection control	Without inspection control	Allow access
Without inspection control	Disabled	Next policy
Without inspection control	Refuse	Block access
Without inspection control	Allow	Allow access
Allow	Without inspection control	Allow access
Block	Without inspection control	Block access
Disabled	Without inspection control	Next policy
Disabled	Disabled	Next policy
Disabled	Allow	Allow access
Disabled	Refuse	Block access
Allow	Disabled	Allow access
Allow	Allow	Allow access
Allow	Refuse	Block access
Block	Disabled	Block access
Block	Allow	Block access
Block	Refuse	Block access
Do not match any policy		Block access

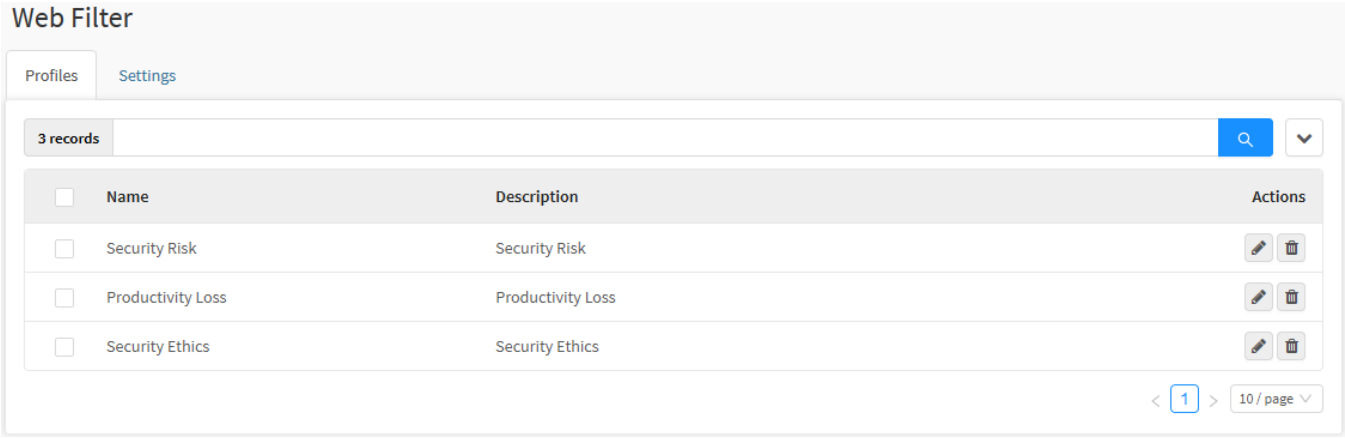
For more information on application control, see this page.

If the tab is not selected, click on "Profiles".



Profiles tab

The “Profiles” screen of Web Filter will appear, as shown by the image below:



Web Filter - Profiles

This session will cover how to register, edit and remove Web Filter profiles;

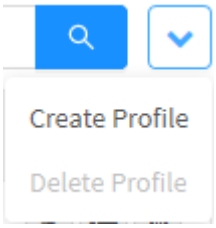
Next, we'll look at the functions located at the top of this panel.

Web Filter - Profiles - Actions Menu

At the top right of the screen we have the actions menu:

Web Filter – Actions Menu Button

By clicking on this button the menu below is displayed:



Web Filter – Actions Menu

The menu consists of the following options:

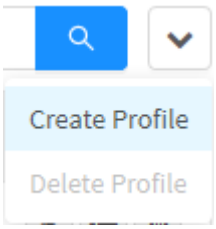
- *Create Profile*;
- *Delete Profile*.

Next, each action menu option will be detailed.

Web Filter - Profiles - Actions Menu - Create Profile

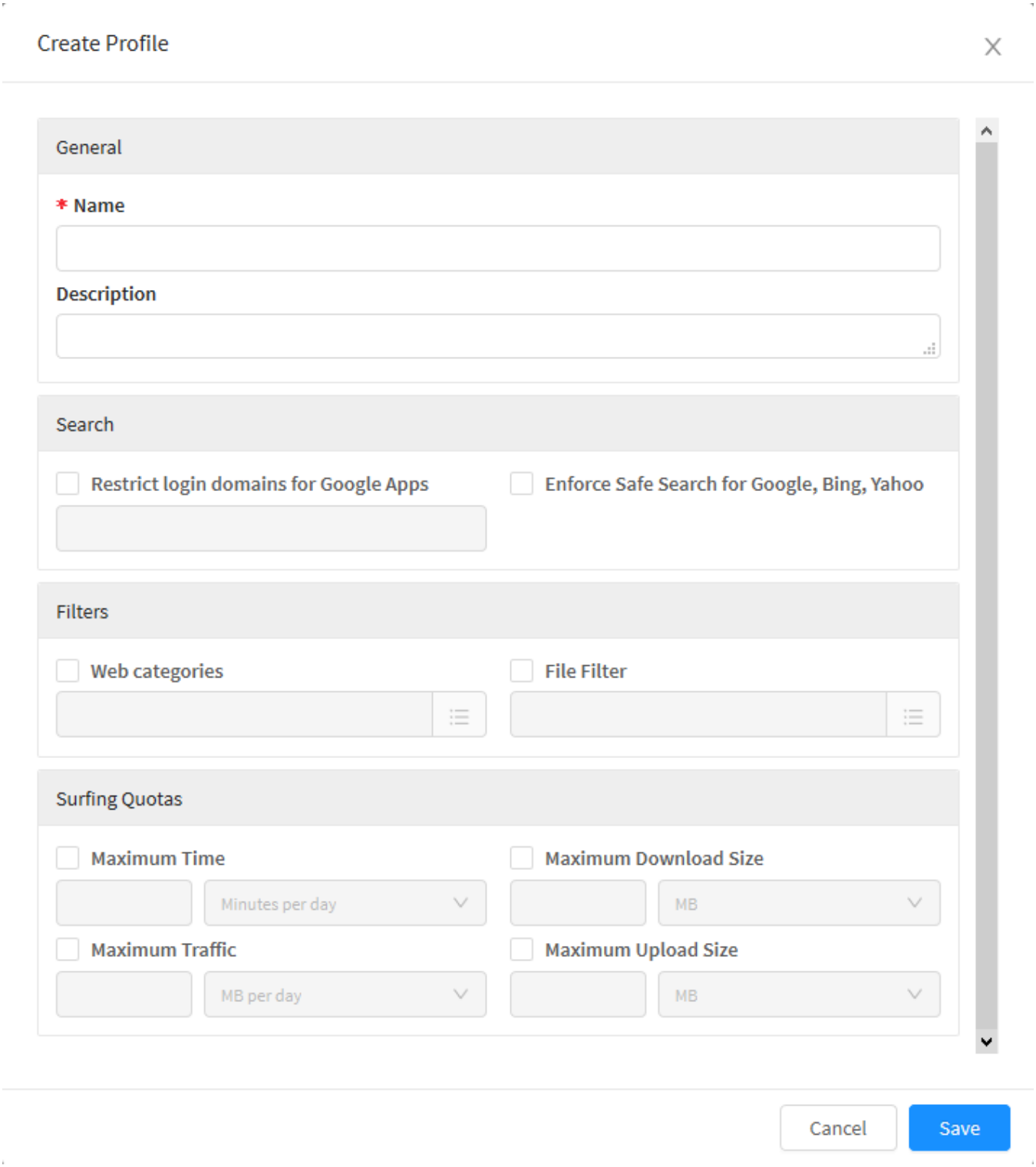
Through the option “Create Profile” it is possible to create a new Web Filter profile. To access, click on the actions menu **[**  **]** button.

1. Click on the “Create Profile” option;



Web Filter - Create Profile

2. The “Create Profile” screen will be displayed. As shown by the image below:



Create Profile

In this window it is possible to make the general configurations, configure filters and quotas that will be used in this profile. Next we will analyze each panel in this window:

General

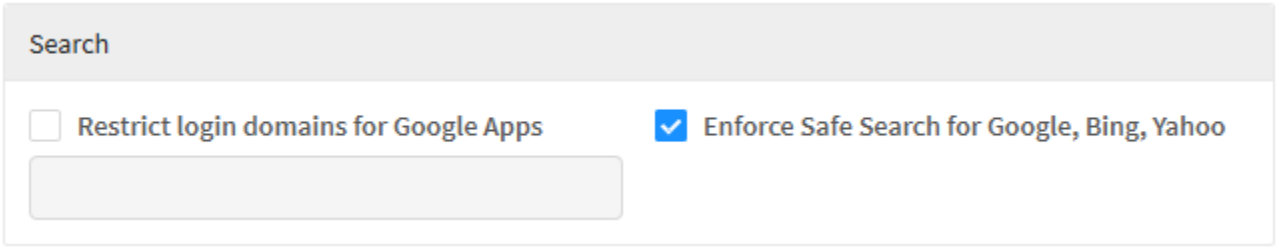
In "General" we have the following text boxes:

Web Filter – General

- ***Name:*** *Define a name for the profile*. Ex.: *Webfilter*;
- ***Description*****:** Set a description for the profile. Ex.: *Webfilter.*

Search

In "Search" it is possible to manage how the search services will be accessed:

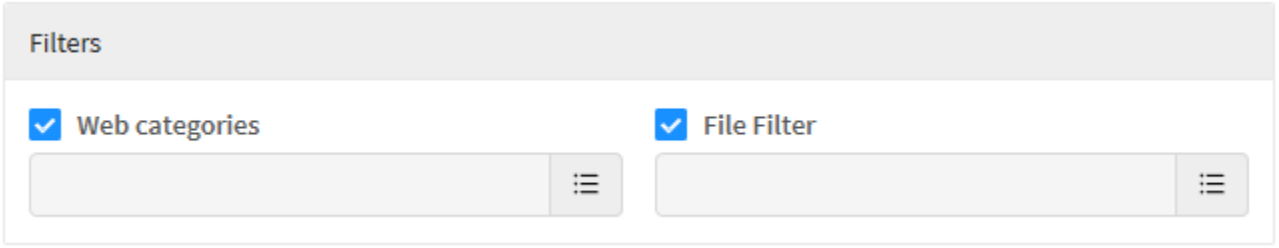


Web Filter - Search

- ***Restrict login domains for Google Apps[ ]:*** *This option allows you to control which domains will access Google Apps*;
- ***Enforce Safe Search for Google, Bing, Yahoo[ ]*****:** This check box forces Safe Search to be activated on search engines. *The NGFW supports Google's Safe Search filters that provide the ability to prevent sites with inappropriate content from appearing in your search results*. This feature applies a secure search filter directly to users' “Search” actions on their workstation from browsers. This secure search feature applies to the main web search engines (Google, Yahoo and Bing).

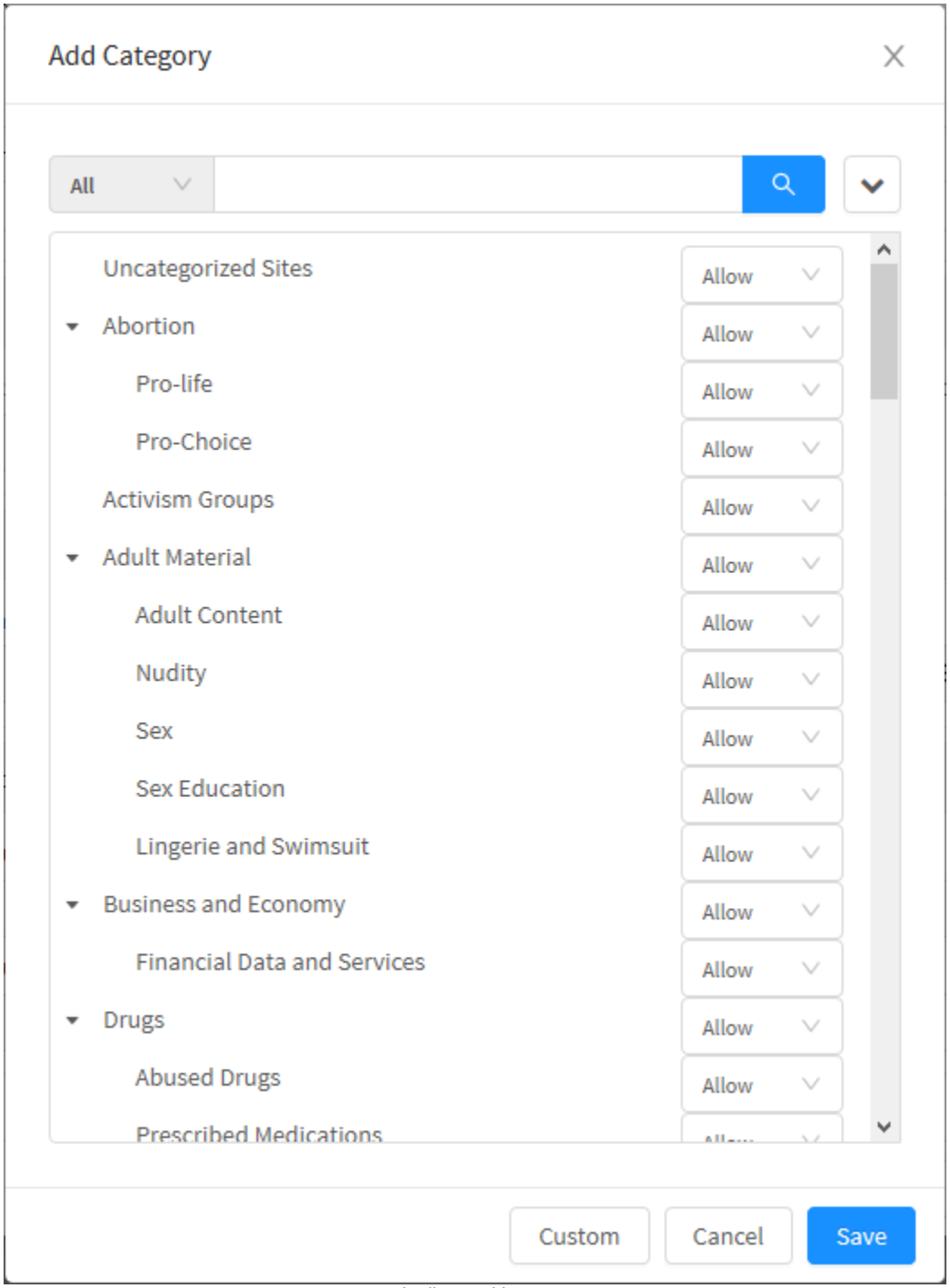
Filters

In "Filters" the following options are available:



Web Filter - Filters

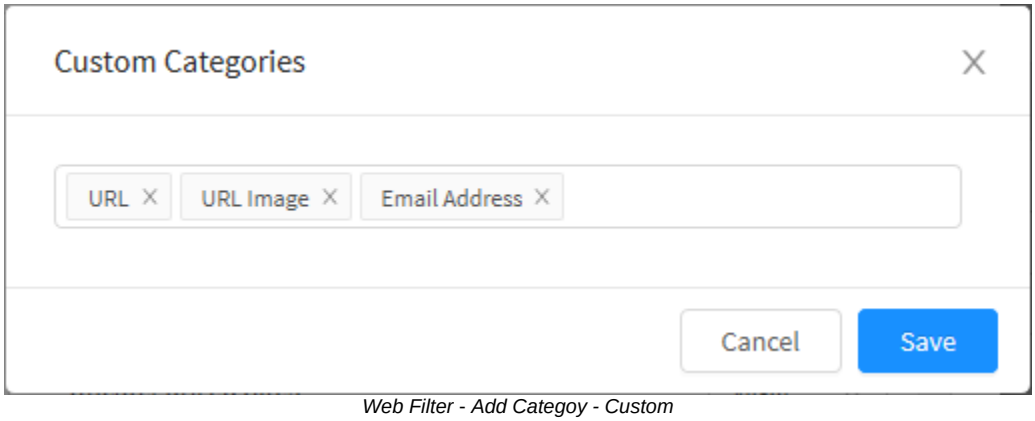
- ***Web categories [ ]:*** *Allows you to select the web categories to apply "Block" or "Exception" filters to the set of applied policies*. To select the categories, click the ***[ ]*** button, choose the desired categories and then select **Allow**, **Block** or **Disable**. In the actions menu **[ ]**, it is also possible to apply any of these options in all categories in ***Allow All***, ***Block All*** and ***Disable All*** to disable them. Below is a brief description of the function of each action:
  - **Allow:** Access to URLs classified with this category is allowed;
  - **Block:** Access to URLs classified under this category is blocked;
  - **Disable:** This category is disabled, this means that the Web Filter will ignore it and will only consider URLs in allowed or blocked categories.



Web Filter - Add Categoy

For more information about the categories displayed in this panel, see the section *Diagnostics - Category Lookup*

It is also possible to add custom categories by clicking on the **[** Custom **]** button;



Web Filter - Add Categoy - Custom

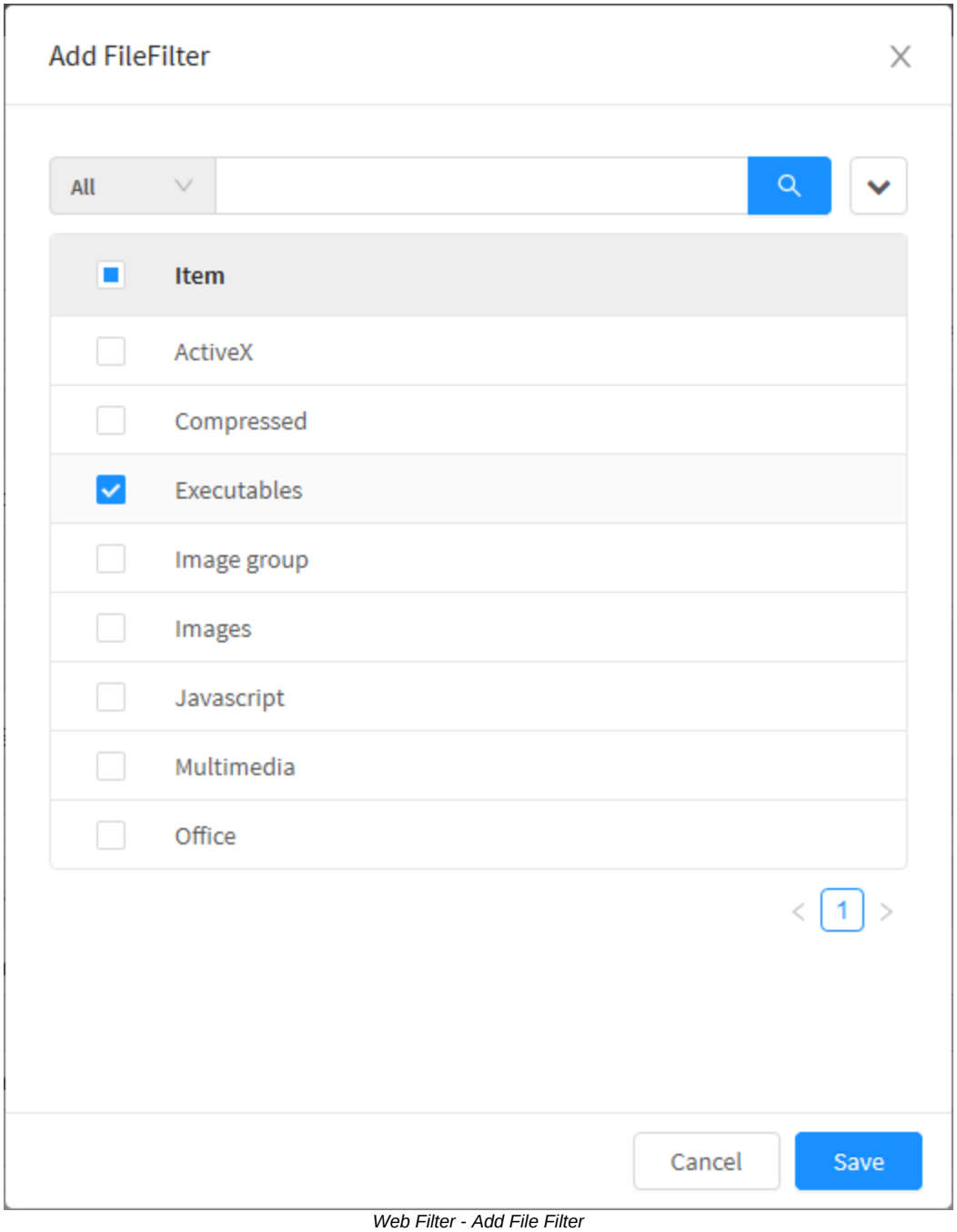
Click in the field and select the desired category, in this field dictionary type objects will be available, the selected objects will be added as tags. Finally, click the **[** Cancel **]** button to exit this window or click the **[** Save **]** button to save.

To finish adding the categories, click the **[** Save **]** button to save or click the **[** Cancel **]** button to exit this window.

- ***File Filter [ ]:*** Allows you to select the file types added in *Objects - Contents* (which are objects created with Mime-types e Extensions: doc, ppt, exe, pdf, bat, dll, ocx, wmi, jpeg, mpeg, etc) to apply filters to the set of applied policies and therefore, check the trafficked files among applications type: P2P, IM, SMB. To select the objects, click on the ***[ ]*** button, and enable the desired checkboxes. In the action menu, you can also click **Select All** to check all or **Deselect All** to deselect all categories:

File Transfer Control: Enables the creation of filters for files and predefined data, and identified by extension and signatures. It also has the capacity of identifying and preventing the transfer of files by type (ex: doc, ppt, exe, pdf, bat, dll, ocx) even if within applications like: P2P, IM and SMB.

It enables the compacted files identification and the application of policies over these kinds of files. It is also able to identify and prevent the transfer of sensitive information (ex: credit card number) enabling the creation of new types of data via regular expression.

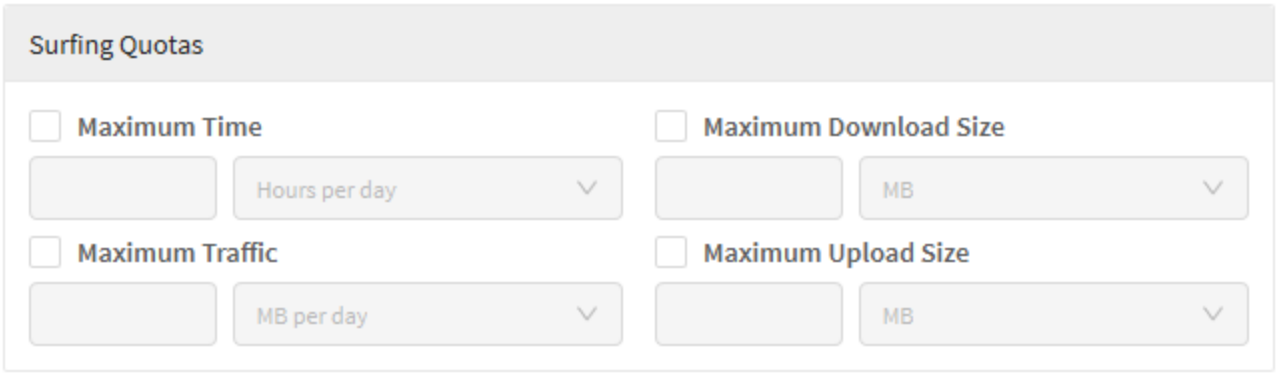


Web Filter - Add File Filter

Click the [Cancel] button to cancel. Click the [Save] button to save.

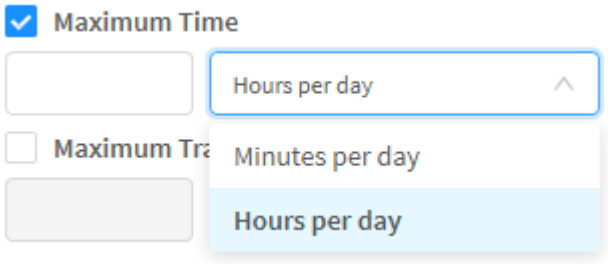
Surfing Quotas

In "Surfing Quotas" the following panel is displayed:



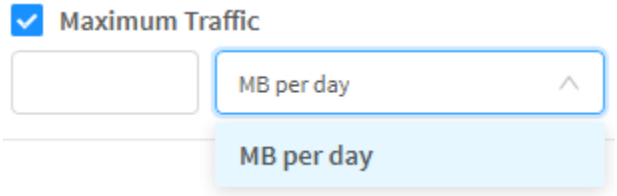
Web Filter - Surfing Quotas

- [☑] ***MaximumTime*:** Allows you to set a time share in minutes or hours per day.



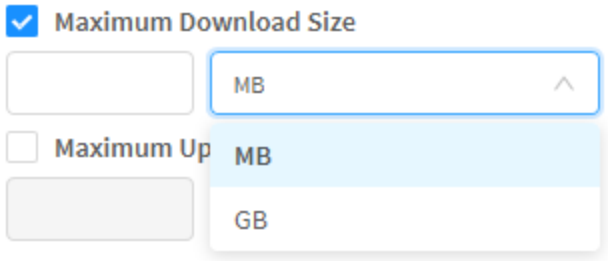
Web Filter – Maximum Time

- [☑] ***Maximum Traffic*:** Allows you to configure a share of traffic in MB per day.



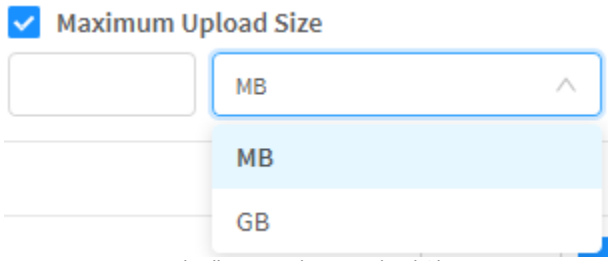
Web Filter – Maximum Traffic

- [☑] ***Max Download Size*:** Allows you to configure the maximum download size, in MB or GB.



Web Filter - Maximum Download Size

- [☑] ***Max Upload Size*:** Allows you to configure the maximum upload size, in MB or GB.



Web Filter - Maximum Upload Size

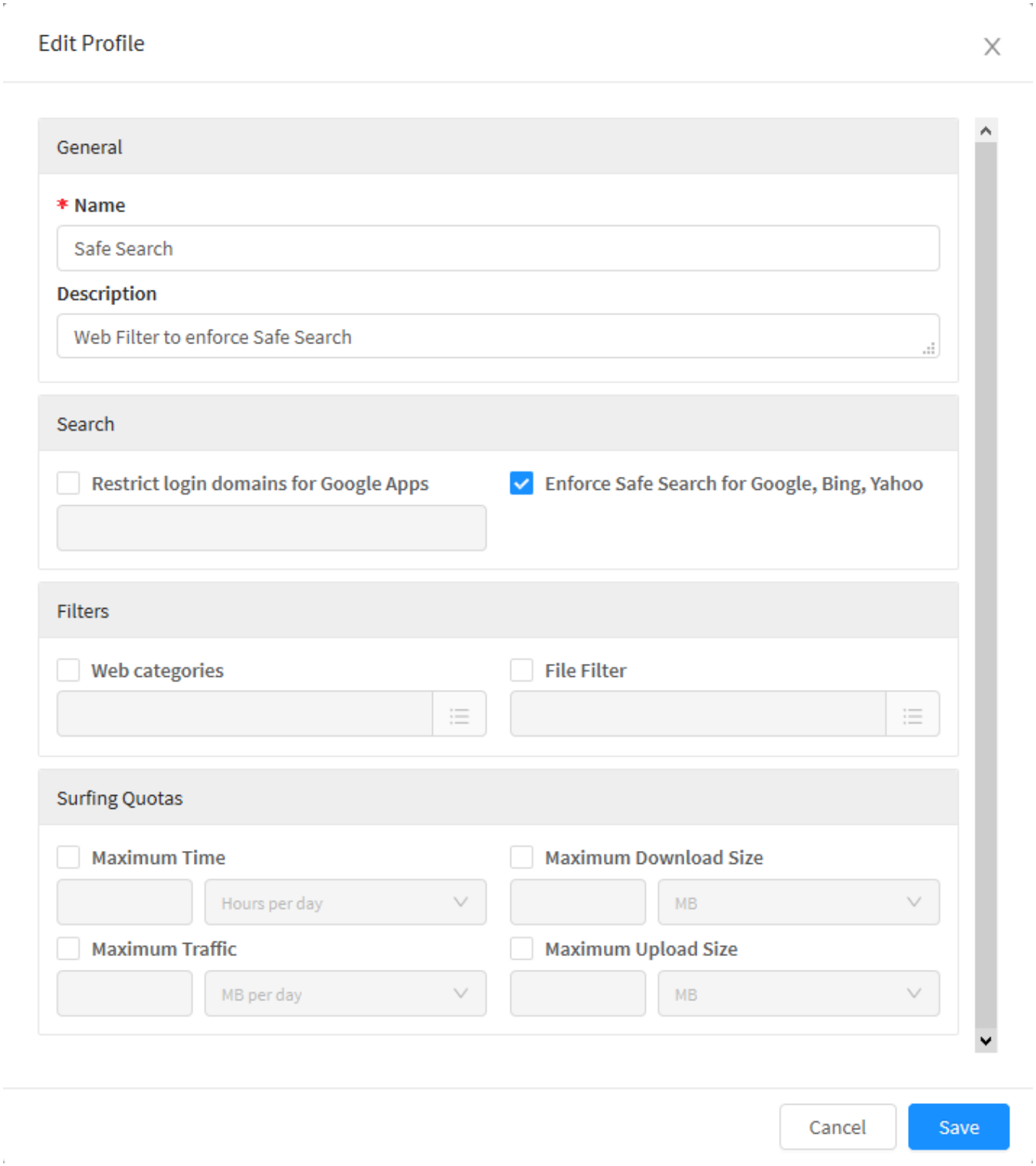
The settings made in the profile can be added to a policy on the *Inspection* tab in the Web Filter option.

After completing all settings, click the [Cancel] button to return to the Profiles panel or click the [Save] button to save.

To view an example configuration, go to this page.

Web Filter - Example: Safe Search configuration

Next, the necessary configuration for Safe Search operation on the local network will be exemplified. In this case, a Web Filter was created simply by forcing Safe Search.

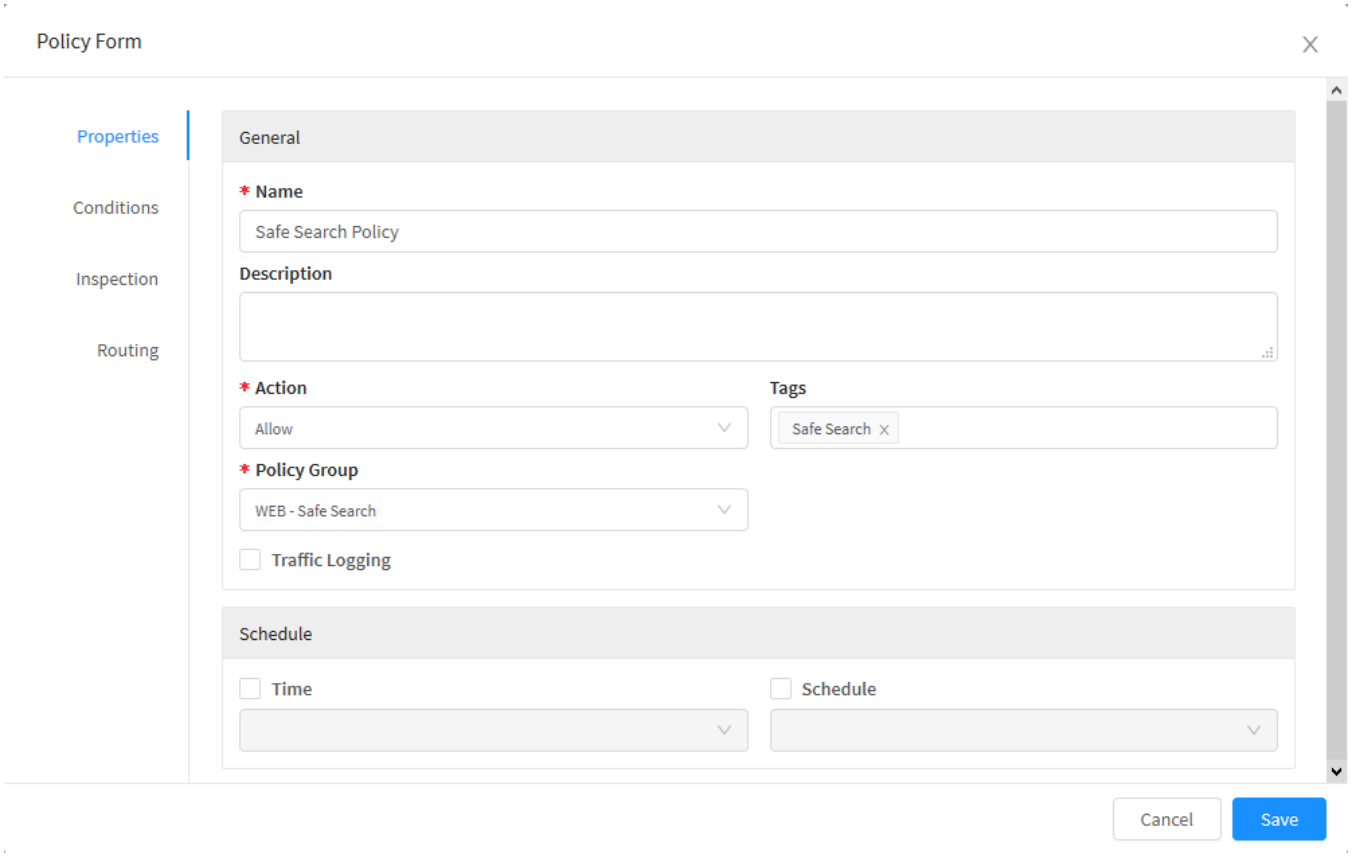


Web Filter - Safe Search

In the Properties tab:

- ***Name:*** *Safe Search;*
- ***Description:*** *Web Filter to Enforce Safe Search;*
- ***Enforce Safe Search for Goole, Bing, Yahoo[☑]:*** Make sure the checkbox is marked*;*

After performing the above configuration, you will need to create a policy as shown in the image below.

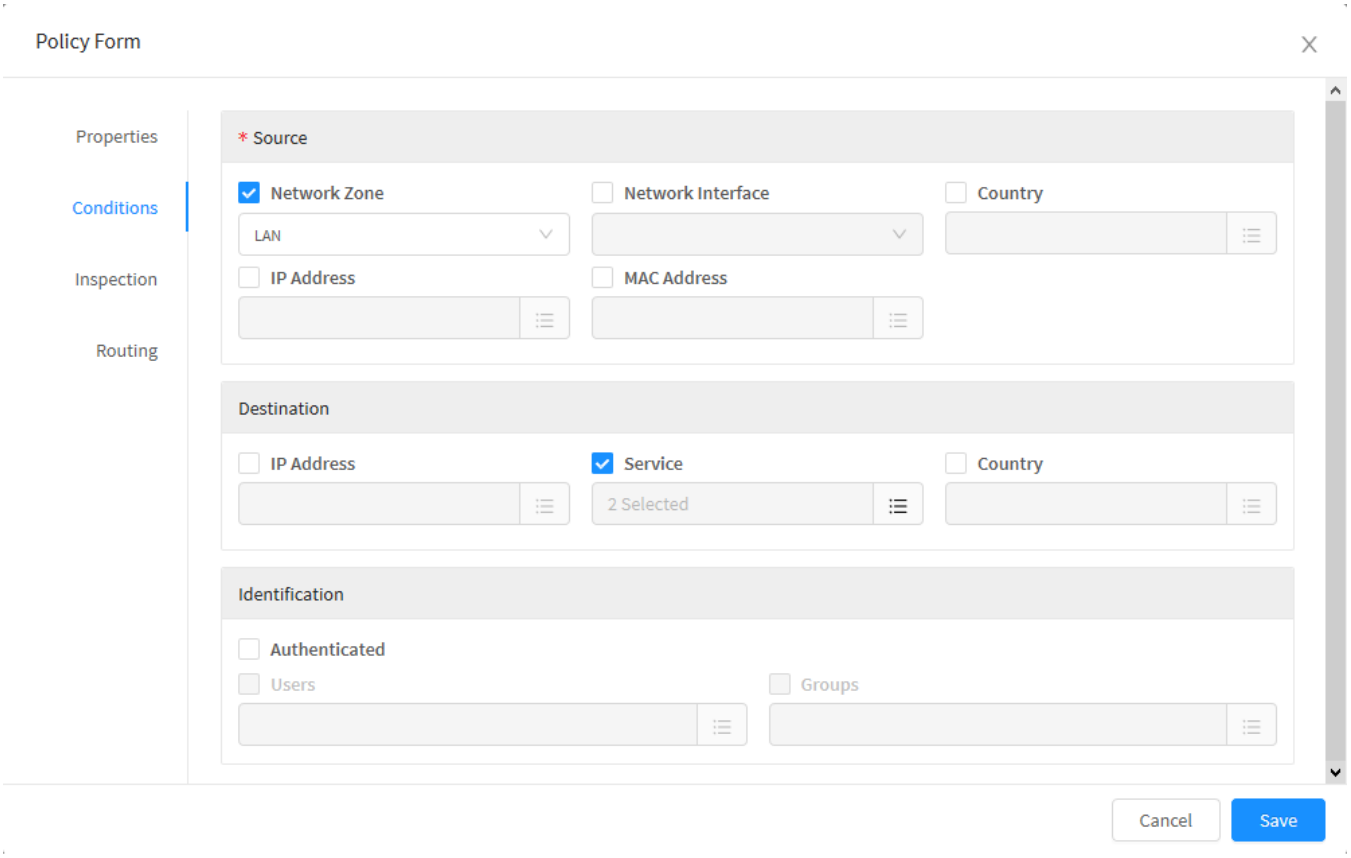


Web Filter - Policy - Properties

In the Properties tab:

- ***Name:*** *Safe Search Policy;*
- ***Action:*** *Allow;*
- ***Policy Group:*** *WEB - Safe Search;*
- ***Tags:*** *Safe Search.*

Then access the Conditions tab:

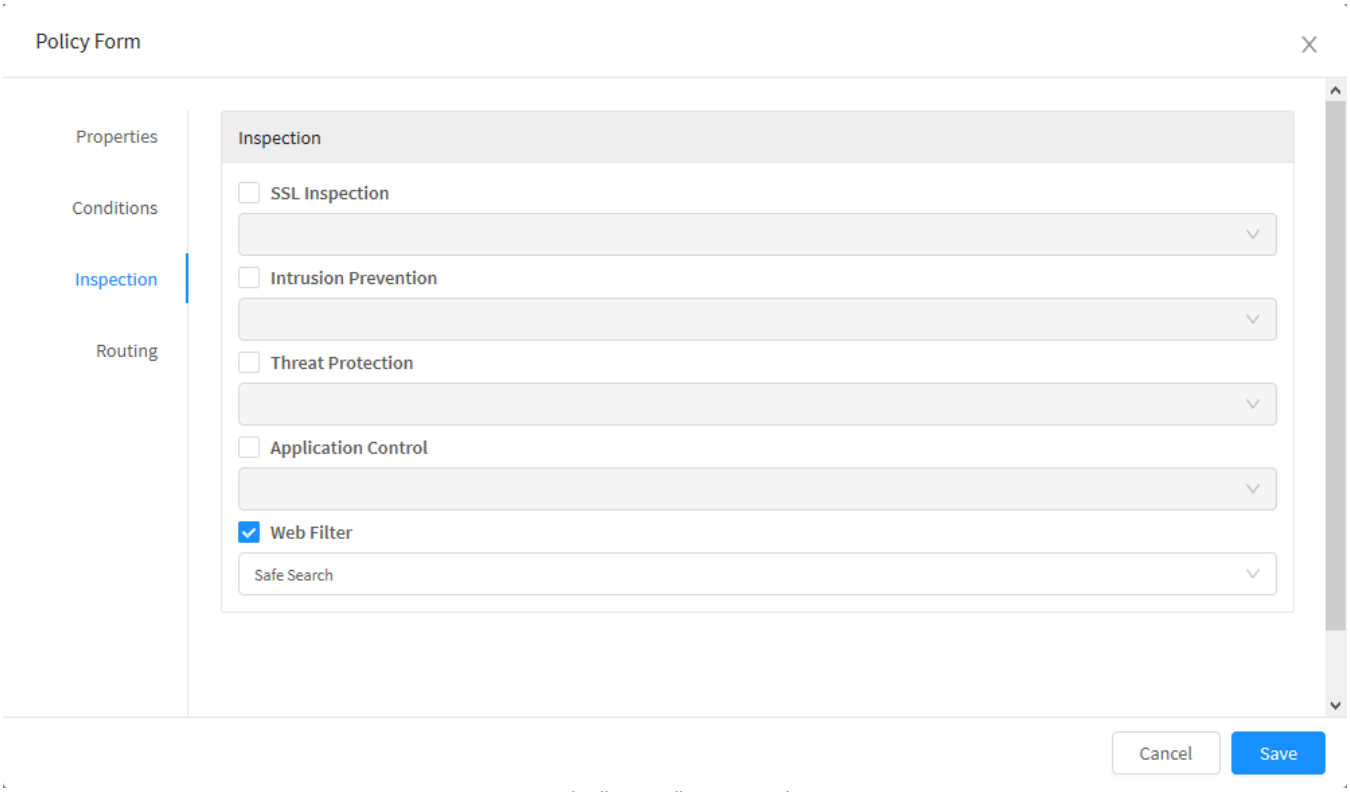


Web Filter - Policy - Conditions

In the Conditions tab:

- ***Network Zone[✓]:*** *LAN;*
- ***Service[✓]:*** *HTTP* and *HTTPS.*

Then access the Inspection tab:

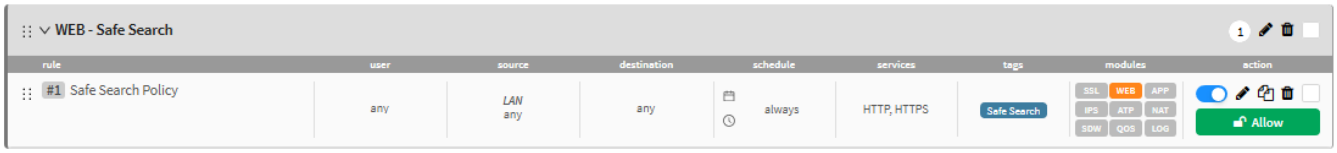


Web Filter - Policy - Inspection

In the Inspection tab:

- ***Web Filter[ ]:*** *Safe Search (or the name of the Web Filter created at the beginning).*

You will have arrived at the result shown below:



Política *WEB - Safe Search*

At the end of this step, Safe Search will take effect.

For correct functioning in the Google Chrome browser and to perform a secure search on Google, it will be necessary to block port 443 UDP, as the Proxy can only perform this SSL inspection on TCP traffic.

Web UDP 443 Block

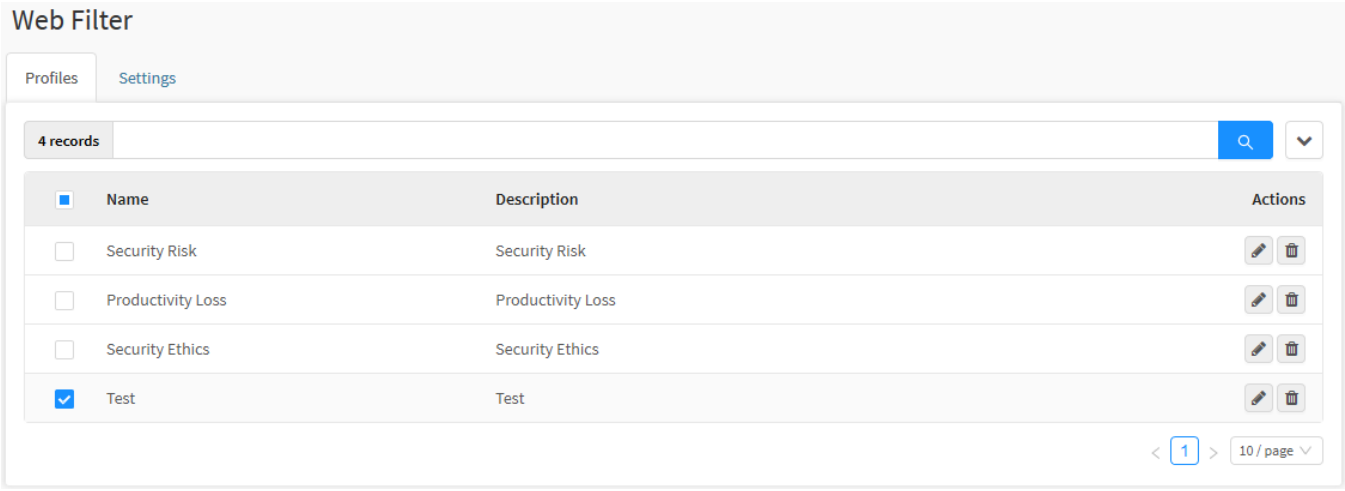
For more information on policies, see the chapter Policy.

Next, we'll detail how to remove a Web Filter profile.

Web Filter - Profiles - Actions Menu - Delete Profile

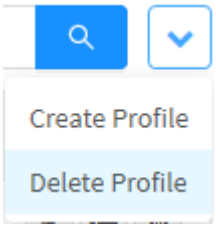
Through the button “Delete Profile” it is possible to delete the selected Profiles. To delete from the Actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Example: Test;



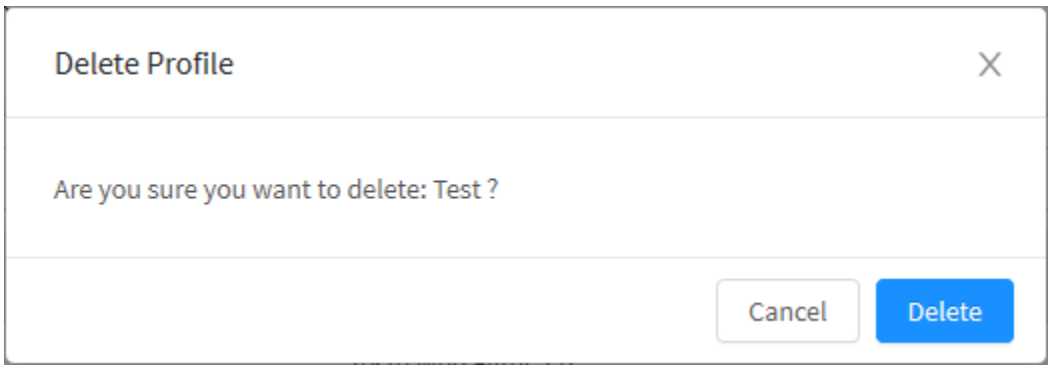
Web Filter – Selection of Profiles to delete

2. Enter the actions menu [ ] and click on the option “Delete Profile”.



Web Filter – Delete Profiles

3. The notification message will appear asking if you really want to delete the selected Profiles:



Web Filter – Profile deletion message

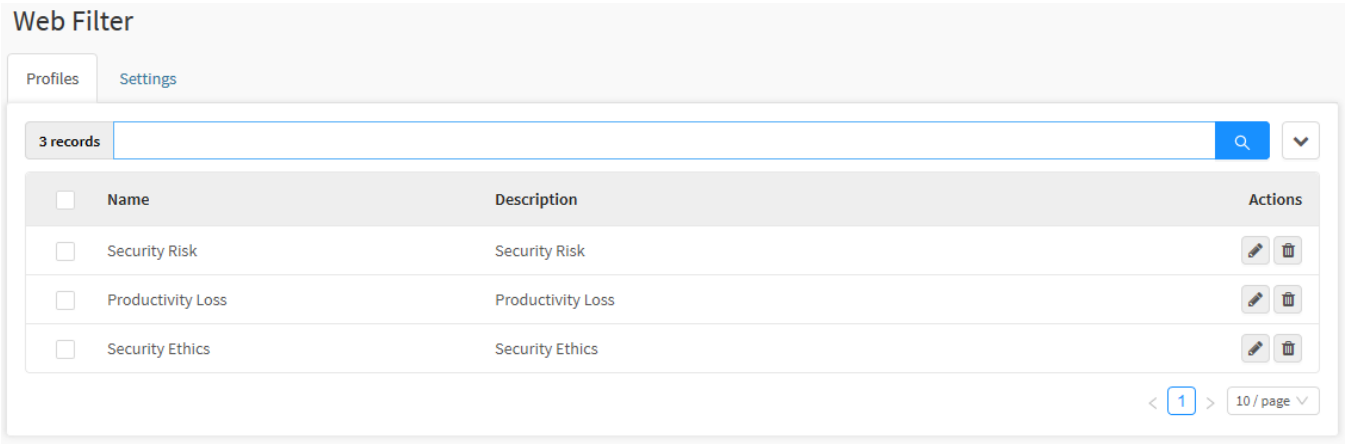
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Profile successfully deleted

After performing these procedures, the profiles will have been successfully deleted.

Web Filter - Profiles - Columns

Below we will explain each column of the Web Filter tab:



Profiles – *Web Filter*

We will explain each column below:

- **Checkbox[ ]:** Select the profile;
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- ***Actions*:** The “Actions” column consists of the buttons:
    - ***Edit* [ ]:** Allows you to edit the profile settings added in the *Create Profile* option of the actions menu;
    - ***Delete* [ ]:** Delete the profile, it is equivalent to the *Delete Profile* option in the actions menu.

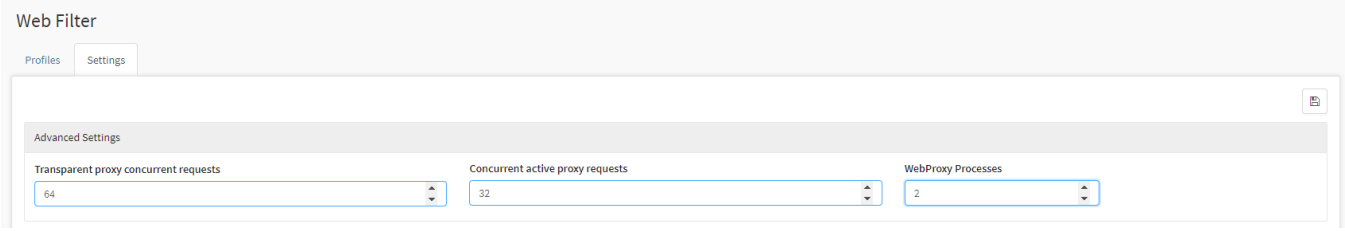
Next, we will analyze the contents of the *Settings* tab.

Web Filter - Settings

This item allows access to both the Proxy processes advanced options, and the options to customize the block page which is returned to network users regarding “Unauthorized” access to Web traffic (intercepted by the proxy).

Advanced Settings

In this section it's possible to optimize the functioning of the Web Filter services through the increase of the number of processes to be run simultaneously. This limit, respects the comptational capacity of the machine in use, and can be increased or decreased accordingly to this very same capacity:



Web Filter - Advanced Settings

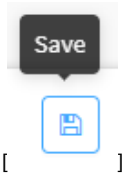
Transparent proxy concurrent requests: Select a number of simultaneous requests for the *Transparent Proxy*, by clicking on the adjustment arrows (*Mini mum of 40 and maximum of 256*).

Concurrent active proxy requests: Select the number of simultaneous requests for the *Active Proxy* by clicking on the adjustment arrows (*Minimum of 2 0 and maximum of 256*).

Web Proxy Processes: Select the number of Web Proxys processes by clicking on the arrows (*Minimum of 2, maximum of 4*). It's important to remember that the values may vary for each appliance model, for they rely on the number of CPU Cores available.

To check the number of CPUs available in your appliance, use the lscpu commando on the terminal interface, then confirm the value on the CPUs field. It is also possible to check the Web Filter for errors by using the "debug-webfilter" command, with the "-t" option debug-webfilter -t.

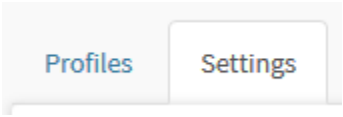
This option will cause the Web Filter service to be reloaded, ehich can cause some intermitences on your web browsing.

After configuring the number of processes in each field, click the save [

] button to record the changes.

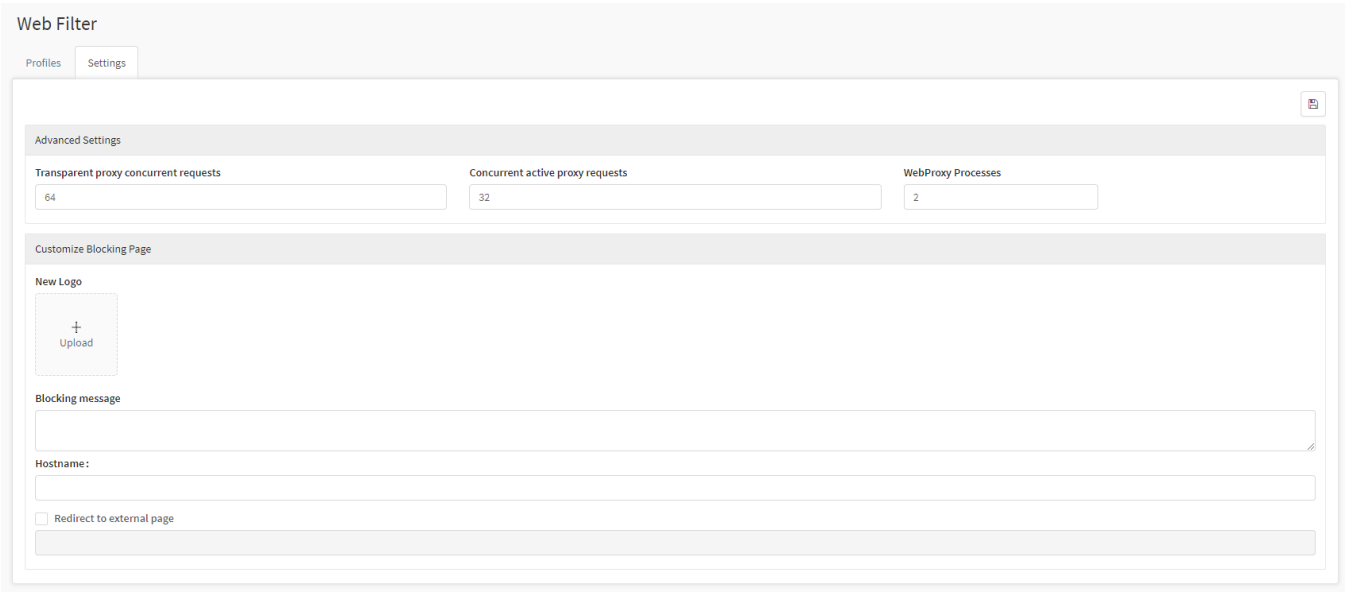
Block Page Customization

To configure the block page, click on "Settings".



Settings tab

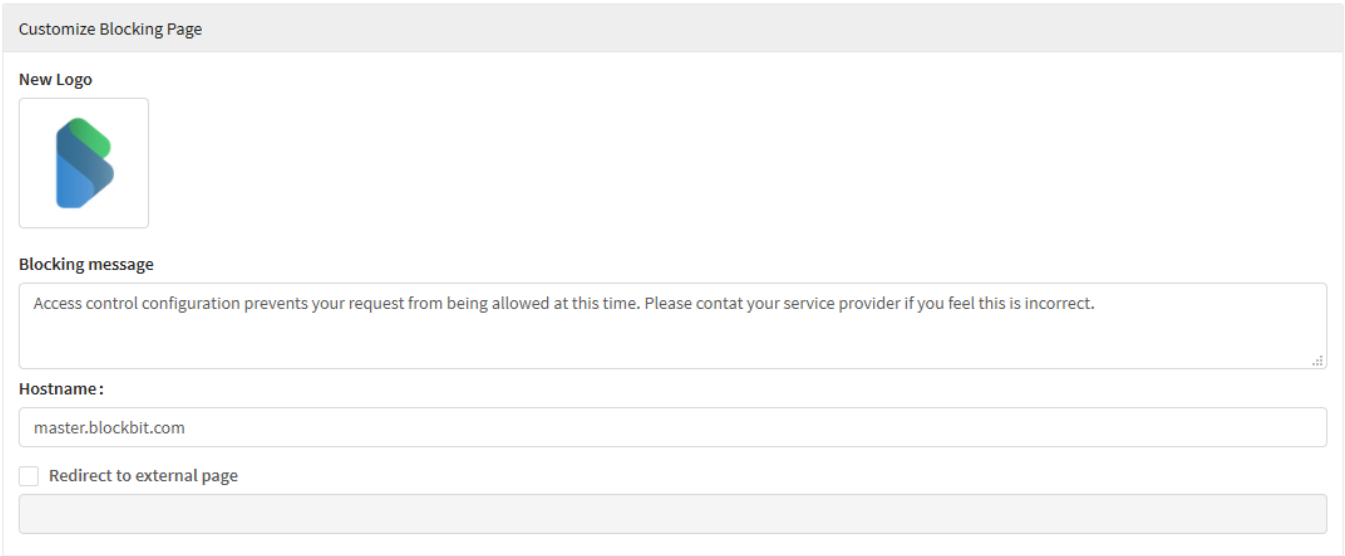
The “Block Page Customization” panel will appear, as shown by the image below:



Web Filter - Settings

It is possible to change the “Logo” and reset the “Block message”:

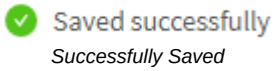
- ***New* logo:** It is possible to select a new logo for the lock screen. To upload an image, just click on **[** Upload **]**, after uploading the image, to preview it, click on ***Preview File*** **[** **]** finally, if you want to remove it click on ***Remove File*** **[** **]**;
- ***Blocking message*:** You can customize the blocking message that is returned to the client;
- ***Hostname*:** It allows defining which Hostname will be used;
- ***Redirect to external page*:** You can redirect traffic to an external block page.



Customize block page - Example

For cases of unauthorized WEB access attempts, that is, defined through security policies with the “Block” action selected, the system will return to the “Block” screen, with the message specified in the settings above.

To save all changes, click **[**  **]**.



Successfully Saved

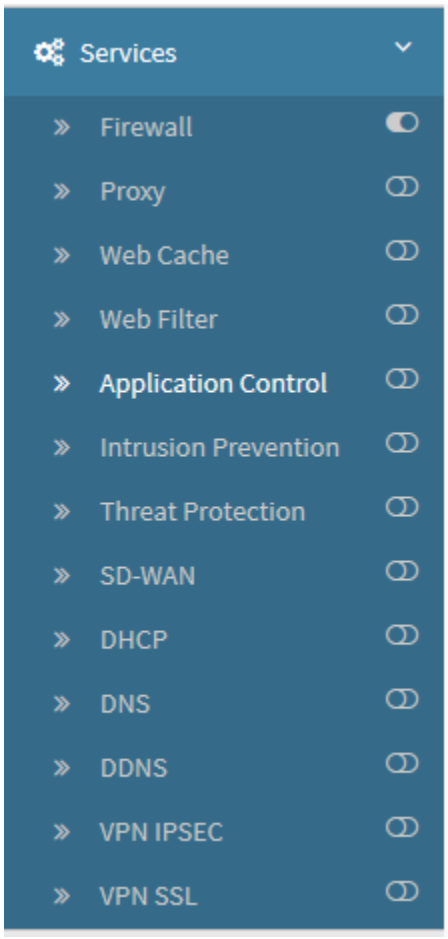
After saving, for the settings to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

UTM - Services - Application Control

Through the Application Control feature, it is possible to control whether users will be allowed access to certain applications or if they will not be authorized to use any application. Applications are divided into categories allowing the administrator to specifically determine the access of each item.

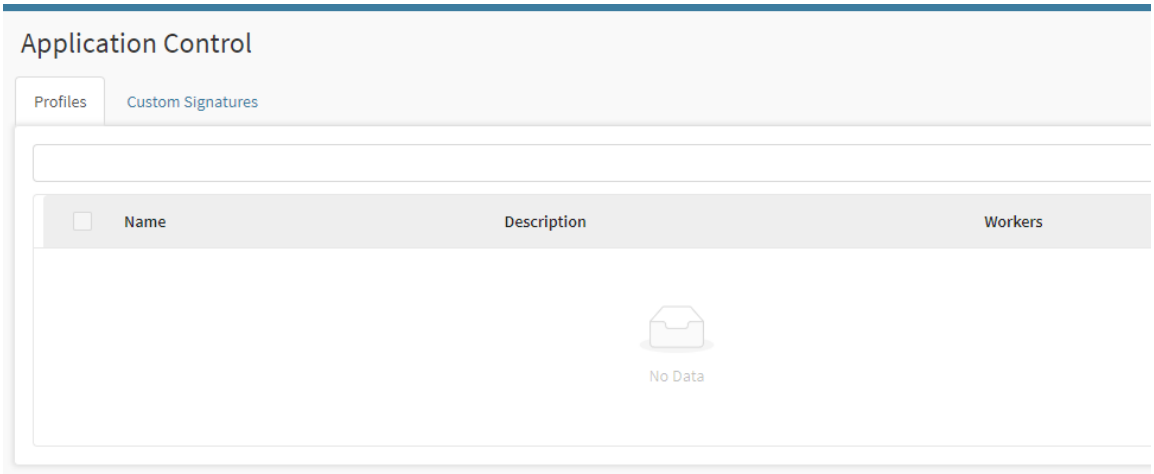
If an Application Control is added to a policy, the Web Filter is enabled in that policy, even if a Web Filter itself has not been selected. For more information about Web Filter, see this page.

To access this screen, just select the “Application Control” option



Services - Web Filter

The screen below will appear:



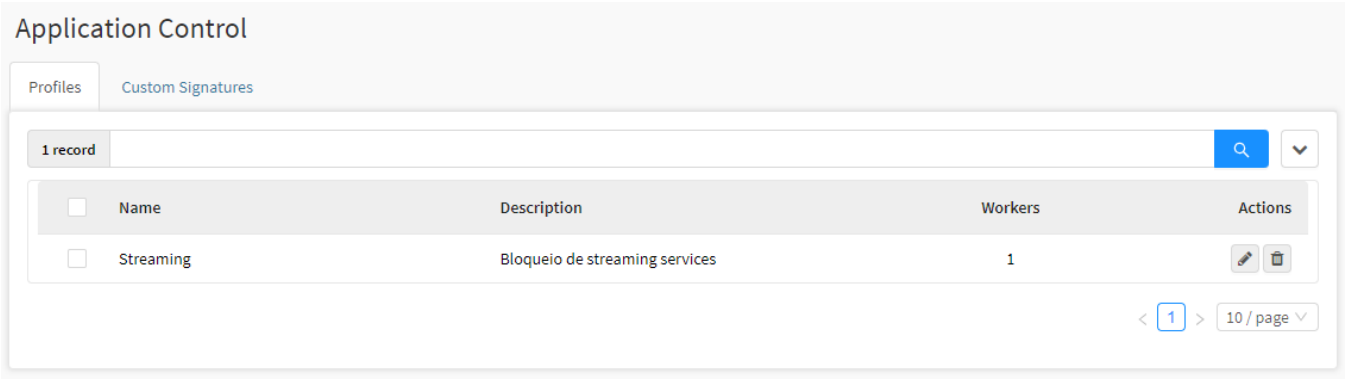
Application Control

Next, we will analyze the content of the columns of the Application Control panel.

Services - Application Control - Columns

Below we will explain each column of the Application Control tab:

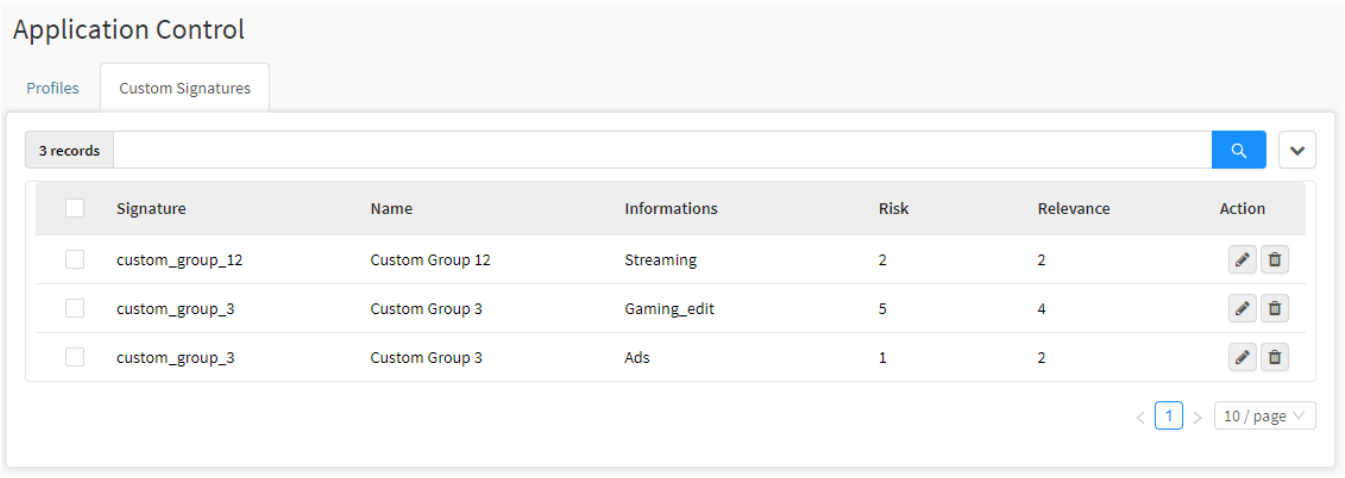
Profile tab:



Profiles – *Application Control*

- **Checkbox[ ]:** Select profile;
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- ***Version:*** Displays the version from which the profile has been created. It's of the utmost importance to create profiles from the same version of the NGFW, otherwise, the profile will not be compatible.
- ***Workers*:** Number of CPU in use.
- ***Actions*:** The “Actions” column consists of several buttons:
    - ***Edit* [ ]:** Allows you to edit the profile settings;
    - ***Delete* [ ]:** Deletes the profile.

Custom Signatures tab:



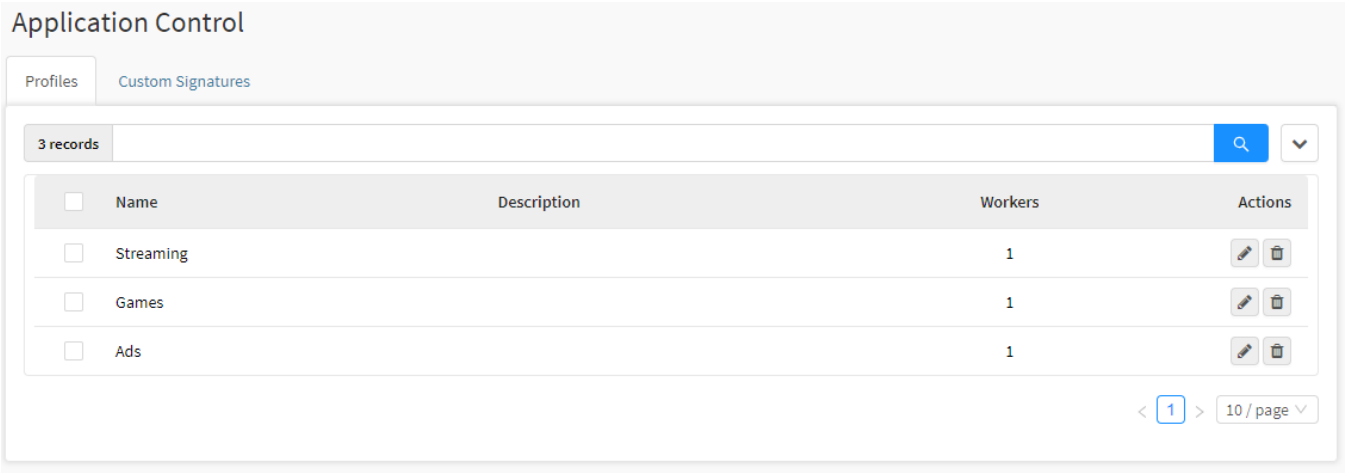
Custom Signature – *Application Control*

- **Signature**: Field filled in automatically according to the 'Name' chosen for the custom signature.
- **Name**: Name chosen for the custom signature.

- **Information**: Custom signature's description.
- **Risk**: Level 1 to 5 where 1 has the highest risk and 5 the lowest.
- **Relevance**: Level 1 to 5 where 1 has the highest priority and 5 the lowest.
- ***Actions*:** The “Actions” column consists on the following options:
    - ***Edit* [ ]:** Allows you to edit the settings;
    - ***Delete* [ ]:** Deletes the signature.

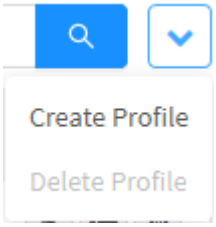
Services - Application Control - Profile Tab

In this tab it is possible to create, edit and delete Application Control Profiles.



Application Control - Profiles

In the top right corner we can search for profiles [ ] if there are many already configured and also have access to the actions menu [ ].



Application Control – Action Menu

Next, we check how to create a Profile.

Services - Application Control - Actions Menu - Create Profile

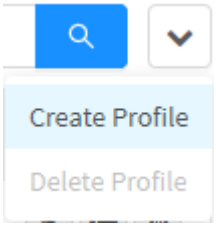
Through the option “Create Profile” it is possible to create a new Application Control profile.

We will analyze the process of creating a profile in Application Control and also check the following sections:

- General;
- Application Control.
- Create customized group

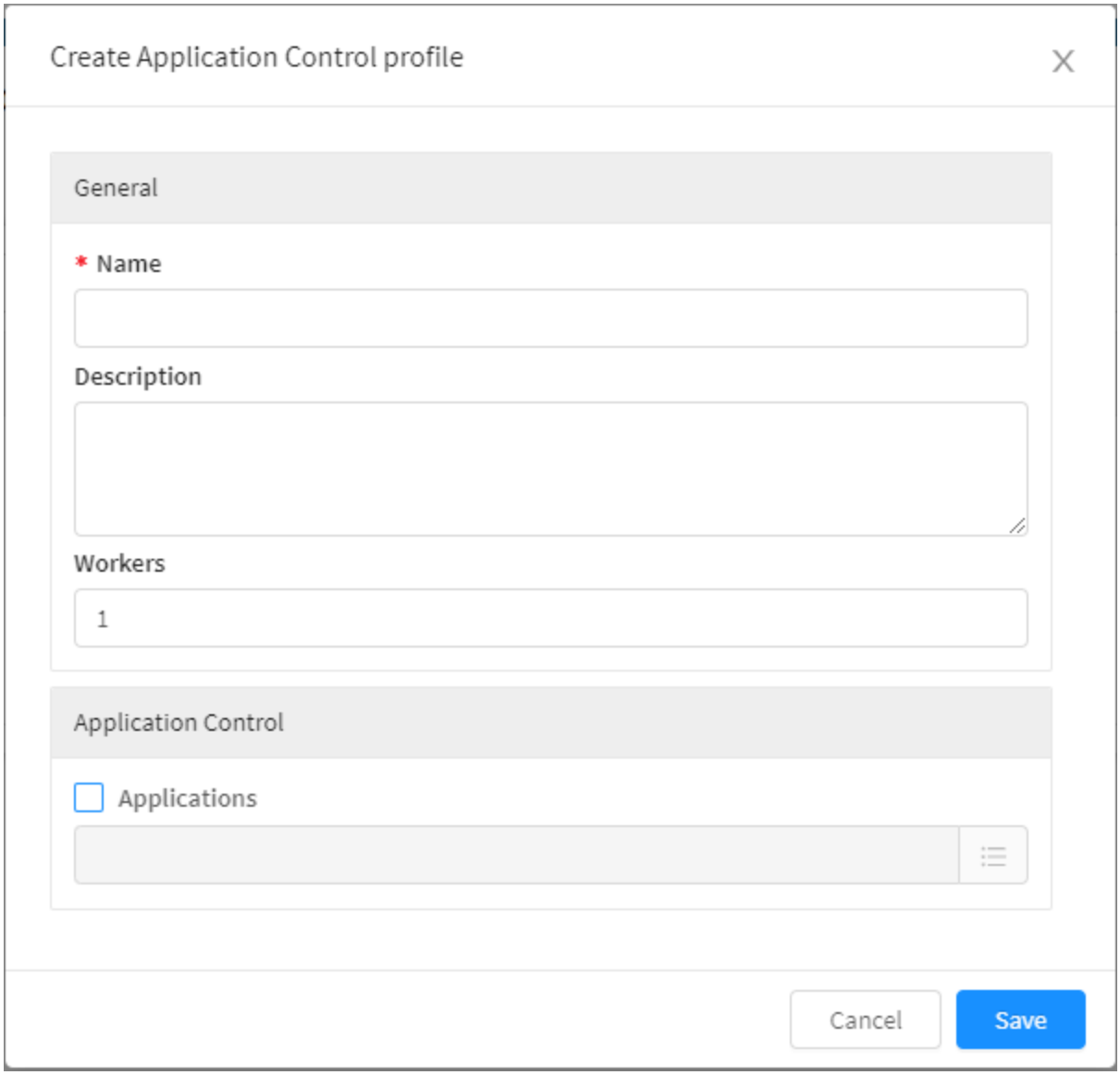
To access, click on the **actions menu [ ]**.

1. Click on the “Create Profile” option;



Application Control - Create Profile

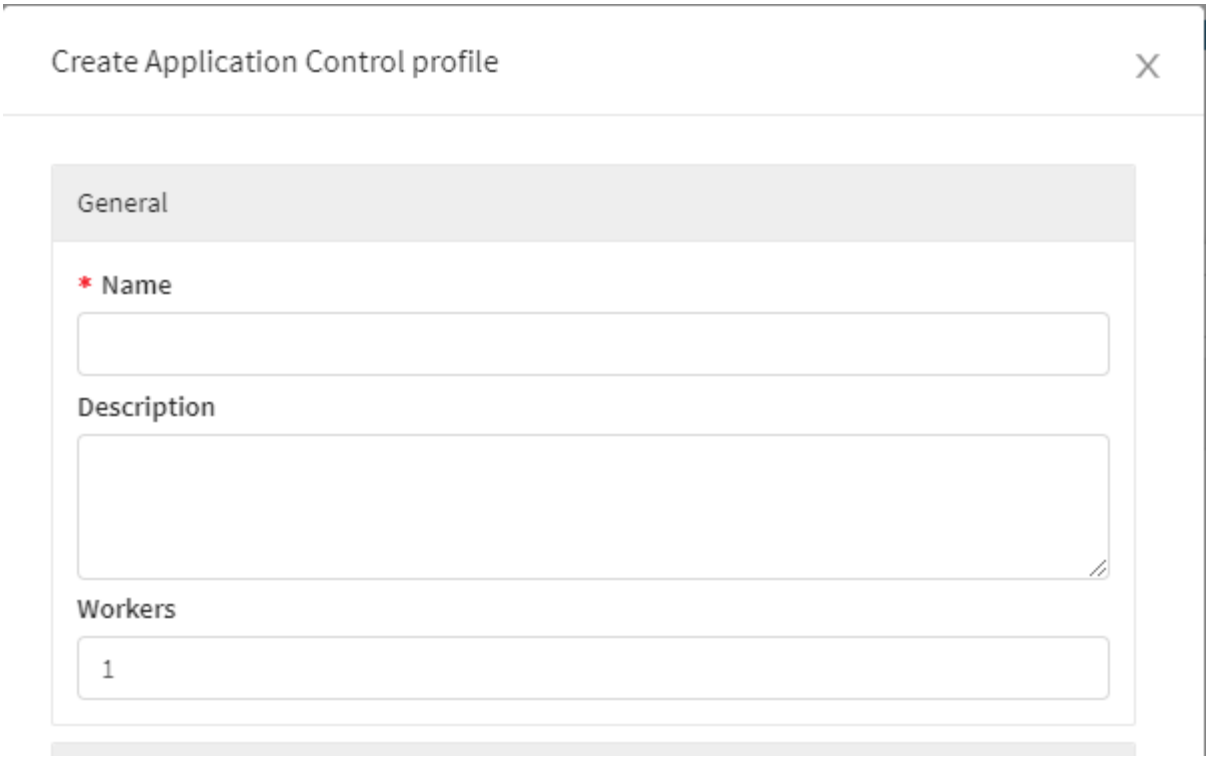
2. The “Create Profile” screen will be displayed. In this panel it is possible to make the general configurations and define the permissions of the applications used in that profile.



Application Control - Create Profile

General

In "General" we have the following text boxes:

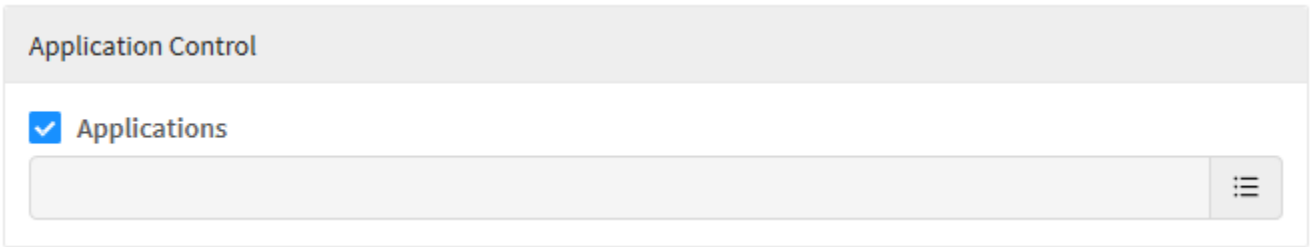


Application Control – General

- ***Name:*** *Define a name for the profile*. Ex.: *Deny All Ads*;
- ***Description*****:** Set a description for the profile. Ex.: *Application Control to deny all ads.*
- ***Workers:*** Define a number of workers, or processes, by inspection profile. Please note that the field is preset as 1.

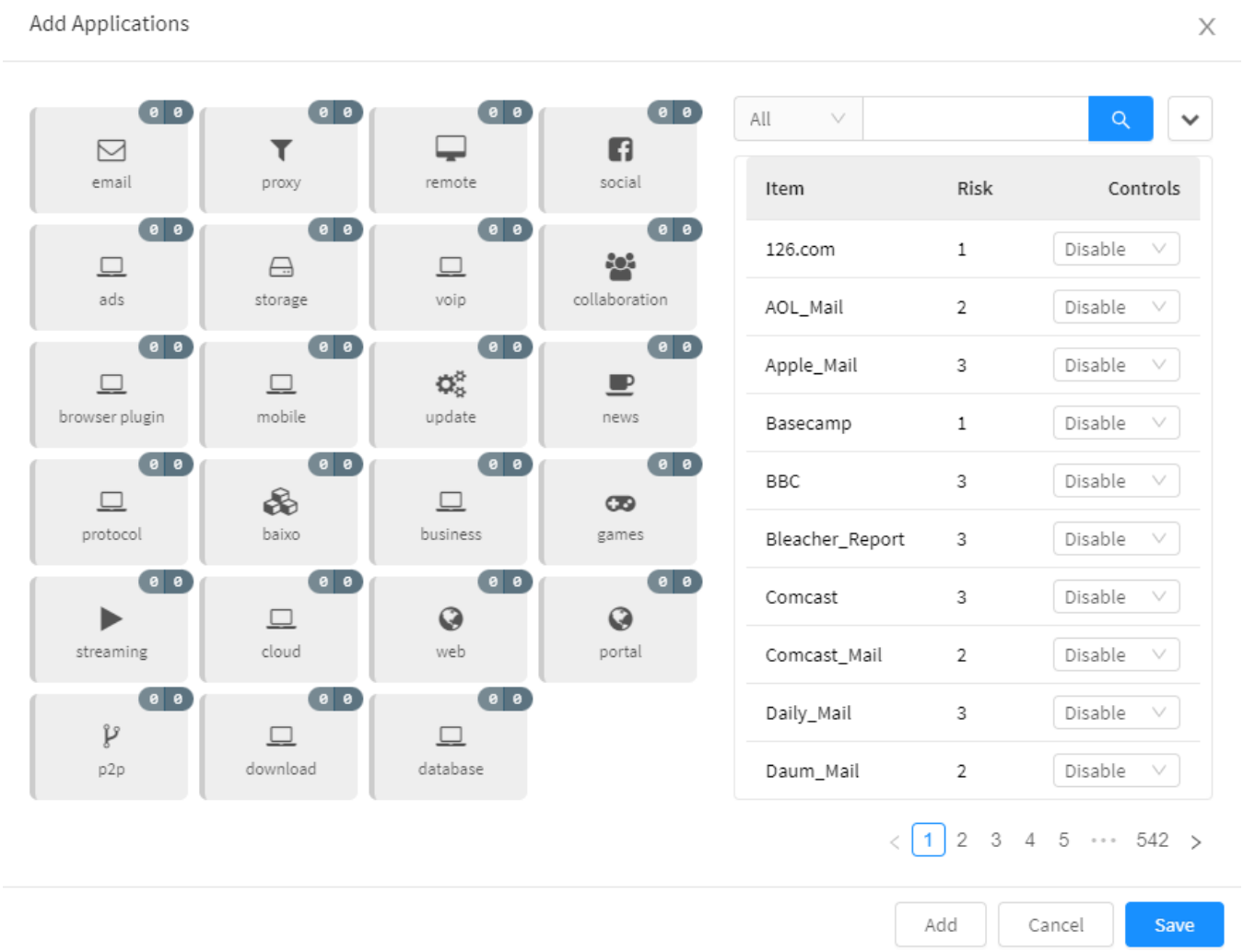
Application Control

"Application Control" determines the applications that will be allowed or denied access:



Application Control - Applications

To edit the applications, decide that the **checkbox [** **]** is enabled, then click the **list applications [** **]** button to manage how to authorize.



Application Control - Add *Application*

By selecting one of the icons on the left, as improved choices in the right panel.

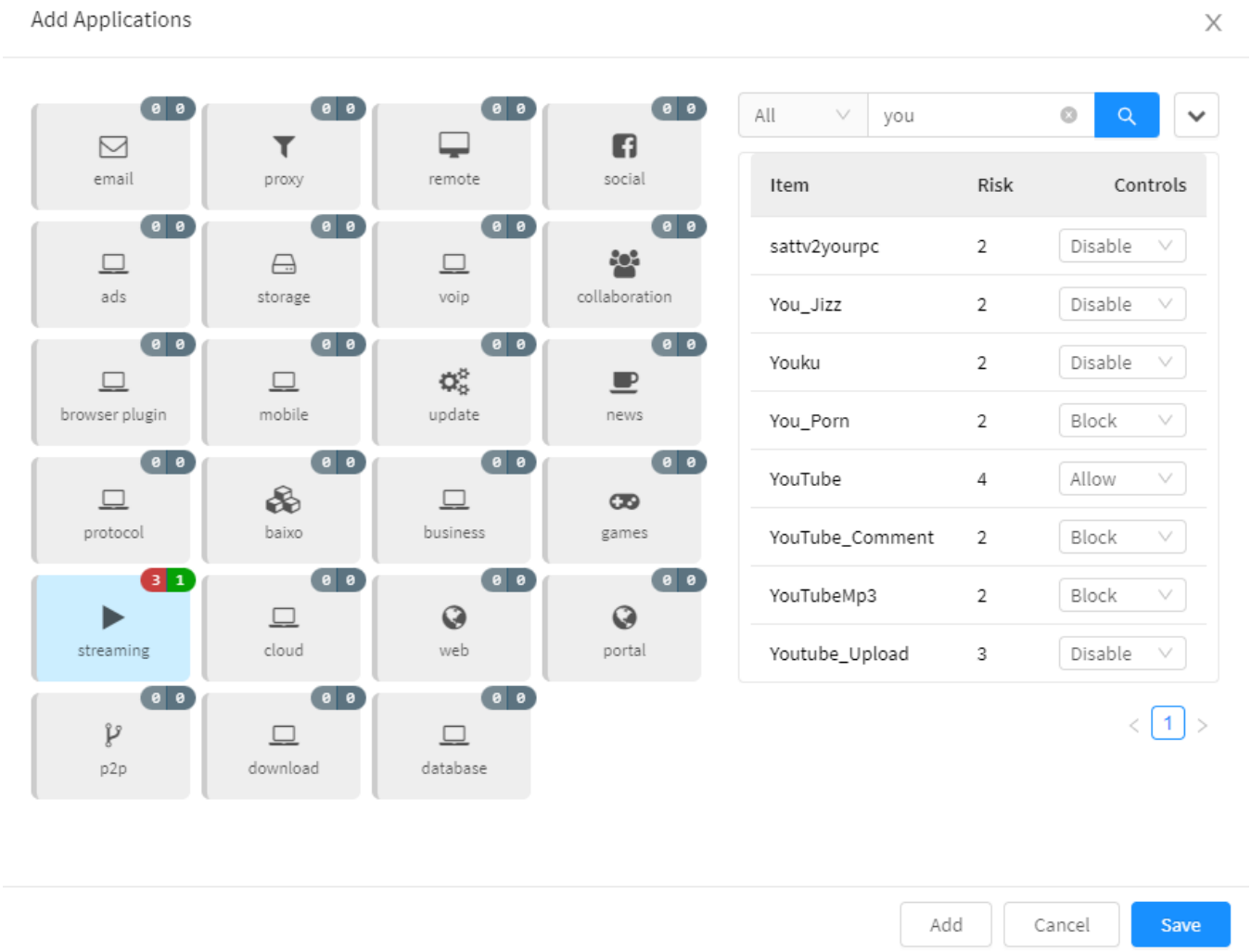
For more information on the categories used by Application Control, see this page.

Choose the desired categories and then select **Allow**, **Block** or **Disable**. In the **actions menu [ ]**, it is also possible to apply any of these options in all categories in **Allow All**, **Block All** and **Disable All** to disable them. Below is a brief description of the function of each action:

- **Allow:** Access to applications classified within this category is granted;
- **Block:** Access to applications classified under this category is denied;
- **Disable:** This category is disabled, this means that Application Control will ignore it and will only consider applications in allowed or blocked categories..

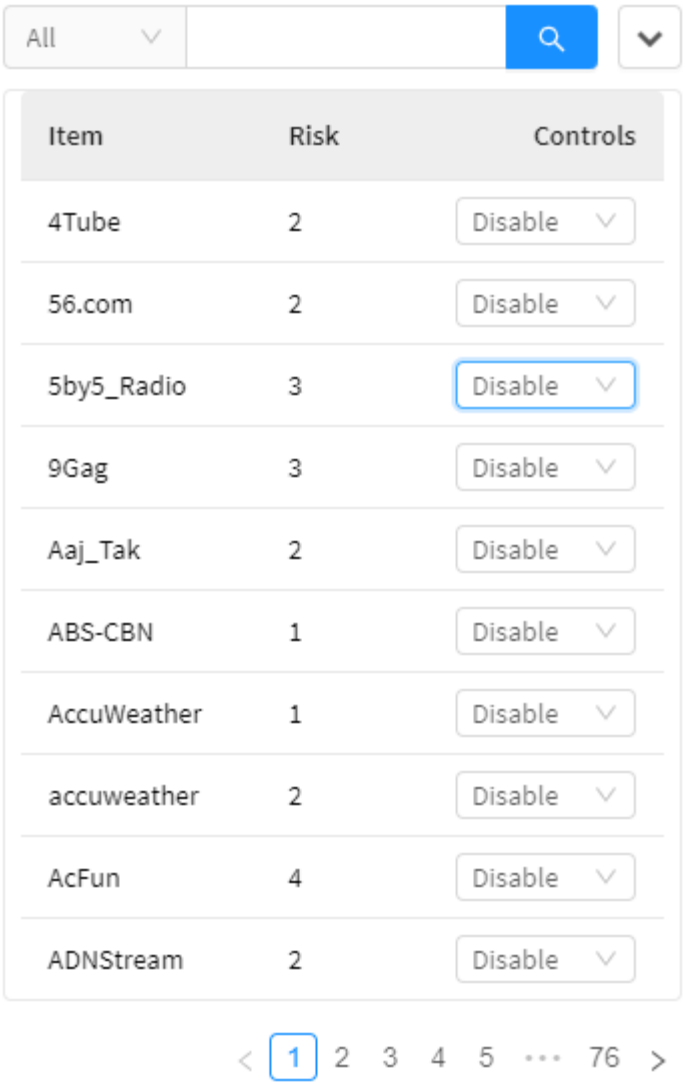
In the example below, we will disable all advertisements.

To do so, select the desired category, in this example, we will select the option "ads":



Application Control - Add Application - "Streaming" option selected

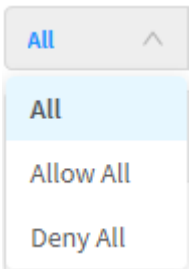
Determine the desired application and in the selection box, choose the option **Deny [** Deny **],** as shown in the image below:



Application Control - Add Application - Denied items

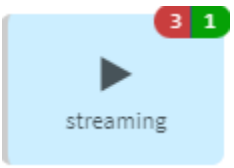
The risk levels of each application from the groups are already preset and will be automatically updates as soon as new applications are included.

In case it is necessary to make a configuration in all the items of a category, just select the desired option in the **actions menu [ ]** or in the selection box shown below:



Application Control - Add Application - All, *Allow All* and *Deny All*

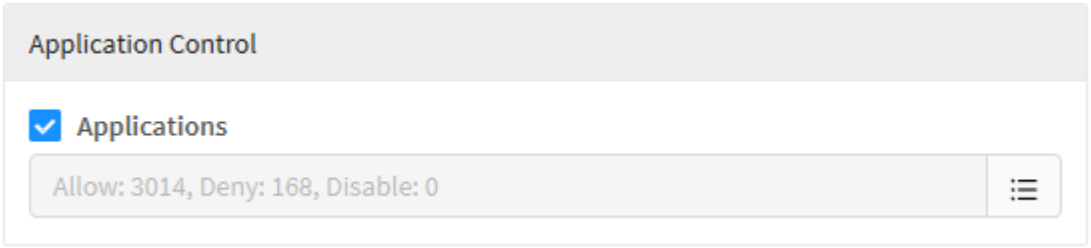
When having an application with permission denied, the amount of applications denied and allowed will be displayed under the icon of its respective category on the left, as shown below:



Application Control - Add Application - 3 items denied and 1 allowed

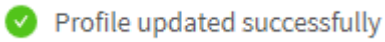
Finally, if you want to cancel click the [Cancel] button. To finish editing the applications click on the [Save] button.

After having performed the previous processes, a summary of all allowed and denied applications will be displayed in the Applications field, as shown below:



Application Control - Applications - Applications allowed and denied

To complete this process, just click the [Save] button again.



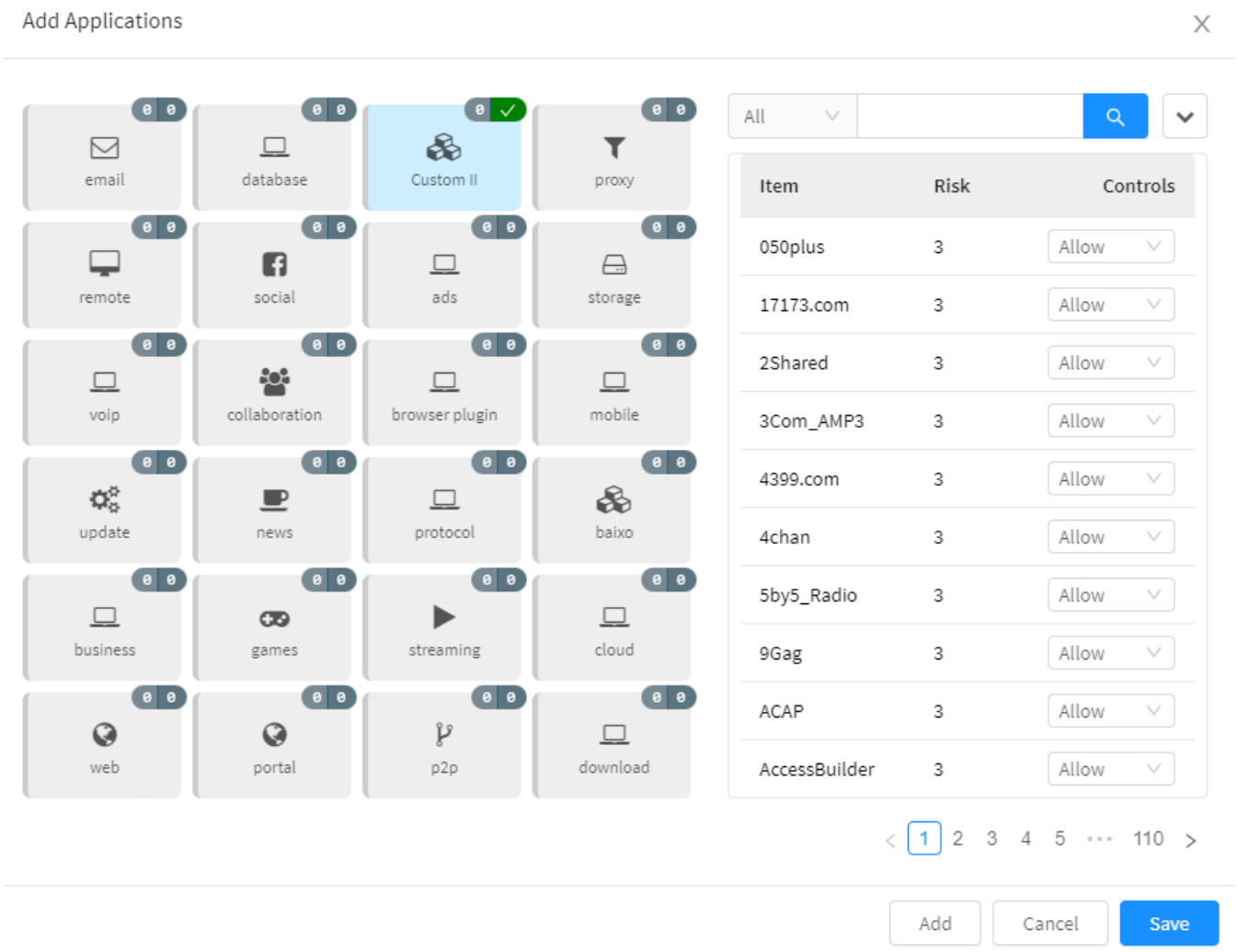
Profile successfully updated

After saving, for the changes to take effect it will be necessary to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

It's important to remember that even if the service is disabled, in case an Application Control profile is associated with an IPv4 or IPv6 Policy, the blocks will be done normally if the Policy is active. To disable the service, besides deactivating it, we must remove the Application Control profile(s) from this (these) Policy(ies).

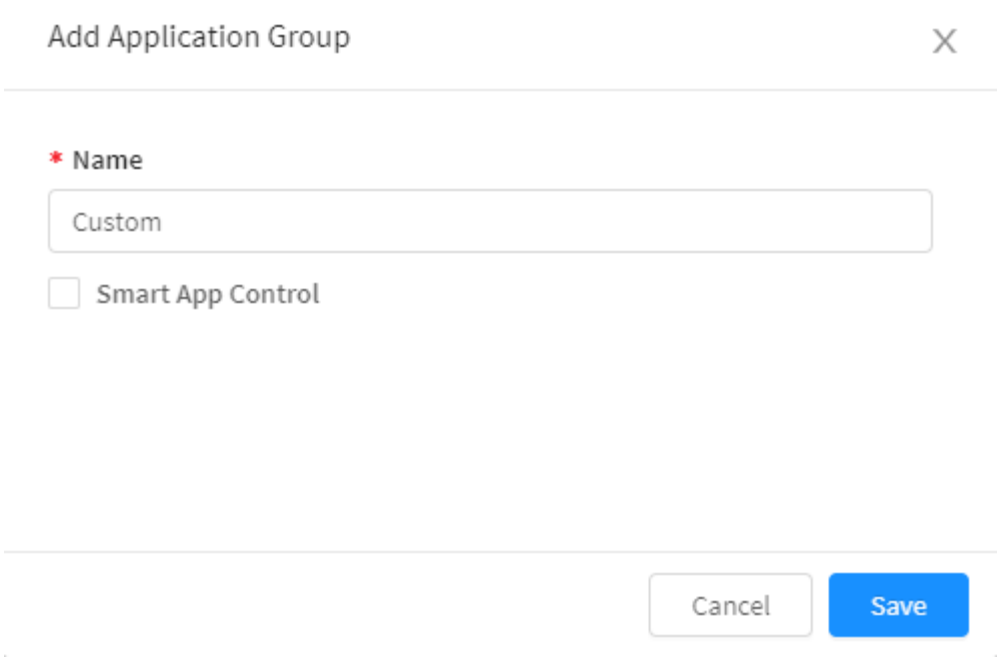
Create customized group

Ao criar um novo *Perfil*, é possível criar novos grupos customizados que serão acrescentados às categorias já existentes.



- ***Add button [Add]:*** Allows dynamic customized group applications to be added based on your characteristics. For example, based on client/server application types, network protocols and others.

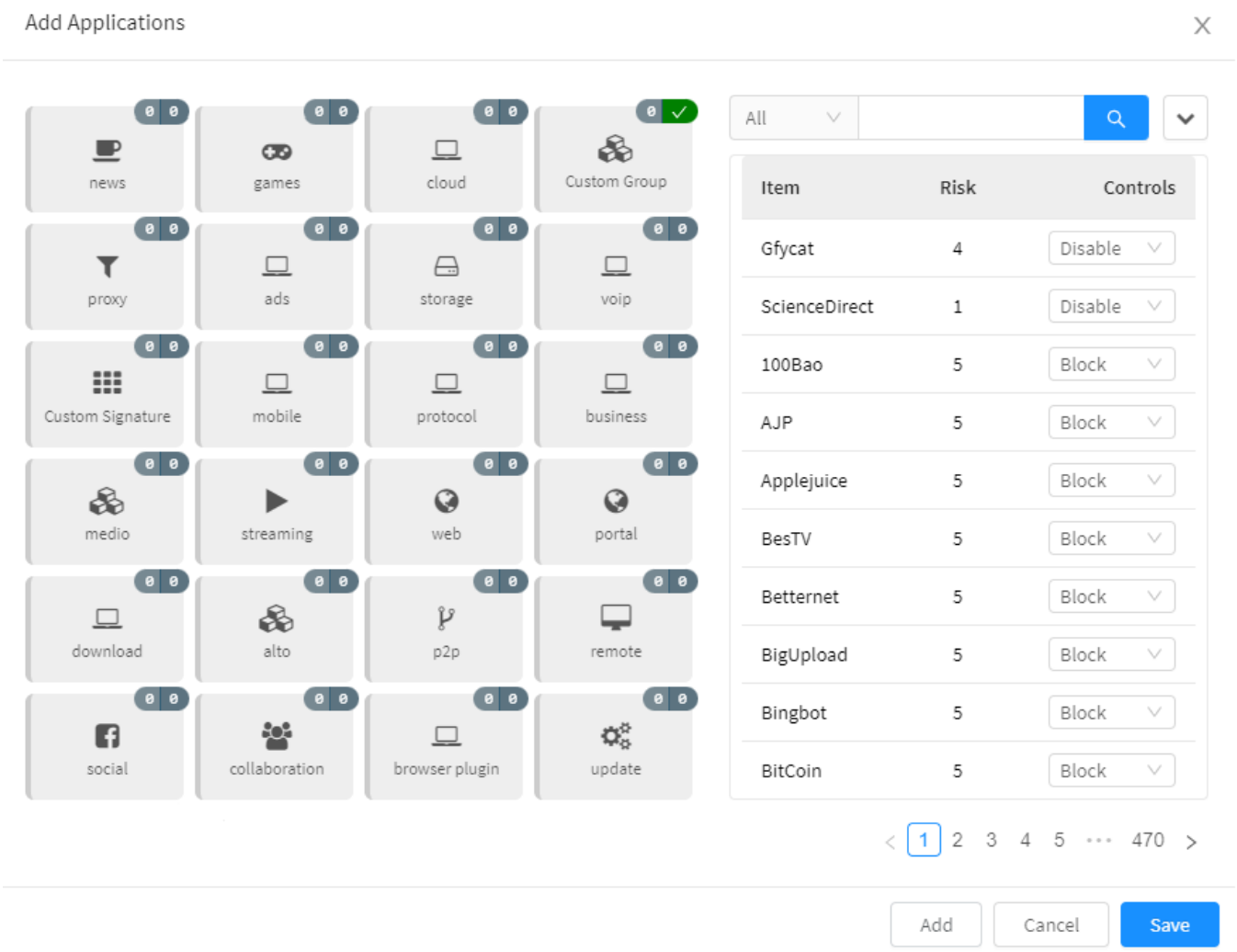
When clicking this option, the following screen will be displayed:



Create Custom Group Application

Insert the name of the group to be created, for example *"Custom"*.

To conclude, click on [Save].



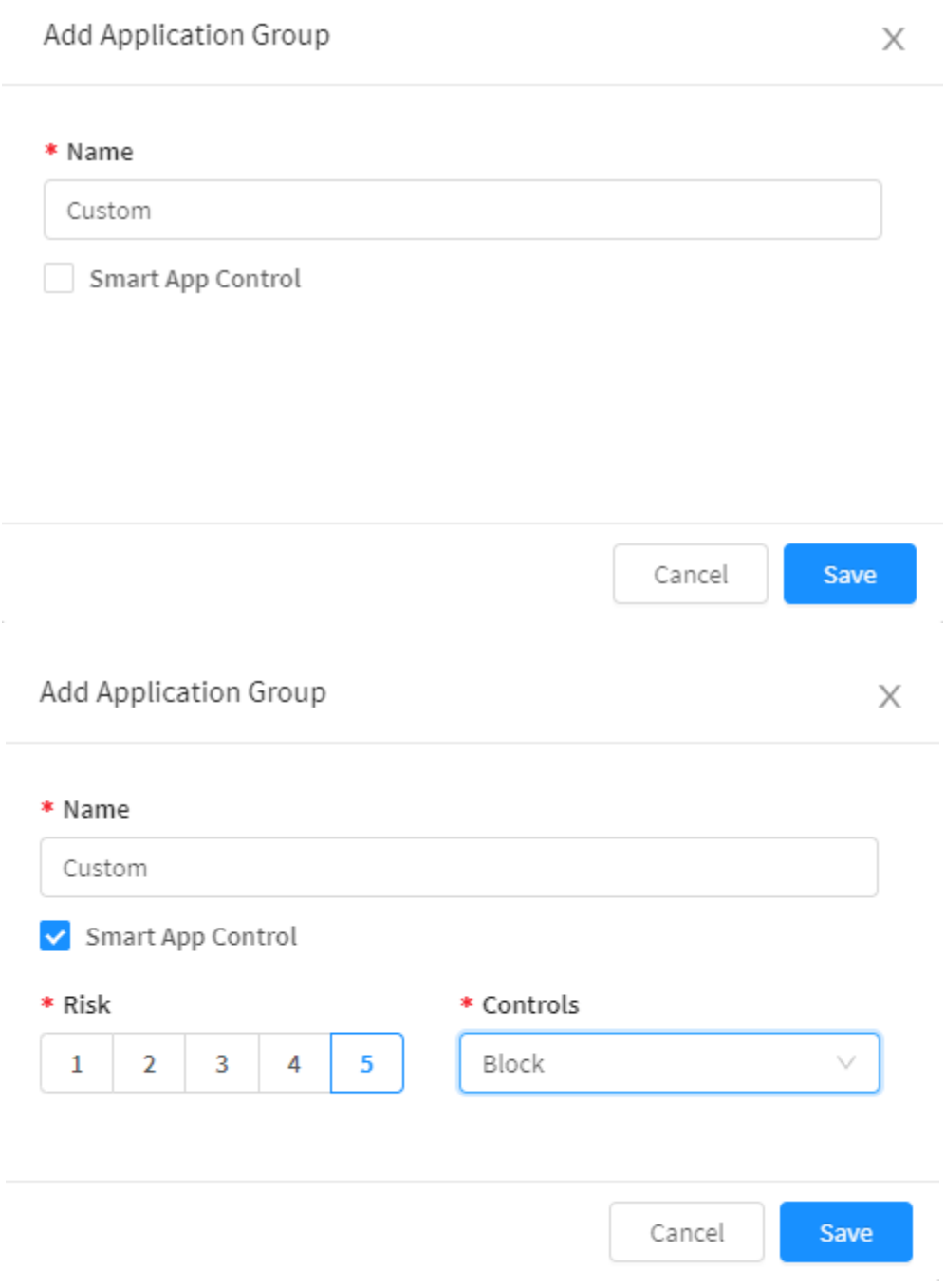
Custom Group Application

After performing these procedures, the settings will have been successfully configured.

So, the custom group will be able to receive dynamically the other application groups.

Smart App Control

When setting up a new customized group using the option, it is possible to select the risk level and the action to take to the applications inserted in the group.



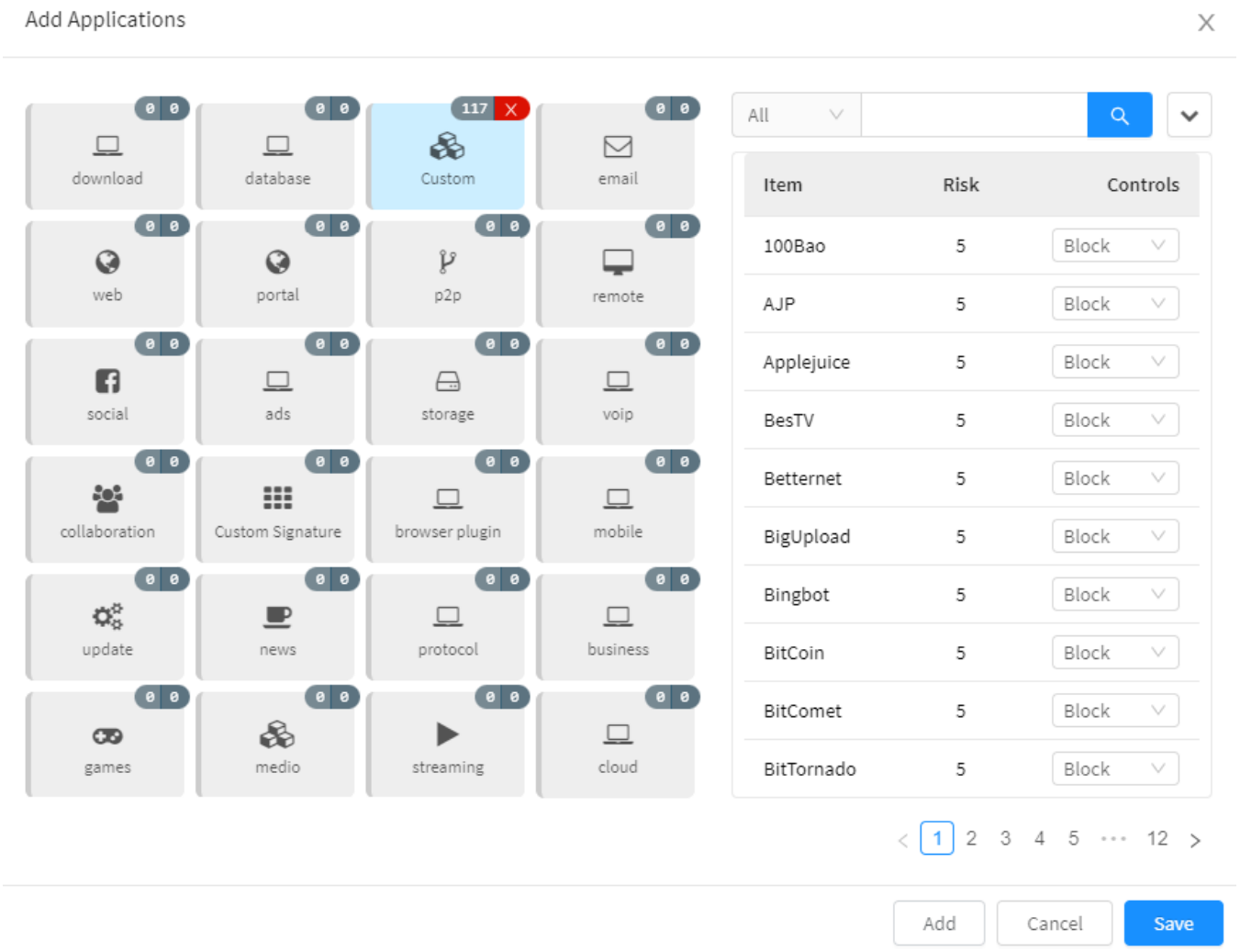
Application Control - Risk Level

The risk levels are classified from 1 to 5, 1 being the lowest and 5 being the highest.

There is a limit of 50 groups per profile.

To conclude, click on [Save].

When selecting the risk level and the action to be taken, all applications that are classified in the same level set, will be blocked or allowed.



After performing these procedures, the settings will have been successfully configured.

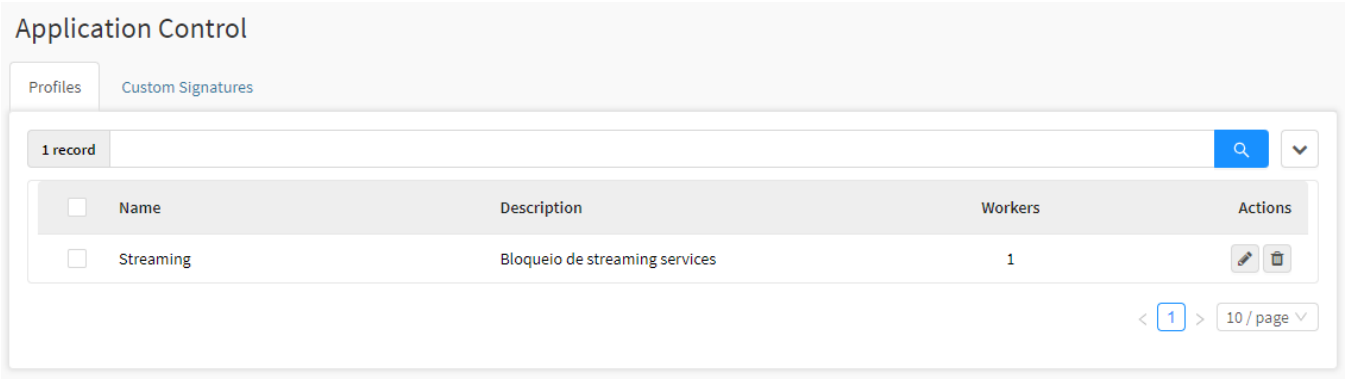
Thus, the custom group enabled with risk level will be automatically updated when new applications are inserted.

Next, we are going to analyze how to delete profiles.

Services - Application Control - Actions Menu - Delete Profile

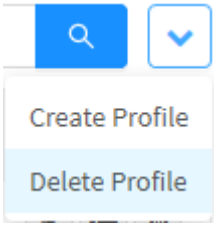
Through the button “Delete Profile” it is possible to delete the selected Profiles. To delete from the Actions Menu, follow these steps:

1. Select which Profile(s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Example: Streaming;



Application Control – Selection of Profiles to delete

2. Enter the actions menu [ ] and click on the option “Delete Profile”.

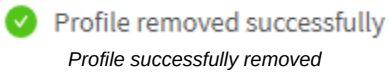


Application Control – Delete Profiles

3. The notification message will appear asking if you really want to delete the selected Profiles:

Application Control – Deletion confirmation message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

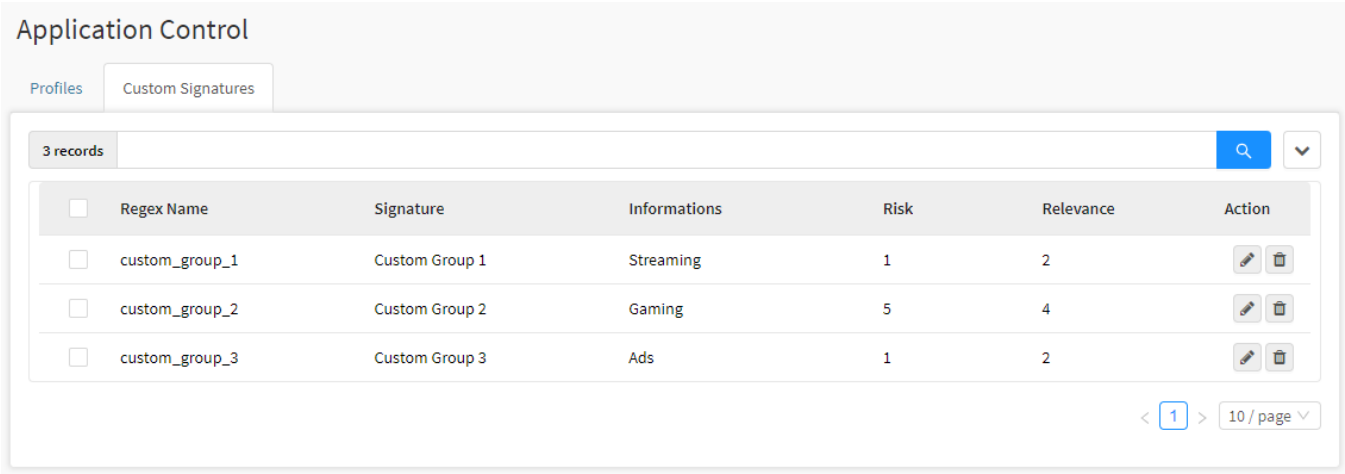


Profile successfully removed

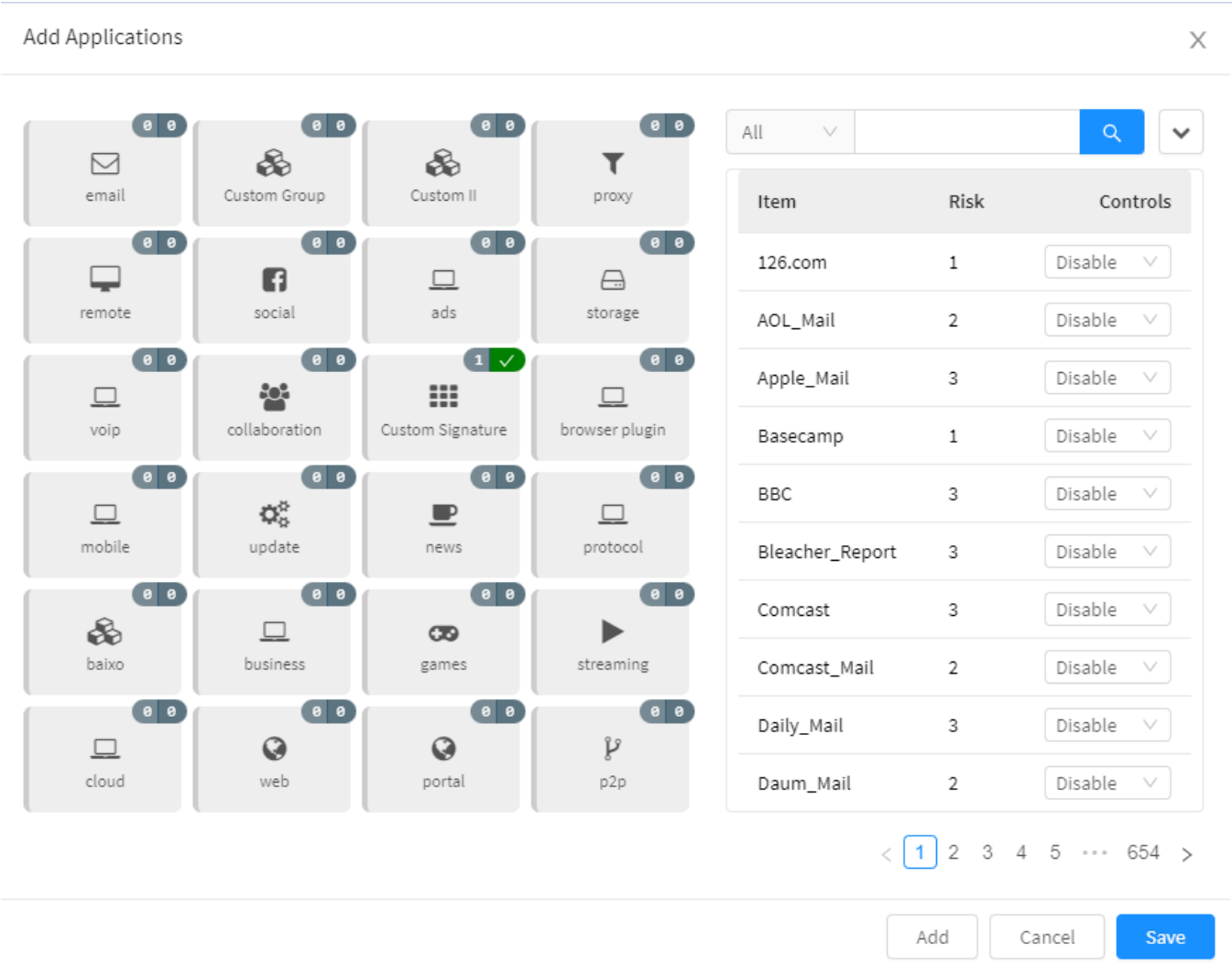
After performing these procedures, the Profiles will have been successfully deleted.

Services - Application Control - Custom Signatures Tab

Application Control's Web-type Customized Signatures service allows the administrator to use a combination of parameters to categorize certain traffic, blocking or allowing access to applications. This service can be used both in Application Control and in Application Routing.



In Application Control profiles, where custom groups are added, there is a Custom Signatures category that will be automatically configured when creating a new Custom Signature.



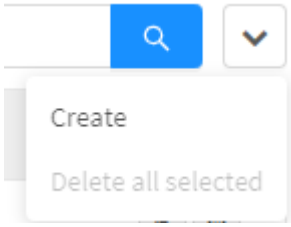
Next we will see how to create a Custom Signature.

Services - Application Control - Create custom Signatures

Using the “Create” option, it is possible to create a new Custom Signature.

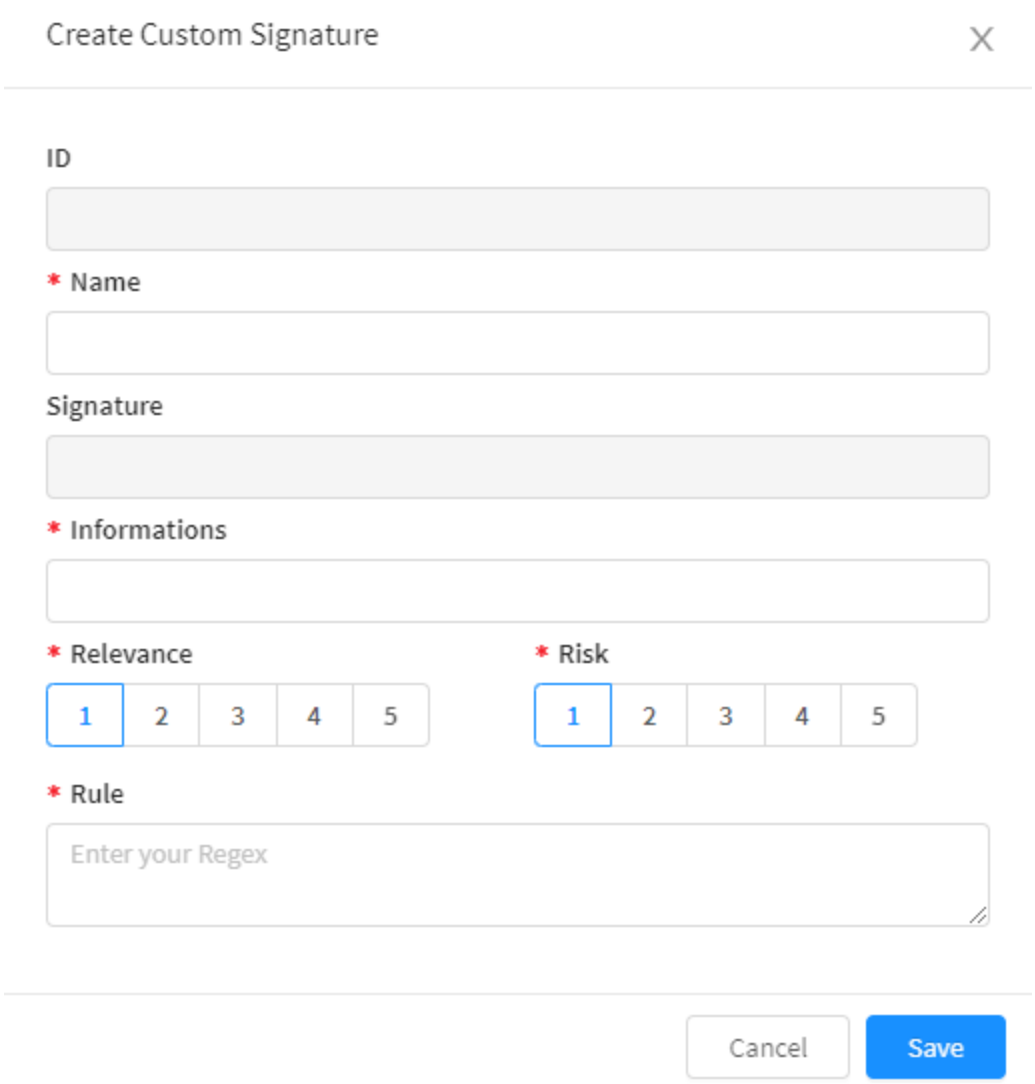
We'll go through the process of creating a custom signature;

To access, click on the **actions menu [**  **]**, and select the “Create” option;



Application Control - Create Profile

Afterwards, the “Create” screen will be displayed. In this panel it is possible to make the general configurations and define what will be allowed or blocked in that profile.



Application Control - Create

- **ID**: Custom signature identification number.
- **Name**: Name chosen for the custom signature.
- **Signature**: Field filled in automatically according to the 'Name' chosen for the custom signature.
- **Information**: Custom signature's description.
- **Relevance**: Level 1 to 5 where 5 has the highest priority and 1 the lowest.
- **Risk**: Level 1 to 5 where 5 has the highest risk and 1 the lowest.
- **Rule**: Regular Expression that will allow or block the application.

The ID number will be automatically generated when saving the configuration.

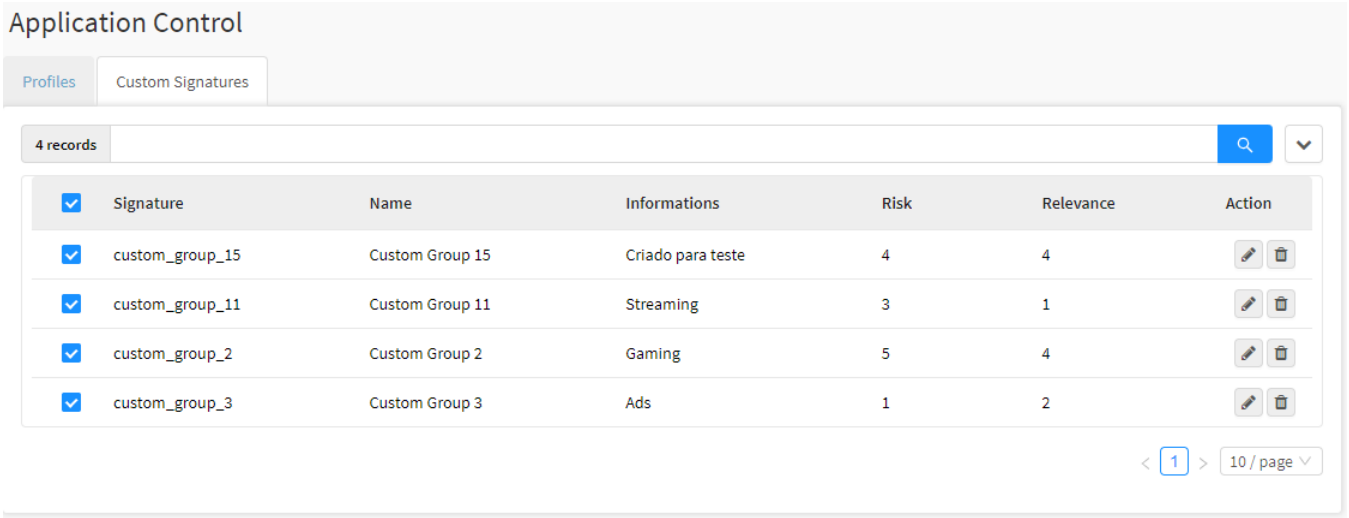
In the "Rules" field, you must insert words related to the application you want to allow or block. As an example, if you want to block streaming services, fill in the field with the name of these services.

Next, we'll look at how to delete a Custom Signature.

Services - Application Control - Custom Signature - Delete Signature

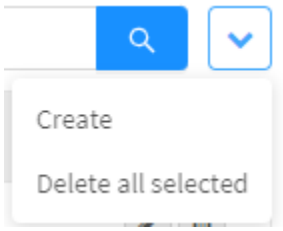
Through the button “Delete” it is possible to delete the selected Signatures. To delete from the Actions Menu, follow these steps:

1. Select which Profile(s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Example: Test;



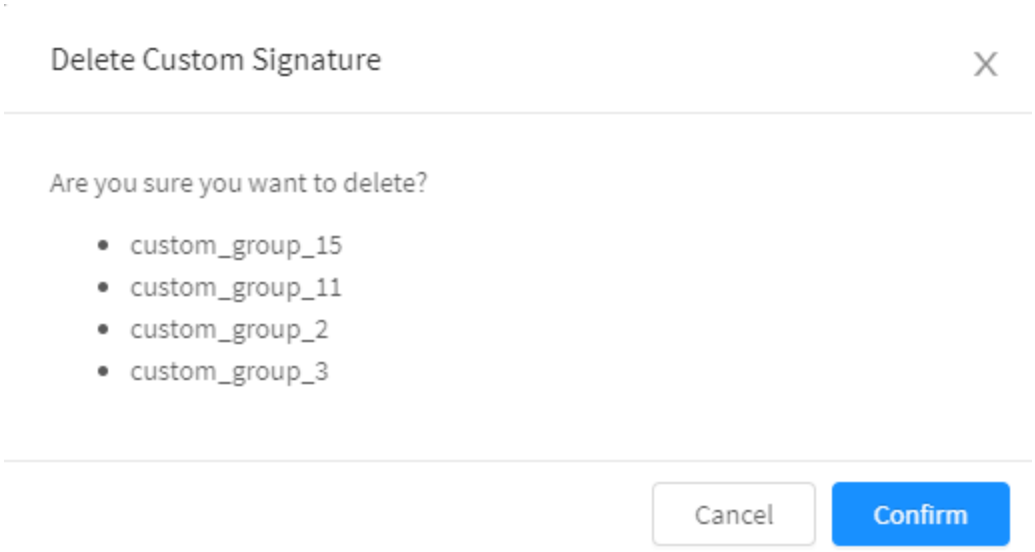
Application Control – Selection of Signatures to delete

2. Enter the actions menu [ ] and click on the option “Delete all selected”.



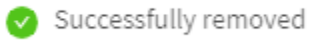
Application Control – Delete Signatures

3. The notification message will appear asking if you really want to delete the selected Signatures:



Application Control – Signatures deletion confirmation message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Confirm **]** button.



Signature successfully removed

After performing these procedures, the Signatures will have been successfully deleted.

Application Control - Categories List

Below we will display several tables informing the categories and their respective applications.

The categories used by Application Control are:

- *Email;*
- *Proxy;*
- *Social;*
- *Remote;*
- *Ads;*
- *VOIP;*
- *Storage;*
- *Collaboration;*
- *Mobile;*
- *Update;*
- *Protocol;*
- *Games;*
- *Business;*
- *Streaming;*
- *Cloud;*
- *Web;*
- *Portal;*
- *P2P;*
- *Download.*

The *instant messaging* and *anonymizers* categories are also included.

Here is a list of the applications, sorted by category:

Categories	Applications
E-mail	126.com; AOL Mail; Apple Mail; Basecamp; BBC; Bleacher Report; Daily Mail; Daum Mail; Eudora; Eudora Pro; Evolution; Exchange; Eyejot; Fastmail; Fox News; Fox Sports; Gmail; Gmail attachment; GMX; GMX Mail; Google Inbox; Google Mail; Hightail; Hushmail; IL; IMAP; IMAPS; IMO; Instan T; Jubii; KMail; LiveGo; Lotus Notes; MailChimp; Maildotcom; Maildotru; MAILQ; Mail.Ru; Mail.ru Attachment; MAPI; Official Major League Baseball; Mutt; Naver Mail; NI Mail; ODMR; Open Webmail; Outlook; Outlook Express; PCMAIL; POP2; POP3; POP3S; QMTP; QQ Mail; RoadRunner; SMTP; SMTPS; Spypig; Squirrelmail; Stack Overflow; Thunderbird; T-Online;Verizon Email; Web.de; Windows Live; Wall Street Journal; XNS Mail; Yahoo! Accounts; Yahoo! Mail; Zoho Mail.
Proxy	ASProxy; Avoidr; Browsec; CactusVPN; Camo Proxy; CDN; FlyProxy; Gom VPN; gpass1; Guardster; Hotspot Shield; I2p Reseed Request; ibVPN; ICAP; KProxy; OpenVPN; Ozyman; Privax; ProxEasy; Proxifier; Proxyorg; Reduh; Suresome; Surrogafier; Ultrasurf; VTunnel; Zalmos; Zen Guard; ZenMate; ZenVPN.
Social	17173.com; 51.com; Adult Friend Finder; aNobii; Athlinks; Badoo; beRecruited; Bigadda; Blogger; BranchOut; CafeMom; Classmates; Cloob; Cyworld; Daily Horoscope; Delicious; deviantART; Diaspora; Douban; eHarmony; Eventbrite; Facebook; Facebook Apps; Facebook Like; Family Tree; Fazed; Facebook Comment; Facebook event; Facebook Message; Facebook Status Update; Facebook search; Facebook video; Facebook video chat; Flixster; Fotolia; FriendFeed; Friendster; FriendVox; Fubar; Funshion; Gaia Online; Gather; GOLFZON; Habbo; Hatena; Hyves; iAstrology; Ibibo; iKarma; Imgur; ipernity; iWiW; Kaixin001; LinkedIn; LinkedIn Contacts; LinkedIn Job Search; LiveJournal; LiveJournal Post; Livemocha; Lokalisten; Match.com; Me2day; MEETin; Meetup; MeinVZ; MetroFLOG; Mister Wong; Mixi; Mixx; Mxit; MyHeritage; MySpace; myUdutu; Netlog; Odnoklassniki; Orkut; Pinboard; Ping FM; Pinterest; Plaxo; Plenty of Fish; Po.st; Qzone; Renren; schuelerVZ; Skyrock; spin.de; Squidoo; StayFriends; studiVZ; Sway; Tagged; The Microsoft Network; Tuenti; Tweet; Twig; Twitter; Twitterrific; Userplane; Viadeo; VKontakte; Weibo; wer-kennt-wen; XING; Yelp; Zoosk; zShare.
Remote	4shared; ADrive; Amazon Cloud Drive Download; AMMYY; AnyDesk; ARCServe; Atlassian; Backblaze; BigUpload; Bitbucket;

	BlazeFS; Bomgar; Box; Boxnet Upload SSL; Brothersoft; Citrix IMA; Citrix Licensing; Citrix RTMP; Citrix SLG; Citrix WANScaler; Clip2Net; Clip2Net; Upload; Commvault; DCE/RPC; DEC LaDebug; DepositFiles; DivShare; dl.free.fr; Docstor; Dropbox; Dropbox Download; Dropbox Share; Dropbox Upload; DynGate; Easy-Share; exec; FileDropper; Filemail; FileServe; Flickr Upload; Fluxiom; FTP Data; FTPS Data; Ganglia; GoToAssist; GoToMyPC; HiveStor; HP VMM; iCloud; ifile.it; ImageShack; Imgur; IMTransferAgent; Issuu; Ktelnet; KVM; KWDB; LeapFILE; Linuxconf; LogMeIn; LogMeIn Rescue; lsh; MediaFire; Megashare; Megaupload; Mendeley; Microsoft Azure; Mionet; Multiupload; NetSarang; NetSight; Netviewer; Okurin; OneDrive; Onehub; Online File Folder; OpenSSH; Pando; PAWSERV; PcAnywhere; PC-Duo; Phanfare; Photobucket; Putlocker; PuTTY; RADIUS-acct; RayFile; RDP; Remote Job Service; Remote Telnet; RJE; Rsupport; Scribd; Scribd Upload; SF MGMT; ShareFile Upload SSL; shell; Windows Live SkyDrive; Skyfex; SQL-NET; SSH; SShell; Su-Mit Telnet; SUPDUP; syslog; TeamViewer; Telnet; Timbuktu; TransferBigFiles.com; TurboUpload; TwitPic; TypePad; Uploading.com; vCOM; VMware Remote; Authentication; VMware vCenter client; VNC; RFB; Webhard; Webshots; Yahoo! Box; yfrog; Yoics; Zannet;ZumoDrive.
ADS	1000mercis; 247 Inc.; 24/7 Media; 33Across; Ad4mat; Ad Advisor; Adblade; Adconion Media Group; AdGear; Adify; AdJuggler; Ad Marvel; Ad Master; Admeld; ADMETA; Ad Mob; AdNetwork.net; Ad Nexus; AdReady; AdRoll; adSage; AdSame; Adtech; Ad Tech; Adtegrity; Advertising.com; AdXpose; Aggregate Knowledge; Amazon Ads System; Amobee; AOL Ads; AppNexus; Atlas Advertiser Suite; AudienceScience; Auditude; Bizo; BlueKai; Brightroll; Brilig; Burstly; BV! Media; Caraytech; Casale; Cedexis; Chango; Chinauma; ClickBooth; ClickTale; CloudFlare; CNZZ; Cognitive Match; Commission Junction; Compete; Compuware; comScore; Connexity; Connextra; ContextWeb; contnet; Conviva; Core Audience; CPX Interactive; Criteo; Crowd Science; cXense; DataLogicx; DC Storm; Dotomi; Doubleclick; DoubleVerify; Dynamic Logic; Effective Measure; engage BDR; Ensighten; EQ Ads; Evidon; eXelate; Exponential Interactive; eyeReturn; Federated Media; Freewheel; Genieo; GoDaddy; Google Adsense; Greystripe; iAd; ICA; Improve Digital; Infonline; InSkin Media; Integral Ad Science; Invitemedia; iPerceptions; Komli Media; Krux; LeadBolt; Ligatus; Lijit; Lotame; Marketo; MaxPoint Interactive; Maxymiser; MdotM; Media6Degrees; Media Innovation Group; MediaMath; MediaV; Microsoft Ads; Millennial Media; Mixpanel; Moat; Mobile Theory; Monetate; Motrixi; MyBuys; Neobux; NetSeer; Neustar Information Services; Nexage; Nielsen; Nugg; OpenX; Optimizely; OptMD; OwnerIQ; PointRoll; Polldaddy; Proclivity; Proxistore; Pubmatic; Quantcast; RadiumOne; Resonate Networks; RichRelevance; Rocket Fuel; Rubicon Project; Scorecard Research; ShareThis; Silverpop; Simpli.fi; Siteimprove; SiteScout; Six Apart; Skimlinks; SLI Systems; Smart AdServer; Softpedia; SpotXchange; Surikate; Telecom Express; The Trade Desk; TLVMedia; TubeMogul; Undertone; Vibrant; VIEWON; VoiceFive; Weborama; Webtrends; Woolik; Xaxis; XiTi; X Plus One; Yabuka; Ybrant Digital; Yieldmanager; Zanox; ZEDO.
VOIP	Jajah; Lync; SGCP; Sightspeed; Viber.
Storage	2Shared; Badongo; Beatport; BitTracker; Boxnet; BTMon; Compressed File; Crocko; DB2; DDM-SSL; DRDA; Dropboks; DropSend; Egnyte; Elephant Drive; eSnips; FileFactory; FileSonic; FilesTube; FlipDrive; Foldershare; FreakShare; FreeDrive; GamesTorrents; Informix; IngresNET; Lets Create; LOCKSS; MaxDB; Mega; Mini SQL; Mozy; MS Global Catalog Secure; Microsoft Access; MS OLAP; MySQL; NovaBACKUP; Open Drive; Oracle Database; Oracle SQLNET; PostgreSQL; RapidShare; RIS; RoboForm; Sharingmatrix; SpiderOak; SQL Server; SVN; Syncplicity; Torrent 441; Torrent Hound; Torrent Ino; Torrent Leech; Torrent Reator; TowerData; WebLogic; Your File Host; Zenbe.
Collaboration	Aceproject; AmoebaOS; Aol Answers; Apple Remote Desktop; Asana; Atom; BeamYourScreen; BFGMiner; BitCoin; Getwork; Citrix Online; CVS; DeskAway; Dr. Watson; Fengoffice; Google Docs; Goplan; Group Greeting; Groupwise; iMeet; IMVU; Koolim; Links; Mavenlink; Meeting Maker; Mozilla; Octopz; Pbworks; PlusIM; Projectplace; Quick Base RSS; Saba Meeting; Sametime; Schmedley; ScreenToaster; Sharepoint; ShowDocument; Slack; SparkPeople; Springpadit;

	Sumo Paint; TeamBox; Thinkfree; Viewpath; Vote Yes or No; Vyew; WebAIM; Webex Teams; Writeboard; Zoho Wiki.
Mobile	050plus; 500px; AdobeAIR; AD-X Tracking; Airbnb; Alibaba; Amazon Cloud Player; Android browser; Android Client; Android Download Manager; Android Music; Anipang; AppleCoreMedia; Apple Stocks; Avaya Live; BBC iPlayer; Bebo; Resilio Sync; Blackberry browser; BlueStacks; BlueStacks apps; Brewster; Bria; Buffer; Burnbook; Campfire; Chat; ConnMan; Crittercism; Dictionary.com; DingDing; Dots; Engadget; Feedly; Fetion; Flipboard; Foursquare; Game Center; Glympse; GOMTV Remote Control; Google Duo; Google Earth; Google Hangouts; GREE; Hello; HIKE; HIKE Media; iBooks; iCal; Infinity Blade; INRIX; Instagram; Instapaper; iTunes iPad; iTunes iPhone; iTunes iPod; iTunes Music; iTunes Store; iTunes U; JetBrains; JetBrains feature; JetBrains plugins; KakaoTalk; Kik Messenger; Kontiki; Letterpress; Line2; Linphone; rlogin; Mailbox; MapMyFitness; Mention; Merriam-Webster; Microsoft Stream; Mobilatory; Mobile Device Useragent; Mobile Safari; Nateon; Nest Thermostat; Net2Phone; OCS; Office Mobile; Ovi Browser; Parallels; PDF Expert; Periscope; Philips Hue; Photo Stream; Pocket; Pogoplug; Power BI; Pushover; Readability; RealNetworks; RealPlayer Cloud; Remote Ctrl from iPhone/iPad; Samsung Push Notification; Snapchat; Spotify; ST; Stitcher; Telegram; Telenav; Tempo; TextMe; TextNow; textPlus; Tinder; TomTom; Viki; Vine; Vlingo; Voxer; We7; Weather; WeChat; WhatsApp; WhatsApp File Transfer; Windows Phone Browser; WPS Office; Xunlei Kankan; Yahoo! Mobage; Yik Yak; Youdao Dictionary; Zoho Assist; Zoho Connect; Zoho Docs; Zoho SalesIQ Chat; Zoho Social.
Update	Activesync; Adobe Software; Adobe Updater; Allmyapps; Apple Update; BitDefender; BlueStacks download; BlueStacks update; Eclipse; Eclipse Marketplace; Eclipse Updates; Fedora DSGW; Google Update; Java Update; JetBrains update; ksfetch; Microsoft Visual Studio; Microsoft Update; NVIDIA Update; Python-httplib; Red Hat; Sophos Update; SymantecUpdates; Syncml; Ubuntu Software Center; Ubuntu Update Manager; WD softwares Download/Update; Windows Update.
Protocol	3Com AMP3; 3COM-TSMUX; 914CG; 9P; ACAP; ACA Services; AccessBuilder; Access Network; ACI; ACR-NEMA; Active Networks; ActiveSync; Adobe PostScript; AED512; Aeolon Core Protocol; AEP; AFP; AgentX; Airsoft Powerburst; AJP; Alias; ALPES; AMANDA; AMInet; ANSA Notify; ANSA REX; Trader; ANSI Z39.50; any host; AODV; Apertus Tech Load Distribution; APNS; appleqtcsrvr; AppleShare; AppleTalk Unused 203; AppleTalk Unused 205; AppleTalk Unused 207; AppleTalk Unused 208; AppleTalk Routing Maintenance; AppleTalk Zone Information Protocol; ApplianceWare Managment Protocol; Applix ac; ARCISDMS; Argus; Ariel; Ariel2; Ariel3; ARIS; ARNS; Asipregistry; AS Server Mapper; AUDIT; Aurora; Aurora CMGR; AURP; Avian; Avocent; AX.25; BACnet; banyan-rpc; Banyan VIP; BBN RCC; BFTP; BGMP; BGP; bgs-nsi; BH611; BHEVENT; BHFHS; BHMDS; BITS; Blackjack; bmpp; BNA; Bnet; Boingo; Borland DSJ; Britton Lee IDM; BitTorrent; Bundle Discovery Protocol; Cableport AX; Cabletron Management Protocol; CAB Protocol; CadLock; CAICCI; CA Intl License Server; Call of Duty; campaign contribution disclosures; CAP; CBT; CDC; CDDB; CFDP; cFTP; CHAOSNet; Chshell; CIMPLEX; Cisco DRP; Cisco FNATIVE; Cisco GDP; Cisco NAC; Cisco SYSMAINT; Cisco; TNATIVE; Citrix Static; CL1; Clearcase; CLOANTO; CMIP/TCP Manager; Coda Auth; Collaborator; Combat Radio Transport Protocol; Combat Radio User Datagram; Common Trace Facility; Compaq-Peer; CompressNET; COMSCM; con; connendp; contentserver; Corerjd; Courier Mail Server; Covia; CP Heart Beat; CP Network Executive; cpq-wbem; Cray Network Semaphore server; Cray Unified Resource Manager; Creative Partner; Creative Server; Cross Net Debugger; CRYPTOAdmin; CSNET Mailbox Name Nameserver; CSTA; CU-SeeMe; Customer Ixchange; cvc_hostd; CVS pserver; CVSup; Cybercash; cycleserv; cycleserv2; DAAP; DASP; DataRampSrvSec; DataRamp Svr; DATEX-ASN; dBase; DCAP; DCCP; dcLINK; DCN Measurement Subsystems; DCP; dctp; DDM; DDM DFM; DDM RRDA; DDP; DDS; decap; DEC Auth; Decbsrv; DEC DLM; DECVMS; DEI-ICDA; Desknets; device; DGP; DHCP; DHCP Failover; DHCP Failover 2; DHCPv6;

Diameter; digital-vrc; D-II; DirectPlay; DirectPlay8; Direct TV; Software Updates; Direct TV Tickers; DirecTV Data Catalog; DirecTV Webcasting; Discard; distcc; DIXIE;

DLS; dls-mon; DN6-NLM-AUD; DNA-CML; DNP3; DNSIX; DOOM; DPSI; Dropbear; DSFGW; DSP;

DSP3270; DSR; DTAG; DTK; DTLS; DWR; eDonkey Static; EGP; EIGRP; EMBLNDT; EMC SmartPackets;

EMFIS-CNTL; EMFIS Data; Emission Control Protocol; Encapsulation Header; entomb; entrust-aaas;

entrust-aams; Entrust Administration Service Handler; Entrust-KMSH; Entrust SPS; EntrustTime; Epic;

Epmap; ERPC; errlog copy/server daemon; ESCP; eSignal; ESP; ESRO; ESRO-EMSDP V1.3; EtherIP;

ETOS; Eudora Set; FastCGI; FastTrack; Fatmen; FCP; FDSSDP; FileMaker; Finger; Fink; FLEXlm; FLN-SPX

X font server; FTP; FTP Active; FTP Passive; FTPS; FTP Software Agent System; Fujitsu Device Control;

FXP; GACP; gdomap; GDS DataBase; Genie; GENRAD; GGP; ginad; GIOP; GIST; GKrellM; Glide; Glype

Proxy; GMTP; GNU Generation Foundation NCP 678; GoBoogy; Gopher; GotoDevice; GPFS; Graphics;

GraphOn Login; GRE; Groove; GSI-FTP; Gss X License Verification; GTP User; GVFS; ha-cluster;

Hamachi; HAP; Hardware Control Protocol Wismar; Hassle; HDAP; HELLO Port; HEMS; Heroix;

Longitude; Hitachi Universal Storage Platform; HL7; HMMP Indication; HMMP Operation; HMP;

Hostname server; HP Network Management Center; HP Perf; HTTP; HTTPMGT; HTTP RPC Ep Map;

HTTPS; Hybrid Point of Presence; Hyper-G; Hyperwave-ISP; iafdbase; IAFServer; IASD; IATP; IAX; IBM

App; IBM Director; IBM NetView DM; IBM NetView DM/6000 Server/Client; IBP; ICAD; ICL coNETion

locate server; ICL coNETion server info; ICMP; ICMP for IPv6; ICP; Ident; idfp; IDP; IDPR; IDPR Control

Message; IDRP; IDXRad; IEC 60870-5-104; IEEE-MMS-SSL; iFCP; IFMP; IGMP; IGRP; IMGames; IMP

Logical Address Maintenance; IMSP; InBusiness; i-nlsp; Intecourier; Integra Software Management

Environment; Internet Configuration Manager; Internet telephony tool; intrinsa; ipcd; IPComp; IPCU;

ipdd; IP in IP; IPLT; IP Mobility; IPP; IPv6 encapsulation; IPX over IP; IPX over UDP; IRC; IRCS; IRC-SERV;

iRODS; IRTP; ISCSI; ISI Graphics; ISIS; ISO ILL Protocol; ISO IP; ISO MMS; ISO SAP; ISO-TP0; ISO

Transport Class 2 Non-Control over TCP itm-mcell-s; ITU H.323; iWARP; Jargon; Java RMI; JBoss

Remoting; Kali; K-Block; Kerberos; Kerberos Administration; Key Server; KFTP; KFTPDATA; KIS; Klogin;

KNETCMP; Konspire2b; kpasswd; Kryptolan; kshell; lanserver; LDAP; LDAPS; LDP; Leaf-1; Leaf-2;

Legent; LEGENT-2; ListProc; ljk-login; LLMNR; Locus ARP; Locus Map; Locus PC-Interface Conn Server;

Loglogic; lpr; LWAPP; MacOS Server Admin; Magenta Logic; Mailbox-LM; maitrd; Management Utility;

MANET; Masqudialer; MATIP; MATIP-TYPE-B; McAfee AutoUpdate; MC-FTP; McIDAS; mcns-sec;

mdc-portmapper; Medipac; Memcomm; Meregister; MERIT Internodal Protocol; Metagram; Meter;

MF Cobol; MFE; MFTP; micom-pfs; MICP; Micromuse-lm; Microsoft Global Catalog; Microsoft Rome;

Microsoft Shuttle; Microsoft System Center Operations Manager; mit-ml-dev; MIT ML Device; MIT

Spooler; MobileIP; MobilIP-MN; Mobility XE protocol; Modbus; Monitor; Moodlebot; MortgageWare;

MPLS; MPM FLAGS Protocol; MPTN; MQTT; MRM; MSA; MS CRS; MSDP; MS Exchange Routing;

MSG; msg-icp; MSMQ; Microsoft NCSI; MSOC File Transfer; MSP; Microsoft Web Platform Installer;

Microsoft WNS; MTP; Multiling HTTP; Mylex-mapd; WINS; NARP; NAT-PMP; NBP; NCED; NCLD; NCP;

nCube License Manager; NDMP; NDS Auth; Nest Protocol; NetBackup; NetBIOS-dgm; NetBIOS-ns;

NetBIOS-ssn (SMB); NETBLT; netGW; Netinfo; Netix MPP; Netnews Administration System; Netop

Remote Control; NETSC; NETSC-DEV; NetScout; netvmg-traceroute; NetWall; Netware; Network based

Rev. Cont. Sys.; Networked Media Streaming Protocol; NetWorker; Network Innovations Multiplex;

Network PID Checker; NetWorker Data Setup; Network Systems; New who; NeXTStep; NFA; NFS Lock

Daemon Manager; NI FTP; Nintendo WFC; NIP; nlogin; Nmap; NNSP; NNTP; NNTPS; Novadigm EDM; Novell Netware over IP; npmp-gui; npmp-local; NPMP Trap; NPP; NQS; NSFNET-IGP; NSIIOPS; NSRMP; NSS; NSSTP; NSW User System FE; NTP; NVP; NXEdit; OBEX; OCBinder; OCS_CMU; OCServer; OFTP; OFTPS; Ohimsrv; OLSR; Omginitialrefs; Omron FINS; Omserv; Onmux; opalis-rdv; OPC; OpenDoor; Openport; openvms-sysipc; Operations Manager - Health Service; TNS/Oracle; oracle; Oracle Business Intelligence; Oracle coauthor; Oracle Names; Oracle Net8 CMan Admin; Oracle Net8 Cman; Oracle Remote Data Base; Oracle TCP/IP Listener; Orbix 2000 Config; Orbix 2000 Locator; Orbix 2000 Locator over SSL; ORBIX-CFG-SSL; OSPF; OSUNMS; P10; Packet Radio Measurement; PAPI; PARC Universal Packet; Parsec Gameserver; PassGo Technologies Service; Password Change; Path; PCoIP; PDAP; PDL data streaming port; PDRE; Personal Link; PFTP; PGM RTP Pharos psrserver; Philips Video-Conferencing; Phonebook; Photuris; PIM; PIM-RP-DISC; PIP; PIPE; pirp; PKIX-3 CA/RA; PKIX Timestamp; Pluribus Packet Core; Plus Fives MUMPS; PNNI; POV-Ray; PowerChute; PRM Node Man; PRM Sys Man; PROFILE; PROSPERO; PScribe; PTC Name Service; PTP; PTP Event; PTP General; PubNub; PubSubHubbub; pump; PureNoise; PVP; PWDGEN; Python urllib; Qbik; QFT; QMQP; QNX; qrh; QUIC; Quotad; Radio Control Protocol; RADIUS; Radmin; Rational Method Composer; RDA; RDT; RealVNC; Reliable Datagram Protocol; RemoteFS; Remote-KIS; Remote Method Invocation Activation; repcmd; repscmd; ResCap; Retrospect; RIP; RIPng; RLP; RLZ Dbase; RMCP; rmiregistry; Rmonitor; RMT; rmtis; ROHC; RPC2PMAP; RRH; RRP; RSH-SPX; RSVD; RSVP-E2E-IGNORE; RSVP Tunnel; rtip; RTP; RTSPS; RUSHD; Russell Info Sci Calendar Manager; RVD; rxe; SAFT; Sage; SANity; SAP; SATNET; SATNET and Backroom EXPAK; SATNET Monitoring; SCCM; SCCP; SCC Security; Schedule Transfer Protocol; SCO Desktop Administration Server; scohelp; Sco I2 Dialog Daemon; SCO System Administration Server; SCO WebServer Manager; SCO Web Server Manager 3; SCPS; scx-proxy; SDNS-KMP; SDRP; Secure IRC; SecurSight; Semantix; Semaphore Sec Pro; SEND; Sender Rewriting Scheme; Service Status Update; SET; sFlow; SFS config server; SFTP; Shrinkwrap; Siam; SIFT; SILC; Silverplatter; Sitara Dir; Sitara Management; Sitara Server; SKIP; Skronk; SMAKYNET; Smart Session Description Protocol; SMID; SMP; smpnameres; SMPTE; smsd; SMSP; SNA Gateway; SNARE; SNET; SNNTP; SNP; SNPP; SNTP-HEARTBEAT; Soap; SOCKS; SoftEther; SoftPC; Softros LAN Messenger; Sonar; Splunk; SPMP; Sprite RPC; spsc; SQLSRV; Squid; SRC; SRMP; SRP; SRVFP; srvloc; ss7ns; SSCOPMCE; SSL; SST; STMF; Stock IXChange; streettalk; STUN; STUN over TLS; Submit Protocol; SUBNTBCST_TFTP; SUNDR; Sun IPC server; SUN NDP; Sunquest; Sun RPC; Survey Measurement; SVMTP; Swipe; Sybase SQL; Synergy; Synology DSM; SynOptics SNMP Relay; SynOptics Trap; TACACS+; Tanium; Tapeware; TCF; TCPMUX; TDP; TDS; TeamSound; Technical Analysis Software; Teedtap; tell; TELNETS; TenFold; TESLA; Texar; TFTP; Thin Manager TFTP; TIA/EIA/IS-99 modem client; TIA/EIA/IS-99 modem server; TIME.com; Time; Timeserver; tinc; Tivoli; TLSP; TNS CML; tn-tl-fd1; Tobit David; Tobit David Replica; Tomatopang; TP++; TP4; TPCP; TPIP; TPKT; TPNCP; Transport Independent Convergence; trin00; Trunk-1 Protocol; Trunk-2 Protocol; TRUSTe; TTP; TURN Channel; UAAC; UARPS; UDP Lite; UIS; Ulpnet; Ultrasurf; Unidata LDM; Unify; Unix time; UPMC; UPnP; UPS; User Location Protocol; UTI; UTMPCD; utmpsd; UUCP; UUCP-PATH; UUCP-RLOGIN; uuidgen; VACDSM-APP; VACDSM-SWS; VATP; vemmi; vettcp; Vid; Videotex; Virtual Presence Protocol; VISA; VMNET; VM PWSCS; VMTP; VMware Fault Domain Manager;

	vnas; VPPS-Via; VRRP; vsinet; VSLMP; VVPS-Qua; Wang Span; WAP connectionless session service; WAP Push; WAP Push OTA-HTTP port; WAP Push OTA-HTTP secure; WAP Push Secure; WAP secure connectionless session service; WAP Session Service Secure; WAP Session Service; WAP vCal; WAP vCal Secure; WAP vCard; WAP vCard Secure; War-rock; WCCP; Webfilter; WebSphere MQ; webster WESP; whoami; Wideband EXPAK; Wideband Monitoring; Wii Shop Channel; WLCCP; World Fusion; wpgs; WSDD; XWindows; xact-backup; Xbone; XDMCP; Xfer; XNS; XNS Authentication; XNS Clearinghouse; XNS Time; XTP; xvttp; Xyplex; Zebra.
Games	4399.com; 9p.com; Addicting Games; Aliexpress; Angry Birds; AOL Games; Armagetron Advanced; Armor Games; Battlefield; Battle.net; Battle.net site; Bejeweled Blitz; Bejeweled Chrome Extension; Bet365; Bigpoint; Blizzard; Blizzard Downloader; Blockbuster; Blokus; Bubble Island; Bubble Saga; Bubble Witch Saga; Cabal Online; CanvasRider; Castleville; Cityville; Clear Channel; Destructoid; Diamond Dash; Doof; DoubleDownCasino; EA Download Manager; The Escapist Magazine; ESTsoft; Evony; Farmville; Fire FOX FreeStreams; G4; Game Front; Game Informer; GameSpot; GameSpy; GameStop; GameTrailers; Geewa; GOMTV.net; GTA Online; Hangame; Hattrick; hi5; Ifeng.com; Isoball; Joystiq; King.com; Kongregate; Kotaku; League of Legends; Lineage; LINE Games; Magicland; MapleStory; Mesmo Games; Minecraft; Miniclip; MyOnlineArcade; Neopets; Newgrounds; Nexon; NFL.com; Nintendo; OnLive; PartyPoker; Planetarium; Playdom; Playstation.com; Playstation App; Playstation Games; Pogo; Pool Live; PopCap Games; Premier Football; PSP Activity Agent; PS3 Community Agent; PS3 Downloads; PS3 Home Client; PS3 Messenger; PS3 Updater; PSP Community Agent; Playstation Store; QQ Games; Quake; Quake Live; Raptr; Rockstar Games; RuneScape; Second Life; Shopkick; Slotomania; Social Empires; Sohu.com; SpeedRunsLive; StationLauncher; Steam; Tango; Taringa; Tetris Battle; The Elder Scroll Online; Verizon; VMware Horizon View; Widget Media; Wii; Wooga; Words With Friends; World of Warcraft; Xbox Live; Xbox Live sites; Xfire; Y8; Yahoo! Games; Yeti Bot; Zynga; Zynga Poker.
Business	1-800-Flowers; 1&1 Internet; 5pmweb; 6.pm; 7digital; 99Acres; Ace Hardware Corporation; Acer; Acrobat; Adorama; Airspace; Alibaba; Allstate; Amazon; AMD; American Express; Android.com; Apple Push; Apple sites; Apple Store; Argos; Asus; AutoTrader.com; AutoZone; Backpack; Bank of America; Barnes and Noble; Barneys New York; Best Buy; BitCoin; Blackberry sites; Blackbox; Bloomingdales; Bluefly; Blue Nile; BonPoo; Booking.com; Boxoh; CamerasDirect.com.au; Capital One; CarMax; CC Studios; CDiscount; Central Desktop; Chase; CheapOAir; CheapTickets; Chinaren; Chrome webstore; Citi; Citrix; City Sports; Clarizen; CNET; CNET Download; CNET TV; Concur; CORBA; Costco; Craigslist; Crutchfield; Dangdang; David Jones; Deals Direct; Dell; Dicks Sporting Goods; Dillards; Discover; Drugs.com; Drugstore.com; East Money; eBay Bid; eBay Search; eBay Watch; eBuddy; Edmunds.com; EndNote; E*TRADE; Etsy; Expedia; Fidelity; Fifth Third Bank; Flipkart; Fnac; Freee TV; Frys Electronics; FTD; Gateway; Geico; GoBank; GO.com; Google ads; Google Finance; Google Play; Google Product Search; Google Play Books; Groupon; Home Depot; House of Fraser; H&R Block; HSBC; IBM; IKEA.com; InstaCalc; Intel; Investopedia; IKE; it168; J.C. Penney; Jetsetz; JIRA; J.P. Morgan; Kaspersky Network Agent; Kay Jewelers; Kismet; Kiwoom; Kmart; Kogan Technologies; Kohls; Launchpad; Leap Motion sites; Liberty Mutual; LinkedIn Upload; LiteCoin; Lockerz; LOVEFiLM; Lowes; Luminate; Macys; MakeMyTrip; Megaproxy; Menards; Microsoft Store; MobileAsset; Mondex; Moneycontrol; Morgan Stanley; Morningstar; Motorola; Napster; NBA; NBC; Neckermann; Neiman Marcus; Newegg; Nike; Ning; Nordstrom; NSEIndia; Nvidia; Office 365 Planner; Office Depot; OfficeMax; oo.com.au; Opalis Robot; OPC-UA; Orbitz; Overstock.com; PayPal; PC Connection; Pchome; PC Mall; PDBox; PDF;PerfectIBE; Photoshop; PNC Bank; Prezi; Priceline.com; ProFlowers; Publishers Clearing House; Quill Corporation; QVC; Raging Bull; Redmine; REI; RevenueHits; REVOLVEclothing; RitzCamera.com; Rona; Saks Fifth Avenue; Sams Club; Samsung; Schwab; Scottrade; Sears; Seterus; The Sharper Image; Shoplet; ShopNBC; ShopStyle; ShorTel Sky Communicator; ShowClix; Skype for Business; Snapdeal; Soribada; Sports

	Authority; Staples; Starbucks; State Farm; StubHub; StudentUniverse; SugarCRM; Swarovski; Target; Tchibo; TD Ameritrade; TechCrunch; TED; Tesco.com; Theme Forest; ThinkGeek; Ticketmaster; Tickets.com; TicketsNow; Tiger Direct; Toshiba; Trac; Travelocity; Travelzoo; TripAdvisor; Tripave; Tripwire; T. Rowe Price; Twiddla; UC4; Unicenter; Urban Outfitters; USAA; Vanguard; Vehix; vente-privee.com; Victorias Secret; Voyages-sncf.com; Wachovia; Walmart; Wells Fargo; Wimbledon; Windows Phone sites; WiZiQ; Woot; Wretch; Wrike; Wunderlist; Yahoo! Finance; Yatra; Yodiz; Zales; Zappos; Zip.ca.
Streaming	4Tube; 56.com; 5by5 Radio; Aaj Tak; AccuWeather; ADNStream; Ado Tube; Adweek; Afreeca; AirPlay; AirTunes; AllRecipes; Amazon Instant Video; Ando Media; AOL Video; Apple Music; Apple Trailers; Apple TV; Apple Mobile Yahoo API; Ask.com; Asterisk PBX; Audible.com; AudioDocumentary.org; Autoblog; Axis Camera Stream; Babelgum; Baidu Movies; The Baltimore Sun; Bandcamp; BeeMP3; BesTV; Bild.de; Biography.com; Blekko; blinkx; Blip.tv; Boxee; Break.com; Brightcove; Brighttalk; BuzzFeed; CAM4; CBS; CBS Interactive; CCP; Games; Channel 4; Cheezburger; China Daily; Cisco SIP Gateway; Telepresence Control; ClearSea SIP Client; ClickBank; Cloud Browse; Clubbox; CNBC; CNN.com; Collider; Comedy Central; Cox; Crackle; Crackle Video; Crunchyroll; C-SPAN; CTV; CTV News; Cute Overload; Dailymotion; Deezer; DEOS; DeviantClip; Dilbert.com; Djpod; Dropcam; Drudge Report; EarthCam; Edge; eHow; EmpFlix; EngageMedia; Entertainment Weekly; ESPN; ESPNcricinfo; ESPN Video; Examiner.com; Extremeube; Facebook Photos; FFFFOUND!; FilmOn; FiOS TV; Flash Video; Food Network; FORA.tv; Fotki; FreeCast; FreeSWITCH; Fuq; Fuyin.TV; GG; GIFSoup.com; GOLF.com; GOMTV.com; Google+ Videos; Google Play Music; Graboid; Grantland; Groove Music; Gyao; HardSexTube; HBO; HBO GO; HostGator; Hotstar; HTTP Video; Hulu; Hulu Video; The Hype Machine; I Catcher Cam Streaming; IceShare; iHeartRadio; Indiegogo; iTunes; iTunes Desktop; I Waste So Much Time; Jamendo; Jango; JoinMe; Justin.tv; KBS; Keez Movies; Kickass Torrents; Kodi; Kuaibo; KVOA.com; Last.fm; LA Times; Lequipe.fr; LeTV; Library of Congress; LINE; LINE Media; Live365; LiveFlash; LiveJasmin; Livestream; Lycos; lynda.com; Maestro FM; Manta; Marca; Mashable; Matsushira_Camera_Stream; mck-ivpip; Media Hub; Media Stream Daemon; MegaPorn; Megavideo; MelOn; Metacafe; MixBit; Mixcloud; MKRU Streaming; MobiTV; Mobotix Camera Stream; MOG; Movieclips; MovieTickets.com; MTv; Myspace Videos; NAMP; NBC News; NCAA; Nero SIP Client; Netcam; Netflix; Netflix stream; News Distribution Network; news.com.au; Newser; NHL.com; Nico Nico Douga; Nico Nico Douga Video; NOAA; Nokia Music; NSPlayer; Nuance Voice Platform; NY Daily News; The New York Times; Ogg; Ooyala; Open Films; OpenSIPS; OSSProxy; Outbrain; Panasonic Camera; Pandora; Pandora Audio; Pandora TV; Paramount Network; PBS; Penultimate; People.com; Peoples Daily; People Of Walmart; Picsearch; Piksel; Plex TV; PNAS; POLITICO.com; Pop Salad; Pornhub; Pornorama; Pornoxo; PPStream; PPTV; QDown; Qriocity; Quickflix; QuickTime; QVOD; Rakuten; RealAudio; RealClearPolitics; Reality Kings; Realview TV; Redbox; Redbox Instant; Rediff.com; RedOrbit; RedTube; Reuters; Rhapsody; Roku; RTMP; RuTube; SBS; Shockwave; SHOUTCast Radio; Showbox; SHOWTIME; ANYTIME; Silverlight; Sina Video; SIP; sipXecs; Slacker; Slate Magazine; Slingbox; Slutload; Social-TV; Songs; Songza; Sony Camera Stream; SopCast; SoundCloud; SOUNDROP; Southern Living; SpankWire; Spiegel Online; Sports Illustrated; Square Inc.; Starsports; Star TV; Stereomood; Stickam; Streamate; StreetFire; SURF; TeacherTube; Telly; Tencent Video; The Atlantic; The Blaze; theCHIVE; The Guardian; The Internet Archive; The Week Magazine; Tianya; Tidal; Tightrope Interactive; TMZ; TNAFlix; TopTenREVIEWS; Toshiba Camera; Stream; Tube8; Tudou; TuneIn; Turntable; Tu TV; Tvigle; TVonline.cc; TVU Networks; TwitchTV; Twitter Video; UltraViolet; UOL; USA Today; Ustream.tv; Vdio; VDOLive; Veetle; Veoh; VEVO.com; Viddler; Video Sift; Videosurf; Viewsurf; Vimeo; VLC Media Player; Vonage; Vube; WeatherBug; Weather.com; Weather.gov; WebM; WebM Files; Webs; wetpaint entertainment; wimp.com; Winamp; Windows Media; Windows Media Player; Wired.com; WorldstarHipHop; WTOP; Xhamster; Xiami.com; The Xinhuanet; Xlite SIP Client; XM Radio Online; Xnxx; X-PRO SIP Client; Xtube; Xvideos; XXX Tld; Yahoo! Douga; Yahoo! Flash;

	Yahoo! Screen; Yandex; Yellow Pages; You Jizz; Youku; You Porn; YouTube; YouTube Comment; Youtube Upload; yuvutu; Zattoo; Zaycev; Zippyshare; Zoom.
Cloud	360 Safeguard; 4chan; AOL Instant Messenger; AIM Express; AOL Instant Messenger Netscape; Aliwangwang; Animoto; Avast; Avira Download/Update; BaiduHi; Chatroulette; Check Point; Cisco Jabber; Eset; F-Prot; F-secure; Google Talk Gadget; GSS HTTP; HipChat; ICQ; ICQ2Go; imo.im; ircu; Jabber; Kaspersky; Malwarebytes; Malware Defense System; McAfee; Mediamax; Messenger; Mibbit; MMS; MPM; MSN Messenger; MSNP; Microsoft Windows Messenger; NeoGAF; Nessus; Nimbuzz; ntalk; Omegle; Panda; Pinger; QOTD; QQ; Rypple; Skype Auth; Sophos Live Protection; SUPERAntiSpyware; Symantec System Center; talk; Tencent Cloud; Tinychat; TOC; Vchat; Web Of Trust; WooMe; xda-developers; Yahoo! Messenger; Yahoo! Messenger SMS; YiXin; Zoho Chat.
Web	12306.cn; 2345.com; 2channel; 2Leep; 39.net; 58 City; Abonti; About.com; Acoon.de; Acrobat.com; Adap.tv; Adcash; AddThis; AddThis Bot; AddToAny; Adenin; AdF.ly; Admin5; Adobe Analytics; Adobe Connect; AhrefsBot; Aili; AIM HTTP API; Airtime; Aizhan; Akamai; Akamai NetSession Interface; Alipay; Alisoft; Aliyun; Al Jazeera; Allegro.pl; Allmusic; ALTools; Ameba; American Airlines; Ancestry.com; Android Asynchronous Http Client; Answers.com; AOL; Apache Nutch; Apple App Store; Apple Developer; Apple iForgot; Apple Maps; Apple PubSub; Apple qtpix; Apple Syndication; Aptean; ArcGIS; Arizona Public Media; Arora; ArtStack; ASA; ASF; Asia Times Online; Associated Press; Astraweb; AT&T; auditd; Autodesk; Autohome.com.cn; Avaya; Aweber; Amazon Web Services; Azure cloud portal; Babylon; Backpage.com; Backupgrid; Baidu; Baiduspider; Balatarin; Bazaarvoice; BB; BBB; BigBlueButton; Bing; Bing Bar; Bingbot; Bing Maps ioDigital Human; Bitcoin Forum; BitGravity; bitly; Bizrate; Blackboard; BlekkoBot; Bloglovin; Bloomberg; Bluehost; BoldChat; Bootstrap CDN; Boxcar.io; Browzar; Business Insider; California.gov; Car and Driver; Carbonite; CareerBuilder.com; Catho; CBS Sports; Character Generator; Chartbeat; CheapStuff; Chickipedia; Chimera2; China.com; China News; Chosun; Chrome; Cisco; Cisco Phone; CiteULike; Cleartrip; CloudFront; CloudMe; Coc Coc bot; Collabedit; CollegeHumor; CometBird; Commerce; Comodo Dragon; Conduit; Connexion client; Constant Contact; Convore; Coral CDN; Coupa; Coupons.com; Coursera; Crazy Browser; Creative Commons; CrossLoop; CSDN; cURL; CyberGhost VPN; The Daily Beast; Datei.to; Daum; Daum Blog; Daum Cafe; DCinside; Delta Search; Demandbase; DeNA websites; De Telegraaf; Detroit Free Press; DICOM; Digg; Diigo; DioDeo; DirBuster; Disney; Disqus; DNS; Dogpile; DomainTools; Dooble; Dragon Dictate; Drawbridge; Drupal; DSW; DuckDuckGo; Dwolla; EA Games; EarthLink; Easou Spider; easyMule; eBay; EdgeCast; Edge Chromium; EditGrid; eFax; Egloos; Elinks; Enet; Envato; E! Online; Epiphany; eRecht24; eRoom; Etao; European Union; EVE Online; Evernote; Exchange Online; ezhelp; Eznet; Fab.com; Fancy; Fark; Facebook Applications Other; Facebook Games; Facebook Notes; Facebook Sports; Facebook Utilities; FC2; FedEx; Feed43; FeedBurner; Feedfetcher; Feedly Fetcher; Fileguri; FileHost.ro; FireAMP; Firefox; Fiverr; Flexera Software; Flickr; Flightradar24; Flock; Flurry Analytics; FogBugz; folkd; Forbes; The Free Dictionary; Freelancer; FriendFinder; FrostWire; Funny or Die; Ganji; The Gap; Garmin; Gawker; Gazprom Media; Gbridge; Genieo Web Filter; Ghostery; Giganews; GitHub; Gizmodo; Glype; GNOME; GNU Project; Goal; GOGOBOX; Goodreads; GoodSync; Google; Google Accounts Authentication; Google Analytics; Google APIs; Google App Engine; Googlebot; Googlebot Image Search; Google Calendar; Google Code project hosting; Google Drive; Google Fiber; Google Groups; Google Maps; Google News; Google PageSpeed; Google+ Photos; Google Remote Desktop; Google Safebrowsing; Google Sign in Google Translate; Google URL Shortener; goo.ne.jp; GoToMeeting; GoToTraining; Gravatar; GreenBrowser; GSA Crawler; Guangming Online; Haiku Learning Systems; Hao123.com; Harvard University; Helpshift; HIP; HLN; The Hollywood Reporter; HootSuite; Hopster; Hotels.com; HotPads; HowardForums; HP Home & Home Office Store; HubPages; The Huffington Post; HugeDomains.com; Hupu; iBackup; ICA Browser; IFTTT; iFunny; IGN; IloveIM; Image Venue; IMDB; IMRWorldWide; Inbox.com; In.com; Indeed;

	Indiatimes; Info.com; InfoSeek; Infusionsoft; InsightExpress; Integromedb Crawler; Intermarkets; Internet Explorer; Intralinks; Intuit; IPFIX; iStock; Jalopnik; Java; jdistatic; JetSetMe; JikeSpider; Jimdo; Jingdong (360buy.com); Johns Background Switcher; JonDo; Joomla; Joongel; JSTOR; JustCloud; Justdial; K9 Web Protection; Kakao Story; Kayak; Kickstarter; Konqueror; Kooora.com; Kraken; Leboncoin; Legacy.com; Level 3; Libsyn; Libwww-Perl; Licorize; Limelight; LINK; LinkedIn Inbox; LinkedIn Profile; Linux Mint; Livedoor; Livefyre; LivePerson; LiveStrong.com; LivingSocial; Localytics; Loyalty Innovations; Lynx; Mac App Store; MacPorts; MagicBricks; MagPie; MapQuest; Mathworks; MCStats; MDNS; Mediabot; Meebo; MegaMeeting; Mercado Livre; MetaCrawler; MetaFilter; MGID; Mgoon; Michigan Radio; Microsoft; Microsoft CRM Dynamics; Midori; Mikogo; Mint.com; MissLee; MJ12 Bot; MKRU; MLive; Monster.com; Mop.com; Motley Fool; Microsoft CryptoAPI; MSDN; Microsoft download; MSN; msnbot; Microsoft Excel; MS Office Existence Discovery; Microsoft Powerpoint; MS Office Protocol Discovery; Microsoft Word; MyLife; MyPCBackup; Myspace Photos; MyWebSearch; NAI; NASA; Nate; NATO; Naukri; Naver; Naver Blog; Naver Cafe; Naverisk; ndgsa-crawler; Netease; Neteller; Netnews; NetNewsWire; NetSurf; Netvibes; New Relic; NewsNow; Newsvine; NextBus; NIH; Nokia; Nokia Maps; Nokia Store; Norton AntiVirus; NPR; Nuance; OCLC; OCSPD; Office 365; Office365 Admin portal; OkCupid; Okta; OpenBSD; OpenDNS; OpenSUSE; Opera; Oracle sites; OsiriX; OverBlog; Owlinbot; PACS; PaleMoon; Panoramio; Pastebin.com; Patch.com; Paybill; Perforce; Phoca; PHP; phpBB; PHP-SOAP; Picasa; Picnik; Pingdom; Pivotal Tracker; PixelMags; Plista; Podio; PopUrls; Powermarks; Presto; Printer Pro Desktop; Progressive; PS3 web browser; Psiphon; QQ Music; QQ Pay; QualysGuard; Quick Look; Quora; Quote.com; R6 FeedFetcher; Rackspace; Radian6 CommentReader; Rainmeter WebParser; Rambler; Real Estate ABC; Realtor.com; reCAPTCHA; Reddit; rekonq; RetailMeNot; Rotten Tomatoes; rsync; Safari; Salesforce.com; Salesforce.com Live Agent; Sanook.com; Seamonkey; Searchnu; Search-Result.com; The Seattle Times; SendSpace; ServiceNow; SFGate; Shareman; Sharepoint Online; Shockwave Flash; ShopAtHome; ShowMyPC; Show My Weather; Shutterfly; Shutterstock; Silk; simple-get; SimplePie; Siri; Sky.com; Slashdot; Slickdeals; SlideShare; Slothtrader; SM; SmugMug; Snort.org; SockShare; Softonic; Sogou; Sogou web spider; Soku; Songsari; Sony; Soso; SOS Online Backup; Soufun; Sourcefire.com; Sourceforge; Southwest Airlines; Space.com; SPC Media; Speedtest; Speedtest Upload; Sprint; SPS; SSL client; Stanford University; StatCounter; Storify; StreamWork; StumbleUpon; SugarSync; SuperNews; SurveyMonkey; Svpply; Swagbucks; Tagoo; Taobao; TechInline; Technorati; Tencent; The Independent; The Onion; The Telegraph; TikTok; TimesJobs; Times Union; TinyPic; Tiny Tiny RSS; TinyURL; TISTORY; Tmall; T Mobile; Top Gear; TOR; ToysRUs; Trend Micro; Trulia; TruuConfessions; Tumblr; TurboTax; Turner Broadcasting System; Tus Files; TV Guide; TweetDeck; Twitter Link Service; Twitter Music; Ubuntu; UltraView CCS; United Airlines; Uptobox; UpToDate; Urban; Airship; URLAppendBot; urlgrabber; U.S.Bank; USPS; uTorrent; Venmo; Ventrilo; VeriSign; Verizon Wireless; VMware Server Console; Voilabot; VPNReactor; w3schools.com; Walgreens; wApua; WarriorForum; The Washington Post; Washington Times; WDT; WeatherLink; Weather Underground; Webcrawler; WebEx; WebEx Connect; WebMD; Websense; Weebly; Western Digital; WeTransfer; WhereCoolThingsHappen; WhitePages Inc; Wikia; wikidot; Wikipedia; Wikispaces; Microsoft Windows Live Services Authentication; Windows Help client; Wolfram Alpha; Wondershare; Wood TV8; Woopra; Wordpress; WordReference.com; Workday; WorldCat; Wow; Wyzo; Xanga; Xcode; Xenu Link Sleuth; XProtectUpdater; Yahoo!; Yahoo! Calendar; Yahoo! Slurp; Yahoo! Toolbar; Yammer; Yandex Bot; Yandex Images; Yesky; YY; Zamzar; Zapier; Zbigz; Zendesk; ZergNet; Zhihu.com; Zillow; ZipCloud; Zipskinny; Zmags; Zoho; Zol.com.cn; Zombo.com; Zulily.
Portal	B&H Photo Video; Black & Decker Corporation; Cisco SLA; Cloudnymous Login; CMIP; daytime; echo; Honeywell Experion DSA Server Monitor; Fanpop; Fotolog; Fring; Google Reader; Google Toolbar; Hideman Login; Hide My Ass!; Hindustan Times; Hola; Honeywell Control Station/NIF Server; Hotwire; ibVPN Login; In; Indian Railways; IRCTC; Ivacy Login; J&R; L2TP;

	Lord & Taylor; Megaco; MGCP; MSN2Go; Munin; MUX; Ngrok; Opera VPN; RAP; RSVP; RTSP; SGMP; Sina; Skype; SMPP; SMUX; SNMP; Stat Service; Sulekha; Systat; TeamSpeak; Tiffany & Co.; Tunnelbear Login; Twitter4J; UMA; USAIP; VyprVPN Login; whois; WX; Yahoo! Voice; Zabbix; Zabbix Trap; Zero VPN.
P2P	100Bao; ABC; Aimini; Applejuice; Ares; Baidu Yun; BaoFeng; BearShare; BitComet; BitTornado; BitTorrent; Direct Connect; eDonkey; ExtraTorrent; Faroo; FilesWire; GnucleusLAN; Gnutella; Gnutella2; GoBoogy; Hotline; iMesh; Joost; KAD; Kugou; Manolito; Mininova; Mute; MyMusic; Paltalk File Transfer; PeerCast; PeerEnabler; Pipi; The Pirate Bay; Poco; PPTV; SoulSeek; TheCircle; BitTorrent tracker; Torrentz; Vuze; WinMX; Xunlei; Yet ABC; YoTorrent.
Download	Android Marketplace Download; Apple Pipeline; Advanced Packaging Tool; BackWeb; FlashGet; Microsoft AutoUpdate; MyDownloader; Wget; Zedge.
Database	Gfycat; ScienceDirect.
News	Usenet; U.S State; Western Journalism.
Browser Plugin	Grammarly; Honey.

Custom groups and custom signatures are configured according to the applications listed above.

For more information about Application Control, access this link.

UTM - Services - Intrusion Prevention

The Intrusion Prevention System is responsible for monitoring and analyzing network traffic in order to identify malicious code traffic and attacks. By using subscription-based rules and sensors, it is able to analyze the content of all traffic passing through the network, and is also responsible for identifying targeted and persistent applications and threats as well as blocking them. Integrated with a base of electronic signatures it acts in the application layer, capable of analyzing the contents of packages in real time, identifying and blocking the package or even the origin IP.

The system also acts as a threat detector (IDS - Intrusion Detection System) when the signature is enabled on the NGFW.

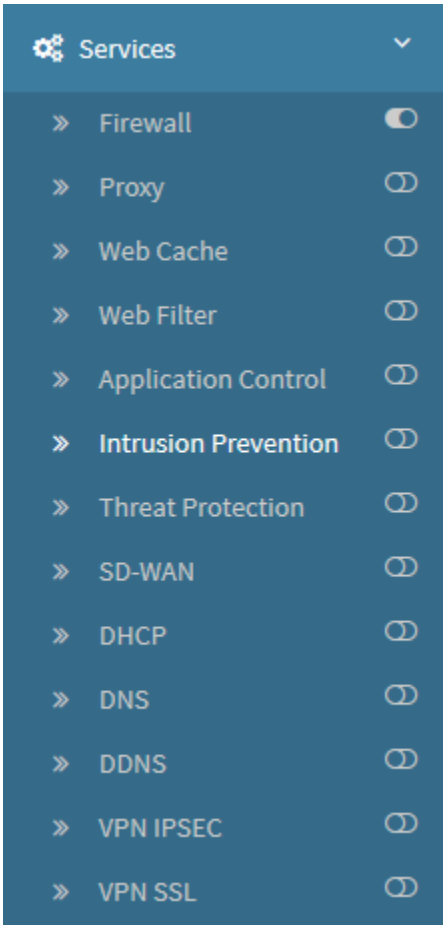
Based on signatures, rules and sensors, it compares and analyzes the content of all “Redirected” Inbound/Outbound traffic to it through detection mechanisms: signatures, protocol anomalies, application control and generates the records of all identified packages in its signature base, whether it is the execution of unauthorized applications, an invasion attempt, or an attack directed to the equipment itself, suporting some techniques such as: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion and Layered Evasions.

The IPS also supports the following VoIP protocols verification:H.323, SIP, MGCP and SCCP.

By default, IPS has more than 72.835 signatures (information validated on November 25, 2021).

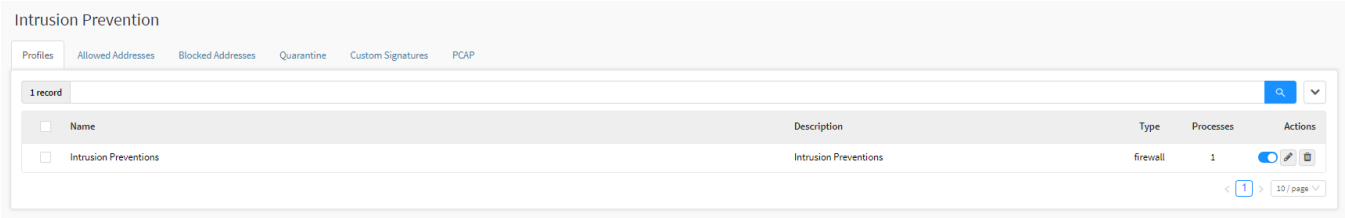
It is worth mentioning that this total amount of subscriptions is dynamic and these subscriptions are managed by the Blockbit Labs Team.

To access this screen, just select the option “Intrusion Prevention”.



Services - Intrusion Prevetion

The screen below will appear:



Intrusion Prevention

The Intrusion Prevention screen has the following tabs:

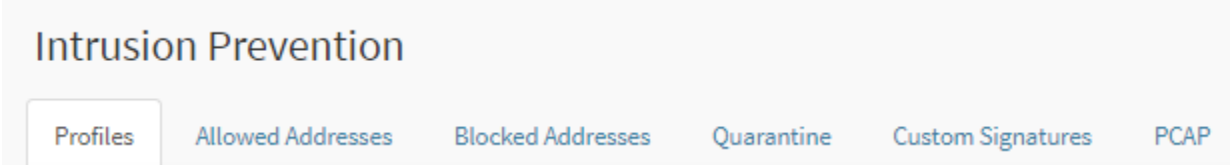
- *Profiles;*
- *Allowed Addresses List;*
- *Blocked Addresses List;*
- *Quarantine;*
- *Custom Signatures;*
- *PCAP.*

Next we will analyze the components of the Profiles tab.

Intrusion Prevention - Profiles tab

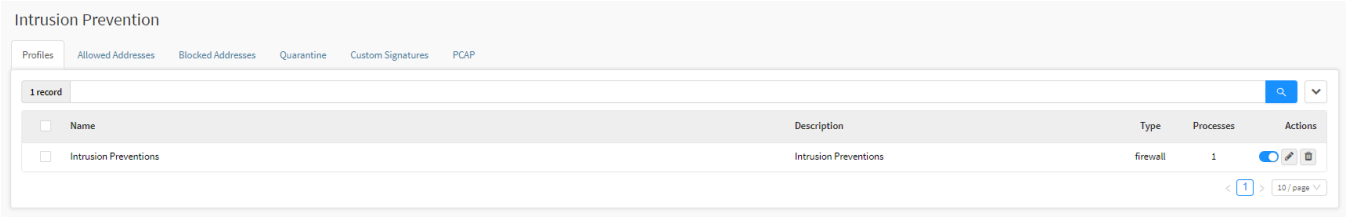
Through this tab it is possible to create protection profiles against threats and exploits of possible vulnerabilities in your network.

If the tab is not selected, click on "Profiles".



Profiles tab

The Intrusion Prevention “Profiles” screen will appear, as shown in the image below:



Intrusion Prevention - Profiles

This session will cover how to register, edit and remove Intrusion Prevention profiles;

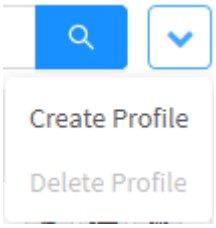
Next, we'll look at the functions located at the top of this panel.

Intrusion Prevention - Profiles Tab - Actions Menu

At the top right of the screen we have the actions menu:

Intrusion Prevention – Actions Menu Button

By clicking on this button the menu below is displayed:



Intrusion Prevention – Actions menu

The menu consists of the following options:

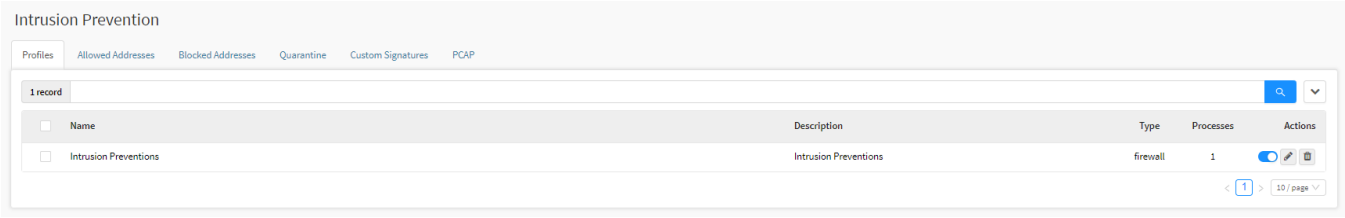
- Create Profile;
- Delete Profile.

Next, each action menu option will be detailed.

Intrusion Prevention - Profiles tab - Delete Profile

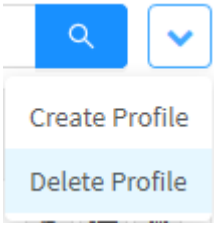
Through the button “Delete Profile” it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Ex.: Test;



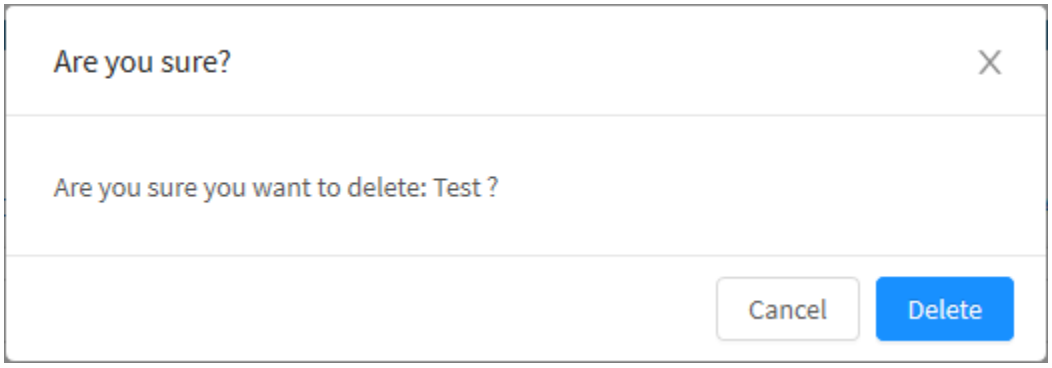
Intrusion Prevention – Selection of Profiles to delete

2. Enter the actions menu [ ] and click on the option “Delete Profile”.



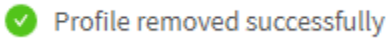
Intrusion Prevention – Delete Profile

3. The notification message will appear asking if you really want to delete the selected Profiles:



Intrusion Prevention – Deletion confirmation message

If you want to cancel, click the [Cancel] button. To finish, click the [Delete] button.



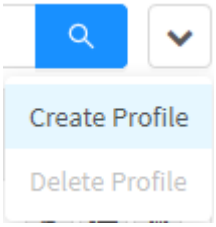
Profile successfully removed

After these procedures, the profiles will have been successfully deleted.

Intrusion Prevention - Profiles tab - Create Profile

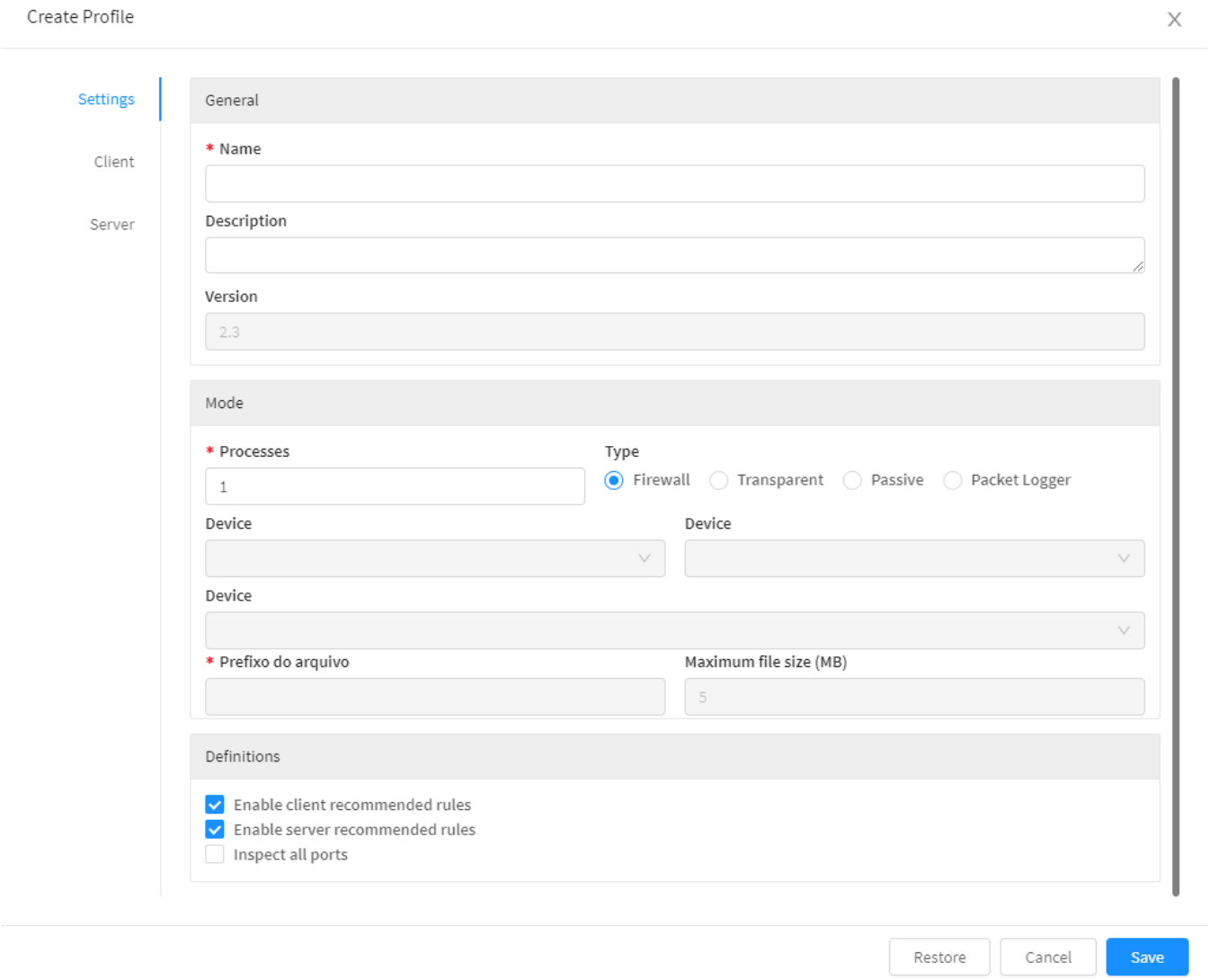
Through the “Create Profile” option it is possible to create a new Intrusion Prevention profile. To access, click on the actions menu **[**  **]**.

1. Click on the “Create Profile” option;



Intrusion Prevention - Create Profile

2. The “Add Profile” screen will be displayed. Fill it with the following data:



Settings tab

In this tab it is possible to make the general configurations, definitions and the mode of action of Intrusion Prevention.

General

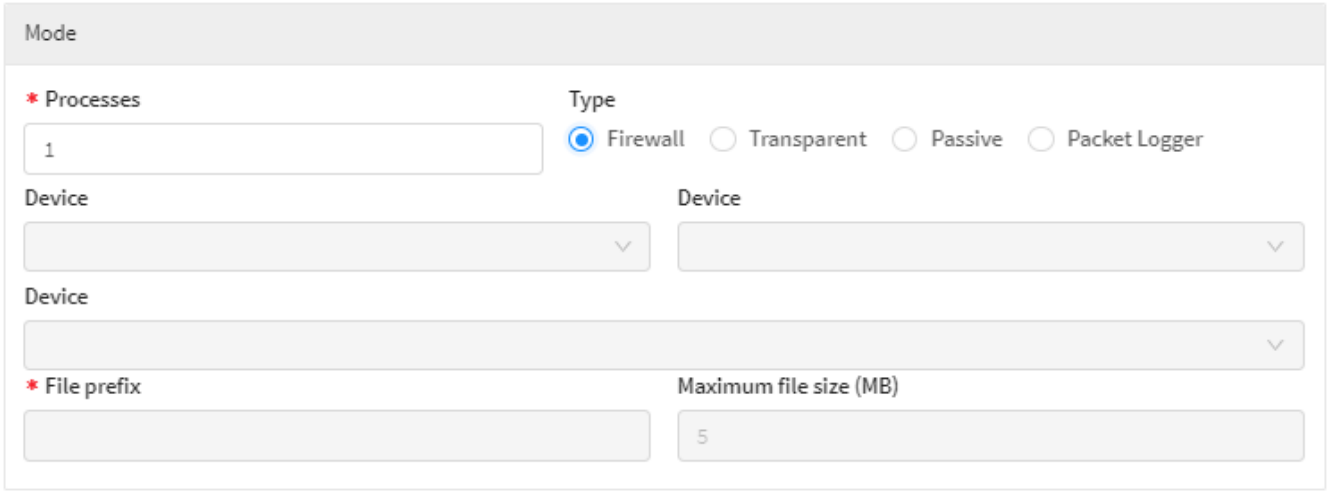
In "General" we have the following text boxes:

Intrusion Prevention – General

- ***Name:*** *Define a name for the profile*. Ex.: Malware Prevention;
- ***Description*****:** Set a description for the profile. Ex.: Block Malwares*;*
- ***Version:*** Determines the version in which the profile was created.

Mode

In "Mode" the applications are determined whose access will be allowed or denied:



Intrusion Prevention - Mode

- ***Processes:*** *Select the number of simultaneous processes to load the profile*. Each process refers to a thread. We recommend that this value is set as " less or Equal" to the number of processing cores in your Appliance*. This field is mandatory*.
- ***Type:*** *Select the IPS Operation Mode*. The available types are: Firewall, Transparent, Passive and Packet Logger;
    - ***Firewall*****:** This mode works as a system of "Protection oriented to Network Assets" through the "Security Policies" it is possible to establish rules of protection against intruder "profiles" oriented for each "network service", "protocol" or even "security network "directing packet traffic for analysis by the IPS;
    - ***Transparent*****:** This mode works as a sniffer applied directly to the network interface. It uses a system of "capture, filtering and analysis of packets at high speed". In simple terms, it is an acceleration agent that allows packets in a single interface to be segmented into multiple threads / cores, allowing for more efficient packet processing. Packages are inspected at a much lower level than traditional sniffer or package engines, thereby reducing resource costs and increasing the efficiency of your device.

About Transparent Mode:

- ***Transparent mode is supported only by physical appliances.***
- *Allows Port mirroring, which is a technique that copies network traffic from one port on a switch or router to another for analysis.*
  The copied traffic is then sent to a network analyzer, intrusion detection system, or another monitoring device.

    - ***Passive*****:** This mode works by monitoring the network and generating log "records" of all packages identified in your subscription base, regarding threats and attacks, taking no action on the malicious package. Operates in bypass mode.
    - ***Packet Logger:*** This mode allows the analysis and capture of the data packets flow, and logging the recorded packets into a report.
- ***Device (Flow):*** This item is only required for configuration in *"Transparent" mode*. Select the packet targeting flow. The flow is determined by the input device of the packet. *Ex.: Eth2 : Eth3*;
- ***Device (Flow):*** This option is also made available in *"Transparent" mode* and allows the selection of a secondary packet input device.
- ***Device (Interface):*** This item is only required for configuration in *"Passive" mode*. Select the incoming packet flow network interface. *Ex.: Eth2*.
- ***File Prefix:*** Prefix of the output file type.
- **Maximum File Size (MB):** Size of the output file, containing the packets flow data.

In the Flow and Interface fields, the network interfaces must be "enabled" and without an IP address. As shown below:

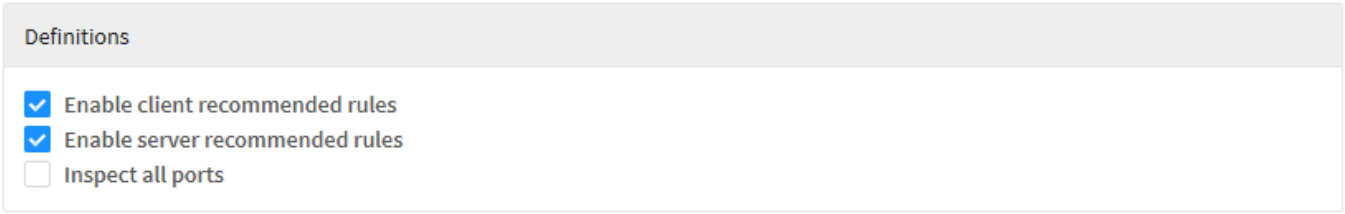
Interface	Address	Gateway	Type	Zone	Action
eth0	-	-	Physical	-	
eth1	172.31.102.220/16	-	Physical	LAN	
eth2	-	-	Physical	-	
eth3	-	-	Physical	-	

Network Interfaces - Example

For more information on how to configure the interfaces check this page.
In addition, to avoid fragmentation, it may be necessary to increase the MTU values of the interfaces. For more information on this, see this page.

Definitions

In "Definitions" are determined the applications whose access will be allowed or denied:



Intrusion Prevention - Definitions

- ***Enable client recommended rules [✓]:*** *This option enables the display of standard Blockbit ATP rules*. These rules will be displayed on the client tab;
- ***Enable server recommended rules [✓]:*** This option enables the display of Blockbit's standard IPS rules. These rules will be displayed on the server tab;
- ***Inspect all ports[✓]*:** Enables independent inspection of the port the application is running on.

Enabling the Inspect all Ports option limits the process of your network traffic.

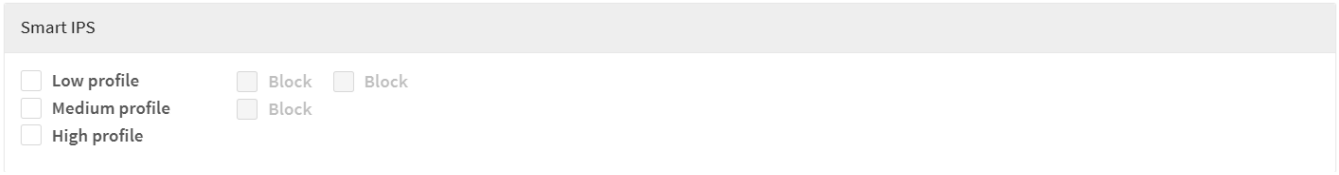
Smart IPS

In Smart IPS, you can enable the Smart Intrusion Prevention System, which looks for malicious activities in packets and can report or block them.

The system classifies packets into three groups according to risk:

- Low profile: low risk;
- Medium profile: medium risk;
- High profile: high risk.

To enable Smart IPS, select a risk level.

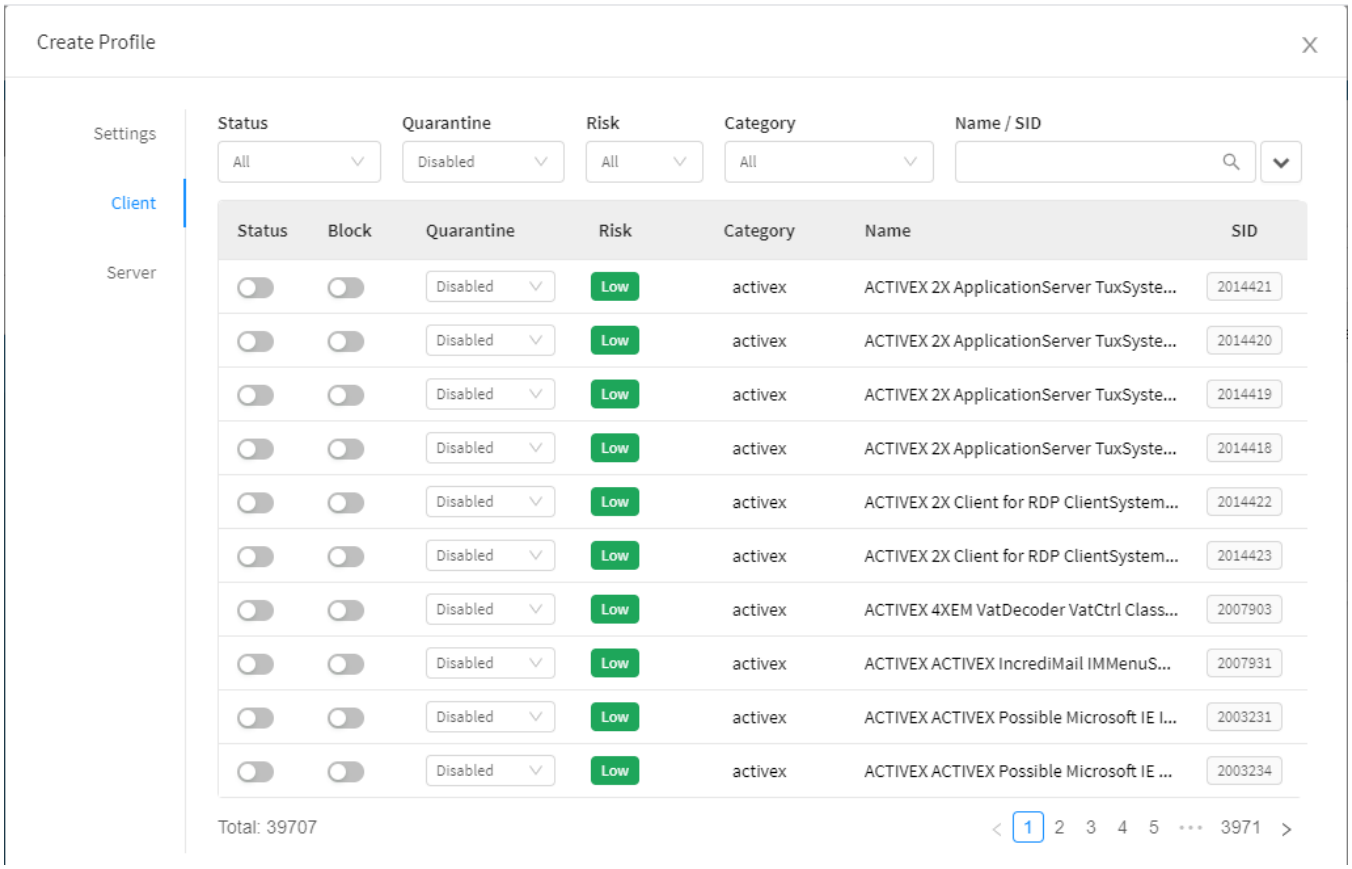


When selecting a risk level (e.g., medium profile), the block box is enabled. By clicking it, packets with the respective risk level will be blocked. By clicking the first Block, only medium risk packets will be blocked. By clicking the second Block, which is enabled when low risk is selected, low risk packets will be blocked.

Standard rule definitions are disabled automatically when Smart IPS is enabled.

Client Tab

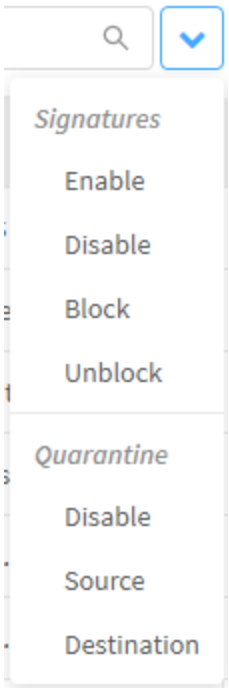
When enabling the ***Enable client recommended rules [✓]*** option in the Settings tab, the Client tab will display the signatures as shown below:



Intrusion Prevention - Client

The signatures are divided as follows:

- ***Status*:** Defines the current state of the subscription, the options are:
  - *All*;
  - *Enabled*;
  - *Disabled*;
  - *Blocked*;
  - *Unblocked*.
- ***Quarantine*:** It is possible to enable or disable the quarantine option informing if it will be validated by source or destination IP. *By enabling the quarantine option automatically, the system will enable the signature with the* ***block*** *status. With that, all traffic that matches the signature will dynamically insert the address into the quarantine in this way, keeping it blocked according to the time that was configured for quarantine*;
- ***Risk*:** Which determines the risk of the signature based on the criticality and complexity of the attack that can be of the types:
  - *Low;*
  - *Medium;*
  - *High.*
- ***Category*:** Defines subscription groups that serve the same purpose;
- ***Name / SID*:** This field allows you to determine the signature name in the system or the signature unique identifier (SID) or CVE code. It's also possible to search for the signatures that are in quarantine, enabled, disabled, among others;
- ***Action [ ]:*** It is possible to manipulate signatures that have been filtered, according to the following options:



Intrusion Prevention - Actions

To change the action of a specific subscription of the base, click on the [/] of "Status" and "Block" of the respective subscription that you want to "Enable / Disable".

It's important to notice that when the service is enabled [Enable], it works on IDS mode (Intrusion Detection System) and will detect and report suspicious signatures. However when the [Block] function is turned on, the suspicious signatures will be blocked and moved to the quarantine.

When activating the **Enable client recommended rules** or **Enable server recommended rules** checkbox in the Definitions tab, some SIDs will be highlighted, the SID in blue is the standard recommended by Blockbit (for example, when editing any of them, it will become gray).

See the example below, where third and fourth SID are highlighted:

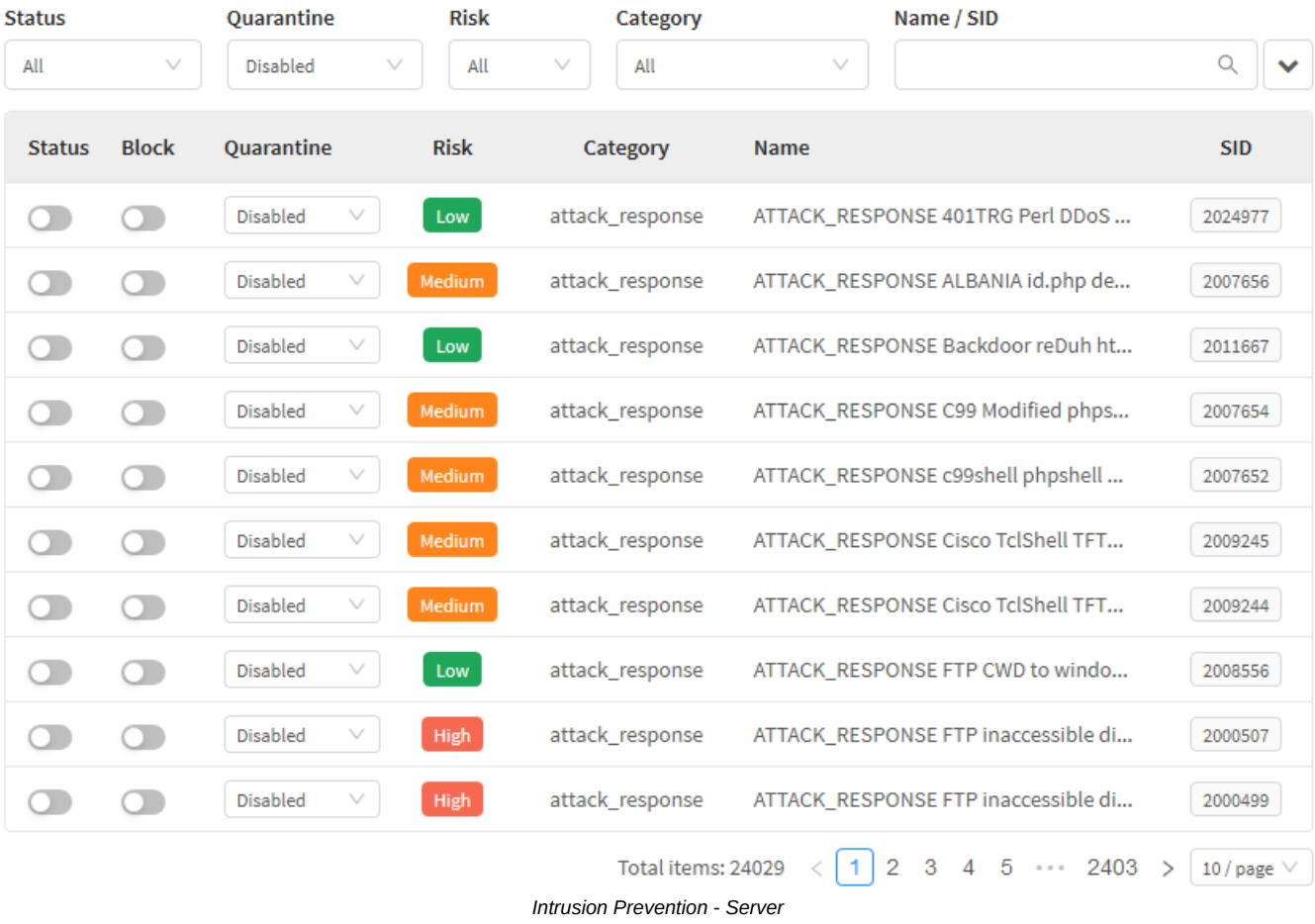
Status	Block	Quarantine	Risk	Category	Name	SID
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46978
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46977
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49360
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49361
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21446
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21447
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome flo...	19710
		Disabled	Medium	browser-chrome	BROWSER-CHROME Google Chrome FT...	16795
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16667
		Disabled	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16668

Intrusion Prevention - Highlighted SID example

The system has a search panel where it can perform searches according to the information entered in the fields previously mentioned, for that, click on **[ ]** .

Server Tab

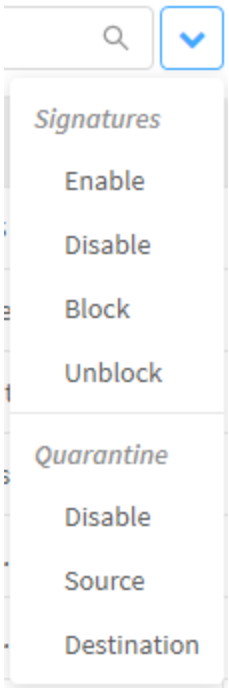
When enabling the **Enable server recommended rules *[ ]*** option in the Settings tab, the Server tab will display the IPS signatures as shown below:



Intrusion Prevention - Server

As in the **Client** tab, signatures are divided as follows:

- ***Status*:** Defines the current state of the subscription, the options are:
  - *All*;
  - *Enabled*;
  - *Disabled*;
  - *Blocked*;
  - *Unblocked*.
- ***Quarantine*:** It is possible to enable or disable the quarantine option informing if it will be validated by source or destination IP. By enabling the quarantine option automatically, the system will enable the signature with the ***block*** status. With that, all traffic that matches the signature will dynamically insert the address into the quarantine in this way, keeping it blocked according to the time that was configured for quarantine;
- ***Risk*:** Which determines the risk of the signature based on the criticality and complexity of the attack that can be of the types:
  - *Low;*
  - *Medium;*
  - *High.*
- ***Category*:** Defines subscription groups that serve the same purpose;
- ***Name / SID*:** This field allows you to determine the signature name in the system or the signature unique identifier (SID);
- ***Action [ ]:*** It is possible to manipulate signatures that have been filtered, according to the following options:

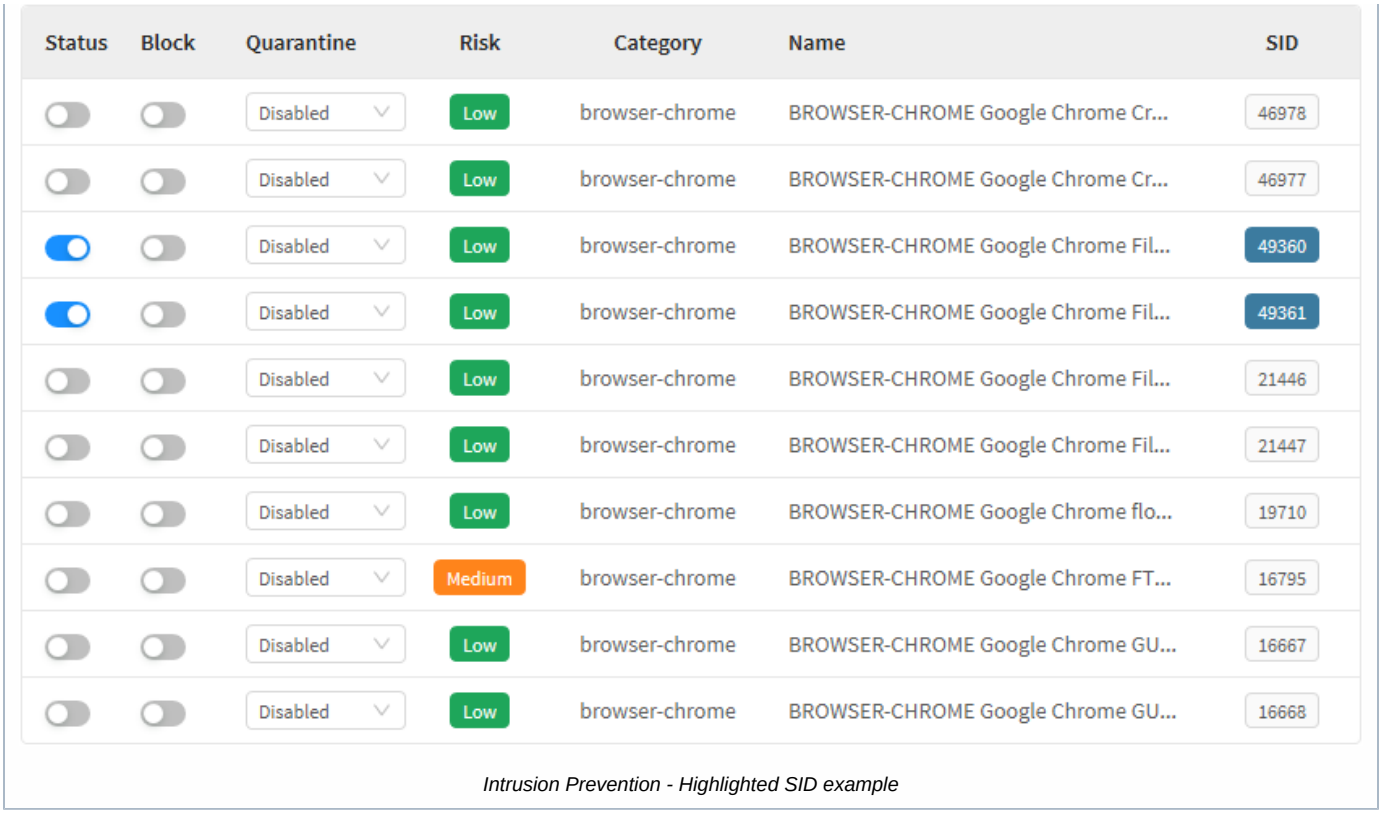


Intrusion Prevention - Actions

To change the action of a specific subscription of the base, click on the **[** / **]** of "Status" and "Block" of the respective subscription that you want to "Enable / Disable".

When activating the ***Enable client recommended rules*** or ***Enable server recommended rules*** checkbox in the Definitions tab, some SIDs will be highlighted, the SID in blue is the standard recommended by Blockbit (for example, when editing any of them, it will become gray).

See the example below, where third and fourth SID are highlighted:

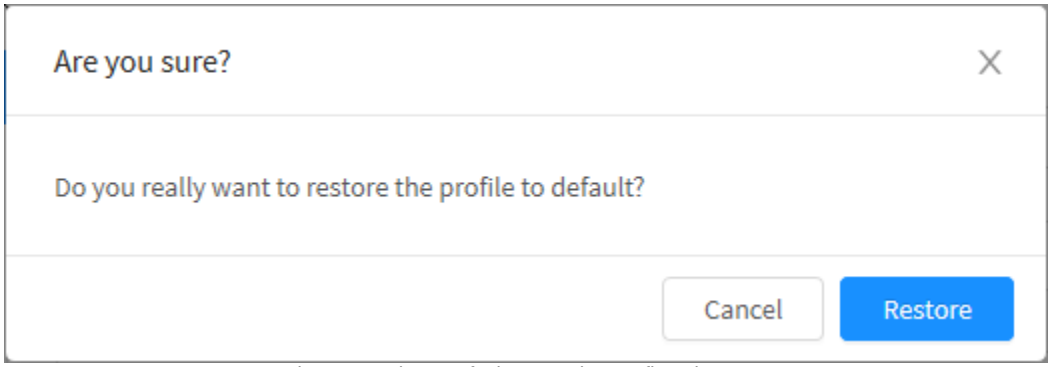


Intrusion Prevention - Highlighted SID example

The system has a search panel where it can perform searches according to the information entered in the fields previously mentioned, for that, click on **[** **]** .

Restore button

If at any time you want to restore the profile and default settings of Blockbit, click on **[** Restore **]**, the following window will be displayed.

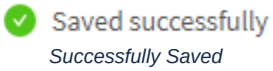


Intrusion Prevention - Default restoration confirmation message

Click the **[** Cancel **]** button to exit this window or the **[** Restore **]** button to restore.

Profile restored

Finally, if you want to cancel click the **[** Cancel **]** button. To finish editing the applications click on the **[** Save **]** button.

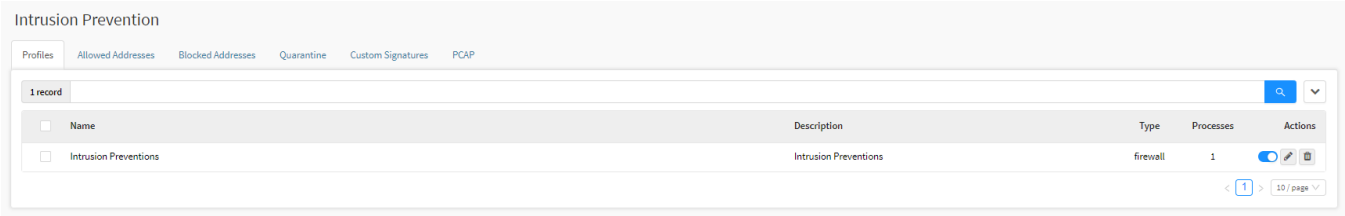


Successfully Saved

The settings have been successfully made.

Intrusion Prevention - Profiles tab - Columns

Below we will explain each column of the Intrusion Prevention tab:



Profiles – Intrusion Prevention

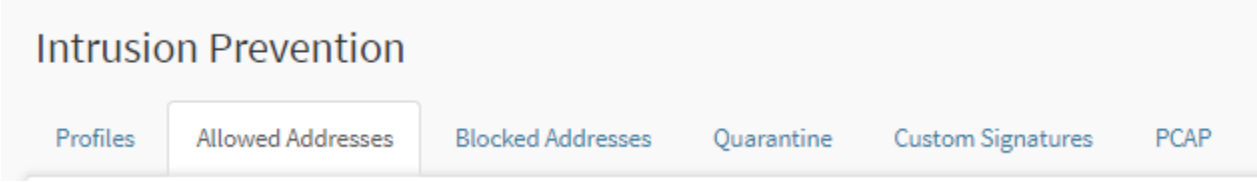
We will explain each column below:

- **Checkbox[ ]:** Select profile*;*
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- **Type:** It determines what type of prevention will be applied. The available options are Firewall, Transparent and Passive;
- **Processes:** Determines the number of simultaneous processes for loading the profile. Each process refers to a thread. We recommend that this value is set " less or Equal" to the number of processing cores in your Appliance;
- ***Actions*:** The "Actions" column consists of the following buttons:
    - ***Edit* [ ]:** Allows you to edit the profile settings added in the *Create Profile* option of the actions menu;
    - ***Delete* [ ]:** Delete the profile, equivalent to the *Delete Profile* option in the actions menu.

Intrusion Prevention - Allowed Addresses tab

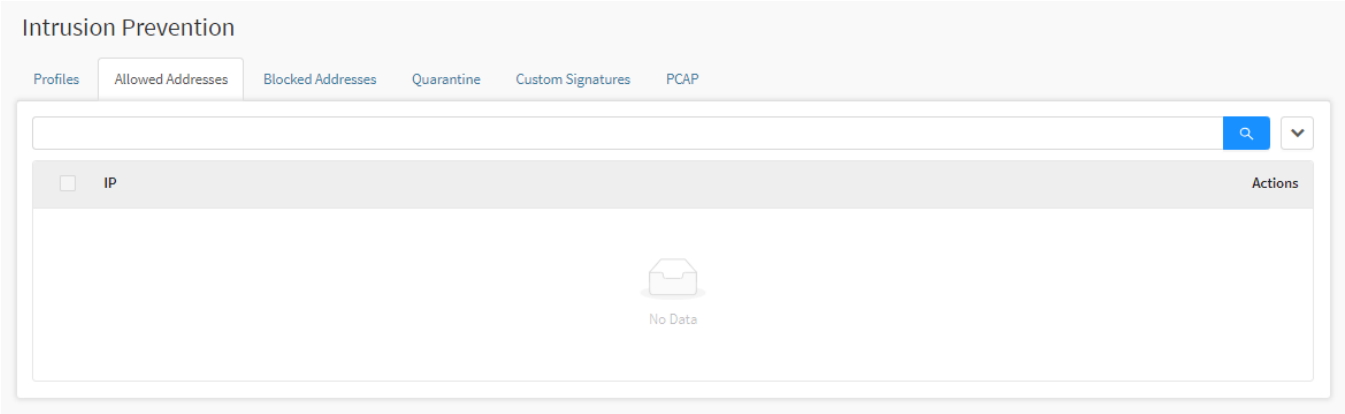
In the Allowed Addresses tab, it is possible to register IPs from both source and destination, or even import a list of IPs to be considered reliable and bypass Intrusion Prevention subscriptions.

If the tab is not selected, click on "Allowed Addresses".



Allowed Addresses tab

The Intrusion Prevention “Allowed Addresses” screen will appear, as shown by the image below:



Intrusion Prevention - Allowed Addresses

This session will cover how to register, edit and remove Allowed IPs from Intrusion Prevention;

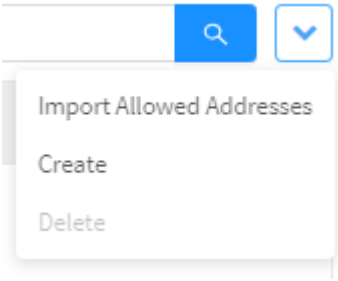
Next, we'll look at the functions located at the top of this panel.

Intrusion Prevention - Allowed Addresses tab - Actions menu

At the top right of the screen we have the actions menu:

Intrusion Prevention – Action Button

By clicking on this button the menu below is displayed:



Intrusion Prevention - Allowed Addresses - Actions menu

The menu consists of the following options:

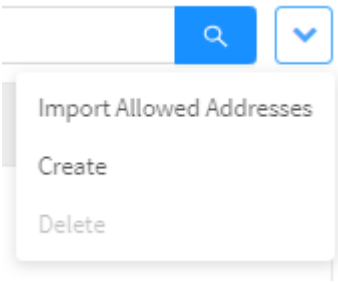
- *Import Allowed Addresses;*
- *Create*;
- *Delete*.

Next, each action menu option will be detailed.

Allowed Addresses - Actions Menu - Import Allowed Addresses

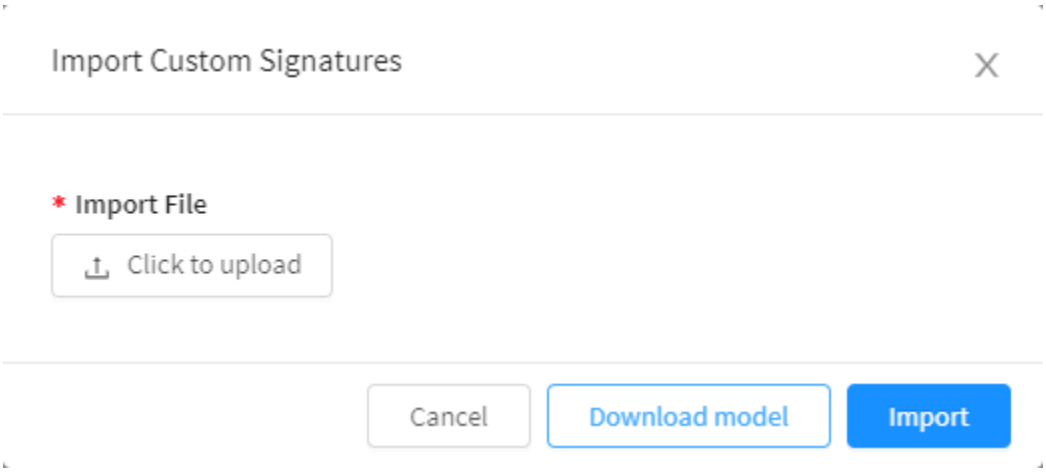
Through the option “Import *Allowed Addresses* ” it is possible to import some *Allowed Addresses* for the NGFW. To access, click on the ***actions menu*** **[**  **].**

1. Click on the “Create Profile” option;

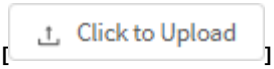


Allowed Addresses - Action menu - *Import Allowed Addresses*

2. The “Import Allowed Addresses” screen will appear. As shown on the image below:



Allowed Addresses - Import Allowed Addresses

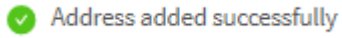
3. Select the desired file by clicking the **[**  **]** button:

This button accepts files with a .txt extension

4. Uppon the successful file upload, the confirmation message bellow will be displayed:

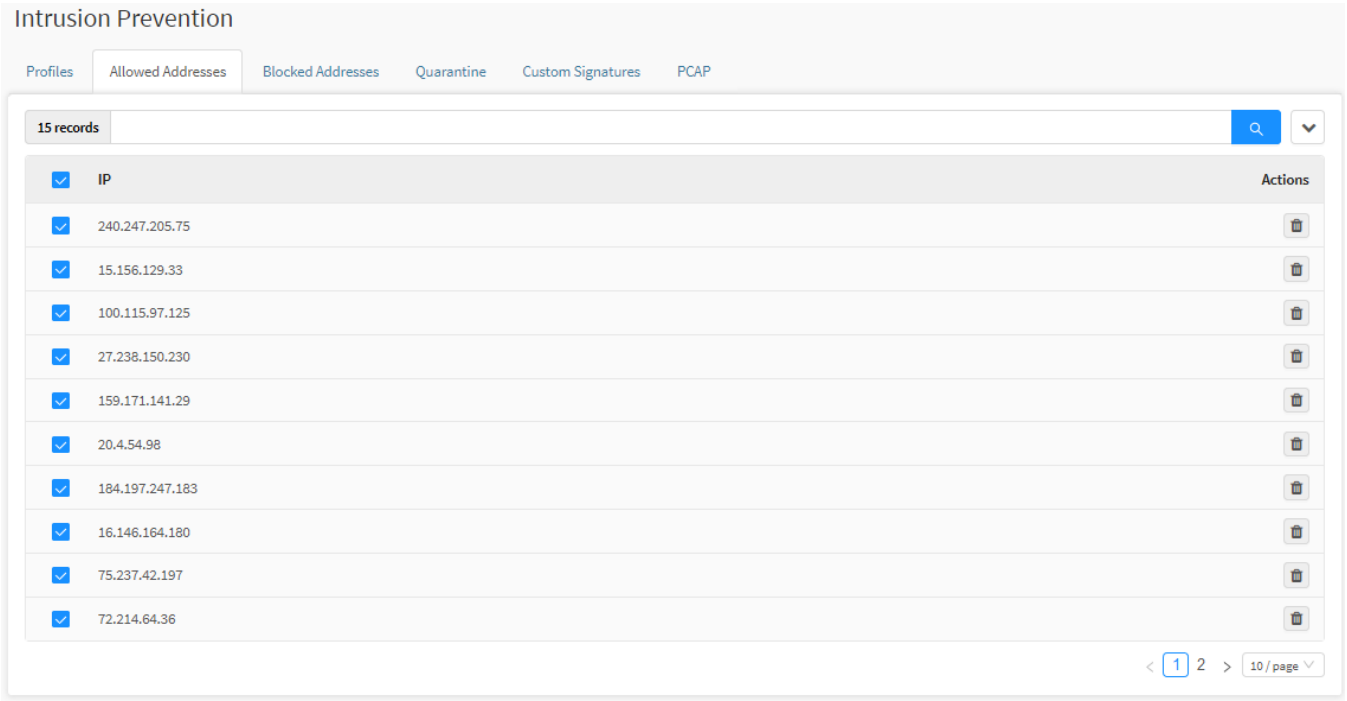
Item(s) successfully imported

5. When you finish adding the items, the following confirmation message will be displayed:



Address successfully added

6. Finally, the screen will display all the added IPs:



Allowed Addresses - Added IPs

After performing these procedures, the import process will have been successful.

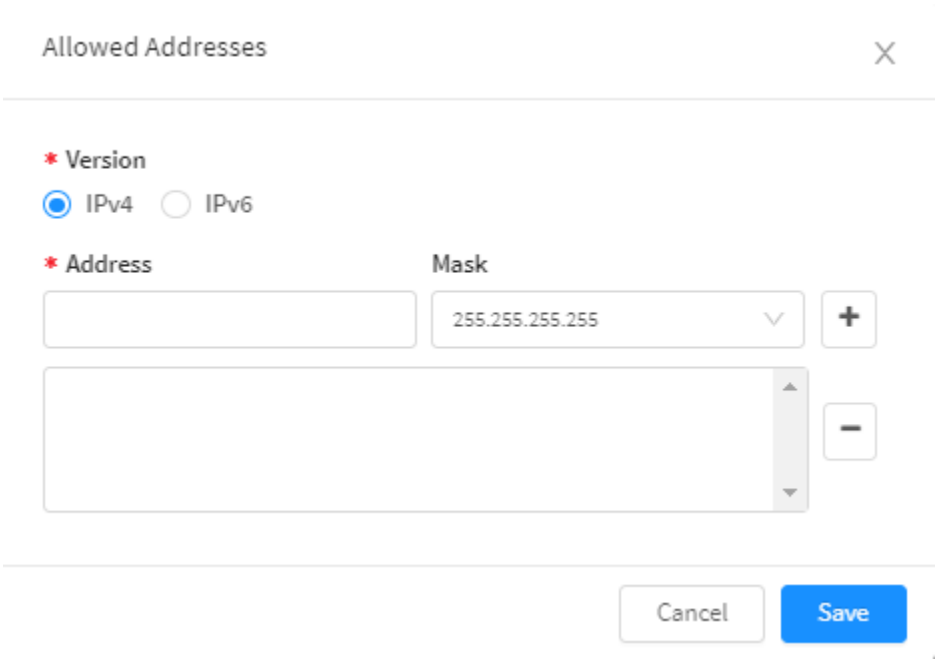
Allowed Addresses - Actions Menu - Create

Through the option “Create” it is possible to create a list of allowed IPs. To access, click on the actions menu **[**  **]**.

1. Click on the “Create Profile” option;

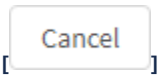
Allowed Addresses - Actions Menu - *Create*

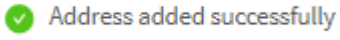
2. The “create *Allowed Addresses*” screen will appear. As shown in the image below:



Allowed Addresses - Import Allowed Addresses

- ***Version*:** Determines between IPv4 and IPv6, which will be used in the Whitelist;
- ***Address*:** In this field, enter the IP address that will be added to the Whitelist;
- ***Mask*:** In this field, type the netmask*;*
- ***List*:** Click the **[**  **]** button, if you want to remove an IP from the list click **[**  **]**.

If you want to cancel, click the **[**  **]** button. To complete the addition, click the **[**  **]** button.



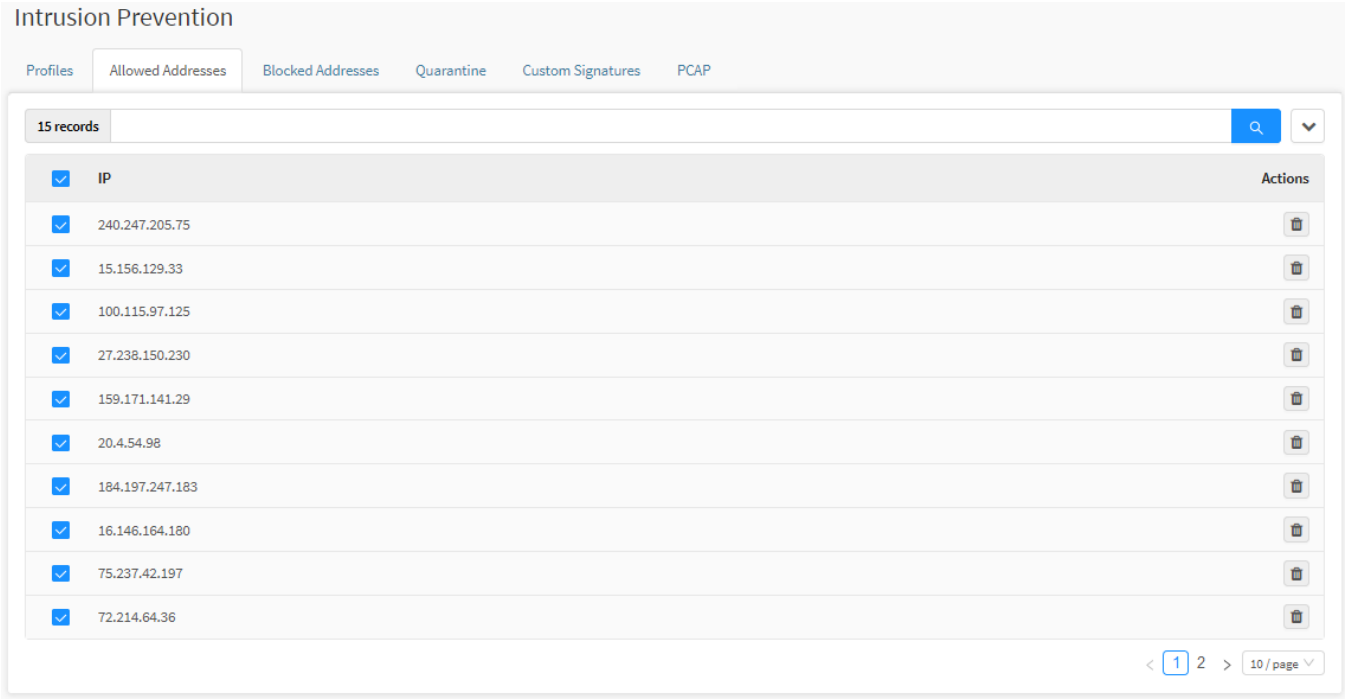
Address successfully added

Settings have been successfully made.

Allowed Addresses - Actions Menu - Delete

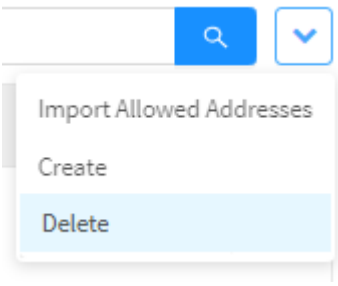
Through the “Delete” button it is possible to delete the selected IPs. To delete items, follow these steps:

1. Select which IP (s) you want to delete. To select, just click with the mouse on the checkbox located next to the IP. In the selected profiles the checkbox will change from gray to blue **[ ]**:



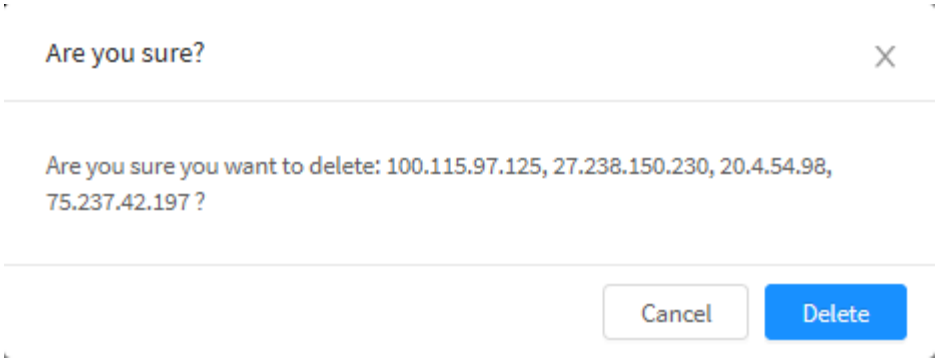
Allowed Addresses - IPs selection

2. Enter the actions menu **[ ]** and click on the option “Delete Profile”.



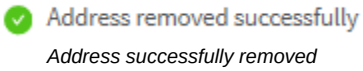
Allowed Addresses – Delete Profile

3. The notification message will appear asking if you really want to delete the selected Profiles:



Allowed Addresses – Deletion confirmation message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.



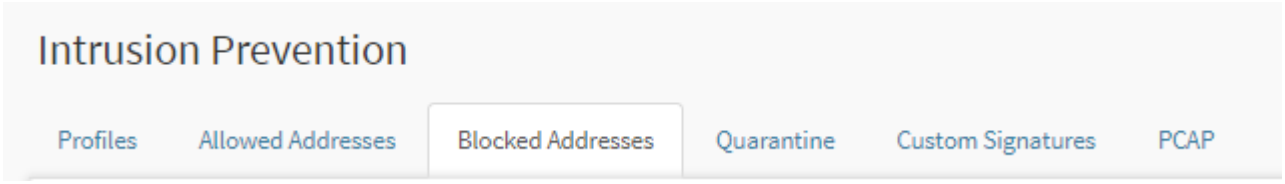
Address successfully removed

After performing these procedures, the IPs will have been successfully deleted.

Intrusion Prevention - Blocked Addresses tab

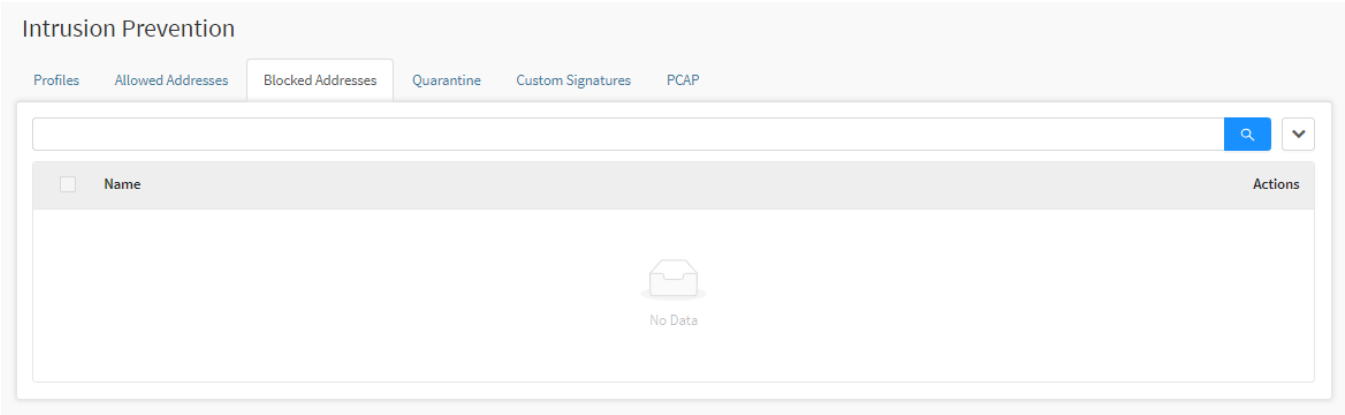
In this tab it is possible to manage the list of suspicious IPs that Intrusion Prevention will use.

To make the settings, click on "Blocked Addresses".



Blocked Addresses tab

The Intrusion Prevention “Blocked Addresses” screen will appear, as shown by the image below:



Intrusion Prevention - Blocked Addresses

This session will cover how to register, edit and remove IPS from the Intrusion Prevention's Blocked Addresses list.

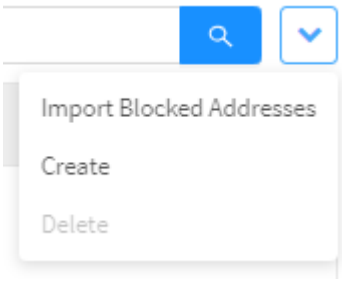
Next, we'll look at the functions located at the top of this panel.

Intrusion Prevention - Blocked Addresses tab - Actions Menu

At the top right of the screen we have the actions menu:

Intrusion Prevention – Actions Menu Button

By clicking on this button the menu below is displayed:



Intrusion Prevention - Blocked Addresses - Actions menu

The menu consists of the following options:

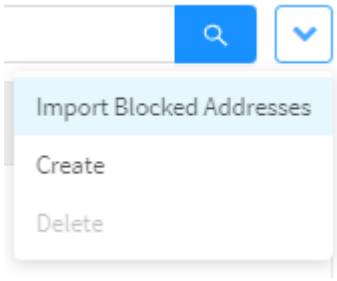
- *Import Blocked Addresses*;
- *Create*;
- *Delete*.

Next, each action menu option will be detailed.

Blocked Addresses - Actions Menu - Import Blocked Addresses

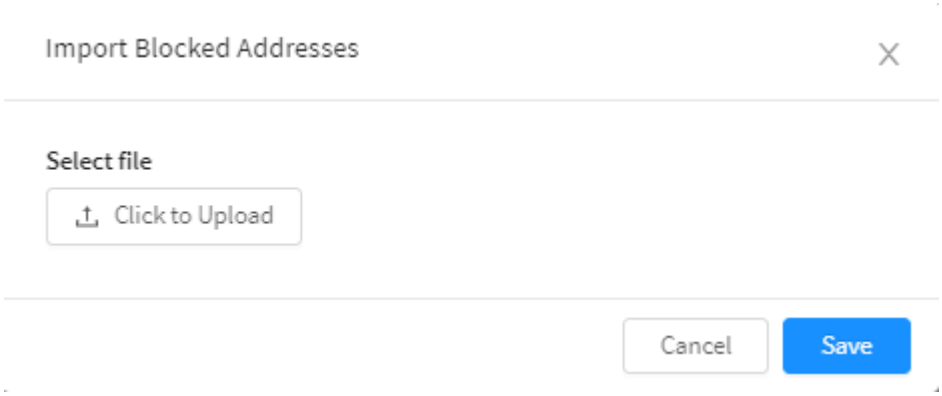
Through the “Blocked Addresses” option it is possible to import a suspicious IPs list. To access, click on the actions menu **[**  **]**.

1. Click on the “Create Profile” option;



Blocked Addresses - Action Menu - *Import Blocked Addresses*

2. The “Import Blocked Addresses” screen will appear. As shown in the image below:

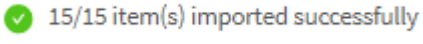


Blacklist - Import Blocked Addresses list

3. Select the desired file by clicking the **[**  **]** button and browsing;

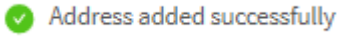
This options is compatible with ".txt" files only.

4. Upon successfully uploading the file, a confirmation message will be displayed:



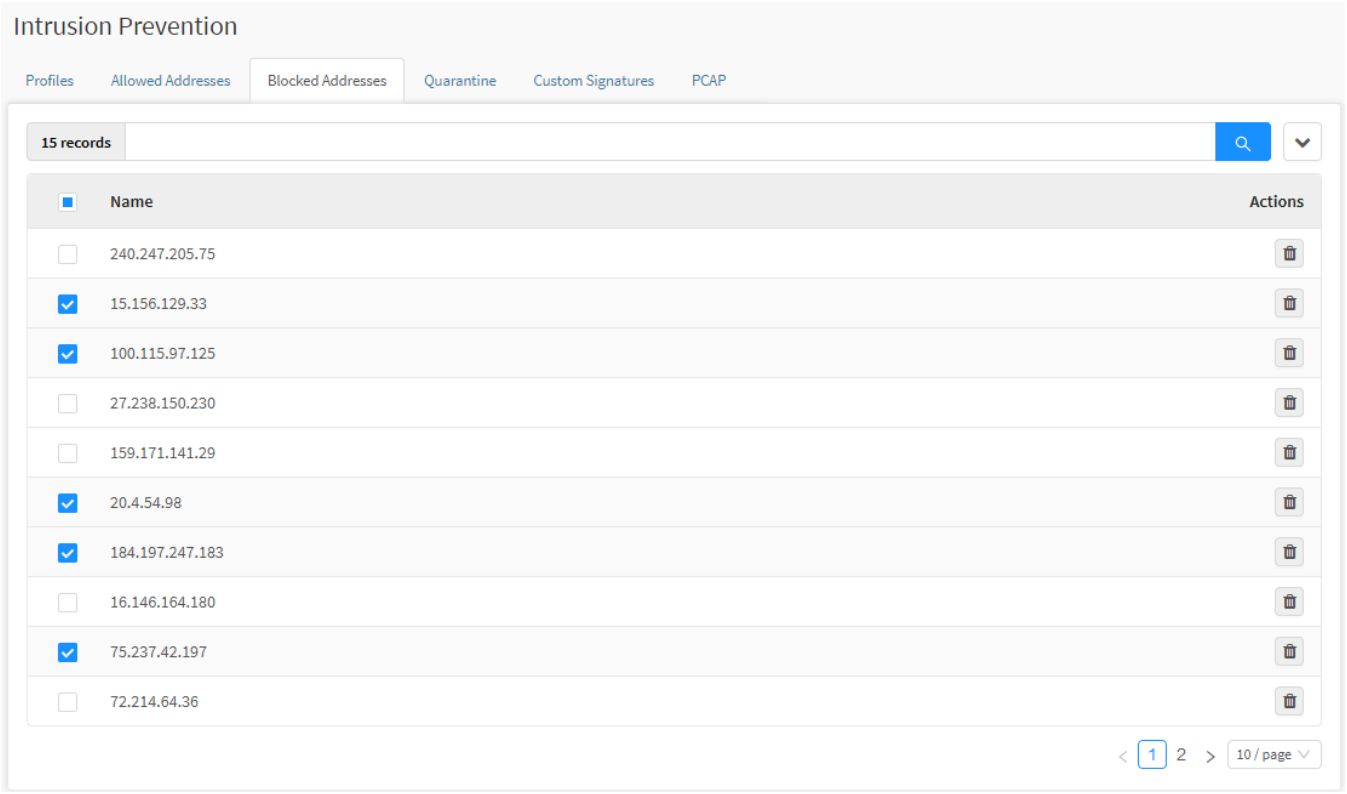
Item(s) successfully imported

5. When you finish adding the items, the following confirmation message will be displayed:



Address successfully added

6. Finally, the screen will display all added IPs:



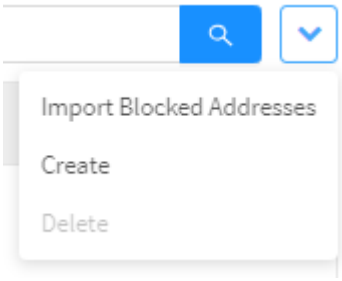
Blocked Addresses - Added IPs

After performing these procedures, the import will have been successful.

Blocked Addresses - Actions Menu - Create

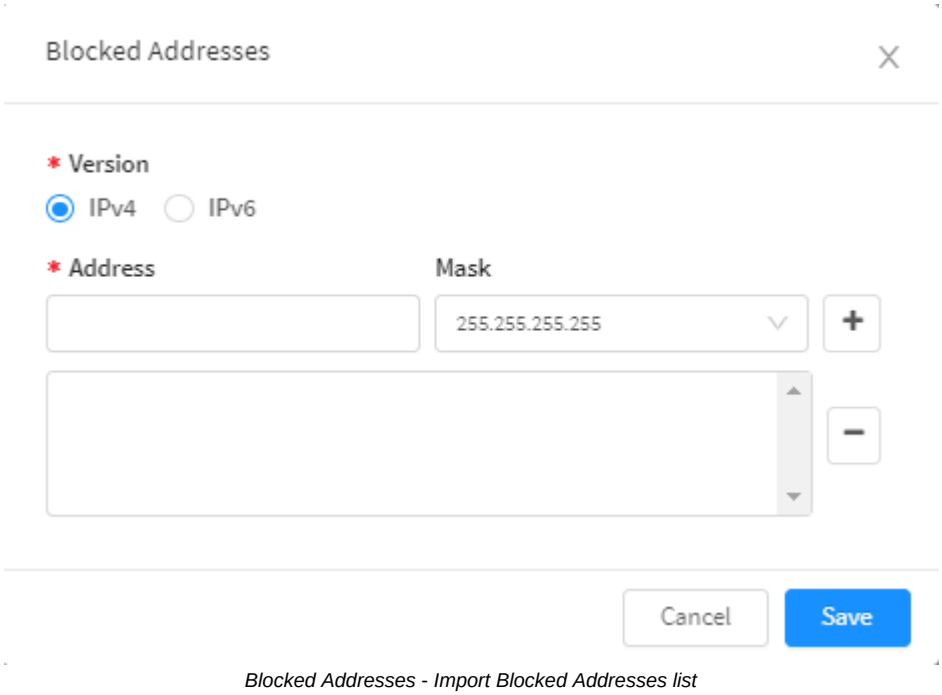
Through the option “Create” it is possible to create a list of suspicious IPs. To access, click on the actions menu **[**  **]**.

1. Click on the “Create” option;



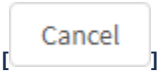
Blocked Addresses - Actions Menu - *Create*

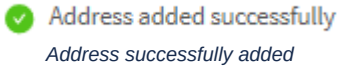
2. The “Blocked Addresses” screen will be displayed. As shown in the image below:



Blocked Addresses - Import Blocked Addresses list

- ***Version*****:** Select between IPv4 and IPv6, to be used in the Blocked Addresses;
- ***Address*****:** In this field, enter the IP address that will be added to the Blocked Addresses;
- ***Mask*****:** In this field, type in the netmask;
- ***List*****:** Click the **[**  **]** button, if you want to remove an IP from the list click **[**  **]**.

If you want to cancel, click the **[**  **]** button. To complete the addition, click the **[**  **]** button.

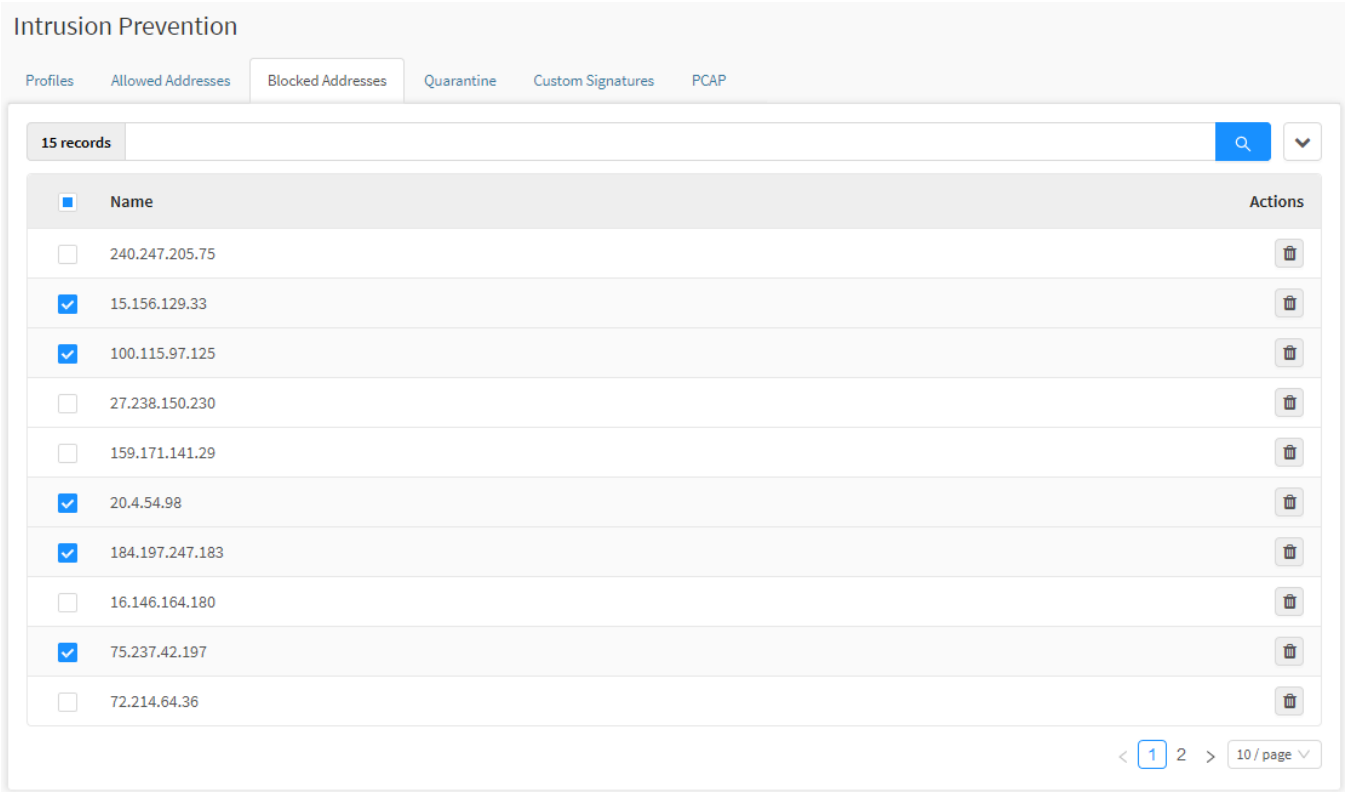


The settings have been successfully made.

Blocked Addresses- Actions Menu - Delete

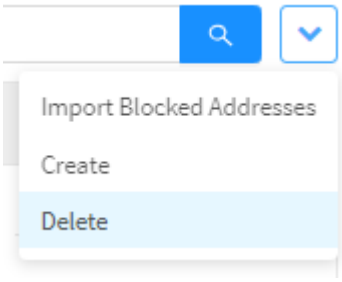
Through the “Delete” button it is possible to remove selected IPs from the blocked list. To delete them, starting from the actions menu, follow these steps:

1. Select which IP(s) you want to delete. To select, just click with the mouse on the checkbox by the left of the IP to be deleted. Those checkboxes will change from gray to blue **[ ]**:



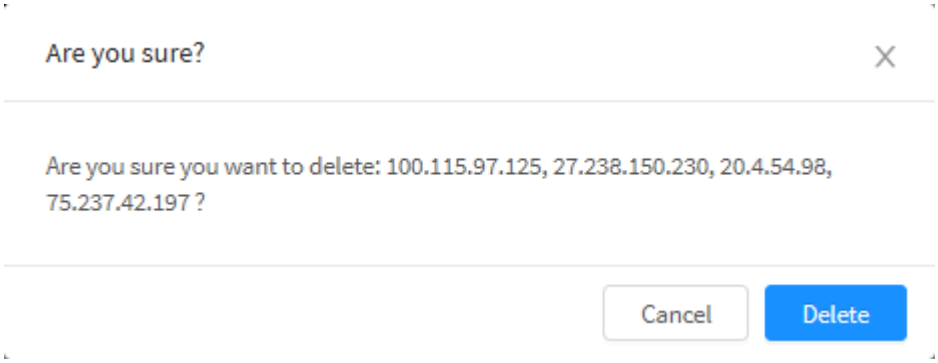
Blocked Addresses - IP deletion

2. Enter the actions menu **[ ]** and click on the “Delete Profile” option.



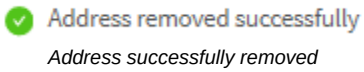
Blocked Addresses – Delete Profile

3. A notification message will appear asking if you really want to delete the selected Profiles:



Blocked Addresses – Profile deletion confirmation message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.



Address successfully removed

After performing these procedures, the IPs will have been successfully deleted.

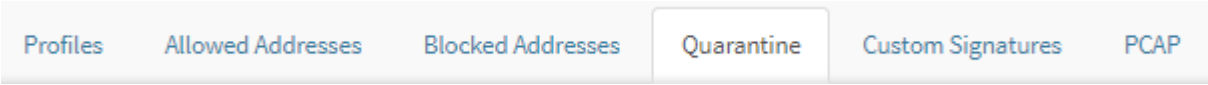
Intrusion Prevention - Quarantine tab

Quarantine allows you to manage all blocked IP addresses (both source and destination) and that in the configuration of the signatures the insertion in quarantine was specified in some Intrusion Prevention profile

The IP addresses contained in the Quarantine for the configured period, will be blocked before being analysed by any subscription of any Intrusion Prevention profile.

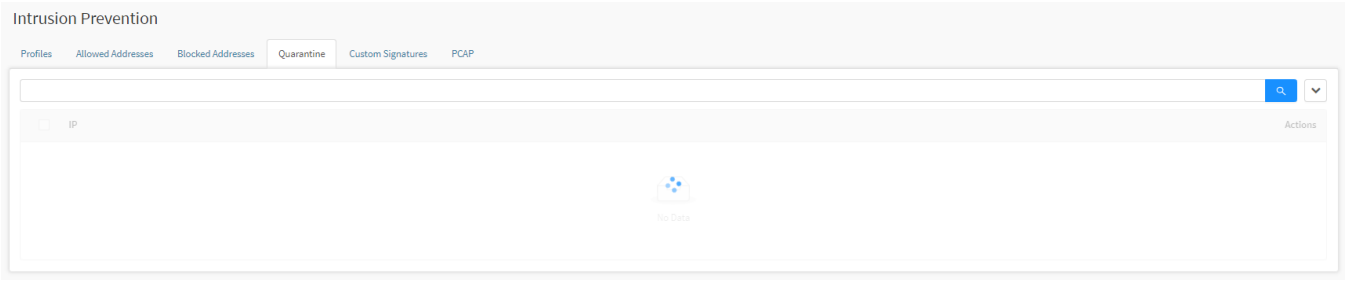
Through the options in the Actions Menu, it is possible to add these IPs to the Allowed Addresses List, Blocked Addresses List, remove them or determine the time limit for them to be deleted.

To make the settings, click on "Quarantine".



Quarantine tab

The Intrusion Prevention “Quarantine” screen will appear, as shown by the image below:



Intrusion Prevention – Quarantine.

Once the address in the quarantine the entire packet of that origin or destination will be blocked before even arriving in a specific subscription, the quarantine time of a given IP is configurable.

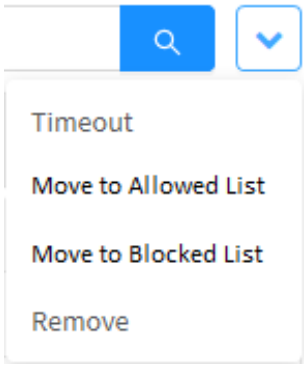
Next we will analyze the options of the actions menu and the function of the columns of the Quarantine tab.

Quarantine - Actions Menu

At the top right of the screen we have the actions menu:

Intrusion Prevention - Actions Menu Button

By clicking on this button the menu below is displayed:



Intrusion Prevention - Quarantine - Action Menu

The menu consists of the following options:

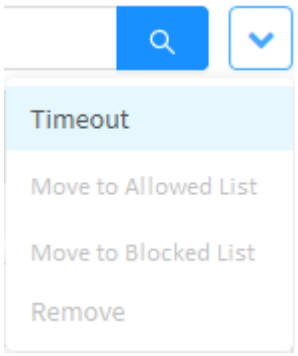
- *Timeout*;
- *Move to Allowed Addresses List*;
- *Move to Blocked Addresses List;*
- *Remove*.

Next, each action menu option will be detailed.

Quarantine - Actions Menu - Timeout

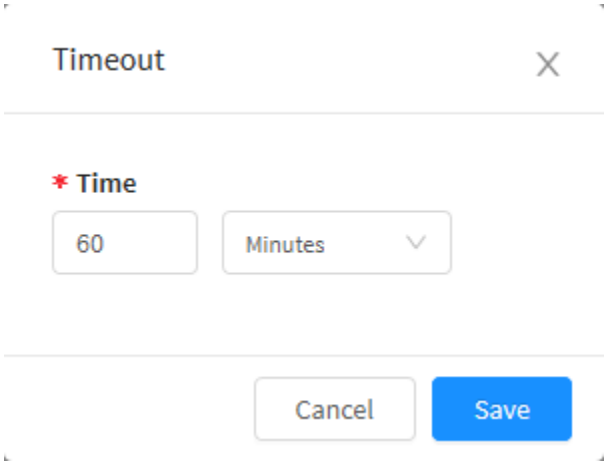
The quarantine time for a given IP is configurable through this option. To access, click on the actions menu **[**  **]**.

1. Click on the “Timeout” option;



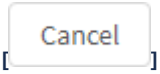
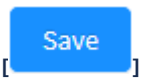
Intrusion Prevention - *Quarantine* - Actions menu - *Timeout*

2. The screen below will appear:



Quarantine - *Timeout*

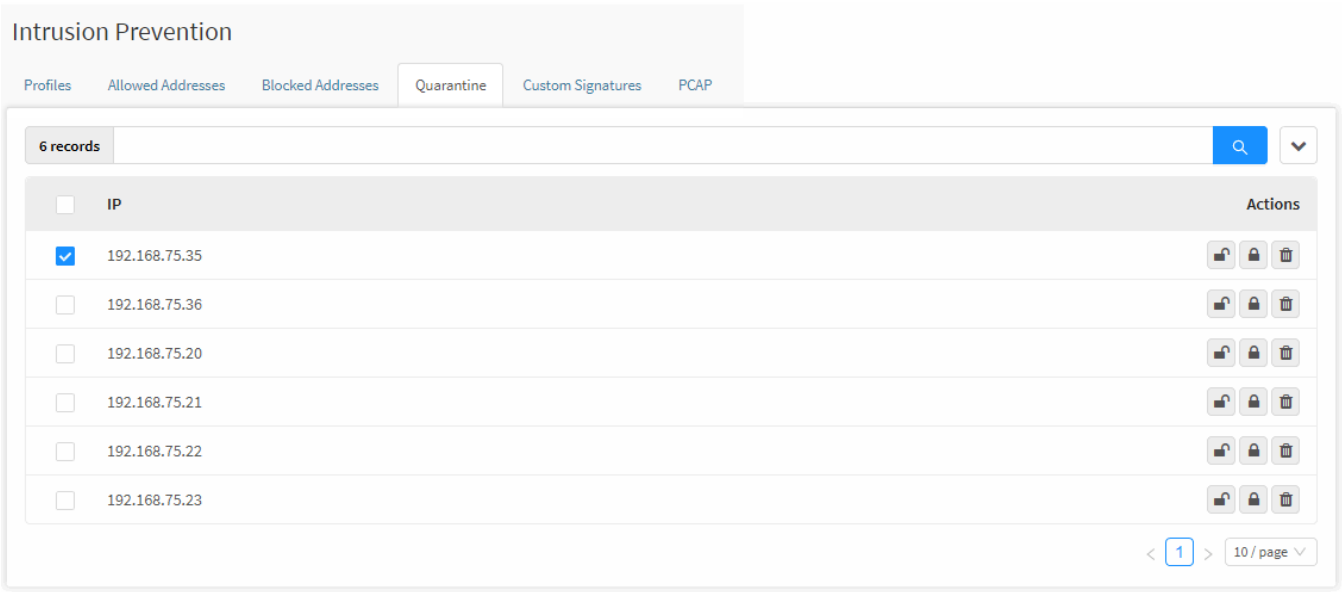
In this panel, the timeout time can be configured to remove the address in the quarantine, by default the system will be configured with the time of 60 minutes. In the first field, it is possible to determine the time, in the selection box it is possible to define whether the time will be in minutes or hours

Finally, if you want to cancel, click the **[**  **]** button. To finish editing applications, click the **[**  **]** button.

Quarantine - Actions Menu - Move to Allowed Addresses List

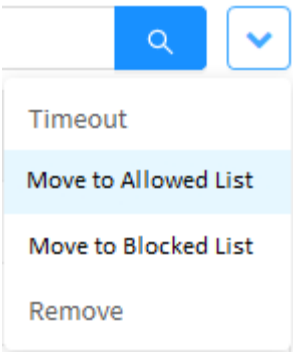
Through this option it is possible to move an IP from the quarantine to the Allowed Addresses List. To do this, follow the steps below:

1. Select which IP (s) you want to move. To select, just click with the mouse on the checkbox located next to the IP. In the selected items the checkbox will change from gray to blue **[ ]**:



Quarantine – Selection of IPs to move to the Allowed Addresses List

2. Click on the “Move to Allowed List” option;



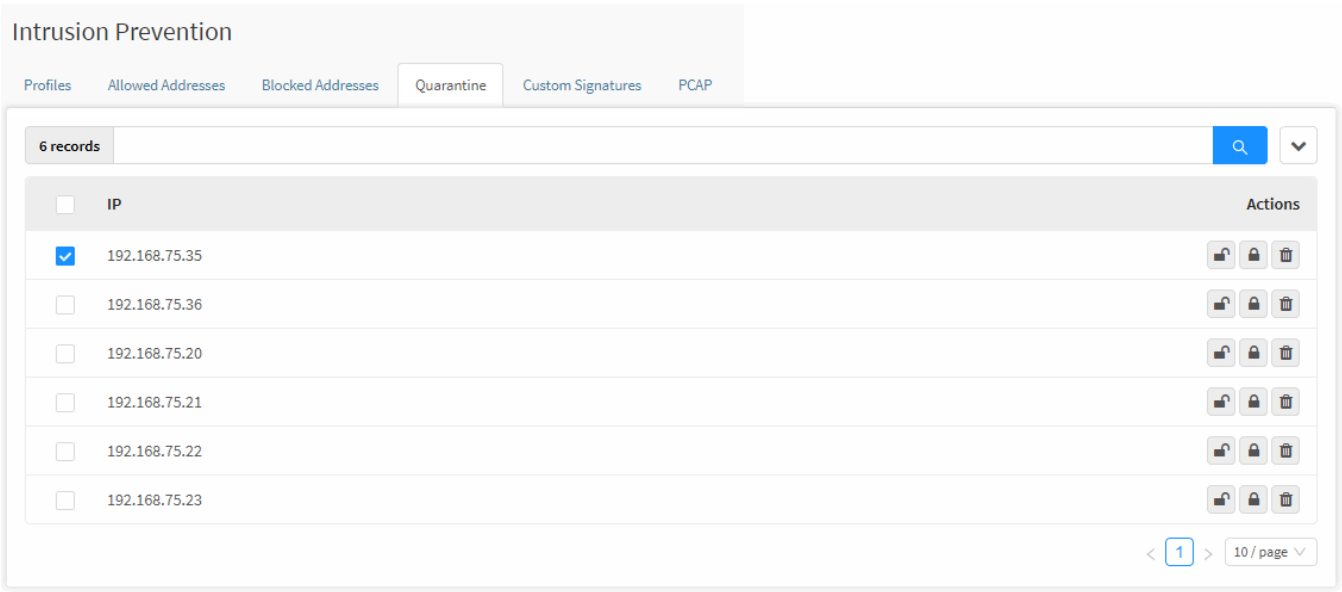
Intrusion Prevention - *Quarantine* - Actions Menu - Move to Allowed List

3. After confirming the notification message asking if you really want to move the selected items, the procedure will have been successfully performed.

Quarantine - Actions Menu - Move to Blocked Addresses List

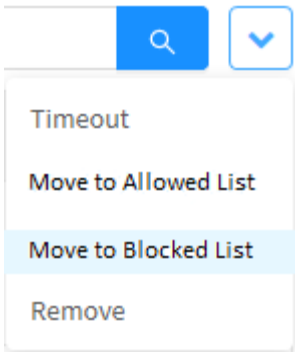
Through this option it is possible to move an IP from the quarantine to the Blocked Addresses List. To do this, follow these steps:

1. Select which IP (s) you want to move. To select, just click with the mouse on the checkbox located next to the IP. In the selected items the checkbox will change from gray to blue **[ ]**;



Quarantine – Selection of IPs to move to the Blocked Addresses List

2. Click on the option “Move to Blocked List”;



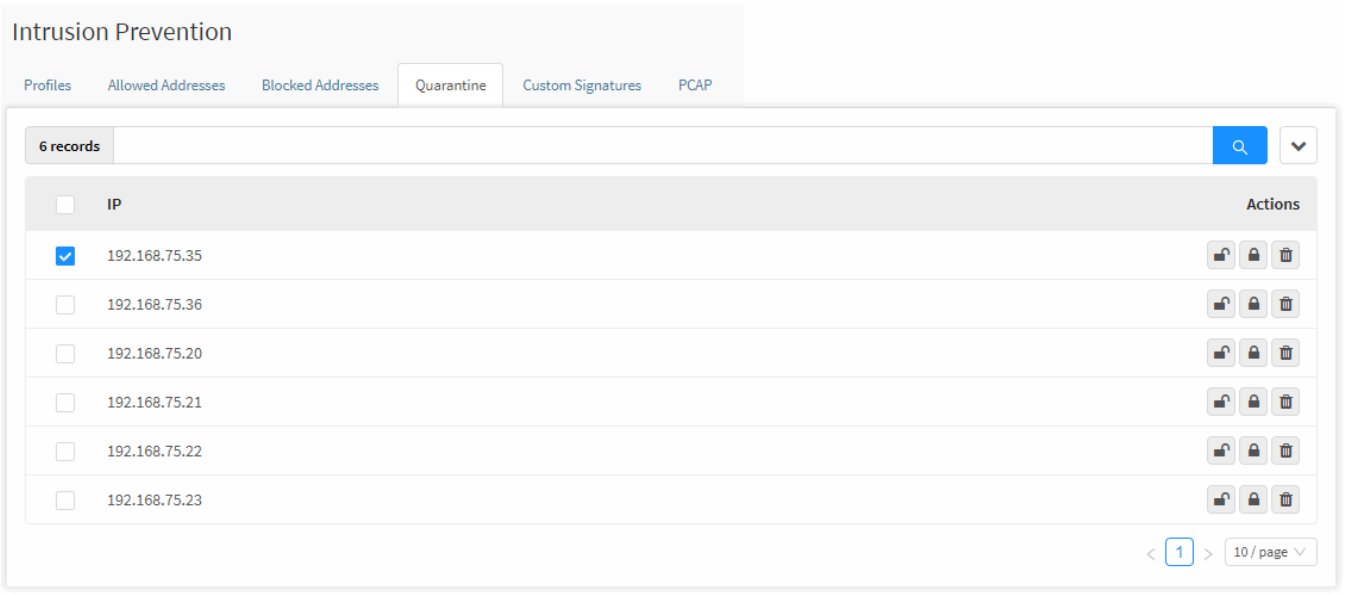
Intrusion Prevention - *Quarantine* - Actions menu - *Move to Blocked List*

3. After confirming the notification message asking if you really want to move the selected items, the procedure will have been successfully performed.

Quarantine - Actions Menu - Remove

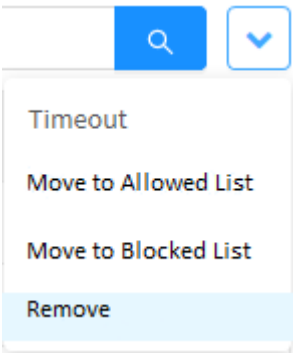
Through the “Remove” button it is possible to remove the selected items. To remove from the Actions menu, follow these steps:

1.Select which item(s) you want to remove. To select, just click with the mouse on the checkbox located next to the IP. In the selected items the checkbox will change from gray to blue **[ ]**. Ex.: *Test*:



Quarantine - Selection for deletion

2. Enter the actions menu **[ ]** and click on the option “Remove”.

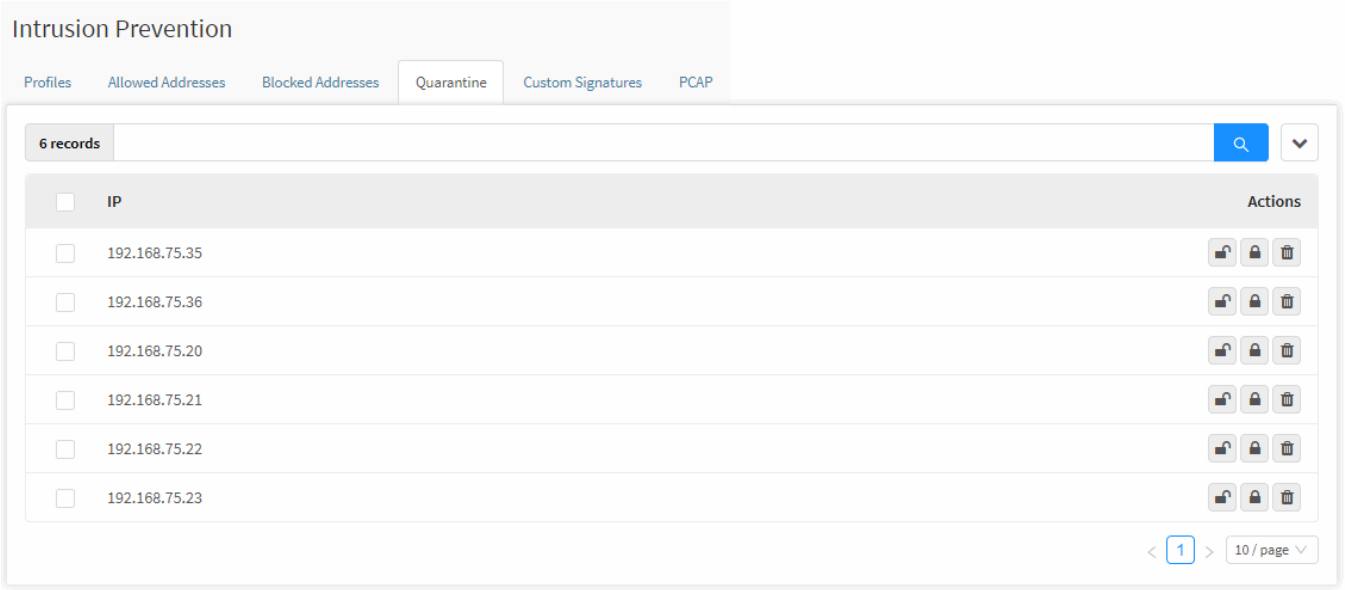


Quarantine - Actions Menu - *Remove*

3. After confirming the notification message asking if you really want to delete the selected items, the removal will have been successfully performed.

Quarantine - Columns

Below we will explain each column of the Quarantine tab:



Intrusion Prevention – Quarantine

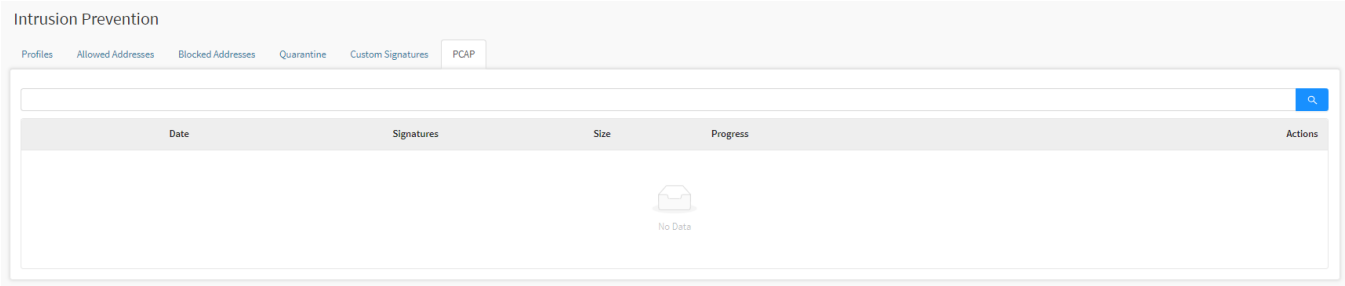
We will explain each column below:

- **Checkbox[ ]:** Select the item;
- ***Actions*:** The “Actions” column consists of the buttons:
  - **[ ]** The system will add the IP address to the Allowed List. It is equivalent to the *Move to Allowed Addresses List* option in the action menu;
  - **[ ]** The system will add the IP address to the Blocked List. It is equivalent to the *Move to Blocked Addresses List option in the action menu*;
  - **[ ]** The system will remove the address from the quarantine, it is equivalent to the *Remove* option in the actions menu.

Intrusion Prevention - PCAP tab

PCAP or Packet Capture is an API (Application Programming Interface) that captures network traffic data packets. Through the reading of TCP/IP and UDP data packets, it allows the saving of network traffic data for monitoring and analysis purposes. It also allows the identification of malicious traffic coming from an external source. The collected signatures are consolidated in a file as logs, that contain the characteristics and behavior of said signatures. In case the (PCAP - Packet Logger) option has not been marked when creating/editing an IPS profile, no file will be displayed in this section.

This tab displays the data of the signatures (profiles) that are with the PCAP functionality switched on.



Intrusion Prevention - PCAP

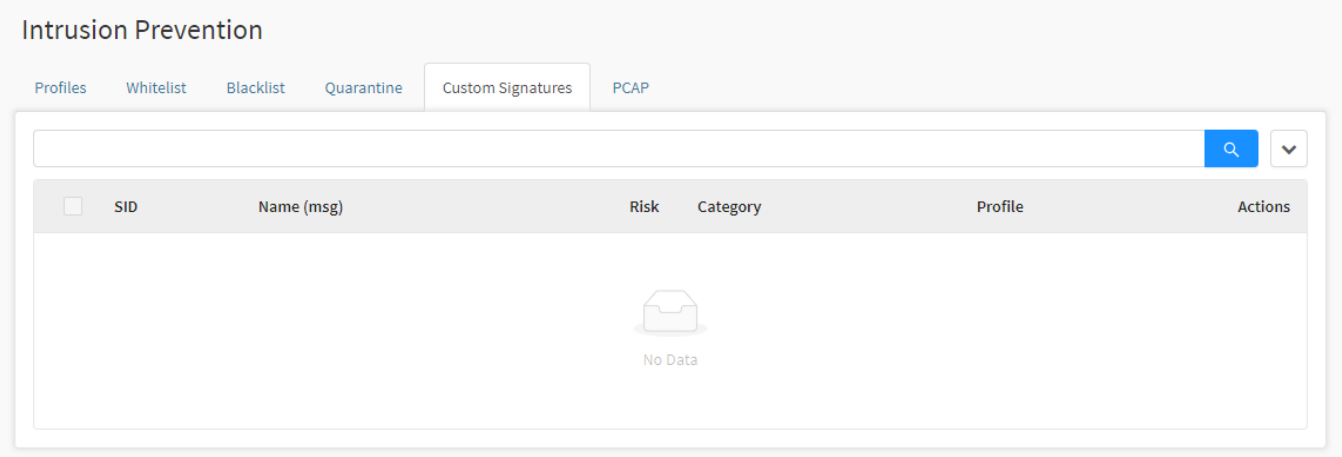
- ***Date:*** Date in which the file containing the logs was created.
- ***Signatures:*** Name of the collected signatures.
- ***Size:*** Total file size.
- ***Progress:*** State in which the file is, in terms of completion (in progress, done).
- ***Actions:*** Actions taken regarding the handling of the files by the system.

Next, we will analyze the features of Custom signatures.

Intrusion Prevention - Custom Signatures tab

In Custom signatures it is possible to include signatures that eventually will become relevant.

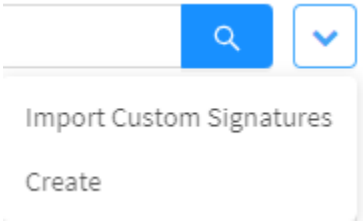
In this section, we will see how to set up a new signature:



Intrusion Prevention - Custom Signatures

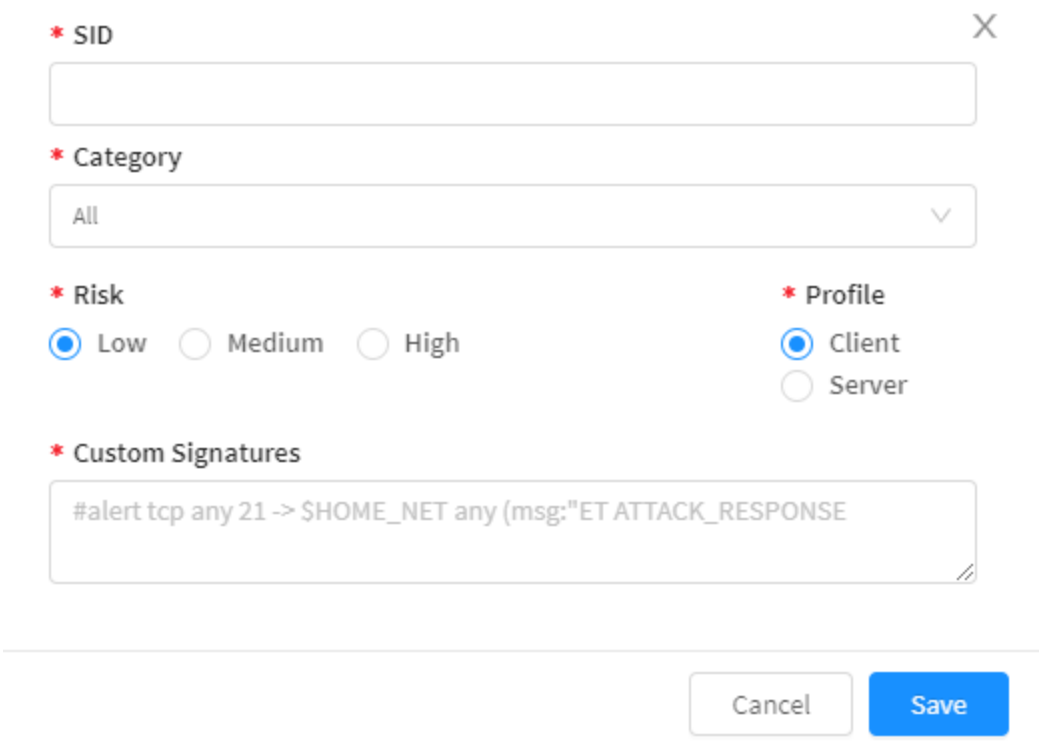
Create Signature

In options [] is the "*Create*" option:



Custom Signatures - Create

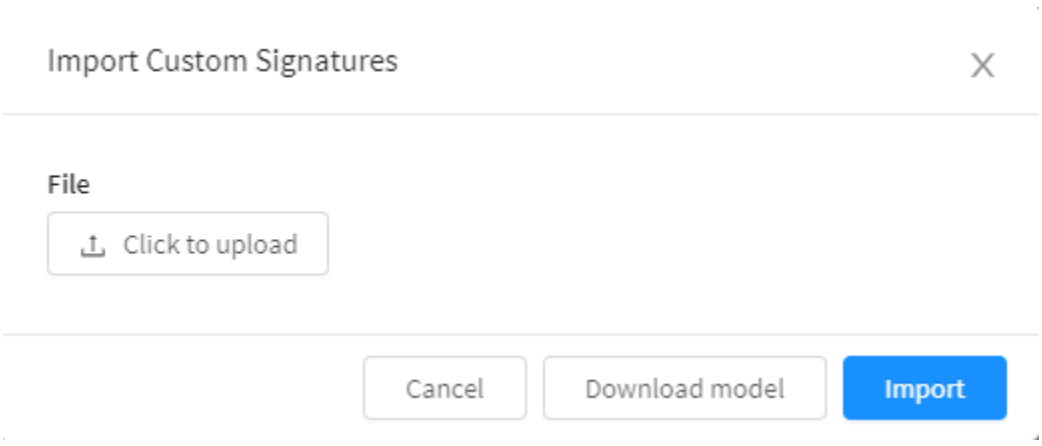
After, the following screen will be available:



Create menu

- ***SID:*** It's the identification code of the signature;
- ***Category:*** Available categories for this SID;
- ***Risk:*** Signature's threat risk level;
- ***Profile:*** Allows the selection of the signature's profile, if Client or Server;
- ***Custom Signatures:*** Allows the naming of the signature.

Import Custom Signatures



Import menu

- ***File***: Click to upload a file containing the signature that will be imported;
- ***Download model:*** In this option a model of the format to be used in the setting of the signature is available;
- ***Import:*** Button that imports the file containing the signature.

Next, we will analyse the functions located in the top of this panel.

UTM - Services - Threat Protection

Threat Protection is a feature that offers protection against malware and viruses to ensure the reliability of content traffic from Proxy services. The feature provides protection from “Downloads/Uploads” of infected files, “PUA" (potentially unwanted applications) files, detection by “Heuristic analysis” and protection against “files with passwords”.

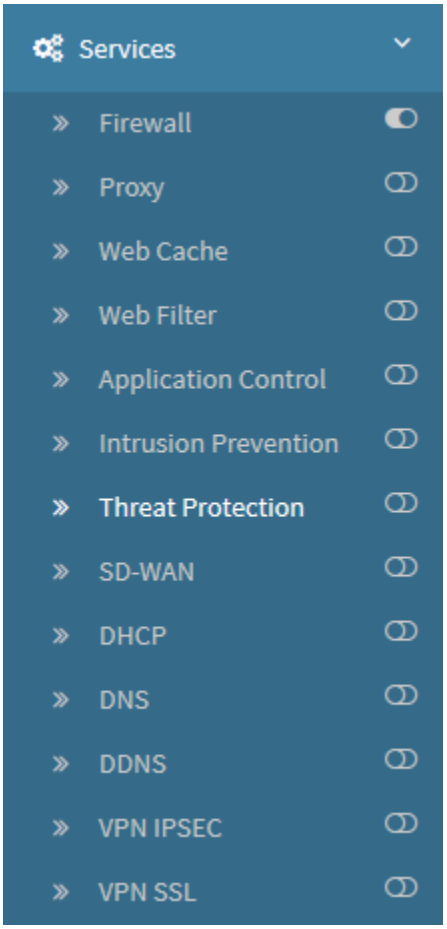
Unlike most Antimalwares and Antiviruses designed to detect and prevent malicious code on EPS “Endpoint Secure” devices, the Blockbit NGFW includes an internal Threat Protection feature that is automatically updated in search for new threats that can infect your network. The first layer of protection in an integrated system with web access via Proxy must be the analysis of malware and malicious codes to ensure the reliability of file traffic via Proxy.

The Blockbit NGFW provides Antimalware technology based on signatures generated by our LAB Security Research Team and integration with the latest Antivirus engines databasis.

Responsible for protecting the server and the network against malware attacks, it includes a technology capable of scanning files, directories, URLs and URIs for identification, item by item, to detect the invasion of some malware in Proxy traffic by security policy.

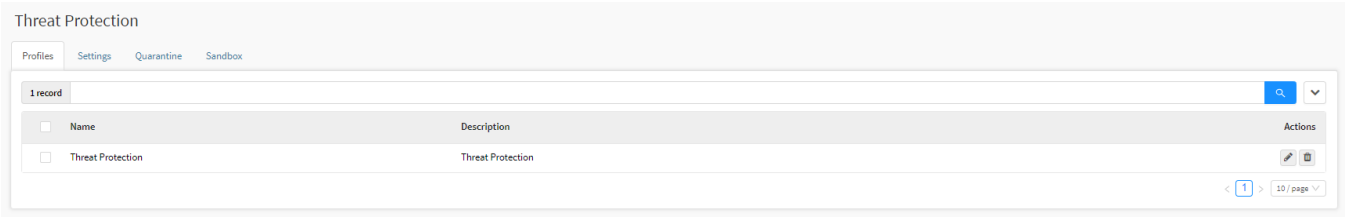
It also sums up the Sandbox technology, that is capable of emulating APT attacks (Advanced Persistent Threat) and Zero Day due to the capacity of emulating operational systems, having the Microsoft Windows as principal, besides daily used files, like the ones from the Microsoft Office. With virtual machines from different OSs (Operational Systems), the Blockbit ATP analyses the malware or malicious code behavior in its entirety, without the necessity of a signature basis.

To access and configure this feature, click on “Threat Protection”, as shown in the image below.



Services - Threat Protection

The screen below will appear:



Threat Protection

The screen has the following tabs:

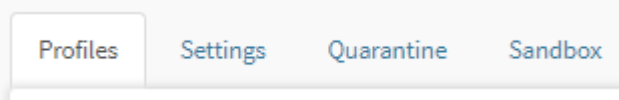
- *Profiles*;
- *Settings*;
- *Quarantine*;
- *Sandbox*.

Next we will analyze the components of the Threat Protection tab.

Threat Protection - Profiles tab

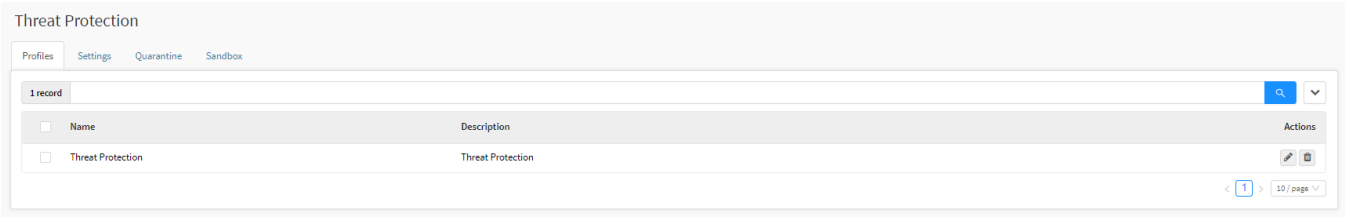
Through this tab it is possible to create protection profiles against threats and exploits of possible vulnerabilities in your network.

If the tab is not selected, click on "Profiles".



Profiles tab

The Threat Protection “Profiles” screen will appear, as shown by the image below:



Threat Protection - Profiles

This session will cover how to register, edit and remove Threat Protection profiles;

Next, we'll look at the functions located at the top of this panel.

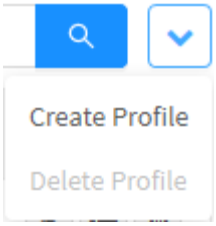
Threat Protection - Profiles - Actions Menu

With Threat Protection profiles, you can analyze files for malware inspection and threat blocking. This section will demonstrate how to create profiles that will later be installed in the policies.

At the top right of the screen we have the actions menu:

Threat Protection – Actions menu.

By clicking on this button the menu below is displayed:



Threat Protection – Actions menu

The menu consists of the following options:

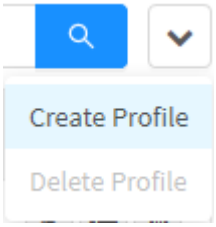
- *Create Profile*;
- *Delete Profile*.

Next, each action menu option will be detailed.

Threat Protection - Profiles - Actions Menu - Create Profile

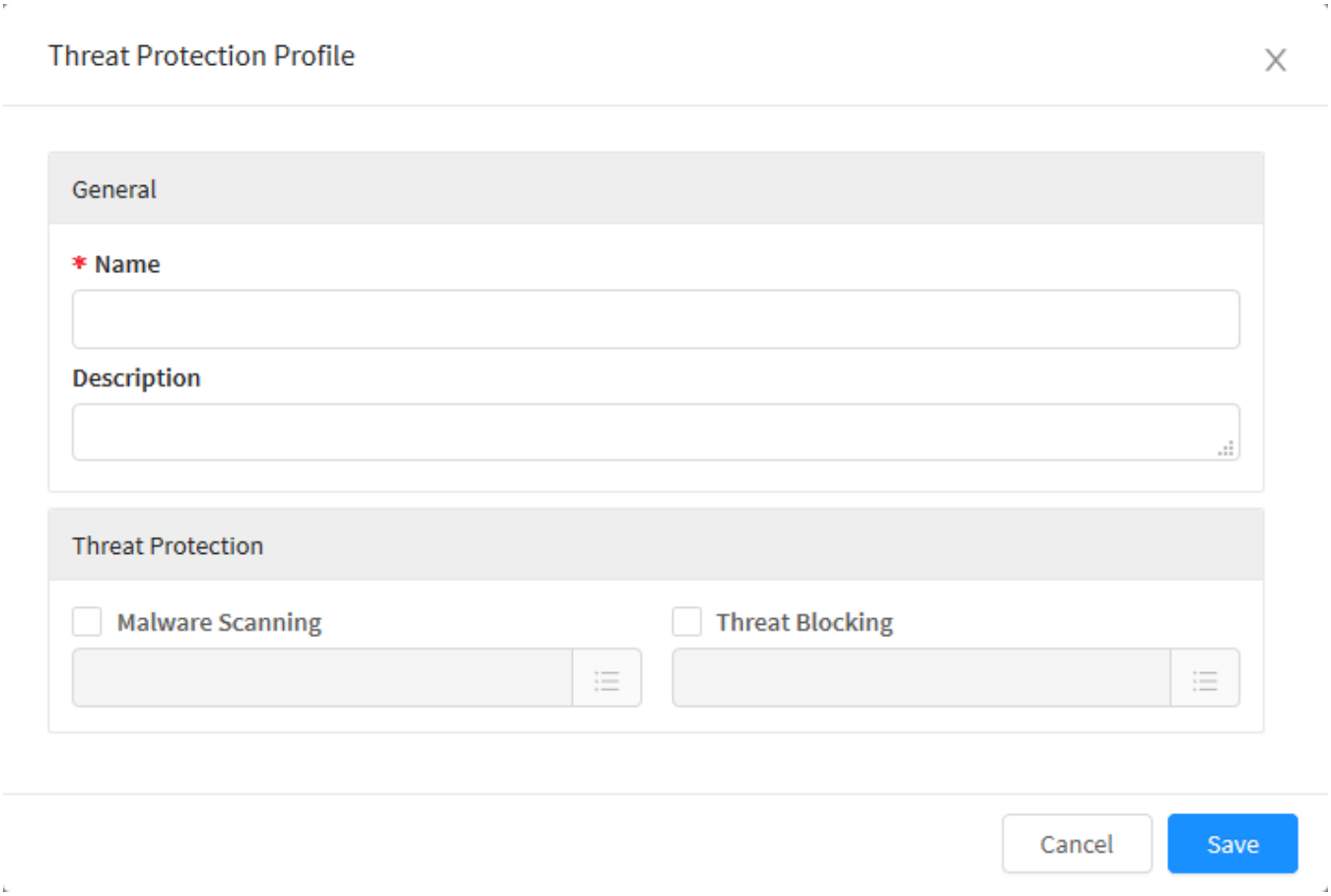
Through the option “Create Profile” it is possible to create a new Threat Protection profile. To access, click on the actions menu **[ ]**.

1. Select the “Create Profile” option;



Threat Protection - Create Profile

2. The “Threat Protection Profile” screen will appear. In this panel it is possible to make the general settings of the profile, trigger malware scan and block threats.



Threat Protection - Create Profile

General

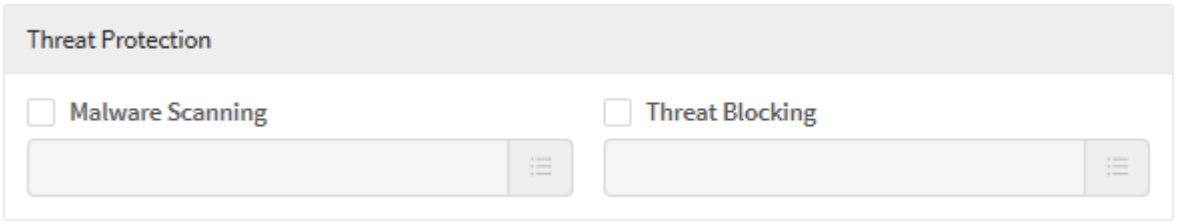
In "General" we have the following text boxes:

Threat Protection – General

- ***Name:*** *Define a name for the profile. Ex.: Web Navigation Threat Protection*;
- ***Description*****:** Define a description for the profile. Ex.: Web Navigation Threat Protection.

Threat Protection

"Threat Protection" determines the scanning of malware and the blocking of threats.

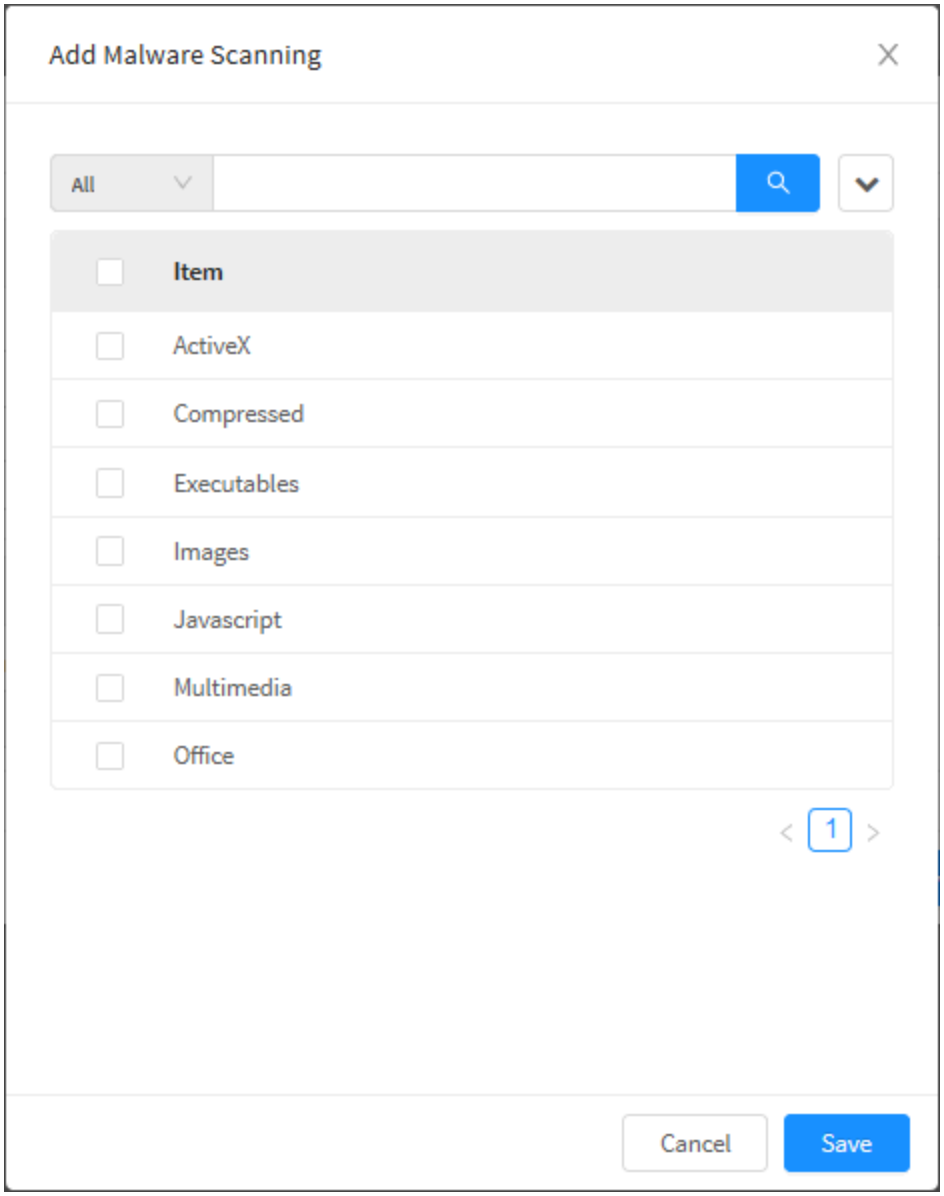


Threat Protection - Threat Blocking

Next, we will analyze in detail these two fields.

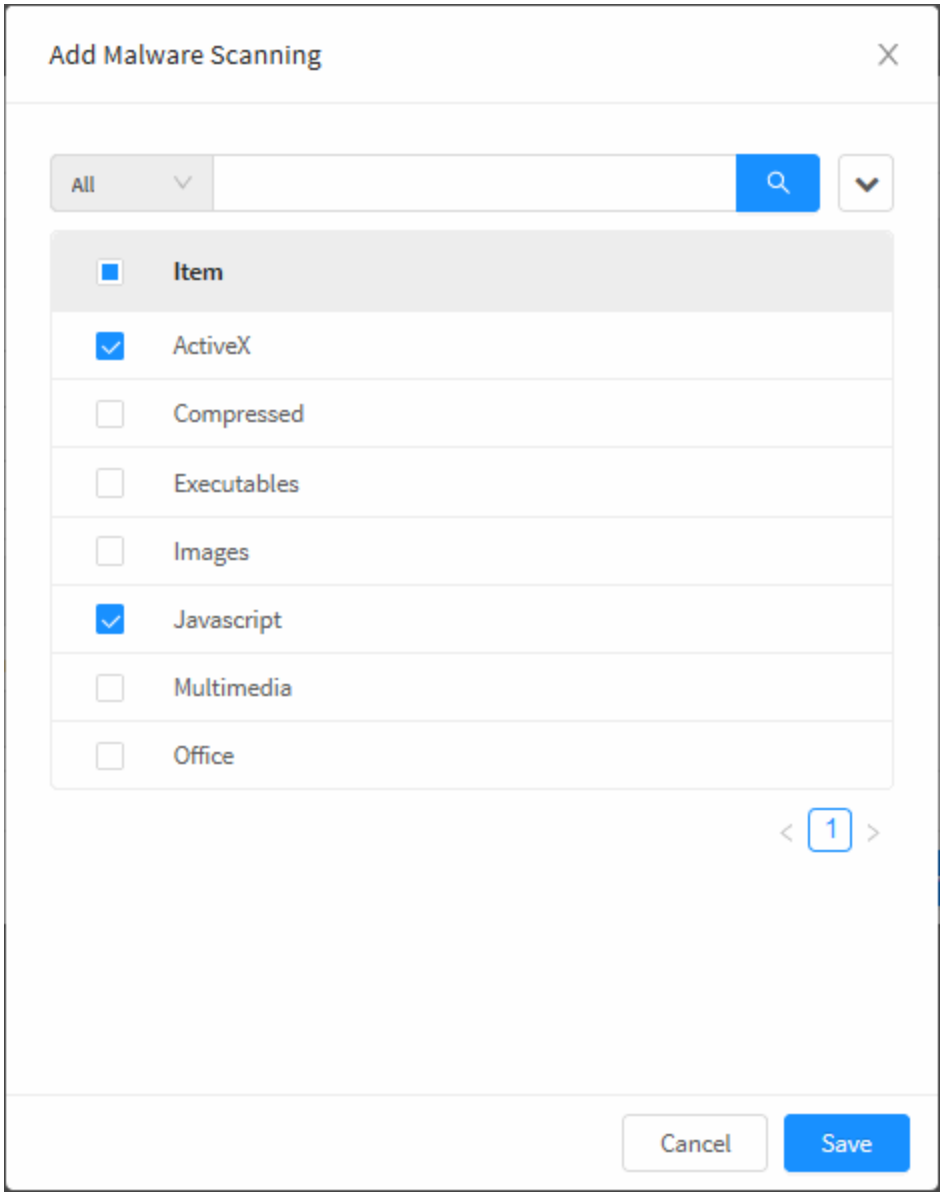
Malware Scanning

To add Malware Scanning, make sure that the checkbox **[**  **]** is enabled, then click on the list applications **[**  **]** button the following panel will be displayed:



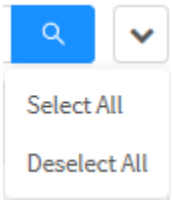
Threat Protection - Add Malware Scanning

Check the checkboxes to add malware scanning, as shown below:

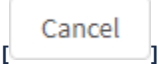


Threat Protection - Checkboxes marked

If it is necessary to make a configuration on all items, just select the desired option in the actions menu **[**  **]**:

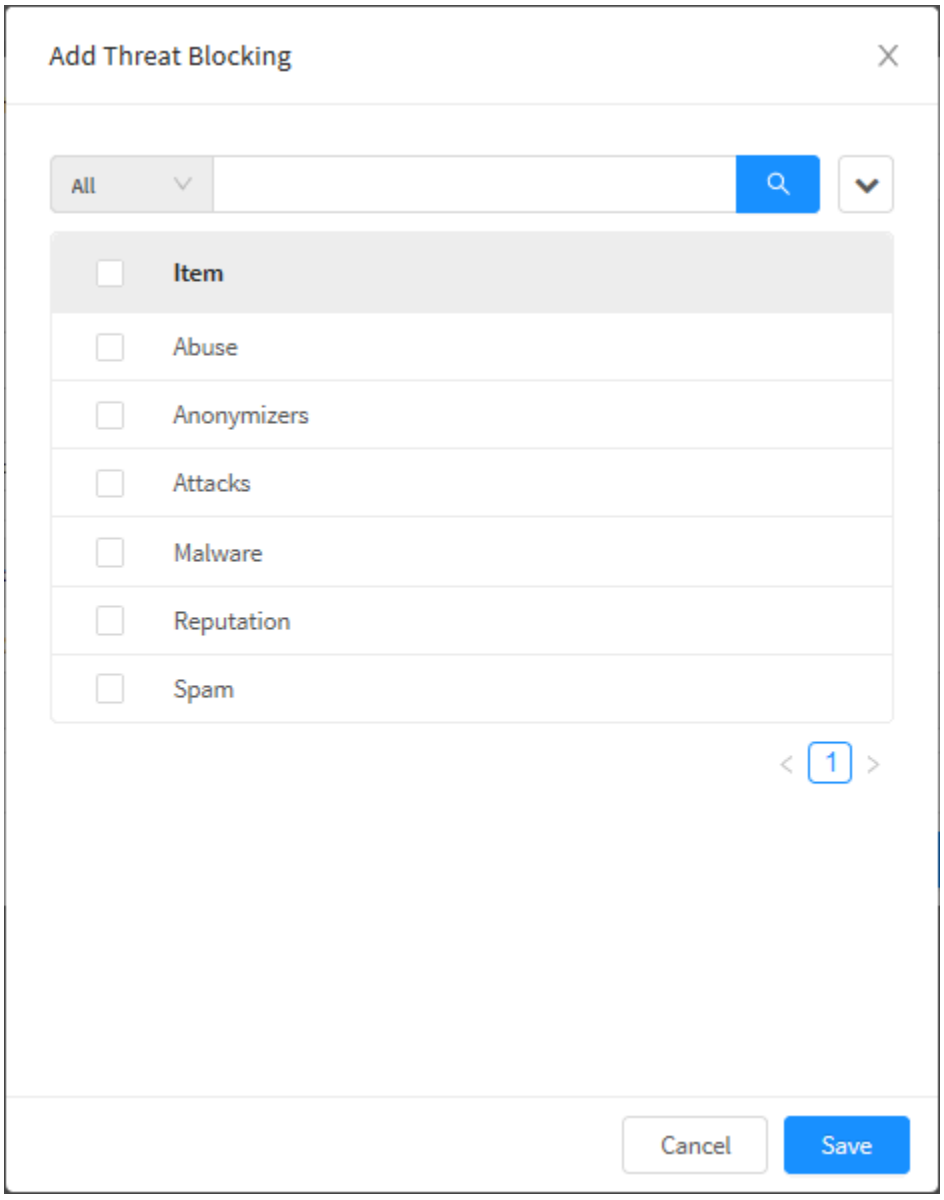


Threat Protection - Select all and *Deselect All*

Finally, if you want to cancel click on the **[**  **]** button. To finish adding Malware Scanning to applications, click the **[**  **]** button.

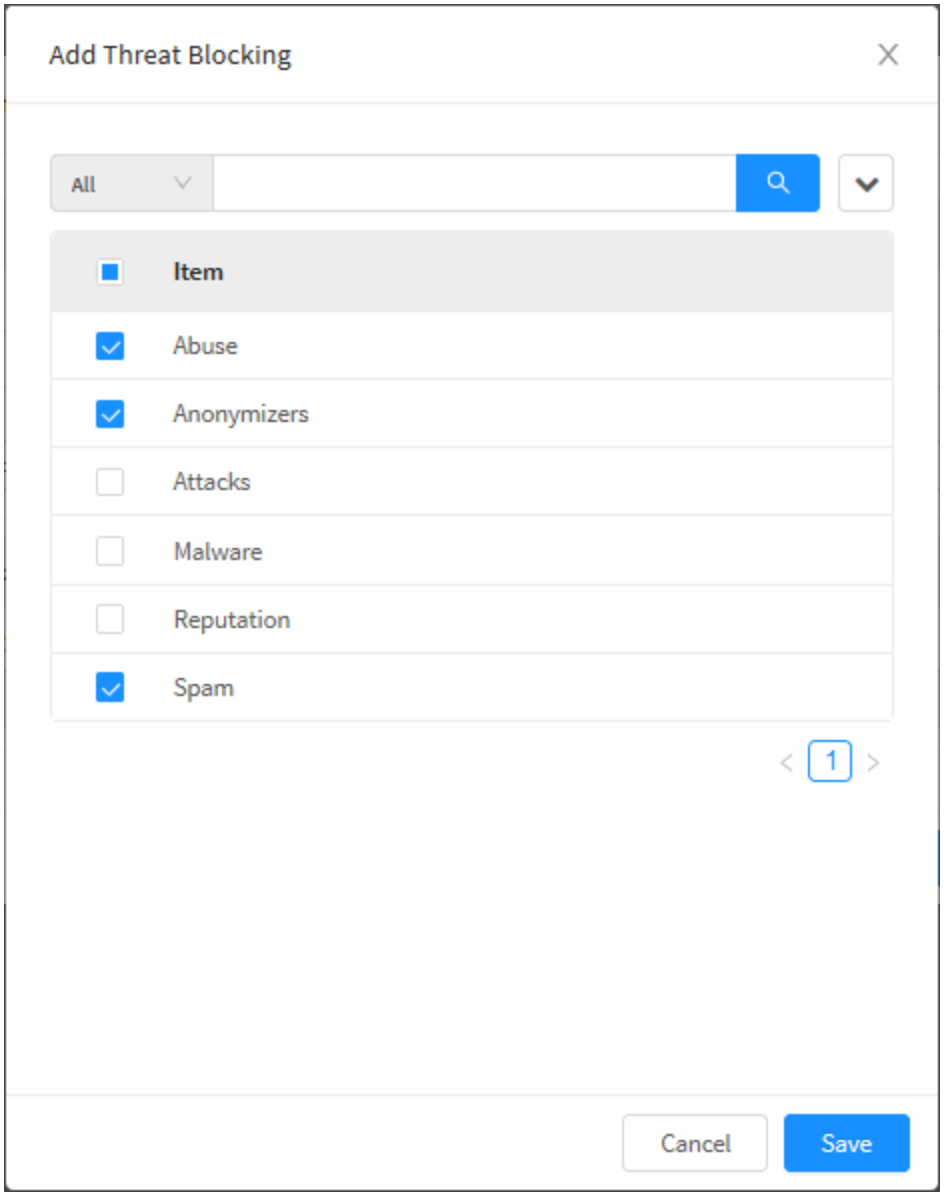
Threat Blocking

To add Threat Blocking, make sure that the checkbox **[ ]** is enabled, then click on the list applications **[ ]** button the following panel will be displayed:



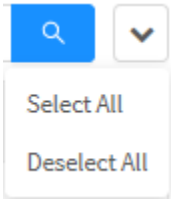
Threat Protection - Add Threat Blocking

Check the checkboxes to add the threat block, as shown below:

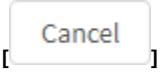


Threat Protection - Add Threat Blocking

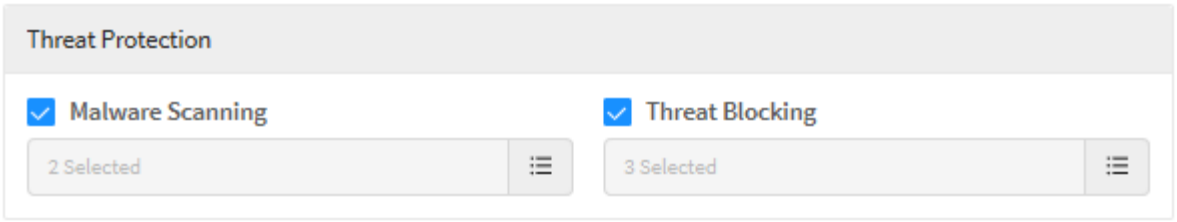
If it is necessary to make a configuration on all items, just select the desired option in the action menu **[**  **]**:



Threat Protection - Select all and *Deselect All*

Finally, if you want to cancel click on the **[**  **]** button. To finish adding Malware Scanning to applications, click the **[**  **]** button.

After having performed the previous processes, a summary of all selected threat protection items will be displayed in both fields, as shown below:



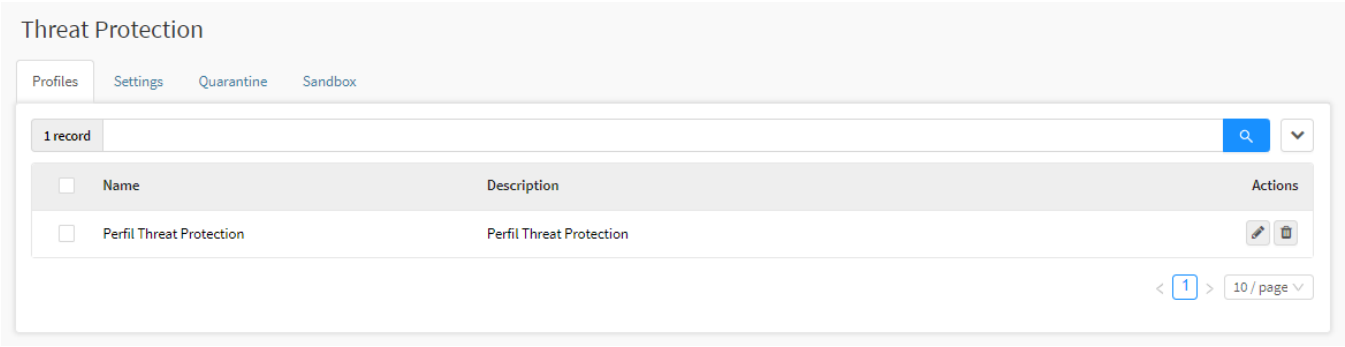
Threat Protection - Selected items

To finish, just click the **[** Save **]** button again.

Threat Protection - Profiles - Actions Menu - Delete Profile

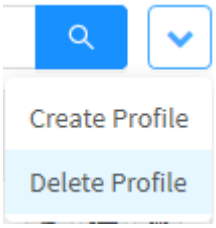
Through the button “Delete Profile” it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue **[ ]**. Ex.: *Test*;



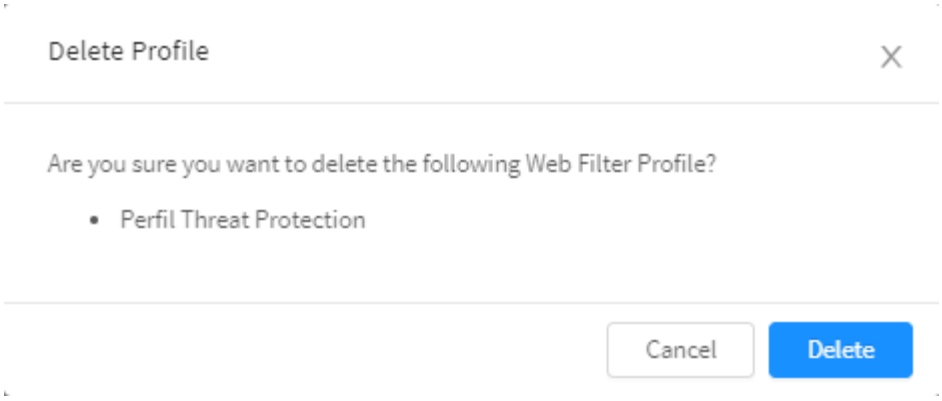
Threat Protection – Selection of Profiles to delete

2. Enter the actions menu **[ ]** and click on the option “Delete Profiles”.



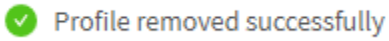
Threat Protection – Delete Profiles.

3. The notification message will appear asking if you really want to delete the selected Profiles:



Threat Protection – Profile deletion confirmation message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

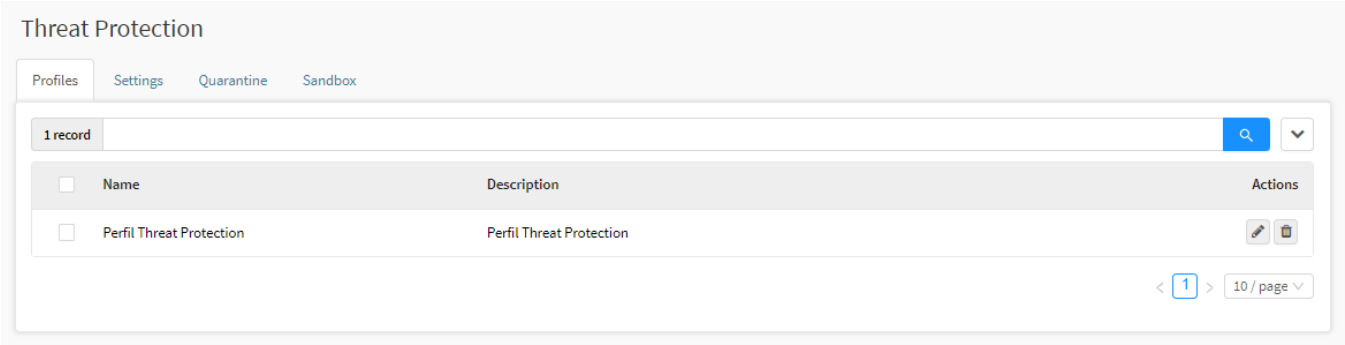


Profile successfully removed

After performing these procedures, the profiles will have been successfully deleted.

Threat Protection - Profiles - Columns

Below we will explain each column of the Threat Protection tab:



Profiles – *Threat Protection*

We will explain each column below:

- **Checkbox[ ]:** Select the profile;
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- ***Actions*:** The “Actions” column consists of several buttons:
  - ***Edit* [ ]:** Allows you to edit the profile settings added in the *Create Profile* option of the actions menu;
  - ***Delete* [ ]:** Deletes the profile, is the equivalent of the *Delete Profile* option in the actions menu.

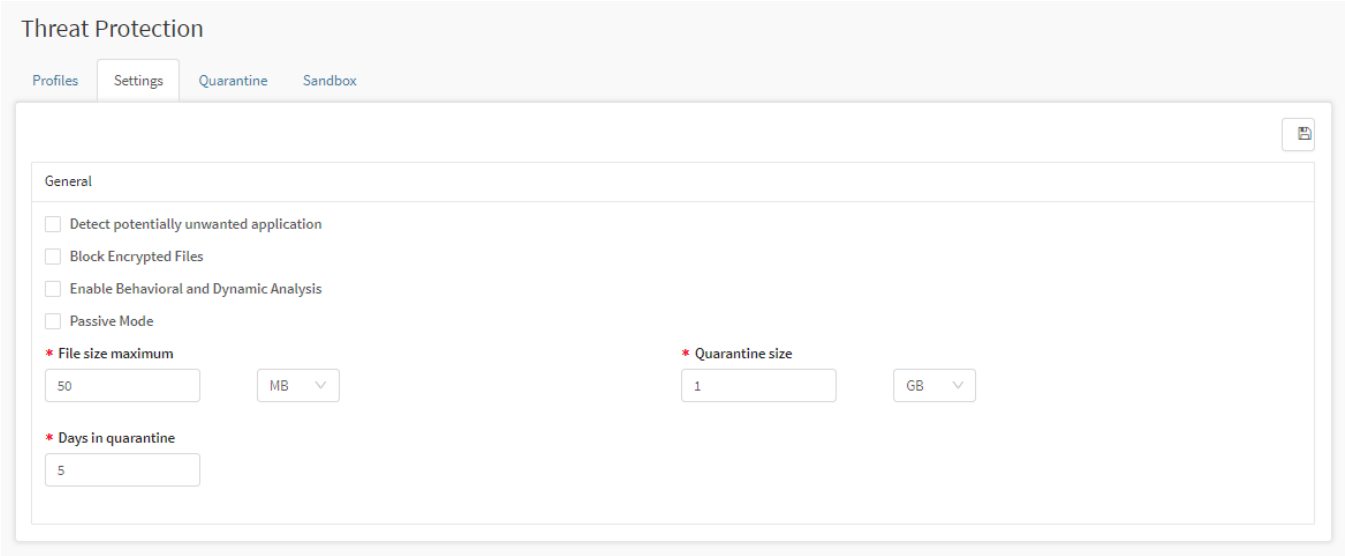
Threat Protection - Settings tab

In this tab, we define the parameters of the “detection types”, the “file sizes” for verification by Threat Protection and the “file lifetime” retained in quarantine.

To access these resources, click on "Settings".

Settings tab

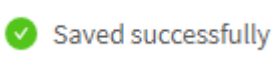
The Threat Protection “Settings” screen will appear, as shown in the image below:



Threat Protection - Settings tab - General

- ***Detect potentially unwanted application* [ ]:** To enable the detection of malicious files;
- ***Block encrypted files* [ ]:** To analyze blocked files and perform blocking;
- ***Enable behavioral and dynamic analysis* [ ]:** The dynamic analysis feature uses dynamic and behavioral detection techniques to identify suspicious or malicious behavior. This feature may flag or put an alert on behaviors that deviates from normal system activities;
- ***Passive mode* [ ]:** To disable the Threat Protection service block, in this option the system only generates reports and does not block the virus;
- ***File size maximum*:** Defines the maximum file size that will be analyzed by Threat Protection;
- ***Quarantine size*:** Sets the maximum quarantine size per user;
- ***Days in quarantine*:** Defines the number of days through which, files will be quarantined.

To complete this process, just click the [ ] button again.



Successfully Saved

After saving, for the changes to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

It's important to note that even if the service is disabled, if there is any Threat Protection profiles associated to an IPv4 or IPv6 Policy, the blocks will occur normally in case the Policy is active. To disable the service, besides deactivating it, we must remove the Threat Protection profile(s) from this (these) Policy (ies).

After performing these procedures the settings will have been successfully made.

Threat Protection - Quarantine tab

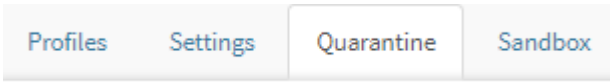
In the Quarantine tab it is possible to manage all detected threats that are in the quarantine of the Blockbit NGFW.

The quarantine is populated with entries thanks to the action of policies that use the profiles of Threat Protection that in its configuration was specifying insertion in the quarantine.

 For more information on Policies, visit this page.

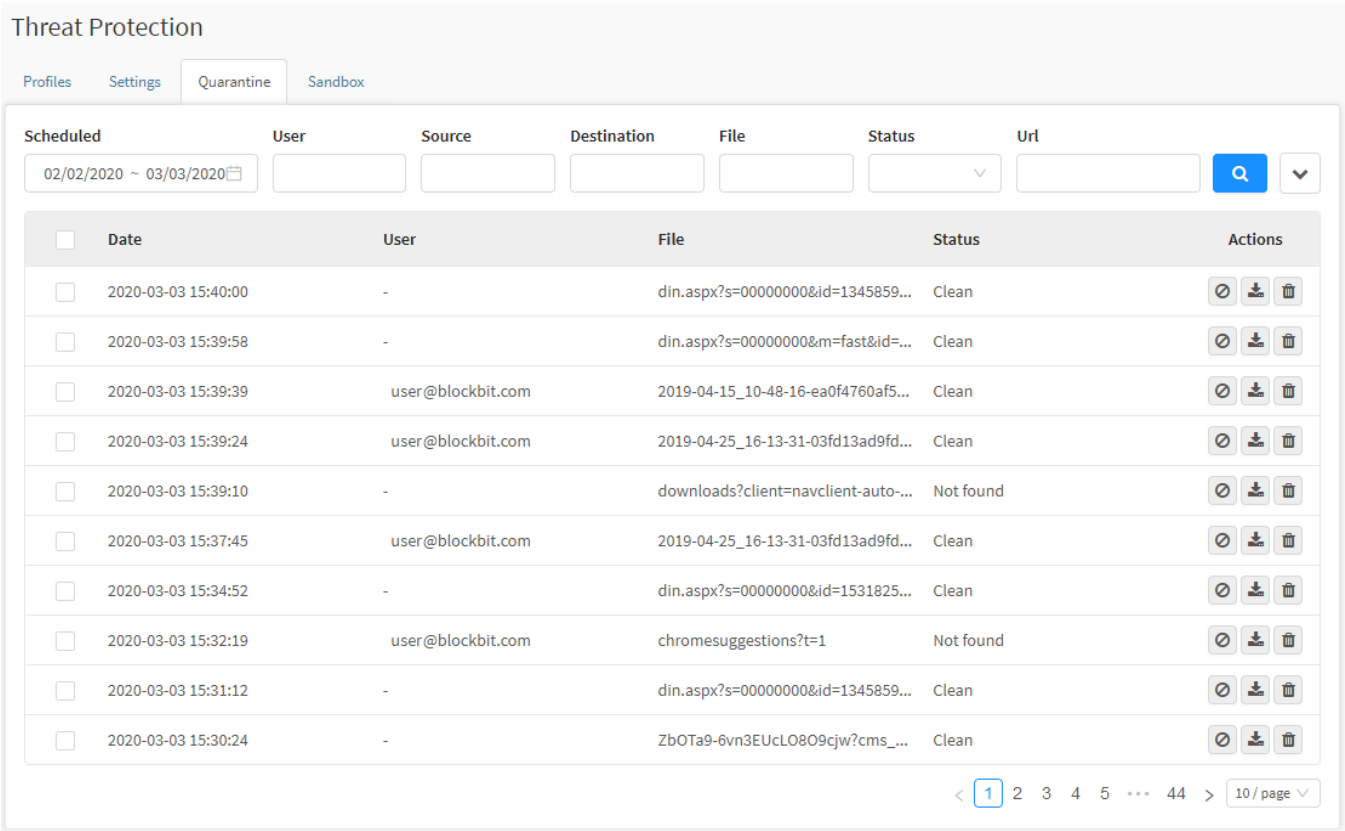
 For more information on Threat Protection profiles, visit this page.

To access this resource, click on "Quarantine".



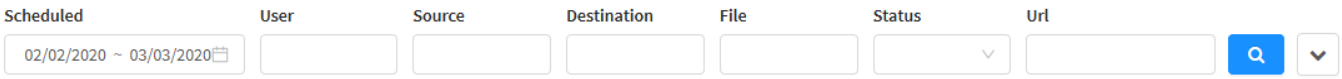
Quarantine tab

The Threat Protection “Quarantine” screen will appear, as shown by the image below:



Quarantine - Populated Quarantine

The quarantine has a search bar that allows the use of filters to perform a more effective search.

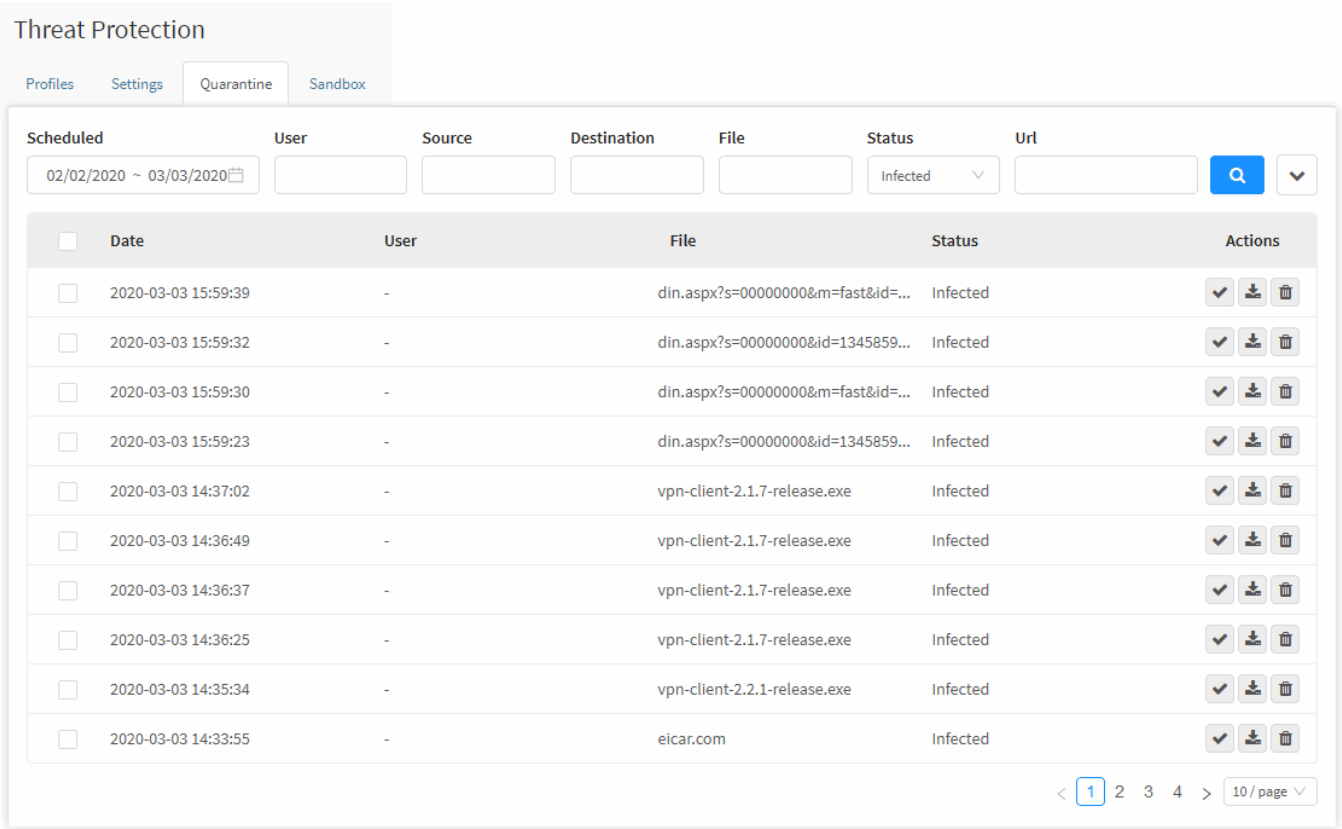


Quarantine - Search bar

This bar has the following fields:

- **Scheduled:** Determines a period of search, between two dates;
- **User:** In this field, it is possible to determine a user, to be used as a filter in the search;
- **Source:** Allows you to determine a source IP, to be used as a search filter;
- **Destination:** Allows you to determine a destination IP, to be used as a search filter;
- **File:** In this field, it is possible to determine the name of a file, to be used as a filter in the search;
- **Status:** Allows you to select the current state of the quarantine item to be used as a filter, the possible options are:
  - *Clean*;
  - *Infected*;
  - *Scanning*;
  - *Download*;
  - *Size Limit*;
  - *Not found*.
- **Url:** In this field, it is possible to determine a Url, to be used as a filter in the search.

To perform a search, just click **[**  **]**. The results are shown in the table below:



Quarantine - Result of a search

Next, we will analyze each component of this table:

- **Date:** Displays the date when the item was placed in quarantine;
- **User:** Displays the user related to this entry;
- **File:** Displays the file related to this entry;
- **Status:** Determines the current state of this road, the possibilities are:
    - *Clean*;
    - *Infected*;
    - *Scanning*;
    - *Download*;
    - *Size Limit*;
    - *Not found*.
- **Actions:** Displays a number of useful buttons:
    - ***Allow Download*** **[**  **]:** By clicking on this button, the file will be downloaded. This button is displayed if the status is "Infected";
    - ***Deny Download*** **[**  **]:** When clicking on this button, the file download will be denied;
    - ***Dowload*** **[**  **]:** Clicking on this button will start the download of the file in question;
    - ***Remove*** **[**  **]:** By clicking this button, this entry will be deleted from the quarantine.

Please note that the act of allowing or blocking the file download will reflect in the download action through the Captive Portal (9803 port).

Threat Protection - ATP Sandbox tab

In the Sandbox tab we are able to analyse the nature and classification of malicious or suspicious files and programs. It is a safe test environment, that ensures the integrity of the user's applications, with closed tests and abrangent threats classification.

As malware gets more sophisticated, monitoring suspicious behaviour to detect malware becomes even harder. Many threats over the last years have employed advanced obfuscation techniques that are able to avoid being detected by network security products and *endpoint*.

Blockbit's Threat Protection module, has the following samples and suspicious files verification flow;

1- Blockbit's Threat Protection generates a hash for the suspicious file*;*

2- Blockbit's Threat Protection verifies the file's generated hash in order to figure if it's on the Denied or Allowed list;

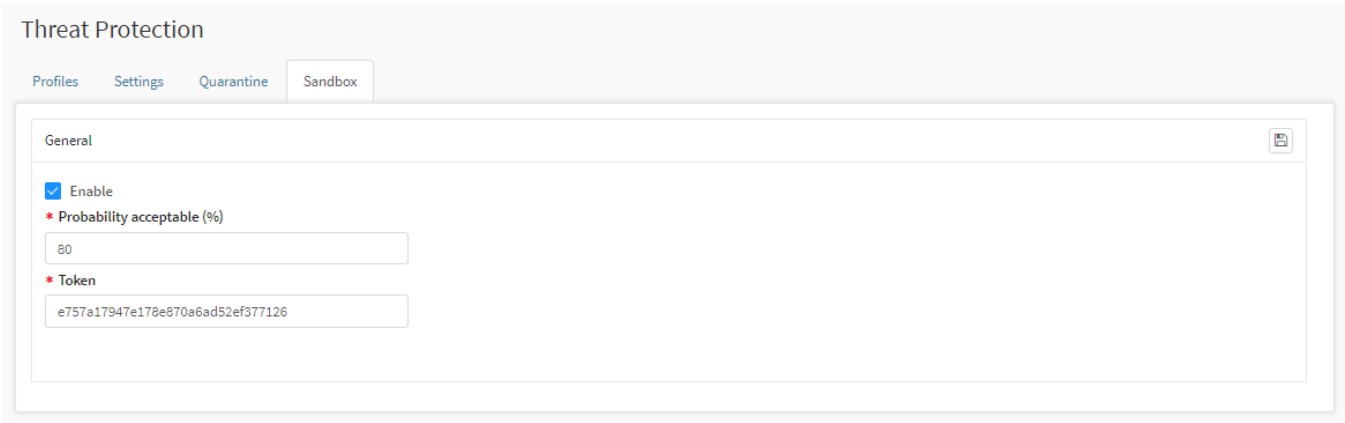
3- Blockbit's Threat Protection verifies if the file's generated hash had been verified and classified by the Blockbit Labs, then takes the block or allow action;

4- Blockbit's Threat Protection analyses the file searching for threats by using the traditional method (matching with known antimalware signatures);

5- If the file doesn't match any known signatures or the hash base fed by the Blockbit Labs, but presents a suspicious behaviour it is then sent for analysis within the Sandbox.

A Sandbox is an isolated test environment that allows users to run programs or open files without affecting the application, system or platform in which they are being run.

Sandboxes are used to safely run malicious codes in order to avoid damage to the host device, to the network or to other connected devices. Using a Sandbox to detect malware offers an aditional layer of protection against security threats, such as stealth attacks and exploits that use zero-day vulnerabilities.



Threat Protection Sandbox

- ***Enable:*** Enables the supected files and applications analysis by the Sandbox.
- ***Probability acceptable:*** Minimum acceptable behaviour/aspect deviation probability of a file or application to be executed on the Sandbox.
- ***Token:*** Validation token to allow the use of the Sandbox alongside the NGFW.

For further detail, please access our Sandbox - Administrator's Guide.

UTM - Services - SD-WAN

The Blockbit NGFW contemplates multiple internet links, being able to segment and prioritize traffic through network interfaces according to the data obtained by monitoring various performance indicators, allowing traffic to be routed through the interfaces configured through the best path available, this benefit is obtained through the SD-WAN.

The acronym SD-WAN stands for Software-Defined Wide Area Network (Software-Defined Networking in Wide Area Network), it is a means of performing dynamic traffic distribution, monitoring and decision making according to the best performance available. Thanks to the dissociation of control methods from the network hardware, the SD-WAN enables a holistic view of the applications in use, which enables the provision of intelligent load balancing, facilitating decision making during the process of creating the SD-WAN.

The monitoring function of the SD-WAN is to allow the supervision of specific data from the WAN, enabling the best network path according to the factors determined by the administrator, which allows directing the most appropriate resources according to predetermined rules and policies or based in the specific profile of users. "Monitoring" follows up these factors below:

- Latency;
- *Jitter*;
- Packet Loss;
- Bandwidth Consumption.

Using the data obtained through this monitoring, the SD-WAN offers the function "Tolerance to failures", having a redundancy feature (Failover) that allows the use of the best link available in case of any irregularity is found on the primary link. In addition, the SD-WAN monitors the status of the network card, if it is detected as off (for example, in a network cable disconnection event), it will automatically mark the affected link as down without waiting for the monitoring time. and immediately switching to the best link available.

The link failure controller is capable of applying availability tests in real time, enabling the performance of Load Balance defined by %, which allows the division of the load between the links, which represents a minimization of the response time, ensuring the quality use of links. Finally, the system also includes the Spillover and Dynamic Selection types.

The SD-WAN contemplates 4 modes of operation:

- *Failover*;
- *Load balance*;
- *Spillover*;
- *Dynamic Selection*.

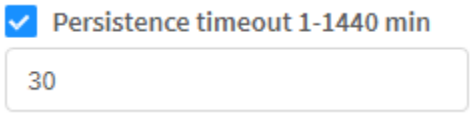
Link persistence

Link persistence is only available in the Load Balance, Spillover and Dynamic Selection options.

The main purpose of the "link persistence" function is to prevent connections drop in applications that use SSL encrypted traffic. With the checkbox enabled, each source IP address will use a single link from the profile specified in the policy that the connection was released, this condition is only changed after the idle time defined in the field “Persistence timeout 1-1440 minutes”, or even if some irregularity is detected in the performance indicators, indicating an instability in the link.

In summary, each source IP address will use only one link defined in the profile, this configuration makes SSL encryption protocols no longer affected by balancing the use of multiple connection links.

To activate connection persistence, the “Persistent connection” check box must be enabled, which will be available in the SD-WAN profile panel in any operating mode where dynamic balancing occurs (Failover does not perform balancing).



Connection persistence

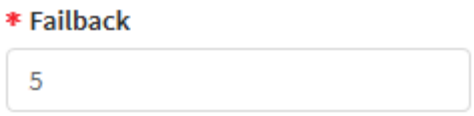
By enabling the checkbox in the SD-WAN profile panel, the administrator determines whether the connection from a single source address will be persistent.

Having this option enabled, it is possible to determine a time limit for the operation of this resource, with the default time being 30 minutes after the last activity.

Failback

The Failback feature is available for all types of SD-WAN, it is a process that makes it possible to restore the service so that it returns to its functional state in case the connection is unstable or inoperable.

If a link stops responding the failback is activated, it acts by performing connectivity tests, taking into account the counter value determined by the user, which determines the number of successes in sequence necessary to define if this inactive link has become stable again. Therefore, packet routing will only be restored if the failback verification tests reach the user-defined limit. If in the middle of the tests a new connection failure is detected, the failback counter is reset.



Failback

If the SD-WAN profile was created before the implementation of this feature, the value will be automatically 1. New profiles are created by default with a value of 5.

SD-WAN Features:

- ***Performance Monitoring*:** Link monitoring based on performance indicators;
- ***Dynamic Path Selection*:** Traffic prioritization based on performance indicators;
- ***Link Failover & Load Balance*:** Redundancy and link balancing based on performance indicators;
- ***Traffic Shapping & QoS*:** Bandwidth control and metrics definition for quality and service prioritization;
- ***Traffic Duplication*:** Duplication of packets across multiple network interfaces;
- ***Secure SD-WAN*:** Routing controls based on security policies.

The error control method - FEC (Forward Error Correction) - when enabled, helps in the reduction of errors in the SD-WAN modules and VPN tunnels.

Note that thanks to the encapsulation, it may be necessary to increase the MTU values of the interfaces in order to avoid fragmentation. For more information, see this page.

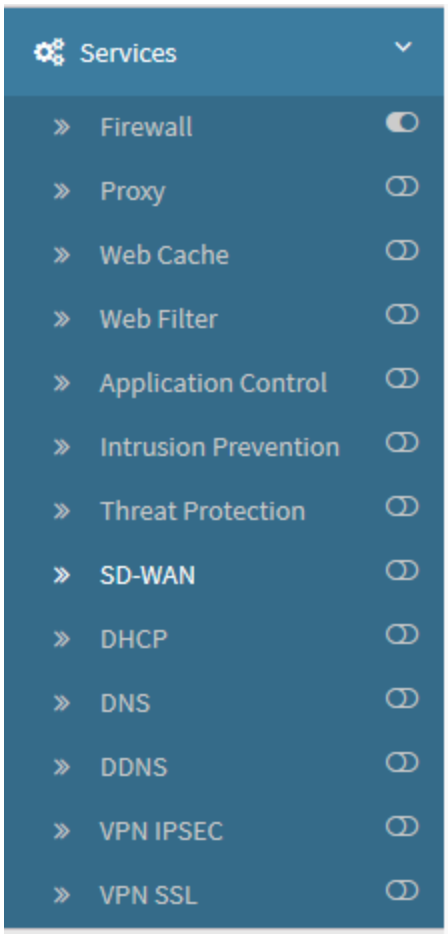
It is possible to view the SD-WAN debug logs through the CLI console, for more information, check the command line chapter.

About the secondary Link operation modes:

***Link Failover (active-passive):* Is an operation method, in which there are two or more configured internet links, being one the active and the other one(s) the passive(s). On the active-passive mode, all the data traffic is directed to the active link, while the passive links remain in standby, waiting for a failure on the active Link. Should the main link fail, the system automaticaly redirects the traffic to one of the passive links, ensuring the internet connection's continuity.**

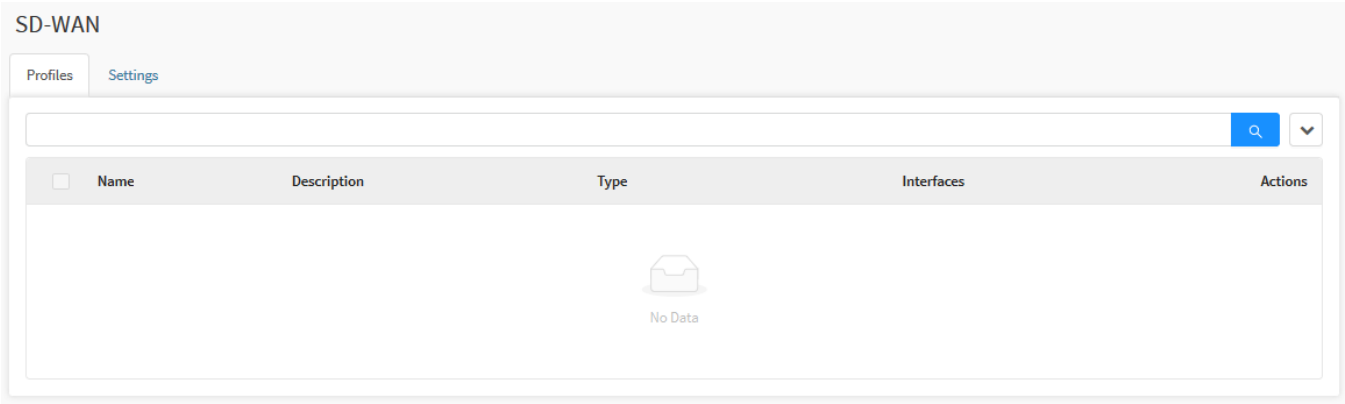
***Load-Balance (active-active):* Is a method used to ensure high availability and take greater advantage on the available links' capacity. In this operation mode, all of the configured internet links are simmultaneously active and share the traffic load on a balanced way. On the active-active mode the traffic is distributed among the links on a balanced way, allowing the links' full capacity to be used. Which means that instead of only a single link being active and the others passive, all of them are at full function, equaly splitting the traffic load.**

To access the SD-WAN screen, select the option as shown on the image below:



Services - SD-WAN

A tela abaixo será exibida:



SD-WAN – Profiles

The SD-WAN screen has the following tabs:

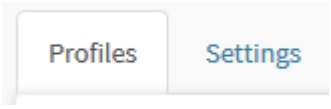
- *Profiles*;
- *Settings*;

Next, we will analyze each component of the *Profiles* tab.

SD-WAN - Profiles tab

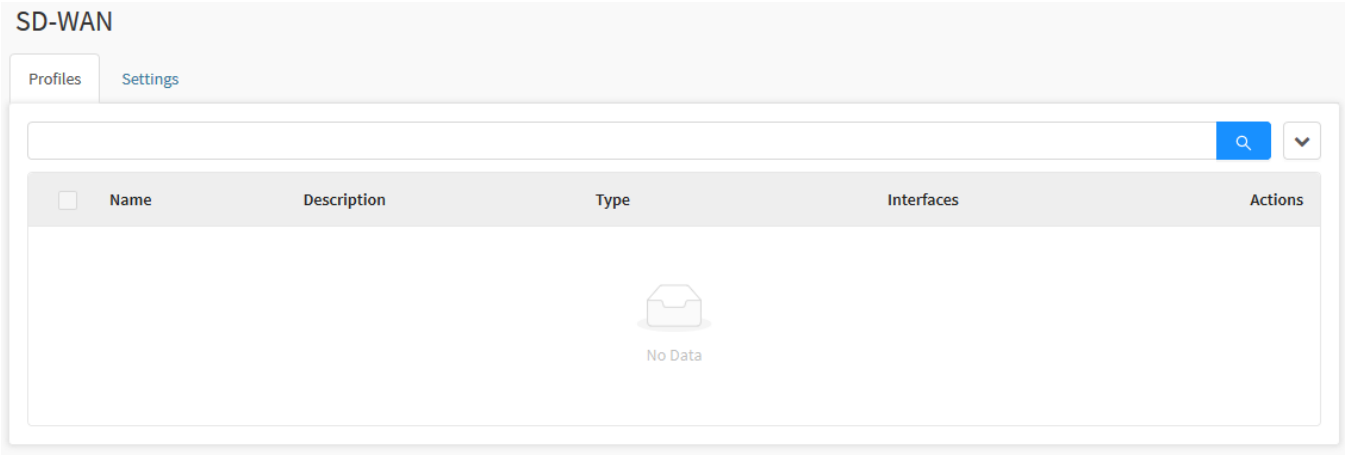
The monitoring function of the SD-WAN supervises specific data from the WAN, enabling the best network path according to the factors determined by the administrator, this allows directing the most appropriate resources according to predetermined rules and policies or based in specific profile of users.

If the tab is not selected, click on "Profiles".



Profiles tab

The following screen will appear:



SD-WAN

This session will cover how to

- Register, edit and remove *SD-WAN profiles*;
- Particular features of each operating mode;
- Step by step of the complete configuration of an SD-WAN.

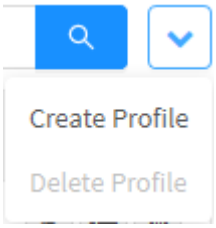
Next, we'll look at the functions located at the top of this panel.

SD-WAN - Profiles - Actions menu

At the top right of the screen we have the actions menu:

SD-WAN – Actions Menu button

By clicking on this button the menu below is displayed:



SD-WAN – Actions menu

The menu consists of the following options:

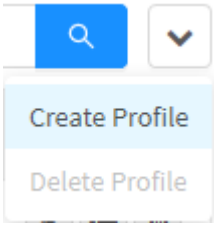
- *Create Profile*;
- *Delete Profile*.

Next, each action menu option will be detailed.

SD-WAN - Profiles - Actions Menu - Create Profile

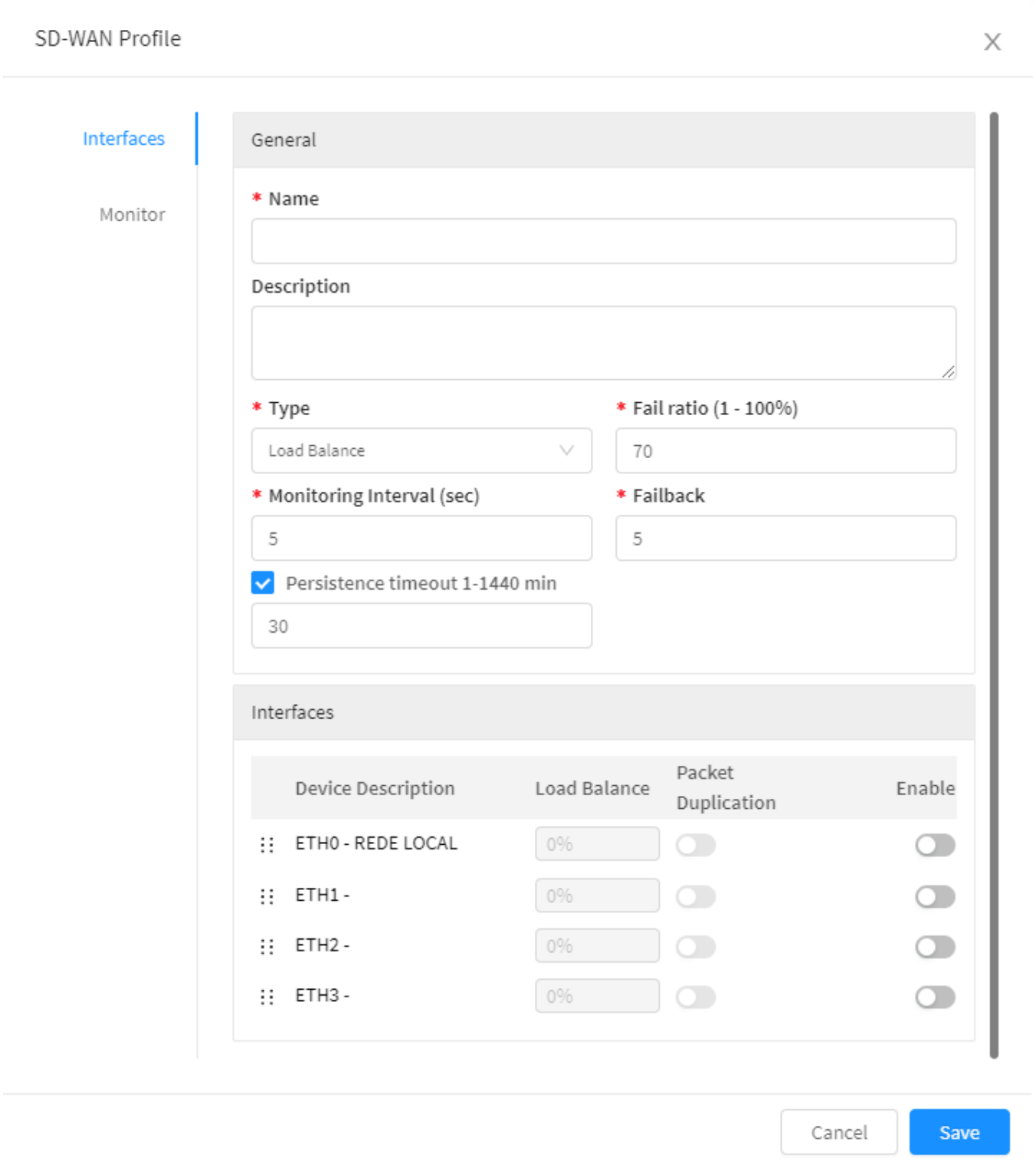
Through the option “Create Profile” it is possible to create a new SD-WAN profile. To access, click on the **Actions Menu [ ]**.

1. Click on the “Create Profile” option;



SD-WAN - Create Profile

2. The screen shown below will be displayed:

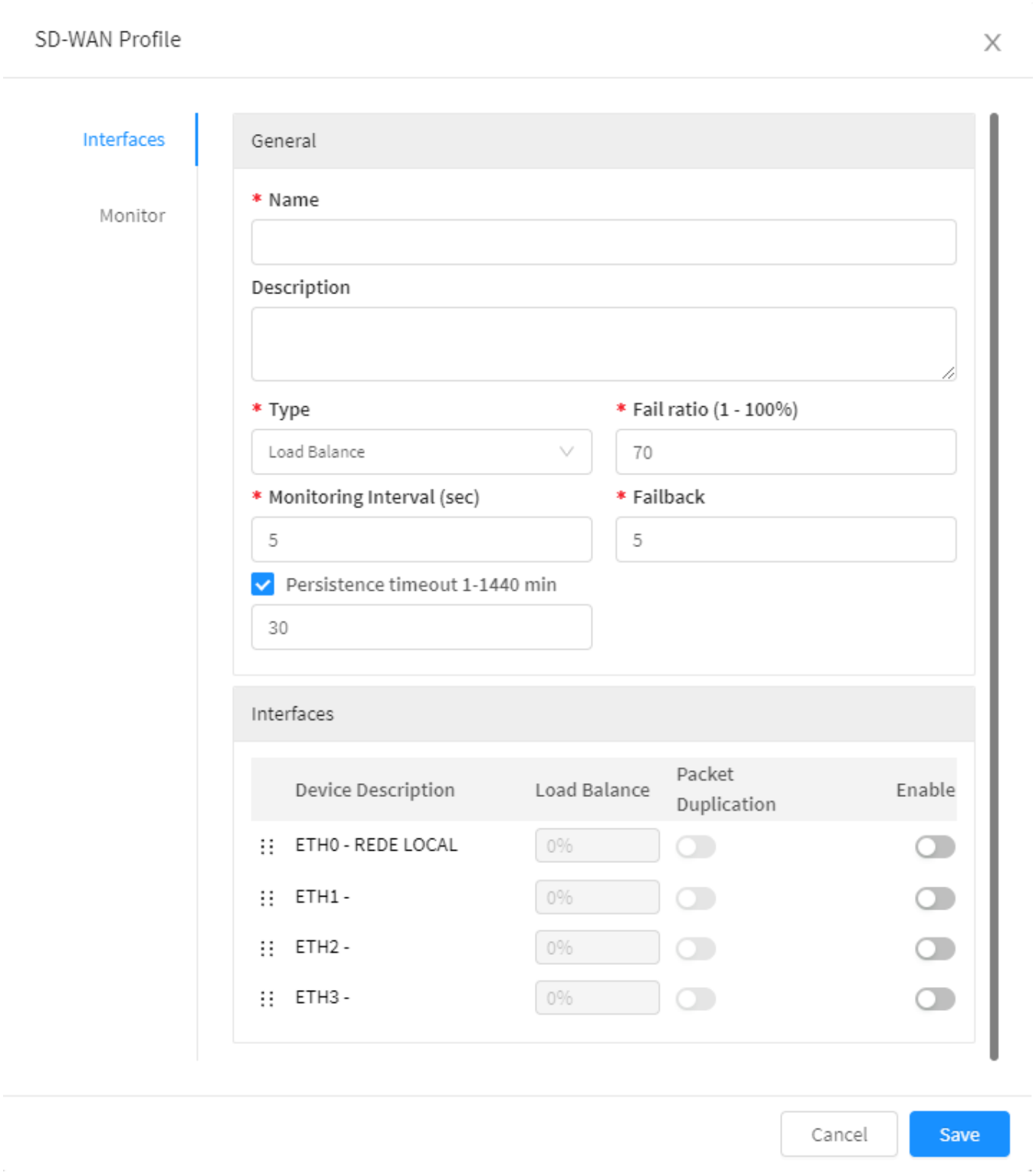


SD-WAN - Profile

In this panel it is possible to make all the configurations regarding the performance of the SD-WAN. Next we will demonstrate how to configure the Load Balance, for more information about SD-WAN profile types check the SD-WAN - Profile Types page.

Interfaces tab

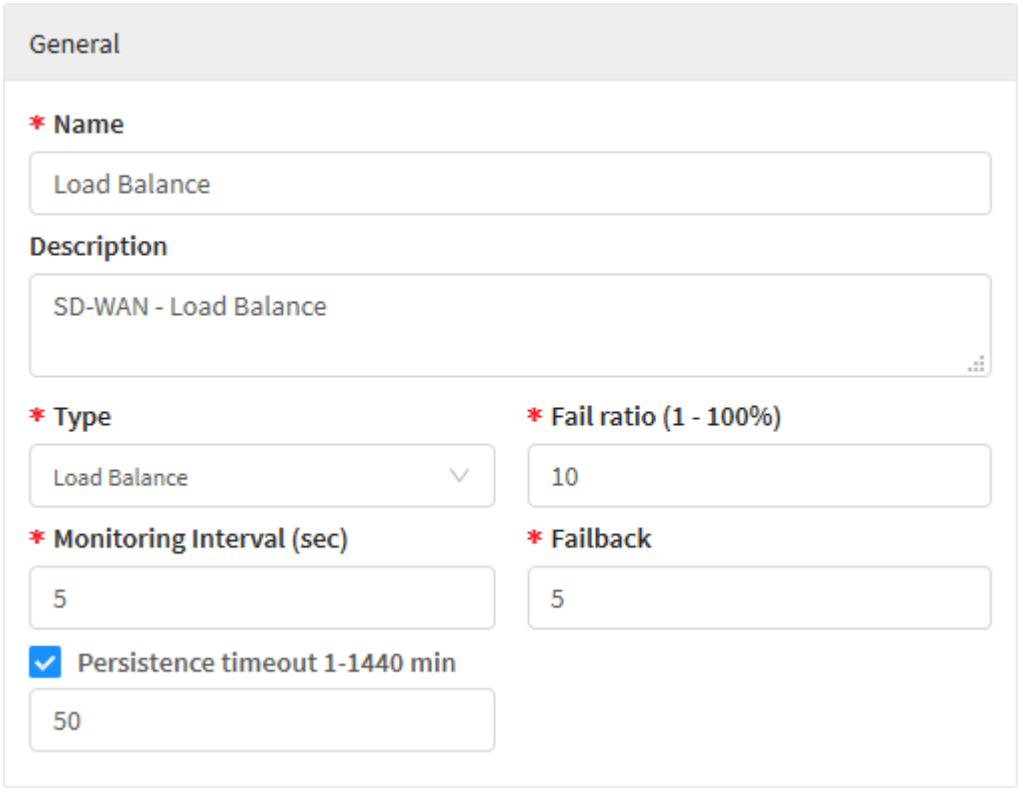
In this tab it is possible to configure how the SD-WAN will interact with the eth interfaces



SD-WAN – SD-WAN Profile - Interfaces tab

General Panel

In "General" we have the following text boxes:

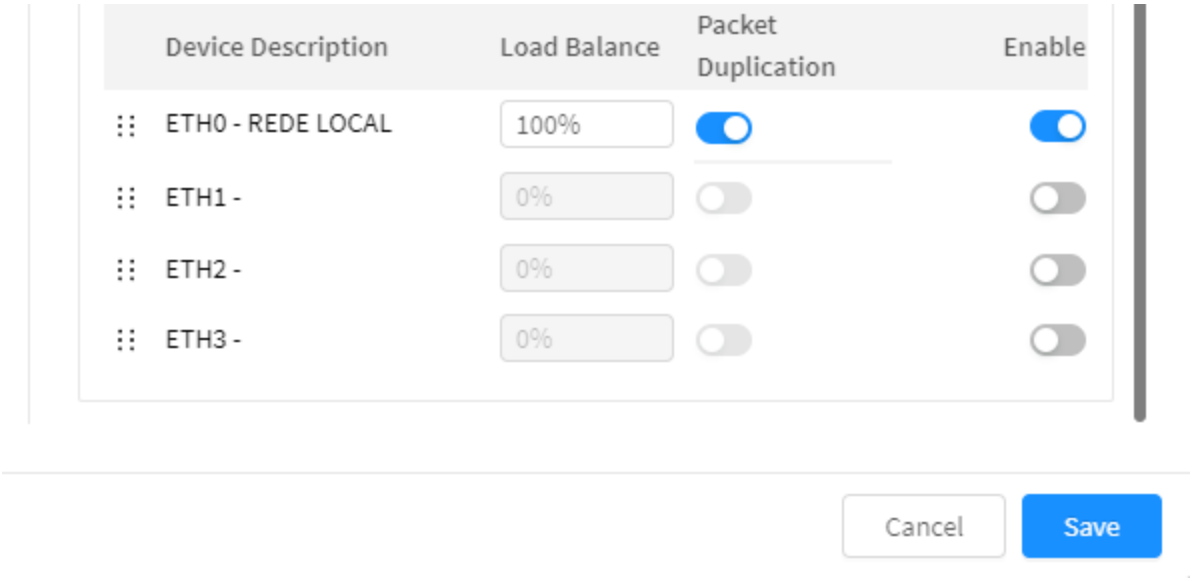


SD-WAN – General

- ***Name:*** *Define a name for the profile*. Ex.: *Load Balance*;
- ***Description*****:** Define a description for the profile. Ex .: SD-WAN - Load Balance;
- ***Type*****:** Sets the SD-WAN behavior. Selecting these options defines which text fields will be displayed in the General panel. It is possible to select any type, but in this demonstration we will use “Load Balance”. For more information about the types of SD-WAN check the chapter about Profile types. The available options are:
  - Load Balance;
  - Failover;
  - Spillover;
  - Dynamic Selection.
- ***Interfaces*****:** It is essential for the correct functioning of the SD-WAN to define the internet link interfaces that will be used in the composition of the profile. In this example we will select the interfaces: "tun0 - Network 10" and "tun1 - Network 11";
- ***Monitoring Interval*** **(sec.):** Defines the monitoring interval between each test. It is recommended to leave it as 1 second. Ex.: 1 second;
- ***Failback:*** Defines the number of times that an interface whose connectivity has failed will be tested to enable routing through it. For example, if the value is 5 (the default), the interface will need to successfully pass 5 consecutive connectivity tests to be considered active again. The maximum Failback value is 100. For more information see this page. Ex.: 5;
- ***Fail Ratio*** **1-100%:** Set the failure rate value between 1 to 100%. It is recommended to leave the default on 70%. Ex.: 70%.
- ***Persistence Timeout 1-1440*** **min:** Prevents connections from falling in applications that use SSL encrypted traffic. For more information, check this page.

Interfaces panel

In "Interfaces" we have the following options:



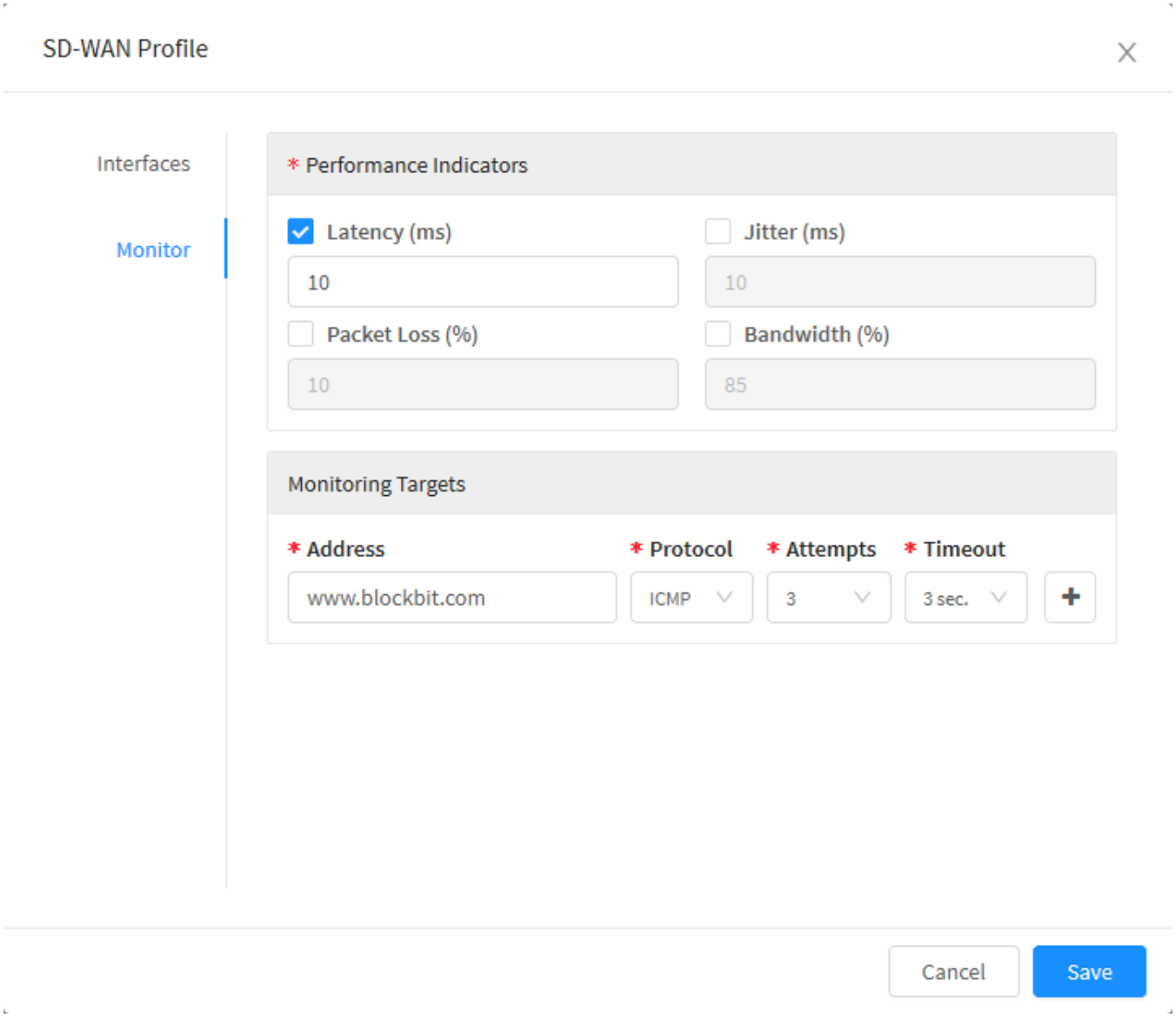
SD-WAN – Interfaces

It is only possible to interact with the interfaces that have been enabled **[** **]** if an interface is disabled **[** **]**, it will be grayed out, it will not be possible to edit it and will be disregarded.

- **Move[ ]:** Click and drag to the desired position, so the link that is in the first position from top to bottom will be used for outgoing traffic, if the link is disabled, the traffic will be automatically redirected to the subsequent link in the list, thus ensuring high availability in internet access, when the link is enabled again the system will automatically return the output to the first link in the list;
- ***Interfaces*:** It is essential for the correct functioning of the SD-WAN to define the internet link interfaces that will be used in the composition of the profile. In this example we will select the interfaces: "eth0" and "eth1";
- ***Load Balance***: When enabling multiple ETHs, please note that the Load Balance, which consists in the volume of data traffic by ETH, will be divided among all of the enabled ones.
- ***Packet Duplicaction***: Enables the packet duplication mode by alternative paths, so that in cases of data loss, a copy of the missing data packet can be sent to the server, allowing a greater integrity in the data traffic.

Monitor tab

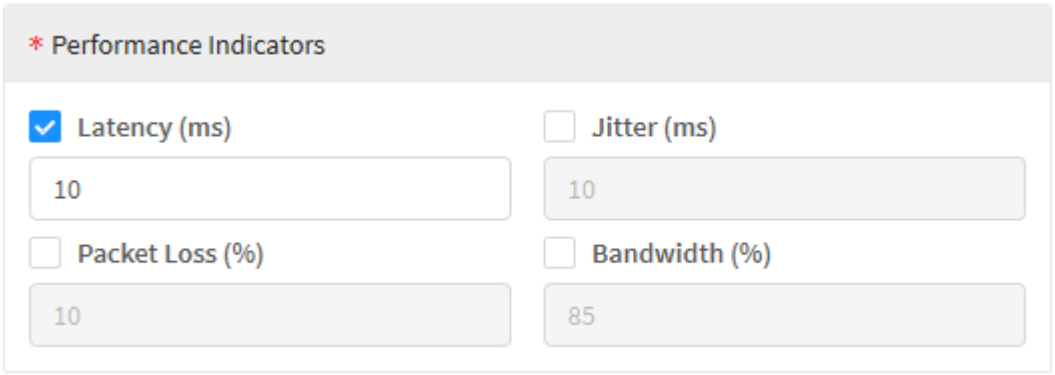
In this tab, the performance indicators and monitoring targets used by the SD-WAN are configured.



SD-WAN – SD-WAN Profile - Monitor tab

Performance Indicators panel

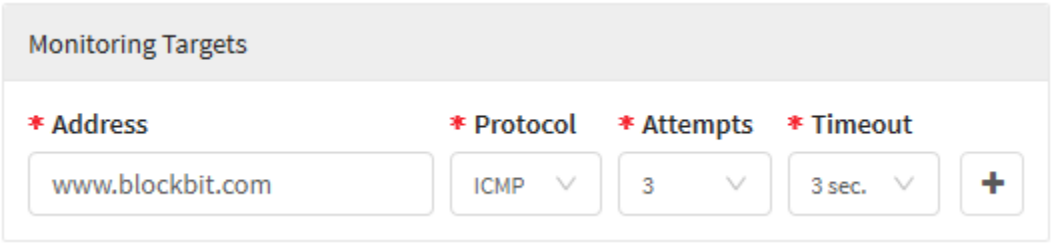
In "Performance Indicators" we have the following text boxes:



- ***Lattency*:** Determines how long it takes for a data packet to leave the origin, arrive at the destination, and return. Ex .: 10 ms;
- ***Jitter*:** Determines the average of how long it takes for a data packet to leave the origin, arrive at the destination and return. Ex .: 30 ms;
- ***Packet Loss*:** Determines the acceptable percentage of packet loss. Ex .: 75%;
- ***Bandwidth*:** Determines the acceptable percentage of bandwidth consumption. Uses as a base the download values in “Traffic Shaping”. Ex.: 70%.

Monitoring Targets panel

In "Monitoring Targets" we have the following text boxes:



SD-WAN – SDWAN Profile - Monitoring Interfaces

Defines the addresses where the tests will be performed. It is recommended that in the "Monitoring Targets" the virtual IPs are placed on the other side of the tunnel so that if the communication is successful, it can indicate that the tunnel is correctly configured.

Finally, if you want to cancel click on the **[** Cancel **]** button. To finish editing the applications, click on the **[** Save **]** button.

For more information about the particularities and differences of each type of profile, check this page.

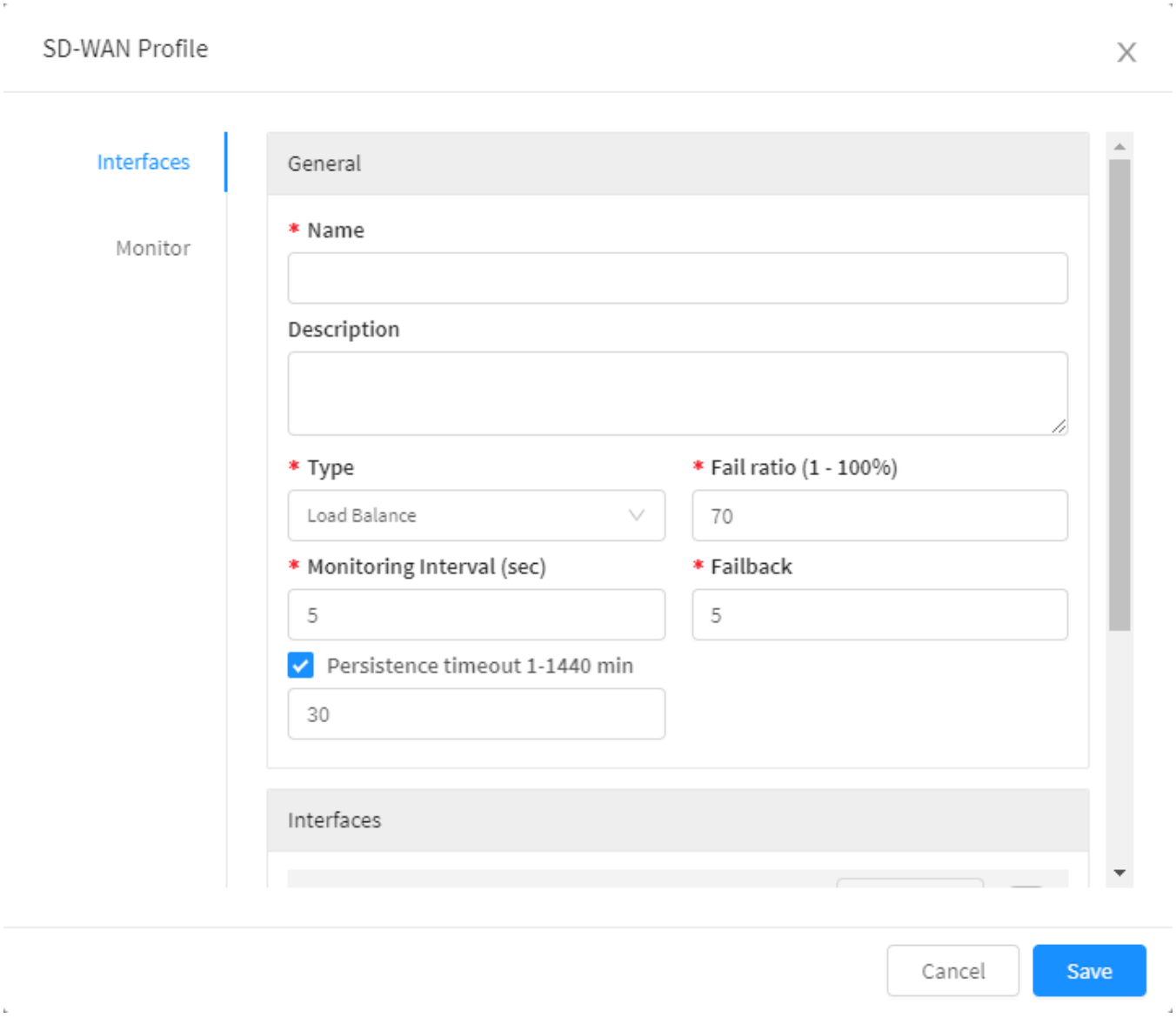
For an example on how to set up an SD-WAN profile, check this page.

SD-WAN - Profile Types

On the following pages, we will thoroughly analyze each particular feature of the SD-WAN's modes of operation.

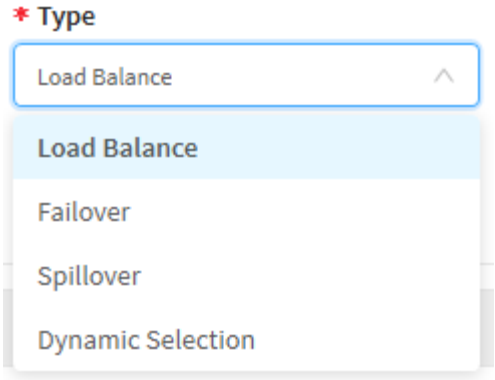
The SD-WAN includes 4 different operating modes, to determine which one will be used in the profile, follow the instructions below:

1. Click on the edit button or create an SD-WAN profile by selecting the Create Profile option in the action menu, the screen below will be displayed.



SD-WAN – Add profile.

2. To determine the SD-WAN's mode of operation, click on the “Type” checkbox and determine the desired option



SD-WAN - Type

As shown in the image above, the SD-WAN contemplates the following modes of operation:

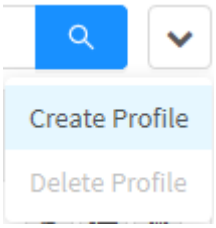
- *Load Balance*;
- *Failover*;
- *Spillover*;
- *Dynamic Selection*.

We will analyze the distinctions between each of these types.

SD-WAN - Load balance

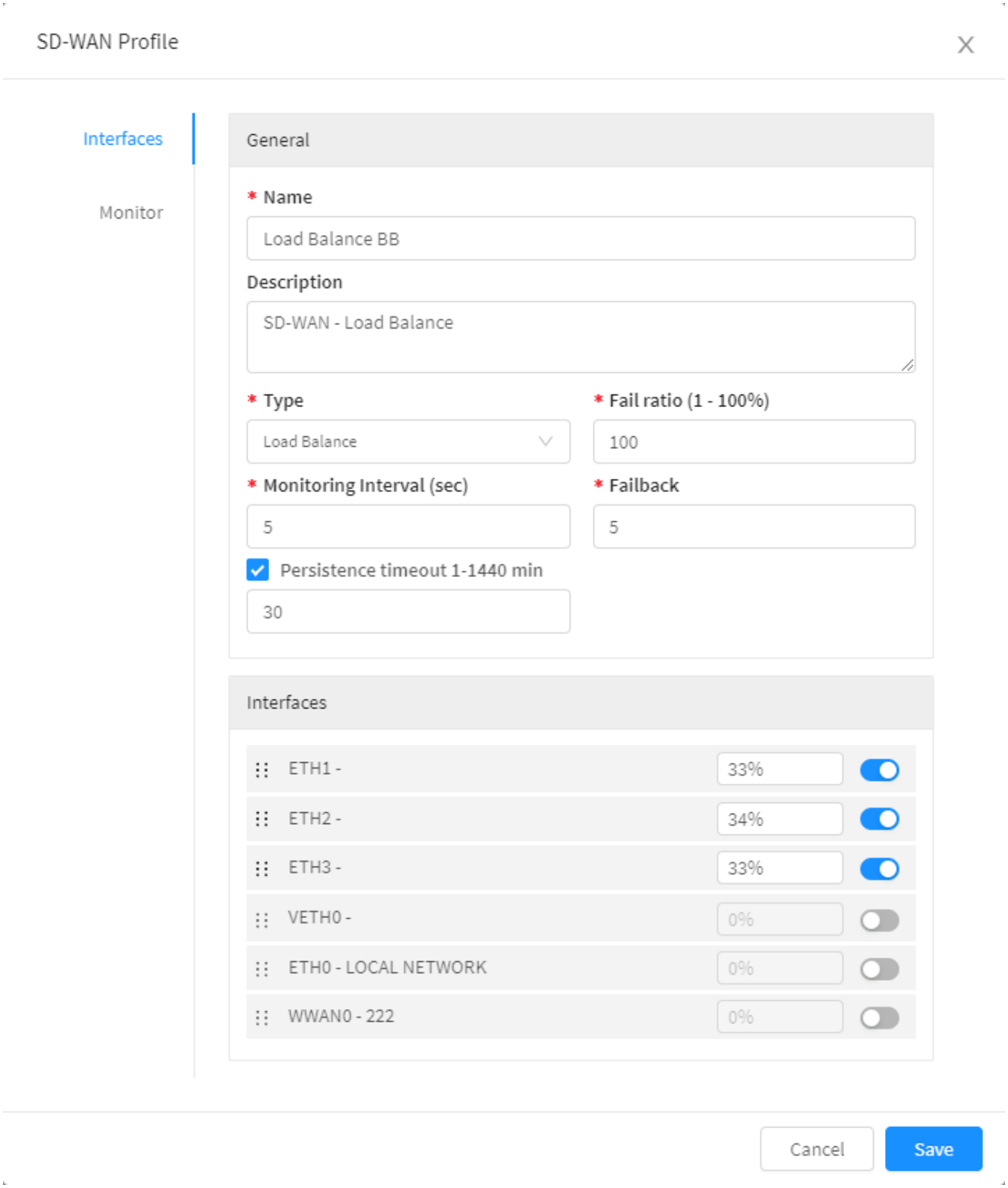
Using Load balance, it is possible to balance through % the new connections in this way, redirecting traffic according to the % defined for each link in order to optimize the use of resources, maximize performance, minimizing the response time by avoiding the overload of a given link, so it is also possible to increase reliability through redundancy.

1.To access, click on the **Actions menu [**  **]** and select the option “Create Profile”;



SD-WAN - Create Profile

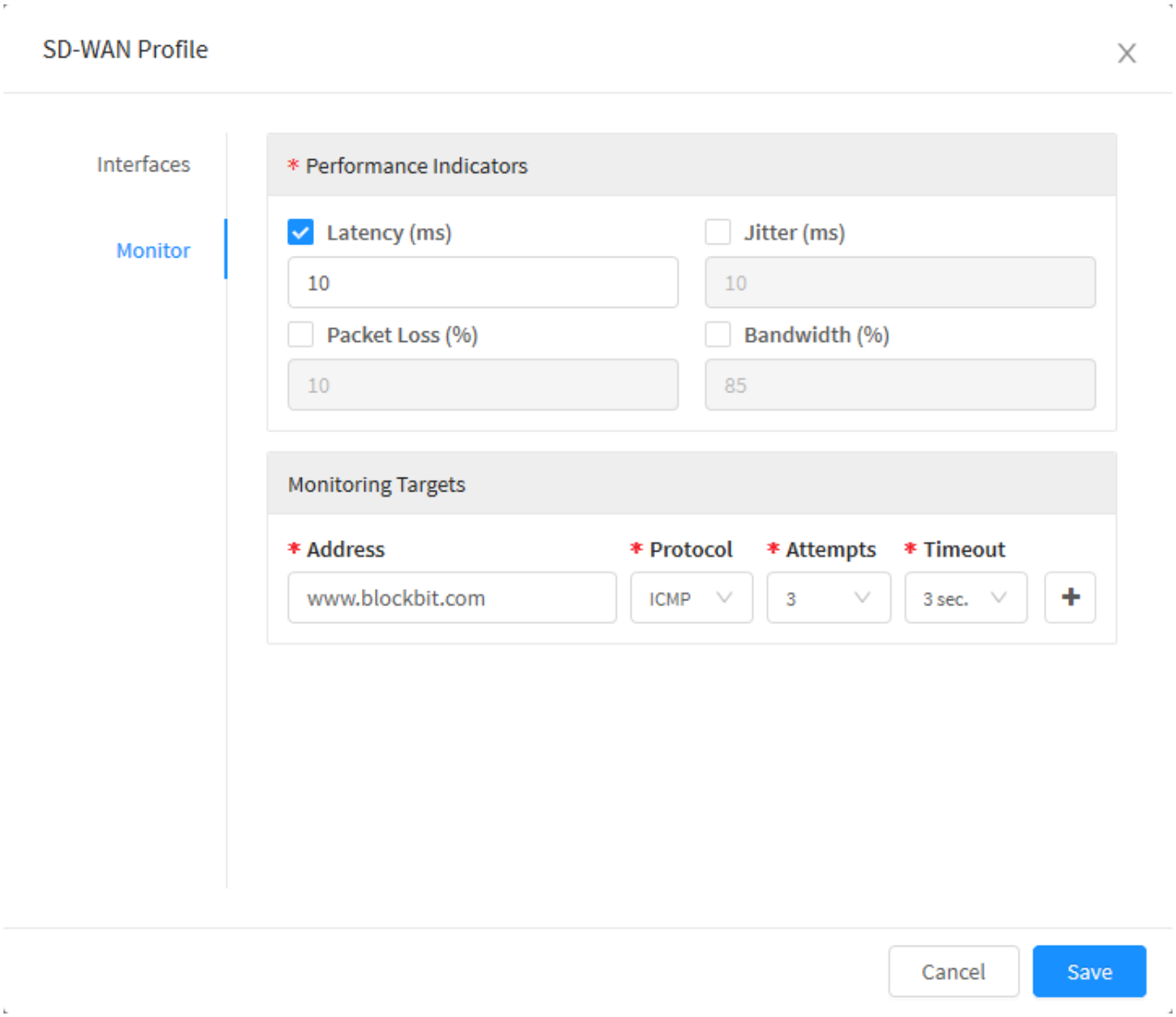
2. The screen shown below will be displayed:



SD-WAN – Load Balance - Interfaces

- ***Fail ratio* 1-100%:** Set the failure rate value between 1 to 100% so that the link is considered offline. Ex.: 70%;
- ***Monitoring interval* (sec.):** Define the monitoring interval between each test. Ex.: 5 seconds;
- ***Failback*:** Defines the number of times an interface whose connectivity has failed will be tested to enable routing through it. For more information see this page. Ex.: 5.
- ***Persistence timeout 1-1440 minutes* [☑]:** Defines the “persistence timeout” time to drop the connection in the event of an idle time. Ex.: 15 min;

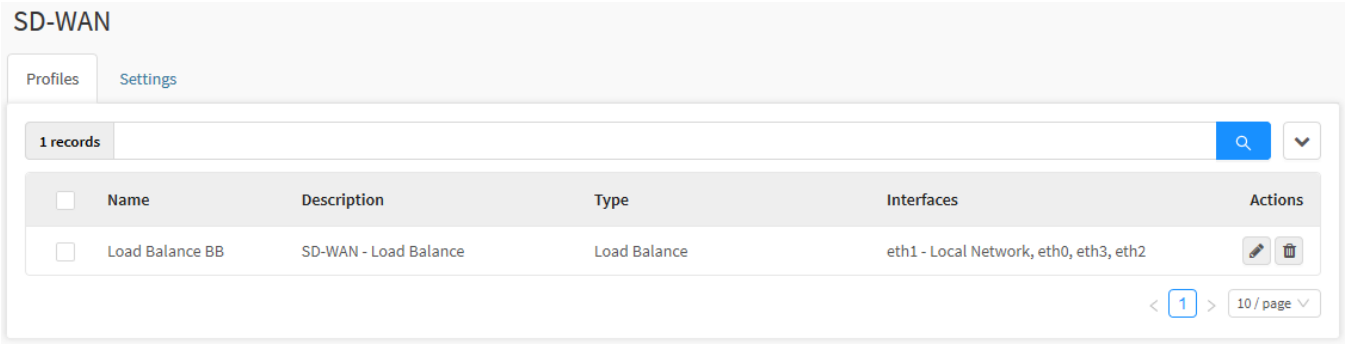
3. Access the "Monitor" tab:



SD-WAN – Load Balance - Monitor

4. Add the performance indicators and monitoring targets you want.

After all the fields duly filled out, click on the [Save] button;

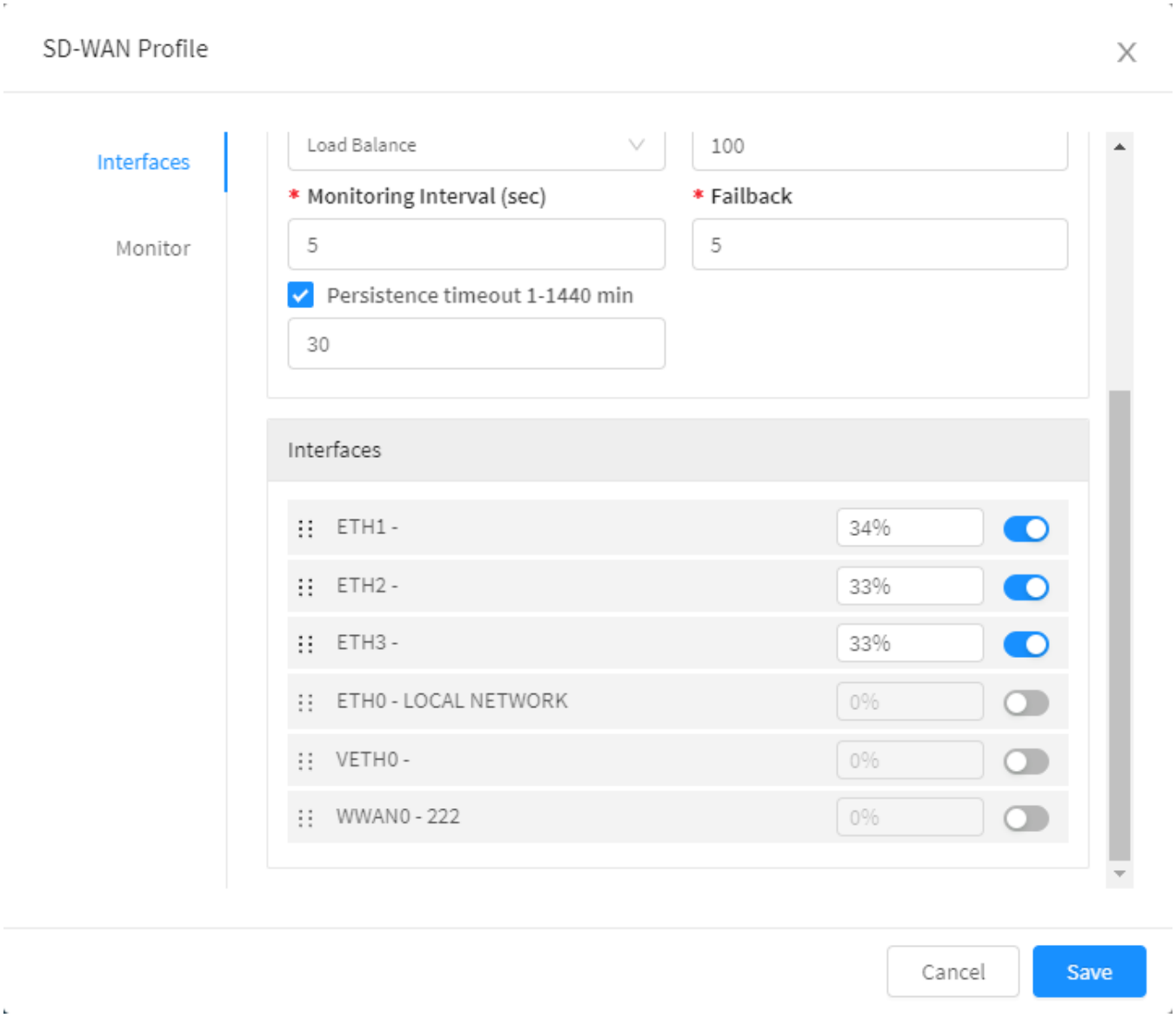


SD-WAN – Profiles

Finally, after saving, for the SD-WAN to take action it will be necessary to access the **command queue [**  **]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures the SD-WAN Load Balance will have been successfully configured.

When editing the registered profile it is possible to view the status of the link according to the screen below.



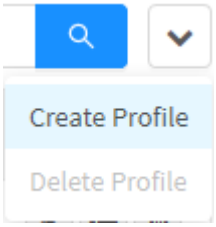
SD-WAN – Edit profile – Load Balance

In the example above, if the interface link eth1 goes offline, the % value that has been set for it will be divided evenly between online links, in our example the 30% that were defined for the eth1 interface link would be divided between the remaining 2 links with online status leaving the 2 links respectively with 70% and 30%, thereby increasing reliability through redundancy of links. Once the system detects which eth1 link has resumed its online status, it will return the balancing weight between all links, so in our example it would return to eth1 = 30%, eth2 = 55% and eth3 = 15%.

SD-WAN - Failover

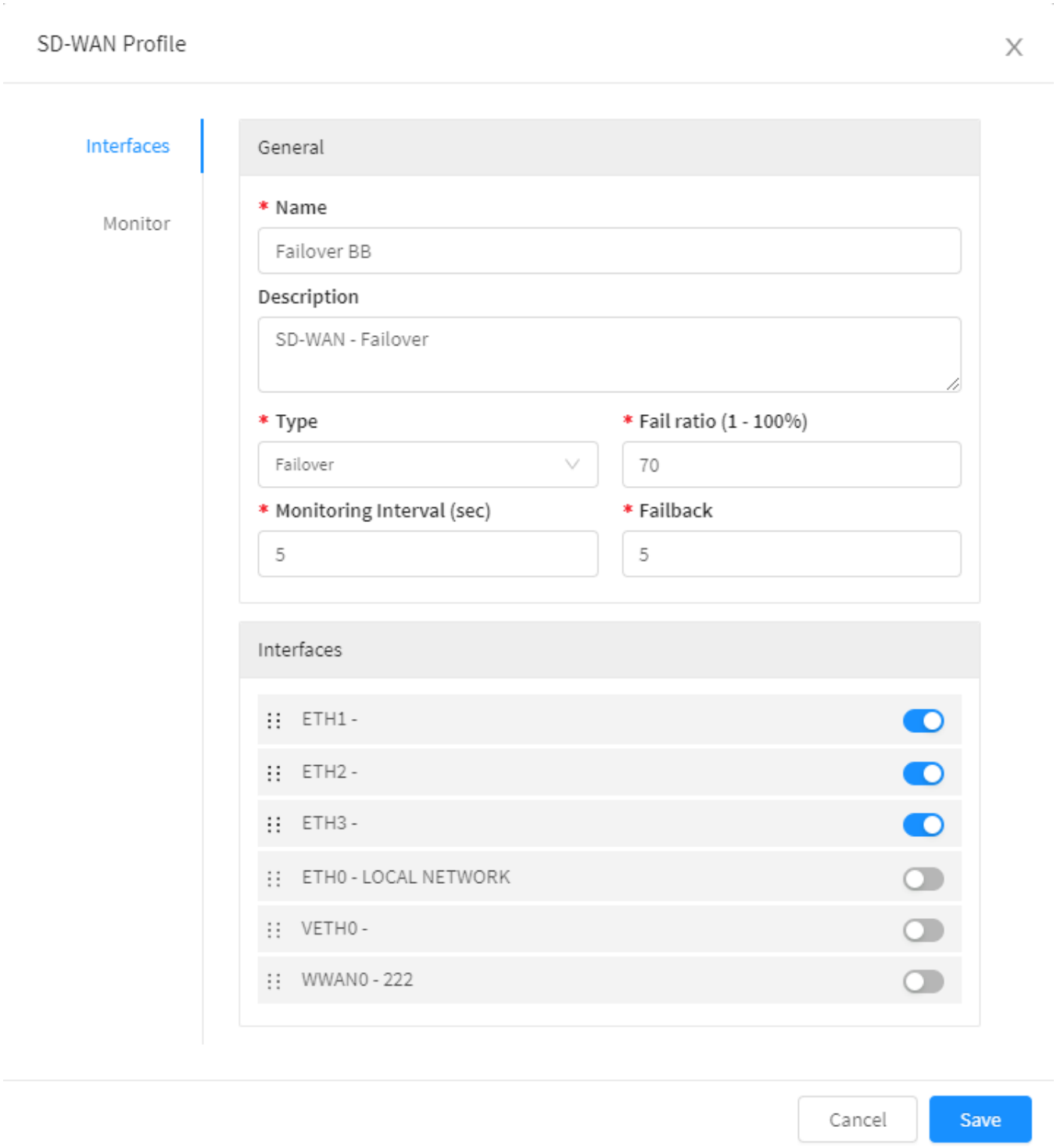
Failover actively monitors internet links and acts according to the failure, being able to apply link availability tests in real time, thus defining an alternative route in case of failure of the main link and automatic re-establishment of link routing.

1. To access, click on the **Actions menu [ ]** and select the “Create Profile” option;



SD-WAN - Create Profile

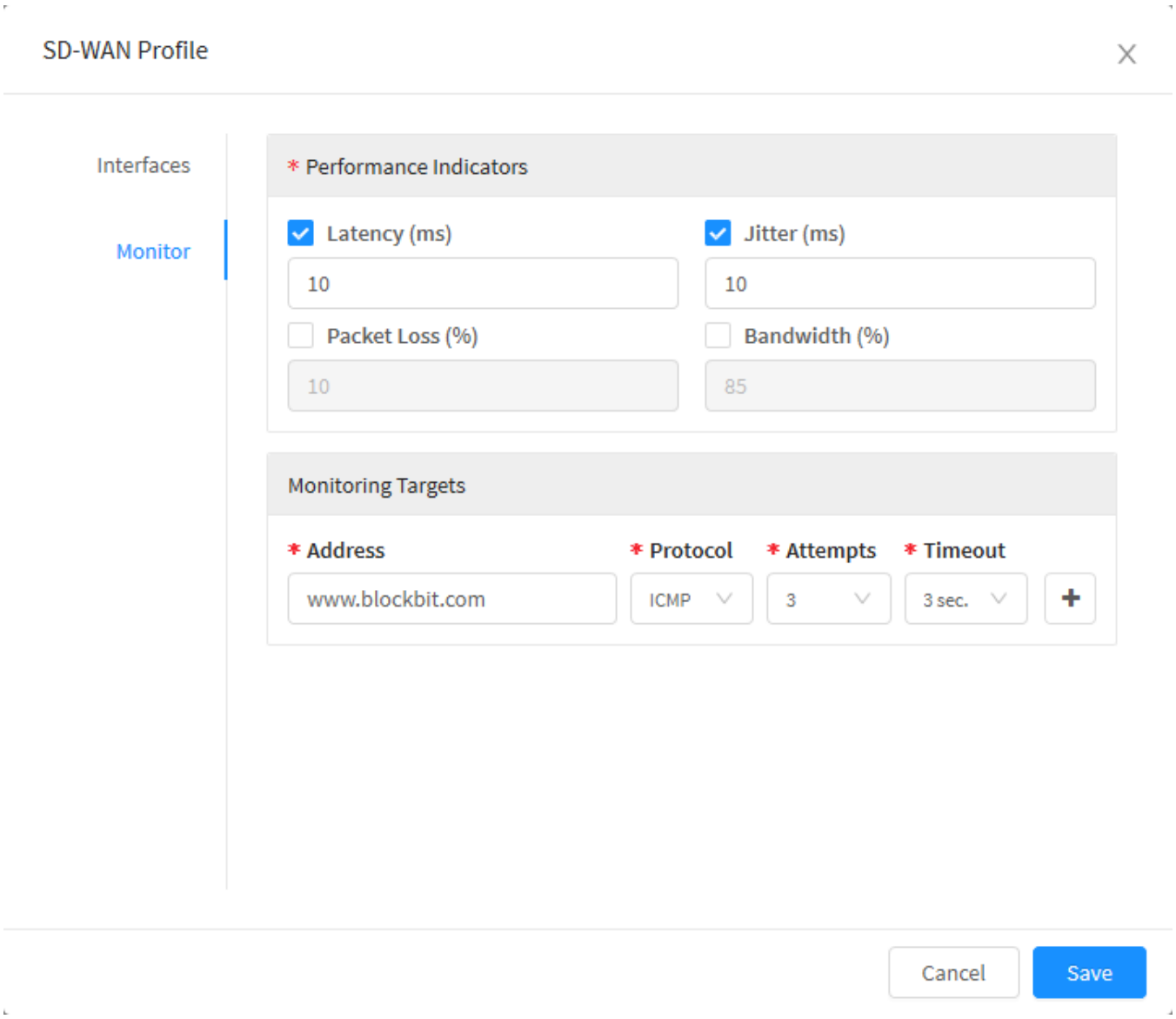
2. The following screen will be displayed:



SD-WAN – Failover - Interfaces

- ***Description*:** Set the name for the profile. Ex.: *Failover BB*;
- ***Type*:** Define the type that the profile will operate, which can be Failover, Load Balance, Spillover and Dynamic Selection. Ex.: *Failover*;
- ***Fail ratio* 1-100%:** Set the failure rate value between 1 to 100% so that the link is considered offline. Ex.: 70%;
- ***Monitoring interval* (*sec.*)[ ]:** Define the monitoring interval between each test. Ex.: 5 seconds;
- ***Failback*:** Defines the monitoring interval between each test. For more information see this page. Ex.: 5;
- ***Interfaces*:** Define the internet link interfaces that will be used in the composition of the profile. Ex.: eth1, eth2, eth3;

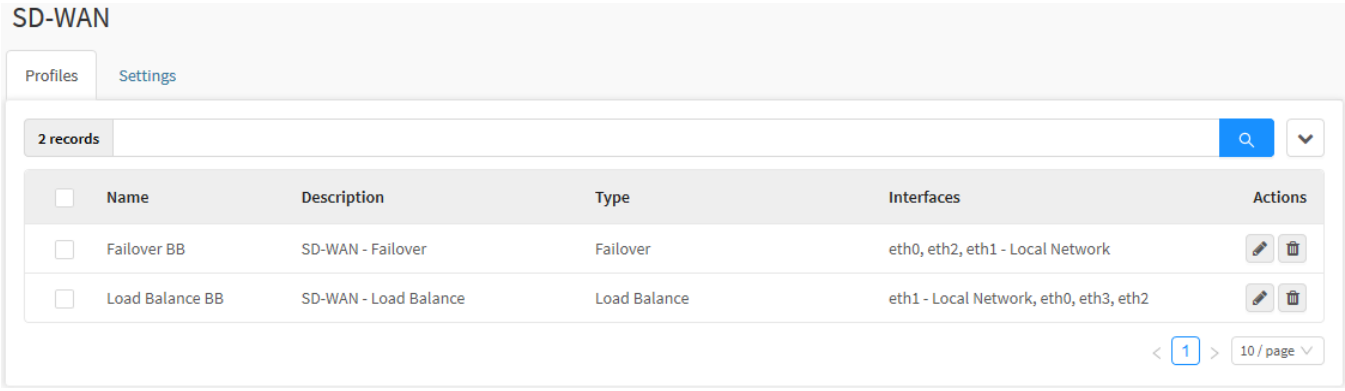
3. Access the "Monitor" tab:



SD-WAN – Failover - Monitor

4. Add the performance indicators and monitoring targets you want.

After all the fields are properly filled out, click on the [Save] button;

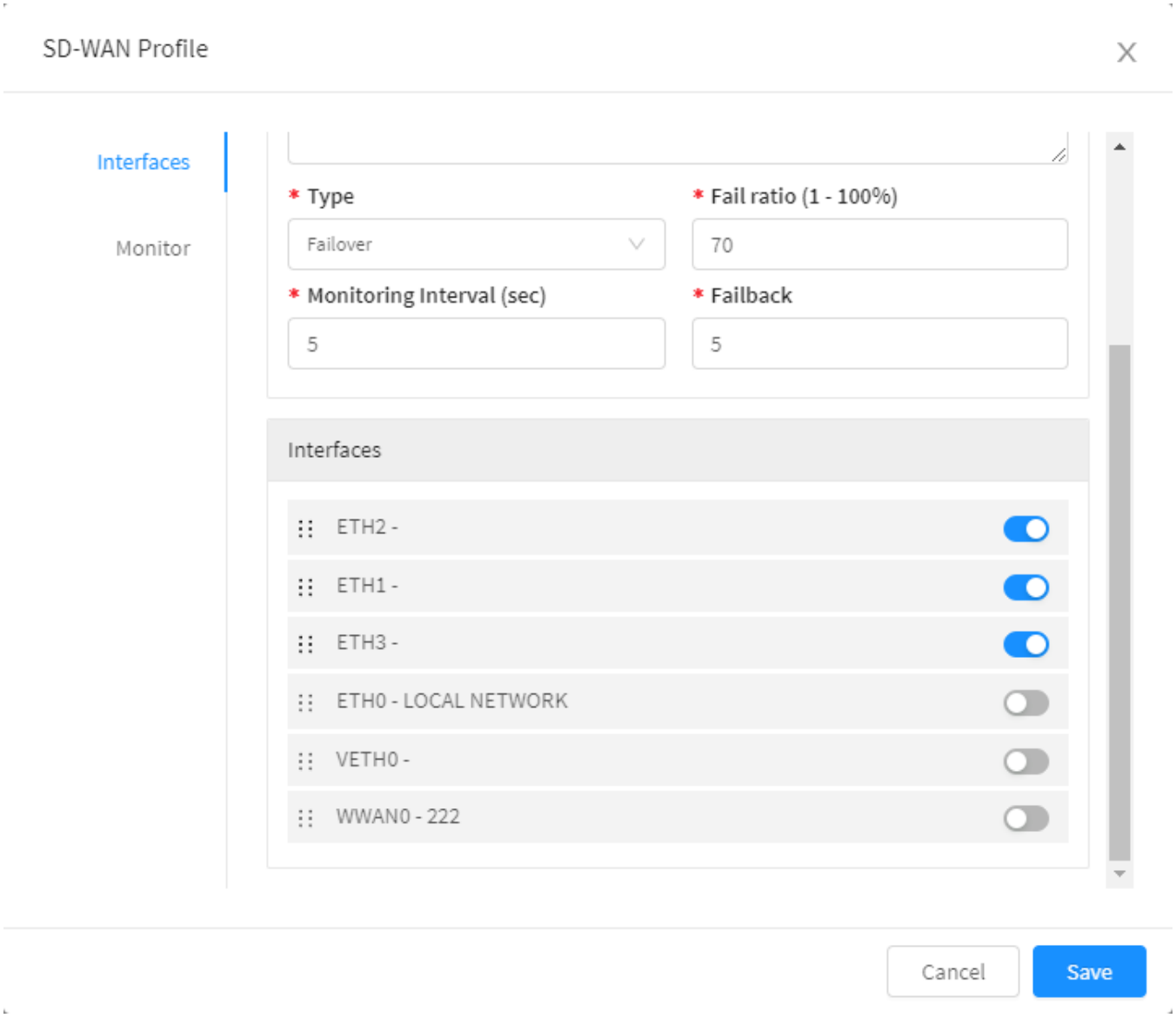


SD-WAN – Profiles

Finally, after saving, for the SD-WAN to take action it will be necessary to access the **command queue [ ]** and apply the changes made. For more information on the command queue, access the UTM - Command queue page.

After performing these procedures, the SD-WAN Failover will have been successfully configured.

When editing the registered profile it is possible to view the status of the link as shown on the screen below:



SD-WAN – Edit profile

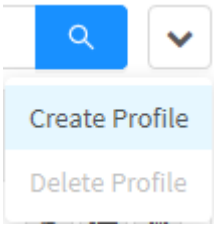
The system operaring in failover module will redirect the packets to the first online link on the list, it is possible to sort the links by clicking **[ ]** and dragging them to the desired position, so that the link which is on the first position from top to bottom will be the one used for outgoing traffic, if the link is offline the traffic will be automatically redirected to the next link on the list, thus ensuring high availability in internet access, when the link goes back online the system will automatically return the output to the first link from the list.

Notifications of “failures and link re-establishment”, and “automatic routing re-establishment” are triggered automatically in real time and can be viewed through the WEB interface by clicking on the *[ ]* icon or by e-mail.

SD-WAN - Spillover

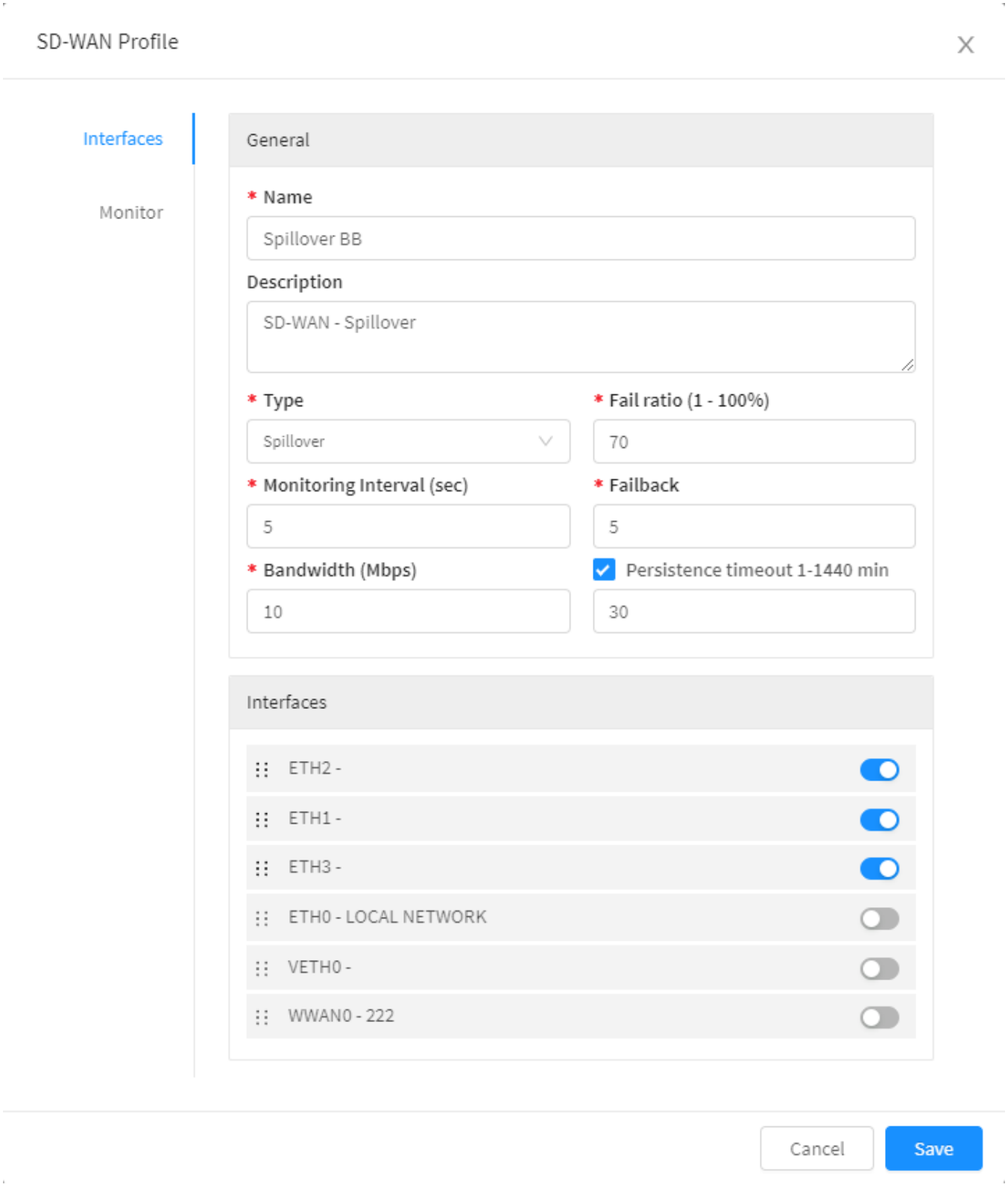
Spillover consists on a traffic overflow process based on the configured bandwidth limit. When the band exceeds the link bandwidth of the first interface configured with online status in the profile, new traffic flows are reallocated in a “Round Robin” way between the remaining enabled interfaces and with online status in the profile.

1. To access, click on the **Actions menu [**  **]** and select the option “Create Profile”;



SD-WAN - Create Profile

2. The screen below will be displayed:

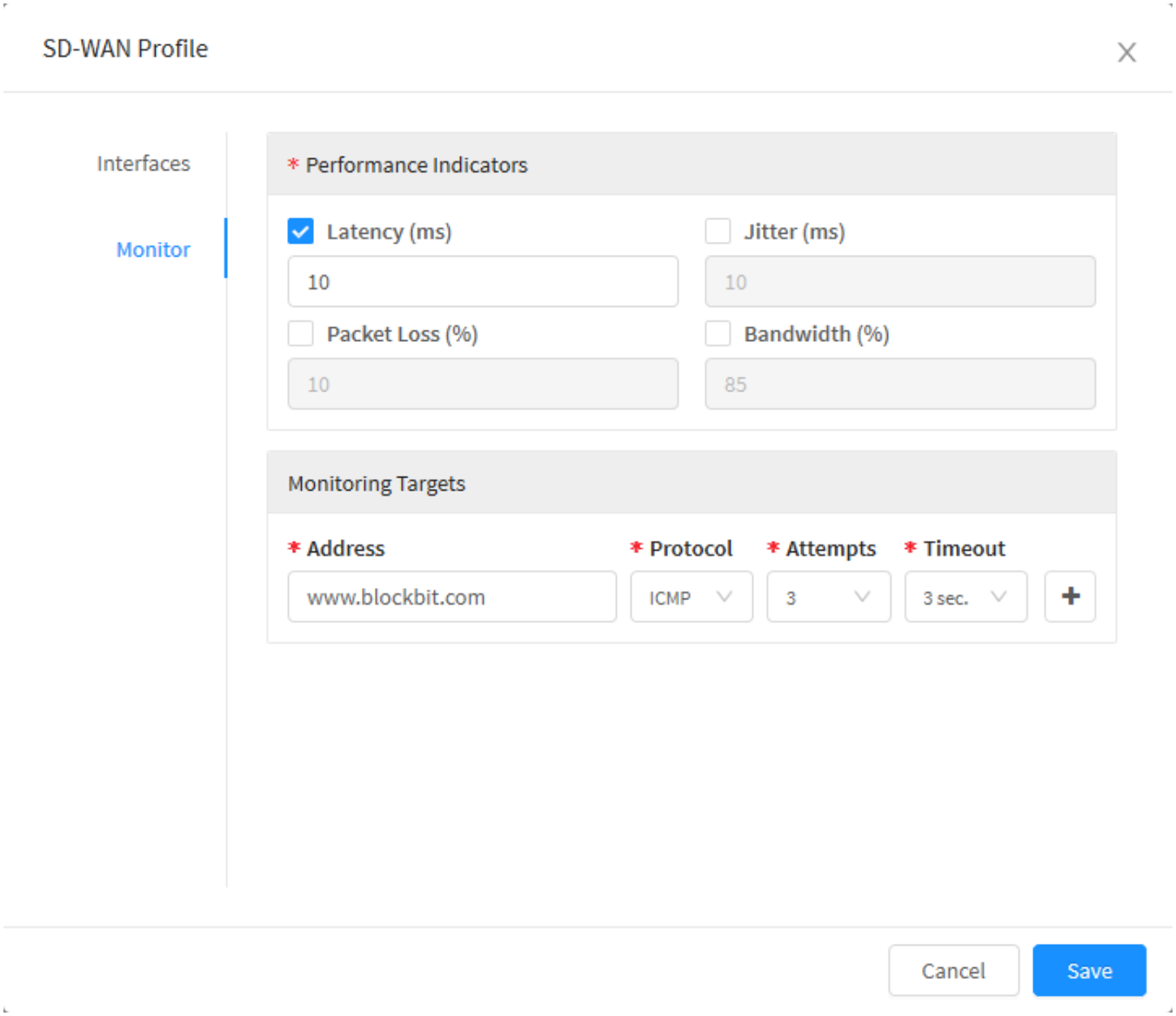


SD-WAN – Spillover - Interfaces

- ***Fail ratio* 1-100%:** Set the failure rate value between 1 to 100% to consider the link as offline. Ex.: 70%;
- ***Monitoring interval* (sec.):** Define the monitoring interval between each test. Ex.: 5 seconds;
- ***Failback*:** Defines the number of times an interface whose connectivity has failed will be tested to enable routing through it. For more information see this page. Ex.: 5;
- ***Bandwidth* (*Mbps*):** Defines the bandwidth limit, if this value is exceeded the traffic flow will be directed to the first interface with online status configured in the profile. Ex.: 150 mbs;

- ***Persistence timeout* 1-1440 *minutes* [ ]:** Defines the “persistence timeout” time to drop the connection in the event of an idle time. Ex.: 15 min.

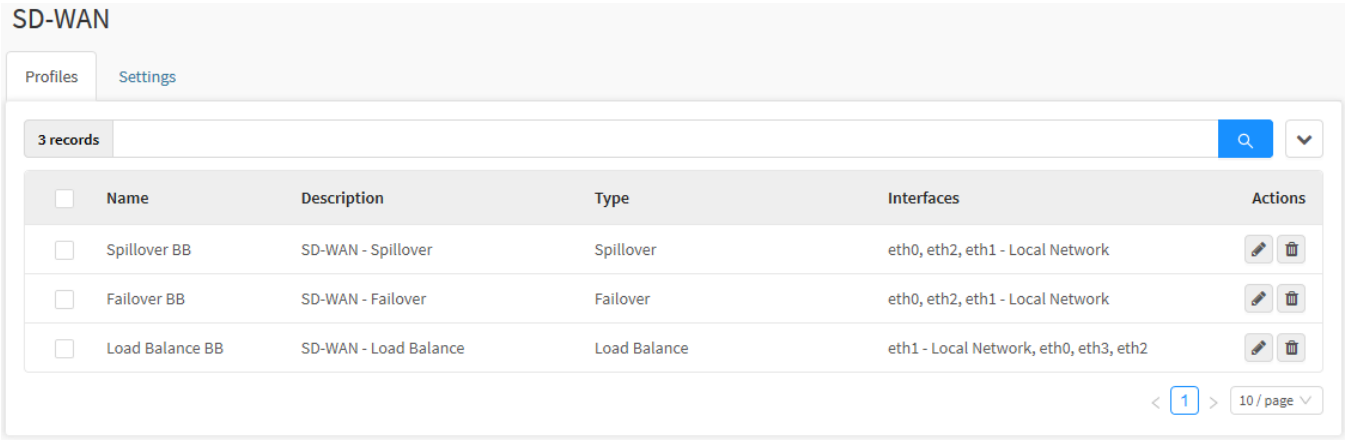
3. Access the "Monitor" tab:



SD-WAN – Spillover - Monitor

4. Add the performance indicators and monitoring targets you want.

After all the fields duly filled in, click on the [Save] button;

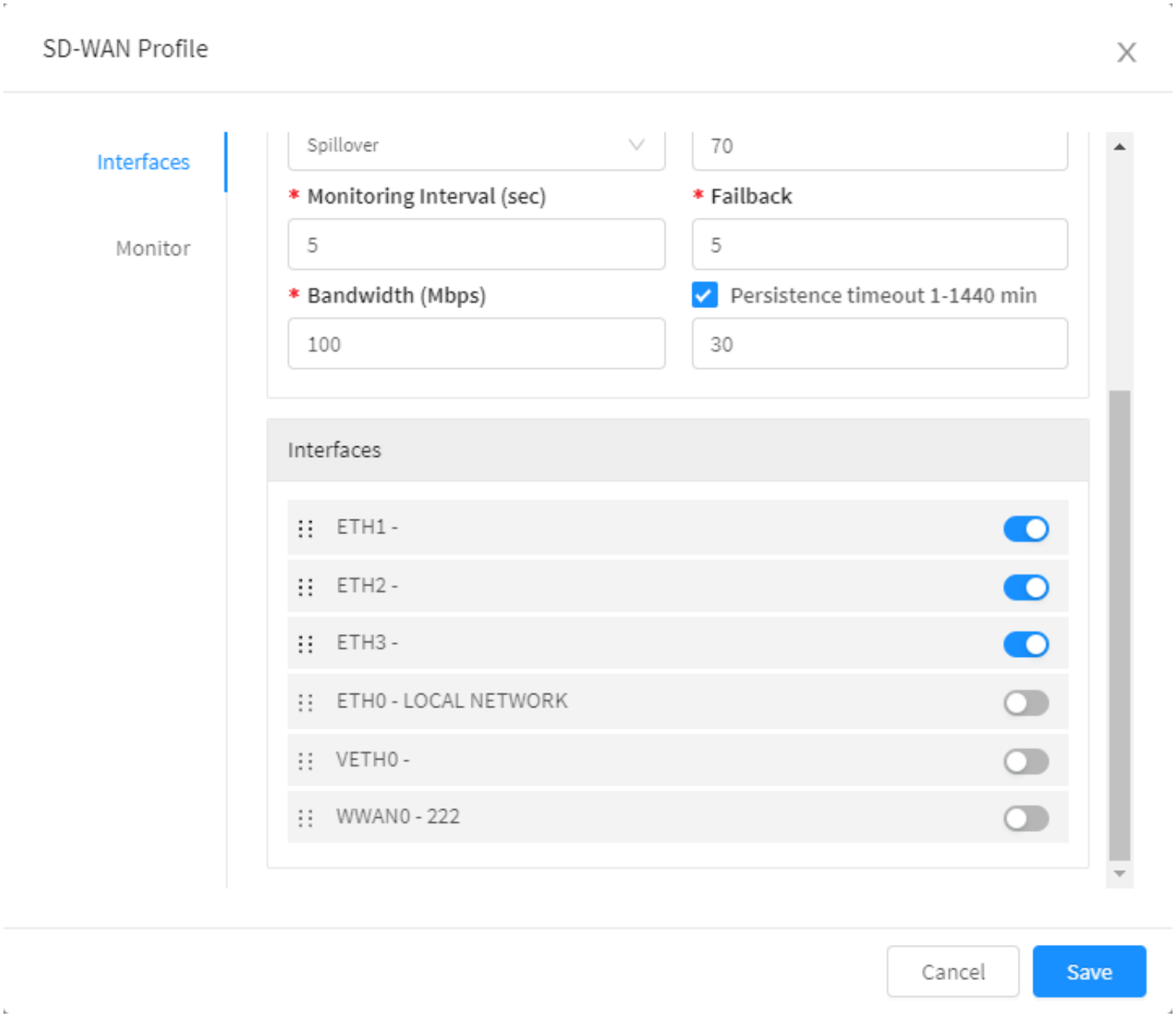


SD-WAN – Profiles

Finally, after saving, for the SD-WAN to take action it will be necessary to access the **command queue [ ]** and apply the changes done. For more information about the command queue visit the UTM - Command queue page.

After performing these procedures, the SD-WAN Spillover will have been successfully configured.

When editing the registered profile it is possible to view the status of the link according to the screen below.



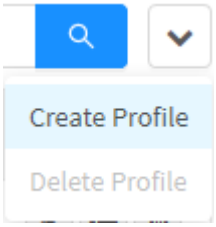
SD-WAN - Edit profile - Spillover Example

In the spillover process, the system directs the entire traffic flow to the first interface with online status configured in the profile, when the value exceeds the configured bandwidth, in our example above, it was configured with the bandwidth of 150 Mb/s (one hundred and fifty mega bits per second) the new traffic flows are reallocated in a “Round Robin” way between the remaining interfaces enabled and with online status in the profile.

SD-WAN - Dynamic Selection

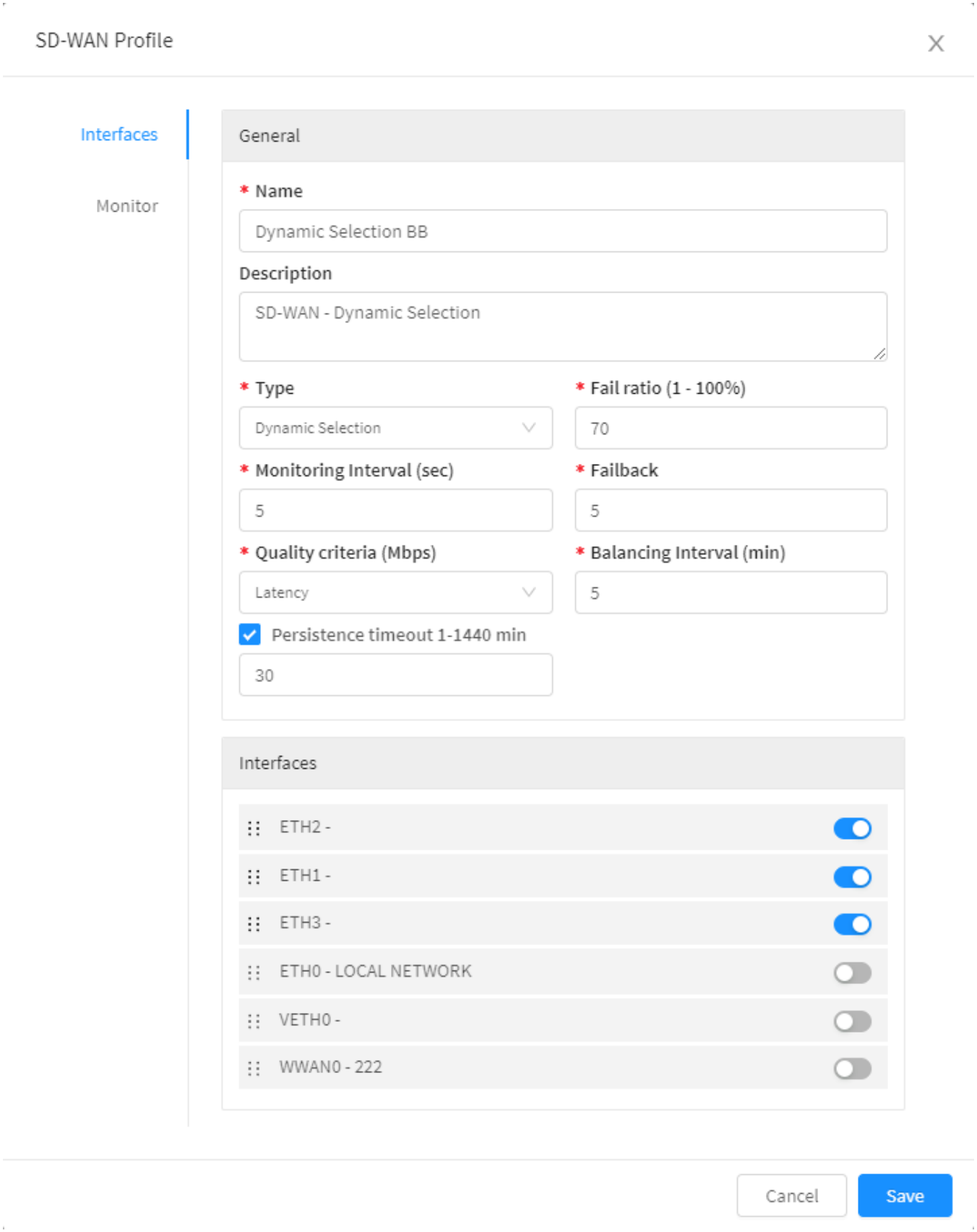
In Dynamic Selection, traffic is prioritized for the link that has the best result against the quality criterion, therefore, new flows will be assigned to it. Therefore, the system dynamically distributes the % among the links with the best performance based on the selected quality indicator.

1. To access, click on the **Actions menu [ ]** and select the “Create Profile” option;



SD-WAN - Create Profile

2. The screen below will be displayed:



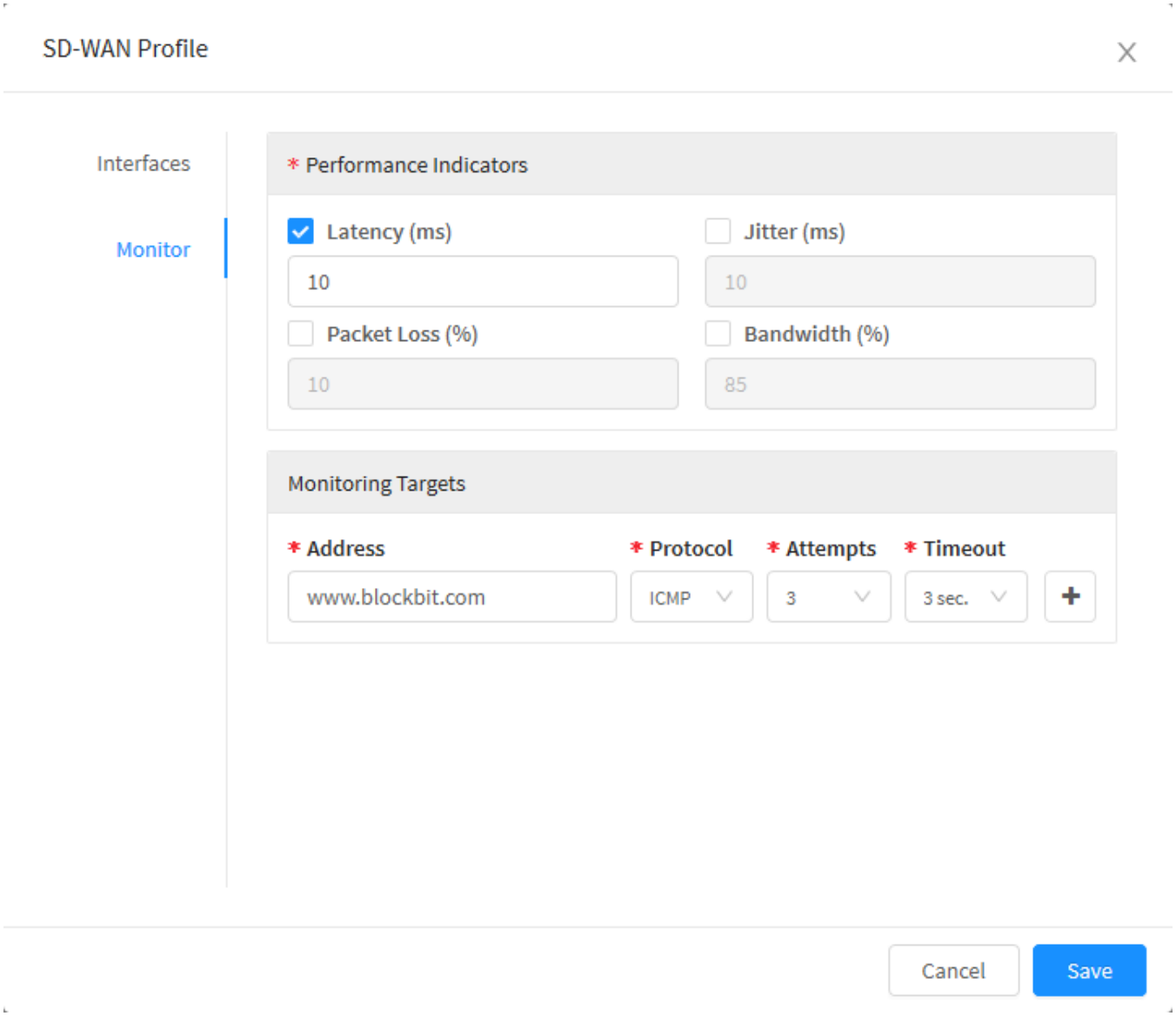
SD-WAN – Dynamic Selection – Interfaces

- ***Monitoring interval* (sec.):** Define the monitoring interval between each test. Ex.: 5 seconds;

When one of the links goes down, the monitoring interval is reset and it will only count again after the link goes up. *If the link drop occurs before the monitoring interval passes, the reports generated will always point the network percentages to 50 since the monitoring interval is being constantly reset by dynamic selection.*

- ***Fail ratio* 1-100%:** Set the failure rate value between 1 to 100% to consider the link as offline. Ex.: 70%;
- ***Monitoring interval* (min.):** Determines the period in which the value of the values will be calculated in %, based on the average of the quality criteria of the active links. Ex.:5;
- ***Failback*:** Defines the number of times an interface whose connectivity has failed will be tested to enable routing through it. For more information see this page. Ex.: 5;
- ***Quality criteria*:** Determines the performance indicator that will be used for dynamic link selection. Ex.: *Latency*;
- ***Persistent connection*:** To enable Link persistence, mark this checkbox. Ex.: *Enable*;
- ***Persistence timeout* 1-1440 *minutes*[ ]:** Set the failure rate value between 1 to 100% to consider the link as offline. Ex.: 70%.

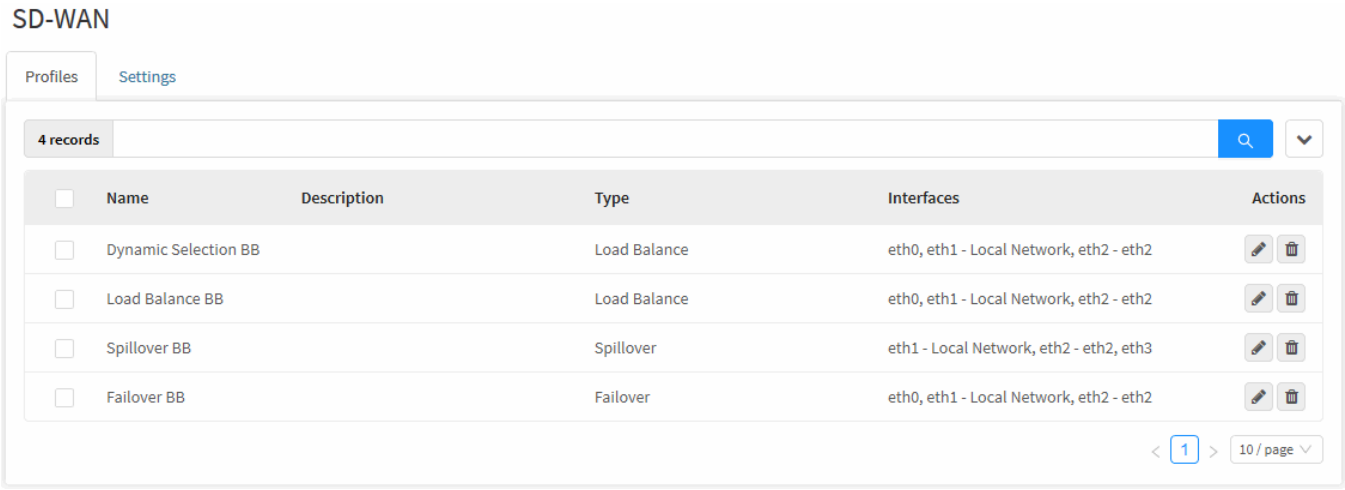
3. Access the "Monitor" tab:



SD-WAN – Dynamic Selection - Monitor

4. Add the performance indicators and monitoring targets that will be used.

After all the fields are duly filled out, click on the [Save] button.



SD-WAN – Profiles

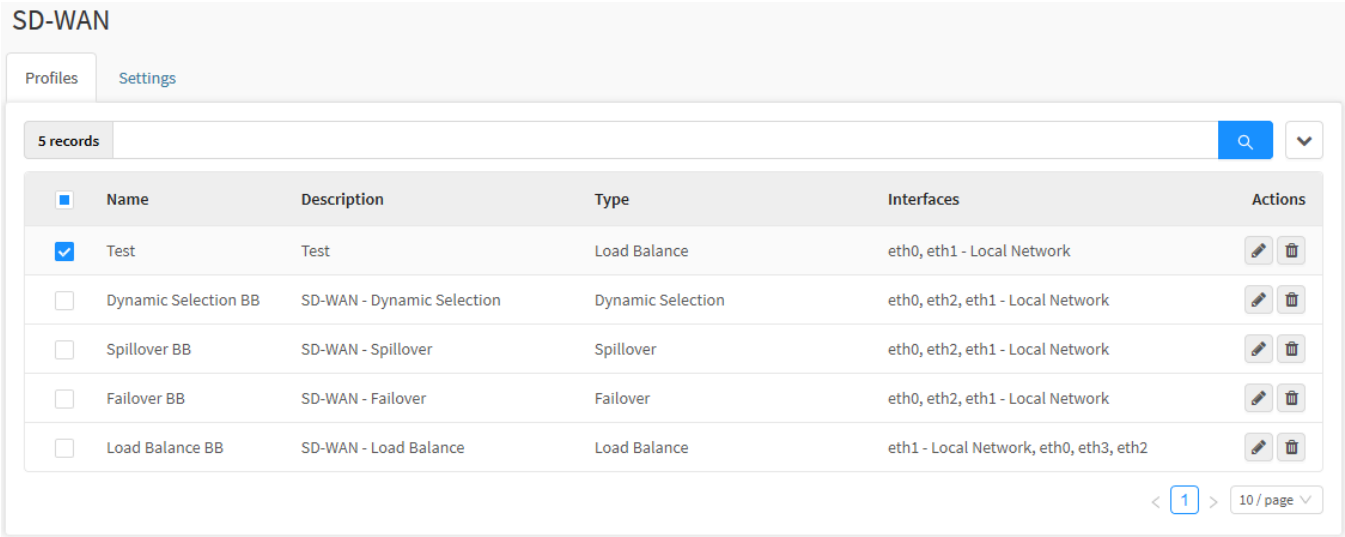
Finally, after saving, for the SD-WAN to take action it will be necessary to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the UTM - Command queue page.

After performing these procedures, the SD-WAN Dynamic Selection will have been successfully configured.

SD-WAN - Profiles - Actions Menu - Delete Profile

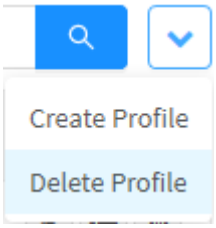
Through the “Delete Profile” button it is possible to erase the selected Profiles. To delete from the actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just check the checkbox located next to the Name. In the selected profiles, the checkbox will change from gray to blue [ ]. Example: Test:



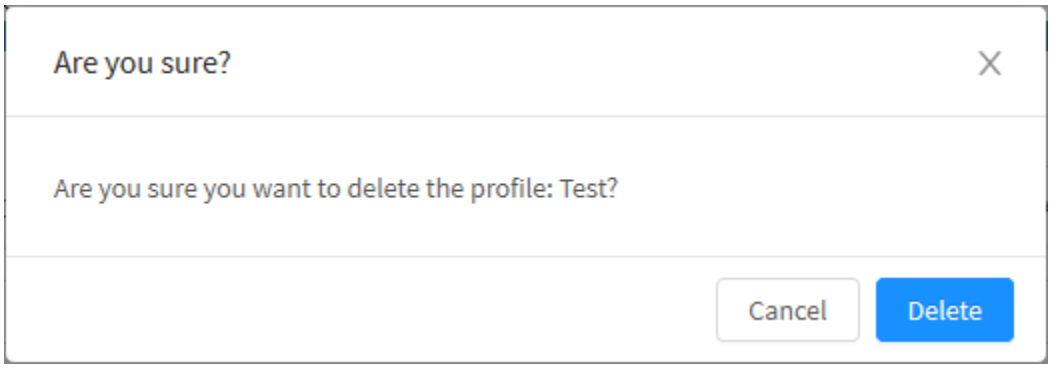
SD-WAN – Selection of Profiles to delete

2. Enter the Actions Menu and click on the “Delete Templates” option.



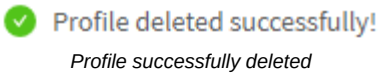
SD-WAN – Delete Profile.

3. The confirmation message will be displayed, to delete the selected profiles:



SD-WAN – Message if you want to delete the Profiles

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

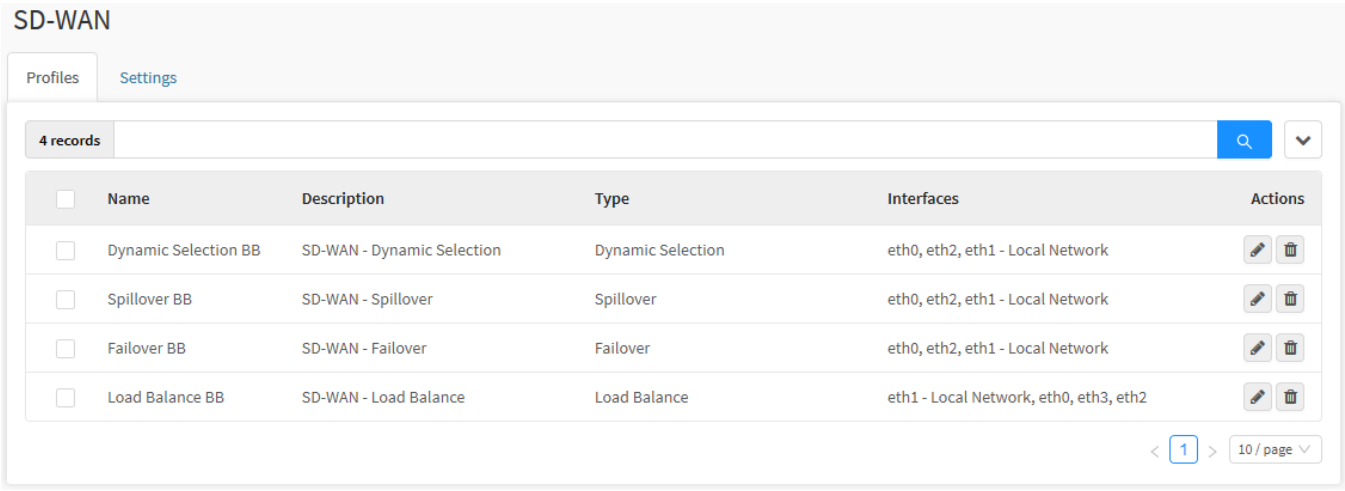


Profile successfully deleted

After performing these procedures, the profiles will have been successfully deleted.

SD-WAN - Profiles - Columns

Below, each column of the SD-WAN tab will be explained:

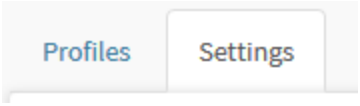


SD-WAN - Profiles

- **Checkbox[ ]:** Selects the profile.
- ***Name*:** Displays the name of the registered profile;
- ***Description*:** Displays the description of the registered profile;
- ***Type*:** Defines the type of SD-WAN. For more information check this page;
- ***Interfaces*:** Displays the interfaces that are affected by the current SD-WAN profile;
- ***Actions*:** The “Actions” column consists on several buttons:
  - ***Edit* [ ]:** Allows you to edit the profile settings added in the *Create Profile* option of the actions menu;
  - ***Delete* [ ]:** Deletes the profile, it is the equivalent of the *Delete Profile* option in the actions menu.

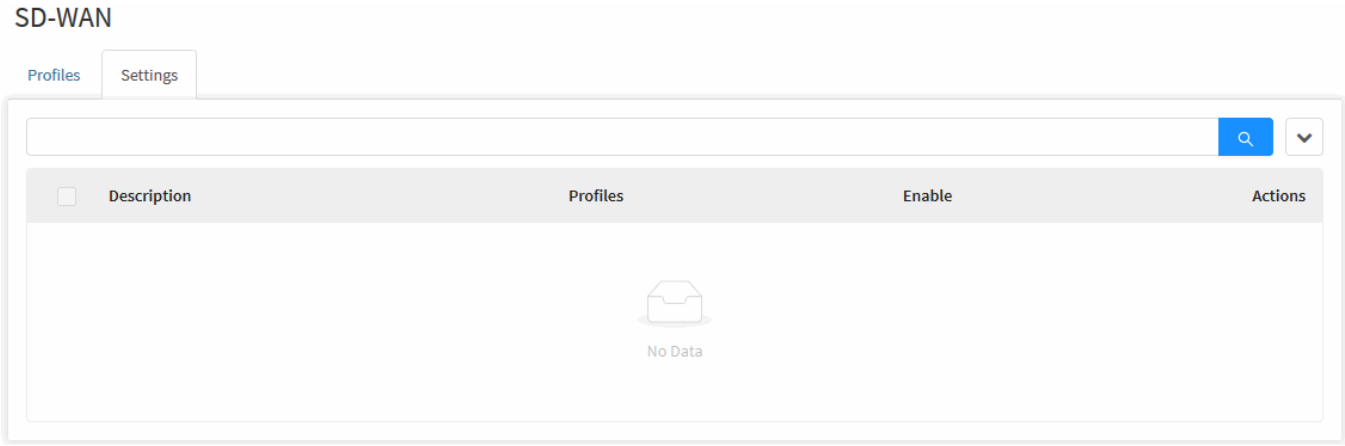
SD-WAN - Settings tab

In this tab it is possible to create and configure SD-WAN services, through this tab it is possible to configure the Firewall output for some services, without the necessity of creating a Policy. To do so, click on the "Settings" tab.



Settings tab

The following screen will be displayed:



SD-WAN - Settings

This session will cover how to register, edit and remove SD-WAN services;

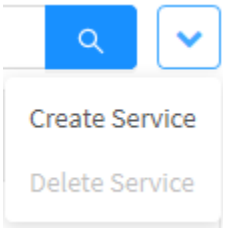
Next, we'll look at each function in this panel.

SD-WAN - Settings - Actions Menu

At the upper right of the screen is the actions menu:

SD-WAN – Settings - Actions Menu button

By clicking on this button the menu below is displayed:



SD-WAN - Settings – Actions Menu

The menu consists on the following options:

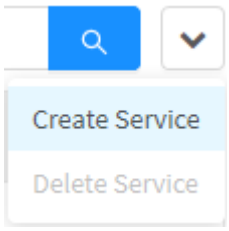
- *Create Service*;
- *Delete Service*.

Next, each action menu option will be detailed.

SD-WAN - Settings - Actions Menu - Create Service

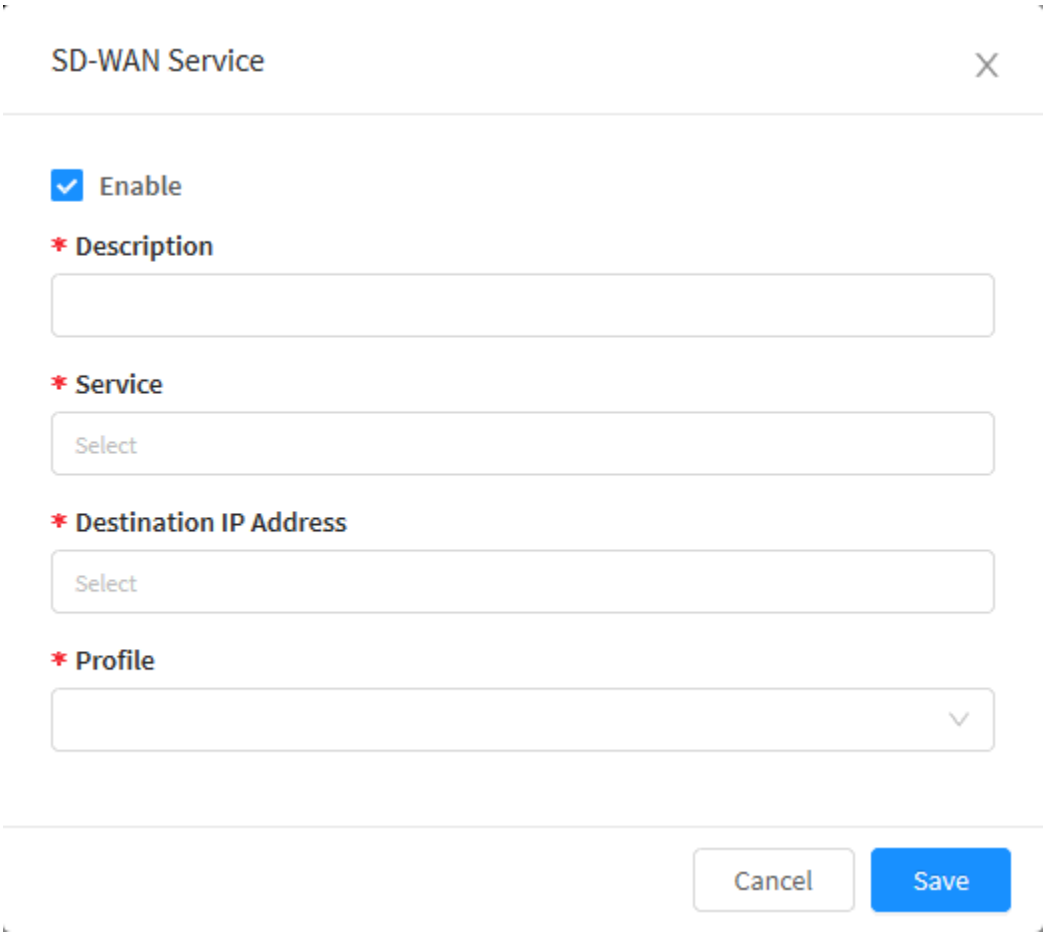
Through the option “Create Service” it is possible to create a new SD-WAN service. To access, click on the **Actions menu [ ]**.

1. Click on the “Create Service” option;



SD-WAN - Create Service

2. The screen shown below will be displayed:

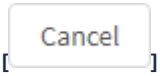


SD-WAN - Service

Next we will demonstrate how to configure this panel.

- **[ ]*Enable*:** By selecting this check box, the service will be enabled;

- ***Description*:** In this field the service description is defined. It will be used for identification in the columns. Ex.: SD-WAN Service;
- ***Service*:** In this field, add the service objects that will be used by the SD-WAN. For more information on how to create a service object, check this page. Ex.: AH, Administration;
- ***Destination IP Address*:** In this field, address objects are added that are used as the destination IP address. For more information on how to create an address object, check this page. Ex.: Class A Network, Class B Network, Class C Network, 192.168.254.13;
- ***Profile*:** Finally, the SD-WAN profile that will be used in the service is added. The objects that are added in this field are added in the Profiles tab, for more information, check this page. Ex.: Proxy Balance.

To cancel click the **[** 

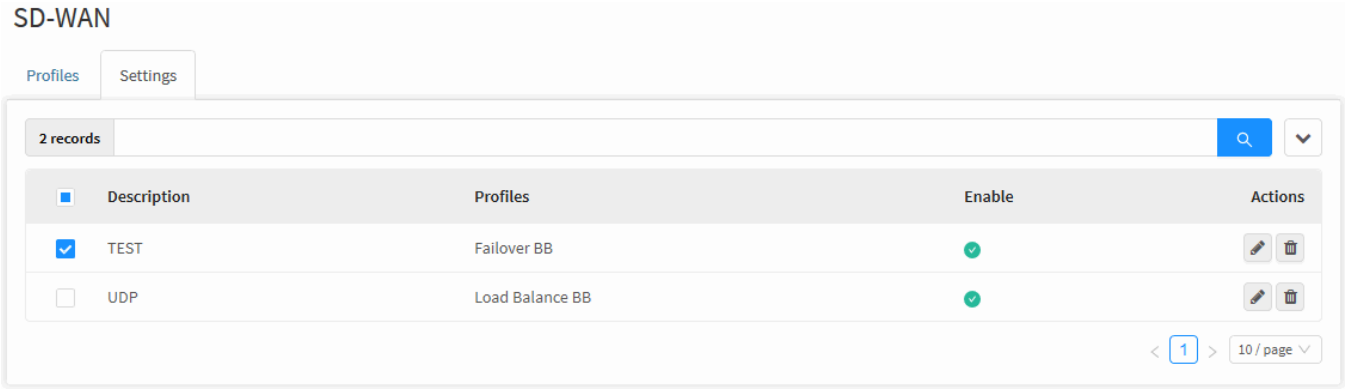
] button. To finish editing the applications, click the **[** 

] button.

SD-WAN - Settings - Actions Menu - Delete Service

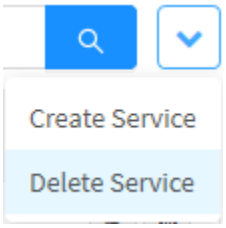
Through the “Delete Service” button it is possible to delete selected Services. To delete from the actions menu, follow these steps:

1. Select which Service(s) you want to delete. To select, just check the checkbox located next to the name. On the selected services, the checkbox will change from gray to blue [ ]. Ex.: Test;



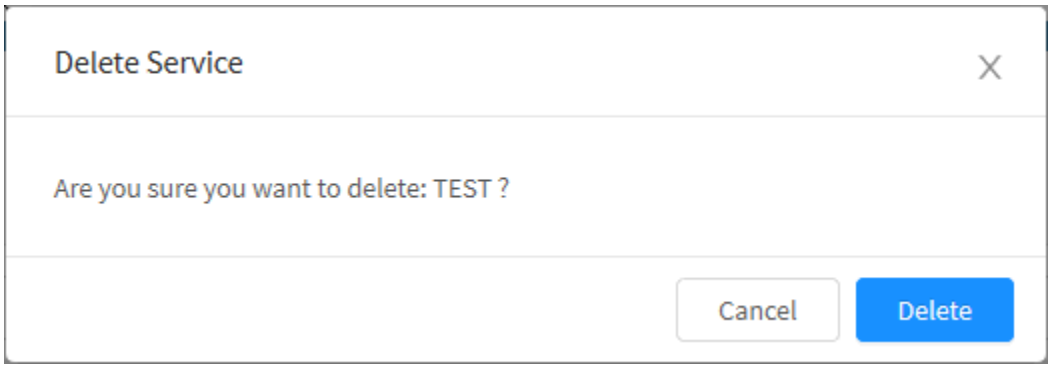
SD-WAN – Selection of Services to delete

2. Enter the Actions Menu and click the “Delete Service” option.



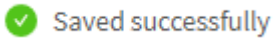
SD-WAN – Delete Service

3. The confirmation message will appear to delete the selected profiles:



SD-WAN – Service Deletion Confirmation Message

If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

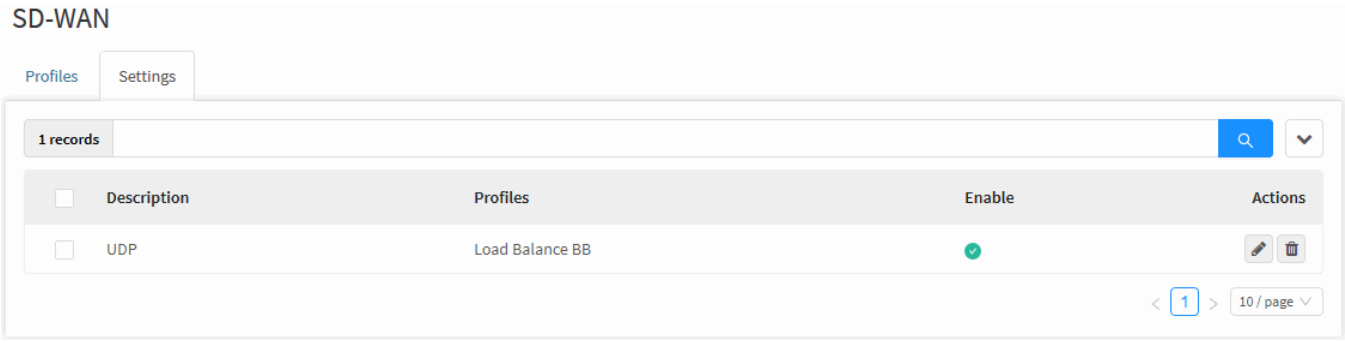


Successfully Saved

After performing these procedures, the services will have been successfully deleted.

SD-WAN - Settings - Columns

Next we will explain each column of the Settings tab:



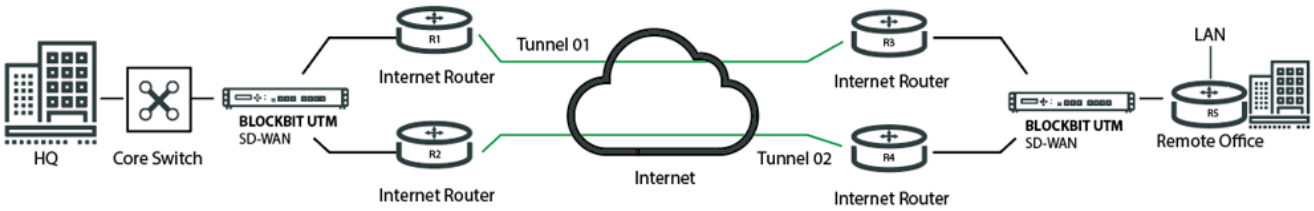
SD-WAN - Settings - Columns

Next, we will explain each column:

- **Checkbox[ ]:** Allows the selection of profiles.
- ***Description*:** Displays the description of the profile registered in the *Create Service* option of the actions menu;
- ***Profiles*:** Displays the description of the profile registered in the *Create Service* option of the actions menu;
- ***Enable*:** Displays the current state, which may be enabled or disabled;
- ***Actions*:** The “Actions” column is made up of two buttons:
  - ***Edit* [ ]:** Allows you to edit the settings of the service added in the *Create Service* option of the actions menu;
  - ***Delete* [ ]:** Deletes the service, it is the equivalent of the *Delete Service* option in the actions menu.

SD-WAN - Example: SD-WAN Configuration

This section will present a guide on how to configure an SD-WAN. This demonstration will take into account the following structure:



SD-WAN

In this structure, two organizational units will be interconnected with multiple links connected through the Internet. The following IPs will be used in this example:

Name	LAN IP address	Administration IP Address	Internet IP address	Virtual IP Address (TUN)
UTM - *HQ*	172.18.0.0/16	172.31.208.40	10.0.0.2	20.0.0.1
			11.0.0.2	21.0.0.1
UTM - *Remote Office*	172.17.0.0/16	172.31.208.41	100.0.0.2	20.0.0.2
			101.0.0.2	21.0.0.2

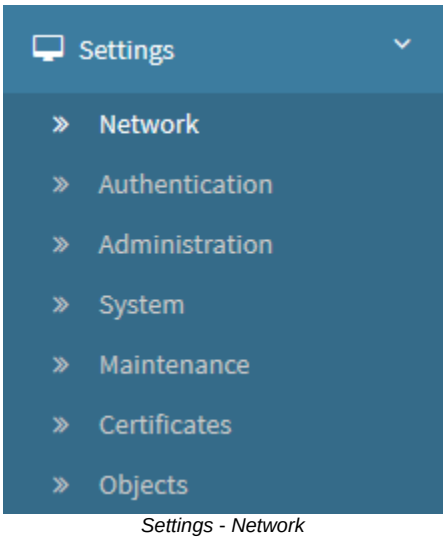
SD-WAN - IP Addressing

The next steps are:

1. ***Configure the Tunnel interfaces:*** In this step, point-to-point encapsulation will be made possible through the creation of Tunnel interfaces, these will be used by the VPN. For more information check the Network Interfaces chapter;
2. ***Configure the VPN:*** In this step, the private tunnel between two networks will be established, allowing them to be interconnected and communication to be carried out in encrypted form. For more information check the IPSEC VPN chapter;
3. ***Configure the SD-WAN:*** The focus of this phase is to effectively configure the SD-WAN, which allows the segmentation of traffic from network interfaces and monitoring through performance indicators;
4. ***Configure the Policies:*** In this step, a Policy will be created to release access, in order to make communication via VPN with SD-WAN viable, for more information check the *Policy* chapter;
5. ***Validation of the SD-WAN Configuration:*** Finally, some tests will be performed to validate if all configurations were created successfully

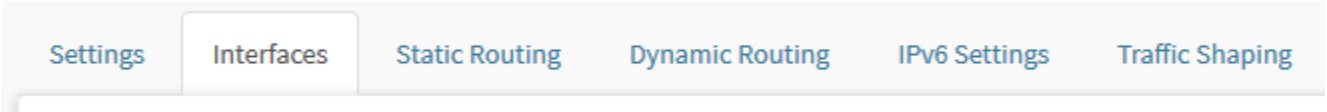
SD-WAN: Configure Tunnel Interface

Initially, access the Settings menu from the Network tab:



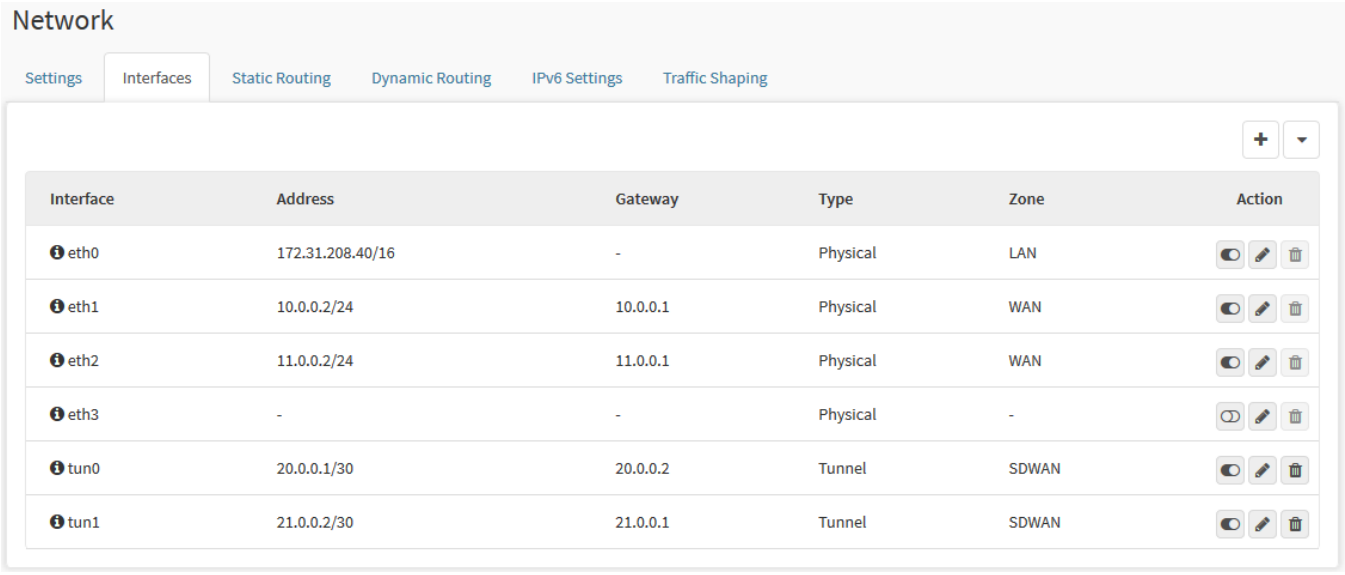
Settings - Network

Finally, click on the Interfaces tab:



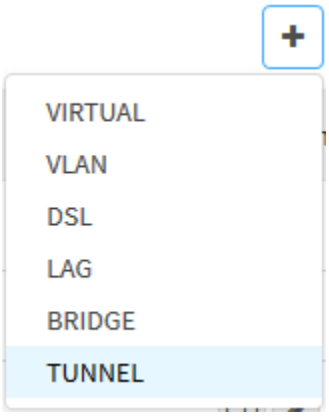
Aba *Interfaces*

Below are the NGFW- HQ settings:



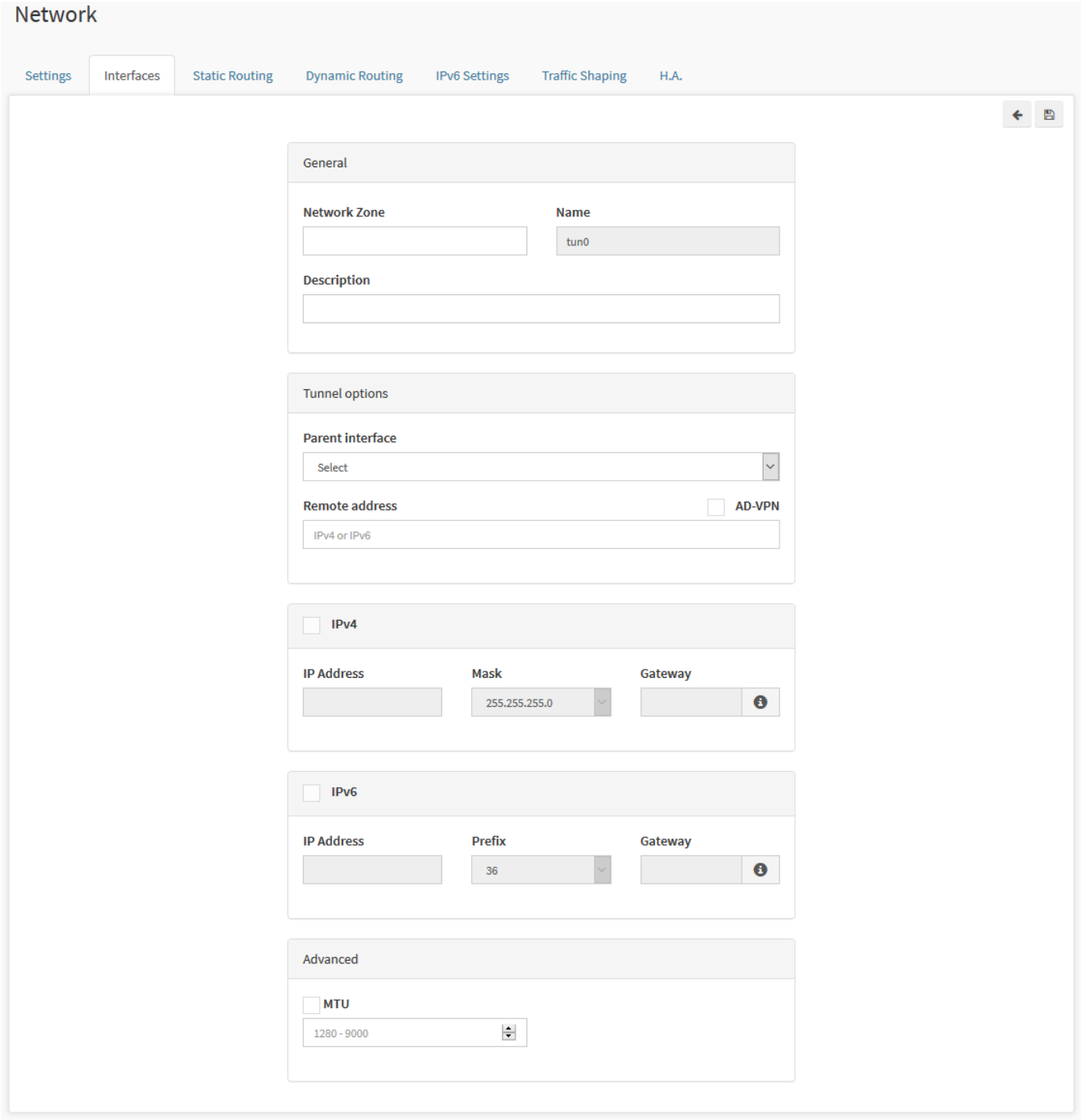
Network - Interfaces

To create TUNNEL interfaces, click Add [ ] and select the TUNNEL option.



Interfaces - Add Tunnel

The following screen will appear:

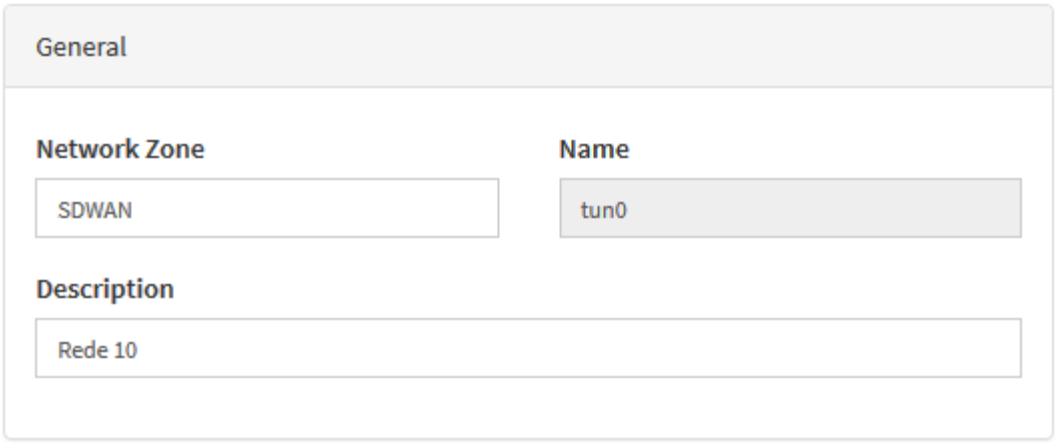


Interfaces – Network

Next we will analyze each component of the panel and point out the specific steps for configuring the SD-WAN, for more in-depth information on this topic, see this chapter.

General Panel

Complete the form as shown below:



Interfaces - General Panel

- ***Network Zone*:** In this field, it is recommended to isolate the traffic segment from the tunnels involved, so as not to have conflicts with security policies that involve other network zones, such as LAN and WAN. So, simply use “SDWAN”;
- ***Description*:** Insert the desired description in order to facilitate the identification of the tunnel interface later.

Tunnel Options

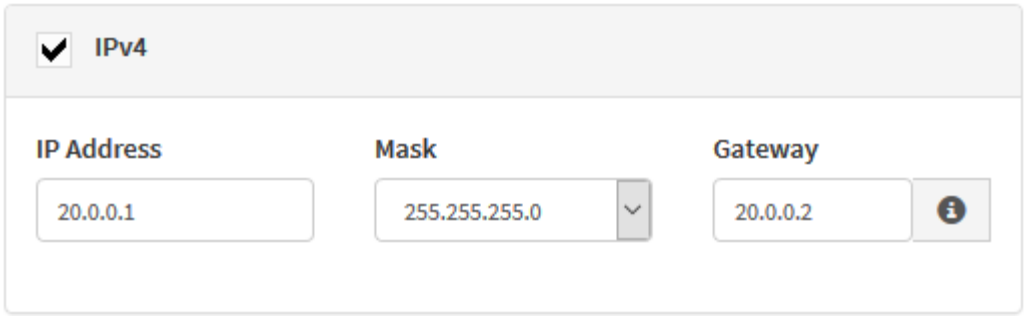
Complete the form as shown below:

Interfaces – Tunnel Options

- ***Parent interface*:** Determine the interface that will be used to establish the tunnel. Eg: eth1;
- ***Remote address***: In this field it is important that the real IP to be used is entered. Eg 100.0.0.2 (Remote BLOCKBIT Internet IP Address);

IPv4

Complete the form as shown below:



Interfaces – IPv4

- ***IP Address*:** Determines the IP that will be used by the tunnel. In this field the address used is the virtual IP. Ex .: 20.0.0.1;
- ***Mask***: The mask in this field can be the default. Ex .: 255.255.255.252;
- ***Gateway***: The gateway used in this field can be the address of the Tunnel interface of the Remote UTM. Ex.: 20.0.0.2;

The other options can be left as they are by default.

Click the **[** **]** button to save the settings done.

After these steps, we will have arrived at the result shown by the image below:

General

Network Zone

SDWAN

Name

tun0

Description

Network 10

Tunnel options

Parent interface

eth1

Remote address

100.0.0.2

AD-VPN

IPv4

IP Address

20.0.0.1

Mask

255.255.255.252

Gateway

20.0.0.2

IPv6

IP Address

Prefix

36

Gateway

Advanced

MTU

1280 - 9000

Interfaces – Tun0 settings

Repeat these steps to create all the necessary interfaces for each link.

In our environment, as we have 2 links and we must create 2 tunnels, we will create one more TUN, with the following settings:

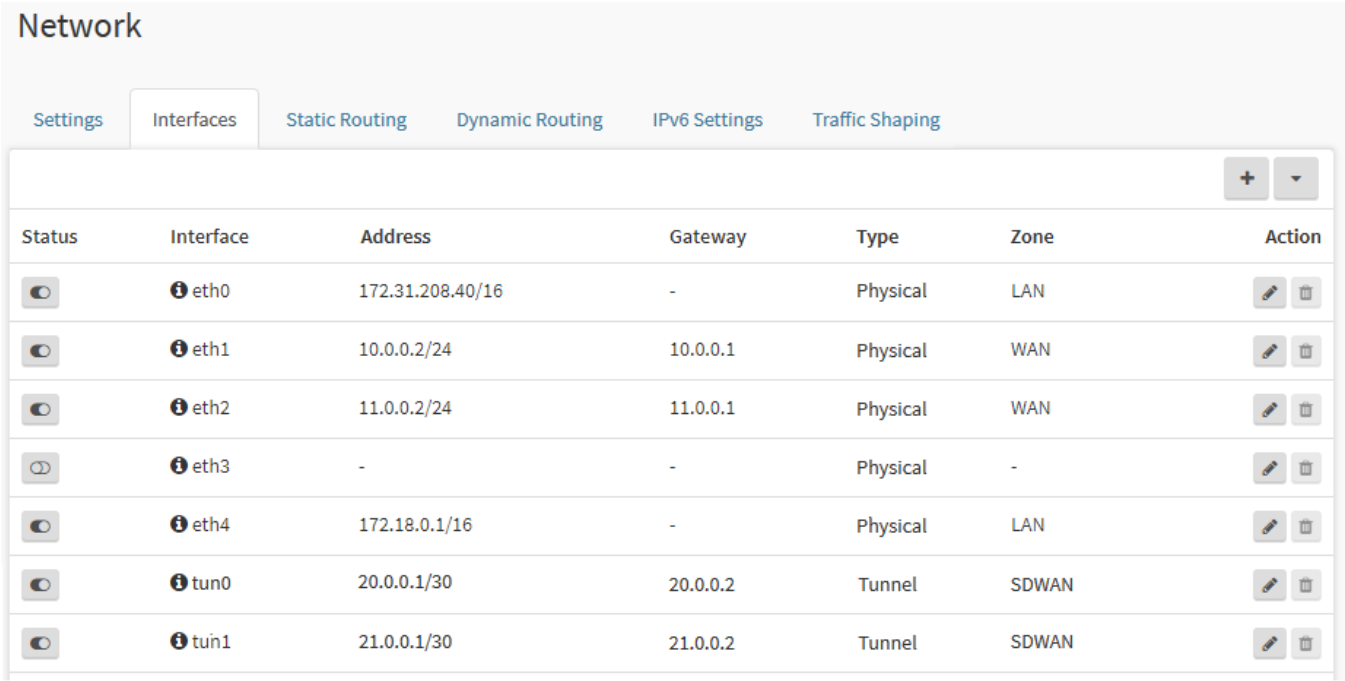
Tunnel Options

- ***Parent interface*:** Determine the interface that will be used to establish the tunnel. Ex.: eth2;
- ***Remote address***: In this field it is important that the real IP to be used is entered. Ex .: 101.0.0.2 (Internet IP address of the Remote NGFW).

IPv4

- ***IP Address*:** Determines the IP that will be used by the tunnel. In this field the address used is the virtual IP. Ex.: 21.0.0.1;
- ***Mask***: The mask in this field can be the default. Ex.: 255.255.255.252;
- ***Gateway***: The gateway used in this field can be the address of the Tunnel interface of the Remote NGFW. Ex.: 21.0.0.2;

Follow the final configurations shown in the image below:



Interfaces – Network Settings

These are the settings for the NGFW tun0 interface - Remote Office:

General

Network Zone

SDWAN

Name

tun0

Description

Network 100

Opções do túnel

Parent interface

eth1

Remote address

100.0.0.2

AD-VPN

IPv4

IP Address

20.0.0.2

Mask

255.255.255.252

Gateway

20.0.0.1

IPv6

IP Address

Prefix

Gateway

Advanced

MTU

Interfaces – Remote Office - Tun0 settings

The tun1 settings of the NGFW - Remote Office should be as shown on the image below:

General

Network Zone

SDWAN

Name

tun0

Description

Network 101

Opções do túnel

Parent interface

eth2

Remote address

11.0.0.2

AD-VPN

IPv4

IP Address

21.0.0.2

Mask

255.255.255.252

Gateway

21.0.0.1

IPv6

IP Address

Prefix

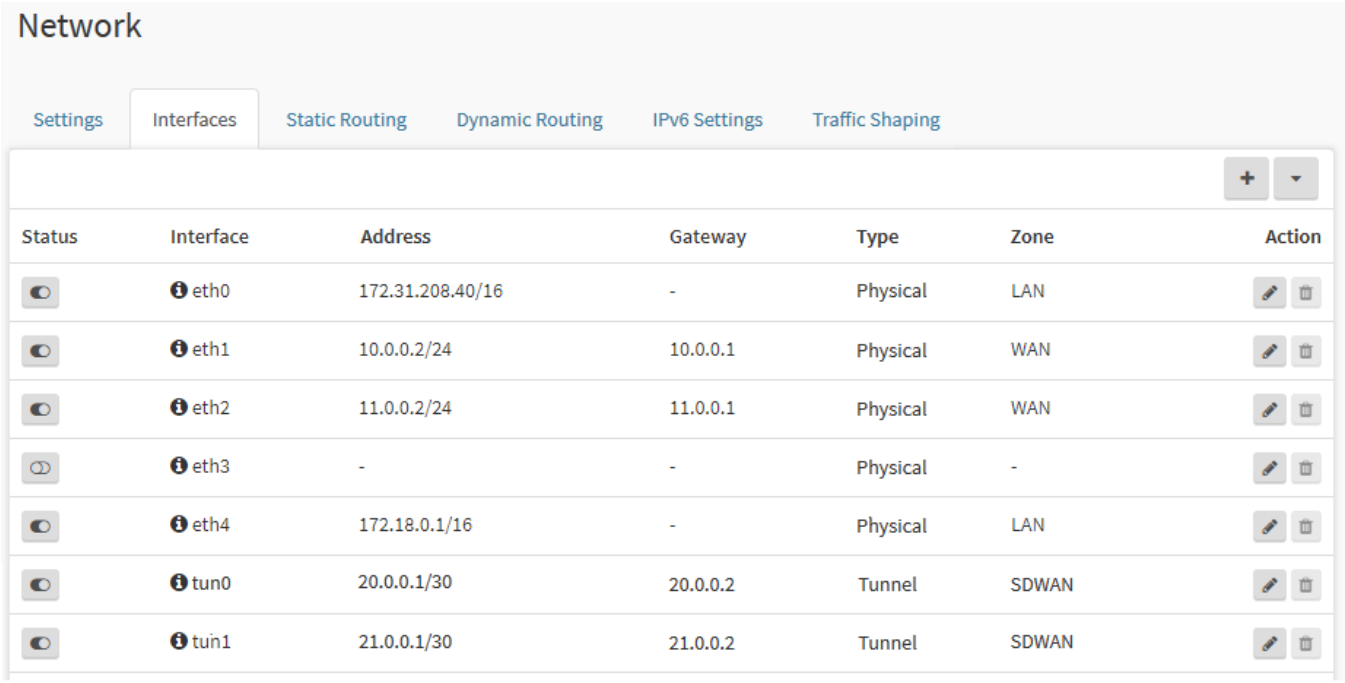
Gateway

Advanced

MTU

Interfaces – Remote Office - Tun1 settings

Final settings:



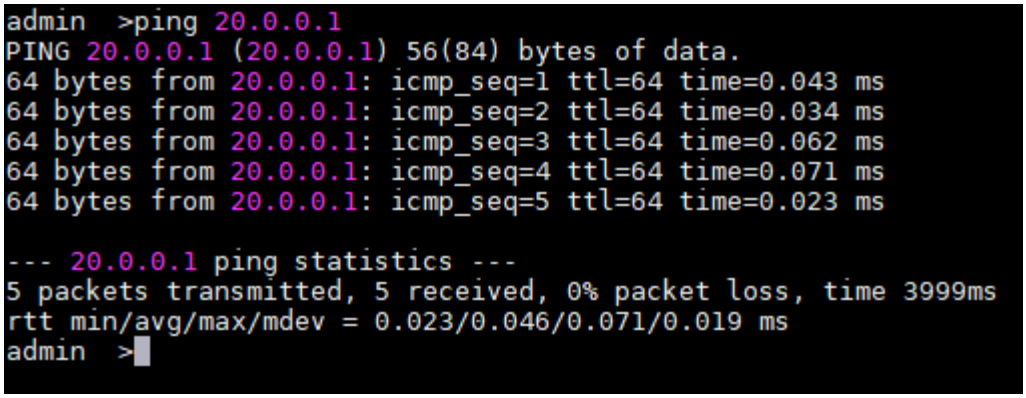
Interfaces – Remote Office - Network Settings

To test the communication between the two interfaces created, access them both by NGFWs via SSH. Using the “ifconfig” command, it will be possible to view the two active tunnel interfaces, as shown on the image below.

```
admin  >ifconfig
dummy1: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 2000
        inet 10.208.40.1  netmask 255.255.255.0  broadcast 10.208.40.255
        ether 4a:6e:3b:0d:66:c3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 172.31.208.40  netmask 255.255.0.0  broadcast 172.31.255.255
        ether 00:0c:29:5d:0e:f1  txqueuelen 10000  (Ethernet)
        RX packets 2525656  bytes 476989639 (454.8 MiB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 570488  bytes 303023442 (288.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.2  netmask 255.255.255.0  broadcast 10.0.0.255
        ether 00:0c:29:5d:0e:19  txqueuelen 10000  (Ethernet)
        RX packets 556507513  bytes 814559914114 (758.6 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 67537448  bytes 9768142420 (9.0 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 11.0.0.2  netmask 255.255.255.0  broadcast 11.0.0.255
        ether 00:0c:29:5d:0e:fb  txqueuelen 10000  (Ethernet)
        RX packets 516846708  bytes 734230151019 (683.8 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50996999  bytes 5733000108 (5.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:5d:0e:05  txqueuelen 10000  (Ethernet)
        RX packets 2  bytes 120 (120.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 00:0c:29:5d:0e:0f  txqueuelen 10000  (Ethernet)
        RX packets 138425908  bytes 9444283493 (8.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 725340609  bytes 1823508535280 (1.6 TiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1  (Local Loopback)
        RX packets 396043765  bytes 80713689468 (75.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 396043765  bytes 80713689468 (75.1 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 20.0.0.1  netmask 255.255.255.252  destination 20.0.0.1
        unspec 0A-00-00-02-00-00-60-B0-00-00-00-00-00-00-00-00  txqueuelen 10000  (UNSPEC)
        RX packets 139205  bytes 3898132 (3.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 139175  bytes 3897292 (3.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 21.0.0.1  netmask 255.255.255.252  destination 21.0.0.1
        unspec 0B-00-00-02-00-00-60-B0-00-00-00-00-00-00-00-00  txqueuelen 10000  (UNSPEC)
        RX packets 139192  bytes 3897600 (3.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 139154  bytes 3896536 (3.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

admin  >
```

CLI - ifconfig

In addition, it is possible to use the "ping" command to try to communicate with these interfaces, if a response is received, it indicates that the establishment of communication was successful.



CLI - ping

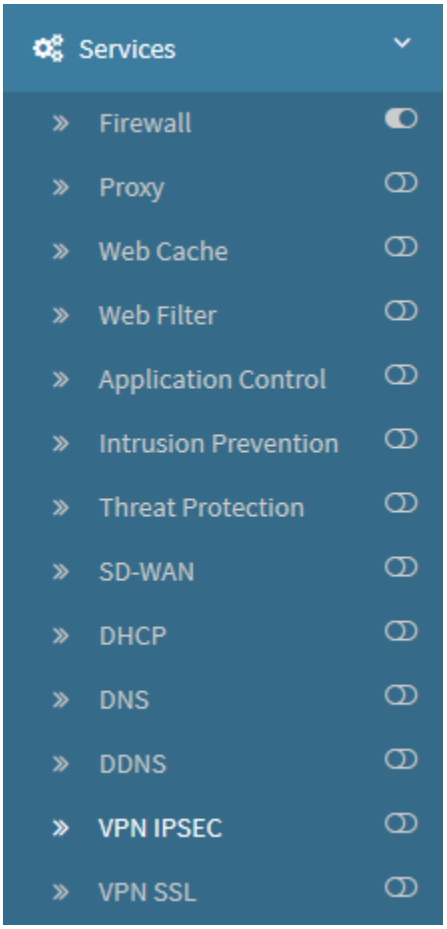
For more information, see the chapter on *CLI*.

Next, we will configure the VPNs.

SD-WAN: Configure VPN

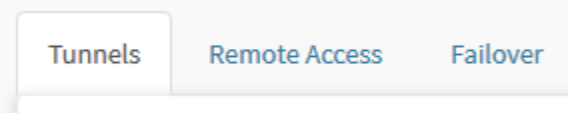
After configuring the *tunnel* interfaces, follow the steps below:

Initially, go to **Services** and click on the **IPSEC VPN** option:



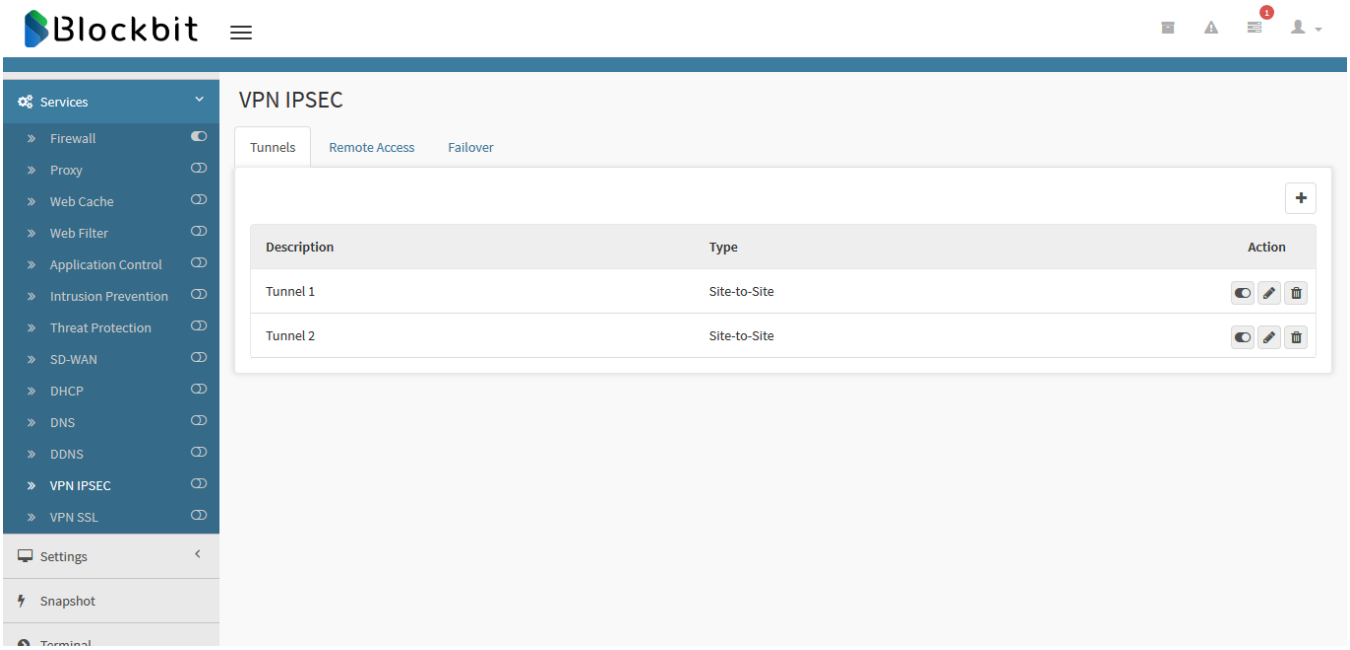
Services - IPSEC *VPN*

Once this is done, select the Tunnels tab:



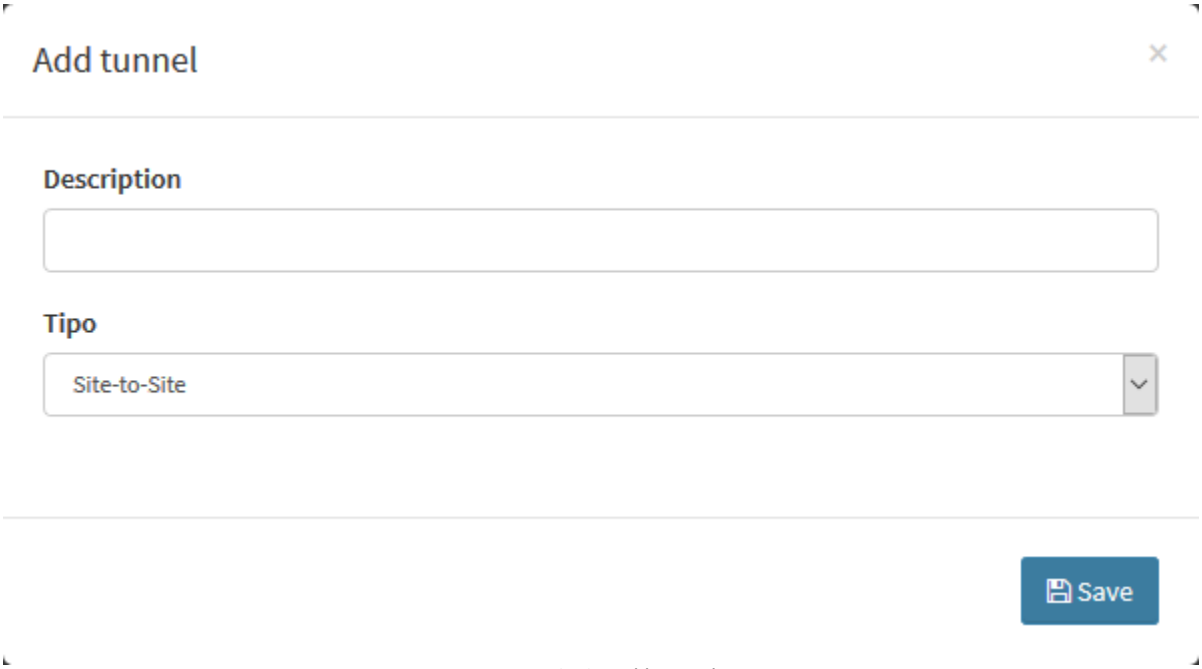
IPSEC VPN - Tunnels Tab

The following screen will appear:



IPSEC VPN - Tunnels

Click the ***Add***[+] button to add a new VPN, the following screen will appear:



VPN IPSEC - Add Tunnel

- ***Description*****:** *Tunnel 1*;
- **Tipo:** *Site-to-Site.*

Click **[** Save **]** to save the changes and after this step, click the **[** ✎ **]** button to continue the settings:

VPN IPSEC

Tunnels | Remote Access | Failover

General

Description
Tunnel 1

IKE version
IKEV1

Local host
IP/ fqdn

Remote host Dynamic
IP/ fqdn

Local ID
IP/ fqdn/ host/ email@domain

Remote ID Dynamic
IP/ fqdn/ host/ email@domain

Tunnel initialization
Automatic

Exchange Mode
Select

Authentication Method
Shared Key

Shared Key
text alpha

Local RSA Key

Remote RSA Key

Network

IP Version
Select

Local networks
0.0.0.0

Remote networks
0.0.0.0

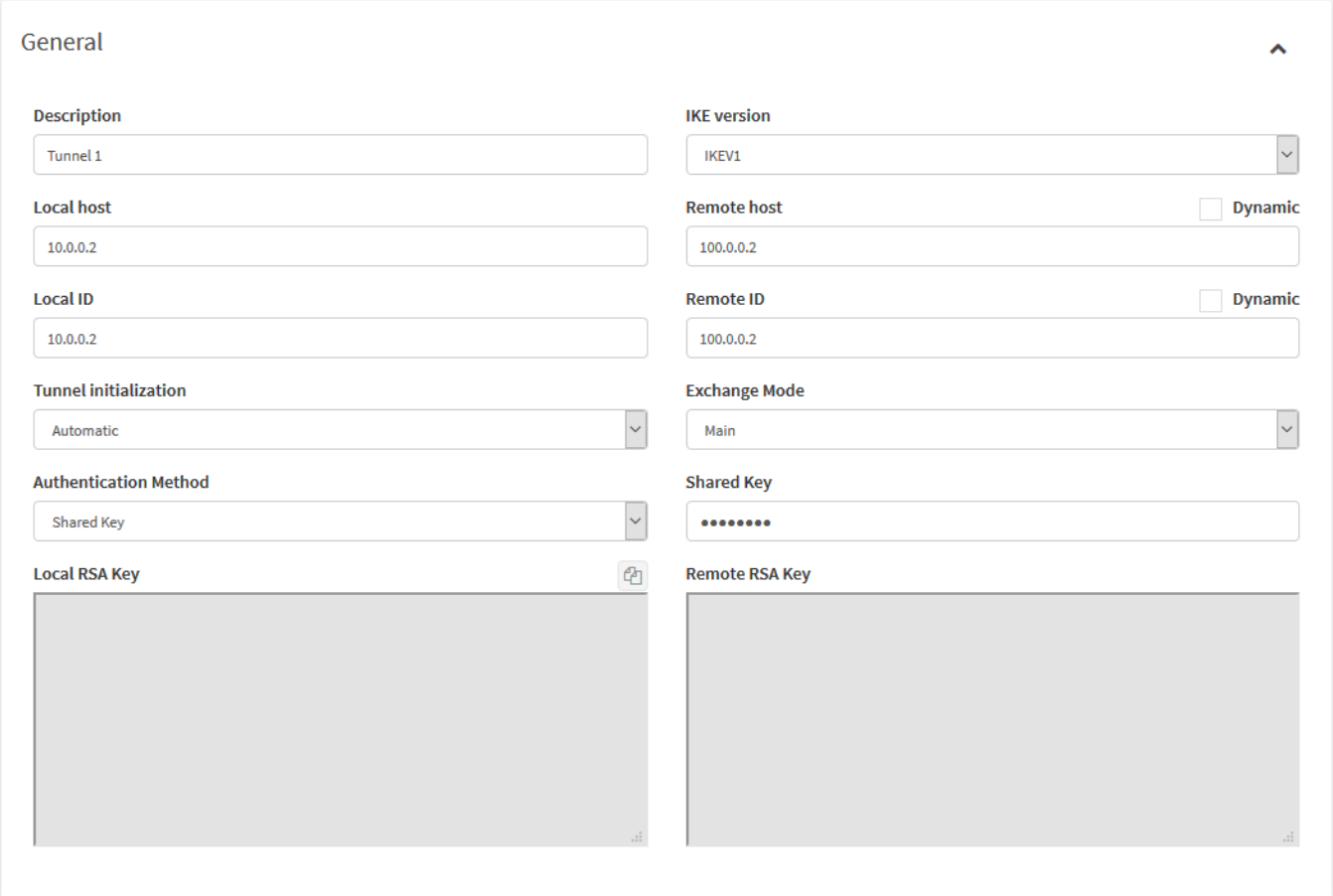
Cryptography

Advanced

Next we will analyze each component of the panel and point out the specific steps for configuring the SD-WAN, for more in-depth information on VPN, check the IPSEC VPN chapter.

General

Complete the form as shown below:

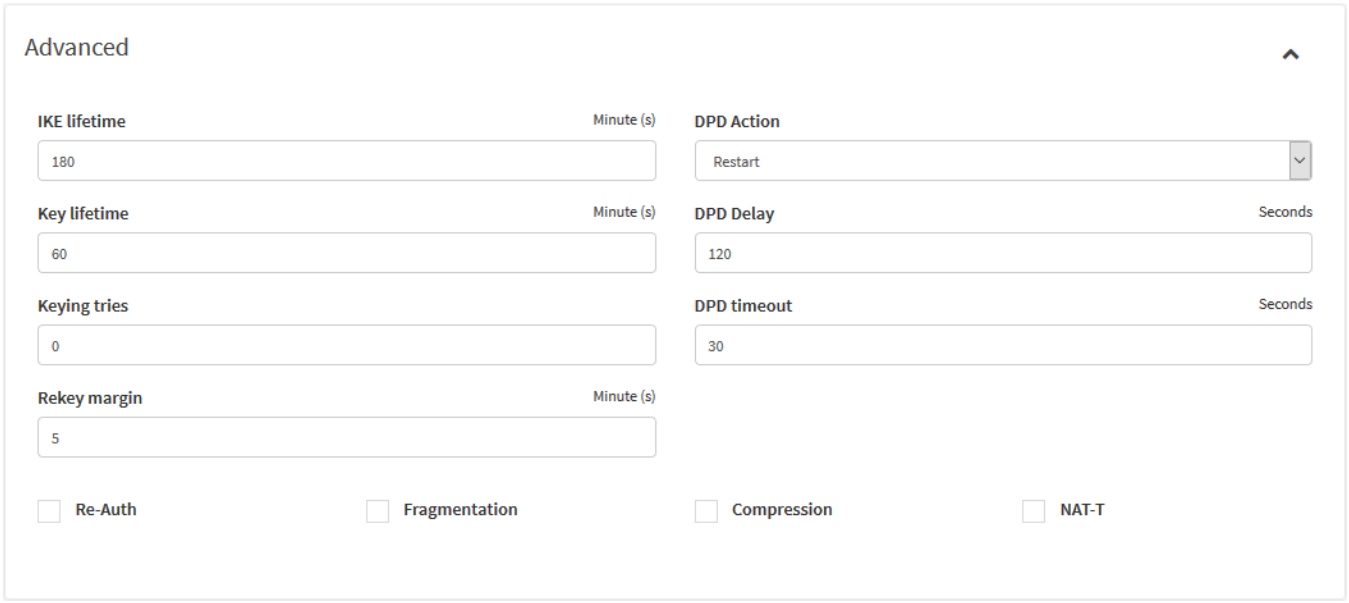


IPSEC VPN - General Panel

- ***Description*:** Enter the desired description in order to facilitate the identification of the VPN later;
- ***IKE Version*:** Determines the version of IKE that will be used. In this example we will use the IKEv1 version;
- ***Local Host*:** Determines the communication address of the LOCAL VPN point to establish the tunnel. In this field it is necessary to add real IP. Ex.: 10.0.0.2;
- ***Remote Host*:** Determines the remote address with which the VPN will attempt to establish a connection. In this field it is necessary to add the real IP of the remote host. Ex.: 100.0.0.2;
- ***Local ID*:** Local VPN tip identification method. In this field it is necessary to add real IP. Ex.: 10.0.0.2;
- ***Remote ID*:** Remote VPN tip identification method. In this field it is necessary to add real IP. Ex.: 100.0.0.2;
- ***Tunnel Initialization*:** Determines how the tunnel will start. Ex.: *Automatic*;
- ***Exchange Mode*:** IKE key negotiation method. Ex.: *Main*;
- ***Authentication Method*:** Determines the authentication method that will be used on the VPN. Ex.: *Shared Key*;
- ***Shared Key*:** The pre-shared key that will be used to authenticate the VPN;
- ***Local RSA Key*:** If the “RSA Key” option is selected in “Authentication Method”, this field will be available. In this example, we will not use the “RSA Key” option;
- ***Remote RSA Key*:** If the option “RSA Key” is selected in “Authentication Method”, this field will be available. In this example, we will not use the “RSA Key” option.

Network

Complete the form as shown below:

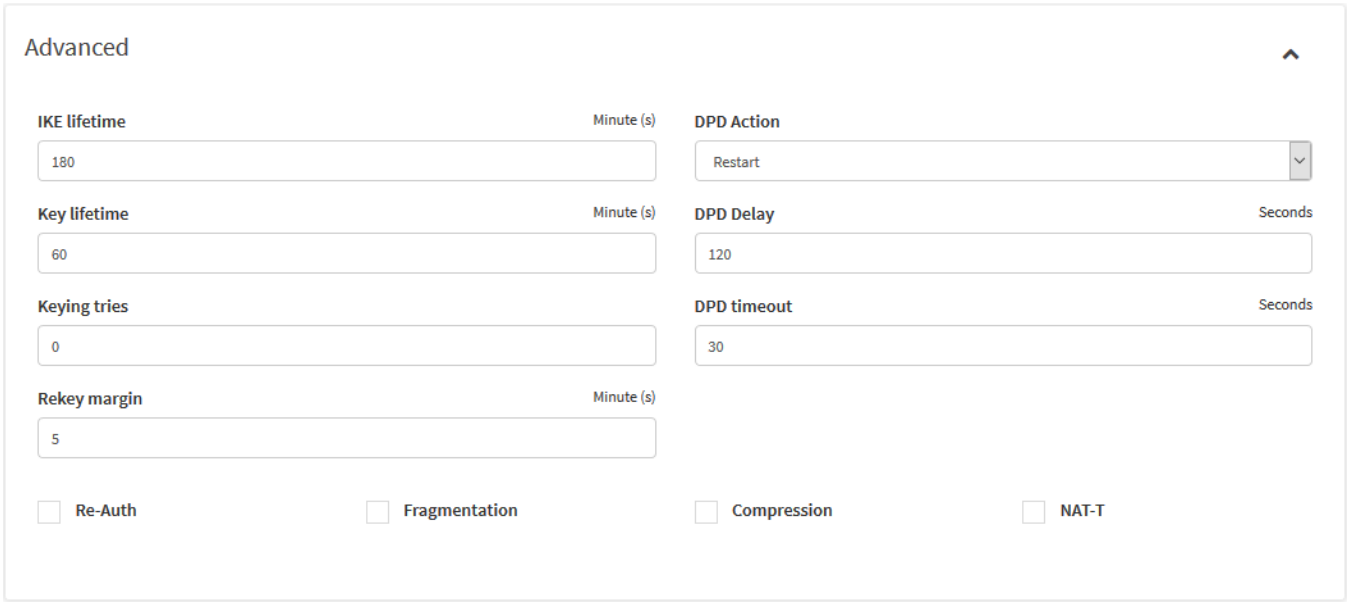


VPN IPSEC – Network Panel

- ***IP version*:** It is not necessary to determine the IP version, it can be left default;
- ***Local Networks*:** It is important for the correct functioning of the SD-WAN that this field remains unanswered. The SD-WAN itself will determine the “Local Networks”;
- ***Remote Networks*:** As in the top field, it is important for the correct functioning of the SD-WAN to leave this field empty. The SD-WAN will determine the “Remote Networks” itself.

Advanced

Complete the form as shown below:



VPN IPSEC – Advanced Panel

- ***Keying tries*:** This is the number of times the VPN points will renegotiate the tunnel or attempt re-authentication after the key expires. In our example we will use the value “0”;

All other options can be left at the default, click the **[ ]** button to save the settings done.

After these steps, we will have arrived at the result shown by the image below:

General

Description
Tunnel 1

IKE version
IKEV1

Local host
10.0.0.2

Remote host Dynamic
100.0.0.2

Local ID
10.0.0.2

Remote ID Dynamic
100.0.0.2

Tunnel initialization
Automatic

Exchange Mode
Main

Authentication Method
Shared Key

Shared Key
••••••••

Local RSA Key

Remote RSA Key

Network

IP Version
Select

Local networks
0.0.0.0

Remote networks
0.0.0.0

Cryptography

Advanced

IKE lifetime Minute (s)
180

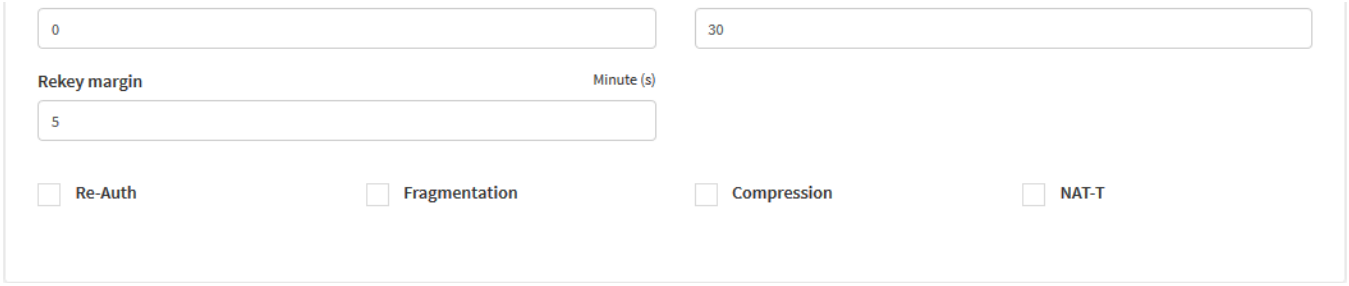
DPD Action
Restart

Key lifetime Minute (s)
60

DPD Delay Seconds
120

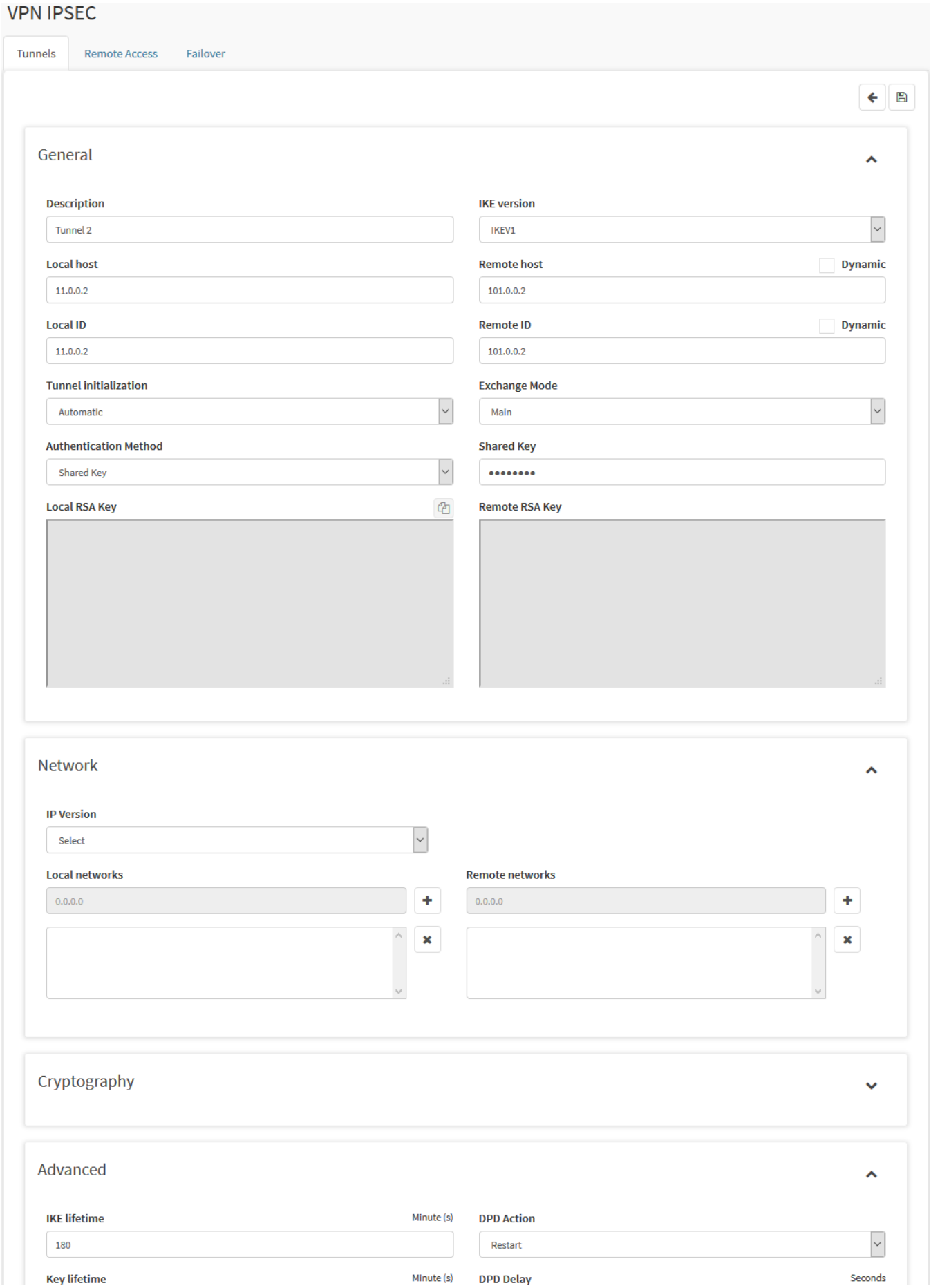
Keying tries

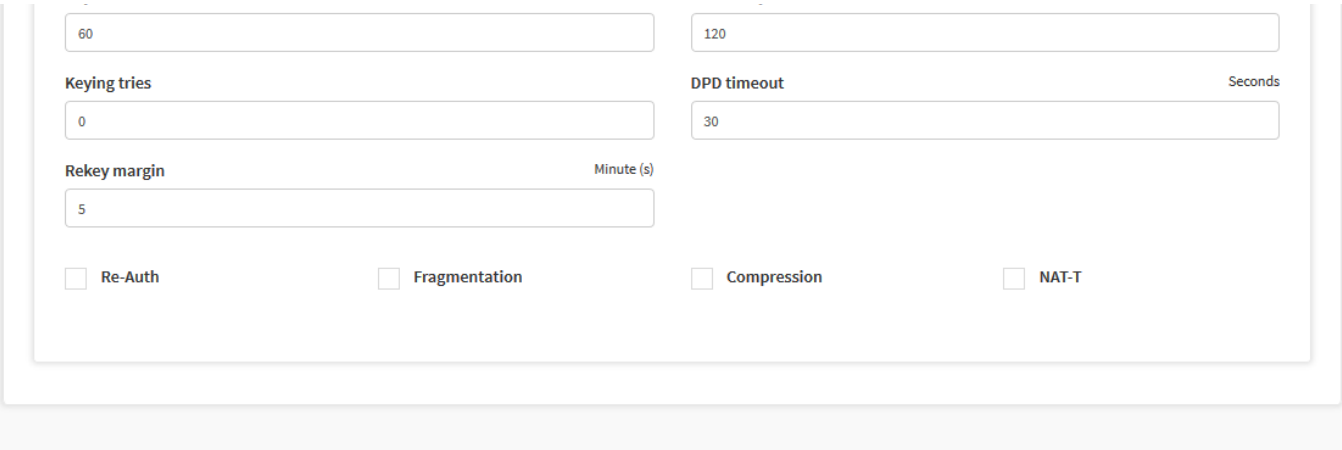
DPD timeout Seconds



IPSEC VPN - Tunnel Settings 1

Repeat these steps at both ends of the net. Tunnel 2 must be configured as shown on the image below:


VPN IPSEC
Tunnels
Remote Access
Failover
General
Description
Tunnel 2
IKE version
IKEV1
Local host
11.0.0.2
Remote host
Dynamic
101.0.0.2
Local ID
11.0.0.2
Remote ID
Dynamic
101.0.0.2
Tunnel initialization
Automatic
Exchange Mode
Main
Authentication Method
Shared Key
Shared Key
Local RSA Key
Remote RSA Key
Network
IP Version
Select
Local networks
0.0.0.0
Remote networks
0.0.0.0
Cryptography
Advanced
IKE lifetime
Minute (s)
180
DPD Action
Restart
Key lifetime
Minute (s)
DPD Delay
Seconds



VPN IPSEC – Tunnel 2 settings

Going to the other point, on the NGFW - Remote Office Tunnel 1 must be configured as shown on the image below:

General

Description
Tunnel 1

IKE version
IKEV1

Local host
100.0.0.2

Remote host Dynamic
10.0.0.2

Local ID
100.0.0.2

Remote ID Dynamic
10.0.0.2

Tunnel initialization
Automatic

Exchange Mode
Main

Authentication Method
Shared Key

Shared Key
••••••••

Local RSA Key

Remote RSA Key

Network

IP Version
Select

Local networks
0.0.0.0

Remote networks
0.0.0.0

Cryptography

Advanced

IKE lifetime Minute (s)
180

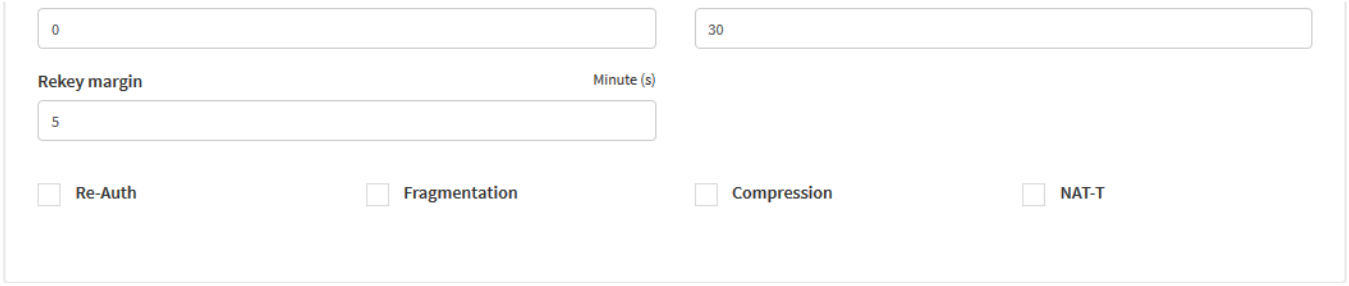
DPD Action
Restart

Key lifetime Minute (s)
60

DPD Delay Seconds
120

Keying tries

DPD timeout Seconds



Remote Office - Tunnel Settings 1

Tunnel 2 settings for NGFW - Remote Office should be as shown on the image below:

General

Description
Tunnel 2

IKE version
IKEV1

Local host
11.0.0.2

Remote host Dynamic
101.0.0.2

Local ID
11.0.0.2

Remote ID Dynamic
101.0.0.2

Tunnel initialization
Automatic

Exchange Mode
Main

Authentication Method
Shared Key

Shared Key
••••••••

Local RSA Key

Remote RSA Key

Network

IP Version
Select

Local networks
0.0.0.0

Remote networks
0.0.0.0

Cryptography

Advanced

IKE lifetime Minute (s)
180

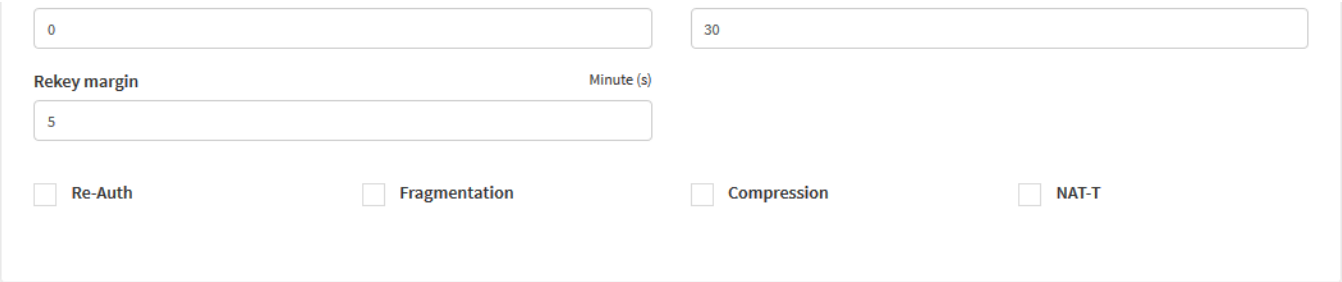
DPD Action
Restart

Key lifetime Minute (s)
60

DPD Delay Seconds
120

Keying tries

DPD timeout Seconds



Remote Office - tun2 settings

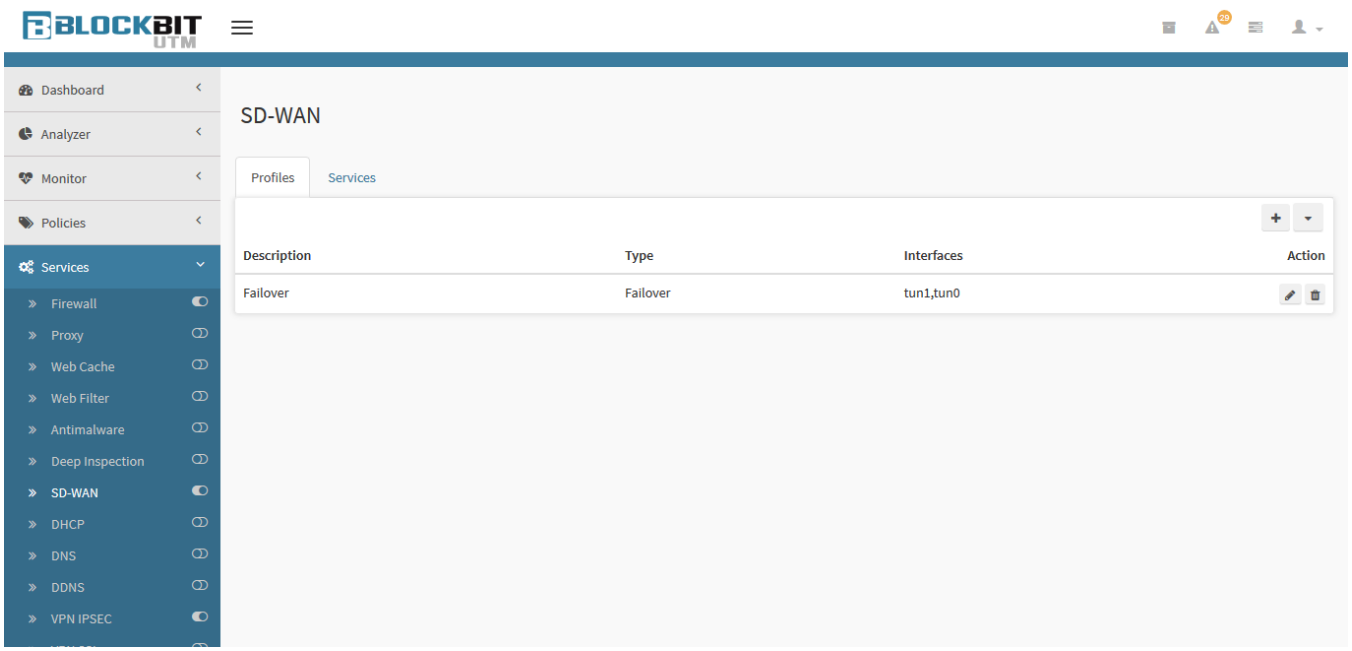
After saving each profile, for the VPN to take action it will be necessary to access the **command queue [ ]** and apply the changes done. For more information on the command queue, access the UTM - Command queue page.

Next, we will add the SD-WAN itself.

SD-WAN: Configure SD-WAN

After configuring the VPNs, follow the steps below:

Once again we will configure the NGFW - HQ, access **Services SD-WAN**.



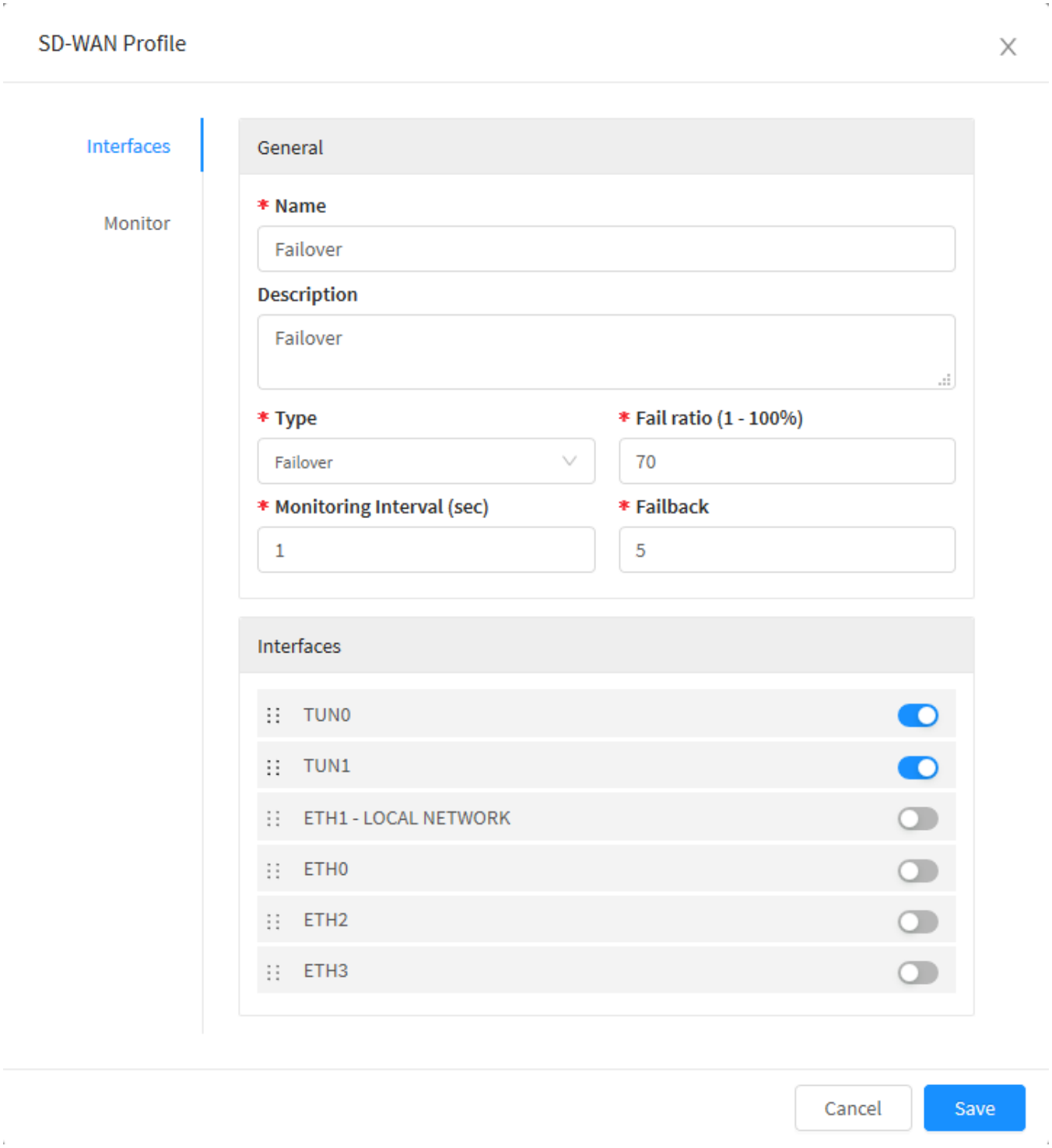
SD-WAN

Click the ***Add***[ ] button to add a new SD-WAN profile.

Next, we will analyze each component of the panel and point out the specific steps for configuring the SD-WAN, for more in-depth information on this topic see the chapter on Profile Types.

Interfaces

Complete the form as shown below:



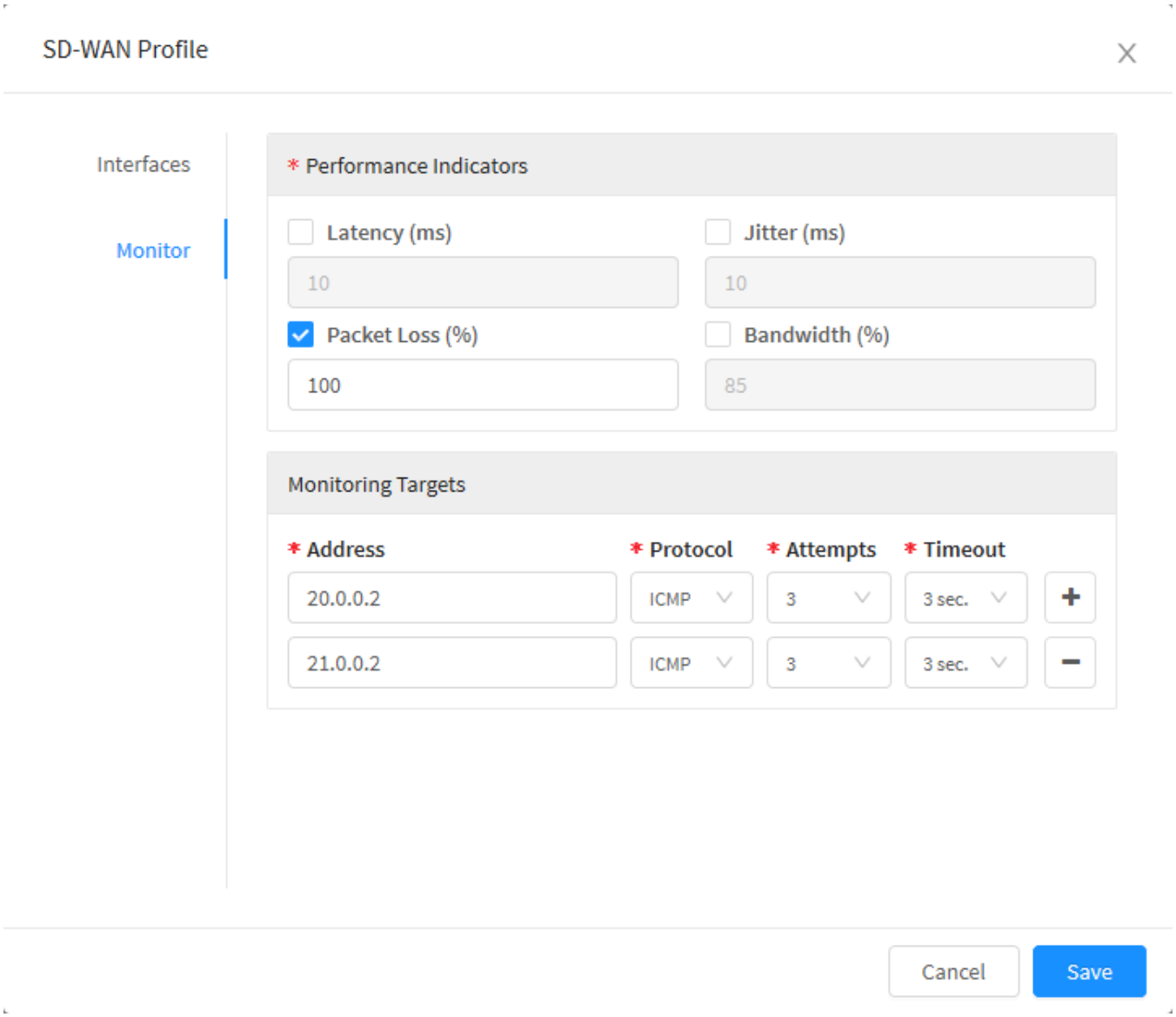
SD-WAN - Interfaces

- ***Description*:** Define a name for the profile. Ex.: Failover;
- ***Type*:** In this field it is defined how the SD-WAN will act. It is possible to select any type, but in this demonstration we will use “Failover”. For more information about the types of SD-WAN check the chapter Types of Profile;
- ***Interfaces*:** It is essential for the correct functioning of the SD-WAN to define the internet link interfaces that will be used in the composition of the profile. In this example we will select the interfaces: "tun0 - Network 10" and "tun1 - Network 11";
- ***Monitoring Interval* (sec.):** Define the monitoring interval between each test. It is recommended to leave it as 1 second;
- **Failback:** Defines the number of times an interface whose connectivity has failed will be tested to enable routing through it. For more information see this page. Ex.: 5;
- ***Fail Ratio* 1-100%:** Set the failure rate value between 1 to 100%. It is recommended to leave the default of 70%. Ex.: 70%.

After this step, click on the “Monitors” side tab.

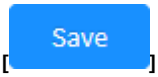
Monitors

Complete the form as shown below:

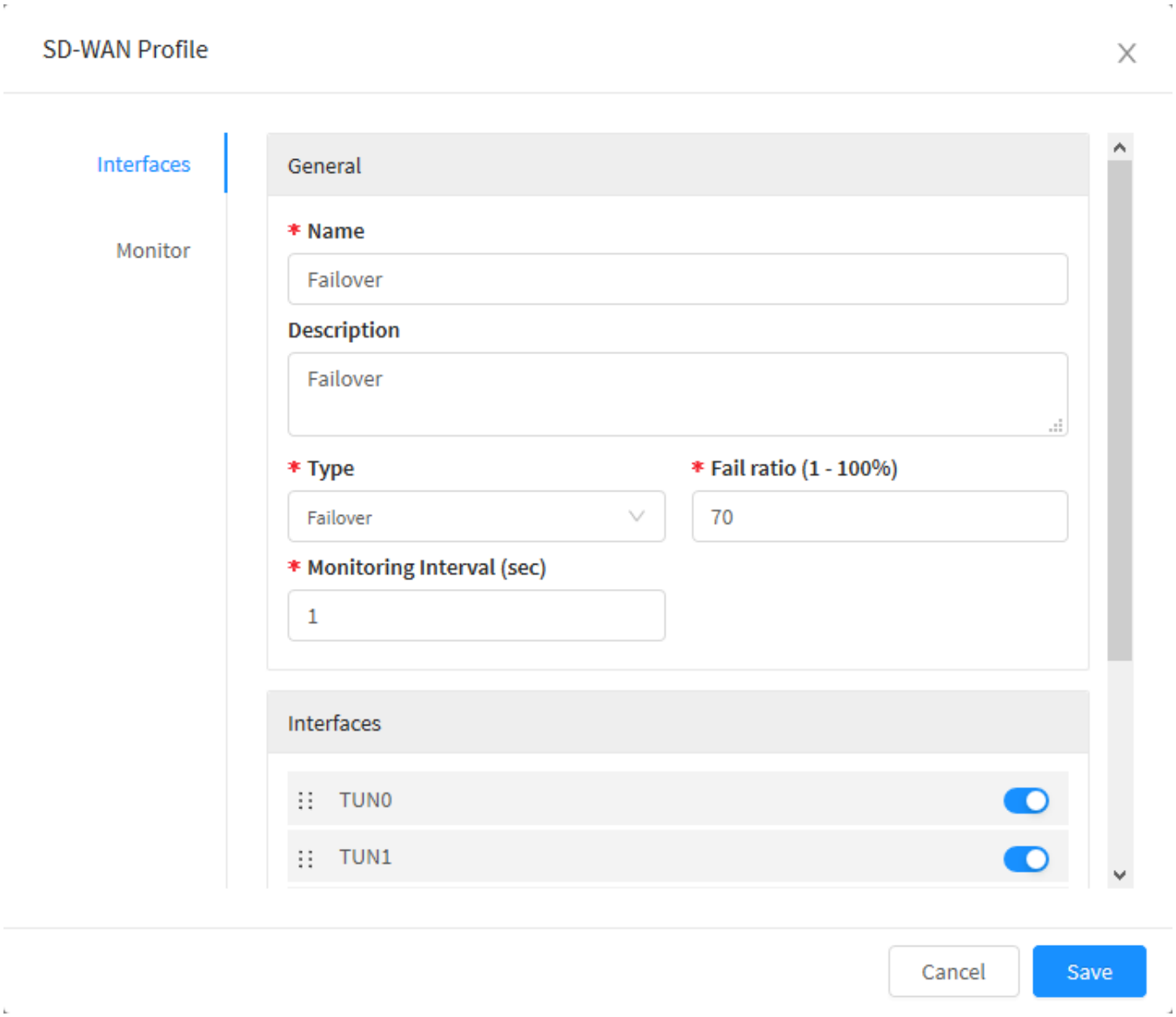


SD-WAN - Monitors

- ***Performance Indicators*:** The options on this panel must be determined according to the tests you want to perform. It is possible to select any type, but in this demonstration we will use “Packet Loss” with a rate of “100%”.
- ***Monitoring Targets*:** Defines the addresses where the tests will be performed. It is recommended that in the "Monitoring Targets" the virtual IPs are placed on the other side of the tunnel so that if the communication is successful, it indicates that the Tunnel is correctly configured. Ex .: 20.0.0.2 and 21.0.0.2.

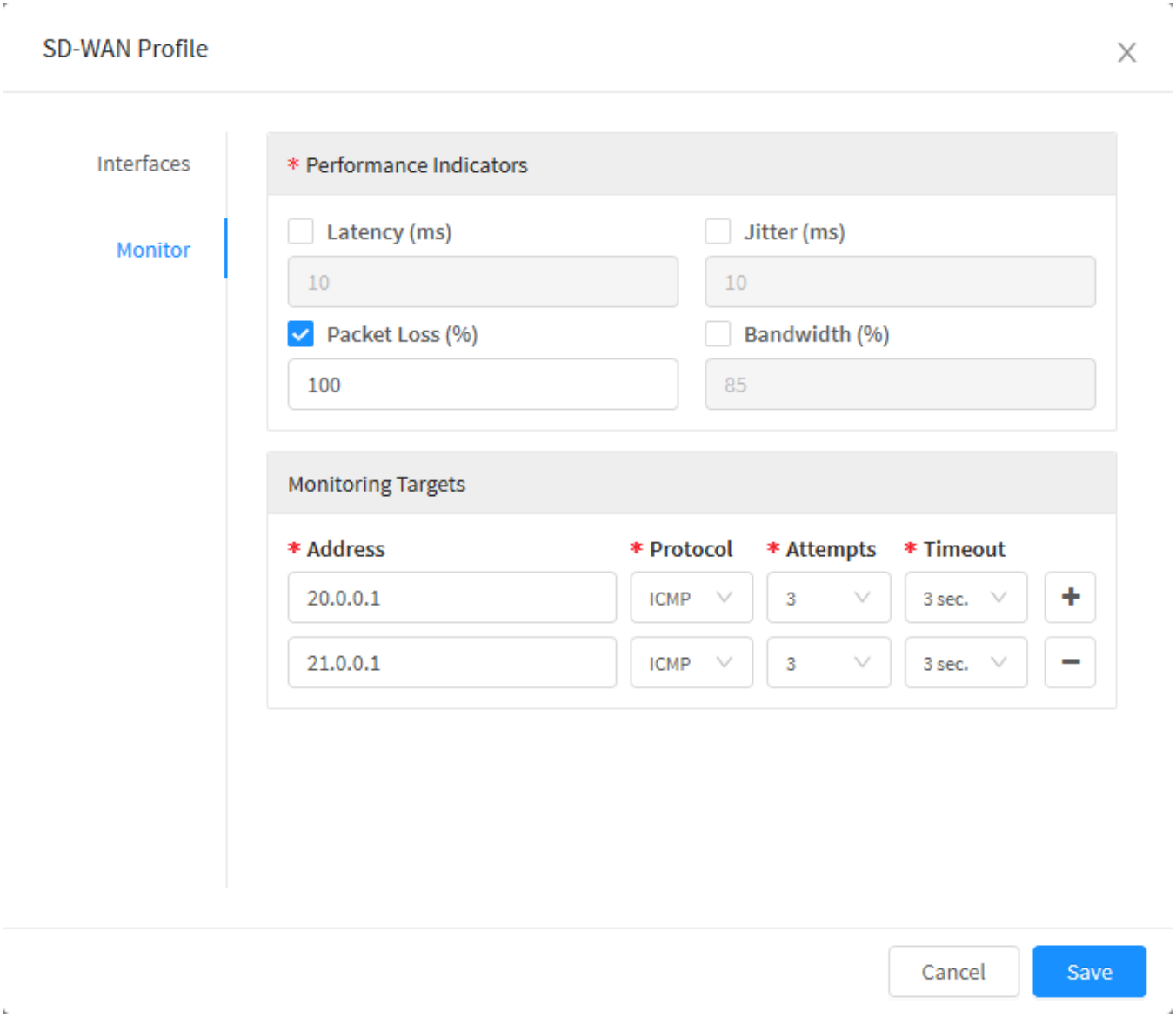
Click the **[**  **]** button to save the settings.

Repeat these steps on the NGFW - Remote Office the “Interface” tab must have been configured as shown on the image below:



Remote Office - Interface Settings

The “Monitor” tab should be as shown on the image below:



Remote Office - Monitor Settings

After saving each profile, for the SD-WAN to take action it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the UTM - Command queue page.

Finally, it is necessary to create a firewall policy to release communication using the SD-WAN.

SD-WAN: Add Policies

After configuring the SD-WAN, follow the steps below:

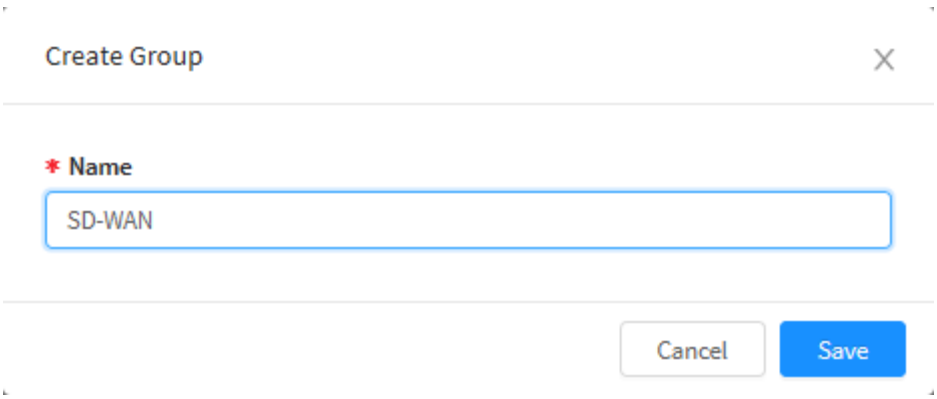
In this example, a Policy will be created using an IP.

> To create a Policy using a Mac Address, check the NAT rules by Mac Address chapter.

Finally, a Policy will be created to allow access, access **Policies IPv4**.

IPv4 – Policies

It is recommended to add a separate group called “SD-WAN” in order to isolate the SD-WAN Policies from the others in order to facilitate control, to do so, click on the **Add group [➕]** icon.



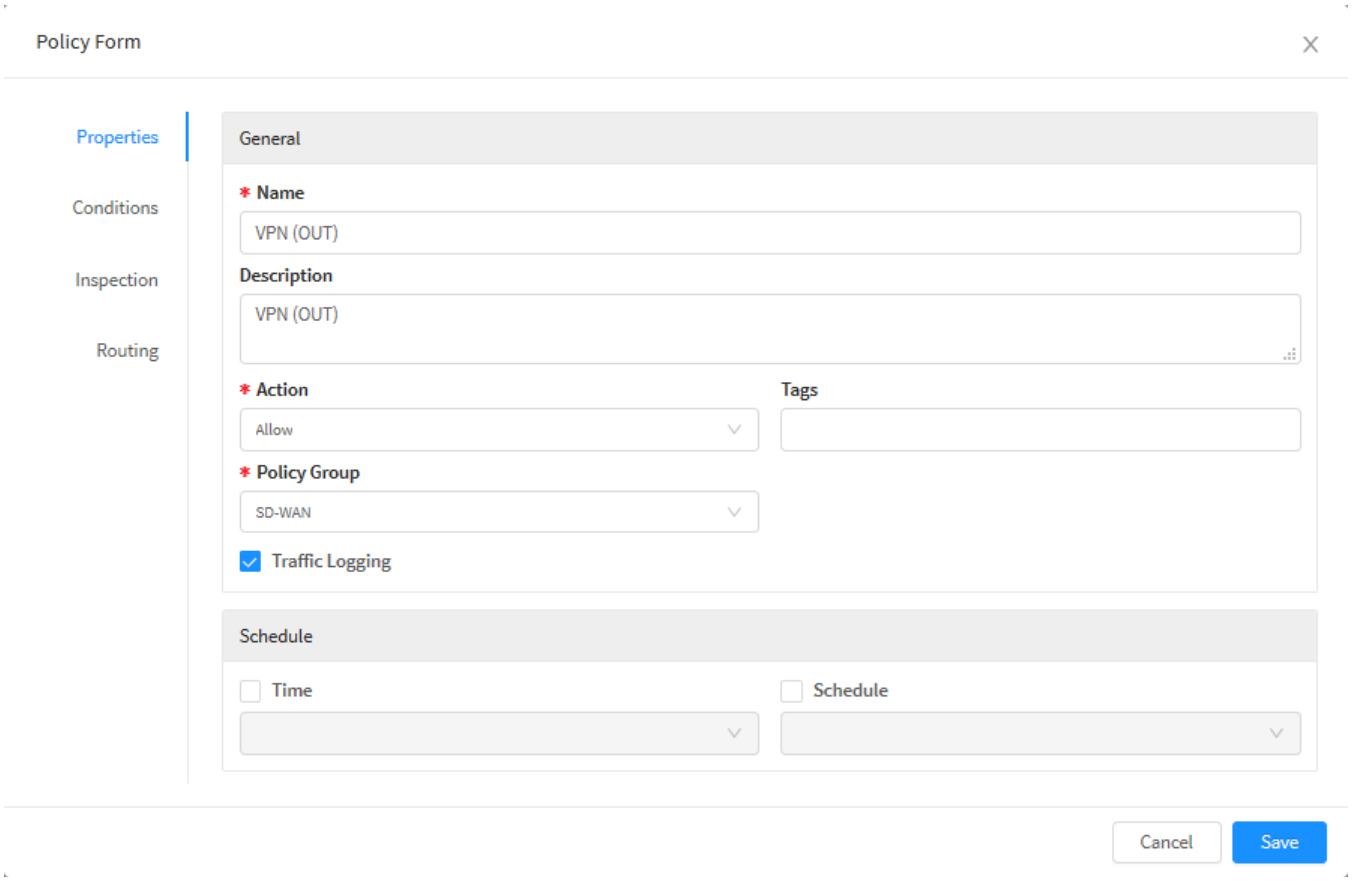
SD-WAN – Add Group of Policies

After this step, click Add [ ] to add a new Policy.

Next, we will analyze each component of the panel and point out the specific steps for configuring the SD-WAN, for more information about Policies check the *Policy chapter.*

Properties

Complete the form as shown below:



IPv4 - Policies - Properties

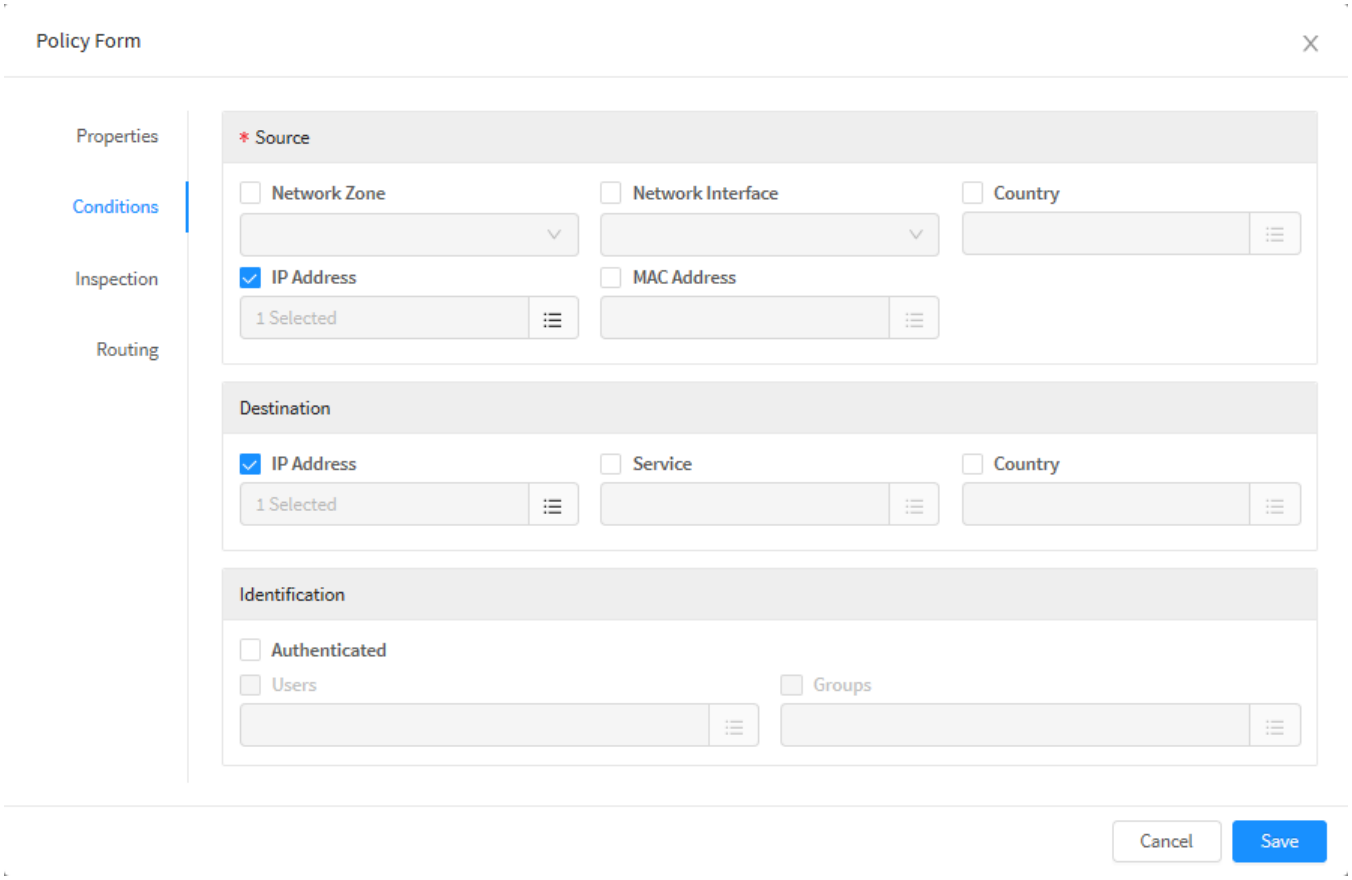
- ***Name*****:** Add the Policy name. In this demonstration we will use “VPN (Out)”;
- ***Description*****:** Insert the desired description in order to facilitate the identification of the policy interface later. In this demonstration we will use “VPN (Out)”;
- ***Tags*****:** No tags will be inserted in this demo;
- ***Action*****:** As this Policy is meant to permit access, we will select "Allow";
- ***Policy Group*****:** In this checkbox, “SD-WAN” will be selected, choose the name of the group that we have created before;
- ***Traffic logging*****:** In this demonstration we will generate reports and, therefore, this checkbox will be selected.

All other options can be left as default.

Click on the "Conditions" side tab.

Conditions

Complete the form as shown below:



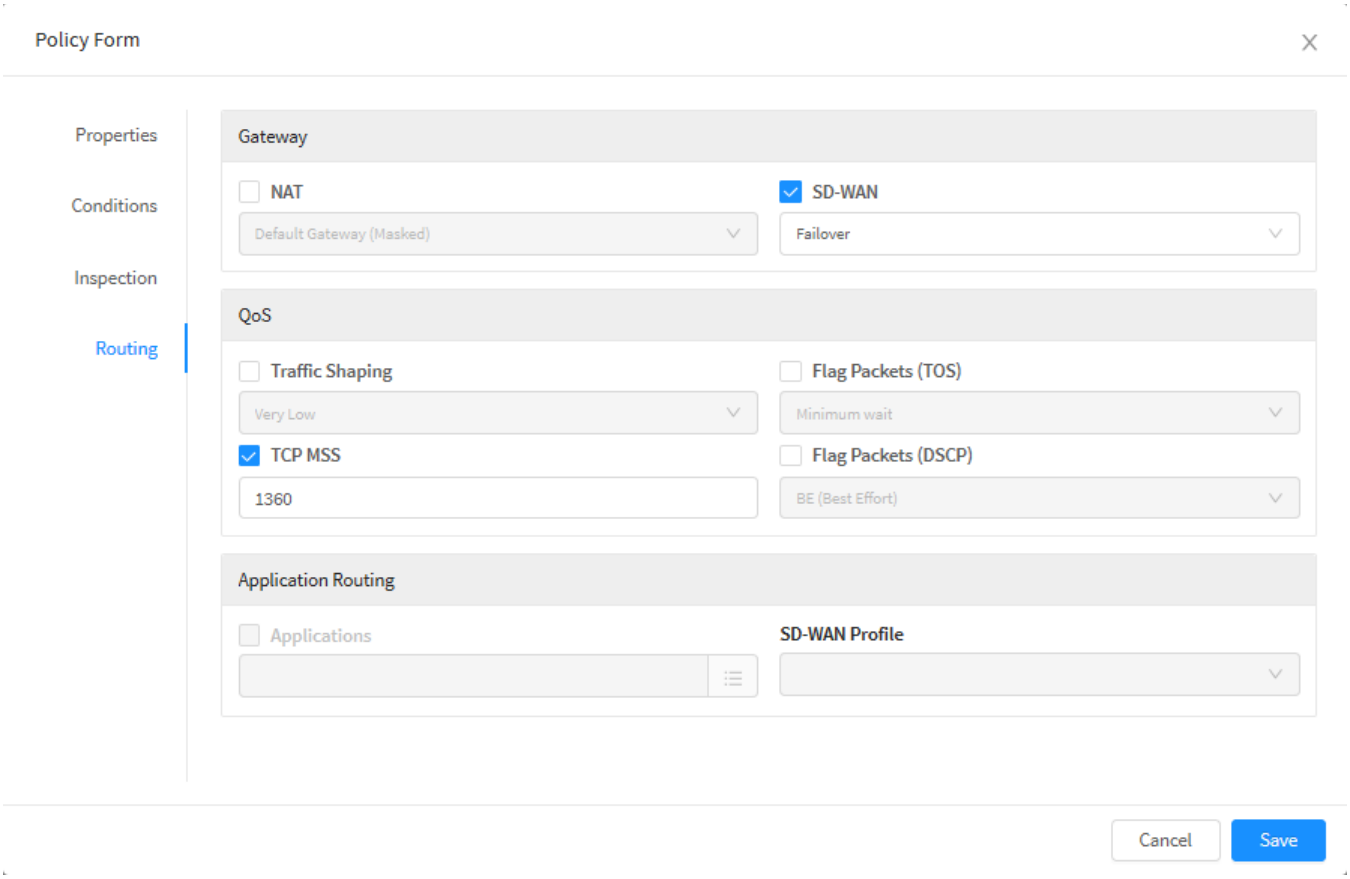
IPv4 - Policies - Connection

- ***Network Zone*:** This checkbox can be left in the default setting;
- ***Network interface*:** This checkbox can be left in the default setting;
- ***Source - IP Address*:** You must select this check box and select the IP that has been configured as the LAN interface. At the NGFW - HQ it will be “LAN - 172.18.0.0/16”;
- ***Source - MAC Address*:** This rule will not use a physical address and, therefore, will not deal with MAC Address, the selection can be left in the default setting;
- ***Destination – IP Address*:** You must select this check box and select the IP that has been configured as a Remote interface. At the NGFW HQ it will be “Remote - 172.17.0.0/16”;
- ***Service*:** This rule will not deal with services and, therefore, the selection may be left in the default setting;
- ***Authenticated***: This checkbox can be left in the default setting;
- ***Users***: This checkbox can be left in the default setting;
- ***Groups***: This checkbox can be left in the default setting.

Click on the "Routing" side tab.

Routing

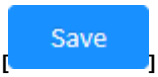
Complete the form as shown below:



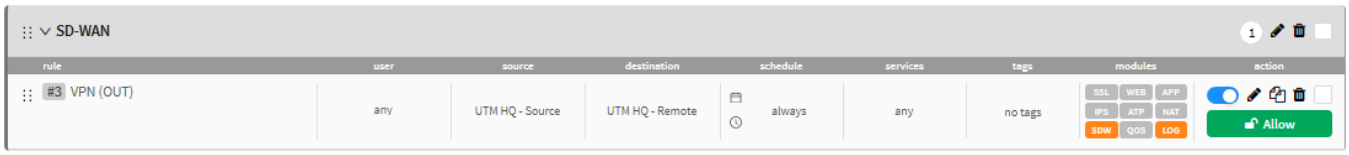
IPv4 – Policies - Routing

- ***SD-WAN*:** It is essential that this checkbox is checked and that the appropriate profile is selected. As was created in the previous session, in our case we will select “Failover”;
- ***TCP MSS*:** Allows you to define a value that specifies the largest amount of data, specified in bytes, that a computer or communication device can receive on a single TCP segment. It is essential for the correct functioning of the SD-WAN that this checkbox is marked and has the value 1360, so traffic is adequate according to the need of each communication device.

All other options can be left at the default setting

Click the save button [] to record all changes done.

After these steps, we will arrive at the result shown by the image below:

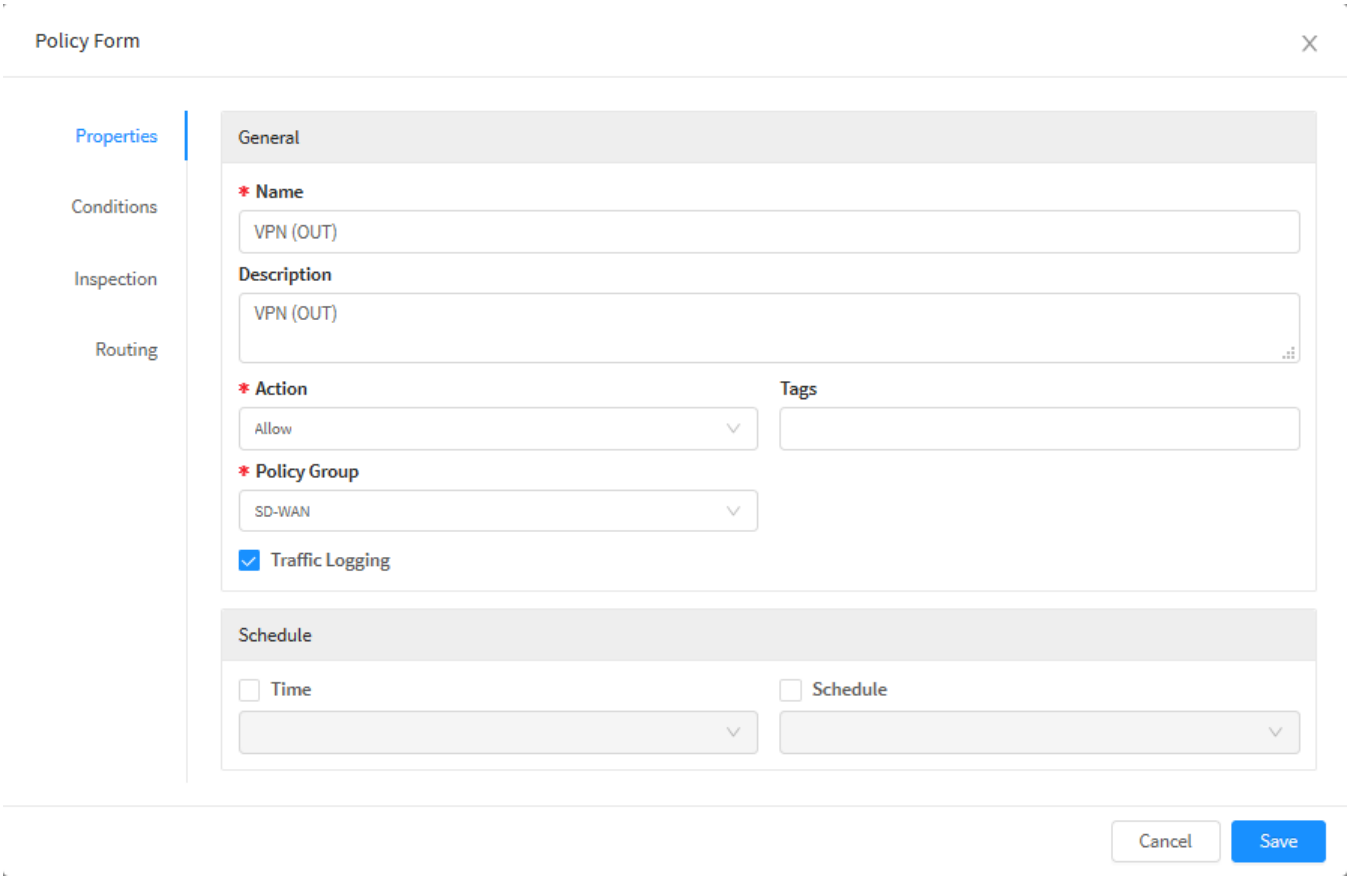


IPv4 – Policies – VPN (Out)

Repeat these steps on the NGFW - Remote Office, as shown below:

Properties

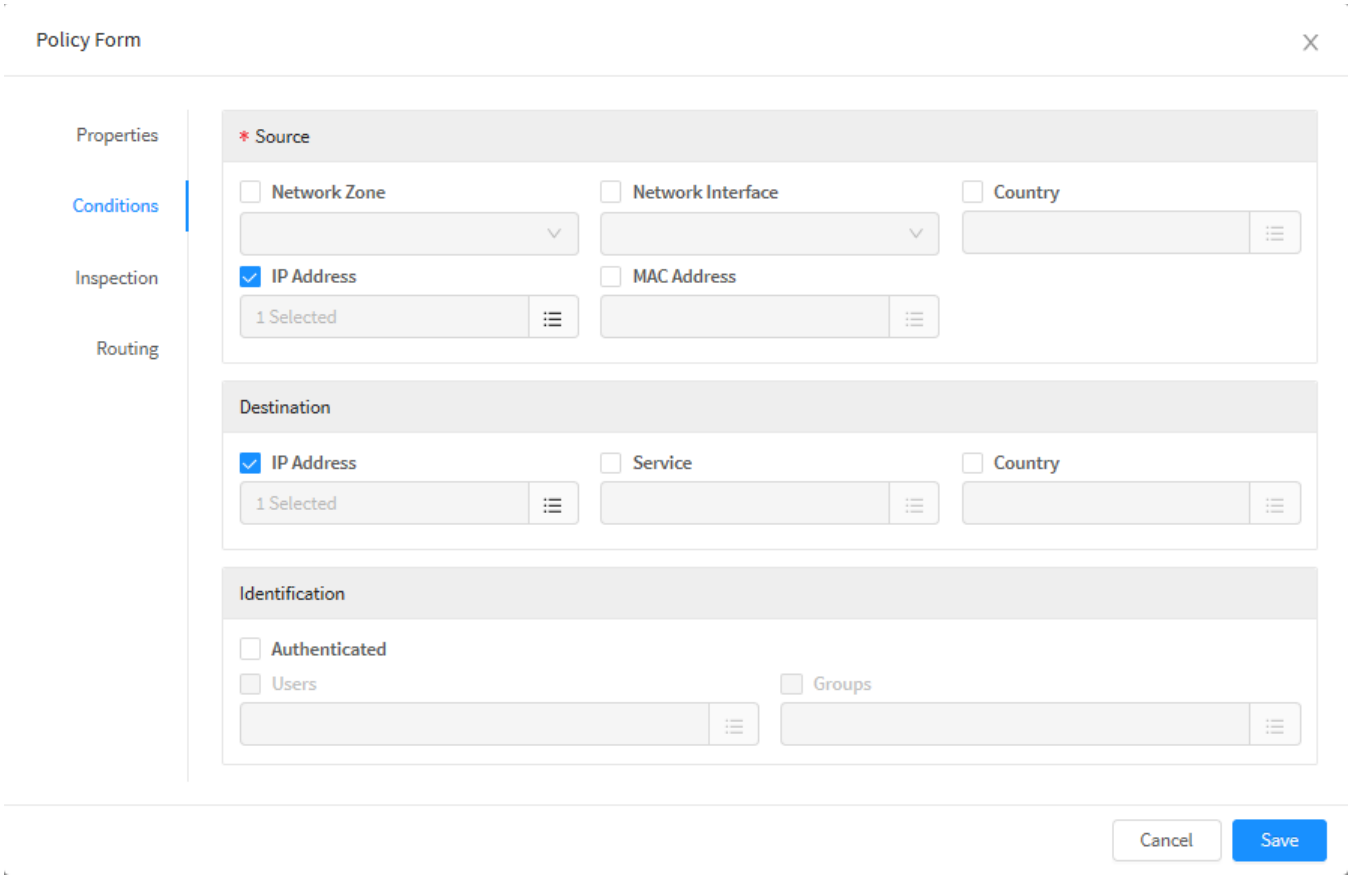
Complete the form as previously done:



IPv4 – Remote Office - Properties

Connection

Complete the form as shown below:

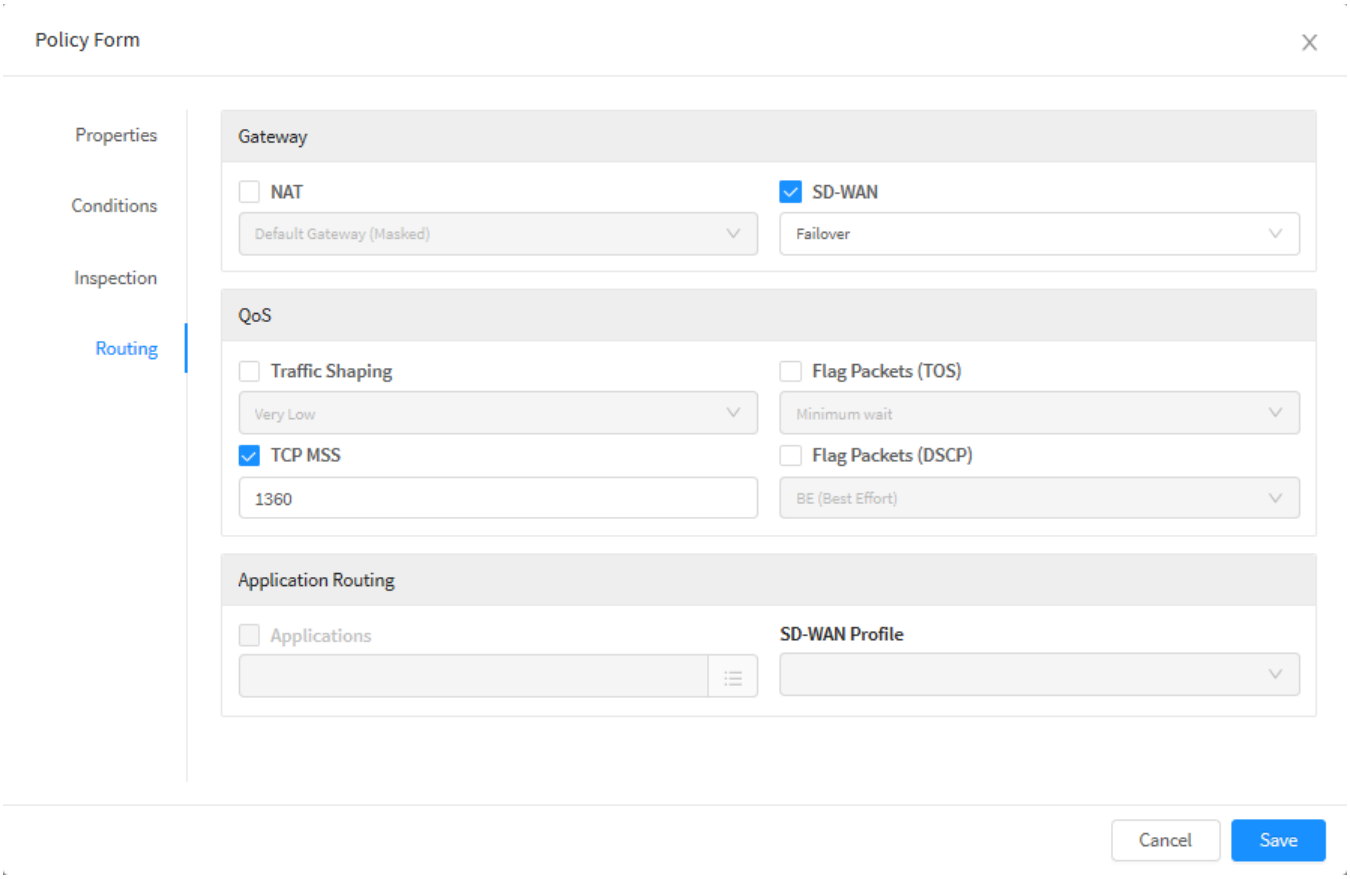


IPv4 – Remote Office - Connection

- ***Network Zone*:** This checkbox can be left in the default setting.
- ***Network interface*:** This checkbox can be left in the default setting.
- ***Source - IP Address*:** You must select this check box and select the IP that has been configured as the LAN interface. In the NGFW - Remote Office it will be “LAN - 172.17.0.0/16”;
- ***Source - MAC Address*:** This rule will not use a physical address and therefore will not deal with MAC Address, the selection may be left in the default setting;
- ***Destination – IP Address*:** You must select this check box and select the IP that has been configured as a Remote interface. In the NGFW - Remote Office it will be “Remote - 172.18.0.0/16”;
- ***Service*:** This rule will not deal with services and, therefore, the selection may be left in the default setting.
- ***Authenticated***: This checkbox can be left in the default setting;
- ***Users***: This checkbox can be left in the default setting;
- ***Groups***: This checkbox can be left in the default setting.

Routing

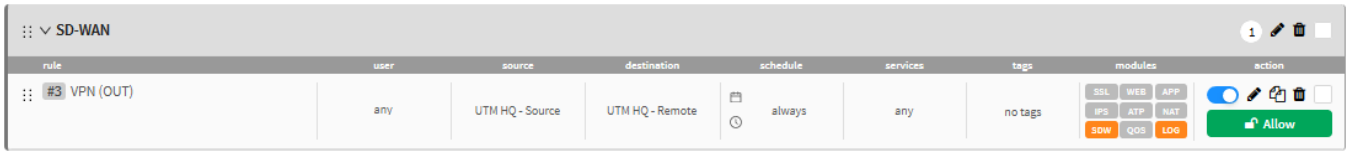
Complete the form as previously done:



IPv4 – Remote Office - Security

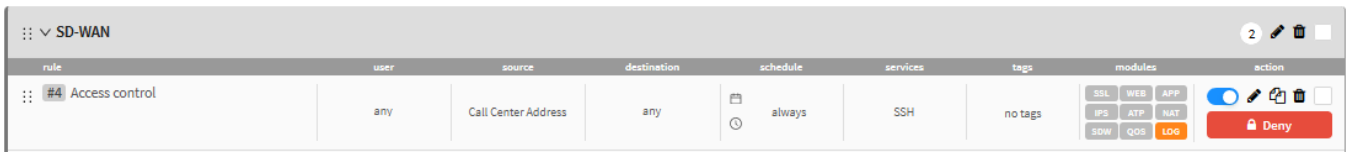
Click the [Save] button to record all changes made.

After these steps, we will arrive at the result shown by the image below:



IPv4 – Remote Office - Policies

After creating this policy, it is possible to create others controlling access, according to the needs, however it is recommended to place them in the same group “SD-WAN” and take into account the policy of “First Match Wins”, as exemplified by image below, for more information check the Policy chapter.



IPv4 – *Policies* – Access control

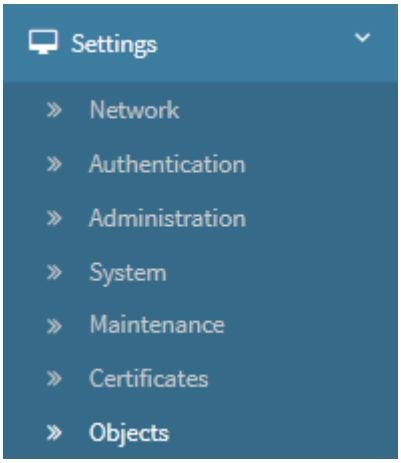
This completes the SD-WAN configuration.

SD-WAN NAT rules by Mac Address

In the example shown in Add Policies, an IP Policy was created, however, considering that if you want to create a Policy by mac address, it is also mandatory to configure the network zone, interface or source address (it is also possible to configure more than just one of these options). Here is a demonstration:

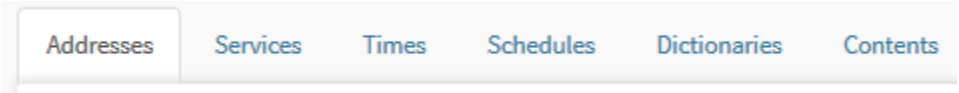
Generating Mac Address object

In the side menu access "Settings" and select the "Objects" option.



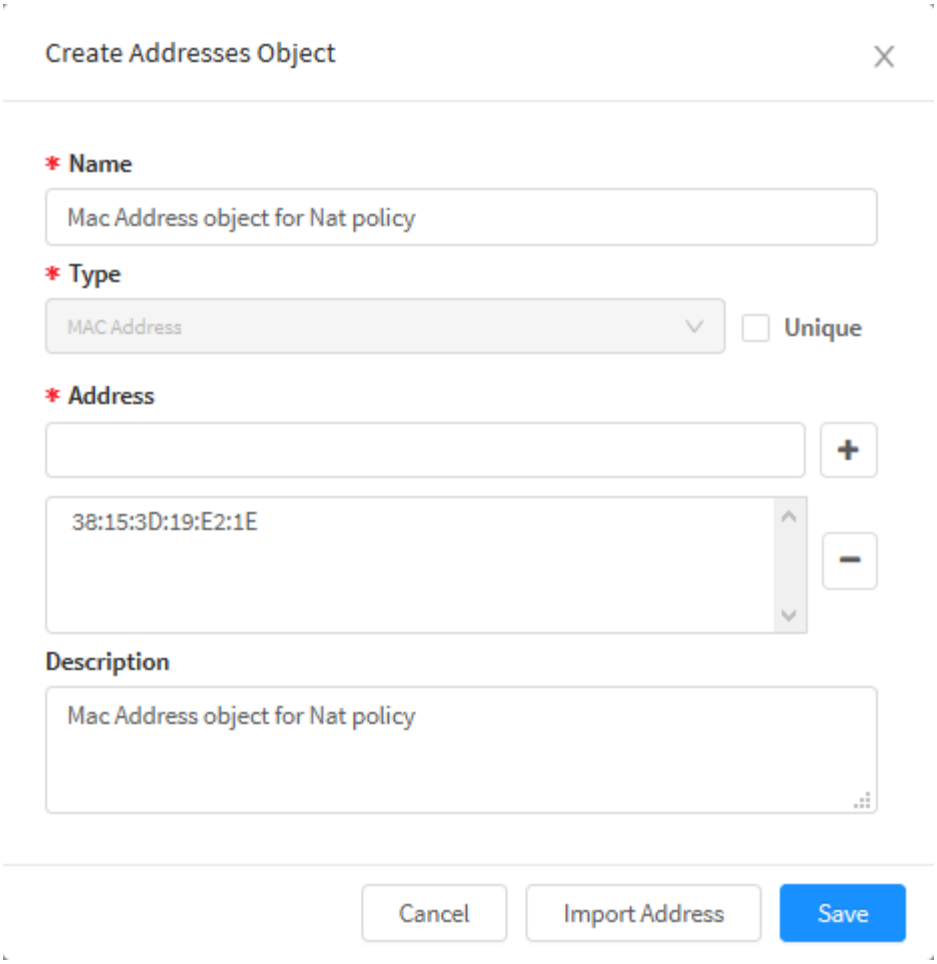
Settings - Objects

In "Objects", select the "Addresses" tab.



Settings - Objects - Addresses

Create a new mac address object by clicking on the **[**  **]** button, the following window will be displayed and complete the form as shown:



New Mac Address object

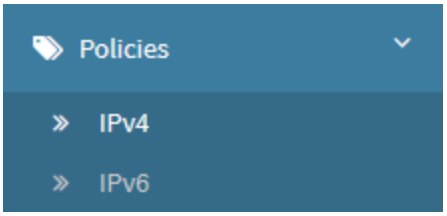
- ***Name*:** Enter the name of the Mac Address object. Ex .: Mac Address object for Nat Policy;
- ***Mac address*:** Enter the physical address and click the **[** + **]** button to add it to the list. If you want to remove a Mac Address, select it from the list and click the **[** − **]** button to remove it. Ex.: 38:15:3d:19:e2:1e;
- ***Description*:** Enter the description of your object. Ex.: Mac Address object for Nat Policy;
- ***Group*:** If you want to add this mac address to a group, add it in this field. In this example, we will not add any groups;

For more information on how to handle objects, check the *Settings - Objects* chapter.

Finally, click the **[** Save **]** button to finish the operation.

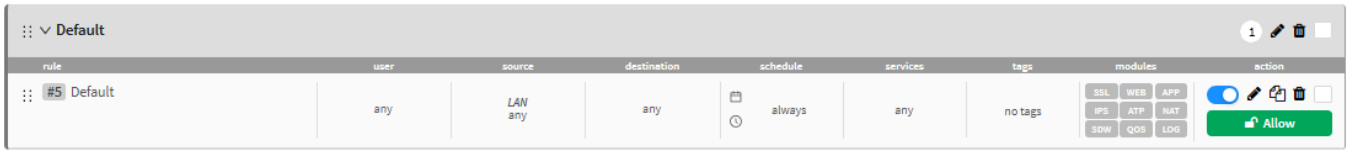
Creating the Mac Address policy

In the side menu access "Policies" and select the option "IPv4".



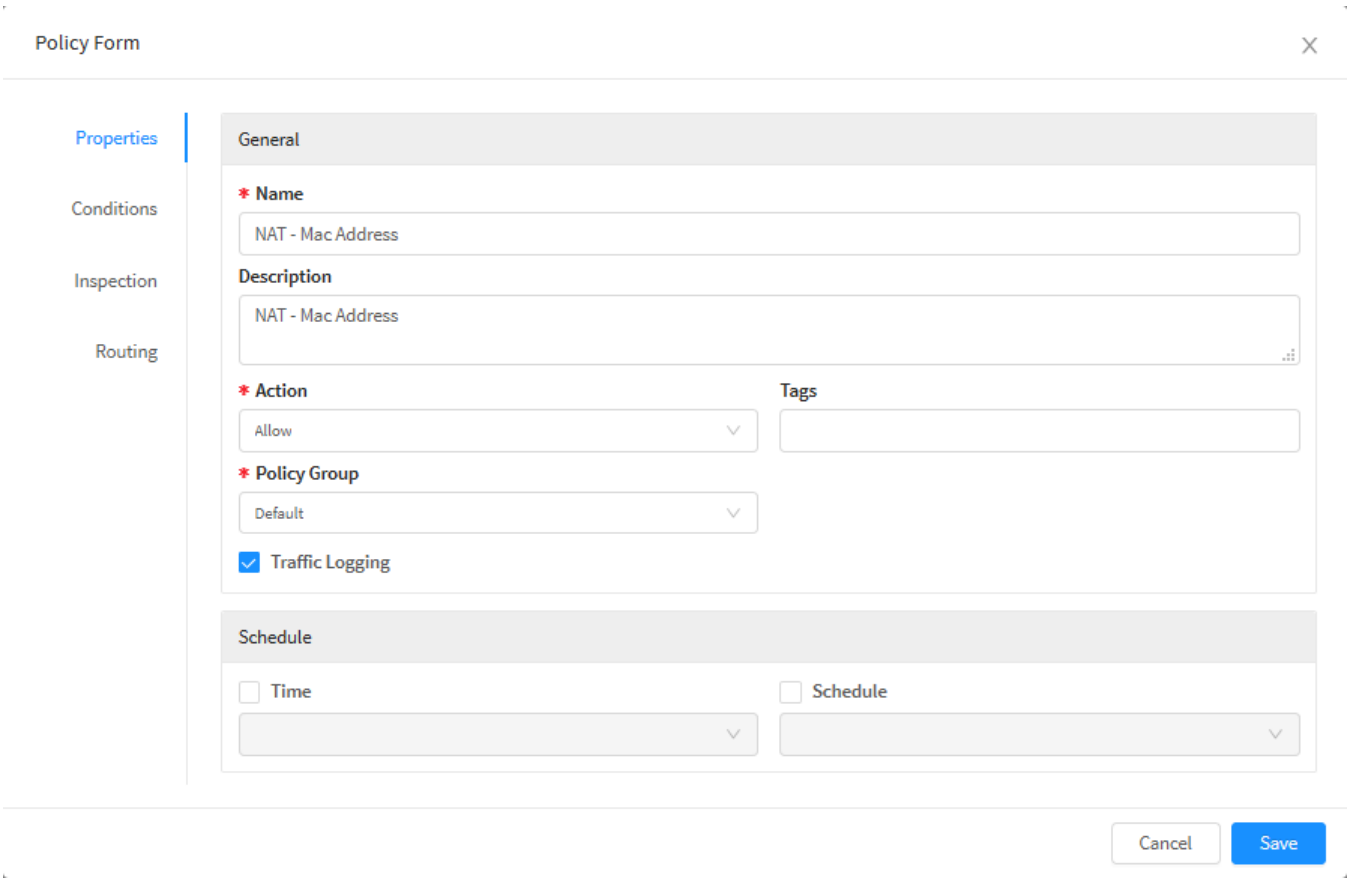
Policies - IPv4

Select the group where you want to create the Policy, in this example, we will use the "Default" group.



Policies - IPv4 - Groups

Click the Create Policy option in the Actions menu to create a new Policy. Complete the form as shown below:

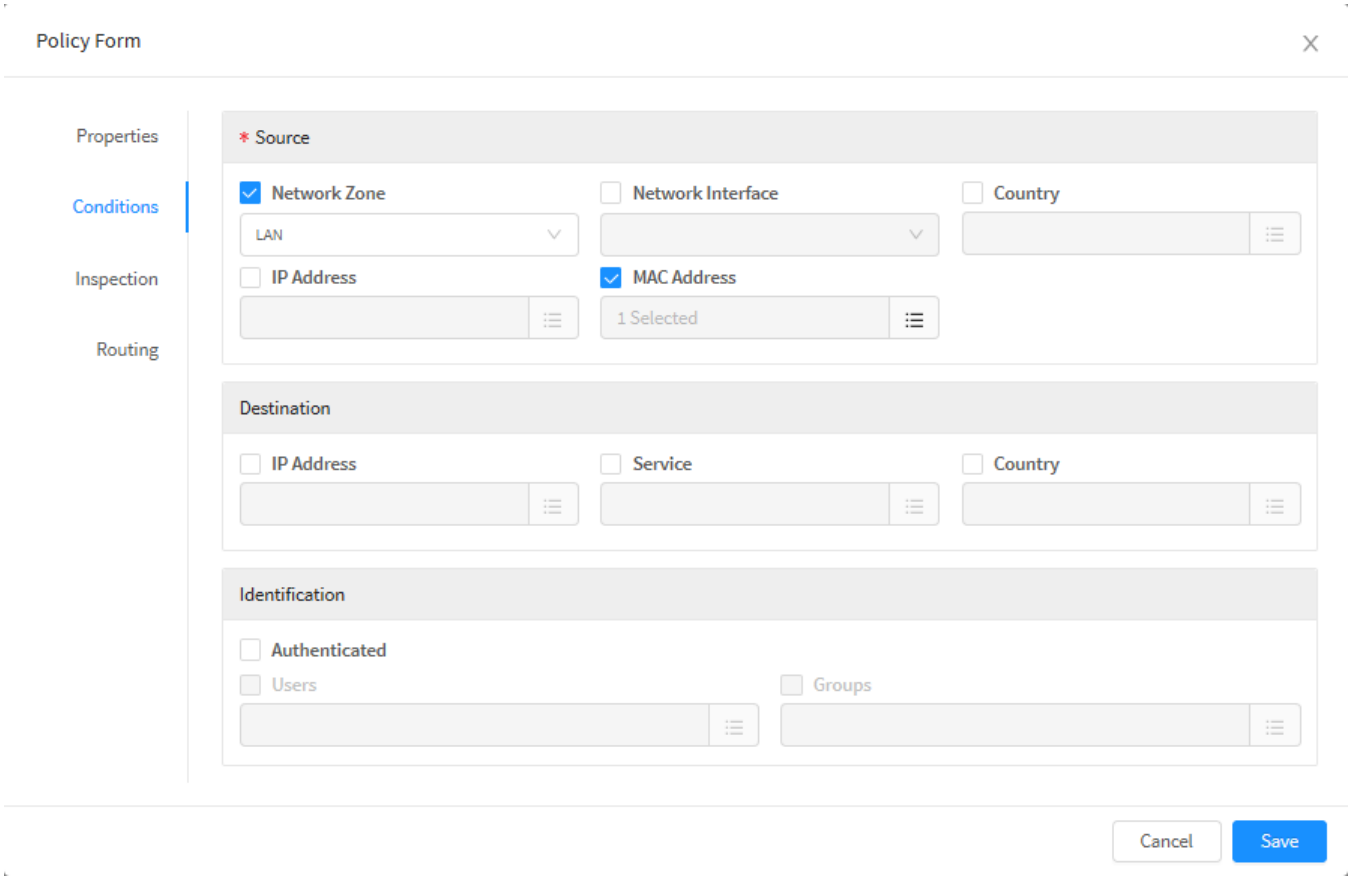


Policies - New Policy - Properties

- ***Name*:** Enter the Policy's name. Ex.: *NAT - Mac Address*;
- ***Description*:** Enter the Policy's description: Ex.: *NAT - Mac Address*;
- ***Action:*** *Allow*;
- ***Policy Group*:** *Default;*
- ***Traffic Logging:*** *Enabled.*

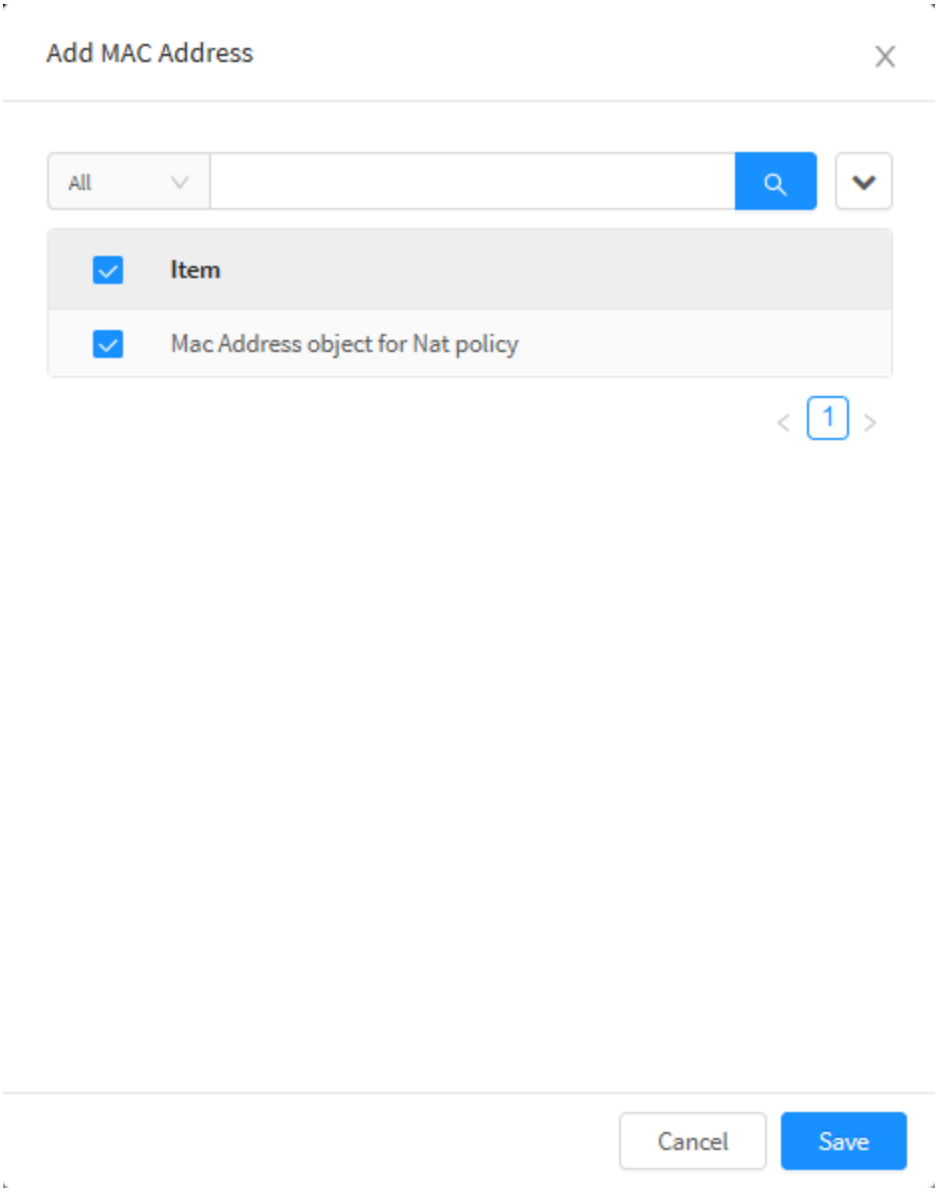
The remaining options can continue with the default values.

Select the "Conditions" option in the side menu.



Policies - New Policy - Conditions

- ***Network Zone*:** LAN;
- ***MAC Address*:** Select the physical address, previously added, as shown below:



Policies - New Policy - Add Mac Address

In this next step, it is important to note that:

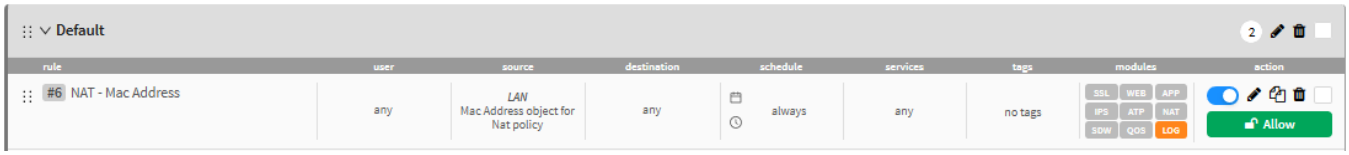
To complement the Mac Address, you must also configure one or more of the following options:

- ***Network Zone***;
- ***Network Interface***;
- ***IP Address***.

Continuing our example, we will simply select the "LAN" option in the "Network Zone" checkbox.

The rest of the options can continue as with the default values.

Click the **[** Save **]** button to save the policy.



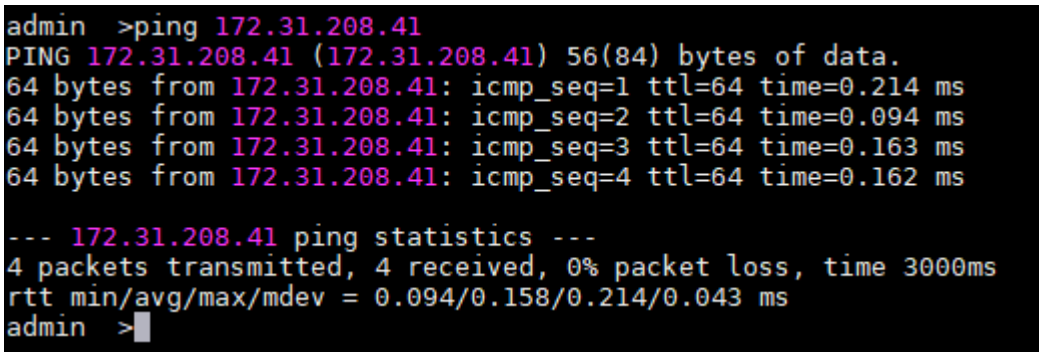
Policy - NAT - Mac Address

For more information on how to deal with policies, check the UTM - POLICIES chapter.

This concludes the creation of the NAT rule for Mac Address.

SD-WAN: Validation of the SD-WAN Configuration

One of the simplest tests to validate the functioning of the SD-WAN is to ping the 172.31.208.40 network to 172.31.208.41, as shown in the image below:

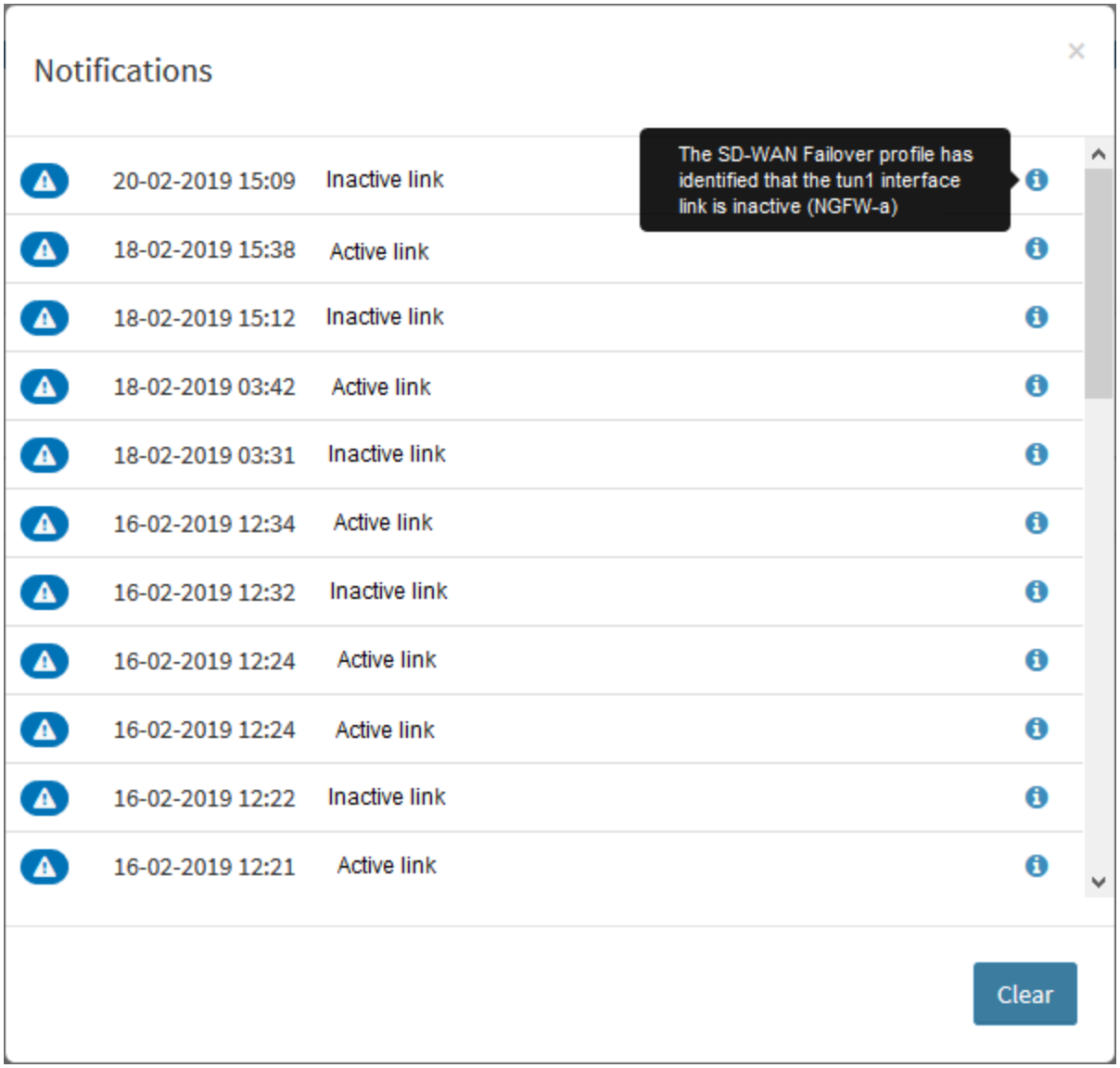


Ping validation

In addition, it is possible to purposely drop the link being used by SD-WAN in order to check if the Failover will assume the interface correctly.

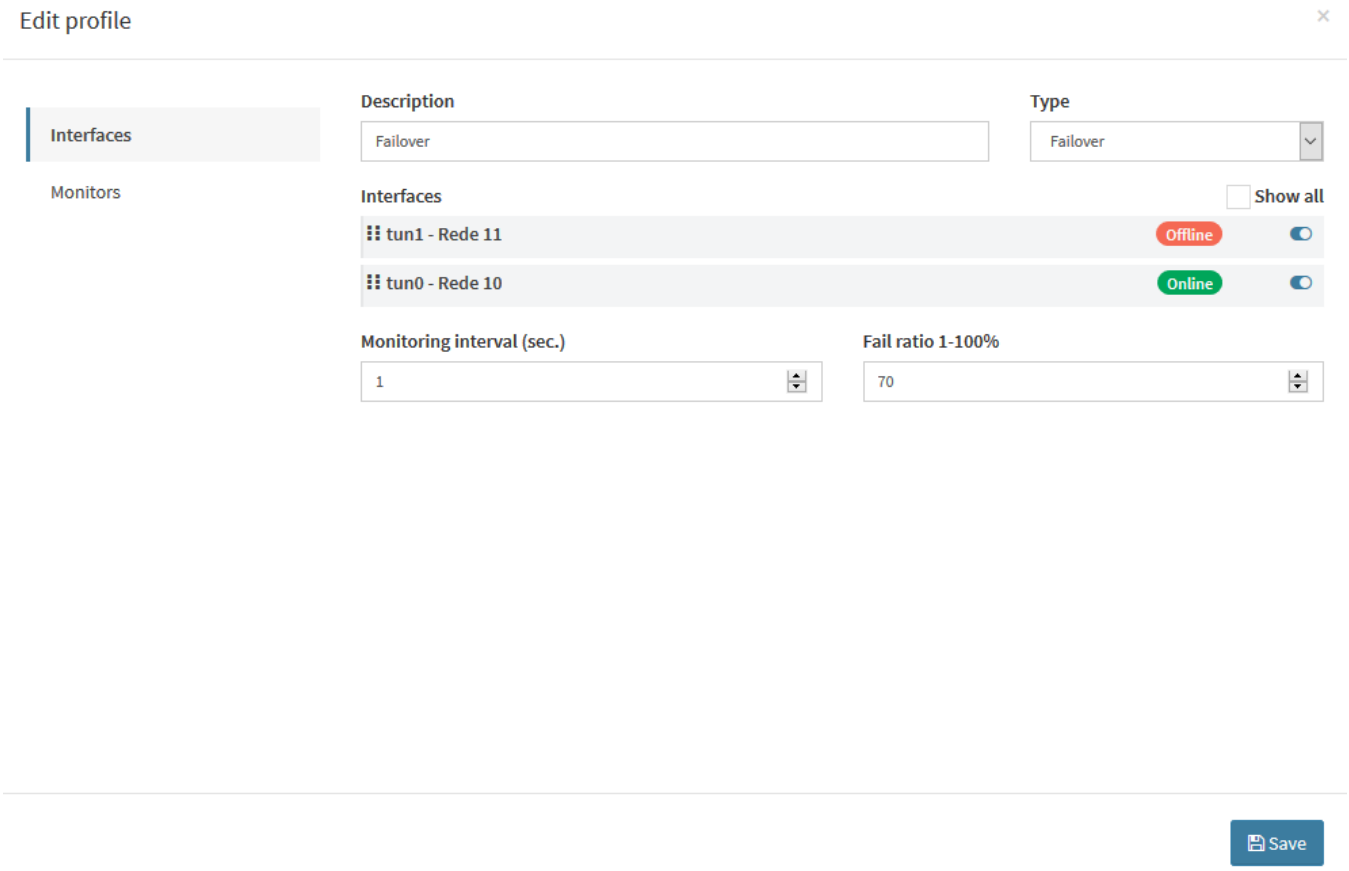
As previously configured, in the NGFW - HQ the interface with priority in SD-WAN is “tun1 - Network 11”, therefore, remove the network cable in order to interrupt the device's communication.

In the notifications window, you can see the alert displayed, as shown in the following image.



Notifications

In addition, go to **Services SD-WAN** and click on the edit button **[** **]**, you will see that the tunnel1 interface is ***offline*** **[** Offline **]**, as shown in the image below.



Example of an offline Interface

It is also possible to observe the effects of this change through the CLI interface using the "debug-sdwan -i results" command.

```
admin  >debug-sdwan -i results
date="2019-02-20 15:35:41" profile="Failover" dev="tun0" latency="0.275" jitter="0.085" packet_loss="0" bandwidth="1291.70" total_error="
0" total_error_percent="0" weight="100.00" status="on"
date="2019-02-20 15:35:41" profile="Failover" dev="tun1" latency="0" jitter="0" packet_loss="0" bandwidth="" total_error="6" total_error_
percent="100" weight="0" status="off"
date="2019-02-20 15:35:42" profile="Failover" dev="tun0" latency="0.295" jitter="0.14" packet_loss="0" bandwidth="1508.35" total_error="0
" total_error_percent="0" weight="100.00" status="on"
date="2019-02-20 15:35:42" profile="Failover" dev="tun1" latency="0" jitter="0" packet_loss="0" bandwidth="" total_error="6" total_error_
percent="100" weight="0" status="off"
```

CLI - Tunnel 1 offline

The “weight” parameter shows a value of 100% for tun0 and a value of 0% for tun1, so the tun0 interface has a higher priority than tun1, which proves that the “failover” worked correctly.

NGFW - Services - DHCP

The DHCP protocol manager *(RFC2131 IPv4 e RFC3315 IPv6)* acts on the application layer on standard *DHCP 67/68 UDP (IPv4)* and *546/547 UDP (IPv6)* ports. In a TCP / IP architecture network, every computer must have a different IP address. DHCP (Dynamic Host Configuration Protocol) is the protocol that provides a means to allocate these addresses dynamically.

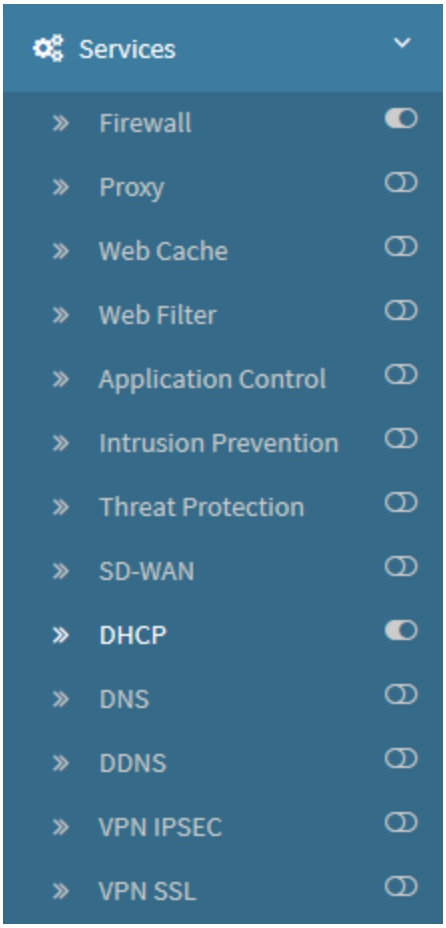
DHCP is responsible for distributing IP addresses and network configurations to your corporate environment. It is an efficient solution since, through it, the BLOCKBIT NGFW server distributes IP addresses as the devices on the network request a connection. It is important to note that, in addition to the IP address, it also assigns other parameters, such as: hostname, DNS, default route.

DHCP features

- Distribution of IP addresses per device / per server:
  - *Ethernet*;
  - *Vlan*;
  - *Mac Vlan* (virtual addressing device).
- Distribution of IP addresses by network / subnet
- Policies for IP address distribution;
- Support for Radius server authentication.
- Models:
  - Range distribution;
  - Distribution of static addresses (IP address reservation by MAC filter)
- Filters:
  - *MAC*;
  - *Host*.
- Parameters:
  - *Gateway*;
  - *DNS* Sufix;
  - Multiple DNS;
  - Multiple Wins;
  - TTL - Renewal time (lifetime)

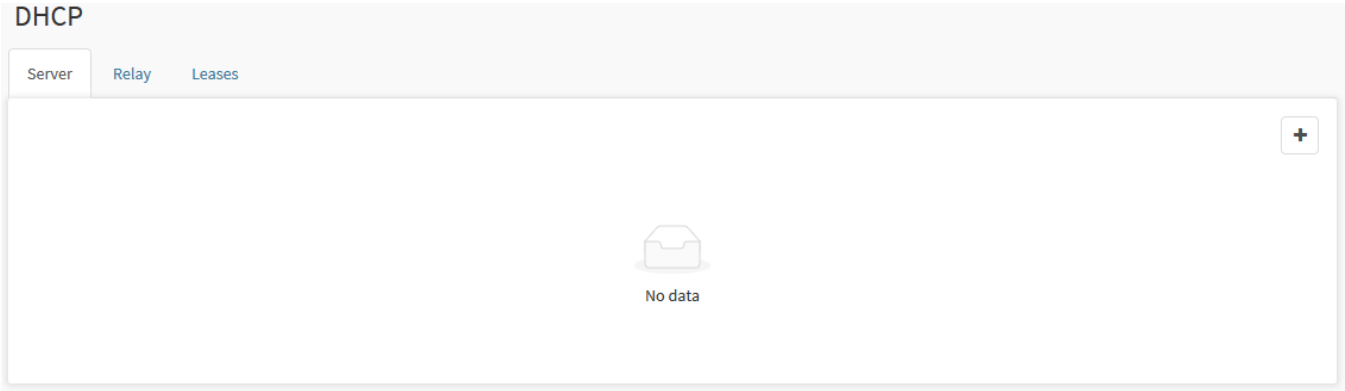
To use the DHCP service with IPv6, it is necessary to configure a Zone Protection rule releasing ports 546/547 UDP, allowing the Firewall to release the incoming traffic.

To access the DHCP screen, select the option as shown on the image below:



Services - DHCP

The following screen will appear:



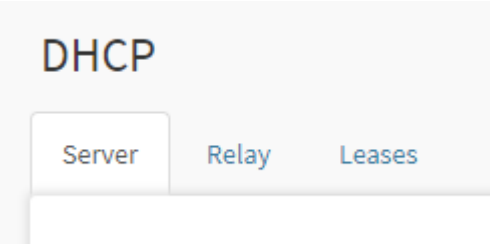
DHCP

Next, we will explain the other tabs of the *DHCP* interface:

- *Server IPv4*;
- Server IPv6;
- *Relay IPv4;*
- *Relay IPv6:*
- *Leases IPv4;*
- *Leases IPv6.*

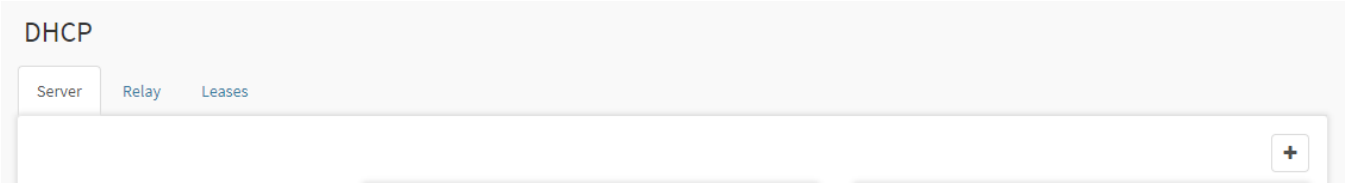
DHCP - Server IPv4 tab

To configure DHCP servers, select the correct tab:



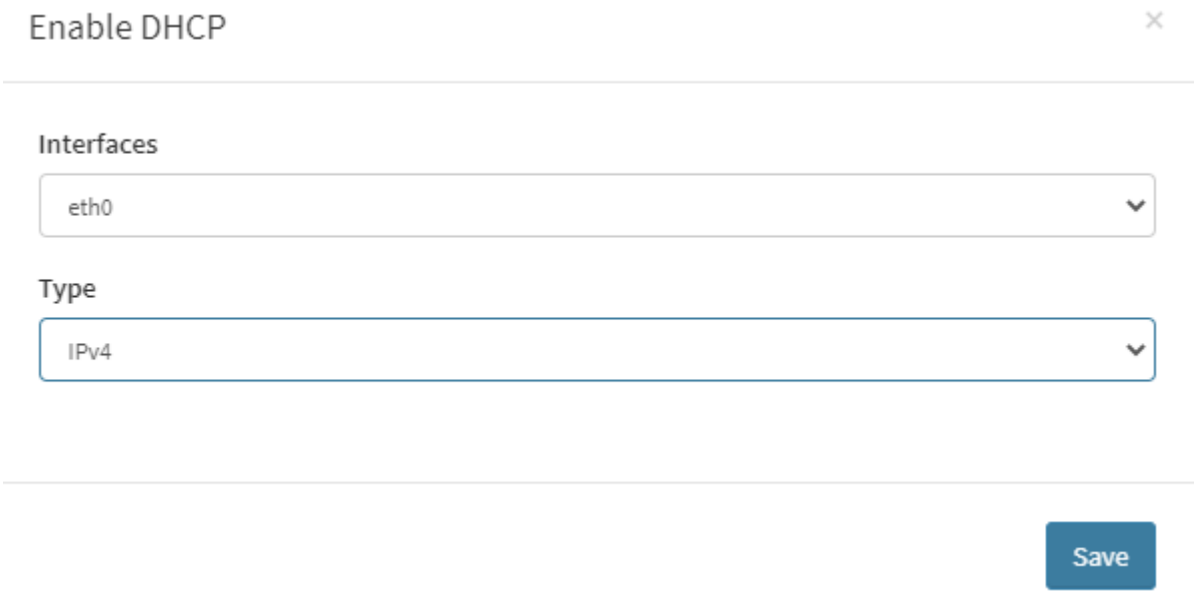
Server tab

The following screen will appear, as shown by the image below:



DHCP - Server

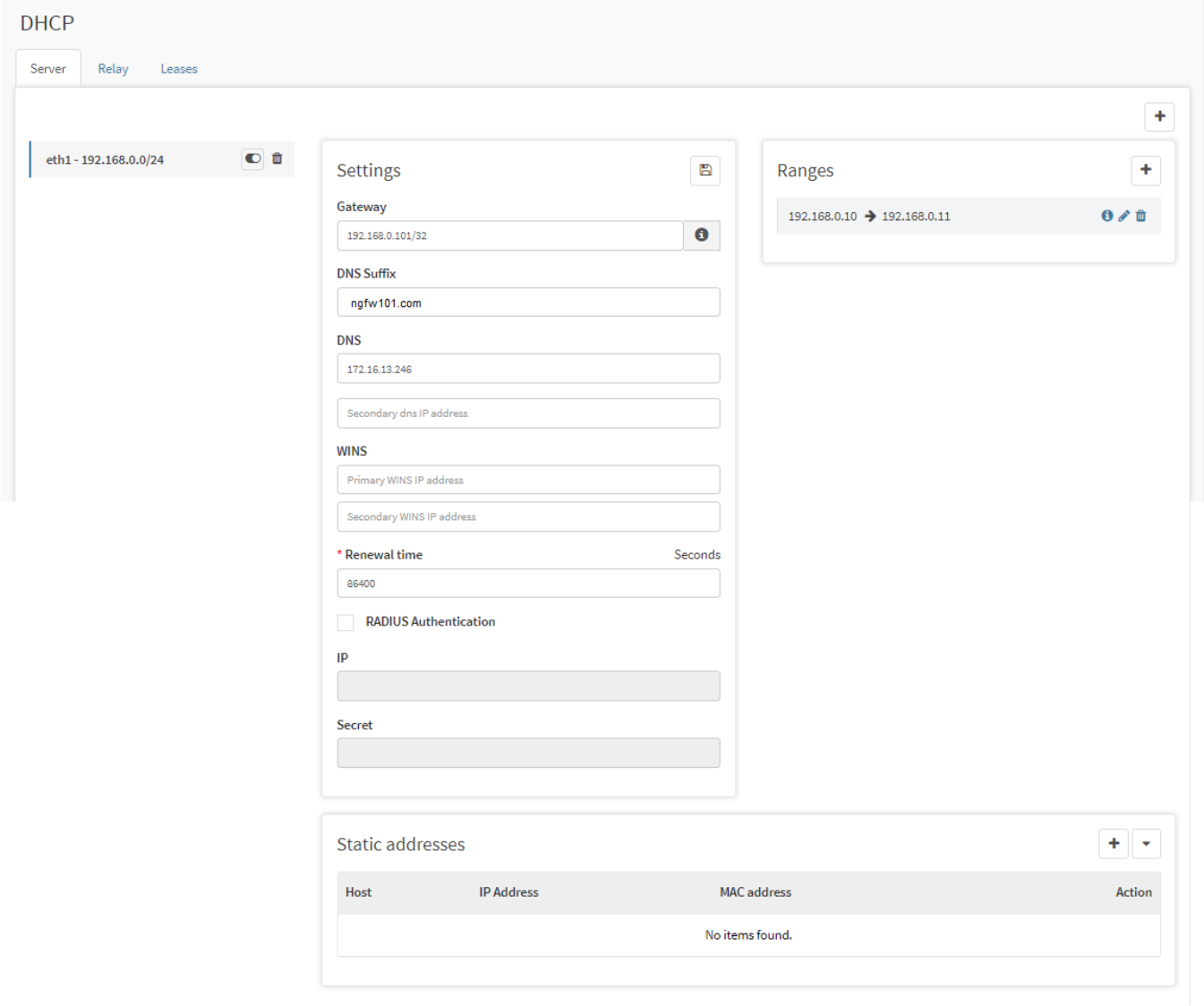
To add a DHCP policy, click **[ ]**, and select a Device for distributing IP addresses on the network. Please note that the default type will be IPv4.



DHCP - Server - Edit Host

After finishing the settings, click the [Save] button.

After saving the selection of the Device for distribution of IP addresses, the system returns the interface for configuring DHCP parameters.



DHCP Server

The DHCP server is responsible for distributing IP addresses and network configurations to your corporate environment. It is an efficient solution since, through it, the BLOCKBIT NGFW device distributes IP addresses as the network devices request a connection. It is important to note that, in addition to the IP address, it assigns other parameters, such as: host name, DNS and default route.

This tab consists on the following sections:

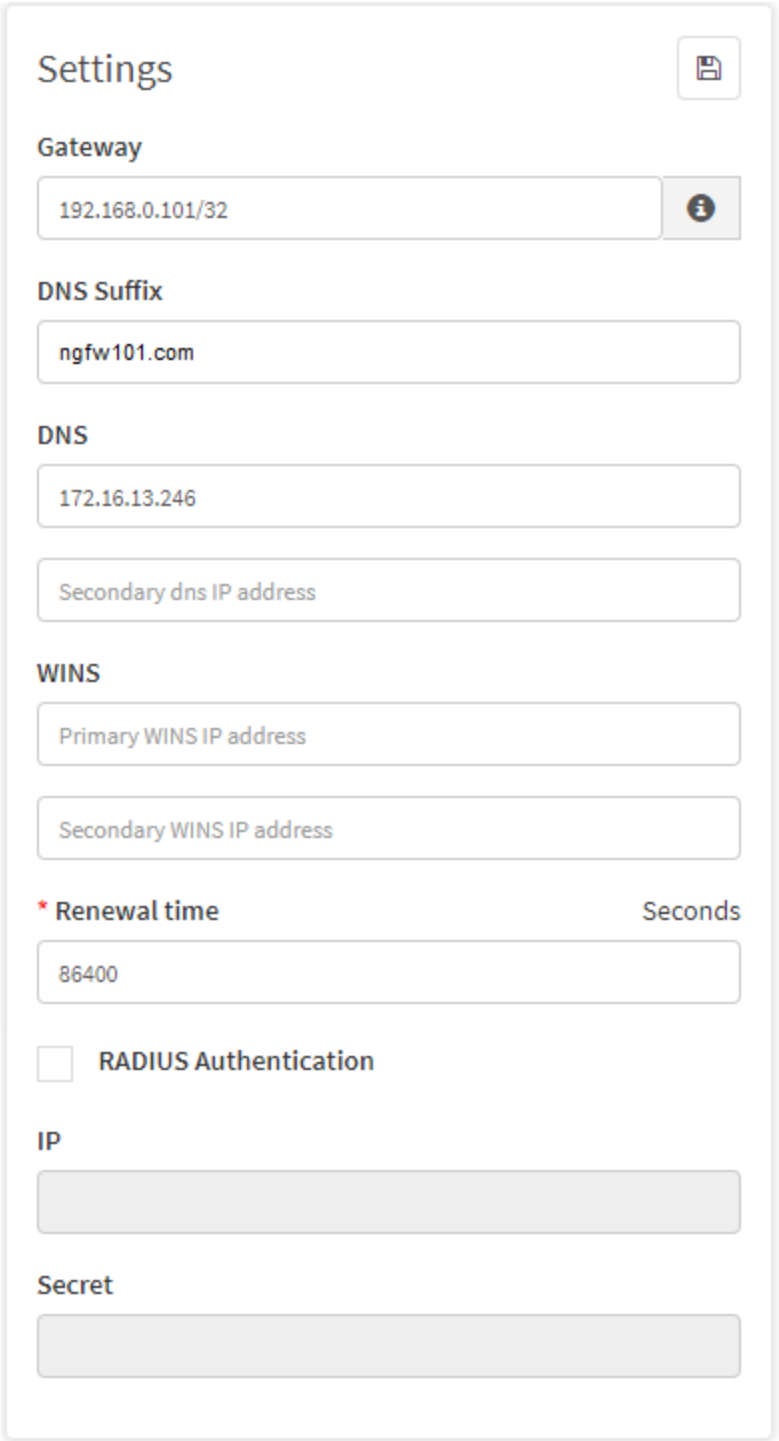
- *Settings*;
- *Ranges*;
- Radius;
- *Static Addresses*.

Next, we will analyze each one of these.

DHCP Server - Settings

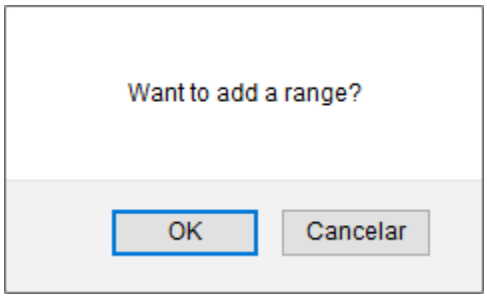
In order to configure the basic parameters for distributing the IP addresses, in the Settings panel configure the fields according to the form and the respective values and addresses that you want to distribute as valid for the DHCP service. Then click **[ ]**.

The Gateway address must be within the network or subnet range declared on the device selected for configuration.



DHCP - Settings

Next to [ ] the DHCP settings parameters, the service asks if you want to take advantage and define the Range of addresses that you will distribute:



DHCP - Adding a range

Clicking [OK] will automatically redirect you to the range settings interface.

Next, we will analyze the following sections:

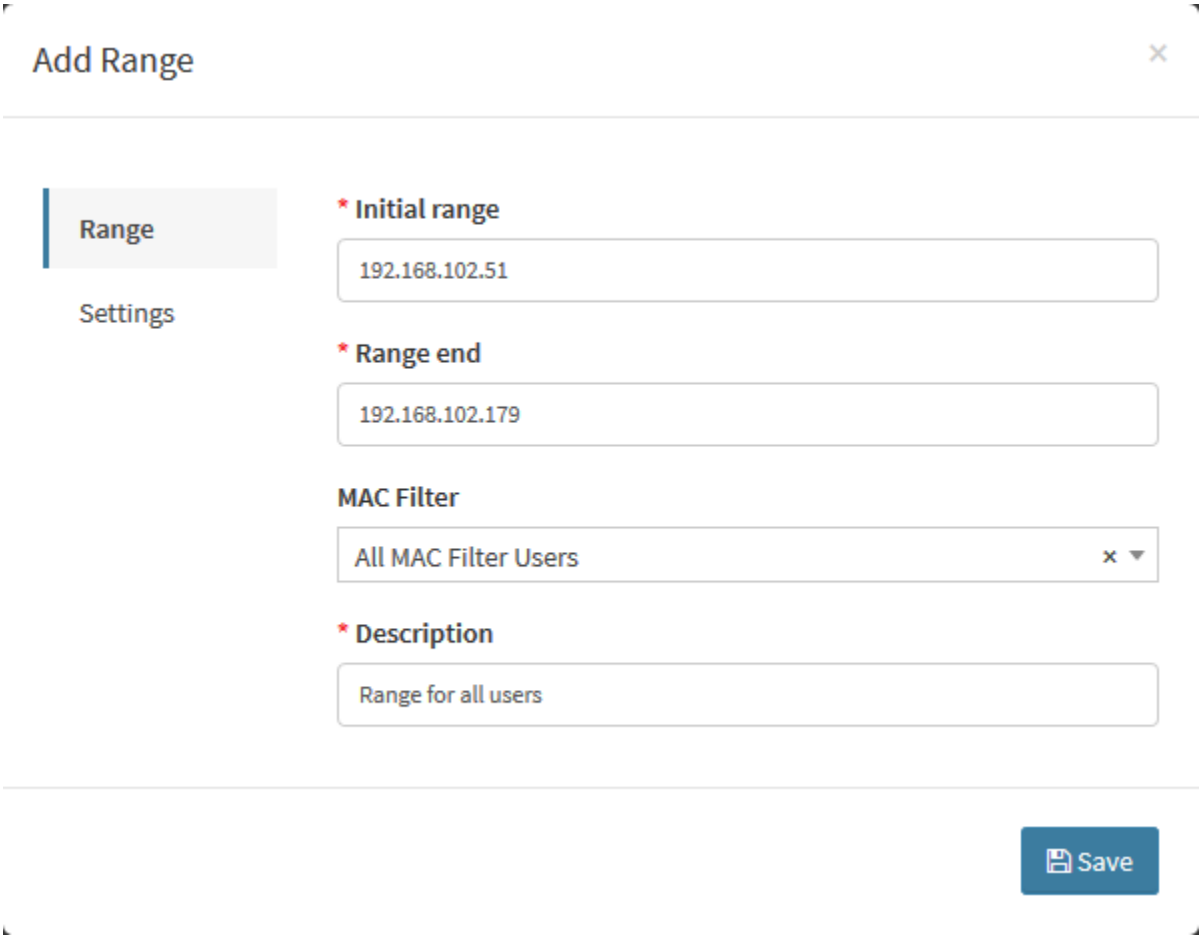
- Ranges;
- Radius;
- Static Address.

DHCP Server - Ranges

In this table you define what is the "range" or "range" of IP addresses that you want to distribute by the DHCP service.

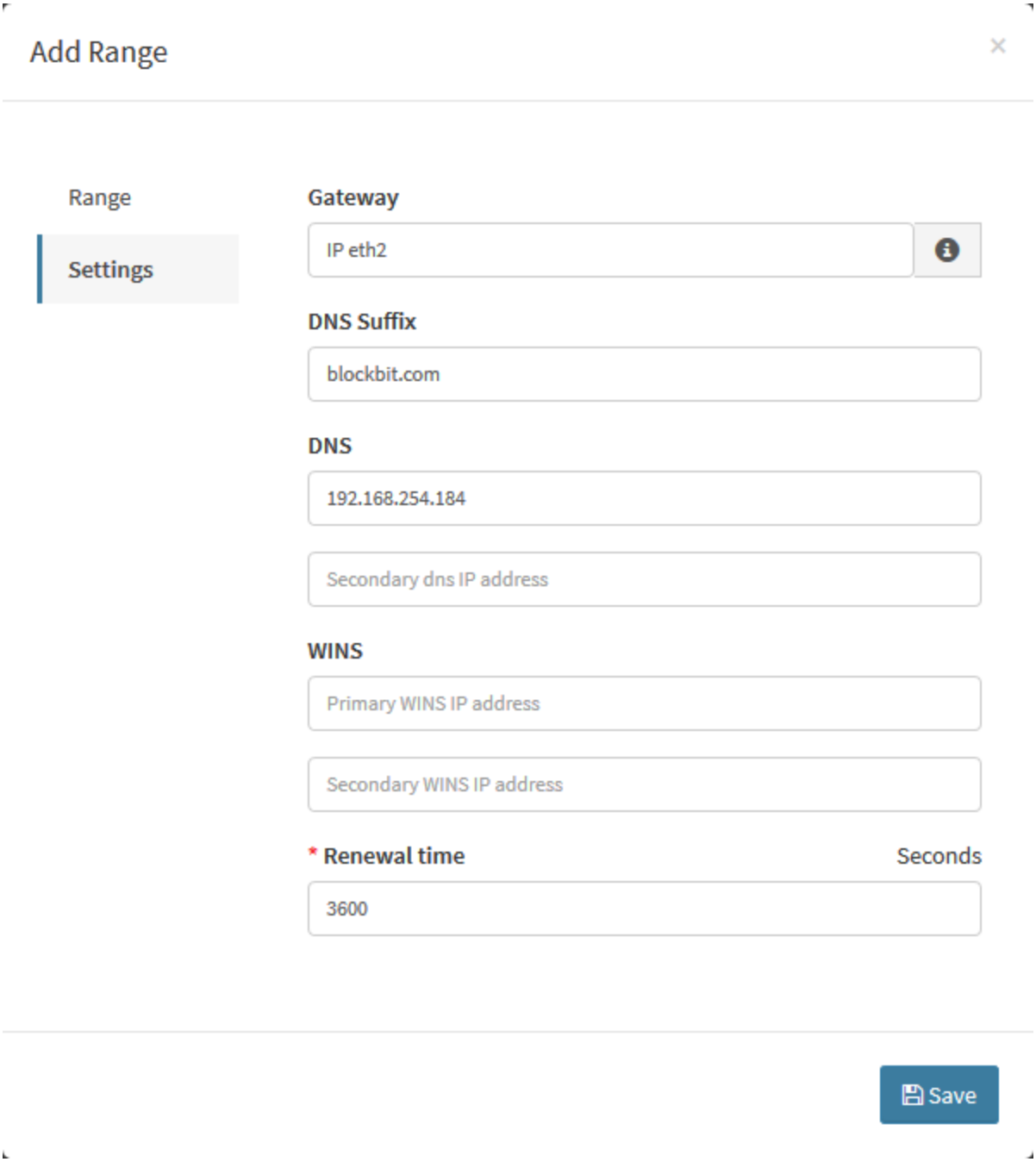
To add a range or IP address range, click [+], and configure the fields accordingly.

The “start and end” ranges of the range or range of IP addresses must be within the network or subnet range declared on the device selected for configuration.



Add Range - Range

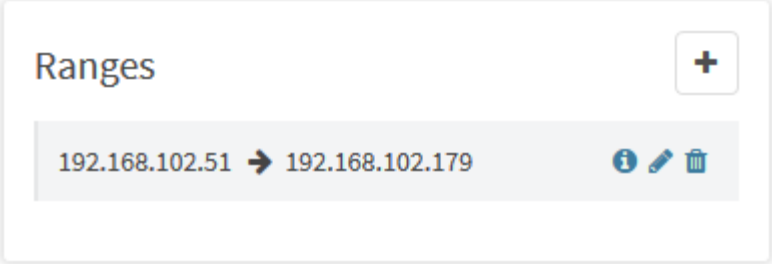
- ***Initial Range*:** Determines the address of the first IP in the range. Ex .: 192.168.254.51;
- ***Range end*:** Defines the address of the last IP in the range. Ex .: 192.168.254.179;
- ***MAC Filter*:** This feature has the function of distributing the IP addresses of the range (which was determined in the previous options) to all devices that have their MAC Address listed in this field;
- ***Description*:** A brief description defining the IP range.



Add Range - Settings

- ***Gateway*:** Determines the gateway of the range. Ex.: 192.168.254.190/32;
- ***DNS Suffix*:** Sets the DNS suffix of the range. Ex.: blockbit.com;
- ***DNS*:** Determines the primary and secondary DNS address. Ex.: 192.168.254.184;
- ***WINS*:** Sets the primary and secondary address of the WINS server;
- ***Renewal time*:** Time in seconds to renew the IP range. Ex.: 3600.

Finally, click the **[** Save **]** button to finish creating the range.



Ranges

Next, we will analyze the other two tabs:

- *Radius;*
- *Static Address.*

DHCP Server - Radius

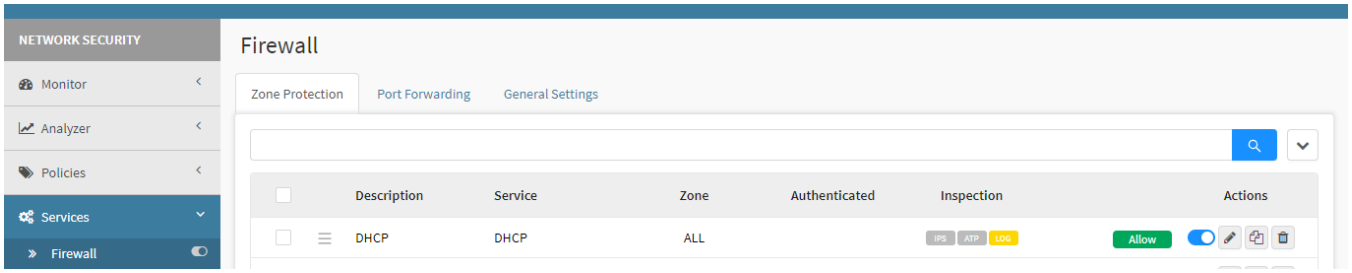
DHCP Authentication through RADIUS Server

In terms of authentication, it is also possible to configure a *RADIUS Server* for the users' validation.

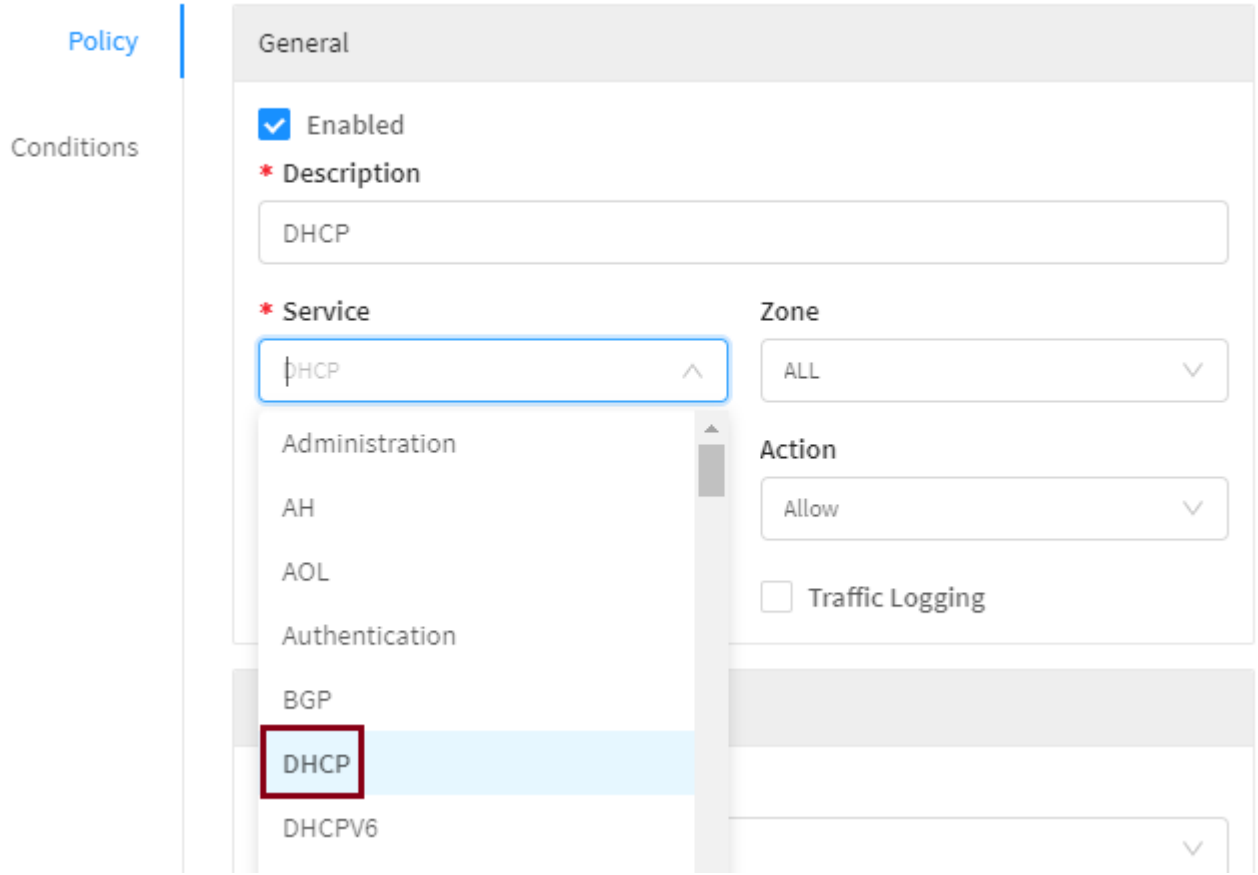
When the *DHCP + Radius* is activated, the Station requests an IP address to the *NGFW* in the *DHCP Service*. The *NGFW* consults if there is a static entry available for this Station (through MAC address), in positive case, it provides the reserved address; on the contrary, it does not.

Sumarizing, the *NGFW* consults the integrated *Radius Server*, in case the *Radius Server* authorizes, the *NGFW* assigns the IP address from the range; otherwise, it does not provide the IP address and the machine does not receive it, and remains without network access.

This option can be enabled in *Services*, *Firewall*, in the *Zone Protection* tab:

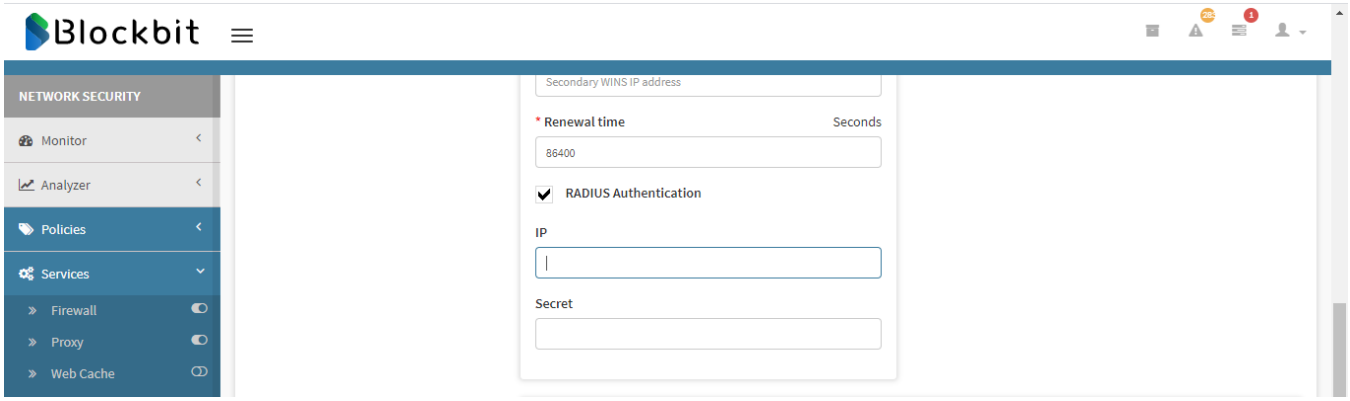


In order to do so, it is necessary to create a Policy in Zone Protection and select "DHCP" among the options:



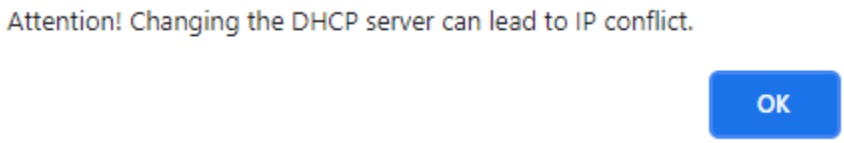
Authentication Service selection: *Services* *Firewall* *Zone Protection* Create[ ] or Edit[ ] Zone Protection.

Next, we should click in the *DHCP* option in Services and enable the Radius Authentication option:

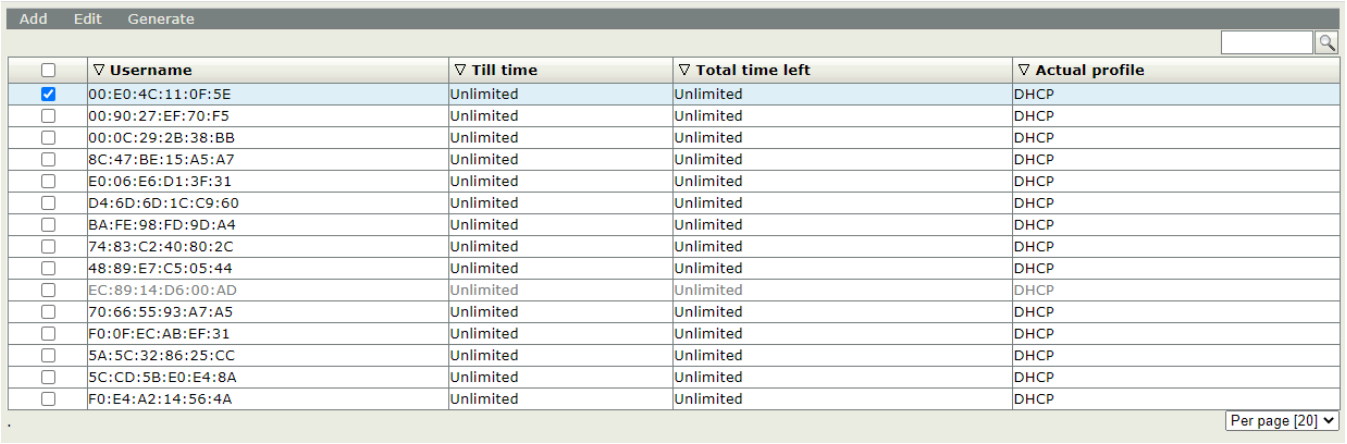


Radius Server user and password input screen.

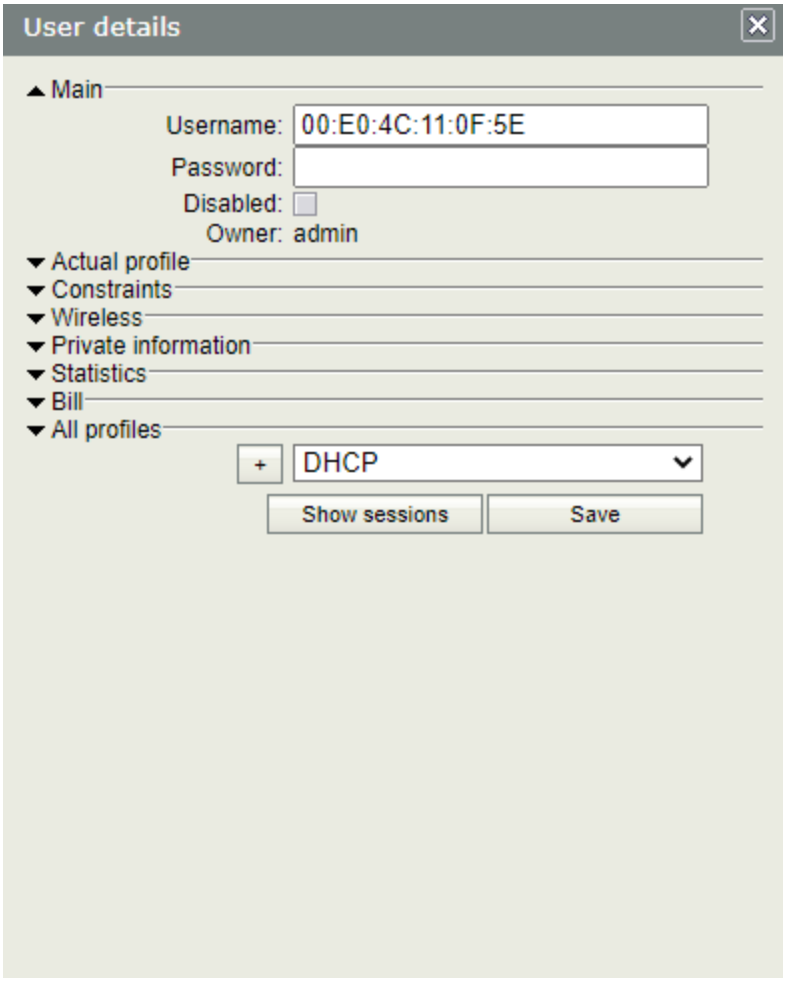
The following message will be displayed, just click "*OK*":



It is important to remember that the user in the Radius server (IP field) is the MAC address:



Example of a *Radius Server* main screen.



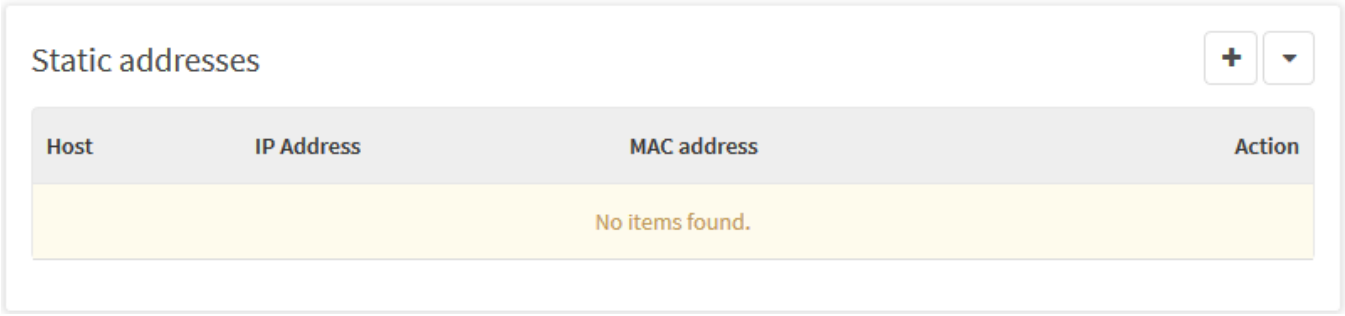
Example of the user details screen.

Finally, just insert the username and password and the authentication through *Radius Server* will be enabled.

- Static Address.

DHCP Server - Static Addresses

The service also distributes addresses in static mode, that is, setting the same “IP address” for a given “host”, based on its “MAC address”.



DHCP - Static Address

To add the IP address distribution rules in static mode, by Host / Mac Address, click **[ ]** and configure it according to the definition of Policies for distribution of fixed addresses on the network. Then click **[ ].**

Ex.1:

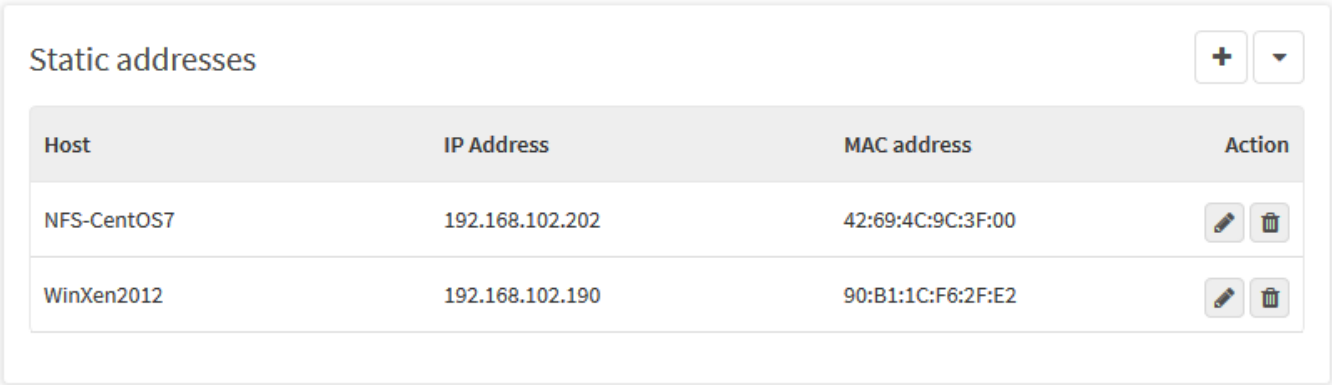
- *Host: WinXen2012;*
- *IP Address: 192.168.254.184;*
- *MAC Address: 90:B1:1C:F6:2F:E2.*

DHCP reserve static address example 1

Ex.2:

- *Host: NFS_CentOS7;*
- *IP Address: 192.168.254.202;*
- *MAC Address: 42:69:4C:3F:00.*

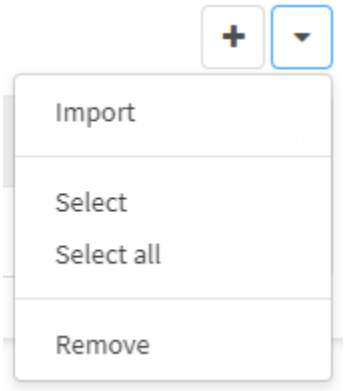
DHCP reserve static address example 2



Static addresses definition

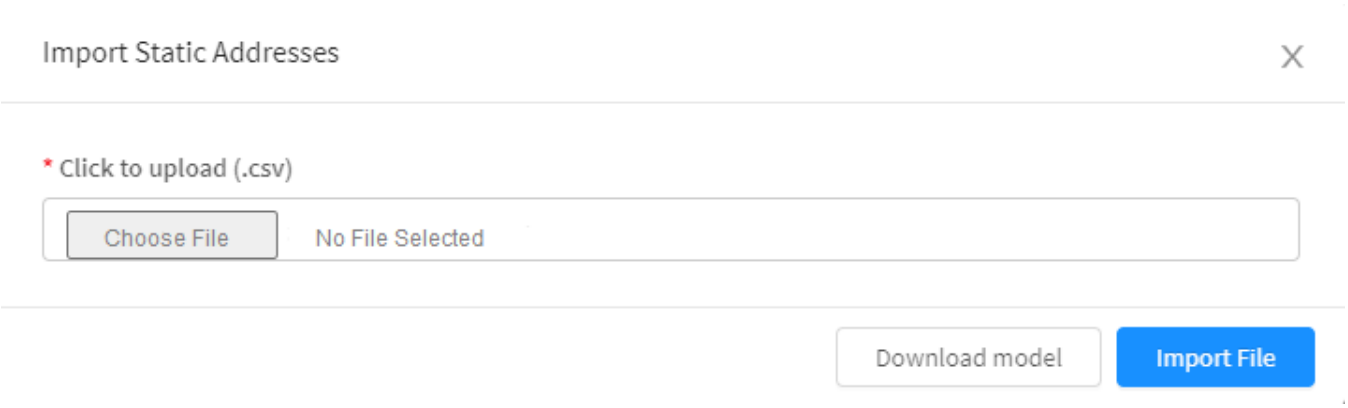
How to import multiple hosts

To import multiple hosts, click[ ]:



Import multiple hosts

In Import, we have the following screen:



In "Download Model", there is a model on how the document containing multiple Hosts should be written. Just insert the Hosts' information according to the model, save and then click "Select File". Through the navigation button select the file containing the Hosts' information and click Import.

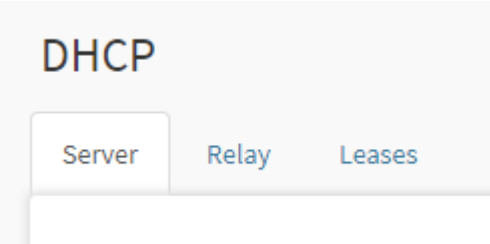
To enable automatic distribution of addresses declared in the DHCP service, click enable **[**  **].**

Now we are moving on to the next tabs:

- Relay IPv4;
- Relay IPv6;
- Leases IPv4;
- Leases IPv6.

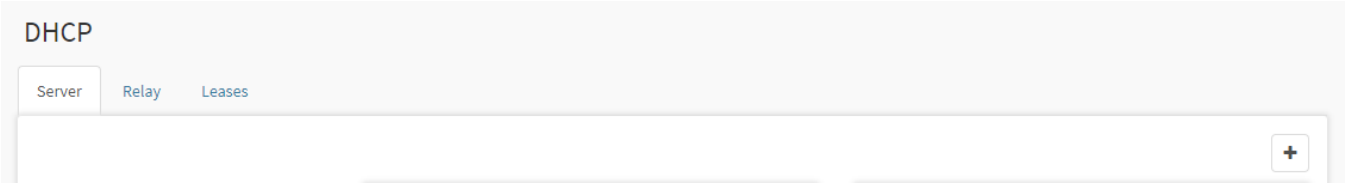
DHCP - Server IPv6 tab

To configure the DHCP servers, select the correct tab:



Server tab

The following screen will appear, as shown by the image below:



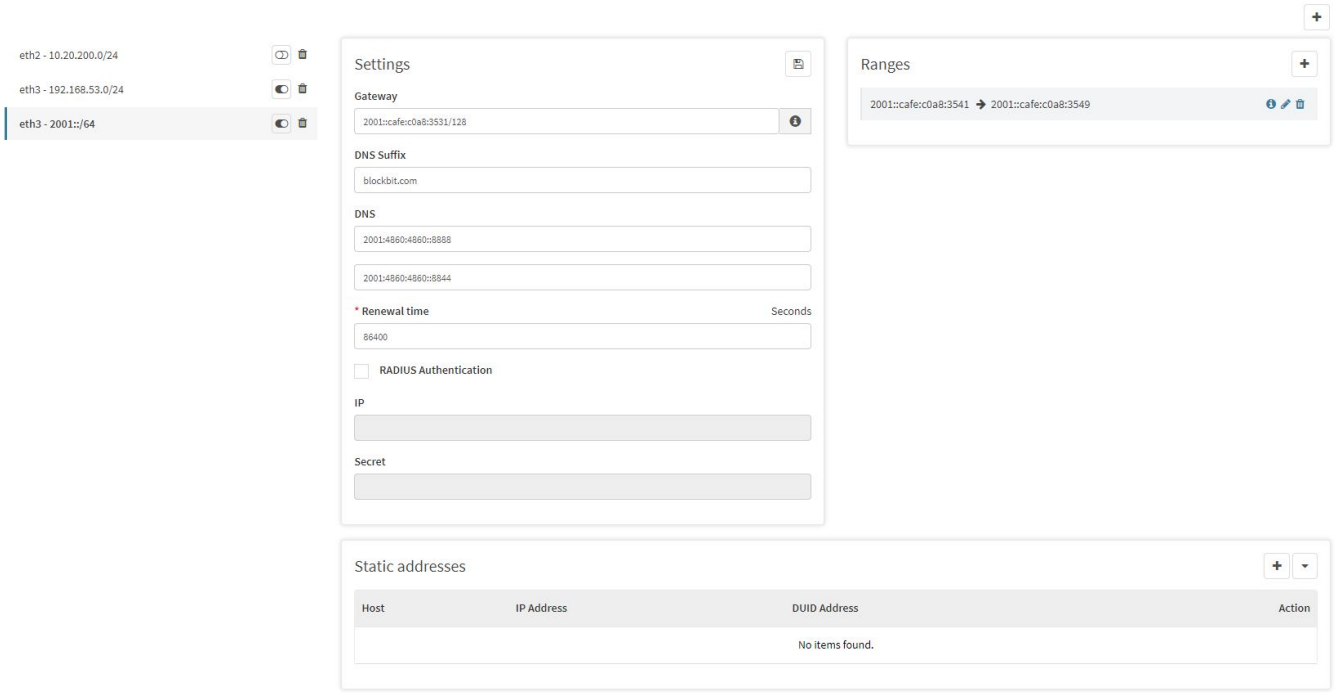
DHCP - Server

To add a DHCP Policy, click **[ ]**, and select a Device for distributing IP addresses on the network. Please note that the default type will be IPv4. Open the *type list* and select IPv6.

DHCP - Server - Edit Host

After finishing the settings, click the [Save] button.

After saving the selection of the Device for distribution of IP addresses, the system returns the interface for configuring DHCP parameters.



DHCP Server

The DHCP server is responsible for distributing IP addresses and network configurations to your corporate environment. It is an efficient solution since, through it, the BLOCKBIT NGFW device distributes IP addresses as the network devices request a connection. It is important to note that, in addition to the IP address, it assigns other parameters, such as: host name, DNS and default route.

This tab consists on the following sections:

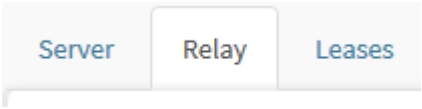
- *Settings*;
- *Ranges*;
- Radius;
- *Static Addresses*.

DHCP - Relay IPv4 tab

DHCP Relay acts as a proxy that receives a DHCP request and relays it to a real DHCP server. This allows multiple segmented networks on separate buses to centralize DHCP requests via the Blockbit NGFW.

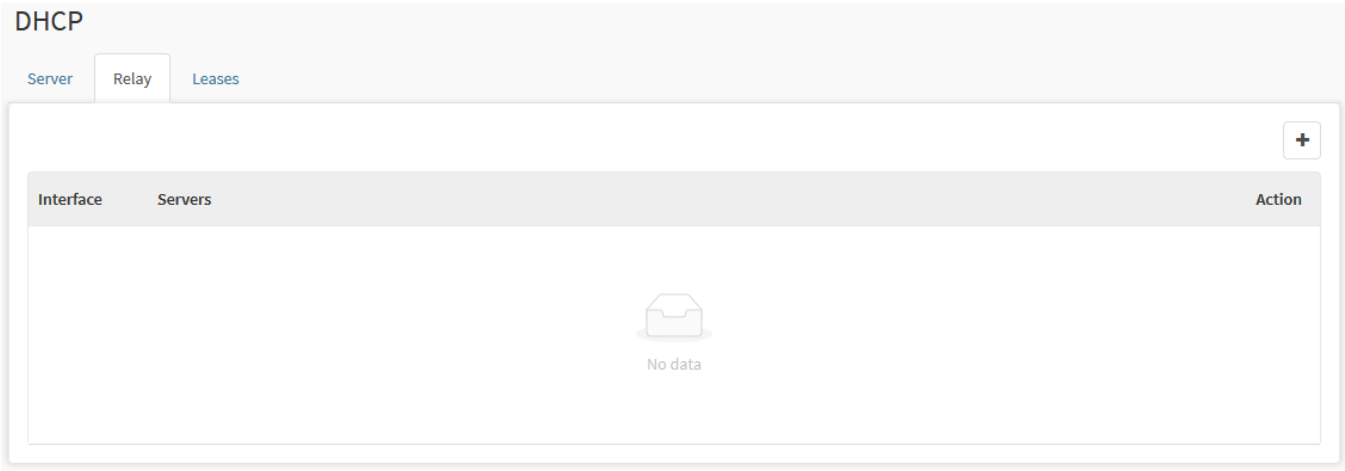
This feature allows requests sent by DHCP clients via broadcast to be forwarded and delivered to the DHCP server located on another segment of the network.

Click on the "Relay" tab, as shown below.



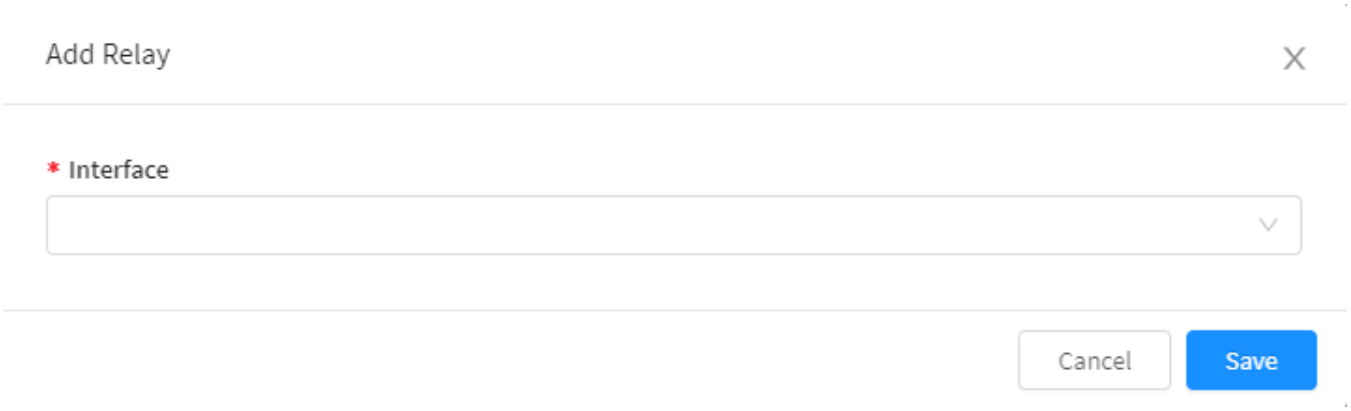
Relay tab

The following screen will appear:

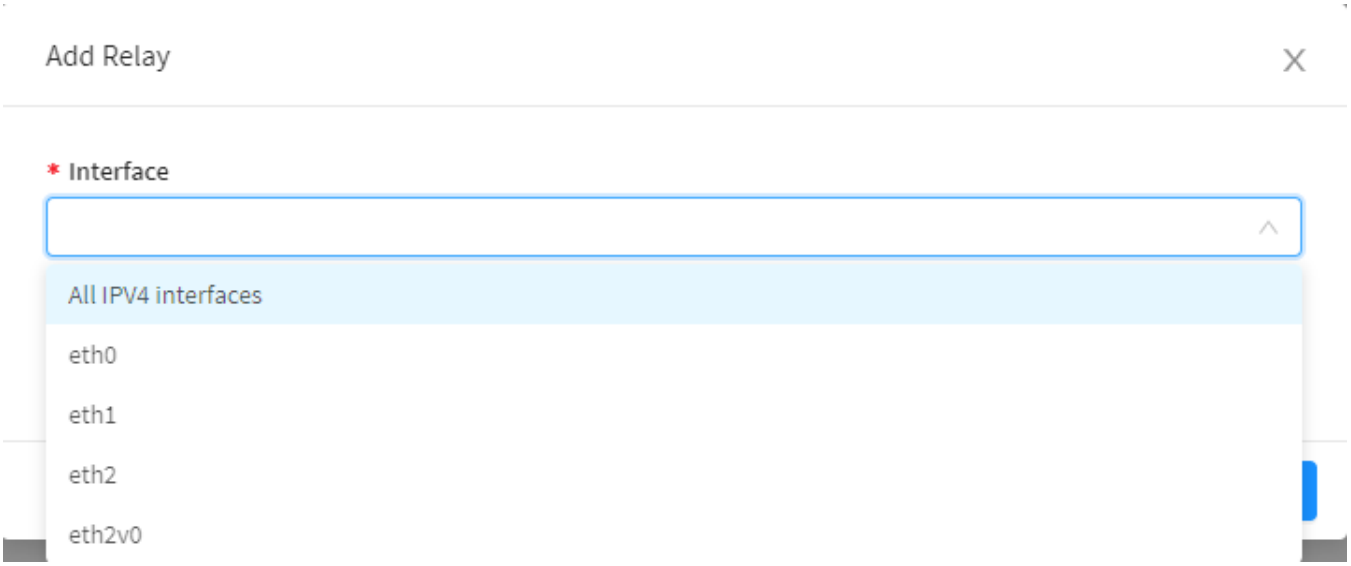


DHCP - Relay tab

To add a relay configuration, click **[**  **]** and select the Network Interface that the service will load from and the IPv4 Servers IP address of the DHCP service.



DHCP - Relay tab - Add Relay



DHCP - Relay tab - Interfaces

It's also possible to select all the available interfaces, or just a single one.

The IPv4 field accepts unique address objects, for more information check this page.
The user must create a DHCP Relay configuration for the input interface of host requests (LAN interface) and a different configuration for the output interface (DHCP server as destination) that will receive forwarding requests from hosts.

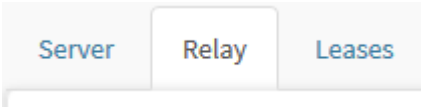
Then click [Save] to complete the changes.

DHCP - Relay IPv6 tab

DHCP Relay *(RFC3315)* acts as a proxy that receives a DHCP request and relays it to a real DHCP server. This allows multiple segmented networks on separate buses to centralize DHCP requests via Blockbit NGFW.

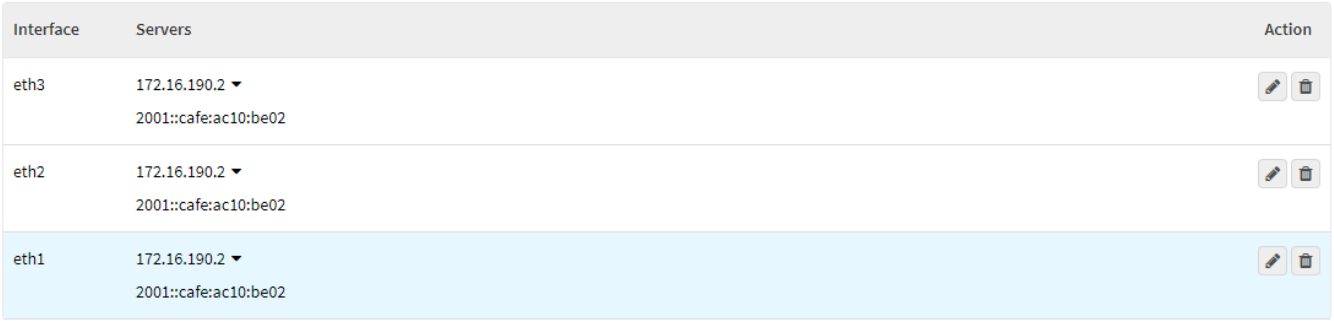
This feature allows requests sent by DHCP clients via broadcast to be forwarded and delivered to the DHCP server located on another segment of the network.

Click on the "Relay" tab, as shown below.



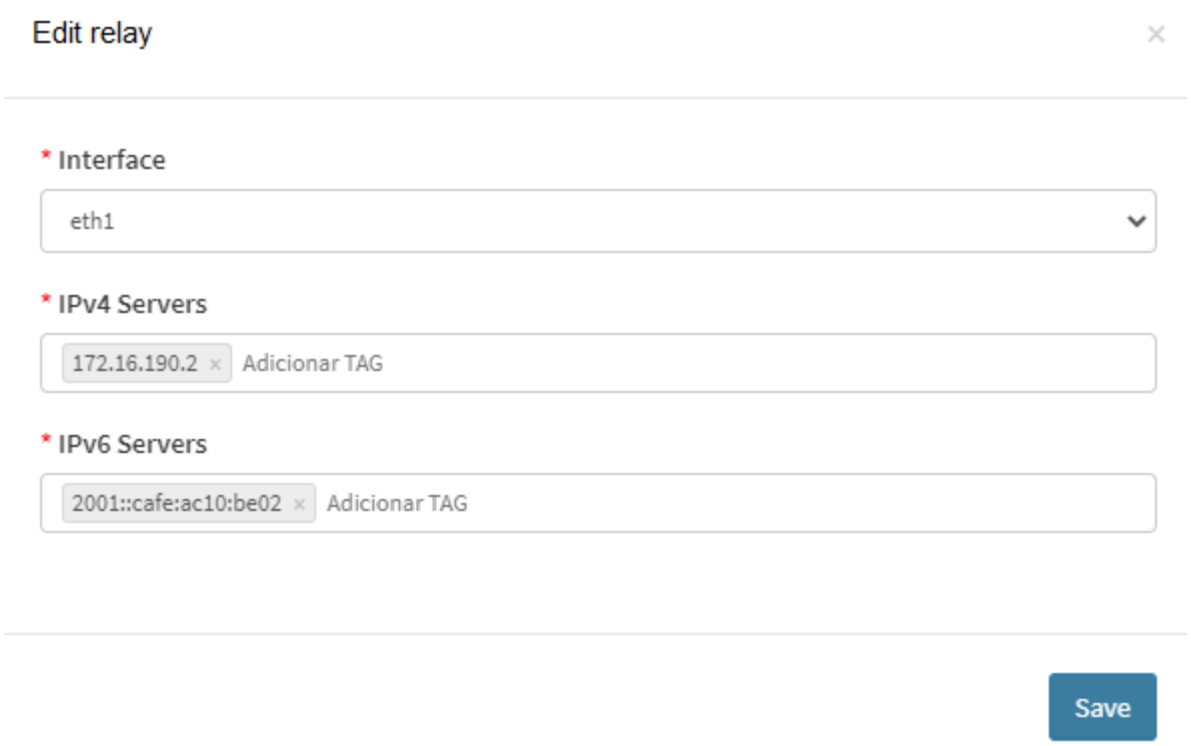
Relay tab

The following screen will appear, as shown by the image below:



DHCP - Relay tab

To add a relay configuration, click **[**  **]** and select the Network Interface that the service will be loaded from and the IPv4 Servers IP address of the DHCP service.



DHCP - Relay tab - Add Relay

The IPv6 field accepts unique address objects, for more information check this page.
The user must create a DHCP Relay configuration for the input interface of host requests (LAN interface) and another configuration for the output interface (DHCP server as destination) that will receive forwarding requests from hosts.

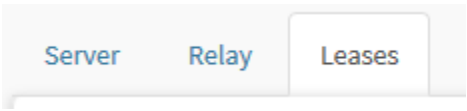
Then click [

] to complete the changes.

DHCP - Leases IPv4 tab

This feature allows the administrator to view the Hostnames, Mac Address, Users, IP addresses and the Date of receipt of the IP distributed by the DHCP server of the Blockbit NGFW. It is also possible to manually erase a *Lease,* in the graphic interface, by clicking on **[ ],** allowing the deletion of an already assigned IP address, releasing this IP address before the DHCP service's timeout.

To view this window, click on the "*Leases*" tab, as shown below.



Leases tab

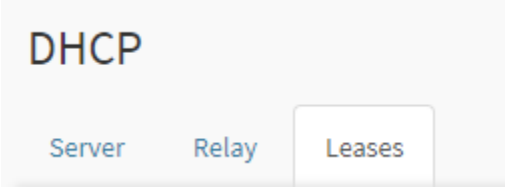
The following screen will appear:

DHCP - Leases

DHCP - Leases IPv6 tab

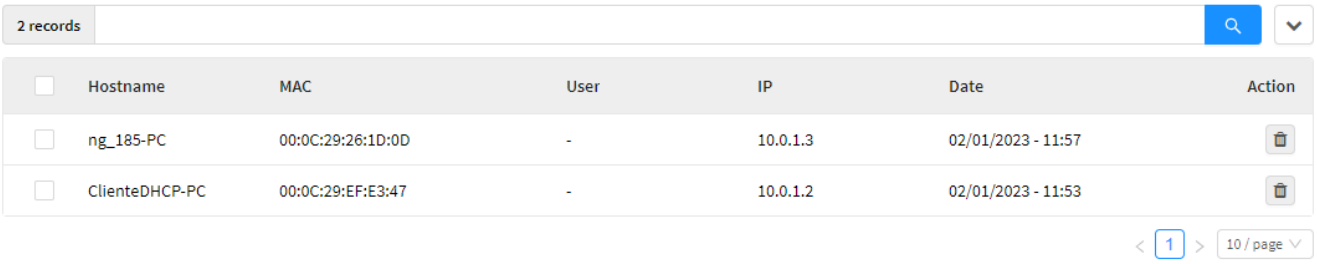
This feature allows the administrator to view the Hostnames, Mac Address, Users, IP addresses and the Date of receipt of the IP distributed by the DHCP server of Blockbit NGFW. It is also possible to manually erase a *Lease,* in the graphic interface, by clicking on **[ ],** allowing the deletion of an already assigned IP address, releasing this IP address before the DHCP service's timeout.

To view this window, click on the "*Leases*" tab, as shown below.



Leases tab

The following screen will appear:



DHCP - Leases

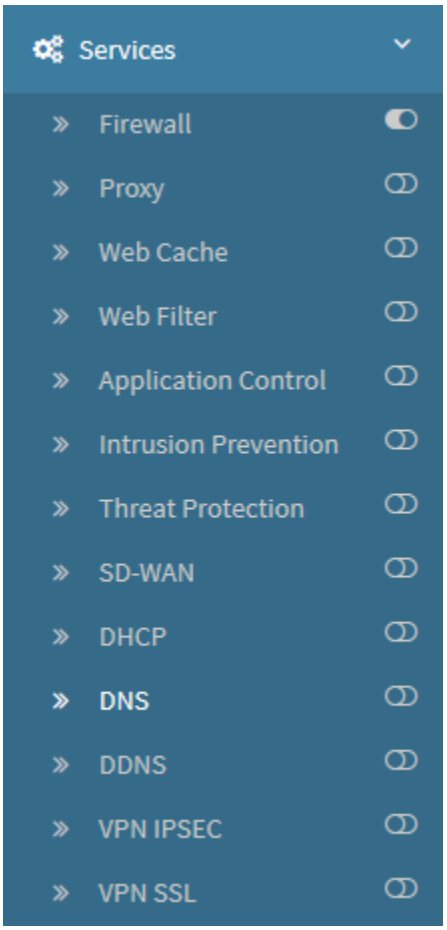
UTM - Services - DNS

The DNS (Domain Name System) Service is responsible for providing the “domain name translation” feature to their respective IP addresses.

The Blockbit NGFW provides the DNS redirection service to other recursive DNS servers, responsible for receiving DNS queries from local DNS clients and querying remote or external servers, in order to obtain responses to queries made from any domain and respond to local clients.

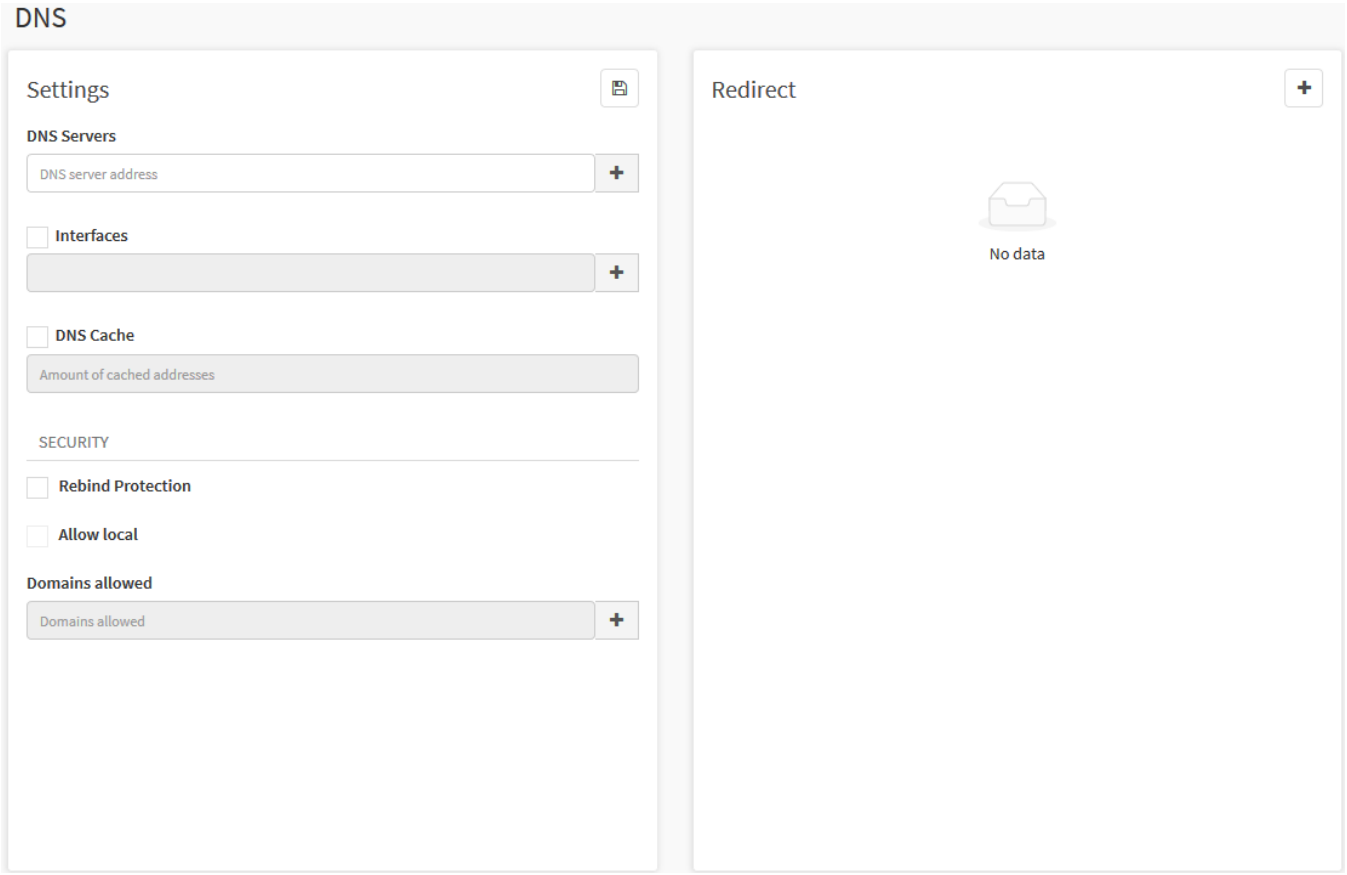
The DNS service is integrated with the Caching feature, handles queries from DNS clients and stores the response in its local cache for a certain time allowed by the TTL of the respective records of the queried domains. The Cache is used as a source for the next orders, in order to optimize the search time for the next domain requests already searched.

To access this screen, just select the “DNS” option.



Services - DNS

The screen below will appear:



Services - DNS interface

The DNS interface is divided into the panels:

- *Settings*;
- *Redirect*.

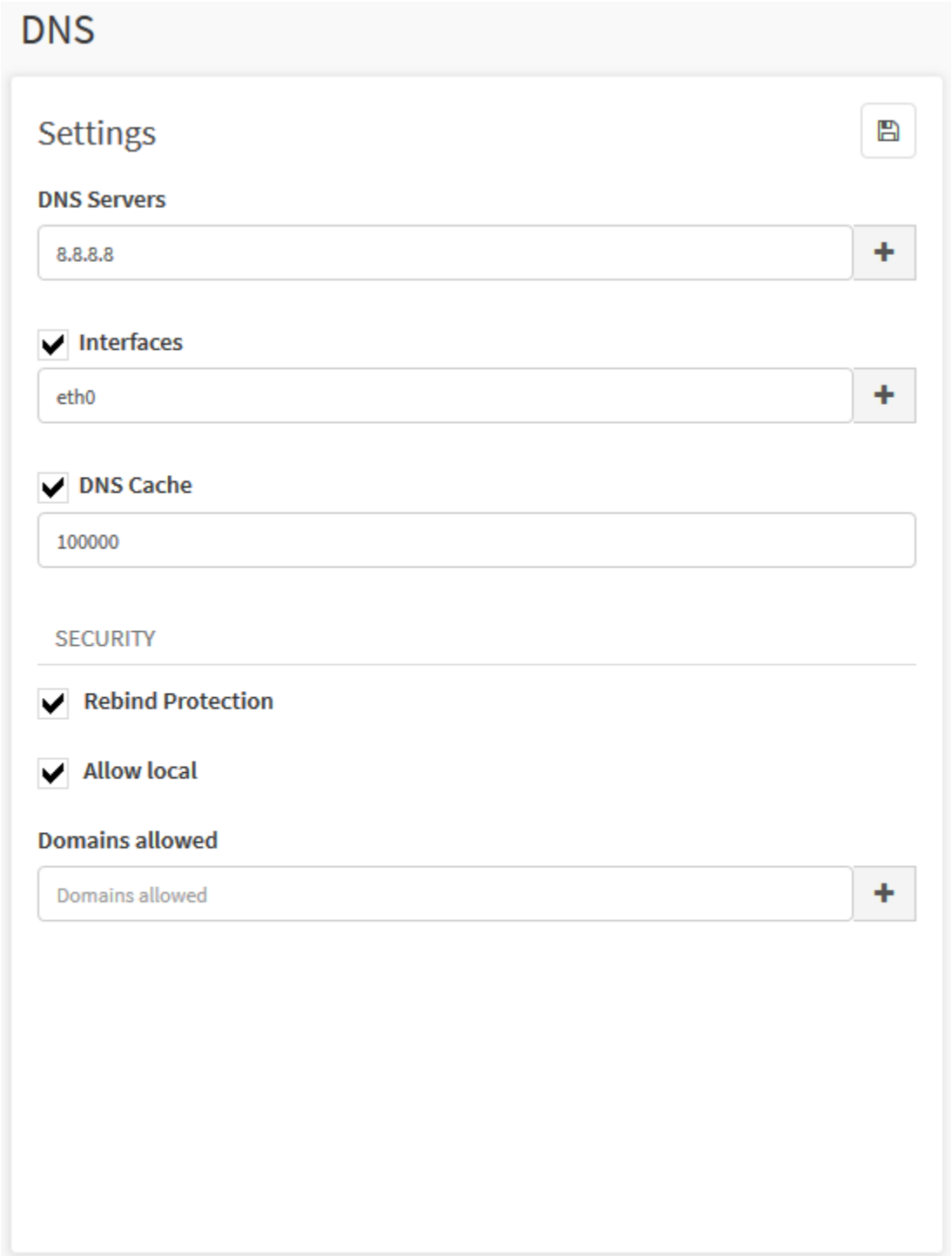
Next we will analyze the components of this screen.

DNS - Settings

In this area you configure the DNS redirection service to another "remote" or "external" Recursive DNS server. You can also select to enable local caching storage for the searched addresses.

- Recursive queries:
  - Multiple servers;
  - Distributed and balanced mode;
  - Listen by device.

In the **[*Settings*]** box, configure the fields according to the form for DNS forwarding to another recursive DNS server.



DNS - Settings

Below we will specify some fields:

- ***DNS Servers:*** *Inform the remote DNS server to which DNS queries will be forwarded. If you want to add other DNS servers, click the [ ] button, after adding other servers, click [ ] to remove them*;
- ***Interface [ ]:*** *Selection of the network interface that will be activated for "Listen" mode. Which allows to make recursive DNS requests from this source. If you want to add other interfaces, click the [ ] button, after adding other interfaces, click [ ] to remove them*;
- ***DNS Cache [ ]:*** *Number of cache addresses for storage in "local caching"*;
- ***Rebind Protection [ ]:*** *This option disables the query of name server addresses that are in the private IP ranges in order to stop attacks in which a browser behind a firewall is used to investigate machines on the local network*. Through this feature, the NGFW effectively filters DNS responses that pass through the firewall, blocking unwanted local addresses and rejecting the resolution of external names tied to internal IPs;

The Rebind Protection option is especially effective against DNS Rebinding. This is a type of attack that aims to tamper with the DNS service and ignore the policy of the same origin of the browsers, causing communication to be made with an undesirable server. Basically, this is done using a DNS server configured with a very short TTL in order to stop the creation of cache and enable the execution of a query that resolves to an unwanted alternative IP, usually this being a local or private IP.

- ***Allowlocal [ ]:*** *Exempts checks for localhost. This range of addresses is returned by malicious servers in real time, so blocking can disable these services*;
- ***Domains allowed:*** *Detects and blocks DNS reconnection binding on queries to those domains. If you want to add other domains, click the [ ] button, after adding other domains, click [ ] to remove them*;

After you have made the settings, click **[ ]** to save them.

After saving, for the changes to take effect it will be necessary to access the command queue **[ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures the DNS will have been successfully configured.

DNS - Redirect

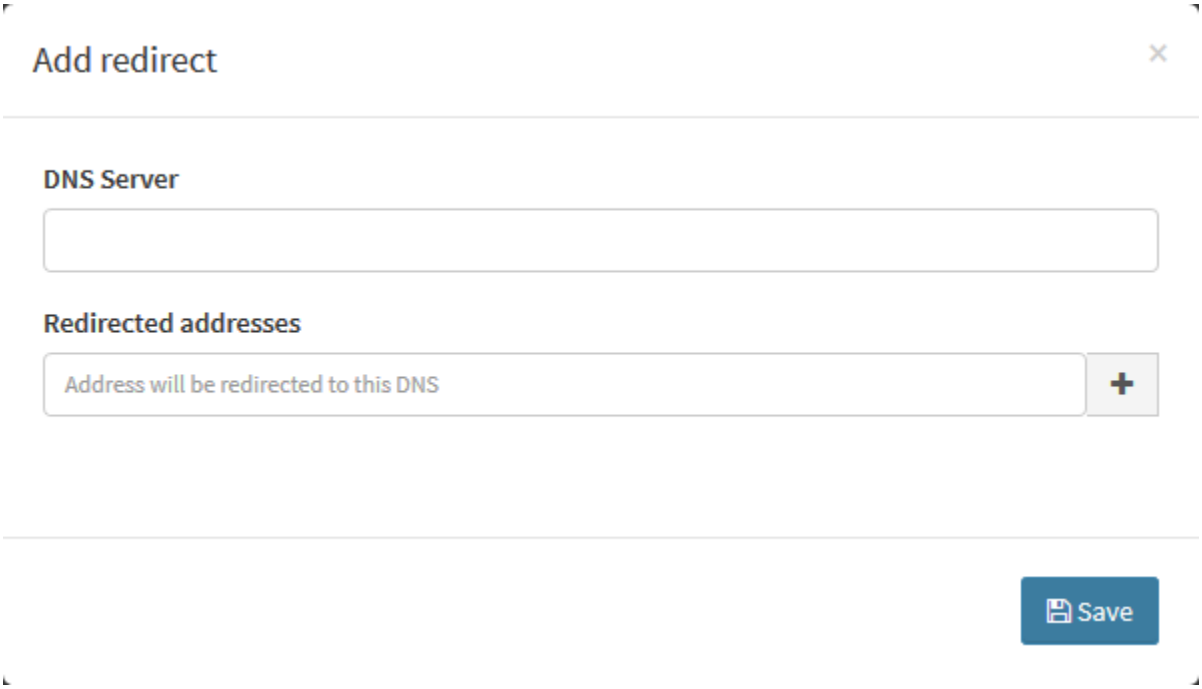
In this area you can configure the service for redirecting DNS requests to let "other DNS servers" be "Responsible" to perform "Exclusive" recursive queries for a "host list".

The service allows by distributing and balancing the searches to specific hosts, redirect the service to another exclusive DNS server for the specified hosts.

It can also be used to redirect searches to an “invalid DNS”, avoiding the resolution of names from certain addresses, thus blocking your access.

- DNS redirection:
  - Multiple servers;
  - Routing by host / IP and FQDN;
  - *Cache*.

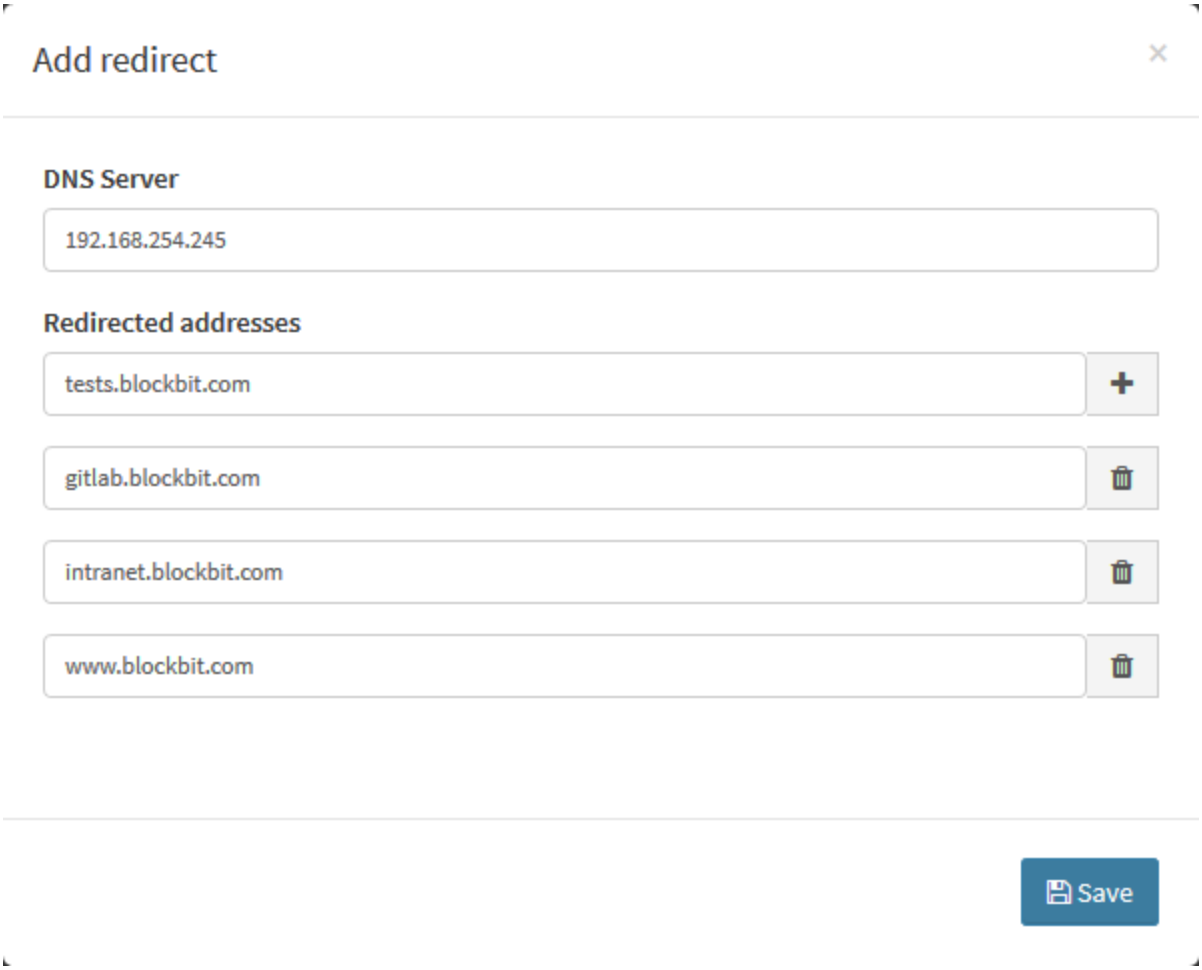
In the Redirect box, click **[ ]** and configure it by pointing the DNS server address and adding the list of hosts that you want to redirect the recursive searches on.



DNS - Add redirect

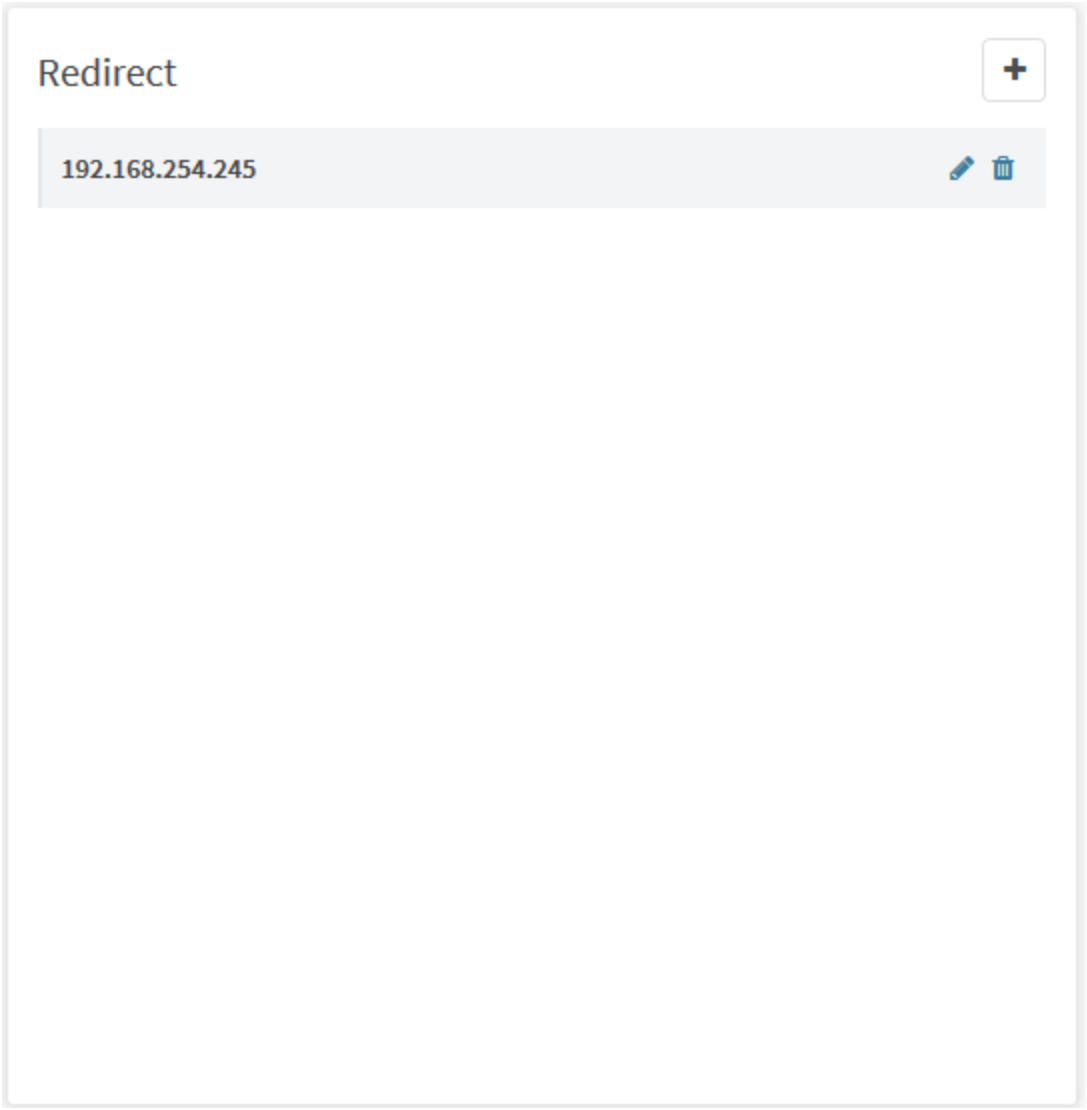
- ***DNS Server*:** Add the DNS server that will be used. If you want to add other domains, click the **[ ]** button, after adding other domains, click **[ ]** to remove them;
- ***Redirected addresses*:** Add the addresses to which the redirection will be made. If you want to add extra addresses, click the **[ ]** button, after adding other addresses, if necessary, click **[ ]** to remove them.

Let's exemplify the search for a list of hosts on a local DNS Server, as shown in the image below:



DNS - Add redirect - Example

Once the changes are made, click [Save] to save all settings.

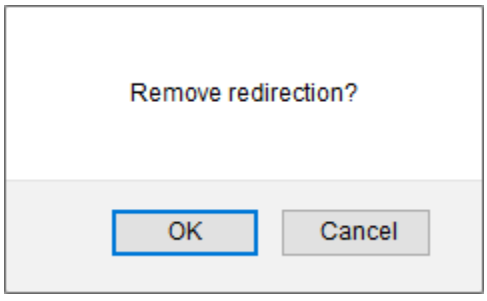


DNS - Redirect added

After saving, for the changes to take effect it will be necessary to access the command queue **[** **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

If it is necessary to edit the added data, click on the **[** **]** button and make the necessary settings.

If you want to remove them click on **[** **]**, the following message will be displayed:



Remove redirection

Click **[** OK **]** to complete the deletion, otherwise, click **[** Cancel **]** to close this window

After these steps, the DNS redirection will have been successfully configured.

UTM - Services - DDNS (DynDns)

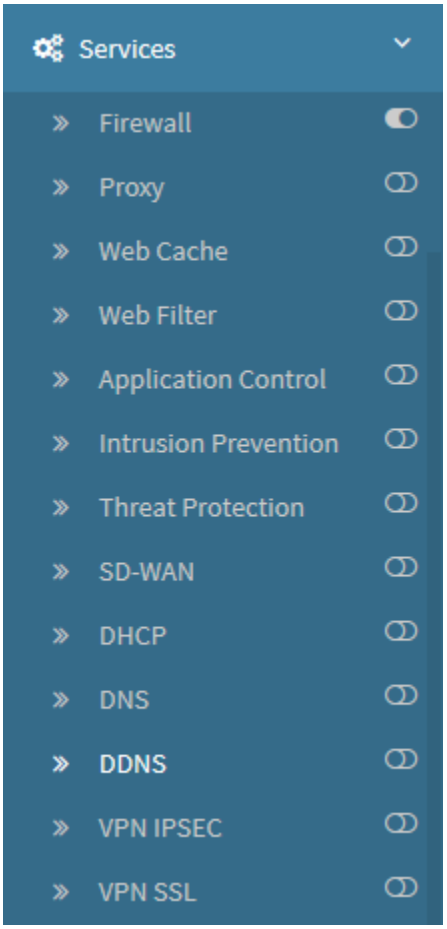
The DDNS (Dynamic Domain Name System) service is a manager of a name translation service for dynamic IP addresses. DDNS is the method used to update the table of public IPs / hosts automatically on a DNS server in real time and this with the purpose of keeping active and published a host or IP address configured for some service or resource through a dynamic link such as: PPPOA; PPPOE, (DSL - Digital Subscriber Line) to provide your remote access.

Dynamic IP addresses pose a problem when we need to do some remote access to some service on the network, such as a web service (intranet / extranet), DNAT (Destination NAT) access, VPN configuration, among others.

How the IP addresses of DSL links can change frequently, associating host and domain names with dynamic IP addresses is a task that requires almost real-time remapping for services to continue responding to requests and remote access without interruption to public users.

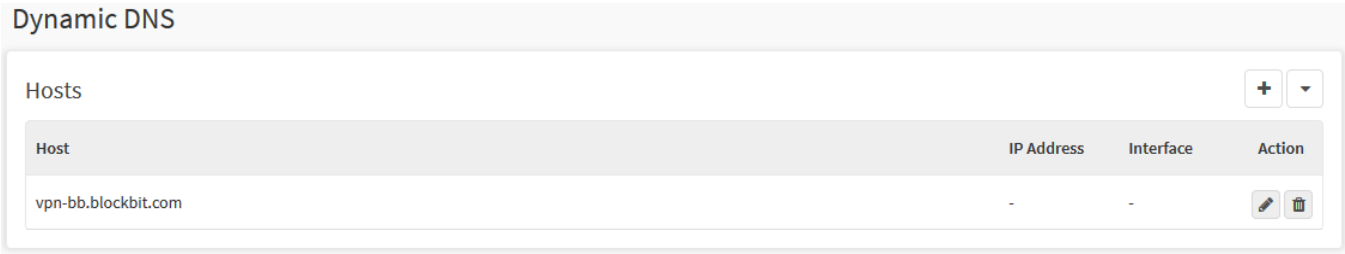
Dynamic DNS is an expected or even required feature in our appliances. Some services such as VPN IPSEC (site-to-site), VPN IPSEC RAS and even remote access by firewall redirection (DNAT), use this resource as an additional tool to securely allow access to network resources through DSL (dynamic IP) links.

Access the management interface by clicking on the “DDNS” option.



Services - DDNS

The screen below will appear:



Services - Interface DDNS

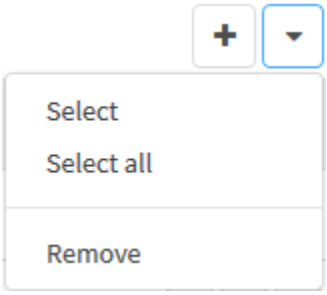
Next we will analyze the components of this screen.

DDNS - Actions Menu

At the top right of the screen, next to the add button we have the actions menu:

DDNS – Actions menu button

By clicking on this button the menu below is displayed:



DDNS – Actions menu

The menu consists of the following options:

- *Select;*
- *Select All*;
- *Remove*.

Next, each action menu option will be detailed.

DDNS - Add Button

Before adding a “Dynamic DNS” let's get to know and identify the configuration features and how they work.

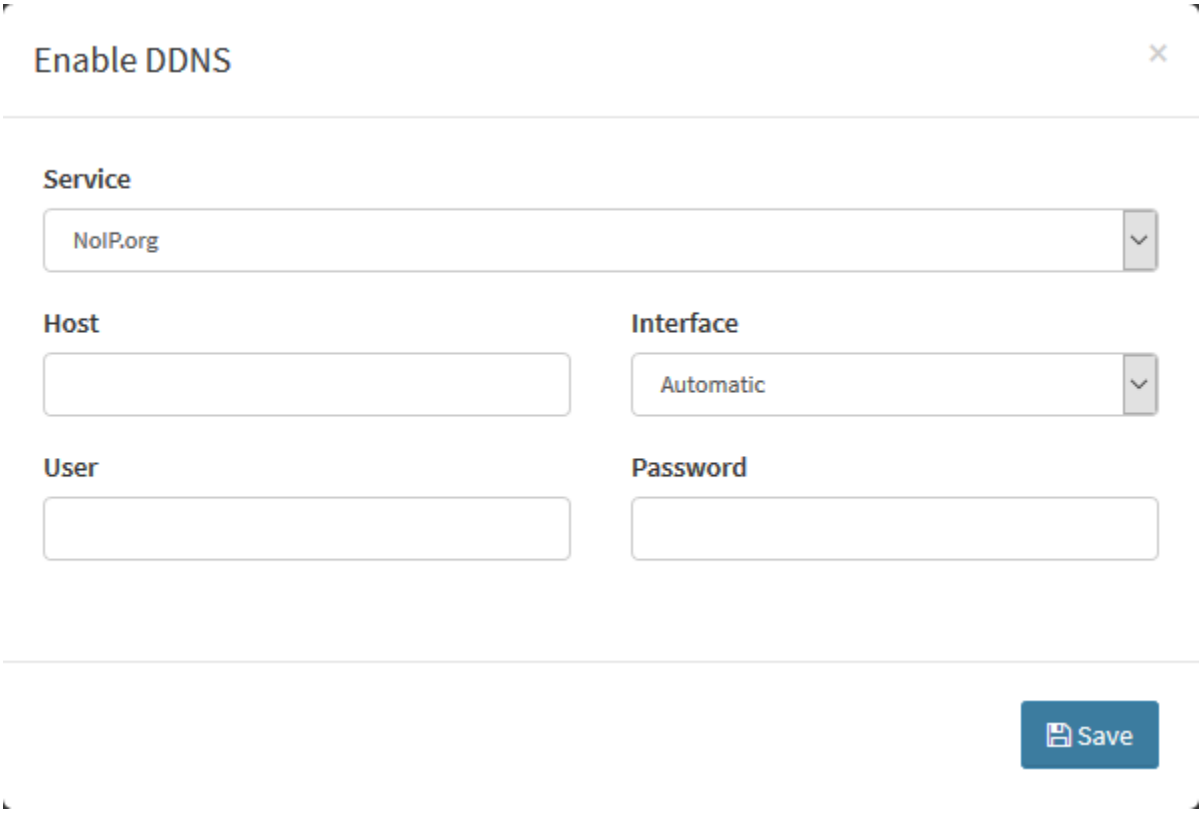
- *DDNS resources.*
  - Service Provider Support.
    - NoIP.org;
    - DynDNS.com.
  - Interface support.
    - *Ethernet*;
    - *Vlan*;
    - *MacVlan* (Virtual interface).
  - Integration with services
    - *DNS*;
    - *VPN*;
    - *Firewall*;
    - Security Policies.
  - 10/10 min automatic hosts / domains (ddns) update.

The DDNS service can be enabled for a specific network interface “[EthX]” or in “Automatic” mode.

- The selection of a specific interface is considered as an example, associating the “host” with the “IP address of the DSL link” of the respective physical device;
- When selecting the interface in "Automatic" mode, it is considered to associate the "host" dynamically with the "IP address" in use by the link that is active as "Default route", no matter which one.

In this way, it is possible to provide “Redundancy” for the IPSEC (site-to-site) VPN, IPSEC RAS VPN and remote access by redirection through the firewall (DNAT) services. It doesn't matter if you use a fixed IP link or a DSL link, it is possible for the DDNS resource to dynamically publish a host's IP address and allow the use of this host “FQDN - full Quality domain name” as an access and configuration address in the services cited.

To add a DDNS, click **[+]**. The following window will be displayed:



DDNS - Enable DDNS

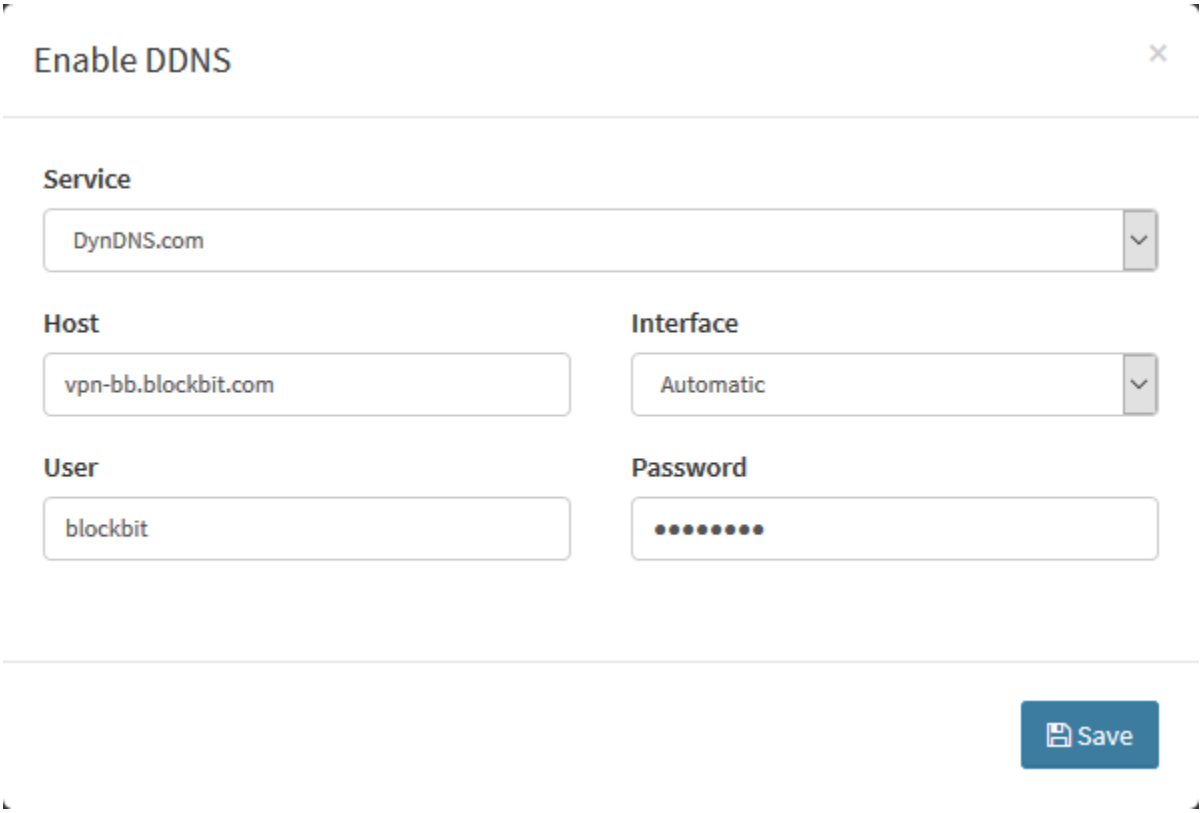
Configure the form according to the specifications for connection to the provider according to the example given.

- ***Service:*** Determines which DDNS service will be used;
- ***Host:*** In this field you must define which Host will be used;
- ***Interface:*** As previously mentioned, the interface can be specific or automatic:
  - **Specific Interface:** The available options are the interfaces registered in *Network - Interfaces*, this resource is used to associate the “host” with the “IP address of the DSL link” of your physical device;
  - **Automatic Interface:** Associates the "host" dynamically with the "IP address" in use by the link that is active as "Default route".

The automatic interface is recommended for cases where it is necessary to access the Blockbit through a router or gateway where it a NAT is running, that is, when there is the delivery of a private IP.

- ***User:*** As previously mentioned, in this field the user used to authenticate with the provider must be entered;
- ***Password:*** As previously mentioned, in this field the password used to authenticate with the provider must be entered.

Let's exemplify the configuration of “Dynamic DNS” for the host “vpn-bb.blockbit.com” for the service provider “DynDNS”. Use username and password provided / registered with the respective provider.

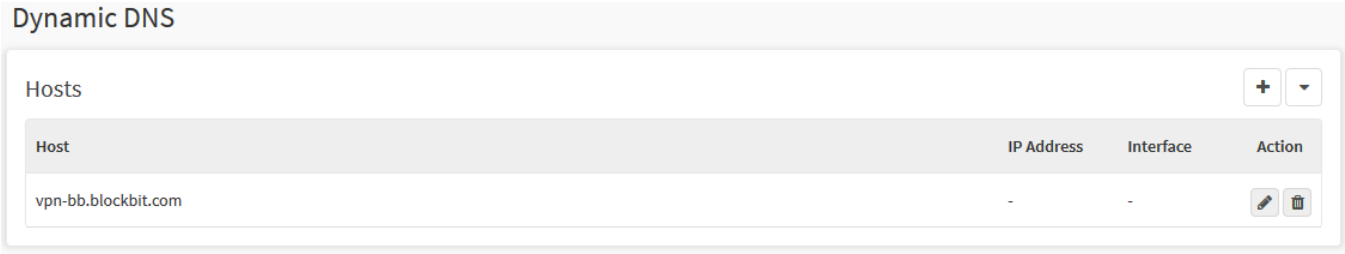


DDNS - Enable DDNS - Example

After you have made the settings, click **[** Save **]** to save them.

After saving, for the changes to take effect it will be necessary to access the command queue **[** 1 **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue

After performing these procedures the DDNS will have been successfully configured.

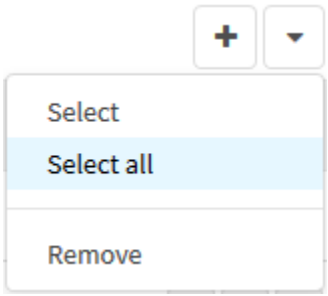


DDNS - Dynamic DNS Added

The DDNS Service is already configured and the host “vpn-bb.blockbit.com” responding by the IP address of the network interface corresponding to the default route.

DDNS - Actions Menu - Select all

By clicking on “Select All” in the action menu all items will be selected.



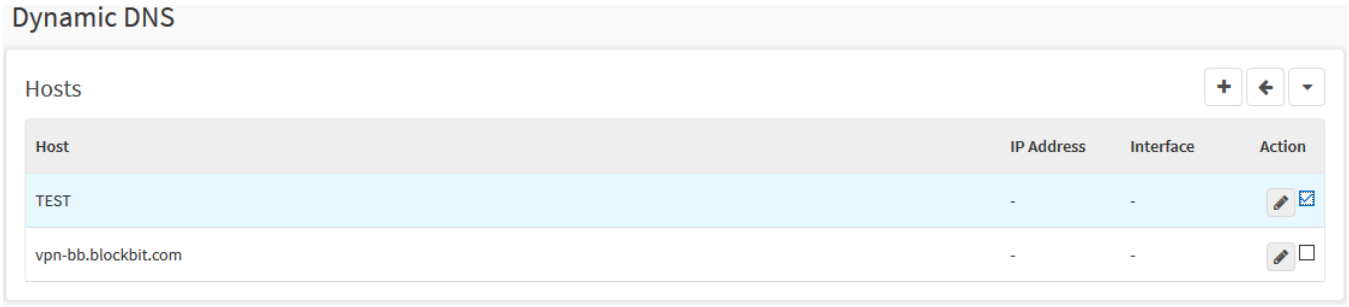
DDNS – Select All

This allows changes that affect all items to be easily implemented.

DDNS - Actions Menu - Remove

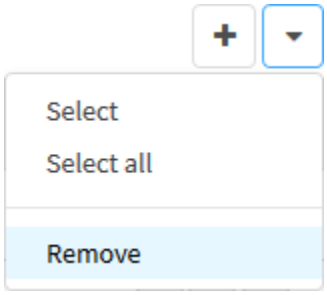
Through the action menu it is possible to delete several items at the same time. Follow the steps below:

1. Select the items you want to delete by clicking the checkbox **[ ]**;



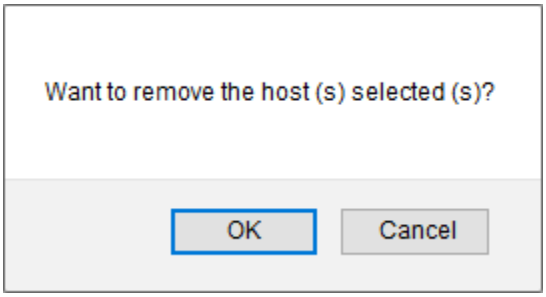
DDNS - Selection for deletion

2. Click on the Actions menu **[ ]** and select the “Remove” option;



DDNS – Actions Menu – *Remove*

4. A screen will appear asking if you want to delete the selected item:



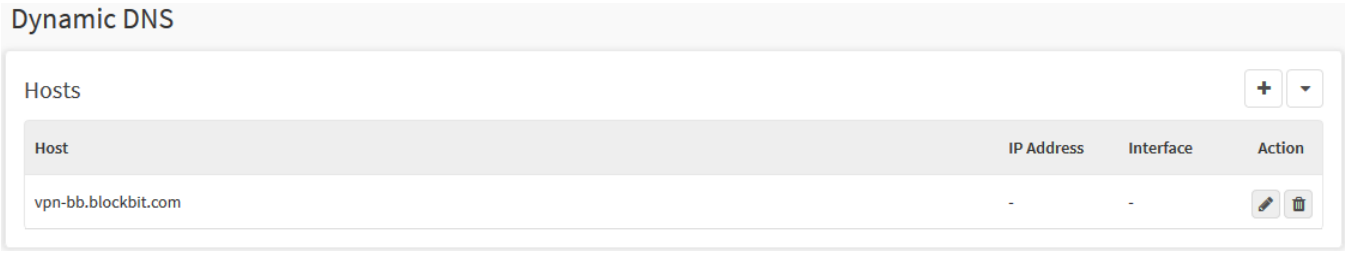
DDNS - Remove itens

If you want to cancel, click the **[** Cancel **]** button. To complete the deletion click on the **[** OK **]** button.

The item was successfully deleted.

DDNS - Columns

Below we will explain each column of the Dynamic DNS tab:



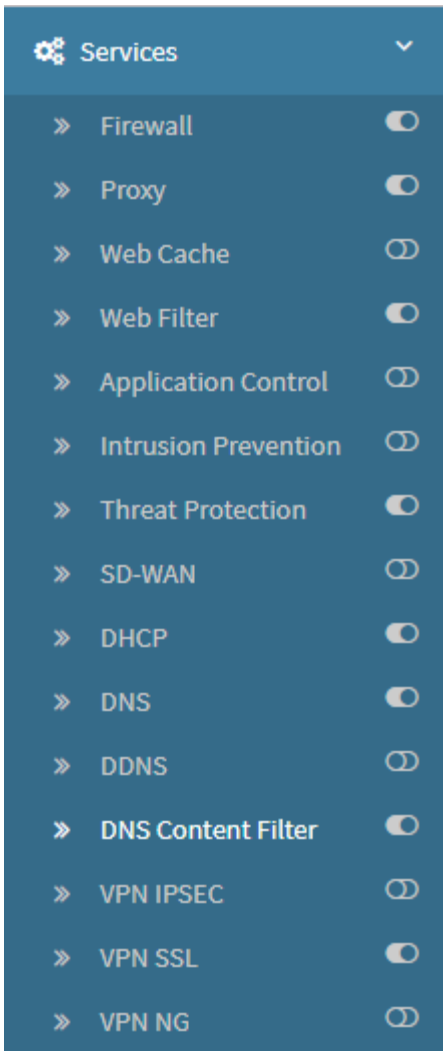
Dynamic DNS

- ***Host:*** Displays the DDNS Host that was registered through the Add Button;
- ***IP Address:*** Displays the IP address used by the DDNS service;
- ***Interface:*** Determines the DDNS interface, which can be specific or dynamically selected;
- ***Action*****:** Provides the following essential actions:
    - ***Edit*****[ ]:** Allows you to edit the settings added via the add button ;
    - ***Delete*****[ ]:** Allows you to remove one of the items, it is equivalent to the *Remove* option in the action menu.

UTM - Services - DNS Content Filter

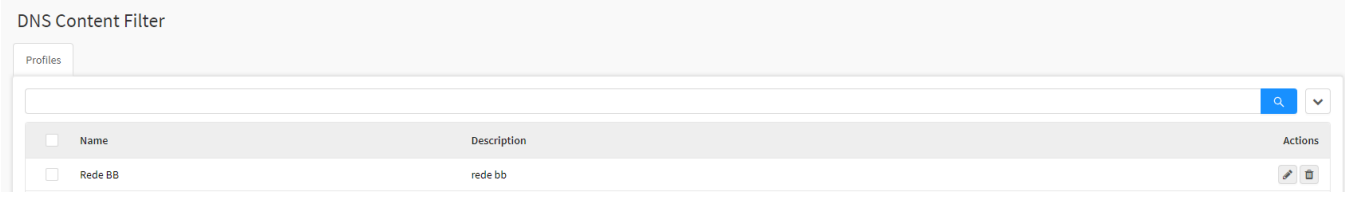
DNS Content Filtering is a protection service for the address translation done by the DNS system (when it converts a domain's specific address into an IP or vice-versa) preventing errors in the translation, which can mislead the user to wrong addresses. It also allows the moderation of access to specific addresses by content. For example, we can block access to the "games" content by selecting this category while we create a DNS content filter profile in the services option, on the NGFW.

Select the DNS Content Filter option:



Services - DNS Content Filter

The screen below will be displayed:

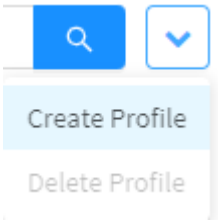


Services - Interface DNS Content Filter

Next, we will analyze this screen's components.

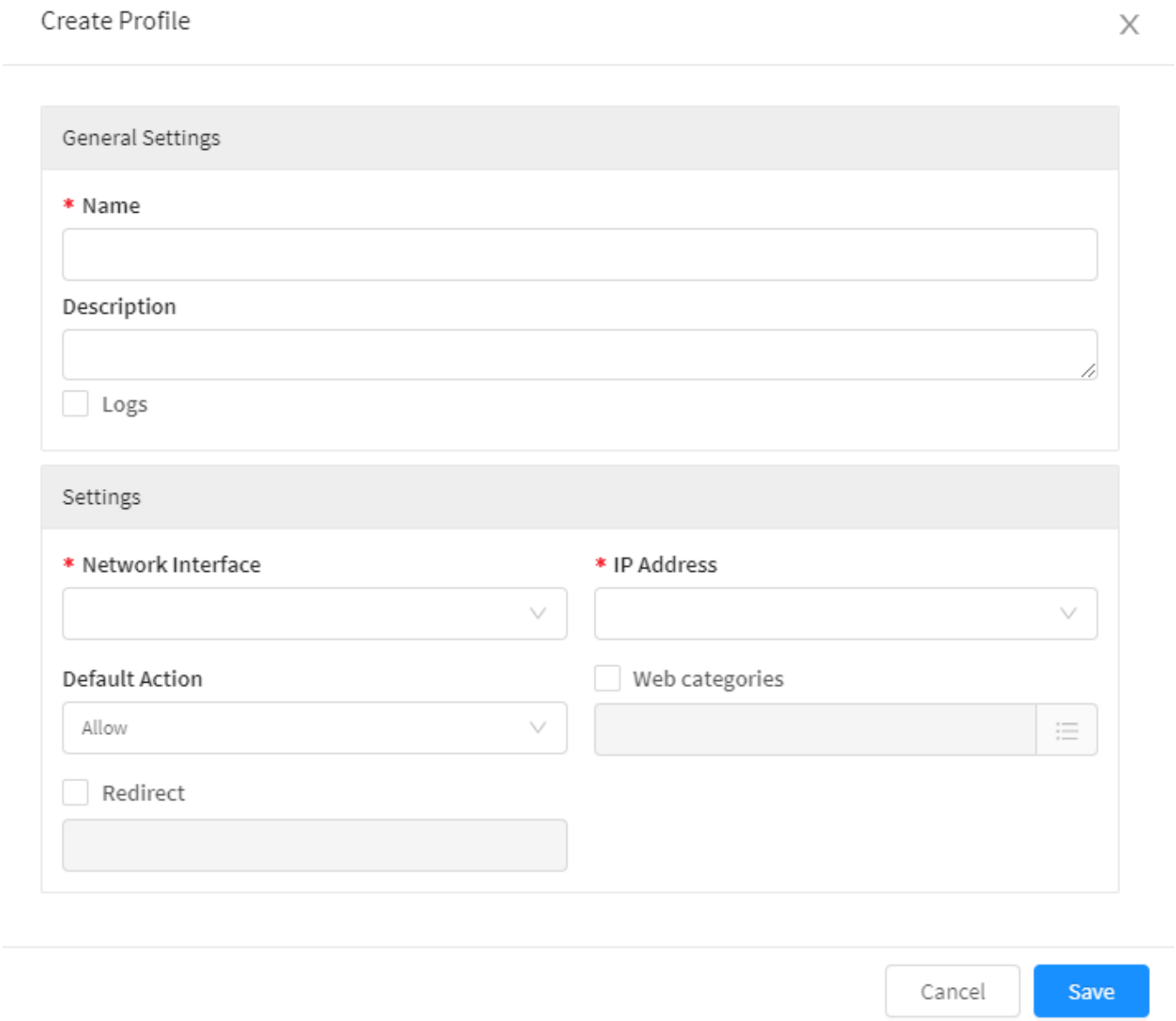
Create Profile

We will analyze the set up of a DNS Content Filter Profile. Initialy, click the create button, on the actions menu:



DNS Content Filter - Create Profile

The next screen will be displayed:

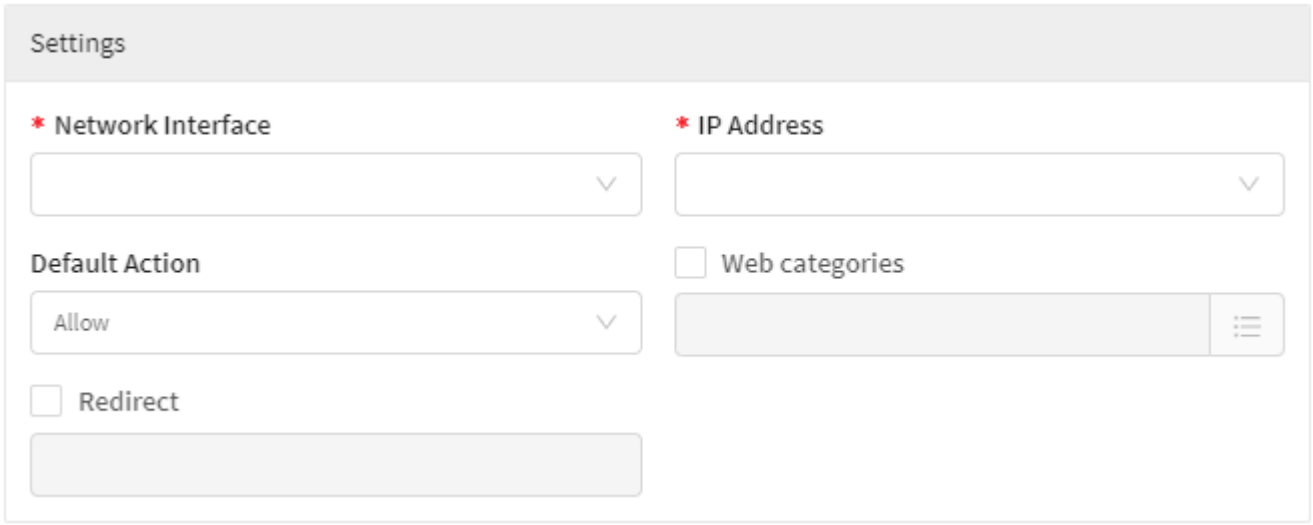


Create Profile - DNS Content Filter

We will analize the settings and functions of both fields in detail:

General Settings - Create Profile

- **Name:** How the profile will be named.
- **Description:** Details of said profile.
- **Logs:** While this option os active, the acesses will be registered on a log, that will be available in Security Events.



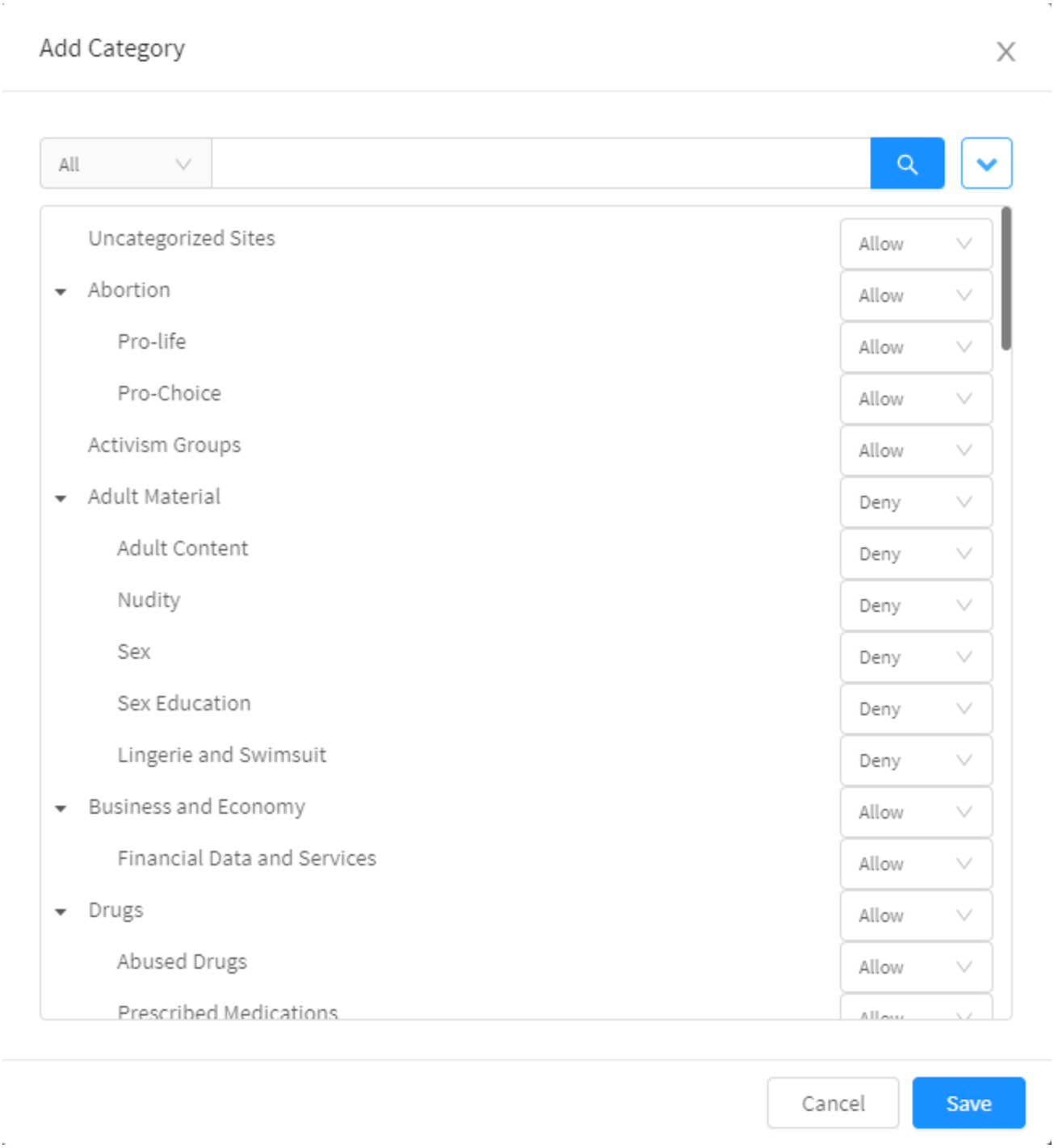
Settings - Create Profile

- **Network Interface:** Select the network interface that the profile will use (eth0, eth1, eth2, eth3).
- **IP Address:** Select the IP address or the address to be monitored.
- **Default Action:** In this option one should select the default action to be taken by the *DNS Content Filter* (if allow, or deny), for requests to be deat with by the system.
- **Web Categories:** In this section we can select the addresses we would like to allow or deny access to (See more details on the next section).
- **Redirect:** Insert the IP for redirecting the user to, in case access is denied to a page. This page will be where a blocked user will be redirected to.

It's important to remember that for the service to function correctly it is necessary that the stations' DNS points to the NGFW's IP. Furthermore, the NGFW's DNS service must be configured and operational. In case there are any doubts about it, just click here.

Web Categories

This is where we select the categories to be allowed or blocked for access, be it through a web site, application or search engine.



Categories List

On the image above the *"Uncategorized Sites"* category allows the user to provide deny or allow status to domains (web sites, apps or search results) that are not present on the categories summarized on this menu.

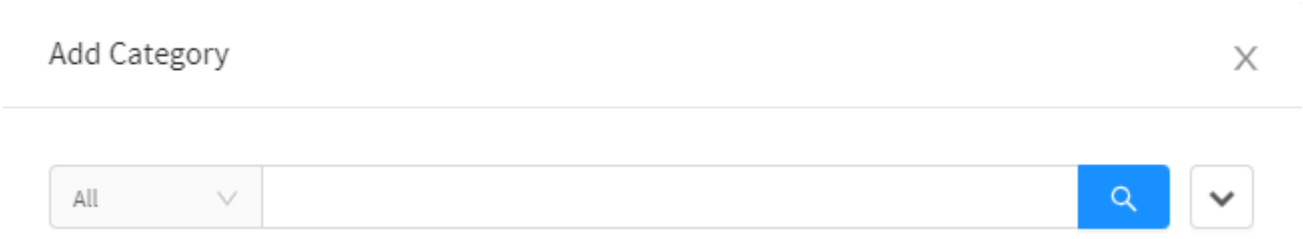
Below are the categories and subcategories, related by topic and can be equally allowed or denied access to, individualy or by groups.

After having granted/denied access to desired categories, click "save" to keep record of the changes done.

It's important to highlight that the DNS Content Filter service will NOT be functional if used together with the Proxy service in Explicit mode.

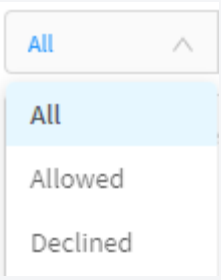
Actions menu

The actions menu consists on the "all enabled/denied" menu, search bar and actions menu:



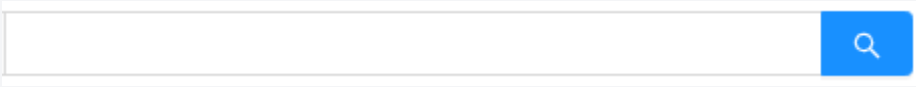
Overview - Actions Menu

Categories display menu:



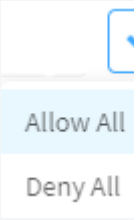
This option displays the categories that are: Allowed, Denied and All.

Display Menu - Search bar:



Allows that a category can be found by using keywords.

Actions Menu



Allows the assignment of Allow or Deny status to all available categories.

After selecting the categories/sub-categories required, click "save".

By having finished the configuration and created the DNS Content Filtering profile, the service will start analysing the traffic right away, without the necessity of being bound to any policies.

Notes

It's important to remember that for the DNS Content Filter to be used alongside the Cluster, It must be set up over a Virtual Interface.
In case the local network gateway is a virtual interface and the physical interface in which this very same virtual network originates has an IP configured for this same network, then the use of the physical interface is recommended instead, on the DNS Content Filter settings so that it can work properly.

It's also worth noting that the access attempts registered by the service will be available for viewing in Security Events, when utilizing the logtype: "dnscontent".

UTM - Services - IPSEC VPN

The IPSEC VPN service is responsible for allowing to configure and establish private tunnels between networks through public means. This service allows the administrator to interconnect networks and provide data sharing, whether between branches, traveling employees, home offices, customers and suppliers, it is essential to maintain a security mechanism so that the traffic of information is safe and without risks of unauthorized access.

The VPN service provides a high level of security through IPSEC security protocols. Incorporating data encapsulation and encryption using a suite of protocols, encryption and authentication methods in communication between hosts on the private network so that, if data is captured during transmission, it cannot be decrypted.

IPSec is the standard protocol used to encapsulate IP packets, it runs on layer 3 (OSI model) and will be used to establish VPN tunnels in both configuration models: VPN tunnels and VPN Remote Access.

The VPN settings are done and changed via web interface, in the same way as all other Blockbit's services and functionalities.

Using the *Live Sessions* - IPSEC *VPN* panel available in Monitor, it is possible to check the current status of your IPSec VPN connections.

IPSEC VPN configuration requirements

For the IPSEC VPN service to be able to manage a secure connection, we first need to make sure that we meet some requirements and then make the VPN service available to the network.

Before configuring a tunnel it is important to know which models of hardware and VPN applications will be used to establish the tunnel. Know the model and characteristics of each application and define exactly what type of VPN tunnel you will establish.

1. It is recommended that the points of the Blockbit NGFW Appliances that will provide the IPSEC VPN service are configured with a valid and fixed IP address. Example: “Dedicated link / IP link”*;*

2. If any of the points of the IPSEC Tunnel VPN or IPSEC RAS VPN is a Blockbit NGFW, the administrator must:

- Enable firewall permission for the IPSEC VPN service for the “Network zone (s)” of the valid IP address(es);

IPSEC Services:

  - *IKE* (*UDP* port 500);
  - *IPSec ESP* (*IP type* 50);
  - *IPSec AH* (*IP type* 51);
  - UDP encapsulation - port (NATT - 4500).
- Configure a "security policy" of the "Allow" type for routing between networks (LANs) of VPN points to the respective services and protocols that will be trafficked by the VPN. Ex .: “TCP / UDP / ICMP”;

3. If you are configuring a remote point, and are protected by a Firewall, it is necessary to request the firewall administrator to deliberate the IPSEC VPN traffic to the respective VPN host in advance.;

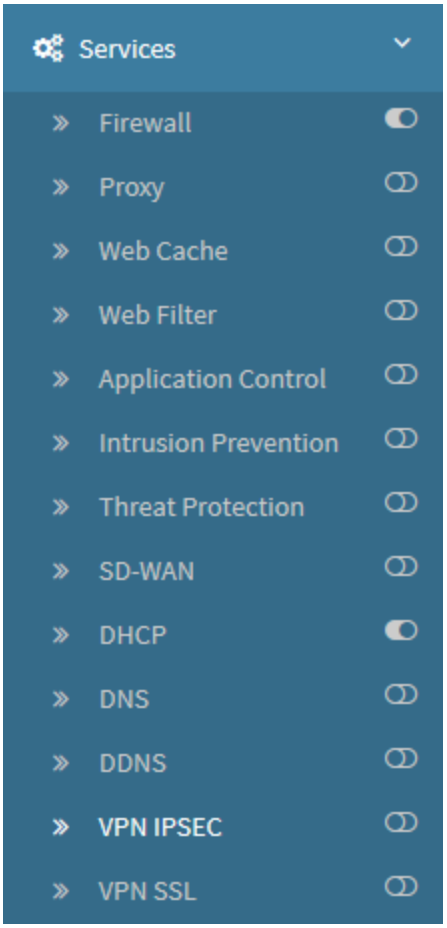
4. Redirection policies (DNAT) + Forwarding policies;

- UDP encapsulation - port (NATT - 4500).

5. If using the Authentication Method is of the RSA Key type, the Local ID field must necessarily be unique.

Also note the particular requirements for IPSEC Tunnel VPN and IPSEC Remote Access VPN, which will be listed on their respective pages.

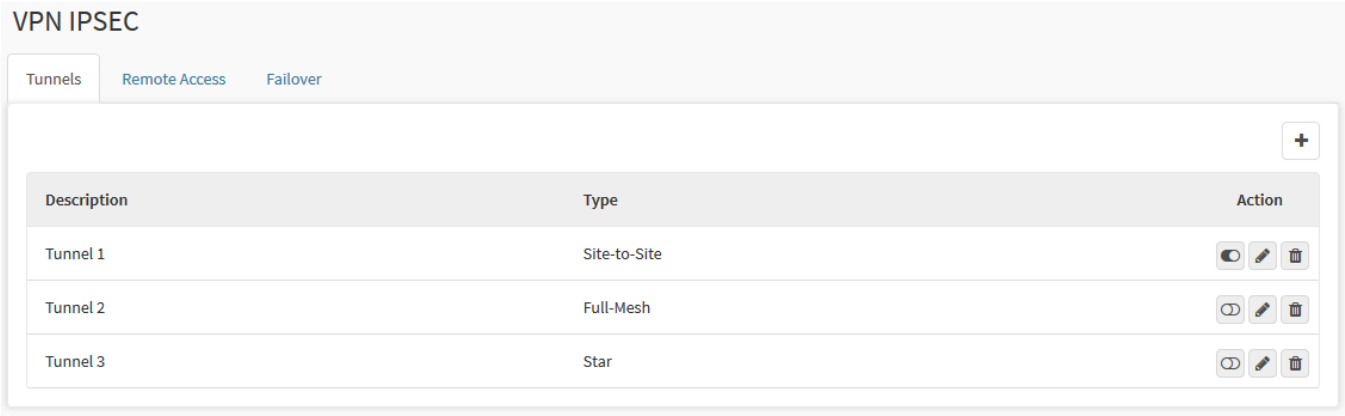
To access the resources click on the IPSEC VPN option.



Services - VPN IPSEC

Recommended: Enabling the service [/] before its configuration.

The screen below will appear:



VPN IPSEC

In addition, the IPSEC VPN screen consists of the tabs:

- *Tunnels*;

- *Remote Access*;
- *Failover*.

Next, we will detail the *Tunnels* tab and analyze some technical specifications.

VPN IPSEC - Tunnels Tab

To configure an IPSEC VPN tunnel correctly, it is recommended to consider some checks and requirements:

1. What models of VPN hardware / applications from remote points?

2. Identify LAN network addresses for each VPN point - make sure that each point has a network address in different classes / subnets.

3. What is the address of the remote points (remote ID)?

- *IP address*;
- *Host FQDN*.

4. Define an encryption key (PSK - Phrase Shared key).

5. Define the model and phase 1's identification (IKE / SA).

- *IP address*;
- *Host FQDN*;
- *Host*;
- email@domain.

6. Define the “Main mode / Aggressive mode” trading method*?*

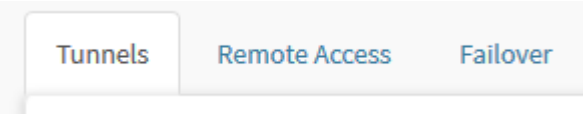
7. Set the parameters for phase 1 configuration (IKE / SA):

- IKE Parameters (Phase 1) - IKE support version 1 and 2. Example.:
  - Cryptography: “3DES, Aes, DES”;
  - Authentication (HASH): “HMAC-MD5, SHA 1”;
  - *Diffie-Hellman* (*DH Group*): “*modp 2048*”.

8. Set the parameters for phase 2 configuration (IPSEC / ESP):

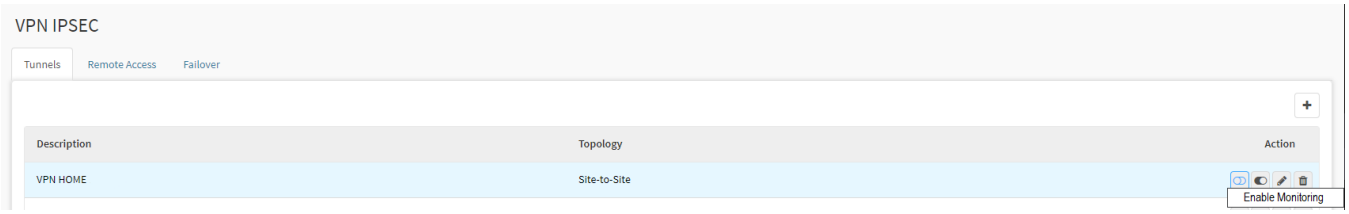
- IPSEC - ESP parameters (Phase 2). Example:
  - Cryptography: “*ESP-3DES*, *Aes*, *DES*”;
  - Authentication (*HASH*): “*ESP-HMAC-MD5*, *SHA* 1”;
  - *Use PFS - Perfect Forward Secrecy*: “*modp* 768”.

To configure and enable IPSEC tunnels, access the Tunnels tab:



Tunnels Tab

The screen bellow will be displayed, where it will be possible to enable the tunnel monitoring system as shown on the image bellow:



VPN IPSEC - Tunnels

By activating the first "enable" button **[ ]**, the system will be able to monitor and identify flaws between two points connected through a VPN, and generate notifications in case the tunnel shuts down**.**

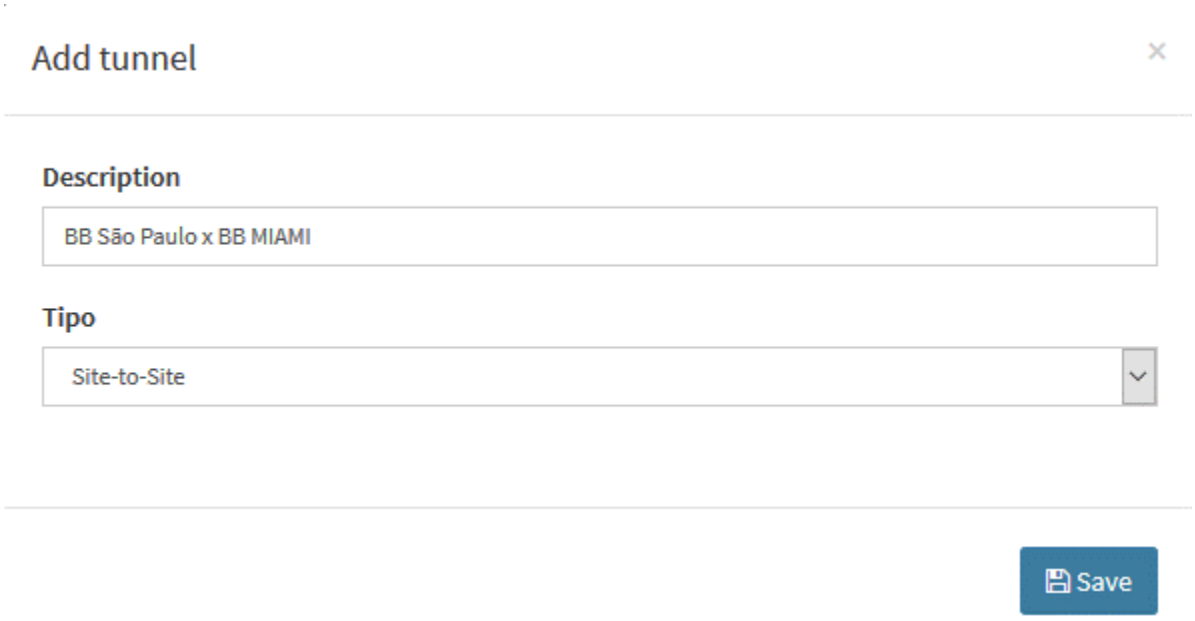
In this session we will analyze:

- Addition Button;
- How to edit each tunnel;
- Composition of each column.

Next we will analyze each component of this screen.

Tunnels - Add button

To add an IPSEC Tunnel click on **Add [ ]**.



VPN IPSEC - Add tunnel

The following fields will be displayed:

- ***Description*:** Complete with the VPN description. Ex.: BB São Paulo x BB MIAMI;
- ***Type*:** Determines the type of VPN, the possibilities are:
  - ***Site-to-Site*:** This type of VPN allows you to create a secure connection between two point-to-point LANs. For more information on how to configure a tunnel with this mode of operation, check this page;
  - ***Full-Mesh*:** This type of VPN creates a connection between all HUBs and Spokes allowing all devices to establish communication with each other, performing independent communication from the HUB*. For more information on how to configure a tunnel with this mode of operation, check this* page;
  - ***Star*:** All devices establish communication with a HUB (usually the company's headquarters), and this allows the exchange of information between devices, however, in a controlled manner. For more information on how to configure a tunnel with this mode of operation, check this page;

Click **[Save]**, to save the changes.

After adding a tunnel, it is highly recommended to configure it using the **[ ]** option.

Next we will analyze the components of the *Edit button*, the types of VPN and their respective options.

Tunnels - Edit button

When creating a tunnel using the **[**  **]** button, it is added without any particular configuration, to make this configuration it is necessary to click on the **[**  **]** button.

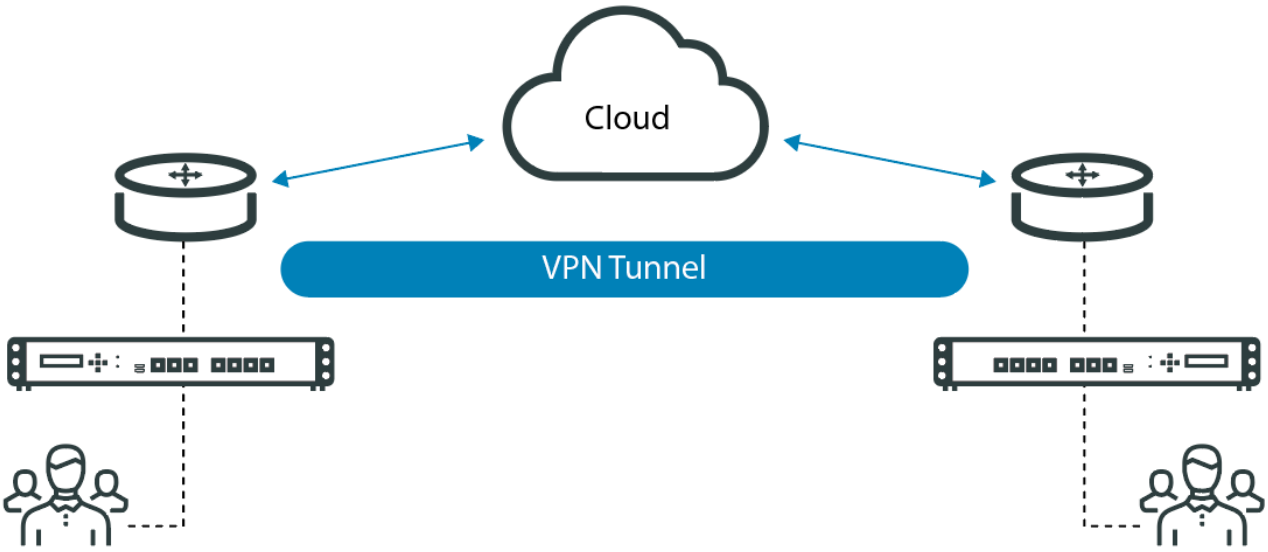
The types of tunnels available are:

- *Tunnels - Site-to-Site*;
- *Tunnels - Full-Mesh*;
- *Tunnels - Star*.

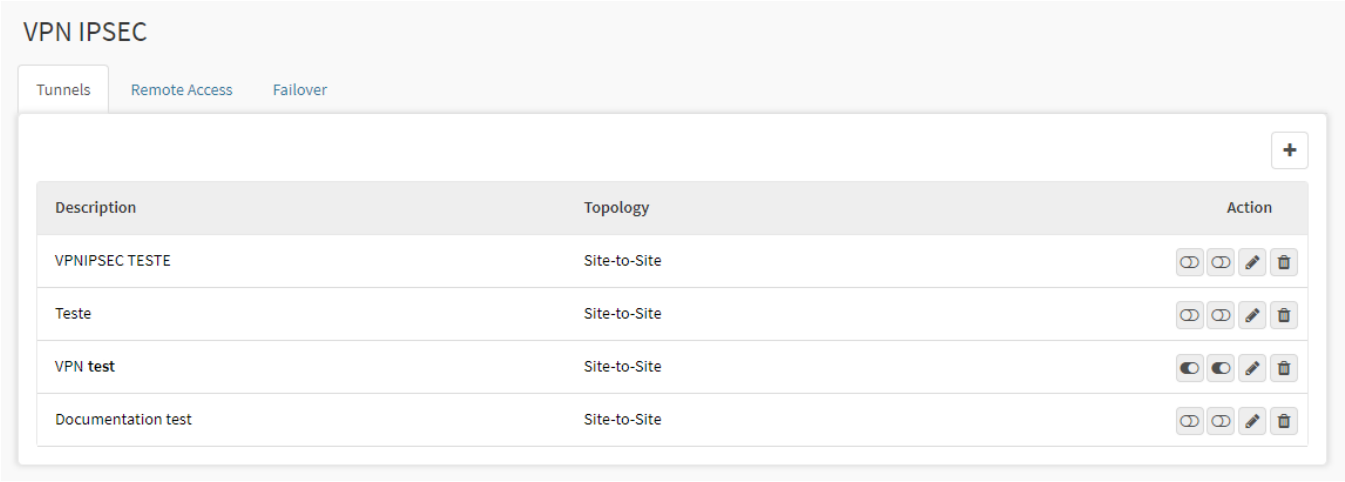
Tunnels - Site-to-Site

The IPSEC Site-to-Site VPN service method aims to manage multiple virtual tunnels from private networks and provides a site-to-site tunnel connection (LAN to LAN);

The VPN can also establish end-to-end cryptographed tunnels (tunnels, site-to-site) with a public or dynamic IP (assigned to it by a DHCP).



IPSec VPN - Site-to-Site Topology



IPSec VPN Tunnels: Site-to-Site

On the image above we can see the VPN's action buttons:

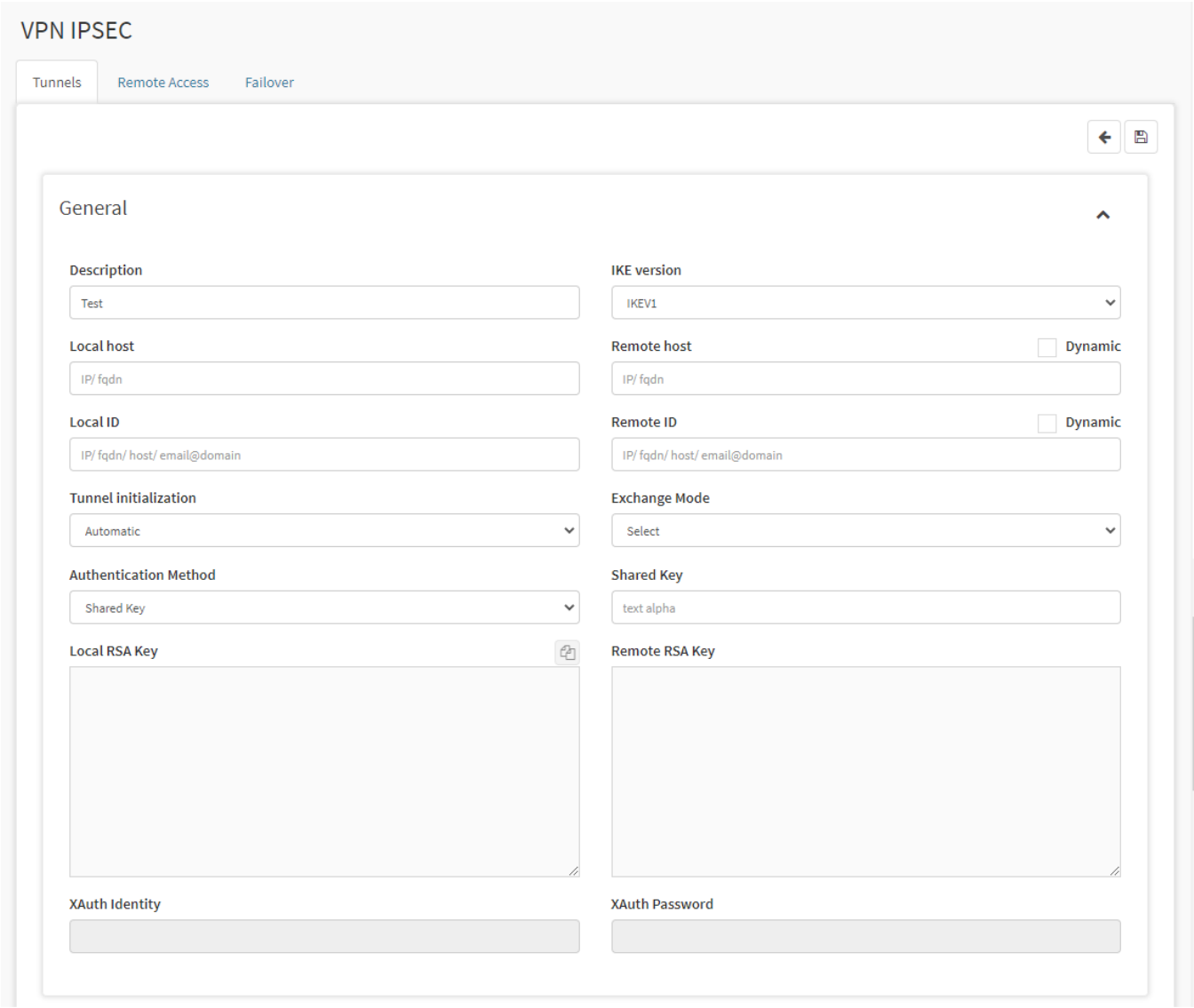
- ***Enable VPN:*** Click on this option to activate a pre-configured VPN Tunnel.
- ***Enable VPN's monitoring:*** This option activates the VPN's monitoring, registering and alerting in case of instabilities, failures or drops.
- ***Edit VPN's settings:*** Allows the editing of the VPN's connection settings.
- ***Delete VPN:*** Deletes a VPN tunnel.

When adding a tunnel, if the selected type was “Site-to-Site” when clicking on edit [ ], the screen below will be displayed:

Next, we'll look at how to set up a "Site-to-Site" tunnel.

General

Below we will analyze each option available in the general panel:



IPSEC VPN - General

- ***Description:*** *Field where the VPN description is being determined, which is being configured*;
- ***IKE version:*** *IKE - Internet Key Exchange is the protocol used to establish a security association (SA) in the IPSec protocol suite*. IKE is based on the Oakley and ISAKMP protocol, uses a PSK authentication key or X509 certificates and a “Diffie Hellman” key exchange;

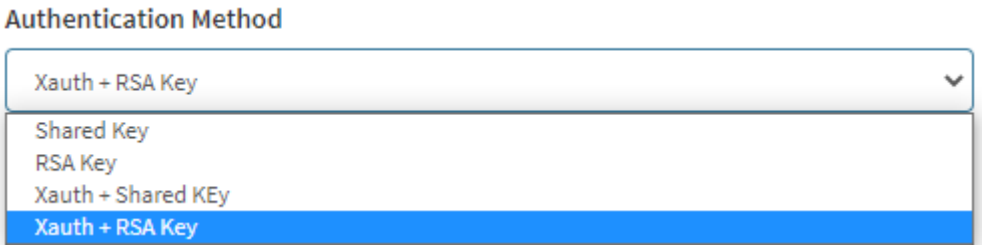
Both the “PSK (Pre-shared key)” key type, and the “Diffie-Hellman” key exchange are used on the Blockbit NGFW. *The system supports IKEV1 and IKEV2*.

It is essential for the correct functioning of the VPN that all devices in this same server community are configured for the same IKE version.

- ***Local host:*** *Communication address of the LOCAL VPN point to establish the tunnel*. It must be identified by: “IP address” or “Hostname (FQDN)”;

- ***Remote host:*** *Communication address of the REMOTE VPN point to establish the tunnel*. It must be identified by: “IP address” or “Hostname (FQDN)”. The Dynamic option is used when the internet and IP link is of the dynamic type;
- ***Local ID:*** *Local VPN endpoint identification method, also used as an IKE authentication method in phase 1*. Define and configure the identification between the types: "IP address", "Hostname (FQDN)" or "email @domain"*;*
- ***Remote ID:*** Remote VPN endpoint identification method, also used as an IKE authentication method in phase 1. Define and configure identification between types: *“IP adress”*, *“Hostname (FQDN)”* or *“email@domain”*. The Dynamic option is used when the internet and IP link is of the dynamic type;
- ***Tunnel initialization:*** *Determines how the tunnel will start, the available options are*:
  - ***Automatic*****:** Adds and initializes the Tunnel;
  - ***Wait*****:** Adds and does not initialize the Tunnel. Waiting for demand request (traffic) from the other end VPN;
  - ***On demand*****:** Initializes and raises the Tunnel only on demand, that is, when there is traffic from any VPN endpoint.
- ***Exchange Mode:*** *IKE (SA) version 1 key negotiation method*:
  - ***Main Mode*****:** Main mode of negotiation of IKE keys (Encryption and authentication). Operates the exchange of information in 6 packages;
  - ***Aggressive Mode*****:** Aggressive way of negotiating IKE keys (encryption and authentication). Operates information exchange in 3 packages.

IKE v2 natively operates “Exchange Mode” in the standard: **[Main Mode].**



Authentication method options - VPN IPSec

- ***Authentication Method:*** *Determines the authentication method that will be used on the VPN, the possible options are*:
  - ***Shared key PSK*****:** It is a pre-shared key (Pre-Shared Key or PSK) is a secret previously shared between the two parties using some secure channel before being used. Such systems almost always use symmetric-key cryptographic algorithms. This key is used in the authentication process by the IKE protocol. The administrator must define this key and configure at both VPN points;
  - ***RSA Key*****:** RSA key consists of an algorithm used in asymmetric cryptography, security technology that uses a pair of keys (public key and private key), applying a different component of the pair in different phases of the algorithm. Any message encrypted using a public key can only be decrypted using the respective private key. Public RSA Keys must be "exchanged" between both "VPN sites"*;*

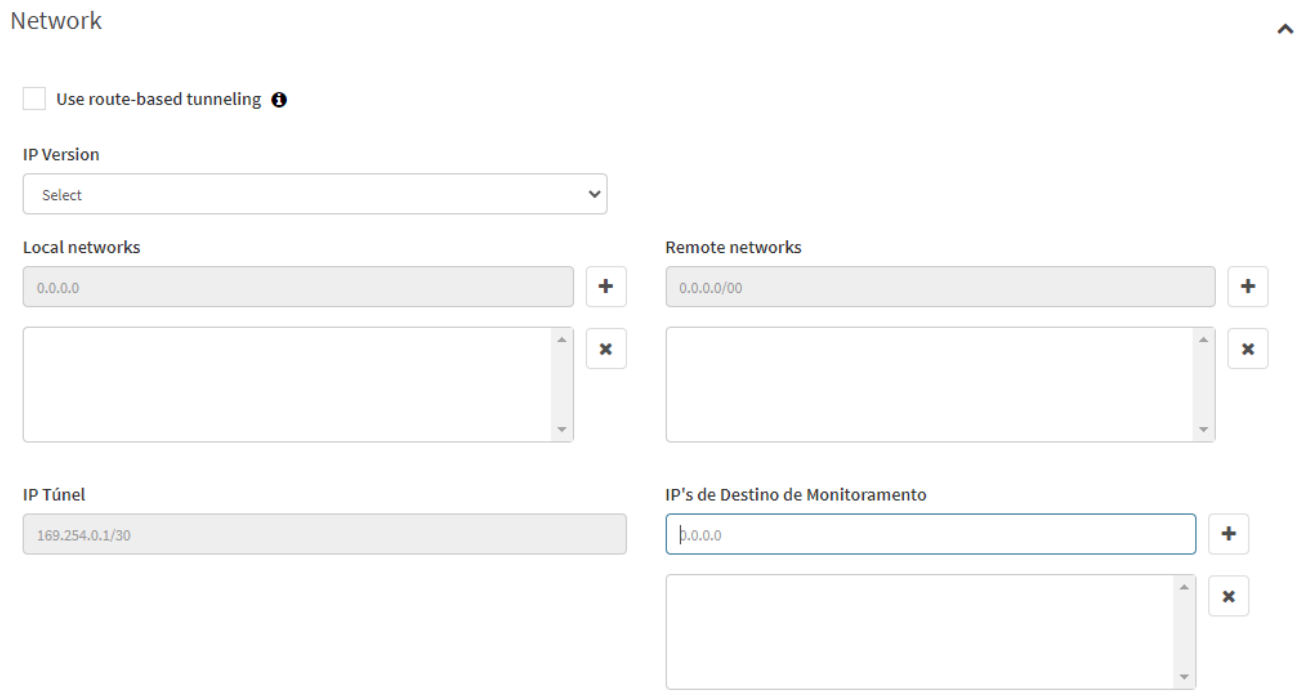
If using the RSA Key Authentication Method, the Local ID cannot be reused in another VPN.

- ***Shared Key:*** *If the option “Shared Key” is selected in “Authentication Method”, this field will be available and this is where the administrator can define the key that will be used to configure both points of the VPN*. It is essential for the correct functioning of the VPN that this field is the same among all devices in the server community;
- ***Local RSA Key:*** *If the option “RSA Key” is selected in “Authentication Method”, this field will be available and this is where the local key will be created, it will need to be entered in the “Remote RSA Key” field of another appliance to establish a connection*;
- ***Remote RSA Key:*** *If the option “RSA Key” is selected in “Authentication Method”, this field will be available and this is where the Local RSA KEY must be added in order to establish a connection*.
- ***XAuth Identity***: This field is used to insert the ID, if you are using the XAuth authentication method.
- ***XAuth Password***: This field is used to insert the password, if you are using the XAuth authentication method.

Below we will analyze each option available in the network panel:

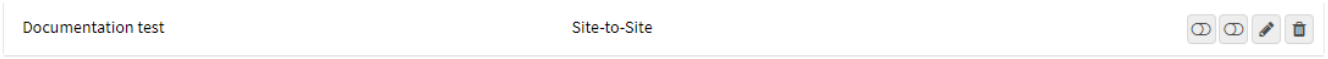
Network

The Network panel consists of the following features:

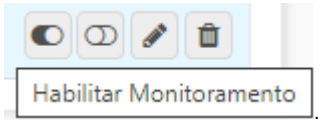


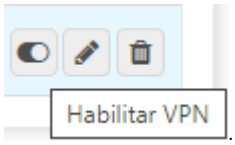
VPN IPSEC - Network

- ***Use route-based tunneling***: Allows the use of a private virtual network, where the traffic routing is held through the tunnel from the creation of a route through a specific interface;
- ***IP Version:*** *Inform the version of the network to be declared, which may be of the* ***IPv4*** *or* ***IPv6*** *type;*
- ***Local networks:*** *Declaration of local network / subnet IP addresses "not valid" from the LOCAL VPN site*. Ex.: *"172.16.10.0/24";*
- ***Remote networks:*** *Declaration of the IP network/subnet IP addresses "not valid" from the Remote VPN site*. Ex.: *"10.16.10.0/24";*
- ***IP Tunneling:*** Used to insert the tunnel's IP address.
- ***Destination IPs monitoring:*** Insert the IPs to be monitored and then click the add button [ ]. After having inserted the information, click the enable button [ ] to start the VPN monitoring, to disable, click the same button [ ]. With the monitoring enabled, the notifications also have to be enabled, as shown below:



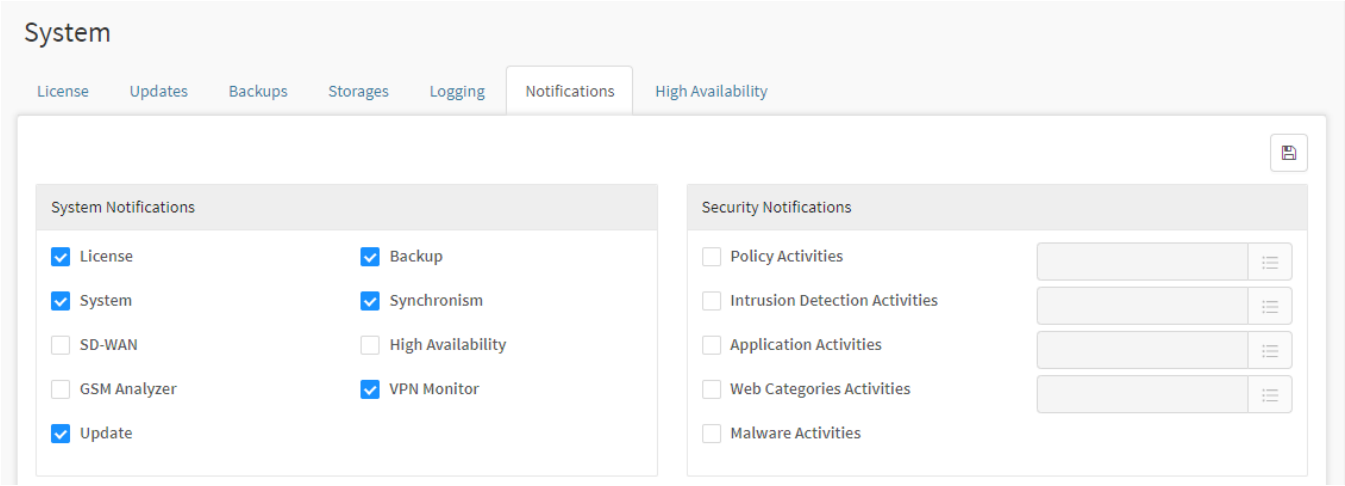
IPSec VPN Tunnel

- ***Enable/disable monitoring:*** Click [ ] to enable the VPN monitoring: 

.
- ***Enable VPN:*** With the Tunnel's settings complete, click [ ] to enable the VPN Tunnel: 

.
- ***Edit the VPN tunnel settings:*** Click this option to edit the VPN Tunnel's settings.
- ***Delete VPN:*** Click this button to delete a VPN Tunnel.

It's important to remember that to receive the notifications it is necessary to configure the email. Settings and enable this option in System Notifications System Notifications:



VPN Monitor notifications enabled

The "Network classes" that are not valid for VPN sites [Local / Remote], require that they are mandatorily in a "Different broadcast network class".

VPN networks using IKEv1, do not support the declaration of "Multiple networks".

VTI Configuration (Virtual Interface)

The virtual interface is used in the site-to-site VPN with BGP (Border Gateway Protocol). The tunnels are used to provide a cryptographed and encapsulated communication, through routes, between the peer and the host (Local NGFW) and the host (your VPN provider, ex: Google).

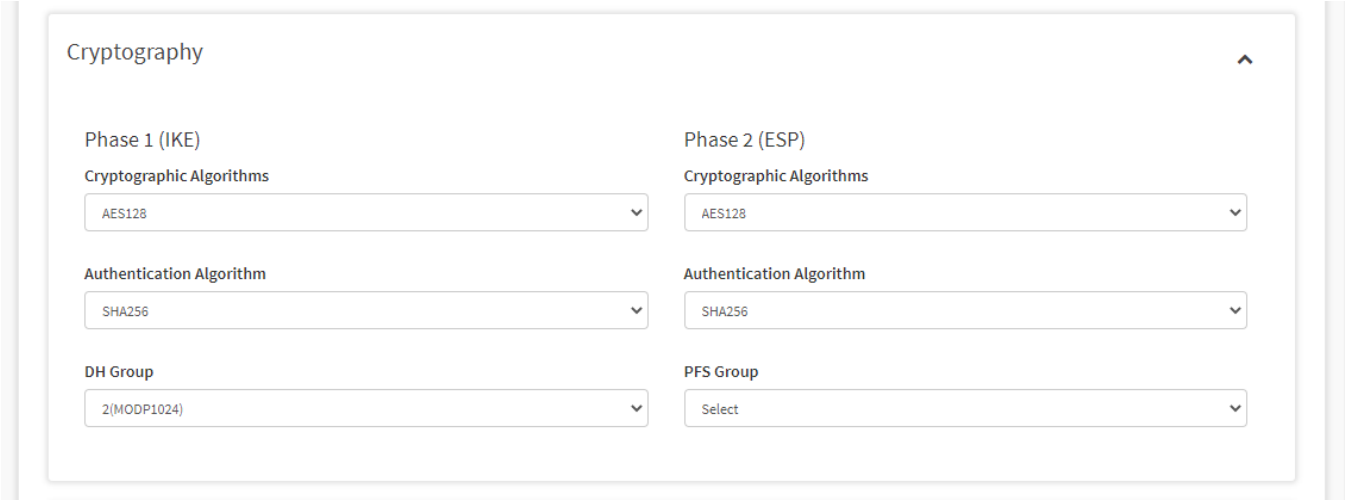
To set up, it's necessary to enable the "***Use route-based tunneling***" field and insert the information obtained when configuring the BGP in the host (tunnel IP).

It's important to remember that the BGP set up, which will provide the tunnel IP, is done in the host (VPN provider). For more information on this topic, access this page.

Next, we will analyze each available option in the Cryptography panel:

Cryptography

The Cryptography panel consists of the following features:



IPSEC VPN - Cryptography

- ***Phase 1* (*IKE*):** Based on the ISAKMP protocol (IKE / SA): defines the grouping of the phase authentication algorithms and technical specifications (IKE / SA) for the VPN device used to establish the VPN tunnel*:*
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *DH Group* (*Diffie Hellman*).

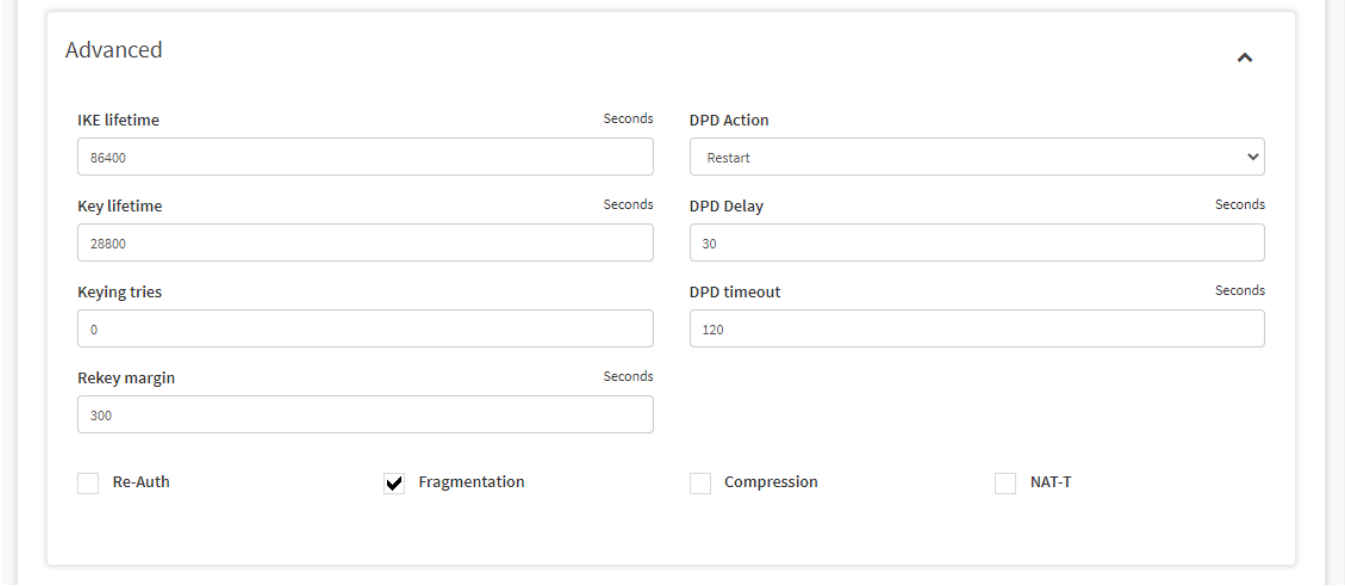
- ***Phase 2* (*ESP*):** The ESP protocol provides data confidentiality (encryption) and authentication (data integrity and data source authentication). ESP is based on the use of the AH (Authentication Header) and ESP (Encapsulating Security Payload) algorithms. Based on the AH and ESP protocols (ESP / AS): Defines the grouping of the phase authentication algorithms and technical specifications (IPSEC / SA) for the VPN device used to establish the VPN tunnel*:*
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *PFS Group*.

If there is any doubt about cryptography forms, check thee Remote Access - Cryptography page for a detailed explanation.

Below we will analyze each option available in the Advanced panel:

Advanced

The Advanced panel consists of the following features:



IPSEC VPN - Advanced

- ***IKE lifetime:*** *Determines the lifetime that the protocol (IKE or IPSEC depending on the phase) will wait to renegotiate the SA (Security Association), which specifies the algorithms to be used, the cryptographic keys, and the lifetime of these keys*. Lifetime must be determined in seconds. The IKE protocol is the IPSec authenticator and negotiator*;*
- ***Key lifetime:*** *Determines the validity time of the successful negotiation key*. Lifetime must be determined in seconds;
- ***Keying tries:*** *This is the number of times VPN points will renegotiate the tunnel or attempt re-authentication after the key expires*. Determines the number of attempts to establish the renegotiation in each IKE / IPSec negotiation phase*;*
- ***Rekey Margin:*** *Determines how long before the connection expires the VPN points and initiates the renegotiation of the tunnel keys*. Minimum time = 5 minutes. Maximum time = 9 minutes. This field is determined in seconds;
- ***DPD Action:*** *The DPD (Dead peer detection action) item controls the use of the lost VPN points detection protocol*. Where IKE v1 and IKE v2 notification messages are sent periodically to check if IPSec points are responding, or are lost; The selection of any value “clear”, “hold” and “restart”, activates the DPD service and determines the action to be performed in a time limit:
  - The “Clear” action closes, or closes the connection without taking any previous steps;
  - The “Hold” action sets up a strategic policy that captures traffic and tries to renegotiate the connection on demand;
  - The “Restart” action immediately initiates an attempt to renegotiate the connection;
  - The default is “None” or none, disables automatic sending of DPD messages.
- ***DPD Delay:*** *Defines the time interval or period in which informational IKE v1 and IKE v2 exchange messages are sent to VPN points*. Standard time 30 seconds. This field is determined in seconds;
- ***DPD timeout:*** *Sets the timeout interval for sending messages to IKE v1 after all connections to a VPN point are lost in the event of inactivity*. Standard time 150 seconds;

For IKE v2 the “DPD delay” retransmission timeout always applies. This field is determined in seconds.

- ***Re-Auth:*** *This check box allows you to enable the reauthentication process*. This feature has the function of renegotiating the IKE keys and checking the validity of the credentials, if this check box is disabled, the connection will remain active even if the certificate has expired;
- ***Fragmentation:*** *By enabling this checkbox, very long IKEv2 messages are fragmented into a set of smaller messages, which in turn are individually encrypted*. The function of this feature is to allow IKEv2 messages to be carried by network devices that do not allow the transport of IP fragments*;*
- ***Compression:*** *This checkbox enables the use of the IPComp protocol to compress the contents of IP packets in conjunction with IPsec encryption*. If both hosts have enough resources to carry out the compression process and if the link used is not showing any instability, communications between nodes is improved;

Small packets (for example: ICMP with default size), are not compressed. *Communication is done through an IPIP tunnel, making it necessary to release the standard service object: IPIP-ENCAPSULATION (IPv4 Encapsulation protocol) between peers through a Zone-Protection.*

For more information about compression check RFC 3173.

For more data on IP encapsulation within IP see RFC 2003.

For more information on fragmentation, see this *page*.

- ***NAT-T:*** *Enable the NAT-T (NAT Transversal) item if one of the VPN sites is behind an address translation (NAT) server "Firewall".* This enabled feature guarantees UDP encapsulation (UDP / 4500) and that packets trafficked will be translated correctly.

Habilitação obrigatória somente para o ***IKE* v1**.

After completing the appropriate settings, click **[**  **]** to save the settings, otherwise, click **[**  **]** to return.

At the end, you can validate your VPN settings using the following means:

- *Live Sessions - VPN* tab;
- In Security Events - VPN;

Using the CLI commands below:

- *debug-vpn -t ipsec*;
- *show-vpn-conn*;
- *show-vpn-info*.

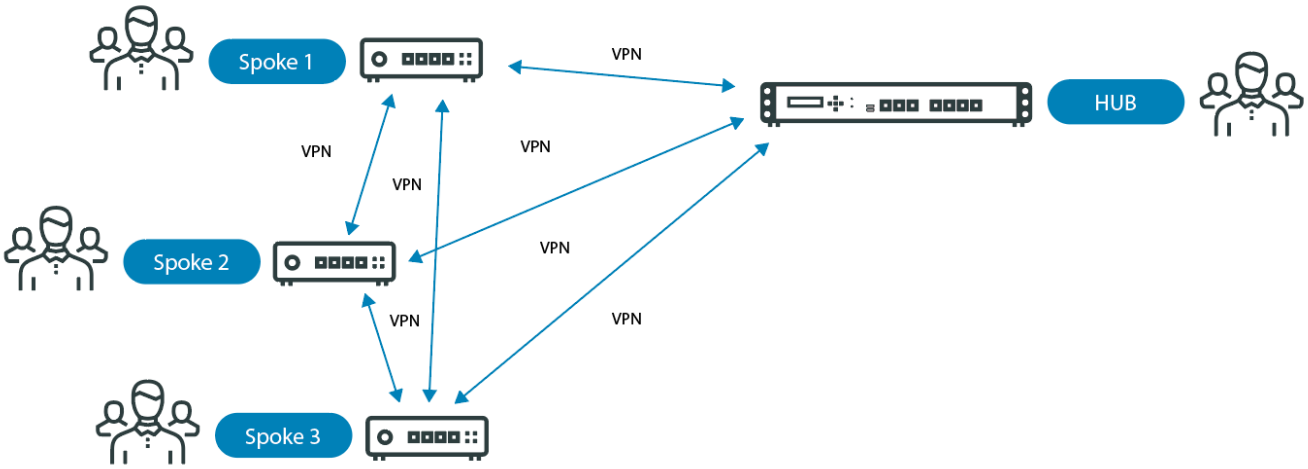
For more information, on each of these procedures, see the *Troubleshooting VPNs*.

Tunnels - Full-Mesh

In Full-Mesh VPN, all devices communicate with each other. Below is an example of a Full-Mesh Topology;

If the spokes have dynamic links (ADSL, Cable Modem, Satellite Link etc.), it is necessary that the devices allow connectivity to the Blockbit NGFW using the following protocols:

- *NAT-T (UDP Port: 4500);*
- *ISAKMP (UDP Port: 500);*
- *ESP (IP Protocol: 50);*
- *GRE (IP Protocol: 47).*



VPN IPSec - Full-Mesh Topology

When adding a tunnel, if the selected type was “Full-Mesh” when editing it [ ], the screen below will be displayed:

VPN IPSEC

Tunnels | Remote Access | Failover

General

Description
BB São Paulo x BB Miami

IKE version
IKEV1

Tunnel initialization
Wait

Shared Key
text alpha

Dynamic VPN

Type
Hub

Spokes Tun IP
0.0.0.0

Device
-

Port
1024 - 65535

Area
1 - 65535

IP Público/FQDN Local
IP/ fqdn

Network

IP Version
IPv4

Local networks
0.0.0.0

Cryptography

Phase 1 (IKE)

Cryptographic Algorithms
AES128

Authentication Algorithm
SHA256

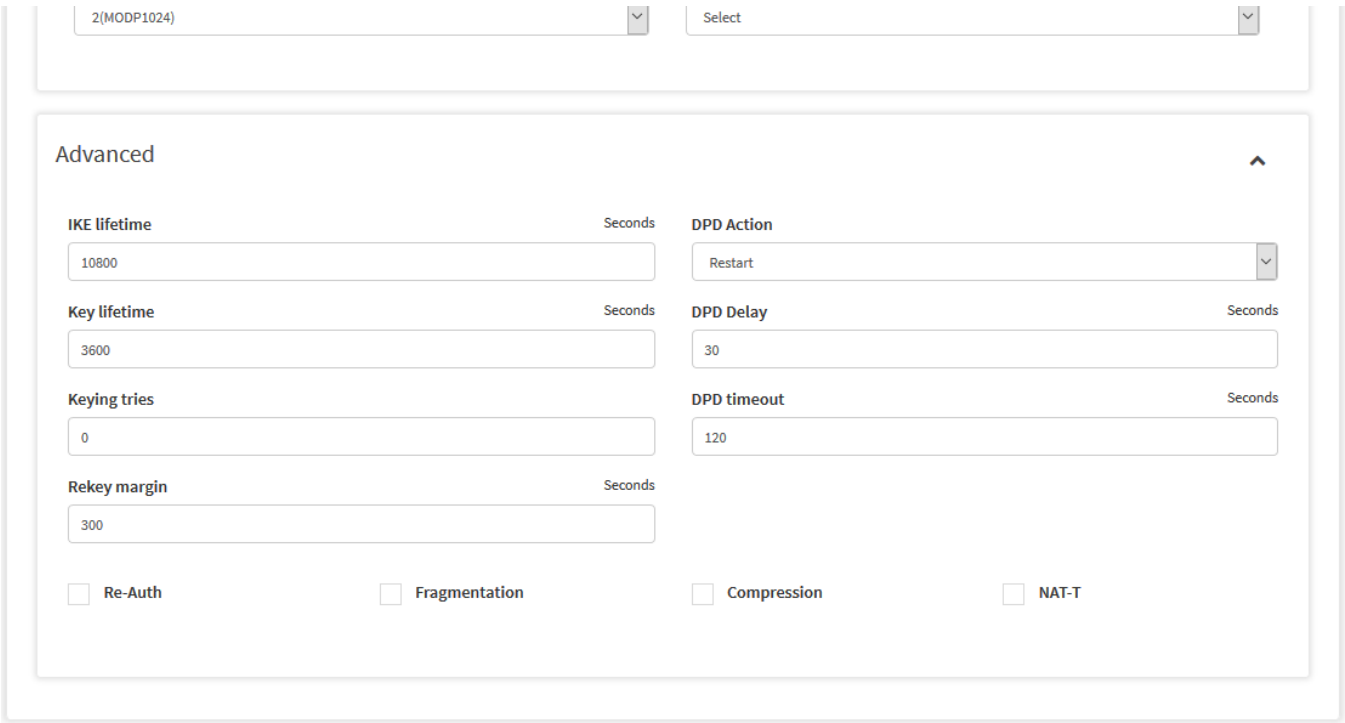
DH Group

Phase 2 (ESP)

Cryptographic Algorithms
AES128

Authentication Algorithm
SHA256

PFS Group



VPN IPSEC Settings – Full-Mesh

AD-VPN Support

Auto-Discovery VPN is an expansion of the IPSec protocol, which improves communication between sites in a VPN tunnel, it allows the generation of dynamic tunnels between different devices (spokes) using a convergent gateway (hub). One of the main benefits of AD-VPN is the fact that the central device (hub) automatically transmits the VPN settings and the information from authorized tunnels to the devices that will integrate the community of servers, this feature facilitates the insertion of new Spokes.

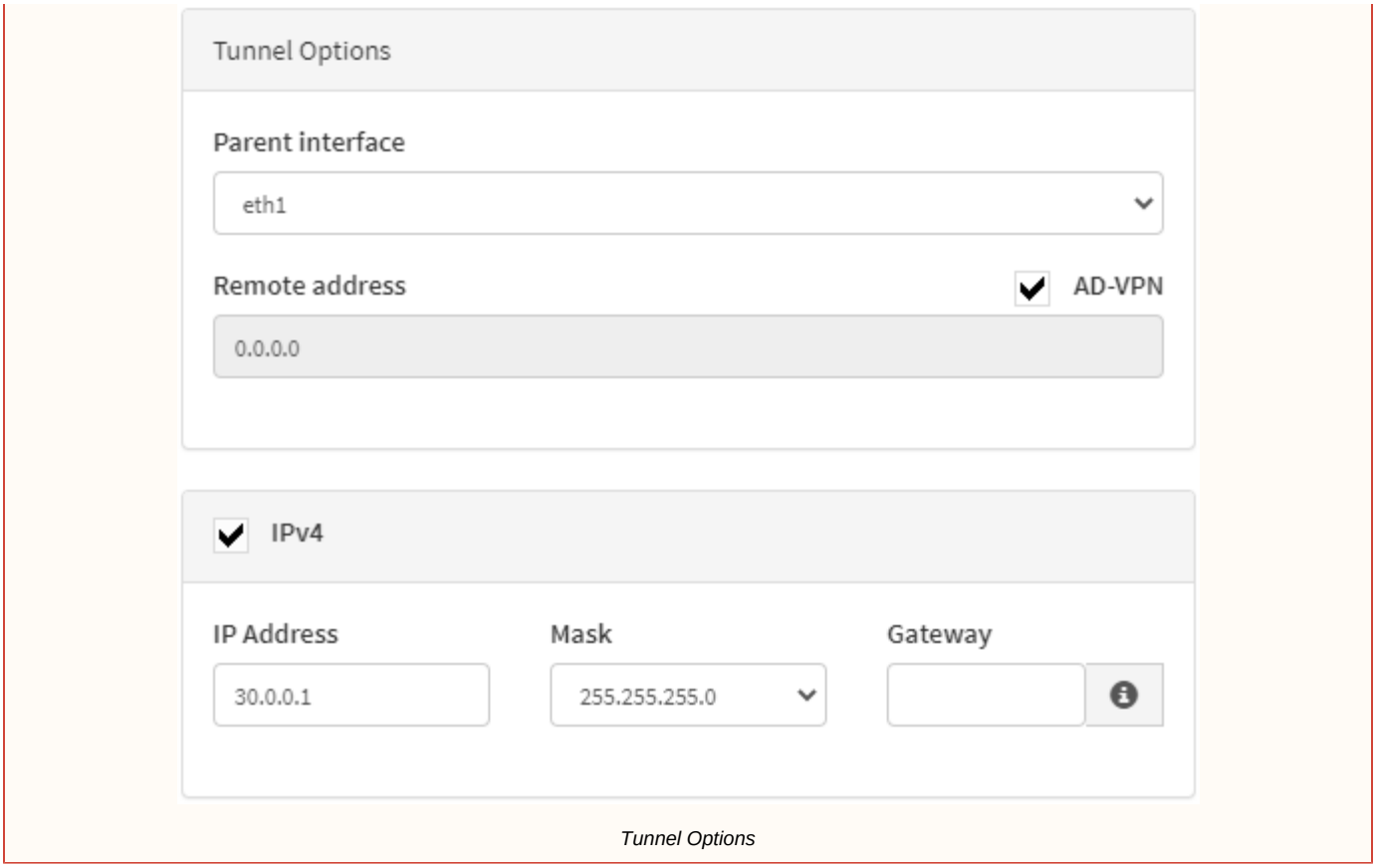
AD-VPN features are only available for *Star* and Full-Mesh VPNs.

Blockbit's AD-VPN was developed based on the BGP protocol, due to its ability to mirror the route, this protocol is particularly advantageous in the process of routing and maintaining the status of each connected link. This feature makes it possible to create direct VPN tunnels based on the most efficient route between devices that need to communicate.

During the process of creating an AD-VPN tunnel, it is mandatory to select a Tunnel type interface (GRE) so that the routes and dynamic routing settings are automatically applied. To create the appropriate interface, check the chapter *Tunnel Interface*.

As shown in the image below, to use a tunnel interface with AD-VPN it is necessary to:

- That the option "Dynamic" in "Remote Address" is checked;
- Let the mask be closed;
- The IP of the TUN interface must be less than 224.0.0.0/24. Ex. 30.0.0.1/255.255.255.255.



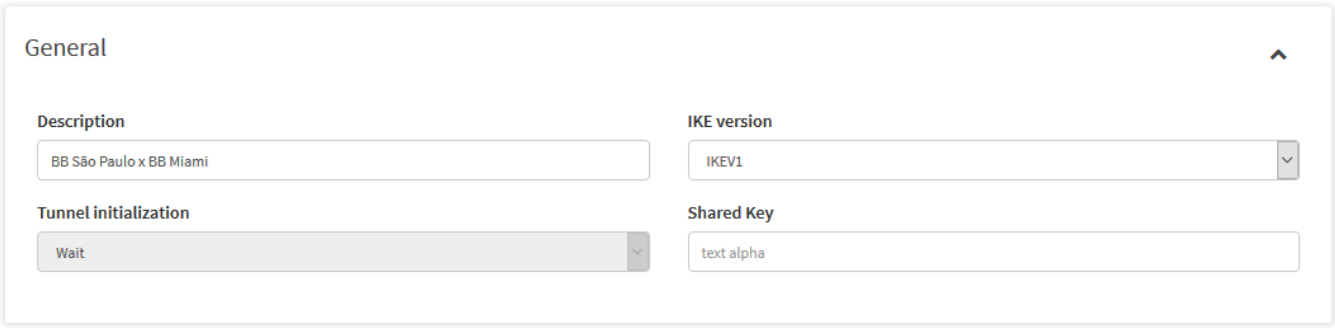
Tunnel Options

In an AD-VPN tunnel, the administrator must declare all networks that will be dynamically routed between the server community (Hub and Spoke).

Next, we'll look at how to set up a "Full-Mesh" tunnel.

General

Below we will analyze each option available in the general panel:



VPN IPSEC - General

- ***Description:*** *Field where the VPN description is being determined, which is being configured*;
- ***IKE version:*** *IKE - Internet Key Exchange is the protocol used to establish a security association (SA) in the IPSec protocol suite*. IKE is based on the Oakley and ISAKMP protocol, uses a PSK authentication key or X509 certificates and a “Diffie Hellman” key exchange;

The “PSK (Pre-shared key)” key type, and the “Diffie-Hellman” key exchange are used on the Blockbit NGFW. *The system supports the IKEV1 and IKEV2 versions.*

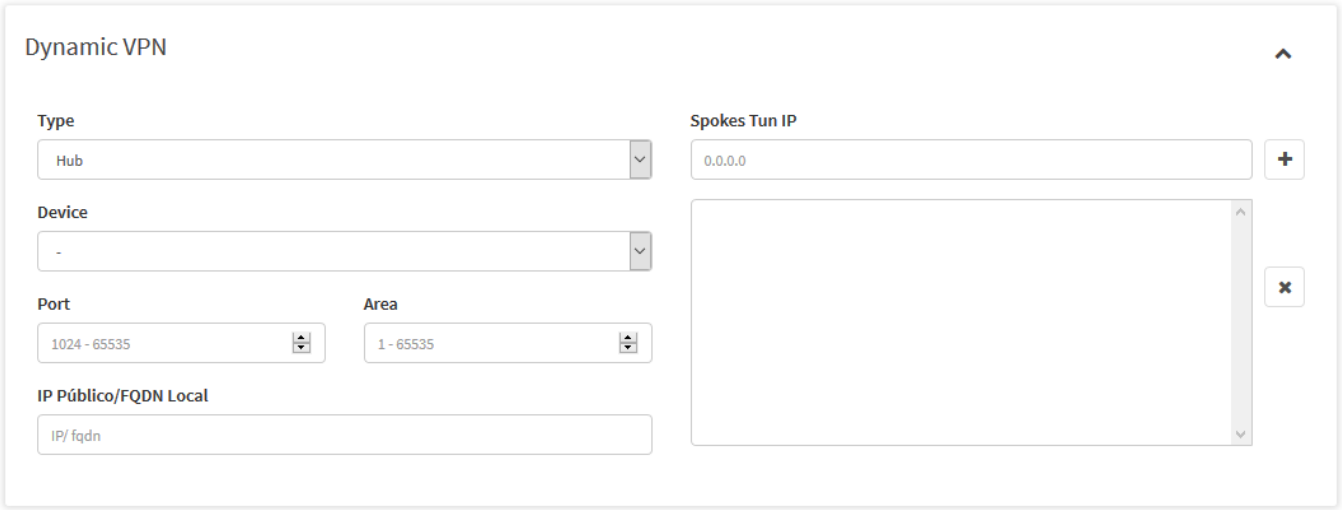
It is essential for the correct functioning of the VPN that all devices in this same server community are configured for the same IKE version.

- ***Tunnel initialization:*** *Determines how the tunnel will start, the available options are*:
  - ***Automatic*****:** Adds and initializes the Tunnel;
  - ***Wait*****:** Adds and does not initialize the Tunnel. Waiting for demand request (traffic) from the other end VPN;
  - ***On demand*****:** Initializes and raises the Tunnel only on demand, that is, when there is traffic from any VPN endpoint.
- ***Shared Key:*** *If the option “Shared Key” is selected in “Authentication Method”, this field will be available and this is where the administrator can define the key that will be used to configure both points of the VPN*. It is essential for the correct functioning of the VPN that this field is the same among all devices in the server community.

Below we will analyze each option available in the Dynamic VPN panel:

Dynamic VPN

The Dynamic VPN panel consists of the following features:



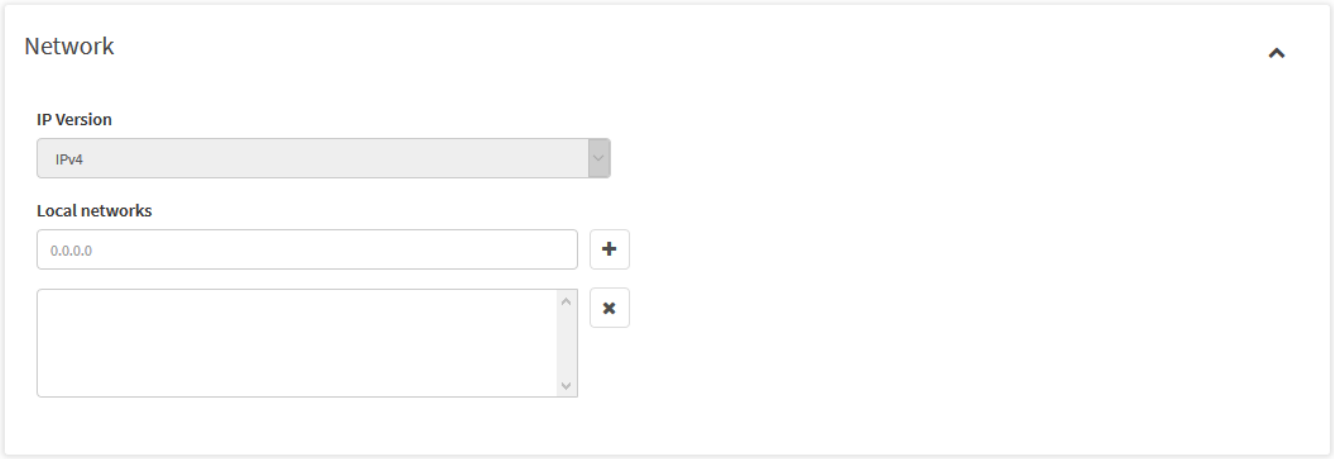
VPN IPSEC - Dynamic VPN

- ***Type:*** *Determines the device's server type, whether it will be used by the VPN as a Hub or a Spoke;*
- ***Device:*** *Determines the physical tunnel interface through which the VPN will exit*. To create the appropriate interface, see the chapter on adding T unnel Interface. It is necessary that in "Remote Address" the check box "Dynamic" is checked and in "IPv4" the mask needs to be closed. For more information check the section on AD-VPN Support;
- ***Port:*** *In this field you must add the port of the VPN dynamic routing service, the determined port can be any one, as long as it is within the range 1024 to 65535*. It is essential for the correct functioning of the VPN that this port is the same on the Hub and Spokes (depends on what is being configured);
- ***Area:*** *Informs the area that will be used by the VPN, the determined area can vary, as long as it is within the 1 to 65535 range*. It is an essential requirement for the correct functioning of the VPN that this area is the same in the Hub and in the Spokes (depends on what is being configured);
- ***Local IP:*** *Determines the IP of the next VPN hop, basically establishing where the packets will be forwarded to*. This field should include the IP of the Hub's physical interface, NOT the IP of the tunnel interface. It is essential for the correct functioning of the VPN that the IP entered in this field is the same on all devices in the server community;
- ***Spokes:*** *Lists all Spokes or Hubs that will be used by the VPN*. This is determined by what was selected in the “Type” item, if the server is of the “Hub” type, the IP of all Spoke servers must be informed, otherwise, in this field, only the IP of the device that must be informed if it is being used as a “Hub”. In this field, add the **IP of the tunnel interfaces** of each device (**not** the actual IP of the spokes).

Below we will analyze each option available in the network panel:

Network

The Network panel consists of the following features:



VPN IPSEC - Network

- ***IP Version:*** *Inform the version of the network to be declared, which may be of the* ***IPv4*** *or* ***IPv6*** *type;*
- ***Local networks:*** *Declaration of local network / subnet IP addresses "not valid" from the LOCAL VPN site. Ex.: "172.16.10.0/24".*

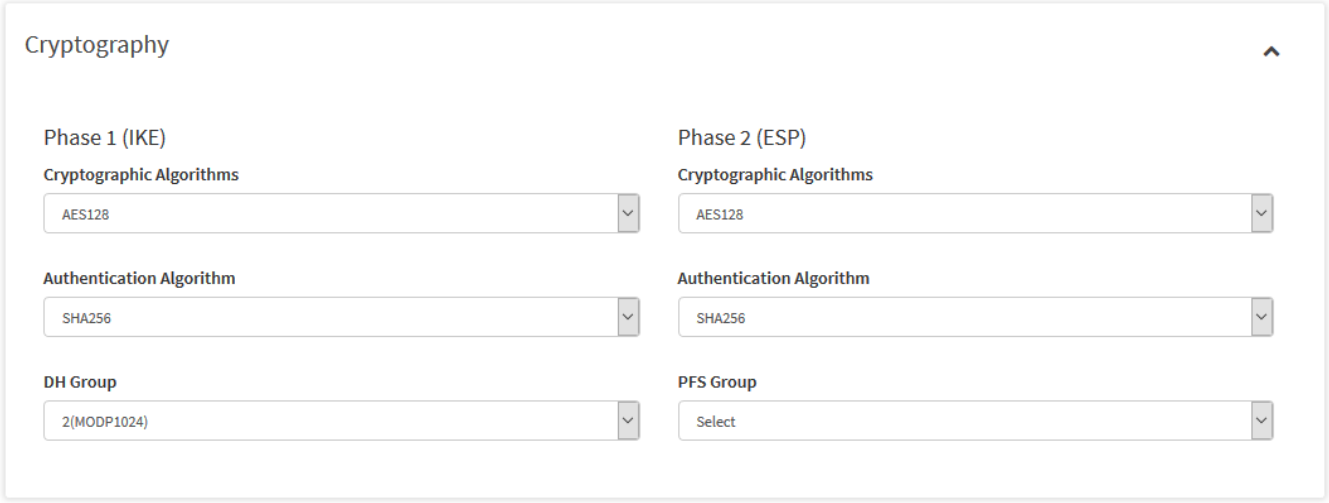
The "Network classes" that are not valid for VPN sites [Local / Remote], require that they are mandatorily in a "Different broadcast network class".

VPN networks using IKEv1, do not support the declaration of "Multiple networks".

Below we will analyze each option available in the Cryptography panel:

Cryptography

The Cryptography panel consists of the following features:



VPN IPSEC - Cryptography

- ***Phase* 1 (*IKE*):** Based on the ISAKMP protocol (IKE / SA): Defines the grouping of the phase authentication algorithms and technical specifications (IKE / SA) for the VPN device used to establish the VPN tunnel:
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *DH Group* (*Diffie-Hellman*).

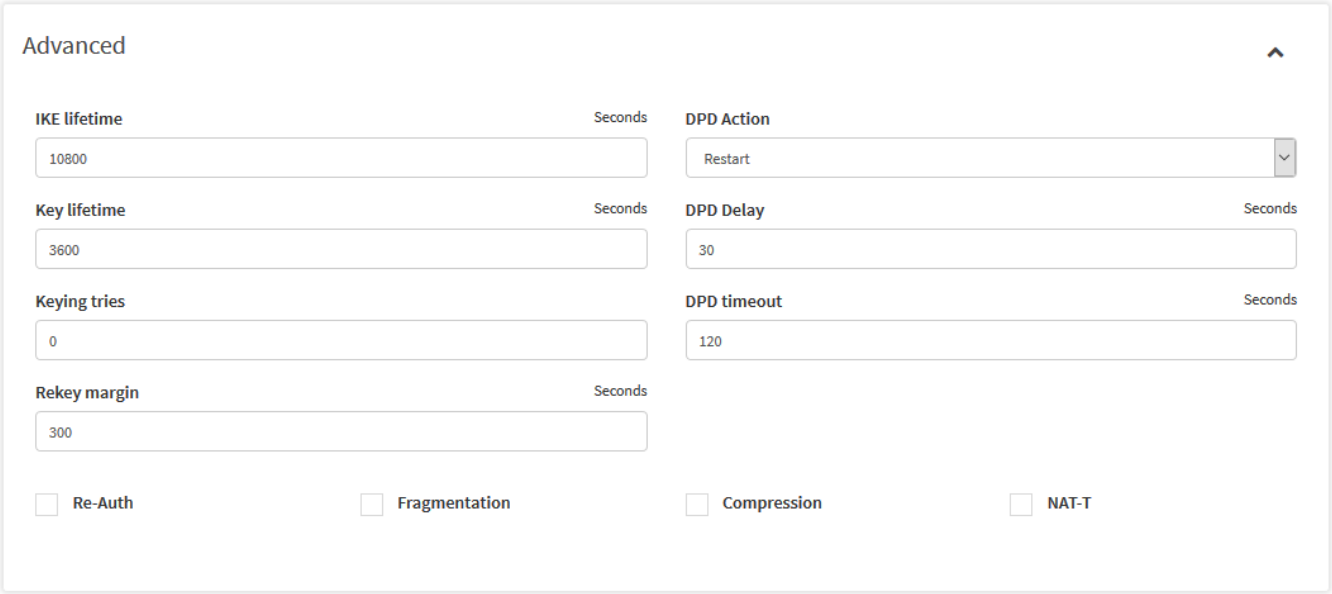
- ***Phase* 2 (*ESP*):** The ESP protocol provides data confidentiality (encryption) and authentication (data integrity and data source authentication). ESP is based on the use of the AH (Authentication Header) and ESP (Encapsulating Security Payload) algorithms. Based on the AH and ESP (ESP / AS) protocols: Defines the grouping of the phase authentication algorithms and technical specifications (IPSEC / SA) for the VPN device used to establish the VPN tunnel*:*
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *PFS Group*.

If there is any doubt about cryptography forms, check thee Remote Access - Cryptography page for a detailed explanation.

Below we will analyze each option available in the Advanced panel:

Advanced

The Advanced panel consists of the following features:



VPN IPSEC - Advanced

- ***IKE lifetime:*** *Determines the lifetime that the protocol (IKE or IPSEC depending on the phase) will wait to renegotiate the SA (Security Association), which specifies the algorithms to be used, the cryptographic keys, and the lifetime of these keys*. Lifetime must be determined in seconds. The IKE protocol is the IPSec authenticator and negotiator*;*
- ***Key lifetime:*** *Determines the validity time of the successful negotiation key*. Lifetime must be determined in seconds;
- ***Keying tries:*** *This is the number of times VPN points will renegotiate the tunnel or attempt re-authentication after the key expires*. Determines the number of attempts to establish the renegotiation in each IKE / IPSec negotiation phase*;*
- ***Rekey Margin:*** *Determines how long before the connection expires the VPN points and initiates the renegotiation of the tunnel keys*. Minimum time = 5 minutes. Maximum time = 9 minutes. This field is determined in seconds;
- ***DPDAction:*** *The DPD (Dead peer detection action) item controls the use of the lost VPN points detection protocol*. Where IKE v1 and IKE v2 notification messages are sent periodically to check if IPSec points are responding, or are lost. The selection of any value “clear”, “hold” and “restart”, activates the DPD service and determines the action to be performed in a time limit:
  - The “Clear” action closes, or closes the connection without taking any previous steps;
  - The “Hold” action sets up a strategic policy that captures traffic and tries to renegotiate the connection on demand;
  - The “Restart” action immediately initiates an attempt to renegotiate the connection;
  - The default is “None” or none, disables automatic sending of DPD messages.
- ***DPD Delay:*** *Defines the time interval or period in which informational IKE v1 and IKE v2 exchange messages are sent to VPN points*. Standard time 30 seconds. This field is determined in seconds;
- ***DPD timeout:*** *Sets the timeout interval for sending messages to IKE v1 after all connections to a VPN point are lost in the event of inactivity*. Standard time 150 seconds. This field is determined in seconds;

> ⚠ For IKE v2 the “DPD delay” retransmission timeout always applies.

- ***Re-Auth:*** *This check box allows you to enable the reauthentication process*. This feature has the function of renegotiating the IKE keys and checking the validity of the credentials, if this check box is disabled, the connection will remain active even if the certificate has expired;
- ***Fragmentation:*** *By enabling this checkbox, very long IKEv2 messages are fragmented into a set of smaller messages, which in turn are individually encrypted*. The function of this feature is to allow IKEv2 messages to be carried by network devices that do not allow the transport of IP fragments*;*
- ***Compression:*** *This checkbox enables the use of the IPComp protocol to compress the content of IP packets in conjunction with IPsec encryption*. If both hosts have enough resources to carry out the compression process and if the link used is not showing any instability, communications between nodes is improved;

> ⚠ Small packages (for example*: ICMP with default size), do not suffer compression. Communication is done through an IPIP tunnel, requiring the release of the standard service object: IPIP-ENCAPSULATION (IPv4 Encapsulation protocol) between peers through a Zone-Protection policy.*
>
> *For more information about compression check RFC 3173.*
>
> *For more data on IP encapsulation within IP see RFC 2003.*
>
> *For more information on fragmentation, see this page.*

- ***NAT-T:*** *Enable the NAT-T (NAT Transversal) item if one of the VPN sites is behind an address translation (NAT) server “Firewall”.* This feature guarantees UDP encapsulation (UDP / 4500) while enabled and that trafficked packets will be translated correctly.

Mandatory only for IKE v1.

After completing the appropriate settings, click **[**  **]** to save the settings, otherwise, click **[**  **]** to return.

At the end, you can validate your VPN settings using the following means:

- Through the *Live Sessions - VPN* tab;
- In Security Events - VPN;

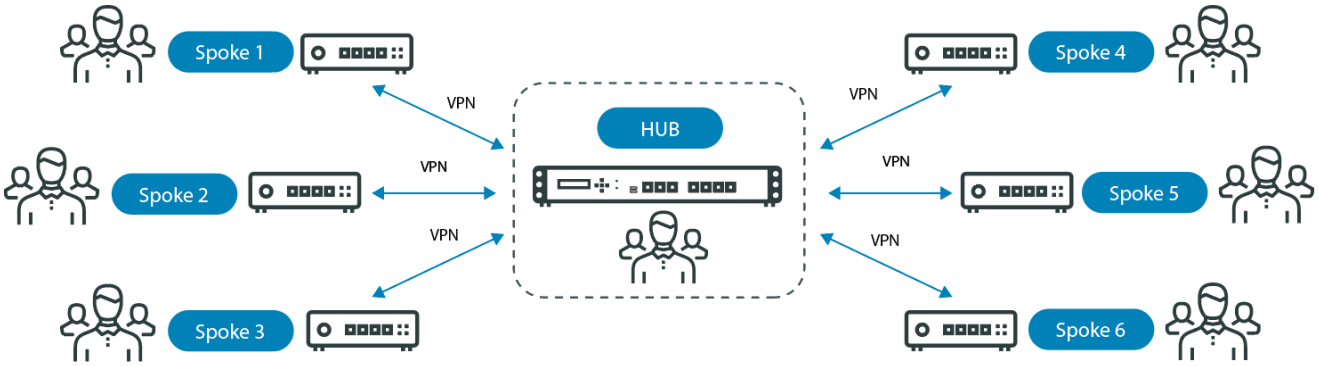
Using the CLI commands below:

- *debug-vpn -t ipsec*;
- *show-vpn-conn*;
- *show-vpn-info*.

For more information on each of these procedures, see the *VPN Troubleshooting* page.

Tunnels - Star

In the Star topology, all devices establish communication with a HUB (usually the company's headquarters), and this allows communication between devices, however, in a controlled manner. The following is an example:



IPSec VPN - Star Topology

When adding a tunnel, if the selected type was “Star” when editing it **[**  **]**, the screen below will be displayed:

VPN IPSEC

Tunnels | Remote Access | Failover

General

Description
BB São Paulo x BB Miami

IKE version
IKEV1

Tunnel initialization
Wait

Shared Key
text alpha

Dynamic VPN

Type
Hub

Device
-

Port
1024 - 65535

Area
1 - 65535

IP Público/FQDN Local
IP/ fqdn

Spokes Tun IP
0.0.0.0

Network

IP Version
IPv4

Local networks
0.0.0.0

Cryptography

Phase 1 (IKE)

Cryptographic Algorithms
AES128

Authentication Algorithm
SHA256

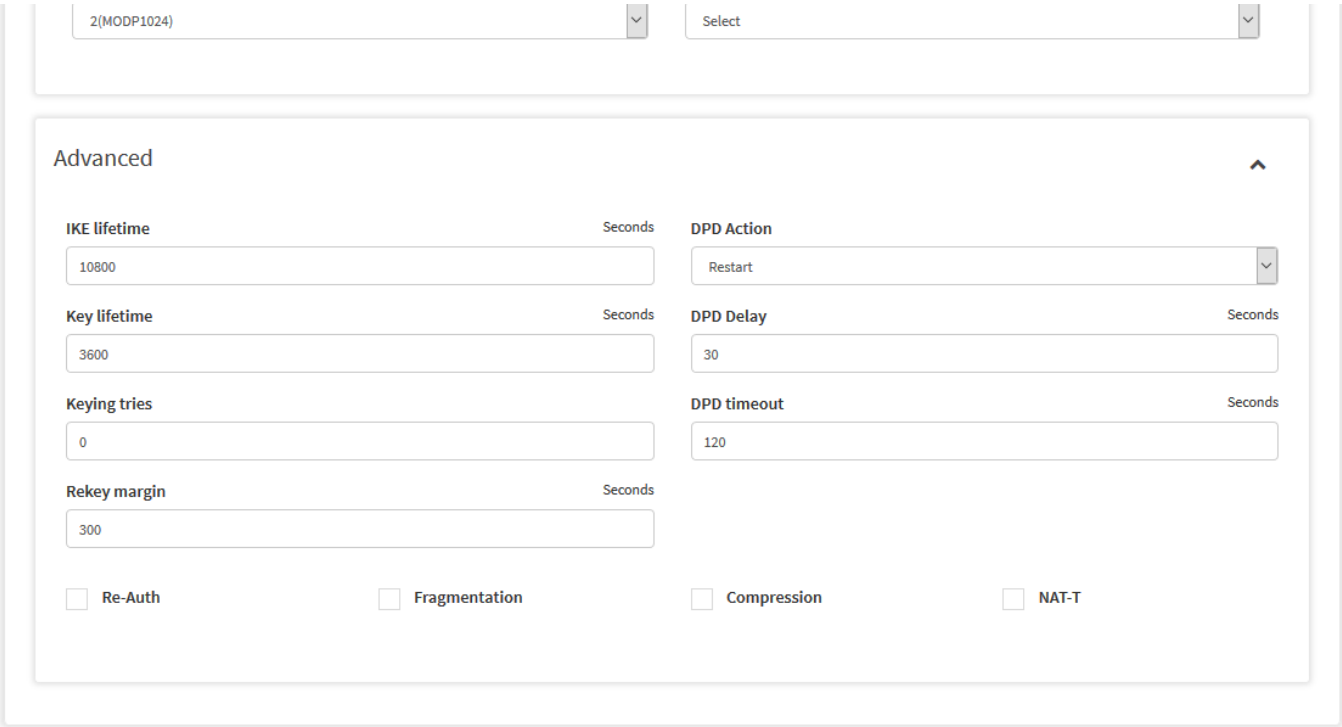
DH Group

Phase 2 (ESP)

Cryptographic Algorithms
AES128

Authentication Algorithm
SHA256

PFS Group



VPN IPSEC Settings – Star

AD-VPN support

Auto-Discovery VPN is an expansion of the IPsec protocol, which improves communication between sites in a VPN tunnel, it allows the generation of dynamic tunnels between different devices (spokes) using a convergent gateway (hub). One of the main benefits of AD-VPN is the fact that the central device (hub) automatically transmits the VPN settings and the information from authorized tunnels to the devices that will integrate the community of servers, this feature facilitates the insertion of new Spokes.

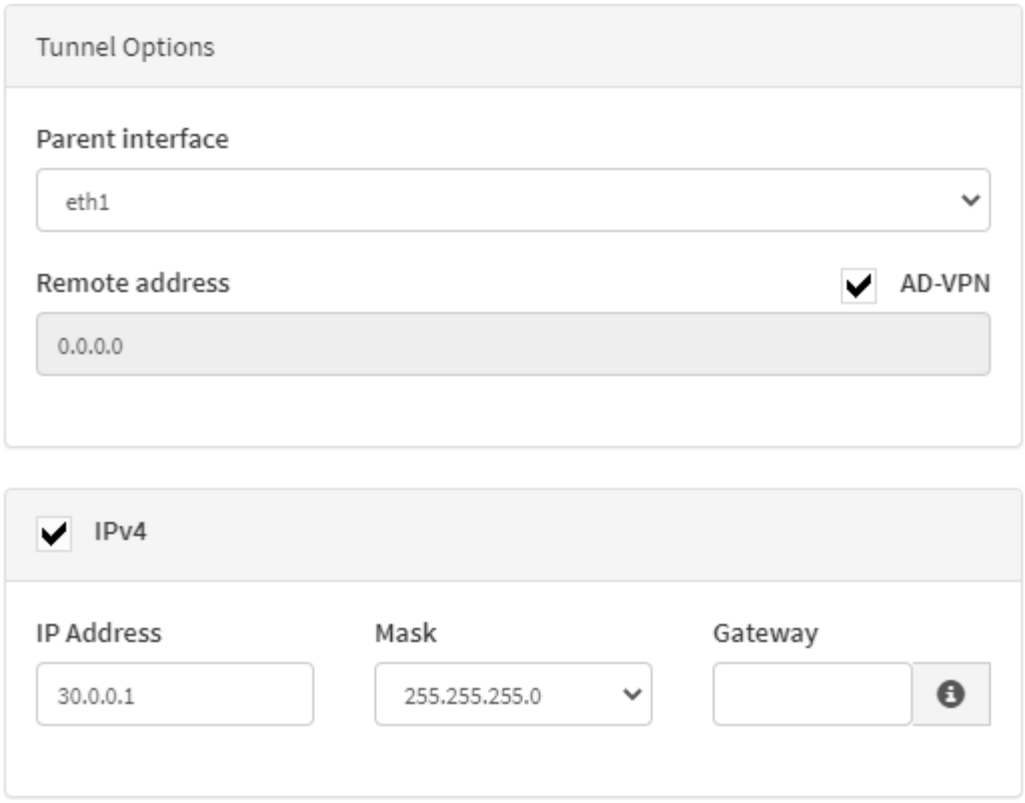
AD-VPN features are only available for Star and *Full-Mesh* VPNs.

Blockbit's AD-VPN was developed based on the BGP protocol, due to its ability to mirror the route, this protocol is particularly advantageous in the process of routing and maintaining the status of each connected link. This feature makes it possible to create direct VPN tunnels based on the most efficient route between devices that need to communicate.

During the process of creating an AD-VPN tunnel, it is mandatory to select a Tunnel type interface (GRE) so that the routes and dynamic routing settings are automatically applied. To create the proper interface, check the chapter *Tunnel Interfaces*.

As shown in the image below, to use a tunnel interface with AD-VPN it is necessary to:

- That the option "Dynamic" in "Remote Address" is checked;
- Let the mask be closed;
- The IP of the TUN interface must be less than 224.0.0.0/24. Ex. 30.0.0.1/255.255.255.255.



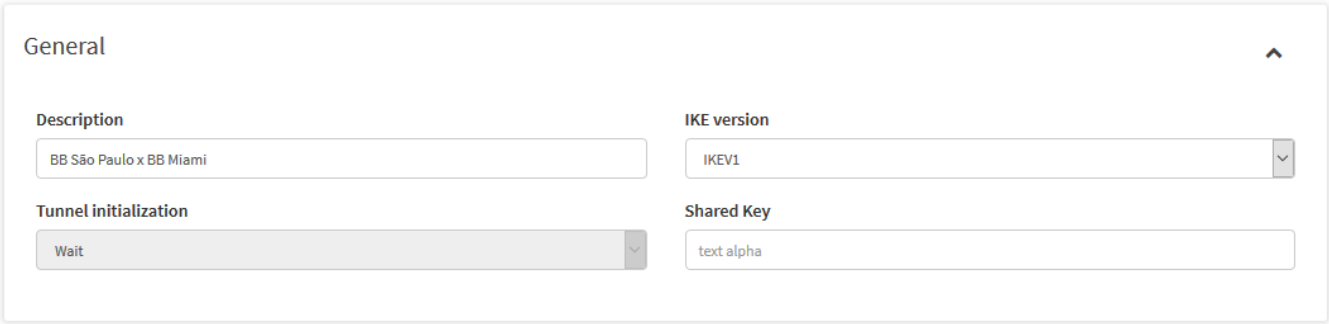
Tunnel Options

In an AD-VPN tunnel, the administrator must declare all networks that will be dynamically routed between the server community (Hub and Spoke).

Next, we'll look at how to set up a "Star" tunnel.

General

Below we will analyze each option available in the general panel:



VPN IPSEC - General

- ***Description:*** *Field where the VPN description is being determined, which is being configured*;

- ***IKE version:*** *IKE - Internet Key Exchange is the protocol used to establish a security association (SA) in the IPSec protocol suite*. IKE is based on the Oakley and ISAKMP protocol, uses a PSK authentication key or X509 certificates and a “Diffie-Hellman” key exchange;

The “PSK (Pre-shared key)” key type, and the “Diffie Hellman” key exchange are used on the Blockbit NGFW. *The system supports the IKEV1 and IKEV2 versions.*

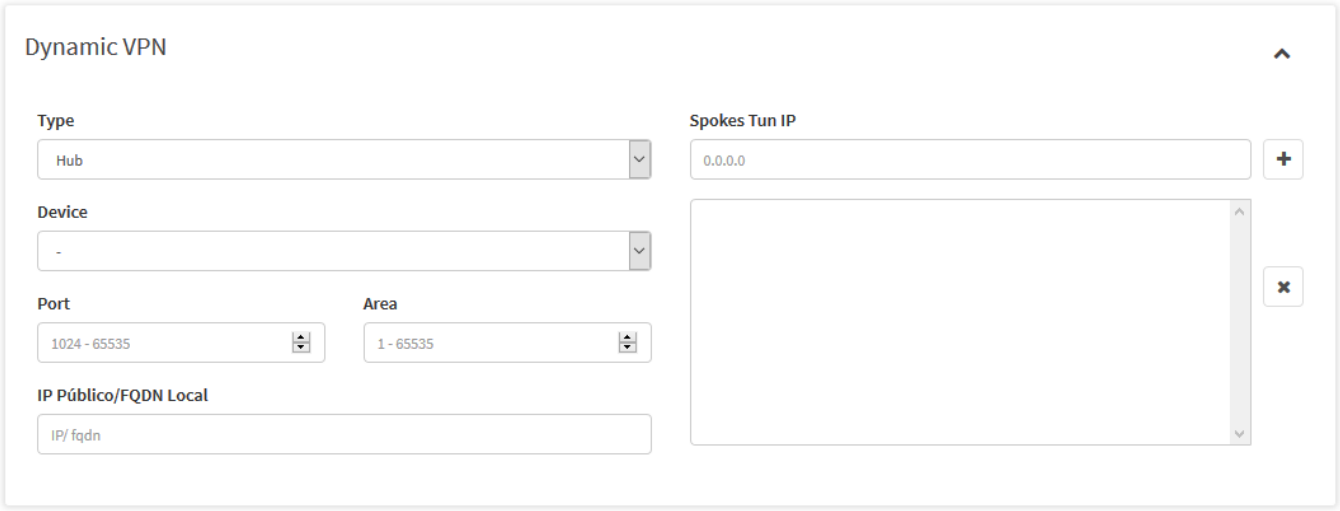
It is essential for the correct functioning of the VPN that all devices in this same server community are configured for the same IKE version.

- ***Tunnel initialization:*** *Determines how the tunnel will start, the available options are*:
  - ***Automatic*****:** Adds and initializes the Tunnel;
  - ***Wait*****:** Adds and does not initialize the Tunnel. Waiting for demand request (traffic) from the other end VPN;
  - ***On demand*****:** Initializes and raises the Tunnel only on demand, that is, when there is traffic from any VPN endpoint.
- ***Shared Key:*** *If the “Shared Key” option is selected in “Authentication Method”, this field will be available and this is where the administrator can define the key that will be used to configure both points of the VPN*. It is essential for the correct functioning of the VPN that this field is the same among all devices in the server community..

Below we will analyze each option available in the Dynamic VPN panel:

Dynamic VPN

The Dynamic VPN panel consists of the following features:



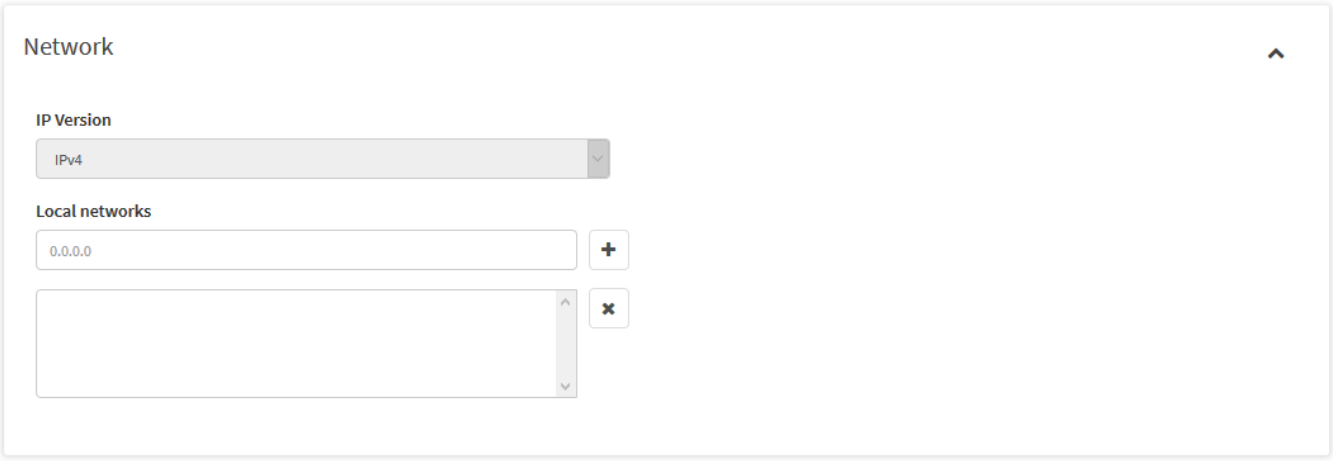
VPN IPSEC - Dynamic VPN

- ***Type:*** *Determines the device's server type, whether it will be used by the VPN as a Hub or Spoke;*
- ***Device:*** *Determines the physical tunnel interface through which the VPN will exit*. To create the appropriate interface, see the chapter on adding Tunnel Interfaces. It is necessary that in "Remote Address" the check box "Dynamic" is checked and in "IPv4" the mask needs to be closed. For more information check the section on AD-VPN Support;
- ***Port:*** *In this field you must add the port of the VPN dynamic routing service, the determined port can be any one, as long as it is within the range 1024 to 65535*. It is essential for the correct functioning of the VPN that this port is the same on the Hub and Spokes (depends on what is being configured);
- ***Area:*** *Informs the area that will be used by the VPN, the determined area can be any one, as long as it is within the range 1 to 65535*. It is an essential requirement for the correct functioning of the VPN that this area is the same in the Hub and in the Spokes (depends on what is being configured);
- ***Local IP:*** *Determines the IP of the next VPN hop, basically establishing where the packets will be forwarded to*. This field should include the IP of the Hub's physical interface, NOT the IP of the tunnel interface. It is essential for the correct functioning of the VPN that the IP entered in this field is the same on all devices in the server community.;
- ***Spokes:*** *Lists all Spokes or Hubs that will be used by the VPN*. This is determined by what was selected in the “Type” item, if the server is of the “Hub” type, the IP of all Spoke servers must be informed, otherwise, in this field, only the IP of the device that must be informed. if it is being used as a “Hub”. In this field, you must add the IP of the tunnel interfaces of each device.

Below we will analyze each option available in the network panel:

Network

The Network panel consists of the following features:



VPN IPSEC - Network

- ***IP Version:*** *Inform the version of the network to be declared, which may be of the* ***IPv4*** *or* ***IPv6*** *type****;***
- ***Local networks:*** *Declaration of local network / subnet IP addresses "not valid" from the LOCAL VPN site*. Ex.: *"172.16.10.0/24".*

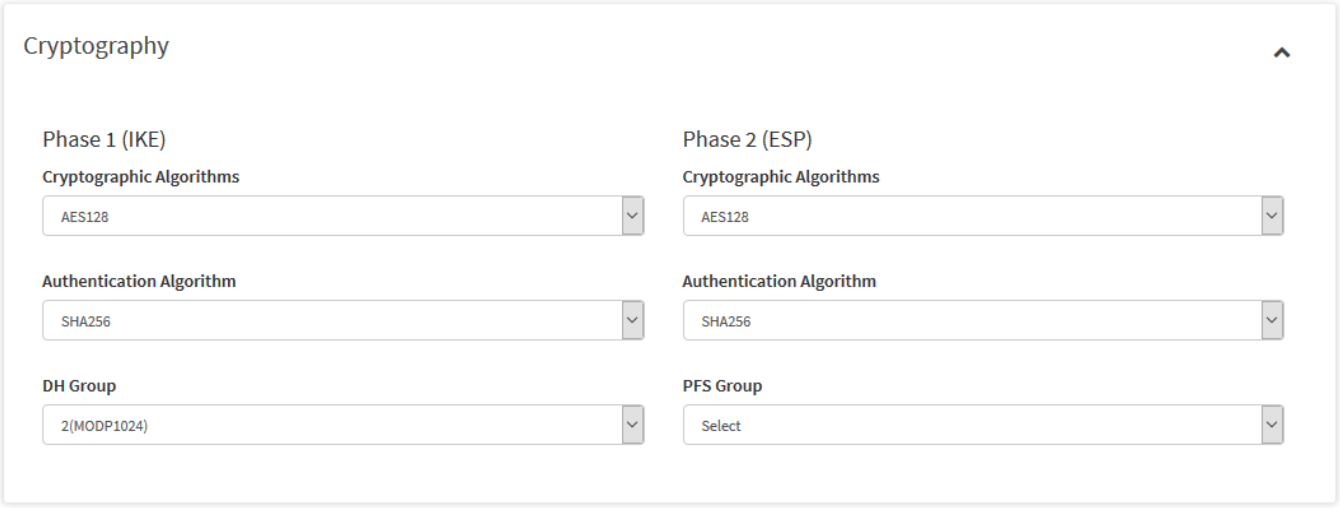
The "Network classes" that are not valid for VPN sites [Local / Remote], require that they are mandatorily in a "Different broadcast network class".

VPN networks using IKEv1, do not support the declaration of "Multiple networks".

Below we will analyze each option available in the Cryptography panel:

Cryptography

The Cryptography panel consists of the following features:



VPN IPSEC - Cryptography

- ***Phase* 1 (*IKE*):** Based on the ISAKMP protocol (IKE / SA): defines the grouping of the phase authentication algorithms and technical specifications (IKE / SA) for the VPN device used to establish the VPN tunnel*:*
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *DH Group* (*Diffie-Hellman*).

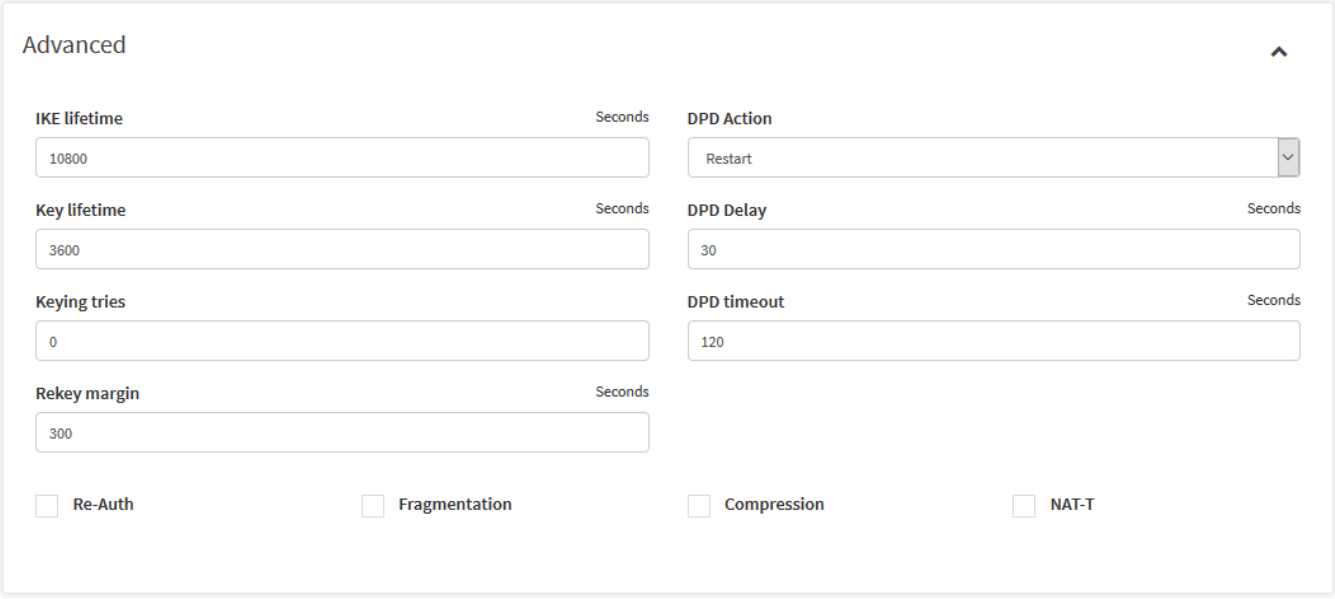
- ***Phase* 2 (*ESP*):** The ESP protocol provides data confidentiality (encryption) and authentication (data integrity and data source authentication). ESP is based on the use of the AH (Authentication Header) and ESP (Encapsulating Security Payload) algorithms. Based on the AH and ESP protocols (ESP / AS): Defines the grouping of the phase authentication algorithms and technical specifications (IPSEC / SA) for the VPN device used to establish the VPN tunnel*:*
  - *Cryptographic Algorithms*;
  - *Authentication Algorithm*;
  - *PFS Group*.

If there is any doubt about cryptography forms, check thee Remote Access - Cryptography page for a detailed explanation.

Below we will analyze each option available in the Advanced panel:

Advanced

The Advanced panel consists of the following features:



VPN IPSEC - Advanced

- ***IKE lifetime:*** Determines the lifetime that the protocol (IKE or IPSEC depending on the phase) will wait to renegotiate the SA (Security Association), which specifies the algorithms to be used, the cryptographic keys, and the lifetime of these keys. Lifetime must be determined in seconds. The IKE protocol is the IPSec authenticator and negotiator*;*
- ***Key lifetime:*** Determines the validity time of the successful negotiation key. Lifetime must be determined in seconds;
- ***Keying tries:*** *This is the number of times VPN points will renegotiate the tunnel or attempt re-authentication after the key expires*. Determines the number of attempts to establish the renegotiation in each IKE / IPSec negotiation phase*;*
- ***Rekey Margin:*** *Determines how long before the connection expires the VPN points and initiates the renegotiation of the tunnel keys*. Minimum time = 5 minutes. Maximum time = 9 minutes. This field is determined in seconds;
- ***DPD Action:*** *The DPD (Dead peer detection action) item controls the use of the lost VPN points detection protocol*. Where IKE v1 and IKE v2 notification messages are sent periodically to check if IPSec points are responding, or are lost. The selection of any value “clear”, “hold” and “restart”, activates the DPD service and determines the action to be performed in a time limit:
  - The “Clear” action closes, or closes the connection without taking any previous steps;
  - The “Hold” action sets up a strategic policy that captures traffic and tries to renegotiate the connection on demand;
  - The “Restart” action immediately initiates an attempt to renegotiate the connection;
  - The default is “None” or none, disables automatic sending of DPD messages.
- ***DPD Delay:*** *Defines the time interval or period in which informational IKE v1 and IKE v2 exchange messages are sent to VPN points*. Standard time 30 seconds. This field is determined in seconds;
- ***DPD timeout:*** *Sets the timeout interval for sending messages to IKE v1 after all connections to a VPN point are lost in the event of inactivity*. Standard time 150 seconds. This field is determined in seconds;

> ⚠ For IKE v2 the “DPD delay” retransmission timeout always applies.

- ***Re-Auth:*** *This check box allows you to enable the reauthentication process*. This feature has the function of renegotiating the IKE keys and checking the validity of the credentials, if this check box is disabled, the connection will remain active even if the certificate has expired;
- ***Fragmentation:*** *By enabling this checkbox, very long IKEv2 messages are fragmented into a set of smaller messages, which in turn are individually encrypted*. The function of this feature is to allow IKEv2 messages to be carried by network devices that do not allow the transport of IP fragments*;*
- ***Compression:*** *This checkbox enables the use of the IPComp protocol to compress the content of IP packets in conjunction with IPsec encryption*. If both hosts have enough resources to carry out the compression process and if the link used is not showing any instability, communications between nodes is improved;

> ⚠ Small packets (for example: ICMP with default size), are not compressed. *Communication is done through an IPIP tunnel, requiring the release of the standard service object:IPIP-ENCAPSULATION (IPv4 Encapsulation protocol) between peers through a Zone-Protection policy.*
>
> *For more information about compression check RFC 3173.*
>
> *For more data on IP encapsulation within IP see RFC 2003.*
>
> *For more information on fragmentation, see this page.*

- **NAT-T:** Enable the NAT-T (NAT Transversal) item if one of the VPN sites is behind an address translation (NAT) server “Firewall”. This feature guarantees UDP encapsulation (UDP / 4500) while enabled and that trafficked packets will be translated correctly.

Mandatory only for IKE v1.

After completing the appropriate settings, click **[**  **]** to save the settings, otherwise, click **[**  **]** to return.

At the end, you can validate your VPN settings using the following means:

- Through the *Live Sessions - VPN* tab;
- In Security Events - VPN;

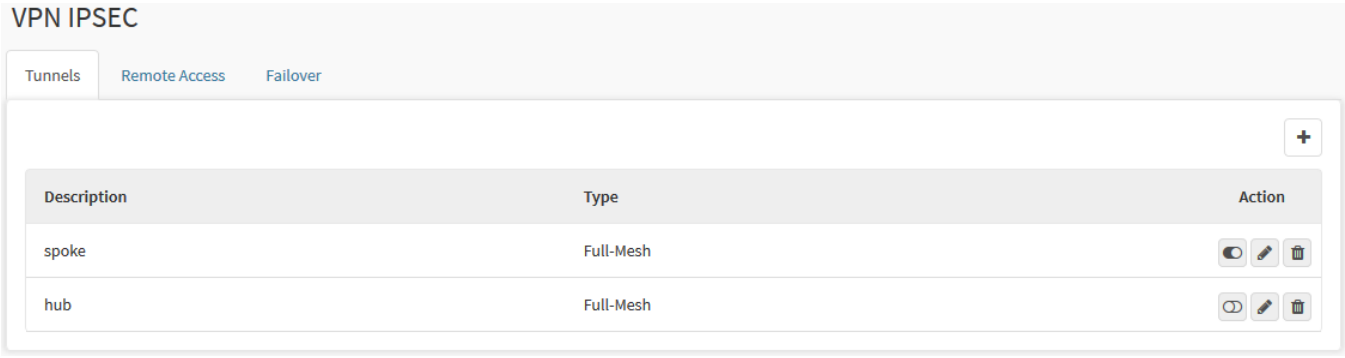
Using the CLI commands below:

- *debug-vpn -t ipsec*;
- *show-vpn-conn*;
- *show-vpn-info*.

For more information on each of these procedures, see the *VPN Troubleshooting* page.

Tunnels - Columns

Next we will analyze each column of the IPSEC VPN screen - Tunnels Tab:

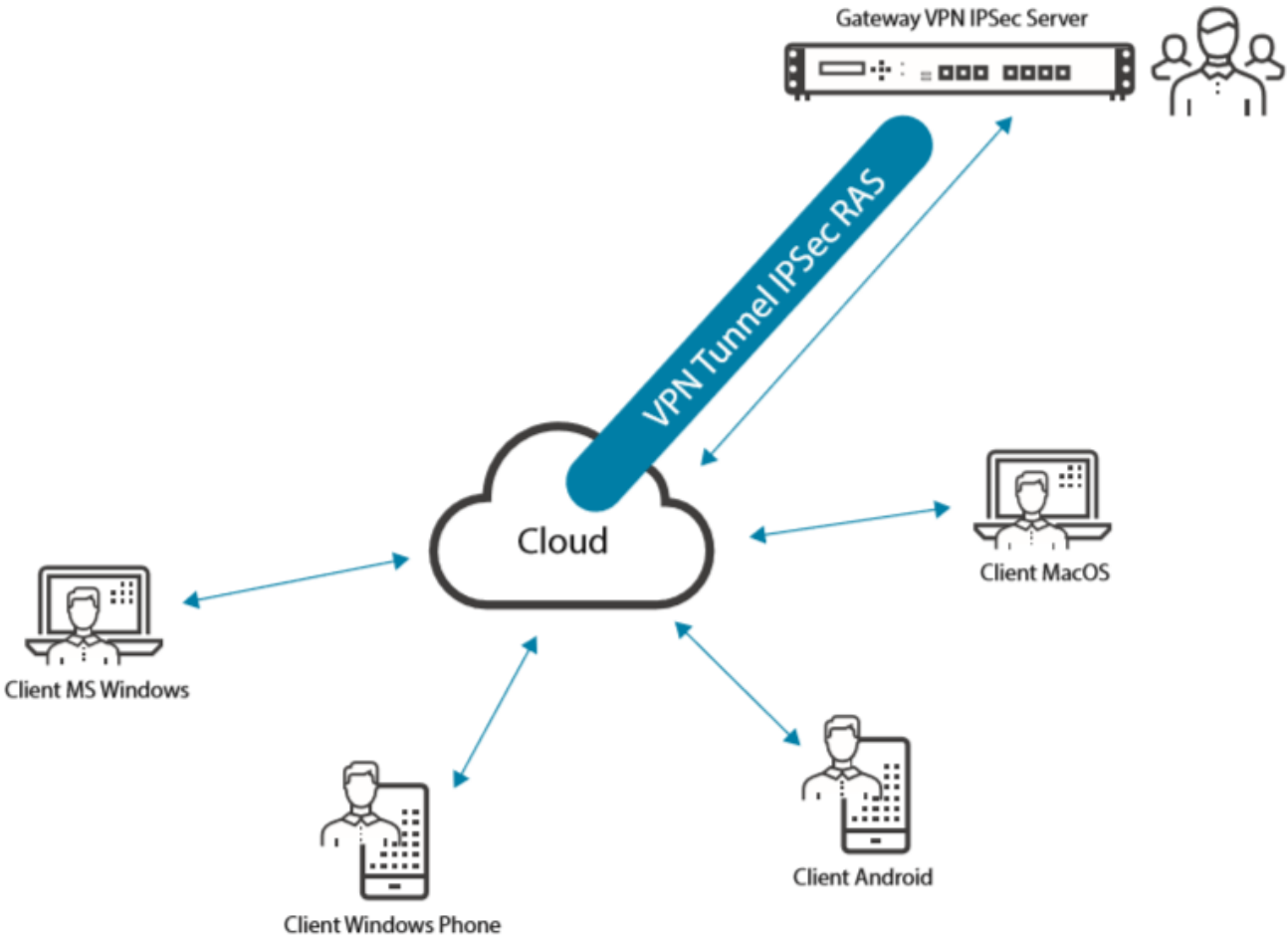


VPN IPSEC - Tunnels

- ***Description*:** Displays the description recorded during the process of adding a VPN tunnel;
- ***Type*:** Determines the type of VPN selected during the process of adding the tunnel*:*
  - *Site-to-Site*;
  - *Full-Mesh*;
  - *Star*;
- ***Action*:** It has a set of essential buttons, these being:
  - ***Enable*[ ]/*Disable*[ ]:** This column enables or disables the VPN tunnel;
  - ***Edit*[ ]:** This button allows you to edit the settings for a VPN connection;
  - ***Delete*[ ]:** Removes a VPN connection.

VPN IPSEC - Remote Access tab

The IPSEC Remote Access VPN method allows you to configure a remote access server providing users with secure access to the internal network through any connection on a public network (Internet). This model defines that the accesses will be made through a client connection with PSK type keys and authentication of the types: X-Auth or EAP-MSCHAP V2.



VPN IPSec - IPSec RAS mode

When configuring the IPSEC RAS VPN, it is recommended to correctly consider the following checks and requirements:

1. Identify LAN network addresses of the Blockbit NGFW (VPN) server. Then define the addressing of the "Virtual VPN RAS Network" in a different class / subnet:

- Local network identification. Ex.: *“192.168.1.0/24”;*
- Remote network definition. Ex.: *“10.0.100.0/24”.*

2. What model of RAS VPN hardware / application (remote point)?

- Must be compatible with iOS 7 or higher, Android 4.4.4 or higher, MacOS X 10.6 or higher, Linux 2.6.36 or higher, Windows 7 or higher.

3. Define an encryption key (PSK - Pre Shared key);

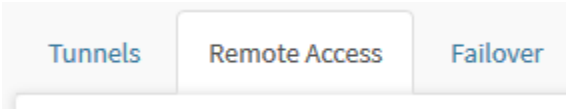
4. Define / identify the parameters for phase 1 configuration (IKE / SA):

- IKE Parameters (Phase 1) - IKE support version 2. Example.:
  - Cryptography: “3DES, DES”;
  - Authentication (HASH): “SHA 1”;
  - Diffie-hellman (DH Group: “mob 8192”).

5. Define / identify the parameters for phase 2 configuration (IPSEC / ESP):

- IPSEC ESP parameters (Phase 2). Example.:
  - Cryptography: “ESP-3DES, DES”;
  - Authentication: “SHA 1”;
  - Use PFS - Perfect Forward Secrecy: “No”.

To configure and enable IPSEC RAS VPN tunnels, access the Remote Access tab:



Remote Access tab

The screen below will be displayed:

VPN IPSEC

Tunnels | Remote Access | Failover

IKEv1

Enable

Authentication Method

Shared Key

Shared Key

Certificate Authority

Select

Service Certificate

Select

Revokation List

Select

Users

Add tag

Groups

Add tag

IKEv2

Enable

Authentication Method

Device/User/Password

Certificate Authority

Local Root CA

Service Certificate

utm.blockbit.com

Revokation List

Select

Device	User	Password
Device	User	Password

Network

IPv4 IPv6

Virtual Network

IPv4/CIDR

IP/User Attribute

Device IP address

User

Range

Begin

End

DNS Suffix

DNS Suffix

DNS 1

DNS server address

DNS 2

DNS server address

Cryptography

Phase 1 (IKE)

Cryptography Algorithm	Authentication Algorithm	DH Group
Select	Select	Select

Phase 2 (ESP)

Cryptography Algorithm	Authentication Algorithm	PFS GROUP
Select	Select	Select

Advanced

VPN IPSEC – Remote Access

ATTENTION: When configuring a VPN RAS it is necessary that the *Concurrent sessions field in the Settings menu, Authentication in the Settings tab*, must be at least with value 2. This is due to the fact that the agent performs an authentication for valid IP and another for virtual IP during the process of acquiring the VPN establishment.

Below specifications of the configuration items for both versions of the ISAKMP protocol.

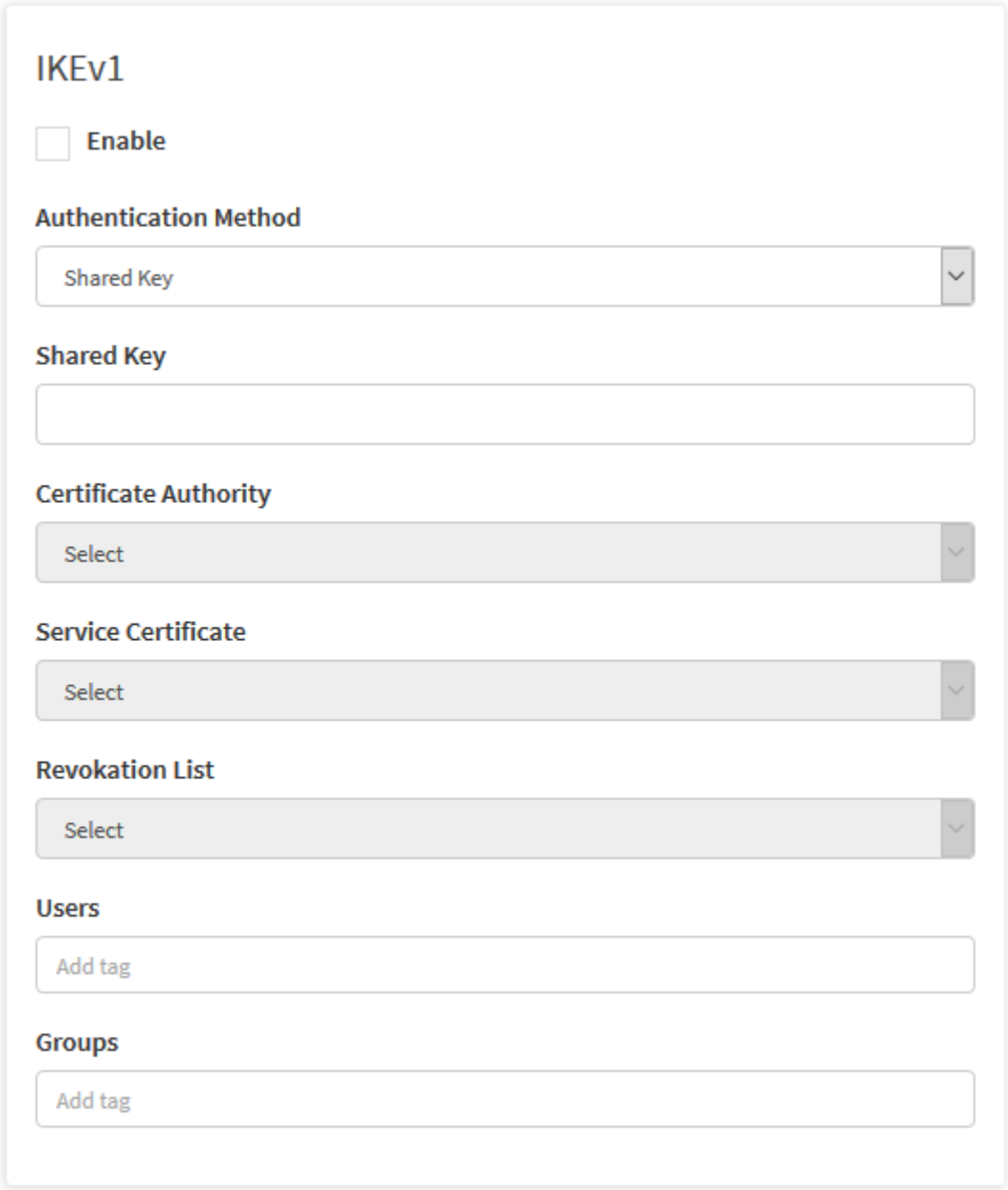
- *IKEv1*;
- *IKEv2*;
- *Network*;
- *Cryptography*;
- *Advanced*.

In addition, we will also exemplify how to perform Device / User / Password authentication with Windows default VPN client.

Next we will analyze each component of this screen.

Remote Access - IKEv1

Next we will analyze each component of the IKEv1 panel:



VPN IPSEC - IKEv1

- [x] ***Enable:*** *Enabling the IKEv1 protocol for IPSEC RAS VPN client connections;*
- ***Authentication Method:*** *Selection of the authentication method. You can choose to select to use a "Shared Key - [Pre Shared Key]" or a "Digital Certificate - [C.S - Service Certificate]";*
- ***Shared Key:*** *Definition of the "Shared key" for authentication when accessing the IPEC RAS VPN client with the IPSEC VPN host. {Item opting for selecting the authentication method}*;
- ***Certificate Authority:*** *Selection of the certifying entity [C.A] responsible for validating the authenticity of the "C.S. - Service certificate "for authentication on the IPSEC RAS VPN client access with the IPSEC VPN host. {Item opting for selecting the authentication method}*;
- ***Service Certificate:*** *Selection of the Digital Certificate used as an authentication method in the IPSEC RAS VPN client access with the IPSEC VPN host. {Item opting for selecting the authentication method}*;

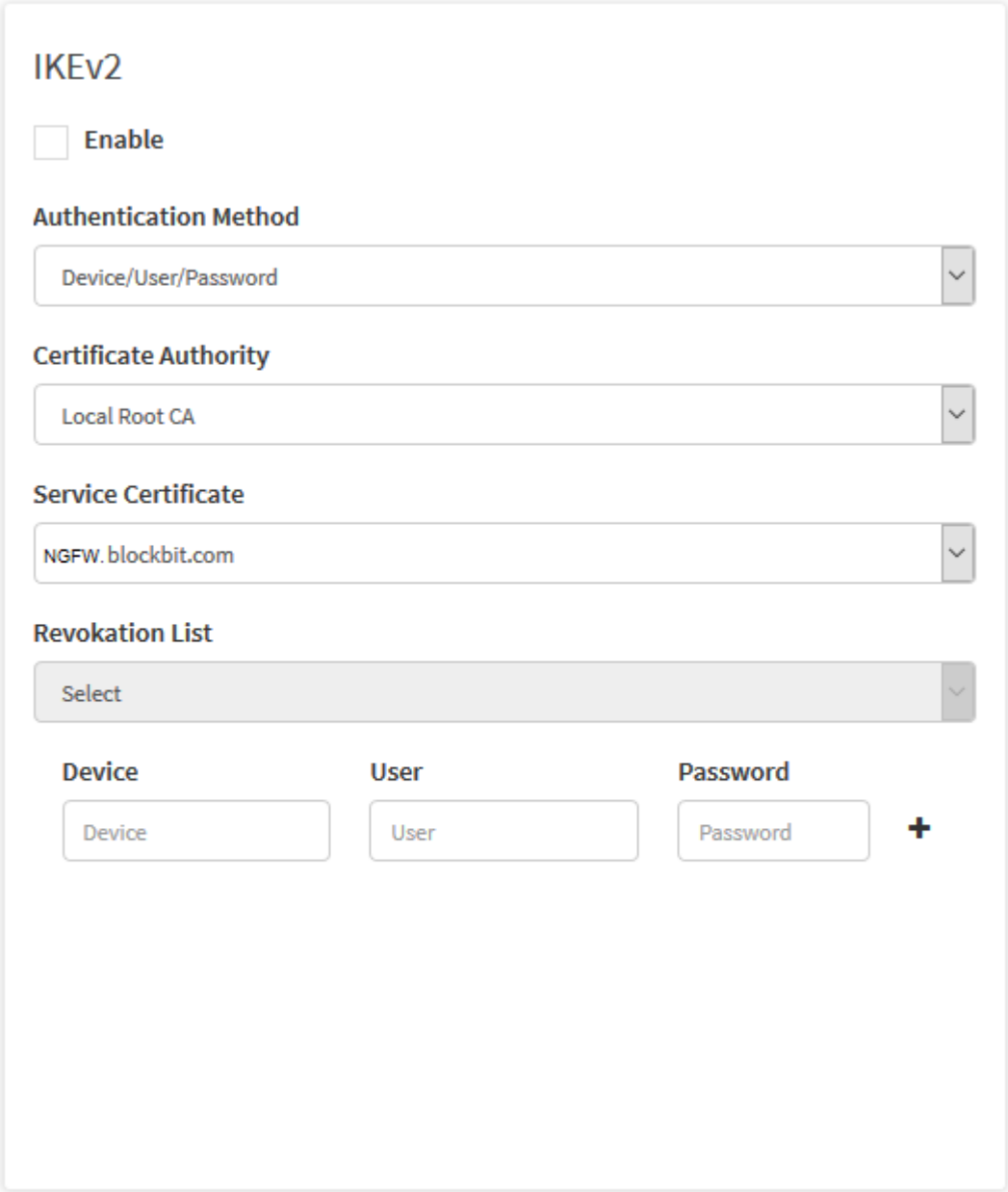
The certificate must have the NGFW's IP or a hostname that resolves the name to the NGFW IP, so that the client has the same data (IP or equal hostname) to make the connection.

- ***Revokation List:*** *Selection of the revoked certificate list to guarantee the exclusive use of valid digital certificates. {Optional item}*;
- ***Users / Groups:*** *Selection of "Users and Groups" for permission filters on IPSEC RAS VPN client access. The selected users / groups must have "User certificate" respectively installed on the "remote host" to validate their authentication*.

Next we will configure the *IKEv2* panel.

Remote Access - IKEv2

Next we will analyze each component of the IKEv2 panel:

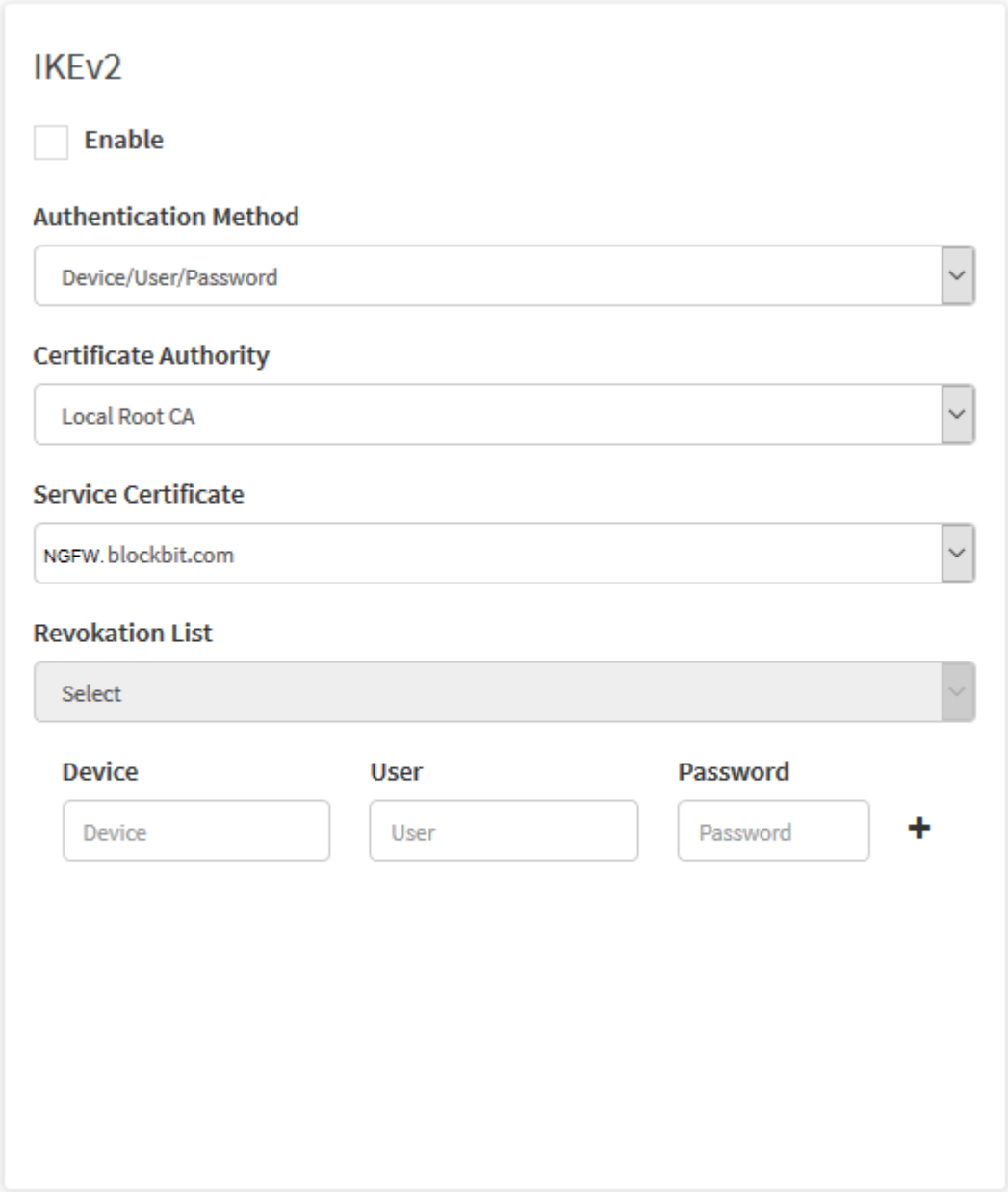


IKEv2 - *VPN IPSEC IKEv2*

The selection in the authentication method field changes what will be displayed on this panel.

Here is a description of each option:

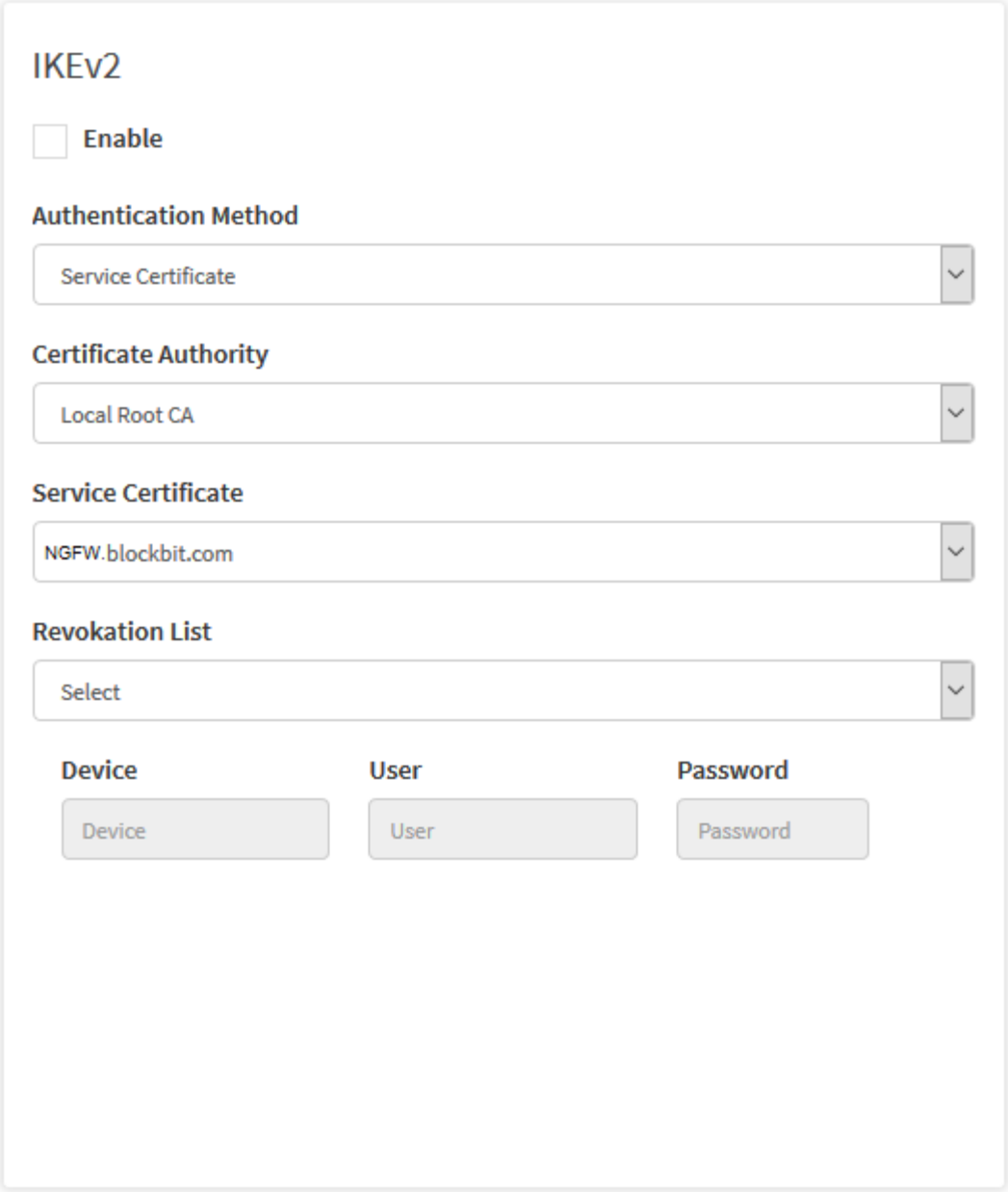
- **[✔] *Enable:*** *Enabling the IKEv2 protocol for IPSEC RAS VPN client connections;*
- ***Authentication Method:*** *Selection of the authentication method. Possible options are*:
  - ***Device/User/Password*:** “Device / User / Password” identification for IPSEC RAS VPN client access, compatible with Windows 7 or higher. When selecting this option, the Revocation List field is disabled. As shown in the image below:



IKEv2 - *Device/User/Password*

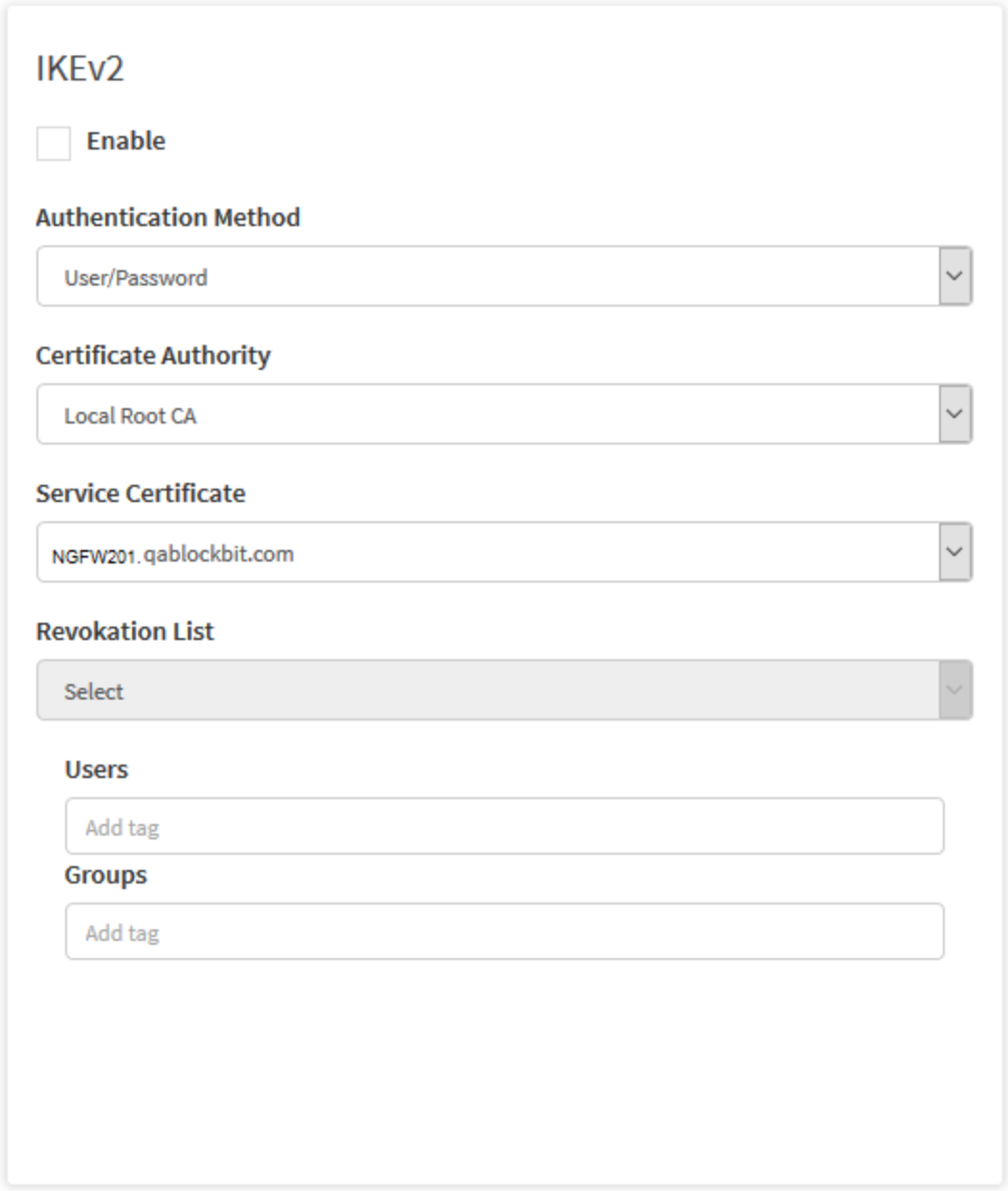
- ***Service Certificate*:** When selecting this option, it is possible to configure the use of a "Digital Certificate - [C.S - Service Certificate]" or EAP-MSCHAP v2 authentication. In this case the user will have to install the NGFW CA Certificate on the workstation together with the user certificate that he must create through the Portal. The digital certificate, created at the time of the Wizard, is the certificate that UTM uses for services. This method is compatible with Blockbit Agent and Blockbit Client. When selecting this option, the Device, User and Password fields are disabled. As shown in the image below:

The certificate must have the NGFW's IP or a hostname that resolves the name to the NGFW's IP, so that the client has the same data (IP or equal hostname) to make the connection.



IKEv2 - *Service Certificate*

- ***User/Password:*** In the User / Password method, authentication is performed specifically in the IKEv2 options, checking the user and password in the user's Client based on those that have been configured in this panel. This option supports the EAP-Radius authentication protocol for searching and authenticating users, performing local authentication or on remote system users through a centralized authentication mechanism (PAM). This mode is only compatible with Blockbit Client. When selecting this option, the Revocation List field is disabled and the User and Groups fields are displayed. As shown in the image below:



IKEv2 - *User/Password*

- ***Certificate Authority:*** *Selection of the certifying entity [C.A] responsible for validating the authenticity of the "C.S. - Service certificate "for authentication on the IPSEC RAS VPN client access with the IPSEC VPN host*. {Not mandatory item for selecting the authentication method};
- ***Service Certificate:*** *Selection of the Digital Certificate used as an authentication method in the IPSEC RAS VPN client access with the IPSEC VPN host*. {Item choosing the authentication method selection};
- ***Revokation List:*** *Selection of the revoked certificate list to guarantee the exclusive use of valid digital certificates*. This field is only available if you have selected the Service Certificate authentication method*;*
- ***Device/User/Password:*** *To allow IPSEC RAS VPN access from MS Windows® VPN clients using* ***EAP-MSCHAP v2*** *passwords*. This field is only available if you have selected the Device / User / Password authentication method.
- **User/Groups:** Defines the list of users and user groups allowed to authenticate to the IKEv2 Remote Access VPN. This field is only available if you have selected the User / Password option.

As long as the user has a certificate installed, it is possible to access through IKEv2.

To do so, specify a description in the "Device" field, and add the "Users" and "Password" used that will be used for access.

The IKE / SA connection (Phase 1) in the IPSEC RAS VPN access through the “Blockbit Client” has support for the IKEv2 protocol only.

In this case, it is mandatory to use “Digital Certificate” as an authentication method.

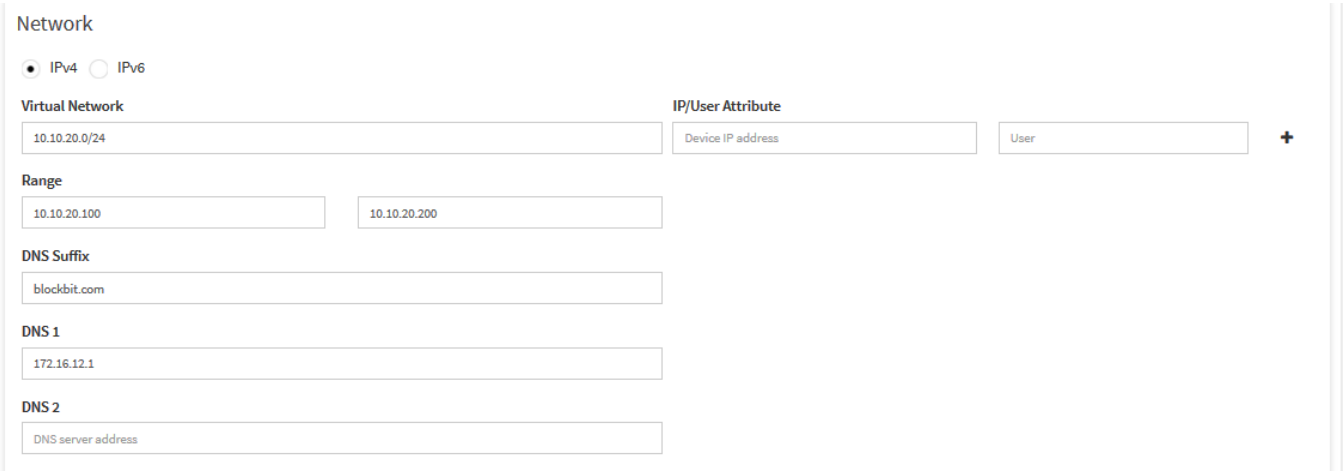
The host address (FQDN) configured for IPSEC RAS VPN access must be published on the valid DNS server and be the same used in the configuration when issuing the C.S in Blockbit NGFW.

With the User / Password authentication method selected and configured in the NGFW, the only accepted authentication method will be exclusively by user and password.

Next we will configure the *Network* panel.

Remote Access - Network

Assignment of the IP network class for IP address distribution (DHCP-Proxy) for IPSEC RAS VPN Client connections.



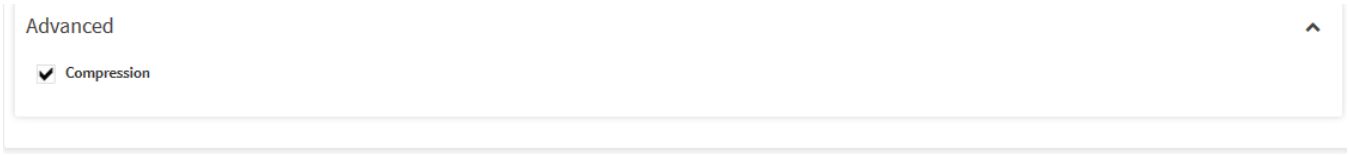
VPN IPSEC RAS – Network

- ***IPv4[ ]/IPv6[ ]:*** Determines whether the assignment will be for IPv4 or IPv6, selecting this field determines which fields will be displayed on this panel*;*
- ***Virtual Network:*** Sets the IP or classless IP addressing of the network. This field is displayed regardless of the selection of IPv4 or IPv6;
- ***IP/User Attibute:*** *In this field, the user and the device's IP address are determined. If you want to add one more field, click* ***[ ]****, if it is necessary to remove them, click* ***[ ]****.* This field is not displayed when selecting IPv6;
- ***Range:*** *Determines the IP range, add the beginning in the first field and the end in the second. This field is not displayed when selecting IPv6. The network added in this field* ***cannot*** *be the same as any of the existing networks in the NGFW, nor the remote network of the clients that will connect;*
- ***DNS Suffix:*** *Enter the DNS suffix in this field*. This field is displayed regardless of the selection of IPv4 or IPv6;
- ***DNS 1:*** *Determines the address of the primary DNS server*. This field is displayed regardless of the selection of IPv4 or IPv6;
- ***DNS 2:*** *Determines the address of the secondary DNS server*. This field is displayed regardless of the selection of IPv4 or IPv6.

Next we will configure the *Cryptography* panel.

Remote Access - Advanced

Finally, the configuration of the Advanced panel:



VPN IPSEC RAS – Advanced

- **[✔] *Compression:*** *Allows you to enable the IPSEC data compression method in the transport of the "Pay-load" in phase 2 IPSEC (ESP / AS)*. Enabling the compression method is mandatory when accessing the Blockbit Authentication Agent.

Small packets (for example: ICMP with default size), are not compressed. *Communication is done through an IPIP tunnel, requiring the release of the standard service object: IPIP-ENCAPSULATION (IPv4 Encapsulation protocol) among peers through a Zone-Protection.*
For more information about compression check RFC 3173.
For more IP encapsulation data within IP see RFC 2003.

For more information on fragmentation, see this page.

This completes the VPN RAS setup.

You can validate your VPN settings using the following means:

- *Live Sessions - VPN* tab;
- In Security Events - VPN.

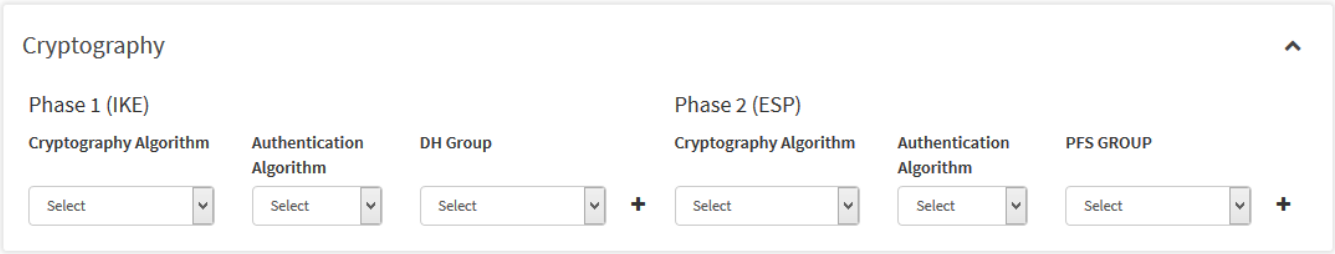
Using the CLI commands below:

- *debug-vpn -t ipsec*;
- *show-vpn-conn*;
- *show-vpn-info*.

For more information, on each of these procedures, see the *Troubleshooting VPNs* page.

Remote Access - Cryptography

In this screen you can select the groupings of Phase 1 (IKE / SA) and Phase 2 IPSEC (ESP / AS) encryption and authentication algorithms for the remote host used to establish the IPSEC RAS VPN Client tunnel.



VPN IPSEC RAS – Cryptography

- **Phase 1 (IKE):** Based on the ISAKMP protocol (IKE / SA): Defines the grouping of the phase authentication algorithms and technical specifications (IKE / SA) for the VPN device used to establish the VPN tunnel.
    - **Cryptographic Algorithms:** Select the encryption algorithm to be used. Possible options are:
        - **3DES:** It means "Triple Data Encryption Algorithm", it is a cipher that originated from DES (Data Encryption Standard), a symmetric based algorithm based on a "Feistel" Network (It uses an iterative block cipher sequence). This encryption algorithm has 64-bit blocks and keys and works by applying the DES cipher three times to each block with 56-bit keys. In the first phase encrypting the data, then decrypting it with a separate key and finally encrypting the decrypted data in phase 2. For more information, see RFC 1851. This option will use 3DES to encrypt the VPN tunnel;
        - **AES:** It means "Advanced Encryption Standard", it was created using part of the "Rijndael cipher block" , it is based on Substitution – permutation network and it is a cipher that uses a matrix of 4x4 bytes to perform the encryption operations; AES works by dividing data into blocks and using the initial key as a base, it generates a sequence of other 128-bit keys for each encryption shift, after that, the initial key is added to the block and each byte takes on the character of a specific algorithm replacement table. The rows of the block are moved, their columns mixed and the sequence of keys with 128 bytes that were previously created are added to the block again. Finally, this last process is repeated taking into account the size of the AES key that was selected (the keys in this standard can reach a maximum of 256 bits). For more information, see the RFC 3602. When selecting this option the VPN tunnel will be established using AES with a 128 byte key;
        - **AES128:** This option acts exactly like the previous option (AES), using a 128 byte key, its function is specifically to provide compatibility with products that may be on the other end of the VPN that by default use the nomenclature "AES128" instead of just "AES";
        - **AES128CCM128:** This option will use AES with a 128-bit key, with CCM (Counter with CBC-MAC) mode enabled and an 128-bit ICV (Integrity Check Value). The CCM mode is an encryption and authentication algorithm that works by generating a flow cipher, and its cryptographic keys are applied to the data entry seeking greater reliability during the transfer process.;
        - **AES128CCM64:** This option will use AES with a 128-bit key, with CCM mode enabled and a 64-bit ICV;
        - **AES128CCM96:** This option will use AES with a 128-bit key, with CCM mode enabled and a 96-bit ICV;
        - **AES128CTR:** This option uses AES with a 128-bit key, with CTR (Counter Mode) mode enabled. The AES-CTR relies on the AES block cipher to create a flow cipher, this is done by encrypting the values in sequence from the counter and creating the key flow blocks;
        - **AES128GCM128:** It means "Galois / Counter Mode", this counter mode uses block ciphers to generate flow ciphers. Using an incremental counter, each block is encrypted with a unique value, the data blocks are enumerated, the result of this operation is combined with an initialization vector called (IV) and the encryption is performed using AES. This option allows you to select an AES with a 128-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
        - **AES128GCM64:** This option will use AES with a 128-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
        - **AES128GCM96:** This option will use AES with a 128-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
        - **AES192:** This option acts like the AES option, however using a 192 byte key;
        - **AES192CCM64:** This option will use AES with a 192-bit key, with CCM mode enabled and a 64-bit ICV;
        - **AES256CCM64:** This option will use AES with a 256-bit key, with CCM mode enabled and a 64-bit ICV;
        - **AES192CCM96:** This option will use AES with a 192-bit key, with CCM mode enabled and a 96-bit ICV;
        - **AES256CCM96:** This option will use AES with a 256-bit key, with CCM mode enabled and a 96-bit ICV;
        - **AES192CCM128:** This option will use AES with a 192-bit key, with CCM mode enabled and a 128-bit ICV;
        - **AES256CCM128:** This option will use AES with a 256-bit key, with CCM mode enabled and a 128-bit ICV;
        - **AES128GMAC:** GMAC, stands for the "Galois Message Authentication Code!, this mode acts like GCM, but focusing specifically on authenticating data entry. GMAC in particular creates incremental message authentication codes, and ignores when ciphertext is zero length, so that the only output is the authentication tag. This option will use AES with a 128-bit key using GMAC mode;
        - **AES192GMAC:** This option will use AES with a 192-bit key using GMAC mode;
        - **AES256GMAC:** This option will use AES with a 256-bit key using GMAC mode;
        - **AES192GCM64:** This option will use AES with a 192-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
        - **AES256GCM64:** This option will use AES with a 256-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
        - **AES192GCM96:** This option will use AES with a 192-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
        - **AES256GCM96:** This option will use AES with a 256-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
        - **AES192GCM128:** This option will use AES with a 192-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
        - **AES192CTR:** This option will use AES with a 192-bit key, with CTR mode enabled;
        - **AES256:** This option will use AES with a 256 byte key;

- **AES256GCM128:** This option will use AES with a 256-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
- **AES256CTR:** This option will use AES with a 256-bit key, with CTR mode enabled;
- **BLOWFISH:** A symmetric block cipher with keys from 32 to 448 bits. It works initially by dividing the data into 32 bits, after that it compares part of the separate input bits with the algorithm's input array and uses the result of this comparison in the "Blowfish" function, after that the output is used in another comparison between the bits with the data that was divided early in the process, this iteration is repeated sequentially 15 times alternating between the components of the array ending with the combination of the last 2 members of the array to create the encrypted text. This option will use "BLOWFISH" with a 128-bit key;
- **BLOWFISH128:** This option acts exactly like the previous option (BLOWFISH), using a key 128 bytes, its function is specifically to provide compatibility with products that can be on the other end of the VPN that by default use the nomenclature "BLOWFISH128" instead of just "BLOWFISH";
- **BLOWFISH192:** This option will use "BLOWFISH" with a 192-bit key;
- **BLOWFISH256:** This option will use "BLOWFISH" with a 256-bit key;
- **CAMELLIA:** It is a "Feistel" symmetric block cipher with keys of 128, 192 and 256 bits, depending on this selection it can be applied 18 or 24 times. It acts by separating blocks following the determinations of their functions and using fragments of the data to mix with their subkeys. Once this is done, the encryption itself is performed according to the type of key selected (as previously mentioned), finally, having the output of this operation, extra bits are added in the subkeys, completing the process. For more information, see the RFC 3713. This option will use "CAMELLIA" with a 128-bit key;
- **CAMELLIA128:** This option acts exactly like the previous option (CAMELLIA), using a key 128 bytes, its function is specifically to provide compatibility with products that can be on the other end of the VPN that by default use the nomenclature "CAMELLIA128" instead of just "CAMELLIA";
- **CAMELLIA128CCM128:** This option will use "CAMELLIA" with a 128-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
- **CAMELLIA192:** This option will use "CAMELLIA" with 192 bits key;
- **CAMELLIA256:** This option will use "CAMELLIA" with a 256-bit key;
- **CAMELLIA128CTR:** This option will use "CAMELLIA" with a 128-bit key, with CTR mode enabled;
- **CAMELLIA192CCM128:** This option will use "CAMELLIA" with a 192-bit key, with CCM mode enabled and a 128-bit ICV;
- **CAMELLIA192CCM96:** This option will use "CAMELLIA" with a 192-bit key, with CCM mode enabled and a 96-bit ICV;
- **CAMELLIA192CCM64:** This option will use "CAMELLIA" with a 192-bit key, with CCM mode enabled and a 64-bit ICV;
- **CAMELLIA192CTR:** This option will use "CAMELLIA" with a 192-bit key, with CTR mode enabled;
- **CAMELLIA256CCM128:** This option will use "CAMELLIA" with a 256-bit key, with CCM mode enabled and a 128-bit ICV;
- **CAMELLIA256CCM64:** This option will use "CAMELLIA" with a 256-bit key, with CCM mode enabled and a 64-bit ICV;
- **CAMELLIA256CCM96:** This option will use "CAMELLIA" with a 256-bit key, with CCM mode enabled and a 96-bit ICV;
- **CAMELLIA256CTR:** This option will use "CAMELLIA" with a 256-bit key, with CTR mode enabled;
- **CAMELLIA128CCM64:** This option will use "CAMELLIA" with a 128-bit key, with CCM mode enabled and a 64-bit ICV;
- **CAMELLIA128CCM96:** This option will use "CAMELLIA" with a 128-bit key, with CCM mode enabled and a 96-bit ICV;
- **CAST128:** It is a symmetric 64-bit block cipher, with "Feistel" network acting in 12 or 16 rounds and using a 128-bit key, it acts very similar to how the DES cipher treats its blocks. CAST128 performs encryption based on functions, rotations that use the key as a reference point, modular addition and subtraction, etc. For more information, see RFC 2144. When selecting this option, the CAST128 cipher will be used with a 128-bit key;

The performance of the encryption algorithms can be defined as follows:

BLOWFISH is the fastest algorithm, followed by AES. On the other hand, DES has the worst performance.

However, on models that have Intel processors with hardware AES acceleration, their performance is much higher than any other algorithm, especially in the encryption process.

Models BB-1 to BB-10 do not have this feature, in these cases BLOWFISH is recommended.

- **Authentication Algorithm:** Select the authentication algorithm to be used. The available options are:
  - **MD5:** It means Message-digest algorithm, is able to generate a 128-bit hash through a cryptographic input function, it processes the data in blocks composed of 16 32-bit words, making case padding over some space. MD5 works by generating hexadecimal values using the initial message as a basis, in the next step the content of the data block goes through operations determined by a non-linear function, a modular addition and other operations are made, the result of which is used to manipulate the next blocks, upon completion, a 128-bit hash value is returned. For more information, see RFC 1321;
  - **SHA1:** Secure Hash Algorithm 1, is a function used in cryptography that using an input, creates blocks of words, processes them and compresses the message using 40-digit hexadecimal notation and outputs a 160-bit hash. For more information, see RFC 3174;
  - **SHA256:** It is a variant of SHA2, SHA256 encrypts the inputs creating 512-bit blocks, after encryption (which is repeated 64 times) and the compression process, a 256-bit hash is generated. For more information about SHA256 and other SHA2 variants, see RFC 4634;
  - **SHA384:** This is a variant of SHA512, but using different input values, after encryption and compression a 384-bit hash is generated. For more information on SHA256 and other SHA2 variants, see the RFC 4634;
  - **SHA512:** As with previous versions (except for SHA1), SHA512 is a variant of SHA2, using the initial input, processing of 1024-bit blocks is performed, after 80 rounds a 512-bit hash is generated as output. For more information on SHA256 and other SHA2 variants, see the RFC 4634.

- **DH Group (Diffie-Hellman):** The Diffie-Hellman method serves to exchange keys securely between two parties. For more information, see the RFC 2631. The groups are used to determine the level of security when exchanging keys, but the impact on performance must be taken into account. Basically: Larger groups are safer but require more resources. The available options are:
  - **Group 1 (MODP768):** Group with 768 bit module;

- **Group 2 (MODP1024):** Group with 1024 bit module;
- **Group 5 (MODP1536):** Group with 1536 bit module;
- **Group 14 (MODP2048):** Group with 2048 bit module;
- **Group 15 (MODP3072):** Group with 3072 bit module;
- **Group 16 (MODP4096):** Group with 4096 bit module;
- **Group 17 (MODP6144):** Group with 6144 bit module;
- **Group 18 (MODP8192):** Group with 8192 bit module;
- **Group 19 (ECP256):** Group with 256 bit module;
- **Group 20 (ECP384):** Group with 384 bit module;
- **Group 21 (ECP521):** Group with 521 bits module;
- **Group 22 (MODP1024S160):** Group with 1024 bits module and 160 bit subgroup;
- **Group 23 (MODP2048S224):** Group with 2048 bit module and 224 bit subgroup;
- **Group 24 (MODP2048S256):** Group with 2048 bits module and 256 bits subgroup;
- **Group 25 (ECP192):** Group with 192 bits module;
- **Group 26 (ECP224):** Group with 224 bit module;
- **Group 27 (ECP224BP):** Group with 224 bit module;
- **Group 28 (ECP256BP):** Group with 256 bit module;
- **Group 29 (ECP384BP):** Group with 384 bit module;
- **Group 30 (ECP512BP):** Group with 512 bit module.
- ***Group 31 (CURVE25519 or X25519):*** Group with 256 bit module;
- ***Group 32 (CURVE*448 or X448*):*** Group with 448 bit module.

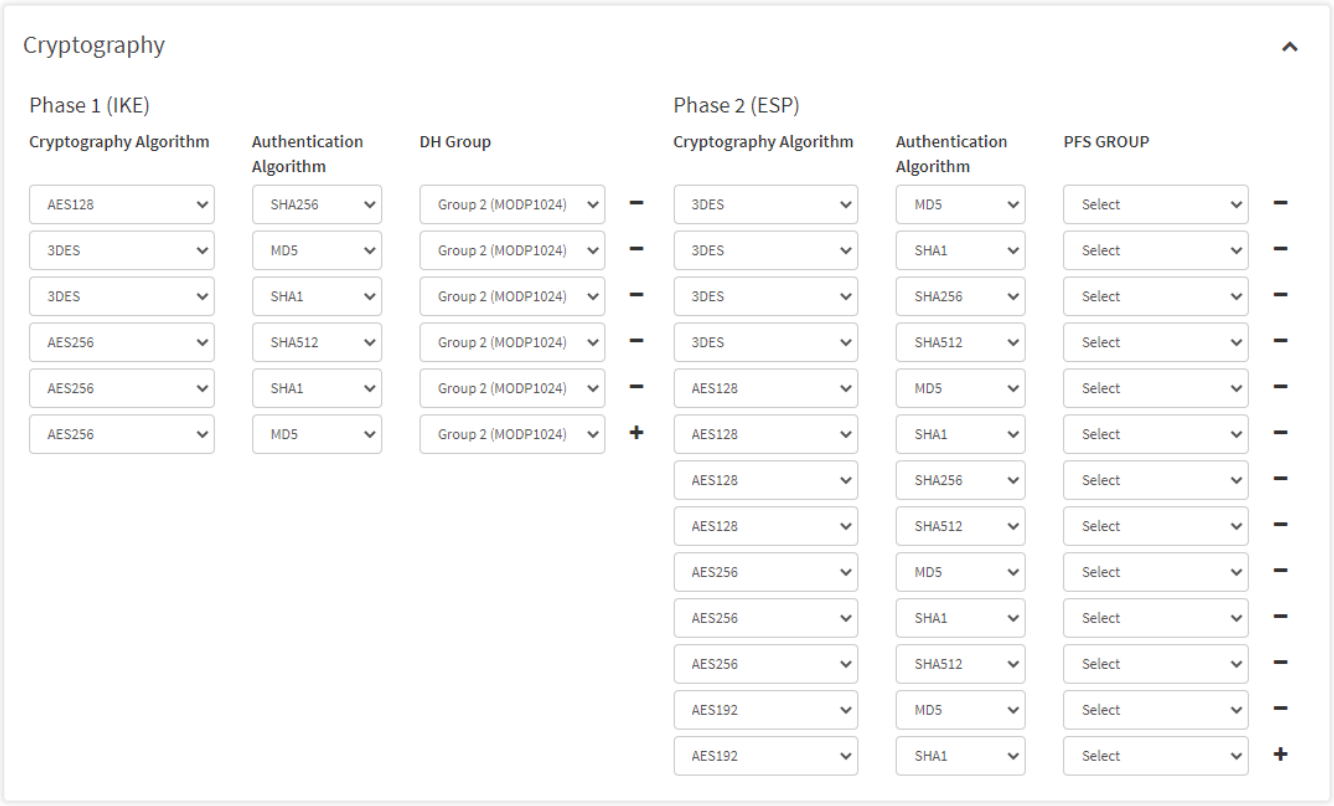
- **Phase 2 (ESP):** The ESP protocol provides data confidentiality (encryption) and authentication (data integrity and data source authentication). ESP is based on the use of the AH (Authentication Header) and ESP (Encapsulating Security Payload) algorithms. Based on the AH and ESP protocols (ESP / AS): Defines the grouping of the phase authentication algorithms and technical specifications (IPSEC / SA) for the VPN device used to establish the VPN tunnel:
  - **Cryptographic Algorithms:** The available options are:
    - **3DES:** Select this option to decrypt 3DES;
    - **AES:** Select this option to decrypt AES;
    - **AES128:** Select this option to decrypt AES with a 128 byte key;
    - **AES128CCM128:** Select this option to decrypt AES with a 128-bit key, with CCM mode and 128-bit ICV;
    - **AES128CCM64:** Select this option to decrypt AES with a 128-bit key, with CCM mode and 64-bit ICV;
    - **AES128CCM96:** Select this option to decrypt AES with a 128-bit key, with CCM mode and 96-bit ICV;
    - **AES128CTR:** Select this option to decrypt AES with a 128-bit key and CTR mode enabled;
    - **AES128GCM128:** Select this option to decrypt AES with a 128-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
    - **AES128GCM64:** Select this option to decrypt AES with a 128-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
    - **AES128GCM96:** Select this option to decrypt AES with a 128-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
    - **AES192:** Select this option to decrypt AES with a 192 byte key;
    - **AES192CCM64:** Select this option to decrypt AES with a 192-bit key, with 64-bit CCM and ICV mode;
    - **AES256CCM64:** Select this option to decrypt AES with a 256-bit key, with 64-bit CCM and ICV mode;
    - **AES192CCM96:** Select this option to decrypt AES with a 192-bit key, with CCM mode and 96-bit ICV;
    - **AES256CCM96:** Select this option to decrypt AES with a 256-bit key, with CCM mode and 96-bit ICV;
    - **AES192CCM128:** Select this option to decrypt AES with a 192-bit key, with CCM mode and 128-bit ICV;
    - **AES256CCM128:** Select this option to decrypt AES with a 256-bit key, with CCM mode and 128-bit ICV;
    - **AES128GMAC:** This option will use AES with a 128-bit key using GMAC mode;
    - **AES192GMAC:** This option will use AES with a 192-bit key using GMAC mode;
    - **AES256GMAC:** This option will use AES with a 256-bit key using GMAC mode;
    - **AES192GCM64:** Select this option to decrypt AES with a 192-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
    - **AES256GCM64:** Select this option to decrypt AES with a 256-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
    - **AES192GCM96:** Select this option to decrypt AES with a 192-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
    - **AES256GCM96:** Select this option to decrypt AES with a 256-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
    - **AES192GCM128:** Select this option to decrypt AES with a 192-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
    - **AES192CTR:** Select this option to decrypt AES with a 129-bit key, with CTR mode enabled;
    - **AES256:** Select this option to decrypt AES with a 256 byte key;
    - **AES256GCM128:** Select this option to decrypt AES with a 256-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
    - **AES256CTR:** Select this option to decrypt AES with a 256-bit key, with CTR mode enabled;
    - **BLOWFISH:** Select this option to decrypt "BLOWFISH" with a 128-bit key;
    - **BLOWFISH128:** Select this option to decrypt "BLOWFISH" with a 128-bit key;
    - **BLOWFISH192:** Select this option to decrypt "BLOWFISH" with a 192-bit key;
    - **BLOWFISH256:** Select this option to decrypt "BLOWFISH" with a 256-bit key.
    - **CAMELLIA:** Select this option to decrypt "CAMELLIA" with a 128-bit key;
    - **CAMELLIA128:** Select this option to decrypt "CAMELLIA" with a 128-bit key;
    - **CAMELLIA128CCM128:** Select this option to decrypt "CAMELLIA" with a 128-bit key, with CCM mode and 128-bit ICV;
    - **CAMELLIA192:** Select this option to decrypt "CAMELLIA" with a 192-bit key;
    - **CAMELLIA256:** Select this option to decrypt "CAMELLIA" with a 256-bit key;
    - **CAMELLIA128CTR:** Select this option to decrypt "CAMELLIA" with a 128-bit key, with CTR mode enabled;
    - **CAMELLIA192CCM128:** Select this option to decrypt "CAMELLIA" with a 192-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;
    - **CAMELLIA192CCM96:** Select this option to decrypt "CAMELLIA" with a 192-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
    - **CAMELLIA192CCM64:** Select this option to decrypt "CAMELLIA" with a 192-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
    - **CAMELLIA192CTR:** Select this option to decrypt "CAMELLIA" with a 192-bit key, with CTR mode enabled;
    - **CAMELLIA256CCM128:** Select this option to decrypt "CAMELLIA" with a 256-bit key, using the "Galois / Counter Mode" and a 128-bit ICV;

        - **CAMELLIA256CCM64:** Select this option to decrypt "CAMELLIA" with a 256-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
        - **CAMELLIA256CCM96:** Select this option to decrypt "CAMELLIA" with a 256-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
        - **CAMELLIA256CTR:** Select this option to decrypt "CAMELLIA" with a 256-bit key, with CTR mode enabled;
        - **CAMELLIA128CCM64:** Select this option to decrypt "CAMELLIA" with a 128-bit key, using the "Galois / Counter Mode" and a 64-bit ICV;
        - **CAMELLIA128CCM96:** Select this option to decrypt "CAMELLIA" with 128-bit key, using the "Galois / Counter Mode" and a 96-bit ICV;
        - **CAST128:** Select this option to decrypt CAST128 with a 128-bit key.

    - **Authentication Algorithm:** The available options are:
        - **MD5:** Select this option to decrypt MD5;
        - **SHA1:** Select this option to decrypt SHA1;
        - **SHA256:** Select this option to decrypt SHA256;
        - **SHA384:** Select this option to decrypt SHA384;
        - **SHA512:** Select this option to decrypt SHA512;
        - **AESXCBC:** Select this option to decrypt AES-XCBC. It is an encryption algorithm based on the CBC-MAC, which uses AES with a 128-bit key and decrypts it by processing this 128-bit input of the entire input together with the first 96 bits, finally making a confirmation with the value to be authenticated. For more information, see RFC 3566.

    - **PFS Group:** It means Perfect Forward Secrecy, guarantees secrecy during the forwarding of the keys and also ensures the reliability of the keys should any of them be compromised the available options are:
        - **Group 1 (MODP768):** Select this option to configure PFS in a group with a 768 bit module;
        - **Group 2 (MODP1024):** Select this option to configure PFS in a 1024-bit module group;
        - **Group 5 (MODP1536):** Select this option to configure PFS in a group with a 1536 bit module;
        - **Group 14 (MODP2048):** Select this option to configure PFS in a group with a 2048-bit module;
        - **Group 15 (MODP3072):** Select this option to configure PFS in a group with a 3072-bit module;
        - **Group 16 (MODP4096):** Select this option to configure PFS in a group with a 4096-bit module;
        - **Group 17 (MODP6144):** Select this option to configure PFS in a group with 6144 bit module;
        - **Group 18 (MODP8192):** Select this option to configure PFS in a group with an 8192-bit module;
        - **Group 19 (ECP256):** Select this option to configure PFS in a group with a 256-bit module;
        - **Group 20 (ECP384):** Select this option to configure PFS in a group with a 384-bit module;
        - **Group 21 (ECP521):** Select this option to configure PFS in a group with a 521-bit module;
        - **Group 22 (MODP1024S160):** Select this option to configure PFS in a group with a 1024-bit module and a 160-bit subgroup;
        - **Group 23 (MODP2048S224):** Select this option to configure PFS in a group with a 2048-bit module and a 224-bit subgroup;
        - **Group 24 (MODP2048S256):** Select this option to configure PFS in a group with a 2048-bit module and a 256-bit subgroup;
        - **Group 25 (ECP192):** Select this option to configure PFS in a 192-bit module group;
        - **Group 26 (ECP224):** Select this option to configure PFS in a group with a 224-bit module;
        - **Group 27 (ECP224BP):** Select this option to configure PFS in a group with a 224-bit module;
        - **Group 28 (ECP256BP):** Select this option to configure PFS in a group with a 256-bit module;
        - **Group 29 (ECP384BP):** Select this option to configure PFS in a group with a 384-bit module;
        - **Group 30 (ECP512BP):** Select this option to configure PFS in a group with a 512-bit module.
        - ***Group 31 (CURVE25519 or X25519):*** Select this option to configure PFS in a group with 256-bit module;
        - ***Group 32 (CURVE448 or X448):*** Select this option to configure PFS in a group with 448-bit module.

The following is an example of a global configuration of the encryption panel, aiming to achieve compatibility with most VPN clients:



VPN IPSEC RAS – Cryptography - Example

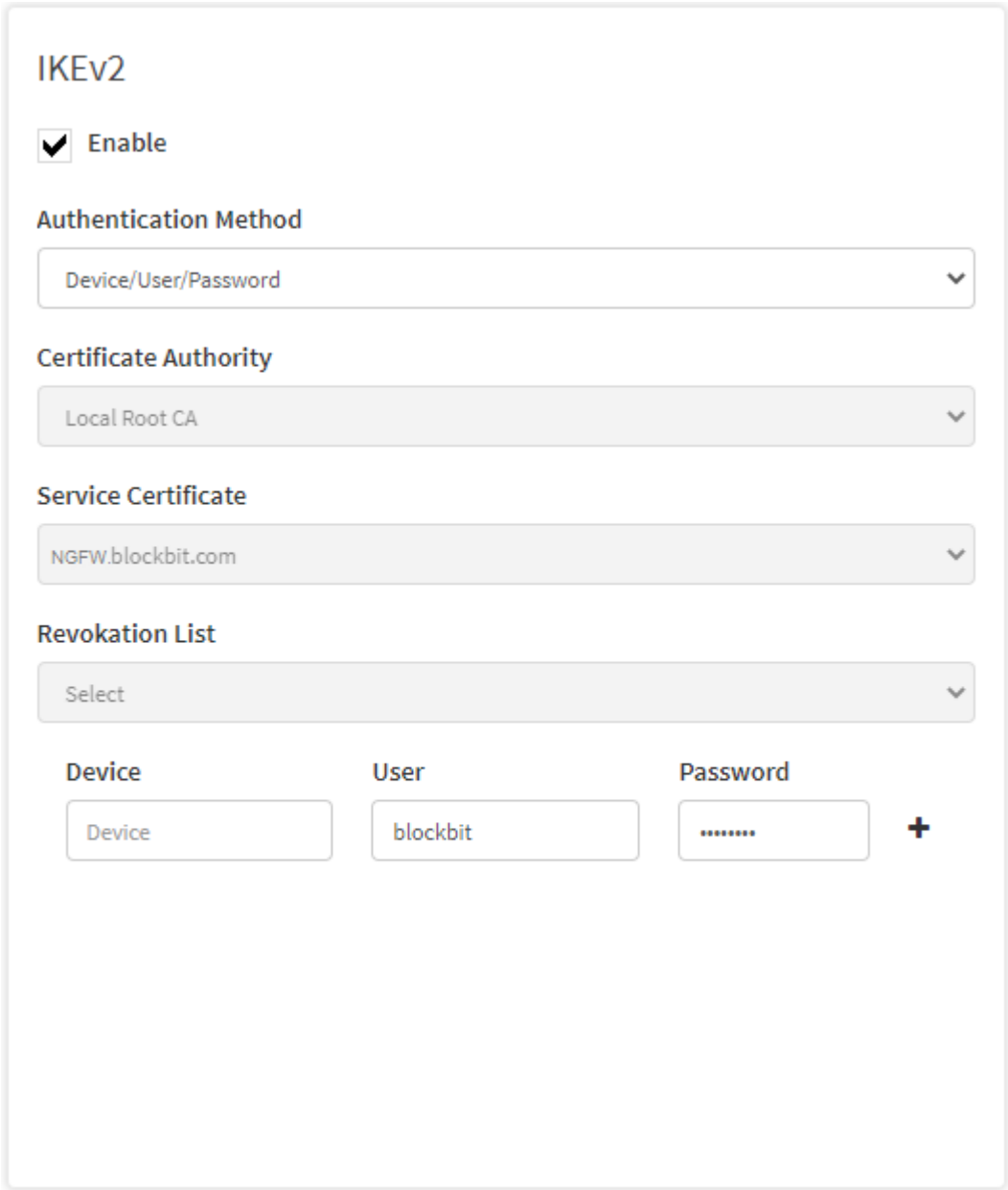
Next we will configure the Advanced panel.

Example - Device / User / Password authentication with default Windows VPN client

Next, we will detail a step-by-step how to configure the IPSEC RAS VPN with the default Windows VPN client.

> The settings were made in Windows 10, but the procedure is the same in other versions.

First, register all users who will have access to the Blockbit VPN Module through the Device, User and Password fields, as shown below:



VPN IPSEC RAS - User registration

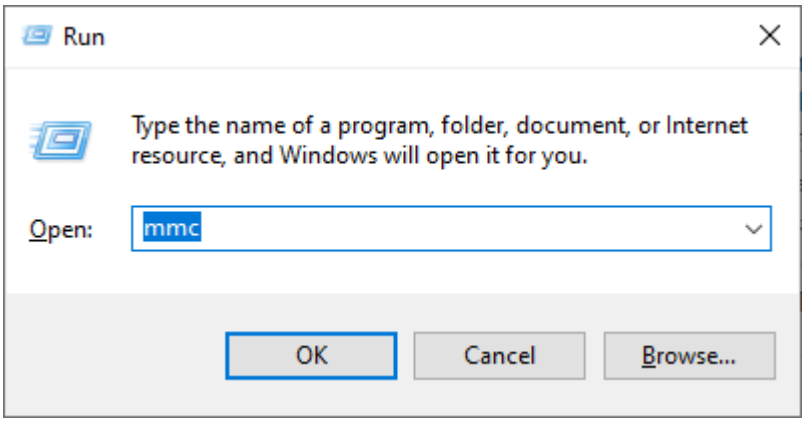
For more information on configuring a VPN RAS, see this page.

After registering the accounts that will use the VPN, it is necessary to import the Blockbit certificate on the workstations.

OBSERVATION:

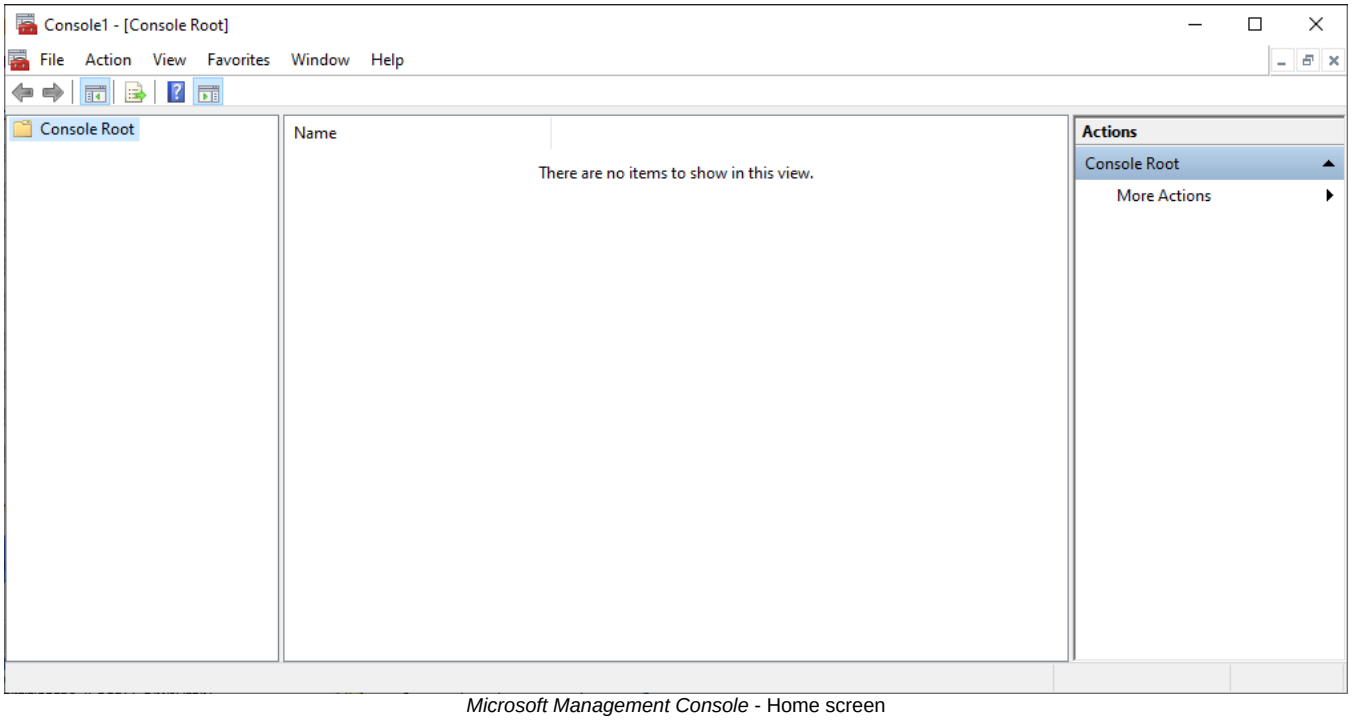
- It is necessary to have HOST in the name of the VALID certificate, that is, that resolves externally or acts with direct editing in the Windows HOSTS file;
- It is mandatory to import the certificate according to the steps described below, since authentication is validated by the same;
- The password / user connection of the Windows client must be the same registered in the Blockbit in VPN IPSEC in the Remote Access tab;
- The VPN connection via Windows client already uses IKEV2, that is, it allows simultaneous connections from the same source (Ex.: 3 stations from the same IP connecting via client).

On the desktop, type the command **Windows + R**, or select "Run" from your Start Menu, the window below will appear, in its text field, type "MMC".



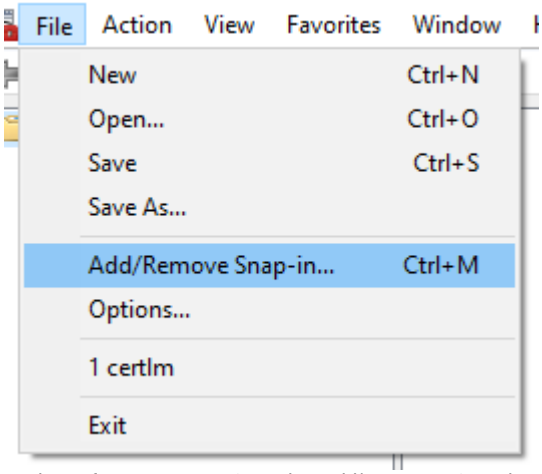
Run - MMC

After clicking **[** OK **]** the Microsoft Management Console will be displayed:



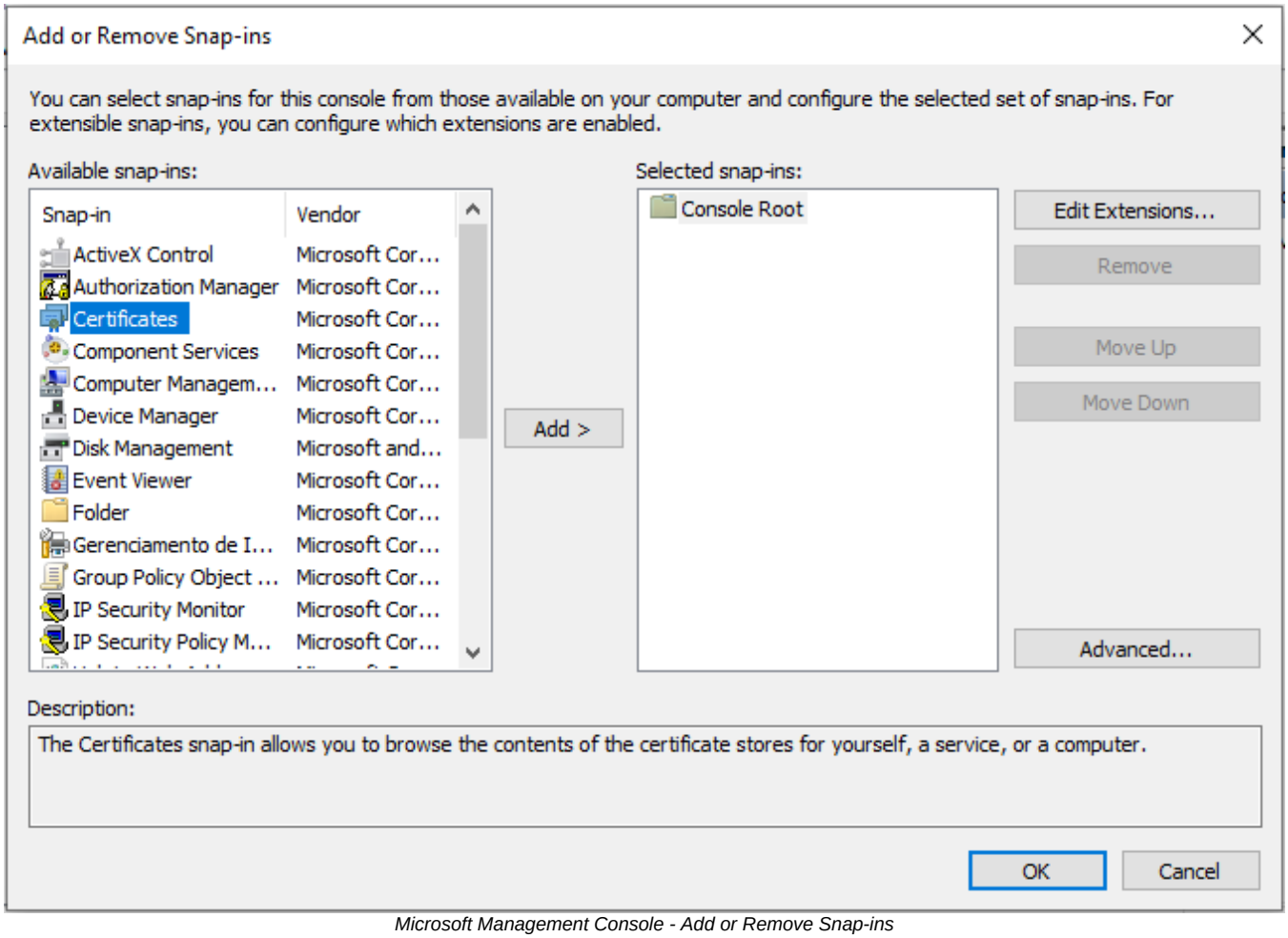
Microsoft Management Console - Home screen

Click on "File" and select the option "Add / Remove Snap-In" or use the shortcut CTRL + M;

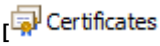
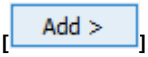


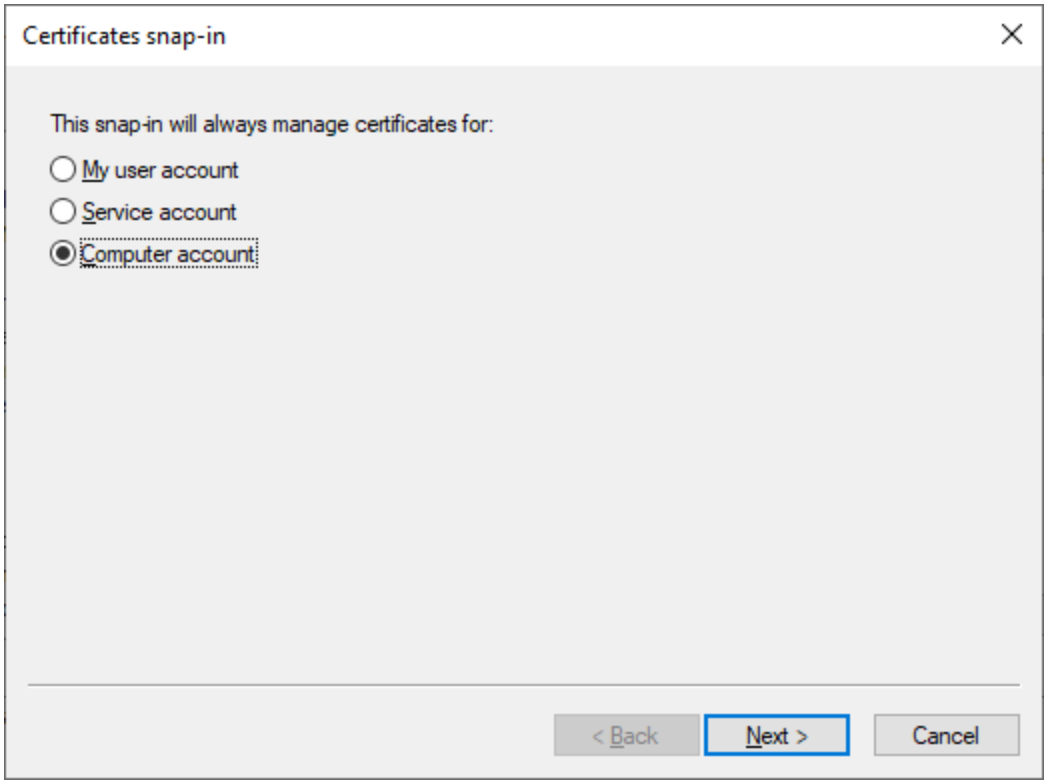
Microsoft Management Console - Add/Remove - Snap-in

The following window will be displayed:

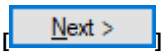


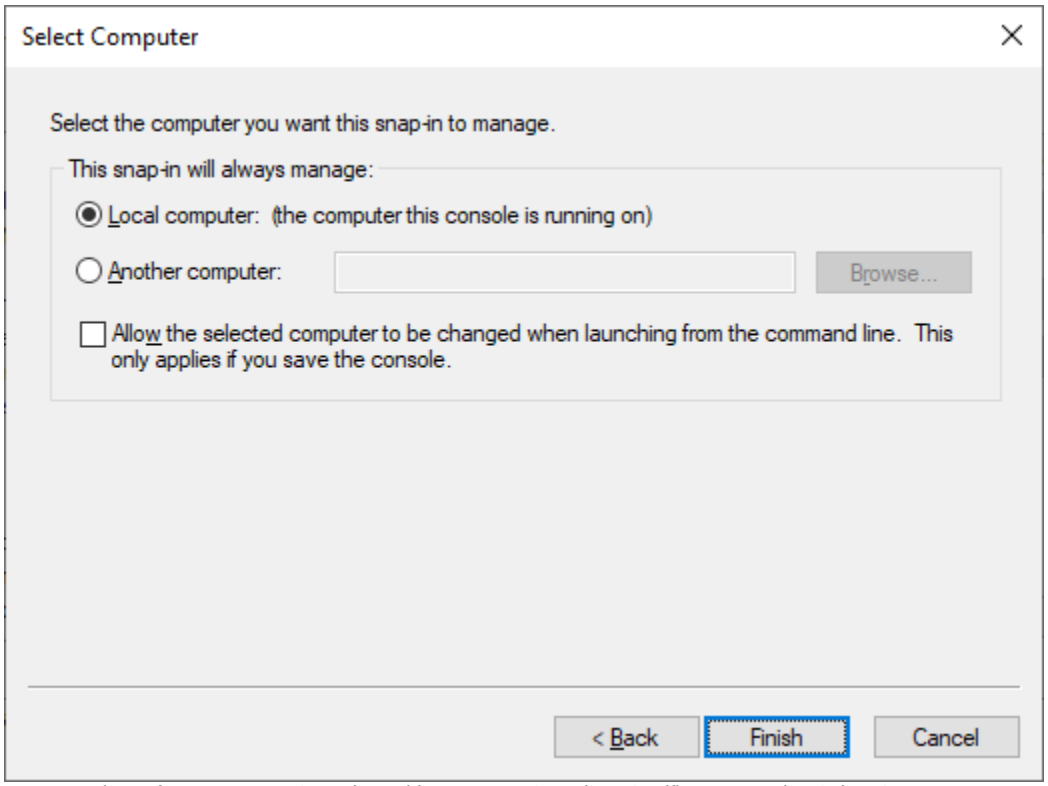
Microsoft Management Console - Add or Remove Snap-ins

Select the **[**  **]** option and click the **[**  **]** button, the window below will be displayed:



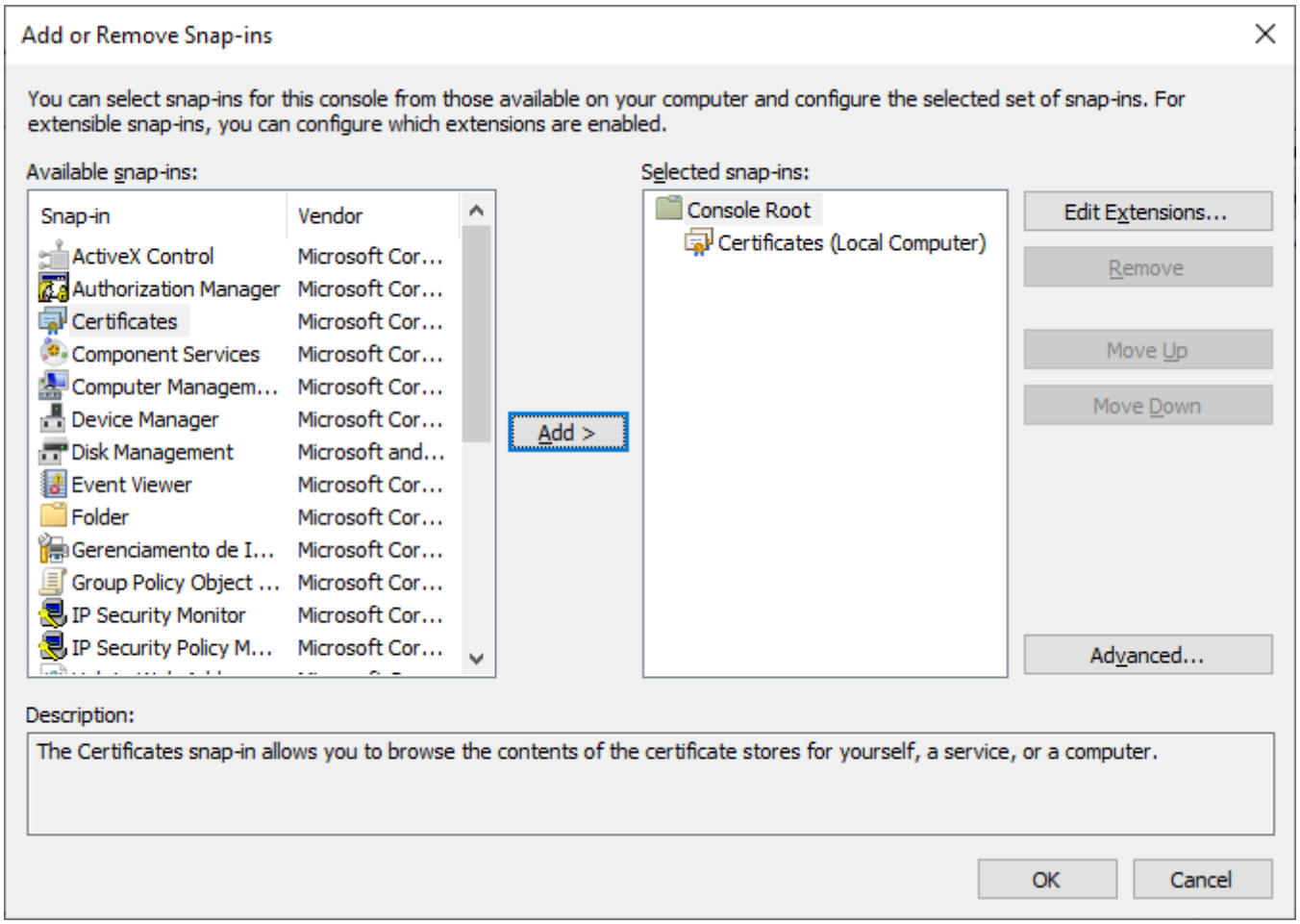
Microsoft Management Console - Add or Remove Snap-ins - Certificates snap-in

Select the "Computer account" option and click the **[**  **]** button.



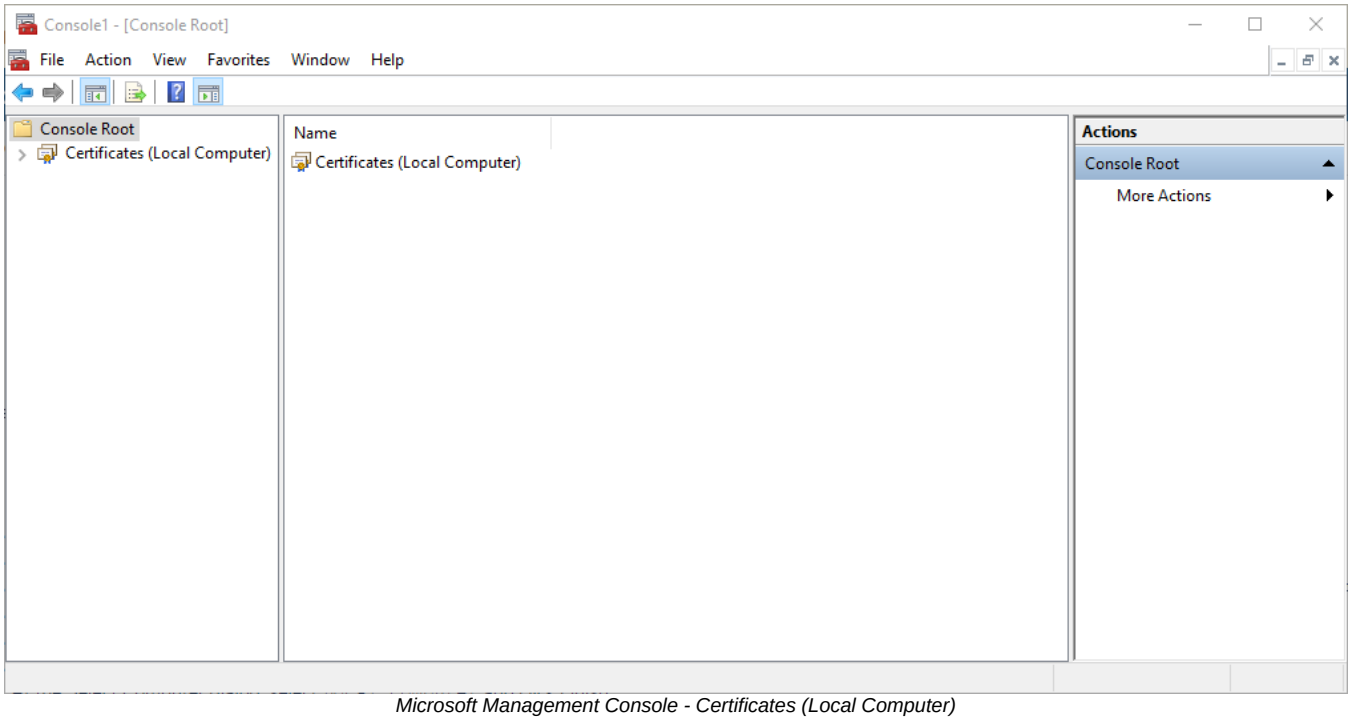
Microsoft Management Console - Add or Remove Snap-ins - Certificates snap-in - Select Computer

Make sure the "Local Computer" option is selected and click the [Finish] button, the window below will appear again, but with the Snap-In added to the right column:



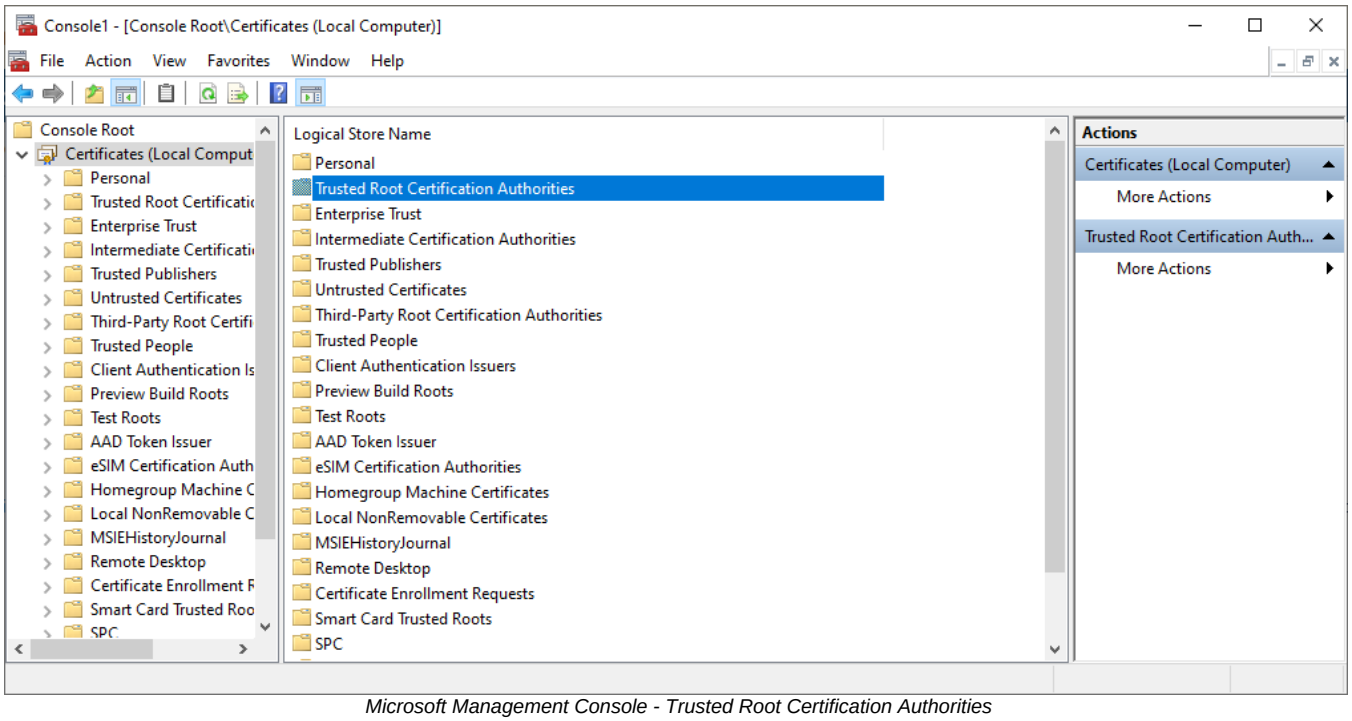
Microsoft Management Console - Add or Remove Snap-ins - Selected snap-ins

Click the [OK] button to return to the home screen, it will now contain the Certificates Snap-In on the local computer:



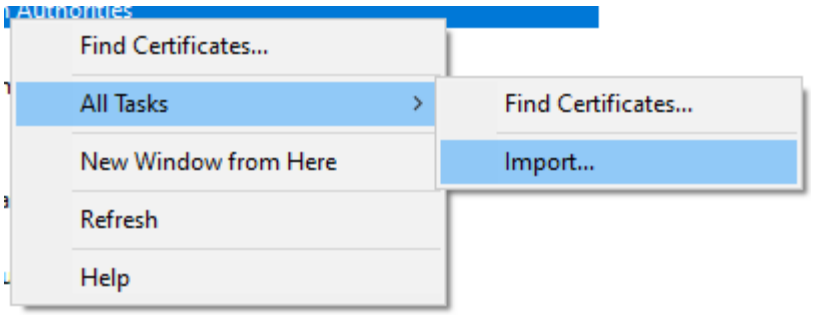
Microsoft Management Console - Certificates (Local Computer)

Select **[** Certificates (Local Computer) **]** in the left column and when the central column loads, select the "Trusted Root Certification Authority" directory, as shown below:



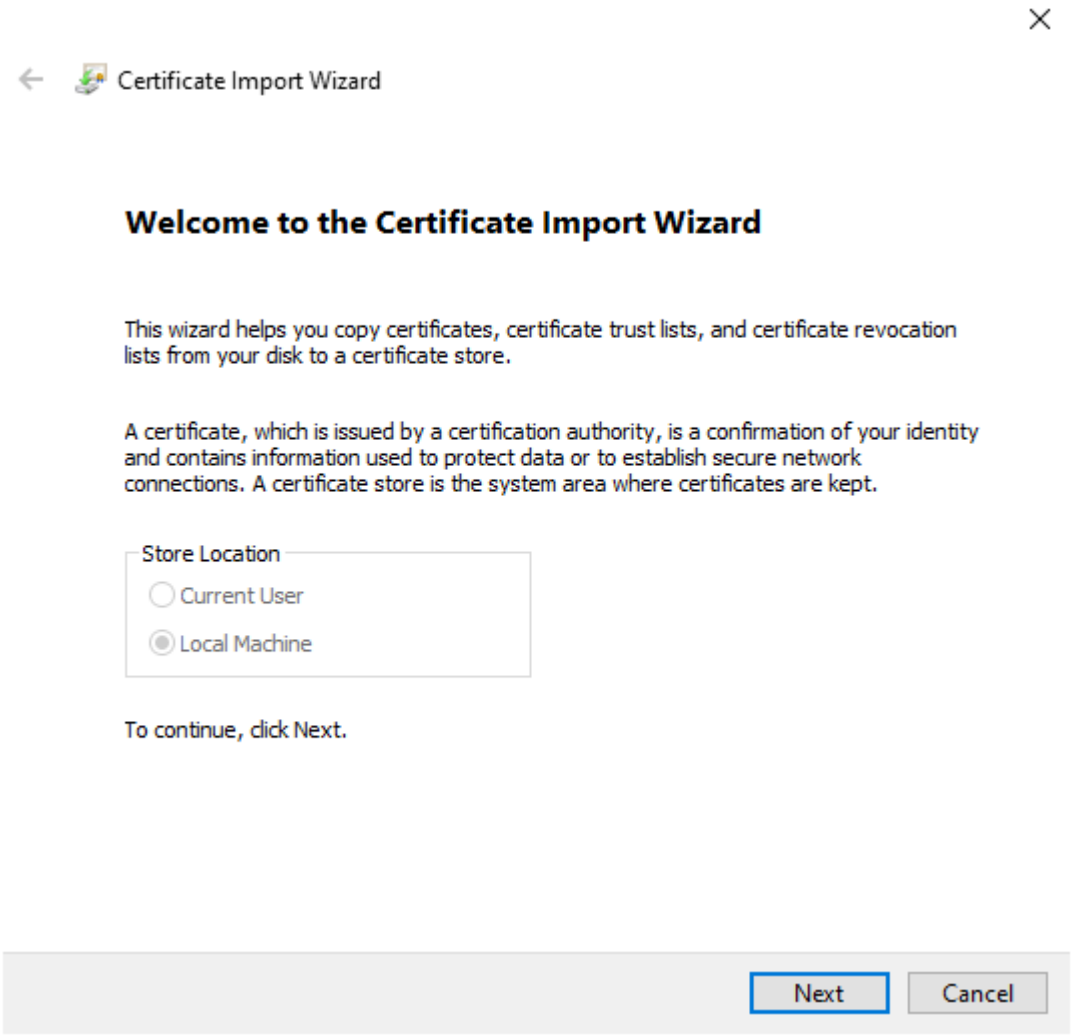
Microsoft Management Console - Trusted Root Certification Authorities

Right click on the directory and select the option "All Tasks" and "Import":



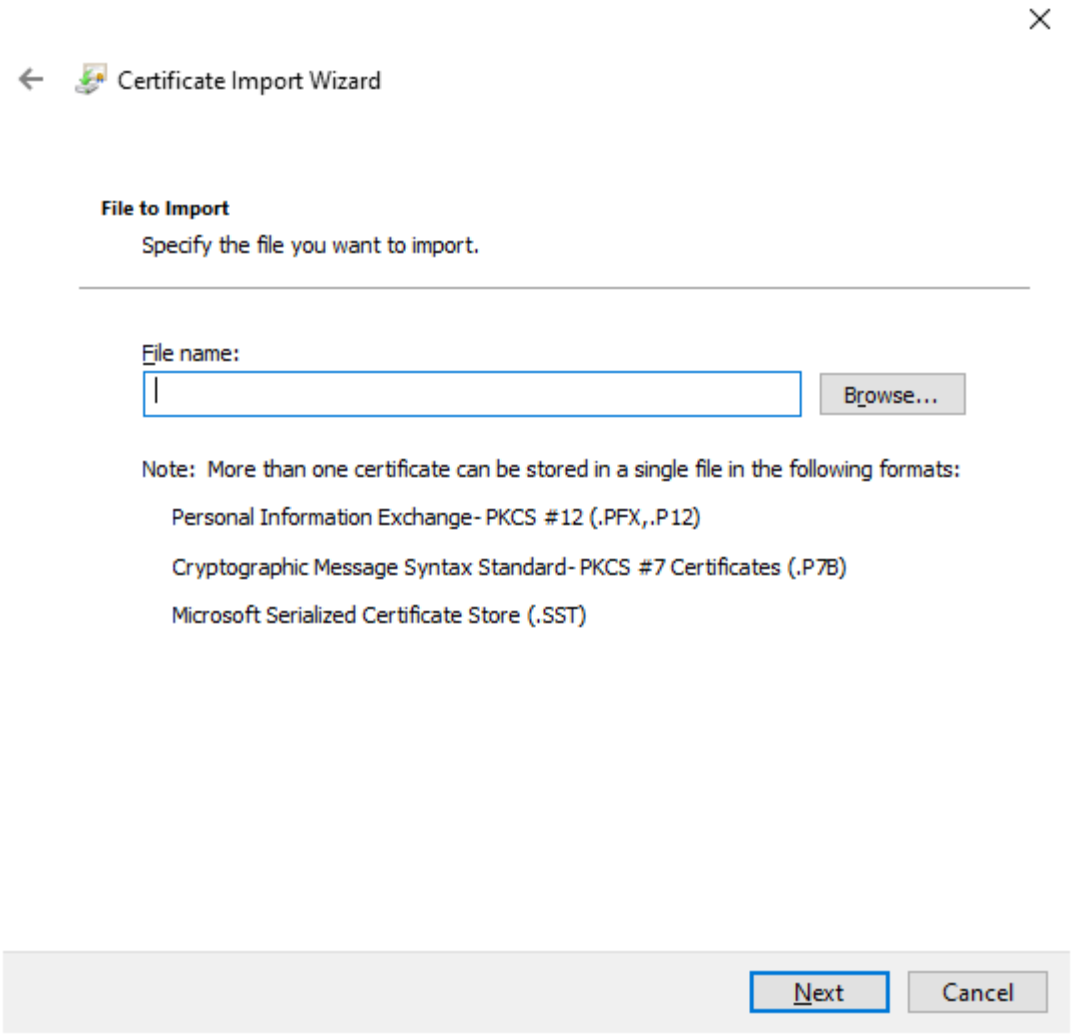
Microsoft Management Console - All Tasks - Import

The Certificate Import Wizard will start, as shown in the image below:



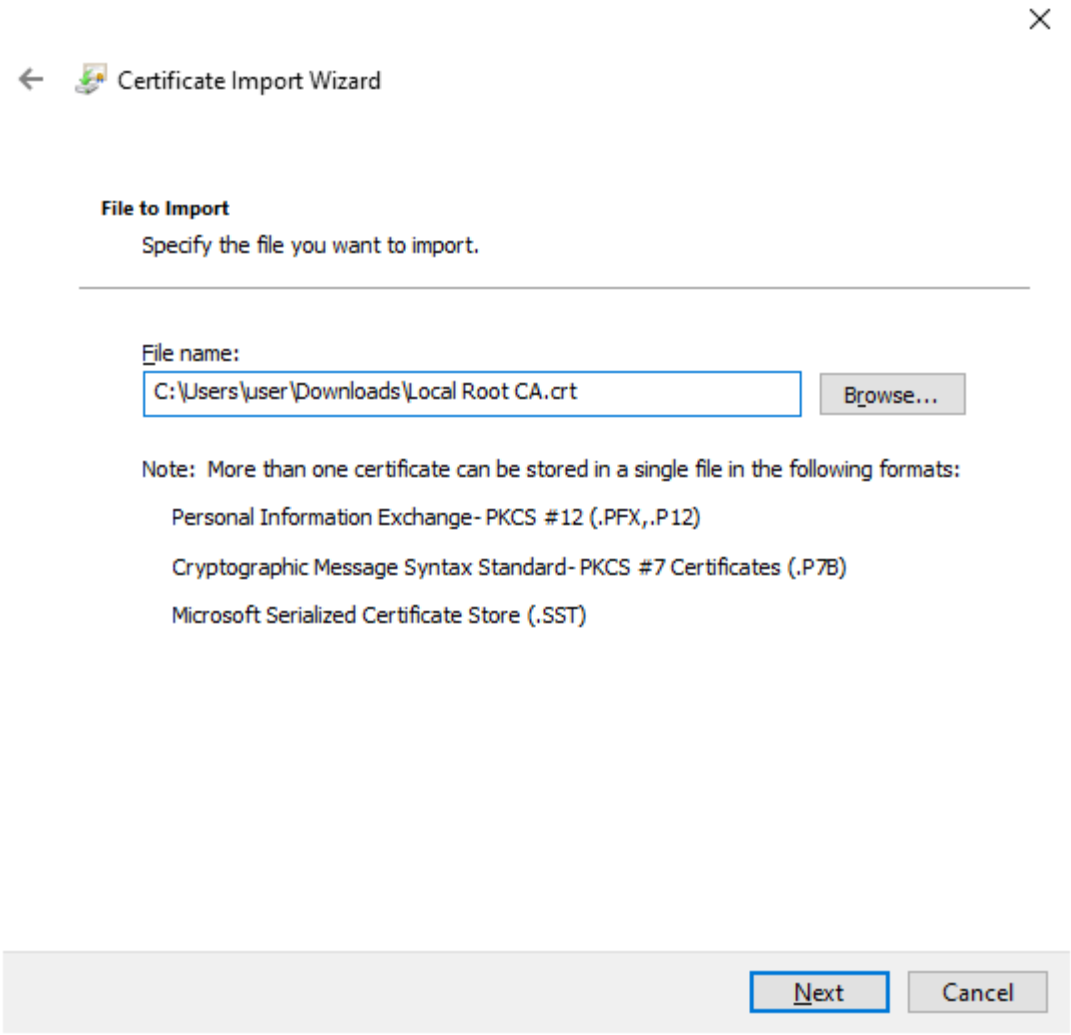
Microsoft Management Console - Certificate Import Wizard

Click [Next] to continue, the next screen will be displayed:



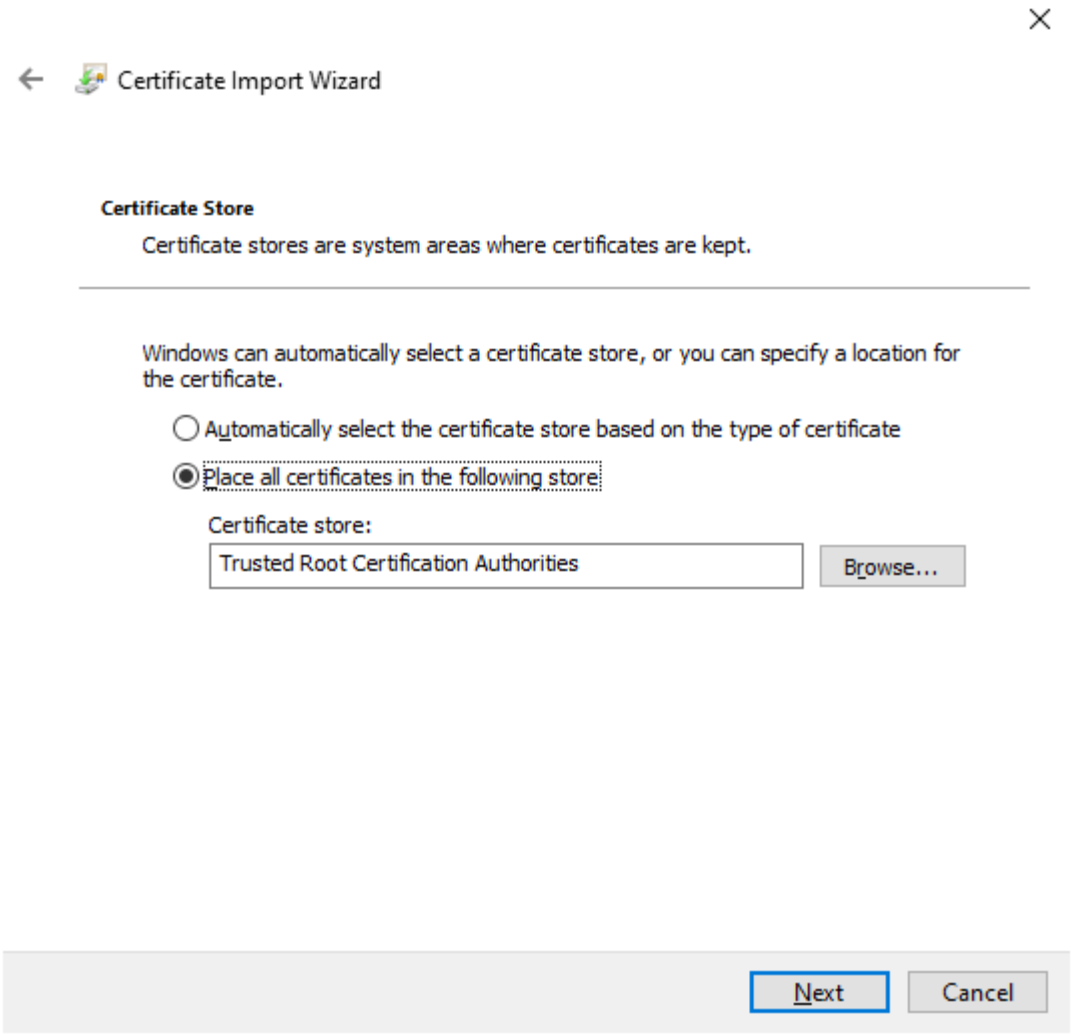
Microsoft Management Console - Certificate Import Wizard - File to Import

Click the **[** Browse... **]** button and select the certificate you want to import.



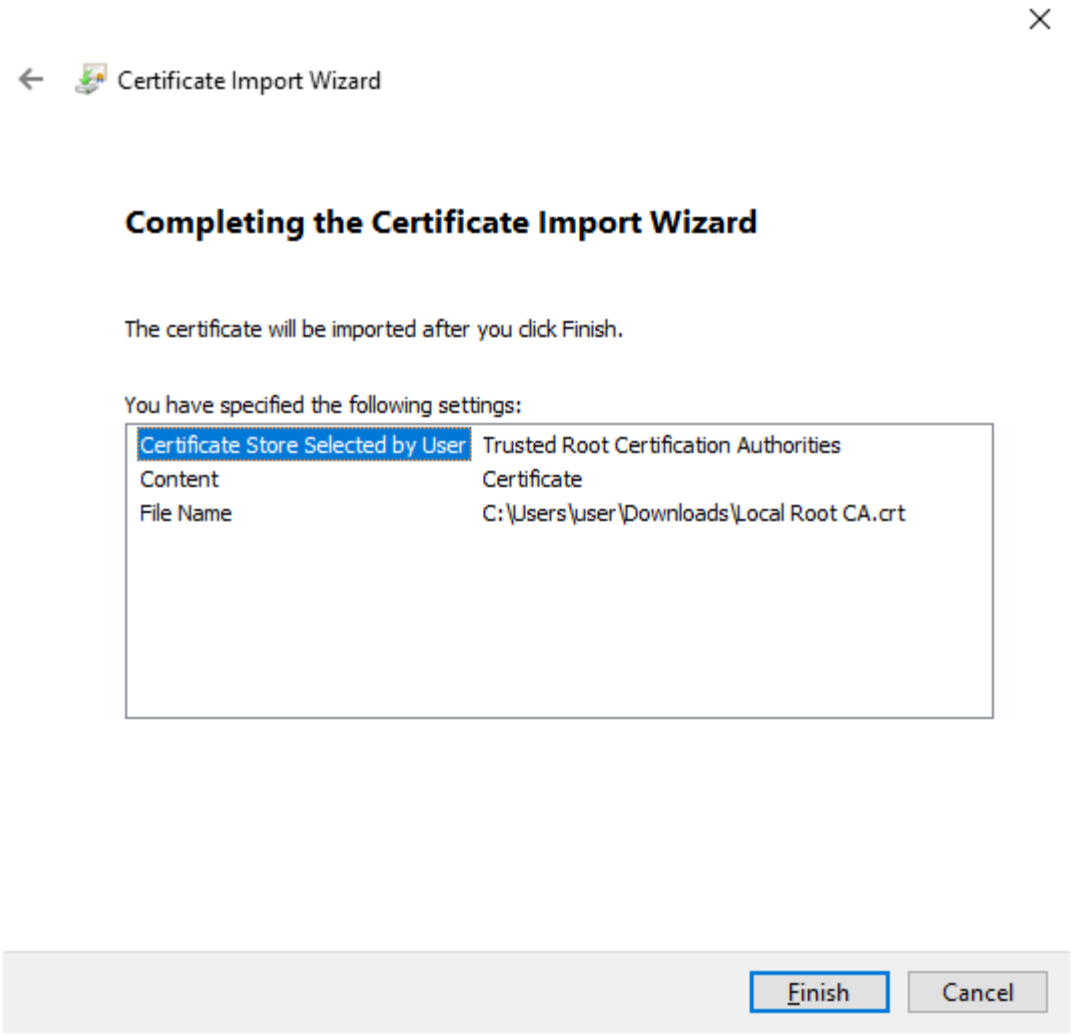
Microsoft Management Console - Certificate Import Wizard - File to Import - Selected

Click [Next] to continue.



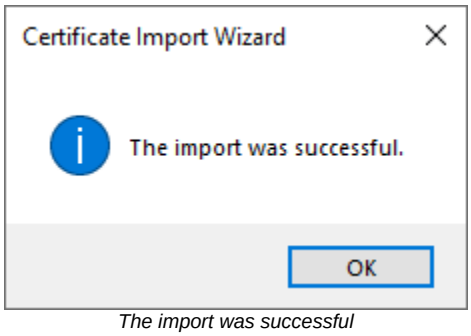
Microsoft Management Console - Certificate Import Wizard - Certificate Store

Just make sure that "Trusted Root Certification Authority" is selected in the text box and do not make any changes. Click [Next], a summary of all selections made will be displayed in this window:



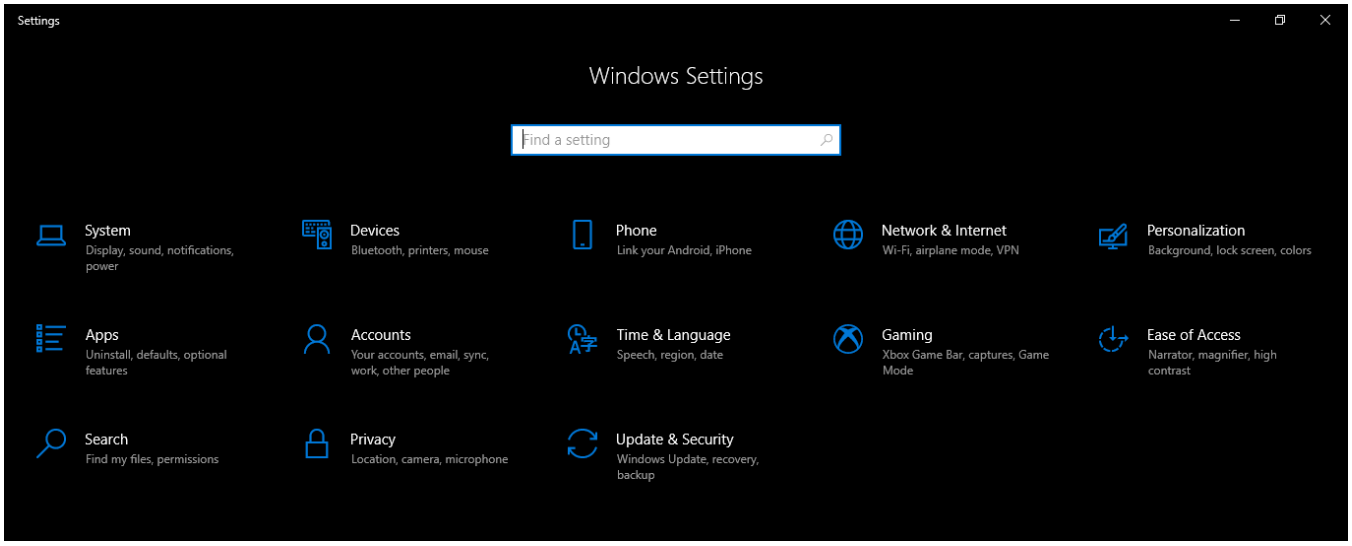
Microsoft Management Console - Certificate Import Wizard - Completing the Certificate Import Wizard

Finally, click [Finish] to complete the import.



The import was successful

After importing the certificate, it will be necessary to configure the VPN client on Windows. Again on the desktop, type the command ***Windows + I***, or click the **Settings icon** [⚙] on your Start Menu, the screen below will appear.

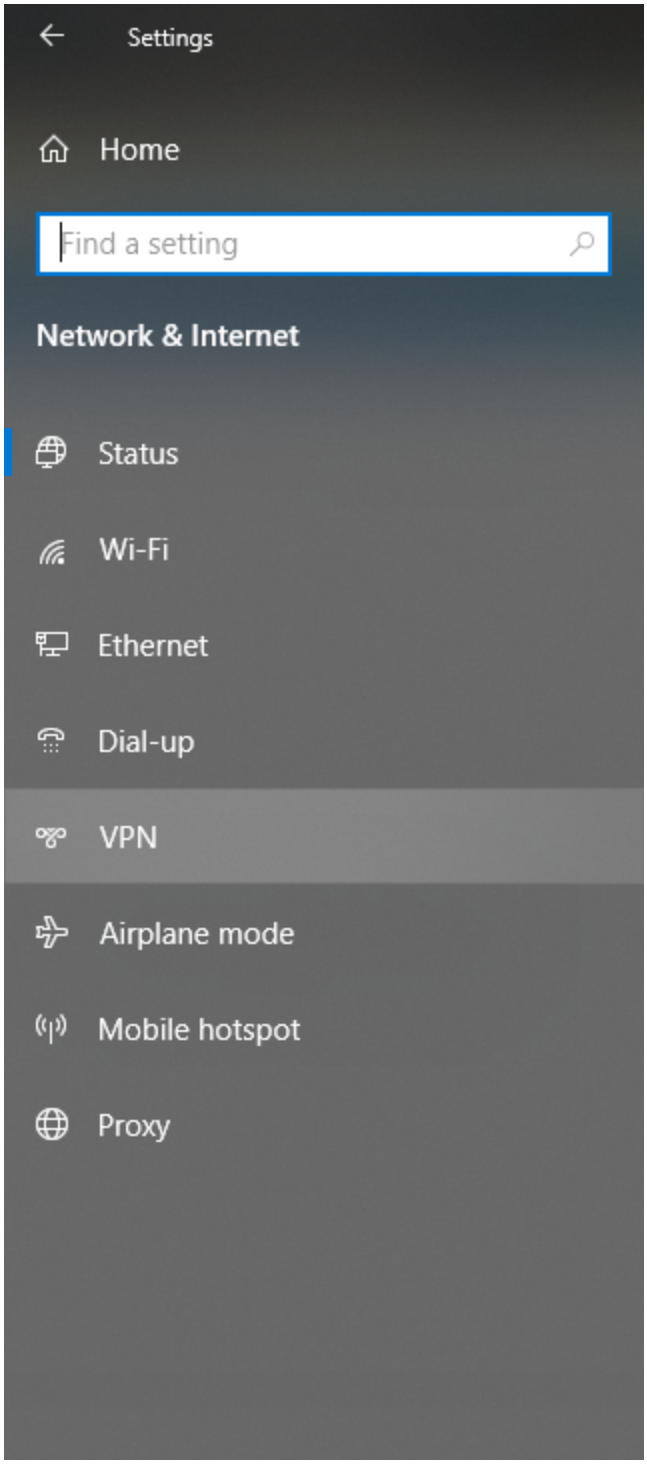


Windows Settings

Select the "Network & Internet" option:

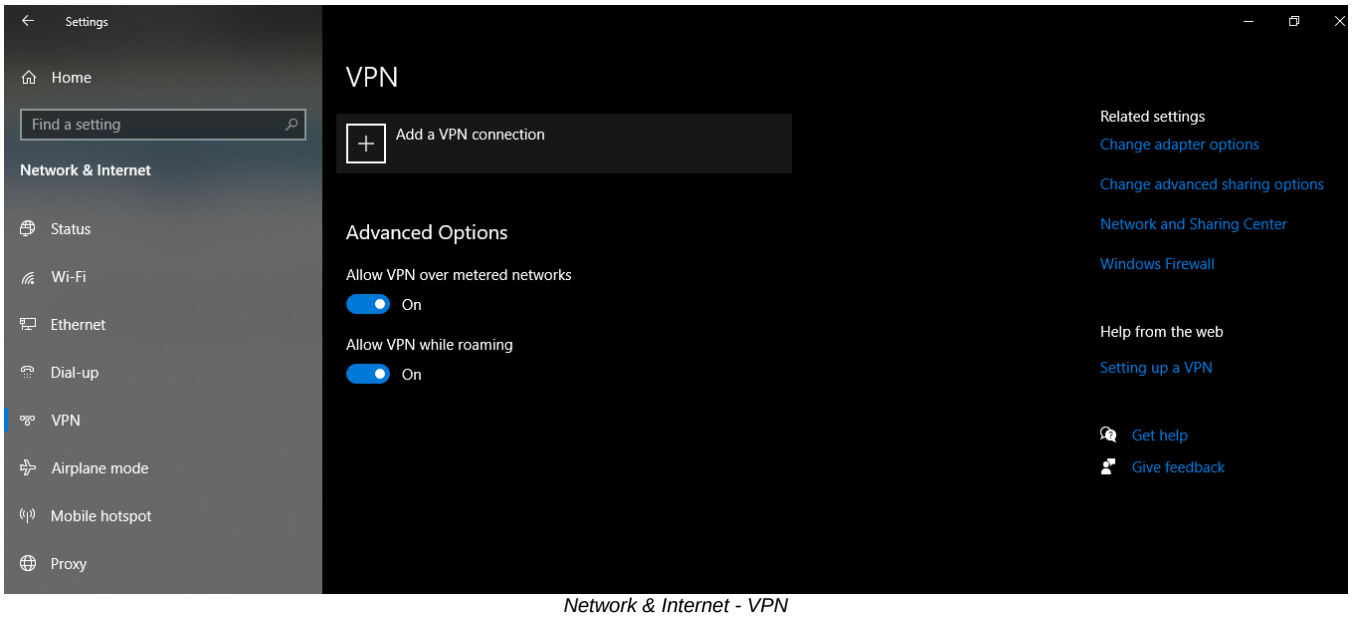
Windows Settings - Network & Internet

In this new window, click on the "VPN" option on the left side menu:



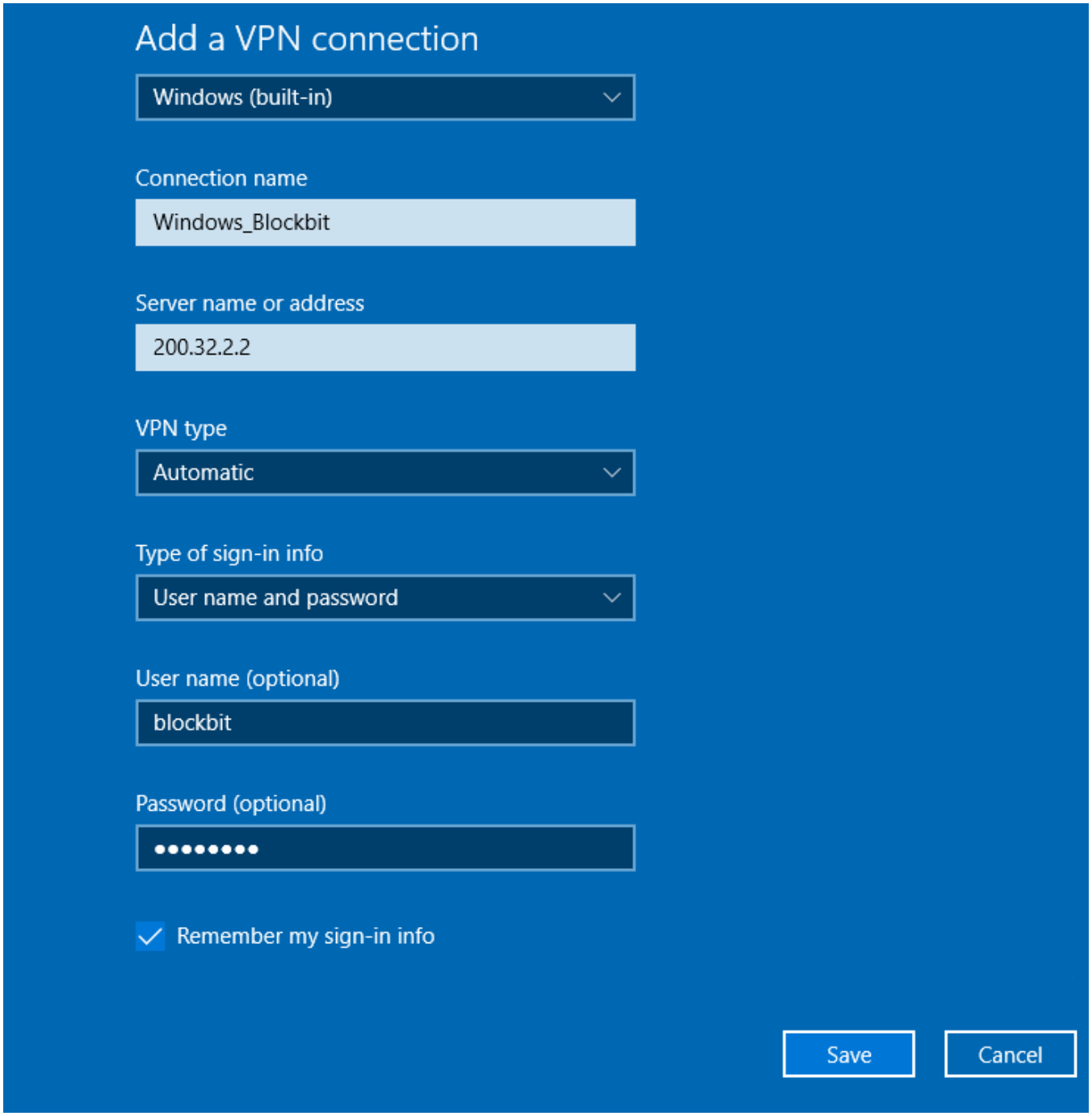
Network & Internet - VPN option

When you get to the screen below, click on the [Add a VPN connection] option:



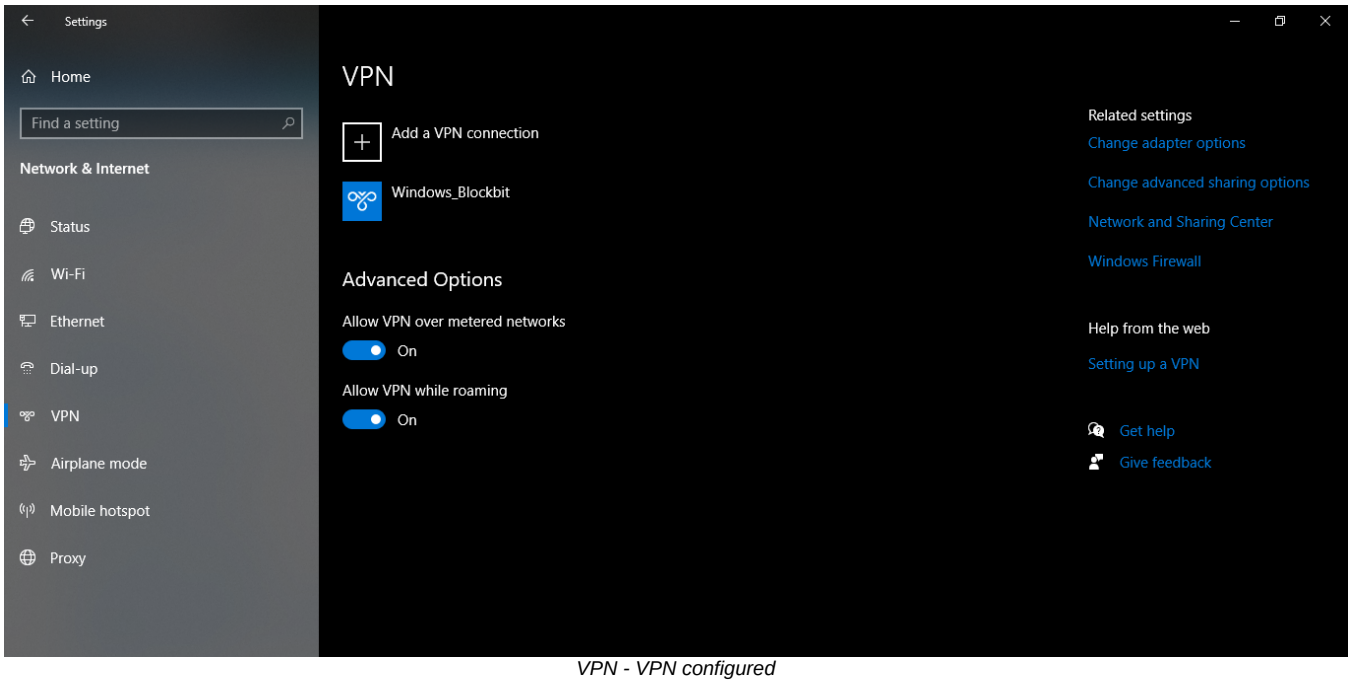
Network & Internet - VPN

The screen for adding a new VPN connection will be displayed, configure it according to the data of your environment, in the example, the VPN will be configured as shown in the following image:



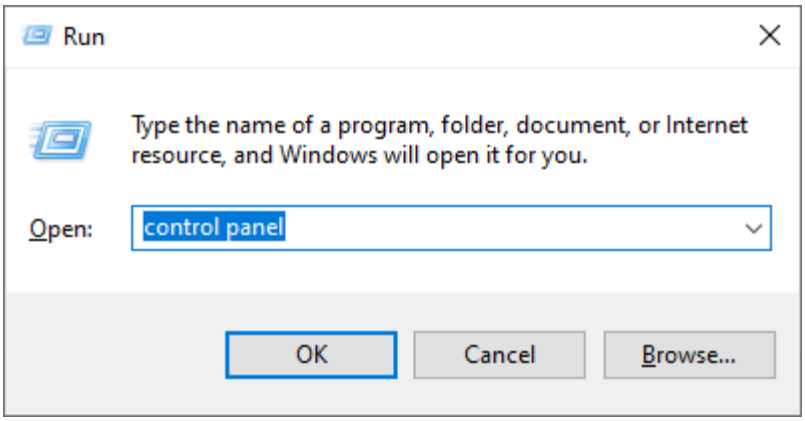
VPN - Add a VPN connection

When finished, click [Save] the VPN will be configured.



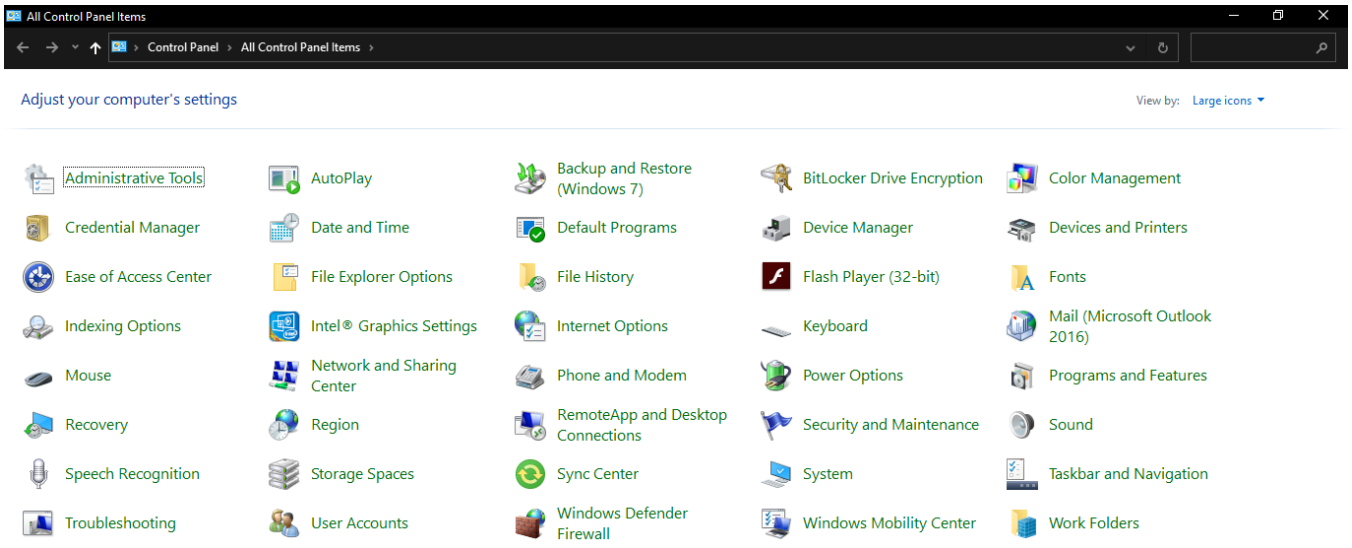
VPN - VPN configured

Next we need to make the last settings on the network connections. Again on the desktop, type the command Windows + R, or select "Run" from your Start Menu, the window below will be displayed, in its text field, type "control panel".

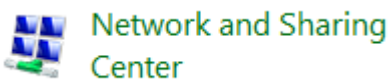


Run - control panel

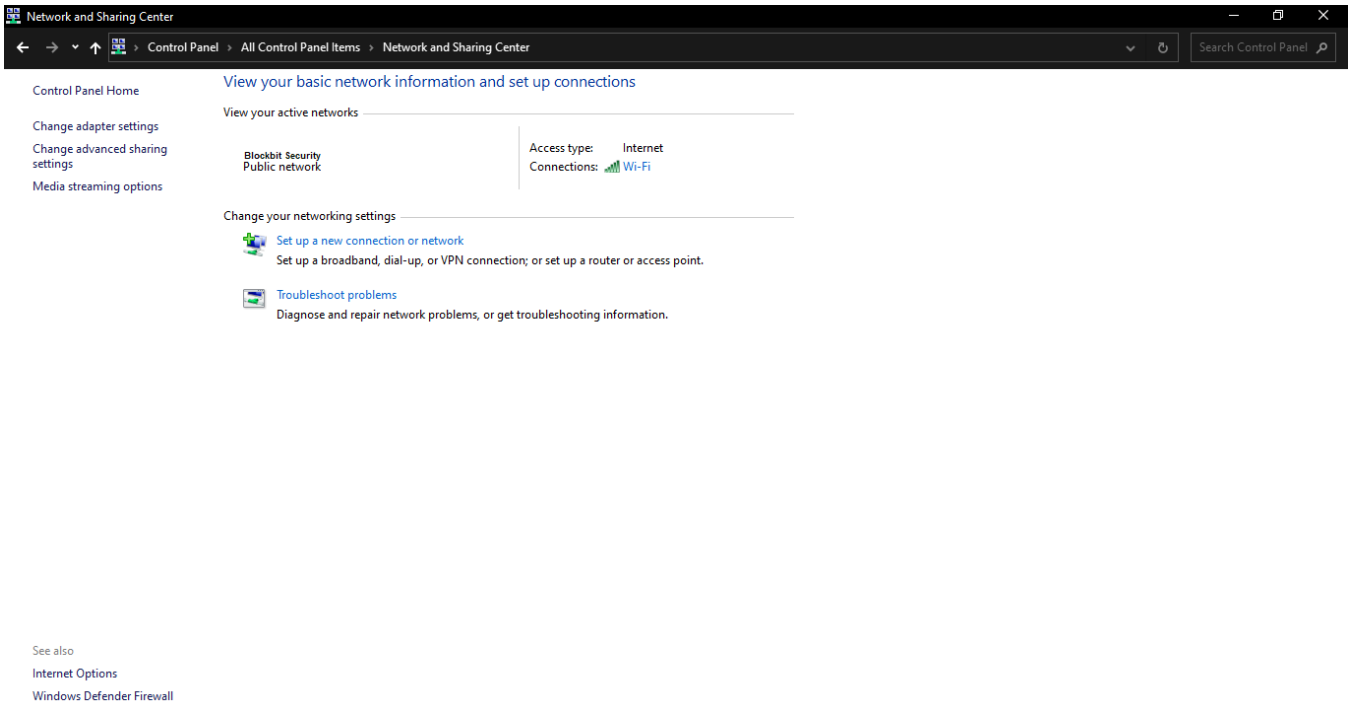
The control panel will be displayed, as shown below:



Control Panel

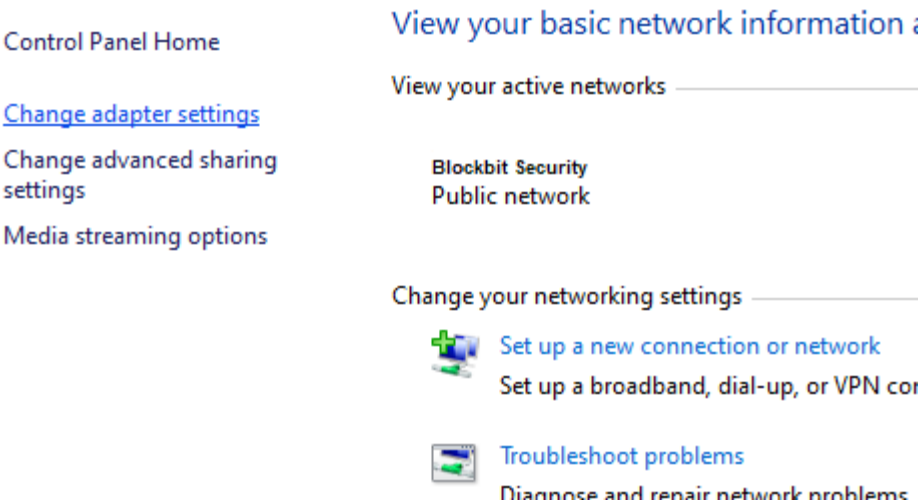
Select option **[** 

], the following screen will be displayed:



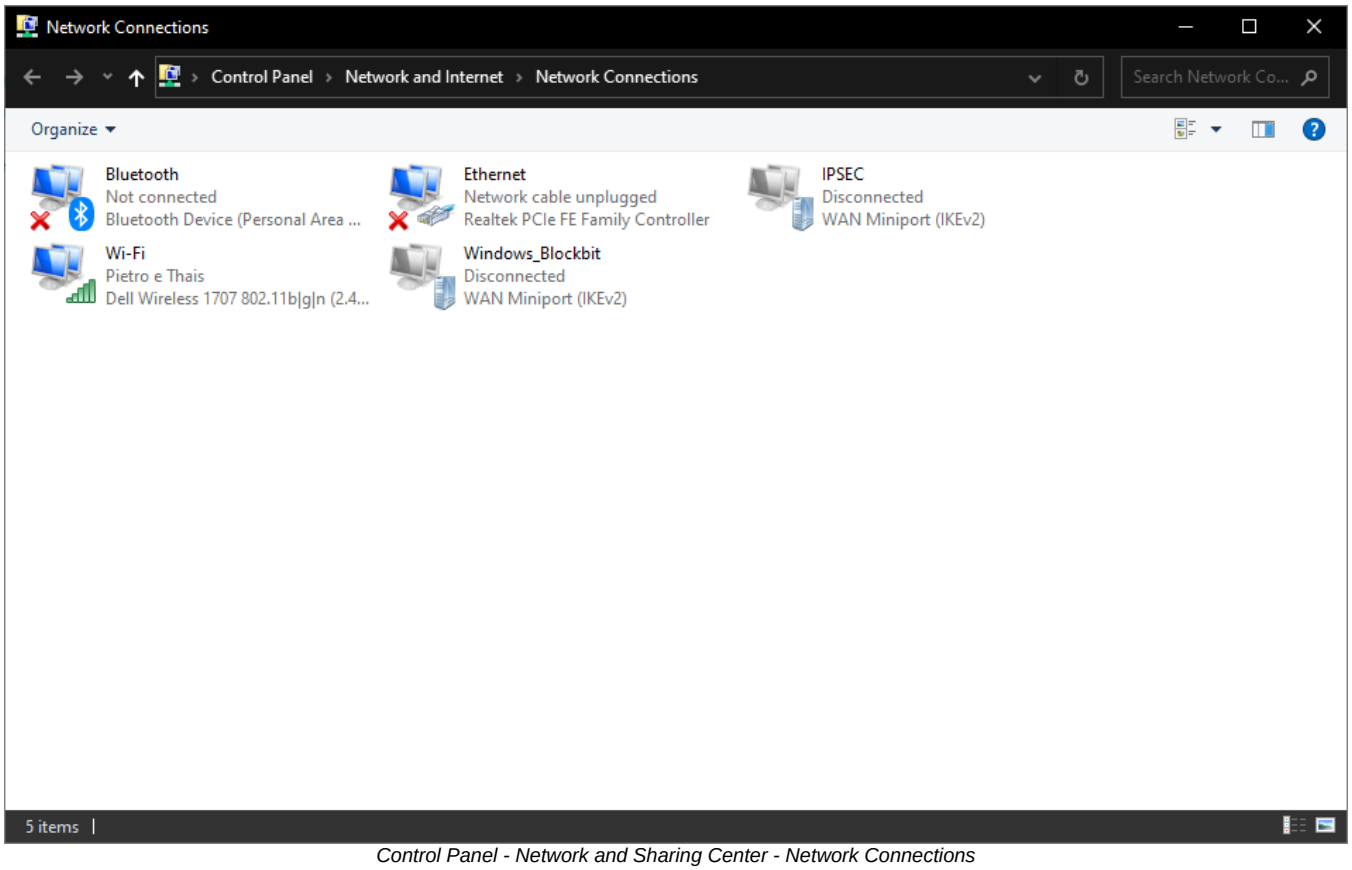
Control Panel - Network and Sharing Center

Click on the "Change adapter settings" option on the left side menu, as shown below:



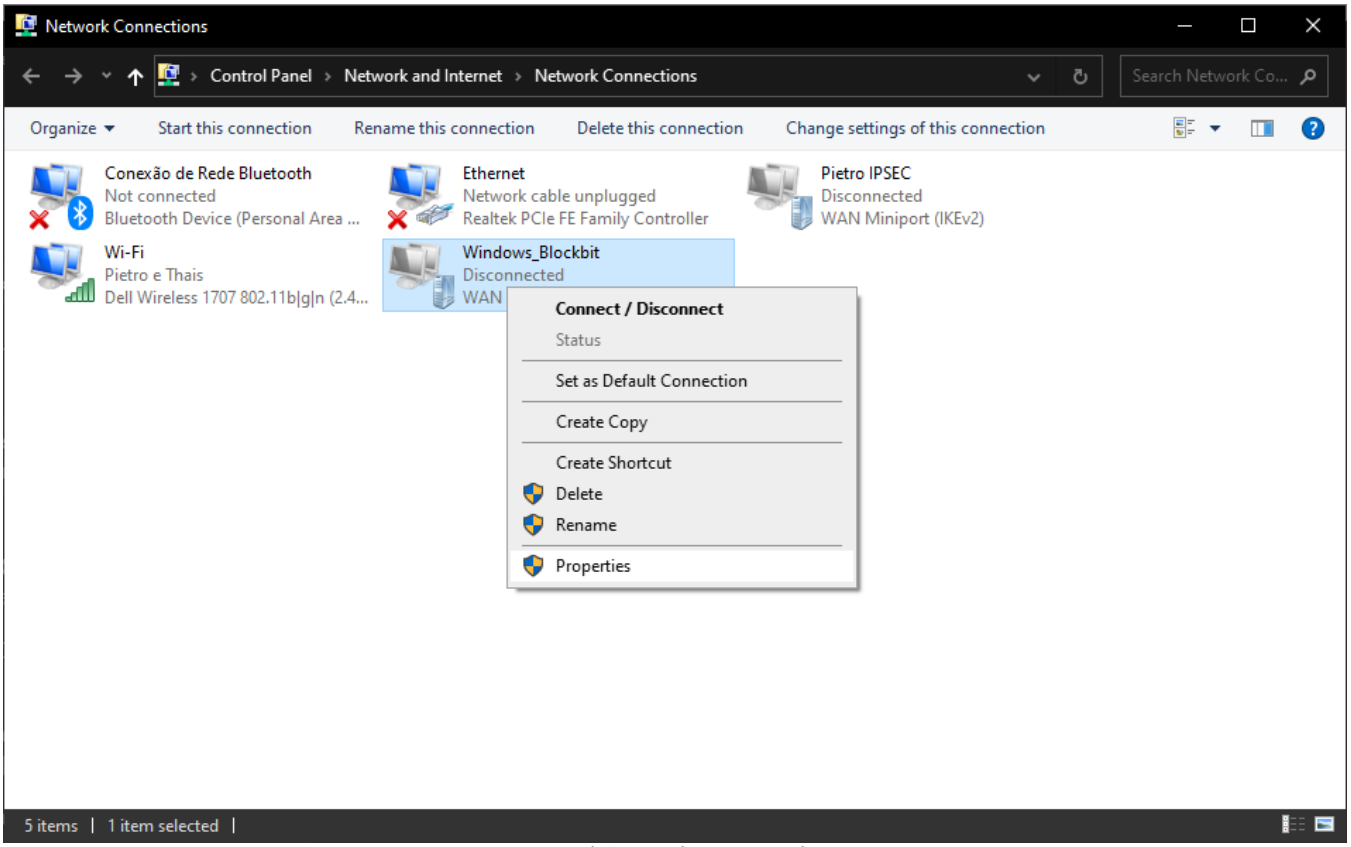
Control Panel - Network and Sharing Center - Change adapter settings

The following screen will be displayed:



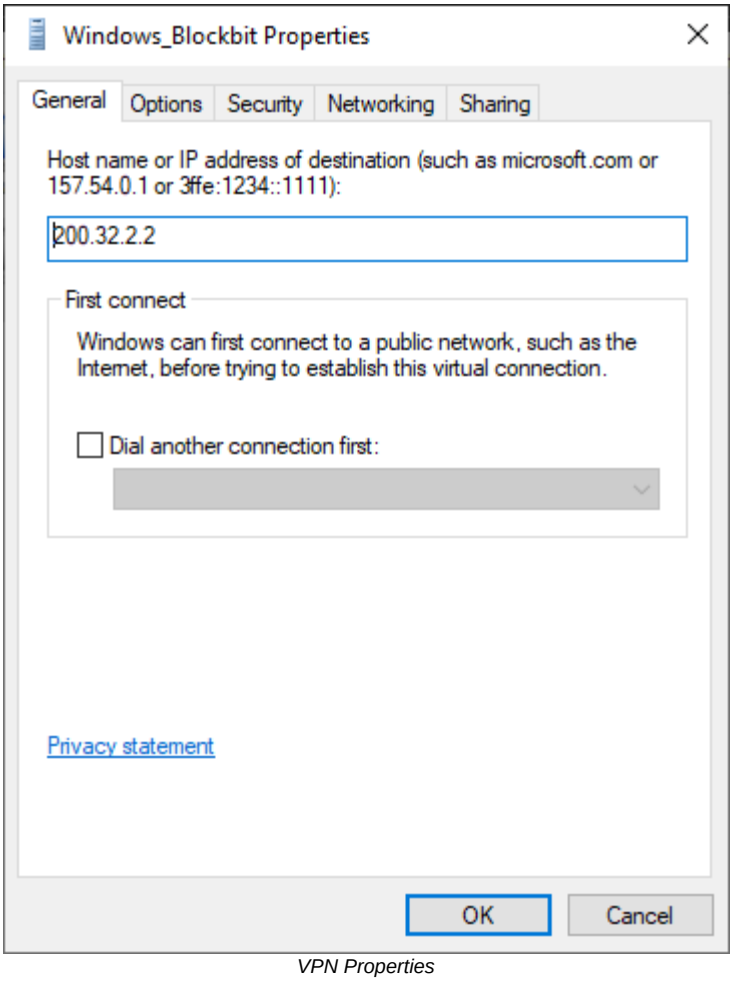
Control Panel - Network and Sharing Center - Network Connections

Right click on the VPN that was created earlier and select "Properties":



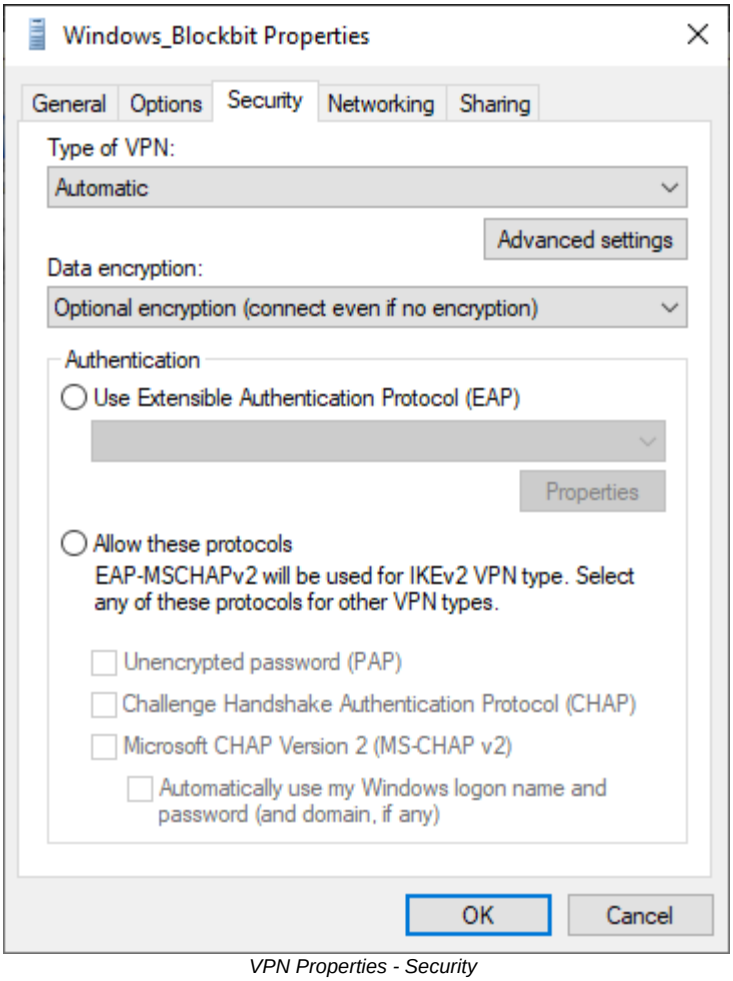
Network Connections - Properties

The VPN properties window will appear:



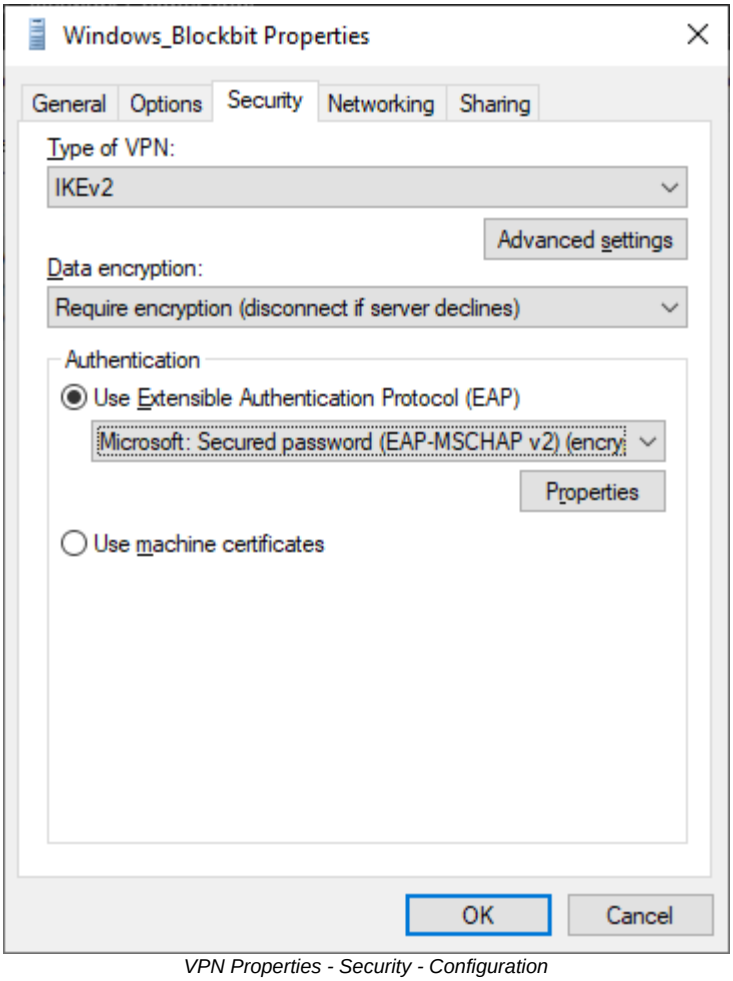
VPN Properties

Select the "Security" tab:



VPN Properties - Security

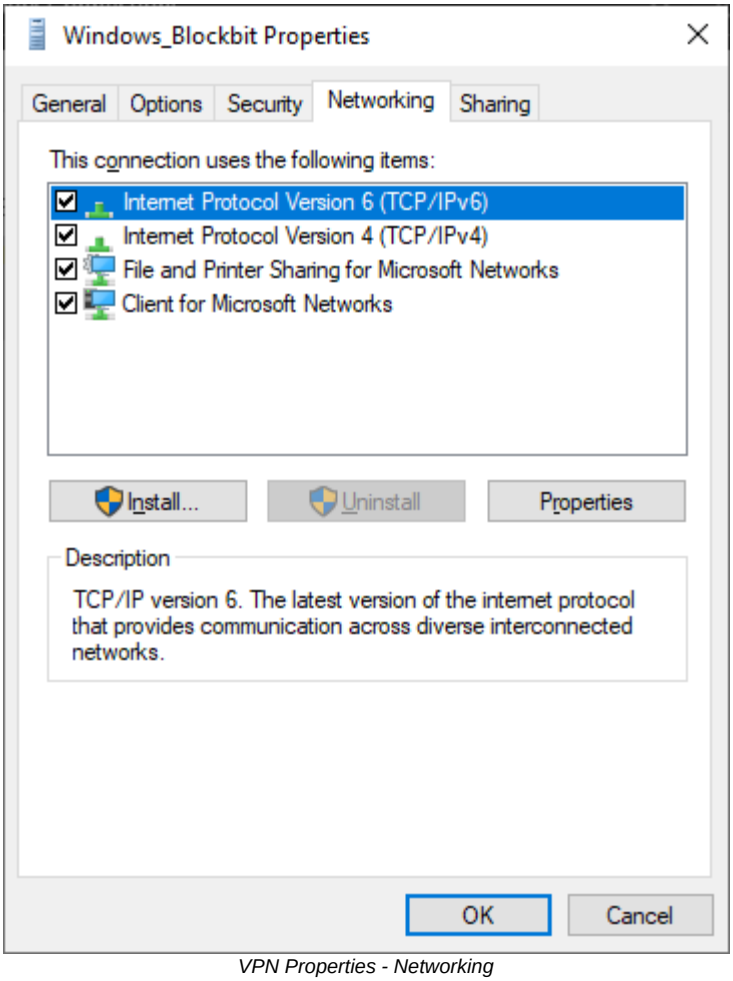
In this tab we will need to make some changes, configure it as shown below:



VPN Properties - Security - Configuration

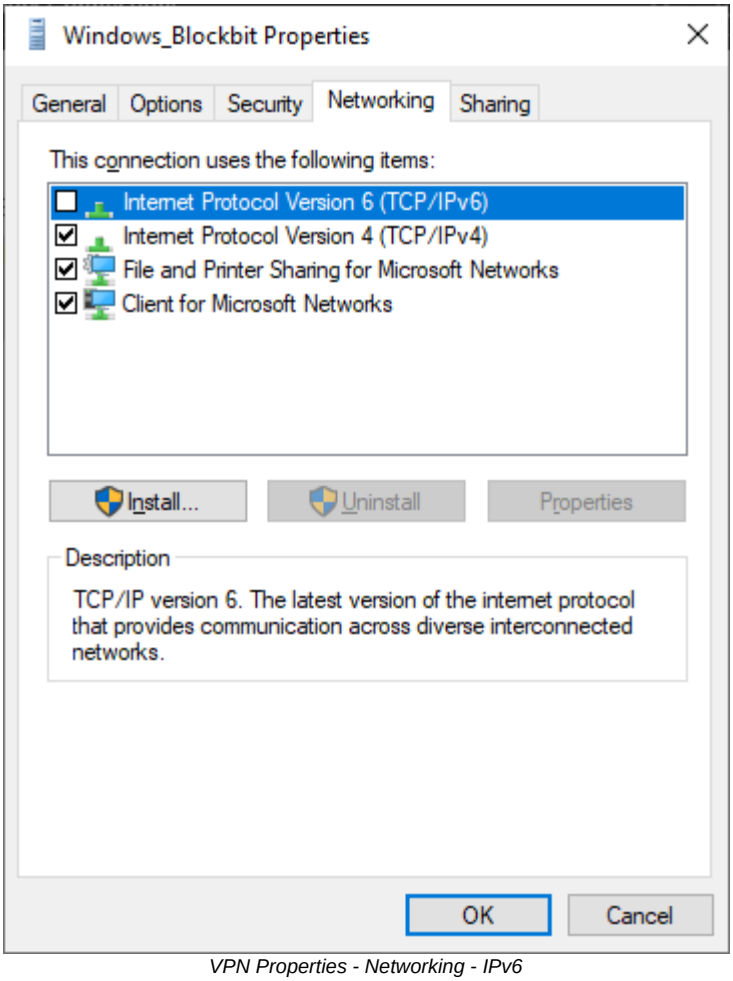
- **VPN type:** Select the "IKEv2" option;
- **Data encryption:** Select "Require encryption (disconnect if the server refuses)";
- **Use EAP protocol [◉]:** Make sure "Microsoft: Secure password (EAP-MSCHAP v2) (encryption enabled)" is selected.

After configuring settings, click on the "Network" tab, as shown in the image below:



VPN Properties - Networking

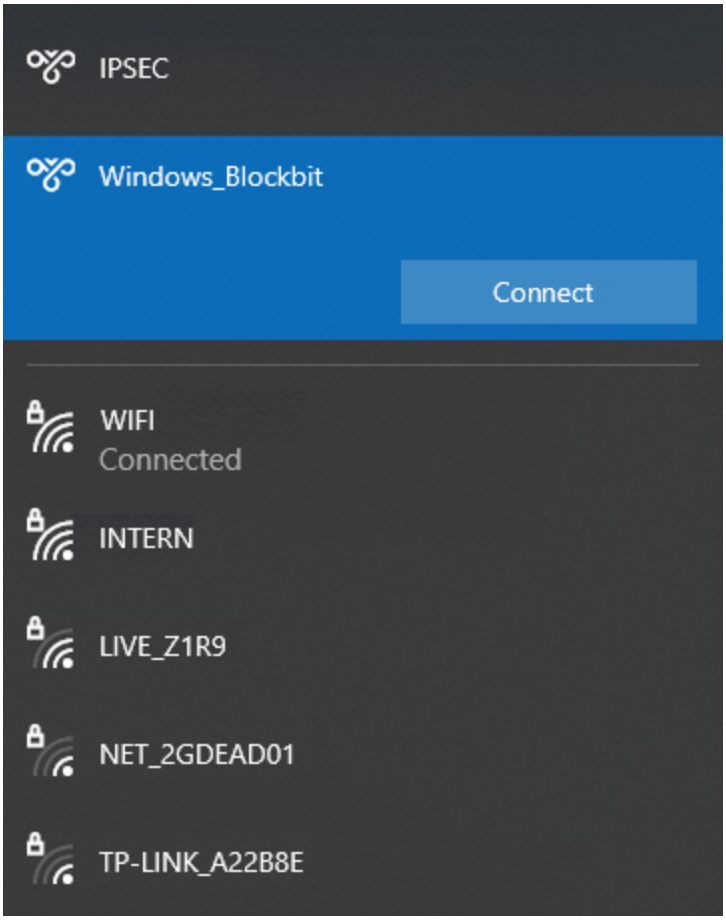
Disable "IPv6", as shown below:



VPN Properties - Networking - IPv6

Click **[** OK **]** to save the settings.

After these steps, the VPN will be ready, to connect, just click on the **[**  **]** icon located in the lower right corner of your screen and select the created VPN, as shown below:



Connect to VPN

Just click [Connect] to access the new VPN.

This concludes the IPSEC RAS VPN configuration walkthrough with the default Windows VPN client, for more information on this type of VPN, see this page
.

VPN IPSEC - Failover tab

Failover is an important function for networks that require high availability.

This section discusses the options to support IPSec Fully Redundant VPN and Partially Redundant IPSec, using approaches based on the routing applied by SD-WAN.

Blockbit NGFW includes the SD-WAN FailOver feature and this feature is extended to the IPSec VPN service (lan to lan).

With the SD-WAN service configured for two or more network interfaces connected to the internet, Blockbit NGFW supports configuration for redundant IPSec VPNs for the same remote point. If the primary connection fails, Blockbit NGFW can re-establish the VPN using the other connection automatically.

The administrator has the option of configuring VPN tunnels and enabling Failover mode for tunnels configured for the same destination network, defining priority levels and listing the main VPN tunnel, in order to automatically re-establish communication with the network. destination without the need for manual intervention.

How VPN Failover Works

Each WAN interface at one VPN point communicates with another WAN interface at the other VPN point. This ensures that the VPN will always be available, as long as each VPN point has the SD-WAN failover service enabled, ensuring the availability of Internet communication.

The administrator must configure the VPN points for both WAN network interfaces enabled on the SD-WAN for the same destination lan network, respectively for each WAN interface of the other VPN point.

The configuration procedure must be applied at both VPN points.

The VPN Failover service monitors the status of links enabled on the SD-WAN.

FailOver VPN changes the routing priority of configured VPN tunnels in the event of the following events:

- If the SD-WAN notifies communication failure with the link in use in the configuration of the active VPN tunnel;
- If physical communication fails with network interfaces of the active VPN tunnel.

If communication with the active tunnel route fails, the VPN failover service disables and drops the active tunnel, and the next failover tunnel enabled on the priority list starts automatically.

When a failover event occurs, connections are lost due to the timeout and the time to reestablish the tunnel with the new SD-WAN gateway. *This period depends on the time settings of the failover tests configured in the SD-WAN service.*

In the restoration of the VPN tunnel the same process occurs.

To configure a Failover VPN correctly, it is recommended to consider some checks and requirements:

1. The interfaces of your Blockbit NGFW device must be listed and configured with the appropriate gateway;

2. SD-WAN Failover must be enabled and configured;

3. Configure 2 (two) or more VPN IPSec tunnels, both VPN tunnels must be configured to start in “Wait” mode;

4. For VPN connection using DSL links, enable the DDNS service of the VPN point with dynamic IP DDNS;

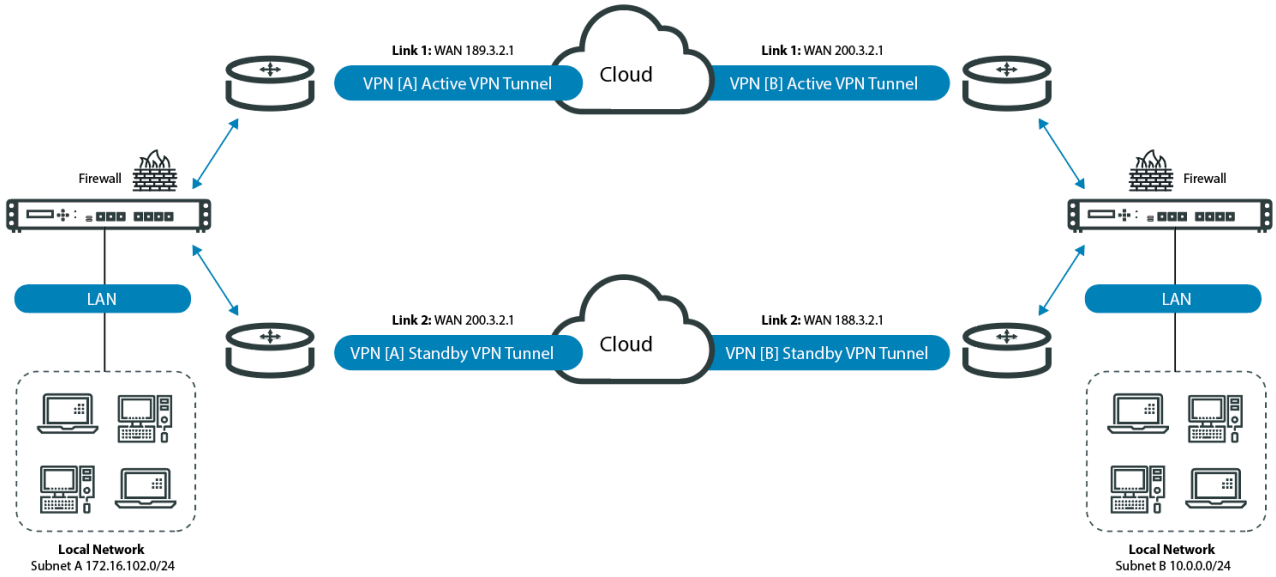
5. When configuring the VPN tunnel for points with DSL links, configure the “Remote host”, “Local ID” and “Remote ID” fields in the FQDN (Full Quality Domain Name) standard. Example: “host.domain”;

6. For the case of the VPN site with dynamic IP, identify with the name of “host.domain” according to the publication in the DDNS service.

Below is an example of a fully redundant topology.

Fully redundant IPSEC VPN topology

Fully redundant configuration requires redundant connections to the Internet at both points of the VPN.



Fully redundant IPSEC VPN

This example of a redundant VPN is based on the routes of the SD-WAN service, and demonstrates a fully redundant configuration for lan to lan VPN.

At each VPN point, Blockbit NGFW has two interfaces connected to the Internet through different internet providers - ISPs (Internet Service Provider).

Table - Redundant IPSEC VPN

BLOCKBIT UTM *VPN* [A] – *WAN* 1		BLOCKBIT UTM *VPN* [B] – *WAN* 1
BLOCKBIT UTM *VPN* [A] – *WAN* 2		BLOCKBIT UTM *VPN* [B] – *WAN* 2

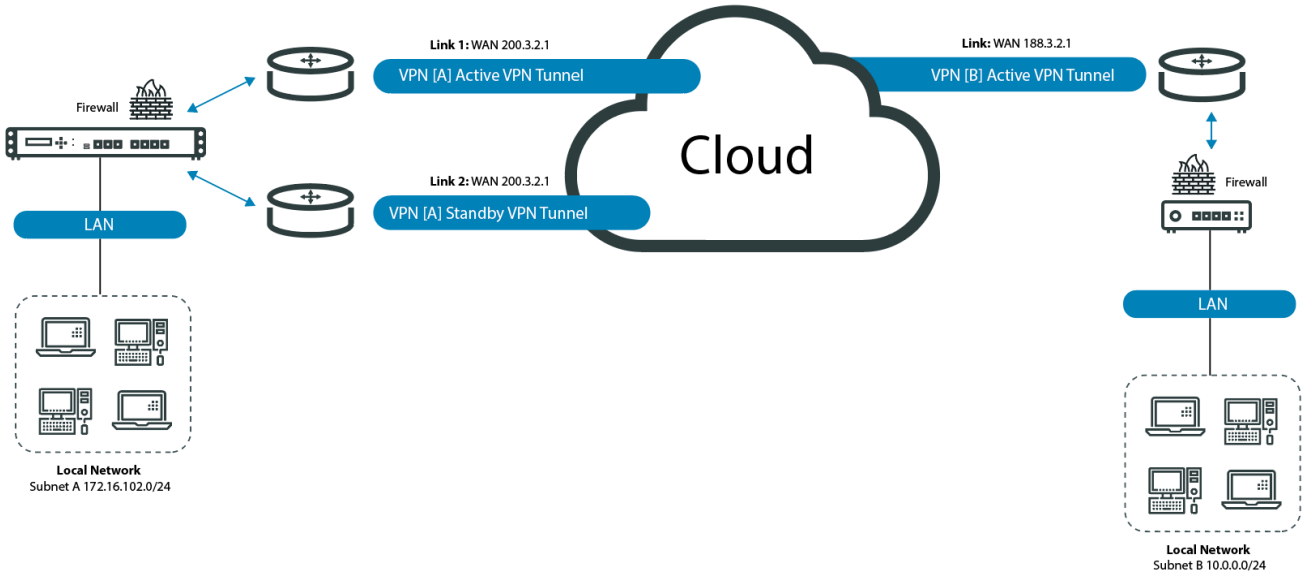
This method is reliable to ensure high availability for a reliable connection between two Blockbit devices with static IP addresses.

In a fully redundant VPN configuration with SD-WAN enabled, we can configure VPN points for all redundant SD-WAN interfaces, as a result we will have a total of SD-WAN interfaces and different routes for VPN traffic lan to lan.

The following is an example of a partially redundant topology.

Partially redundant IPSEC VPN topology

The partially redundant configuration includes only one VPN point with redundant connections to the Internet.



VPN IPSEC - Partially redundant

This example demonstrates a partially redundant IPSec VPN configuration between a BLOCKBIT NGFW device and an IPSec VPN point (can be a Blockbit NGFW device or another VPN device with Standard IPSec support).

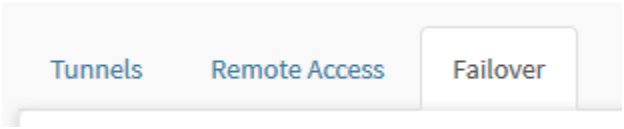
Only at a VPN point does Blockbit NGFW have two interfaces connected to the Internet through different internet providers - ISPs (Internet Service Provider). The IPSec Remote VPN tip has only one interface connected to the internet.

Table - Partially redundant IPSEC VPN

BLOCKBIT NGFW *VPN* [A] – *WAN* 1		BLOCKBIT NGFW *VPN* [B] – *WAN* 1
BLOCKBIT NGFW *VPN* [A] – *WAN* 2		

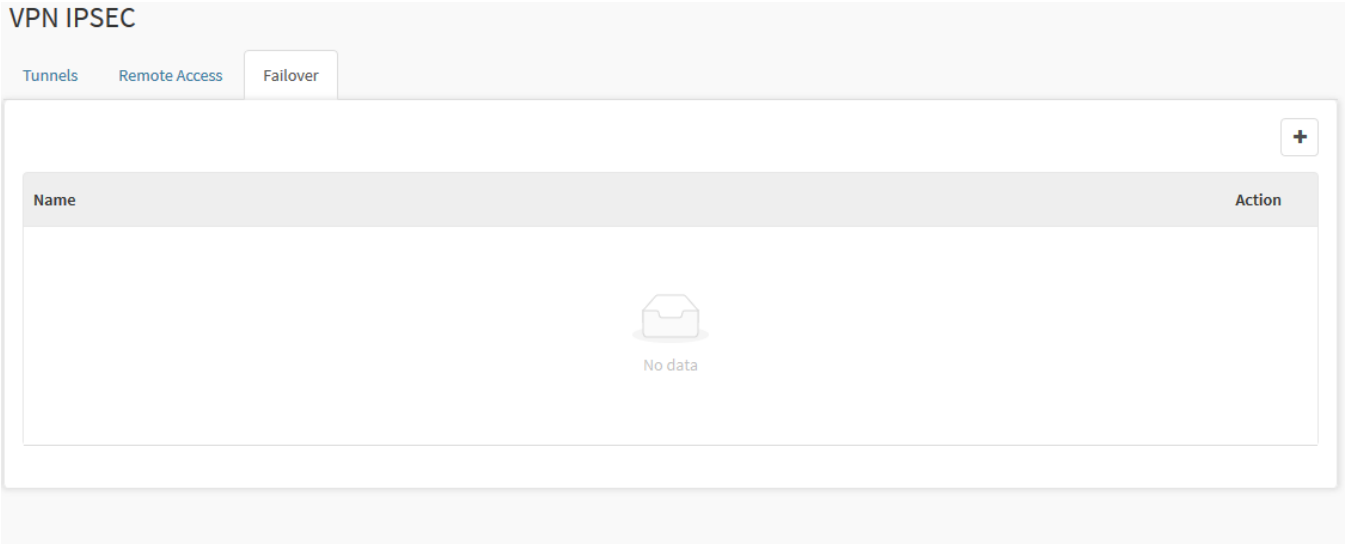
This method does not guarantee high availability for a reliable connection between two IPSec VPN points. In a partially redundant VPN configuration only the point with SD-WAN enabled guarantees availability for VPN traffic. If communication fails with the remote IPSec VPN point with a single WAN address, the connection to the VPN is lost.

To make the settings access the Failover tab:



Failover tab

The screen below will be displayed:



VPN IPSEC - Failover

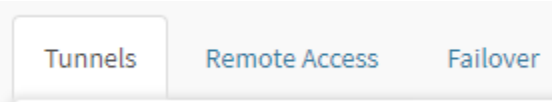
In this session we will analyze:

- Addition Button;
- Composition of each column.

Next we will analyze each component of this screen.

Failover - Add button

To enable IPSec VPN tunnels in failover mode, before the administrator needs to configure the VPN tunnels, access the Tunnels tab:



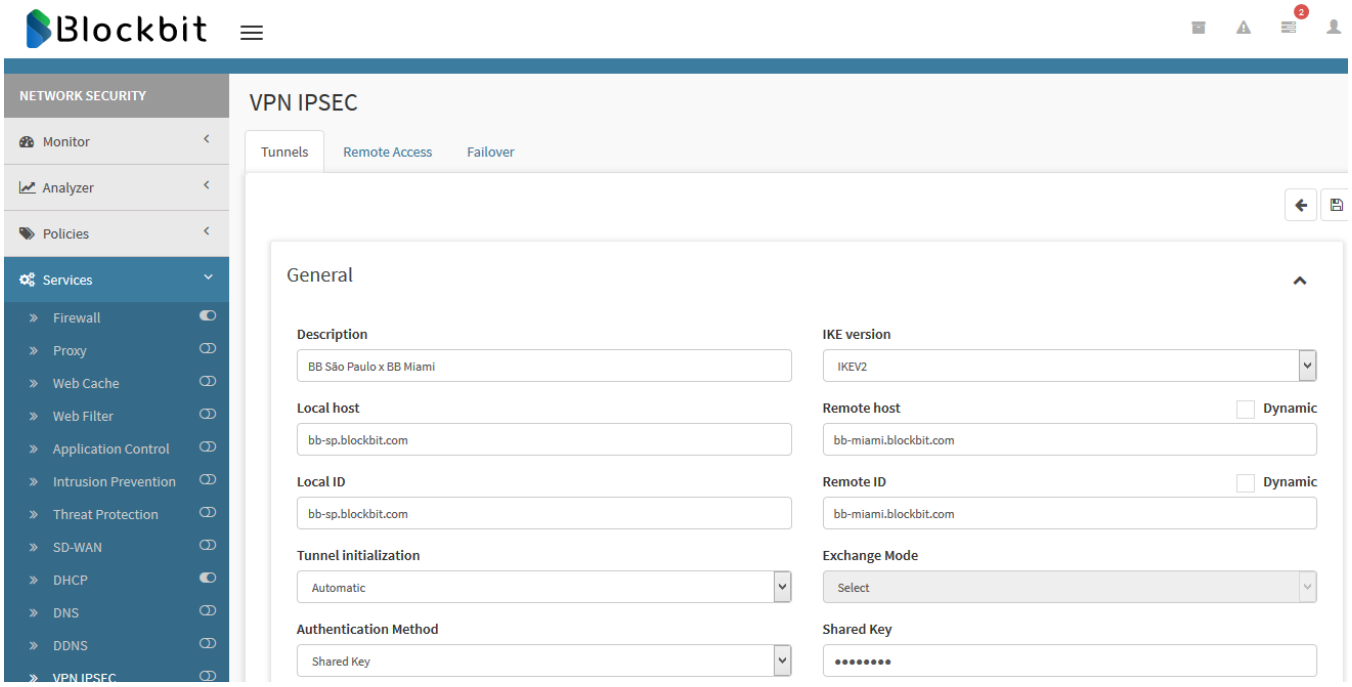
Tunnels Tab

Click the [+] button and configure [N] IPSec VPN tunnels for the same remote IPSec point, for the same target lan network based on security settings for enabling failover mode on Blockbit NGFW devices and the number of redundant links enabled in the SD-WAN.

Configure all fields on the form based on the information gathered and the pre-established requirements checks. Keep both tunnels **“enabled”** and **“configured”** in startup mode on **“Wait".**

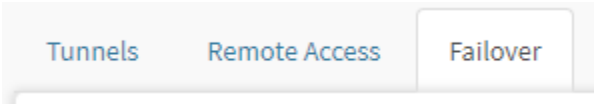
For more information on how to configure IPSEC tunnels, see this page.

After making these settings, the form will be similar to the one shown below:



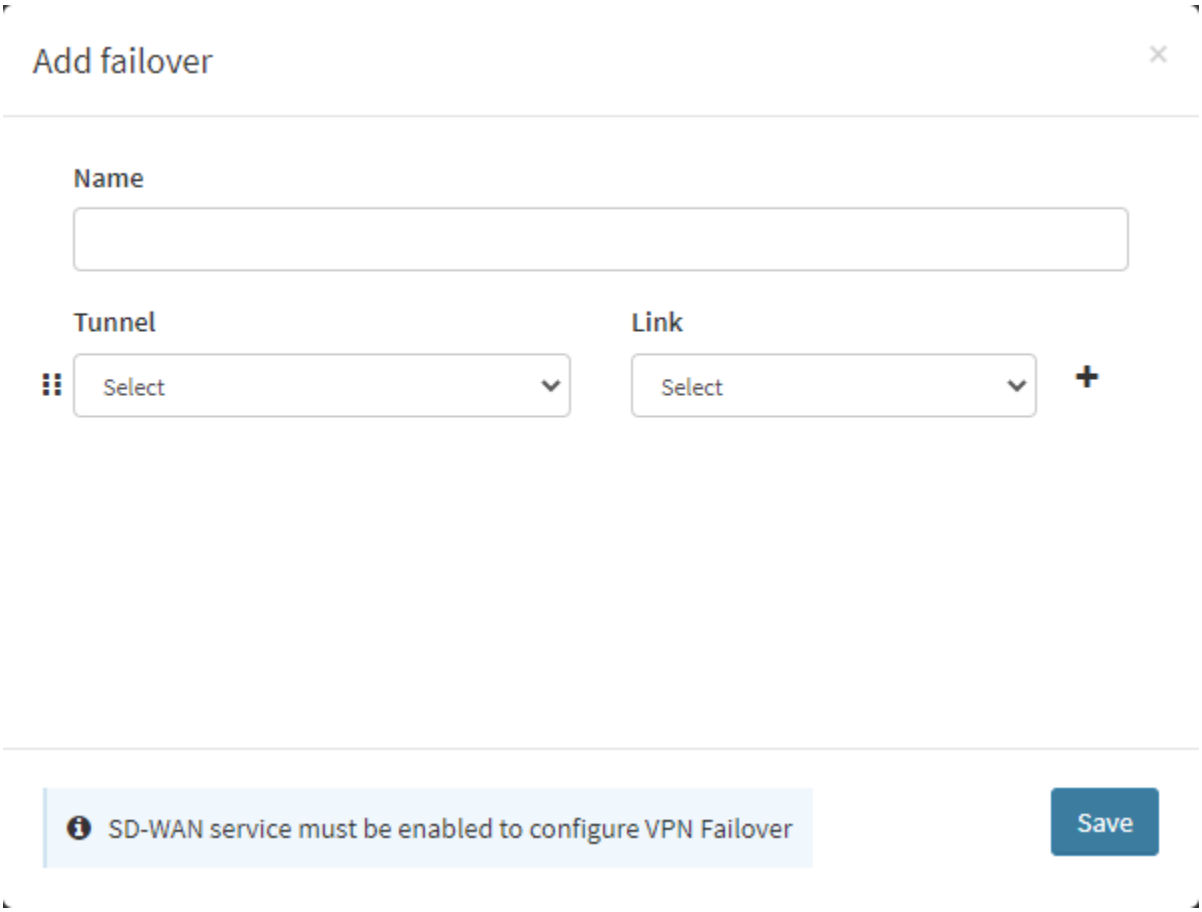
Configuring the IPSEC VPN Tunnel

After this step, access the Failover tab.



Failover tab

Click on the button [+]. The following window will be displayed:



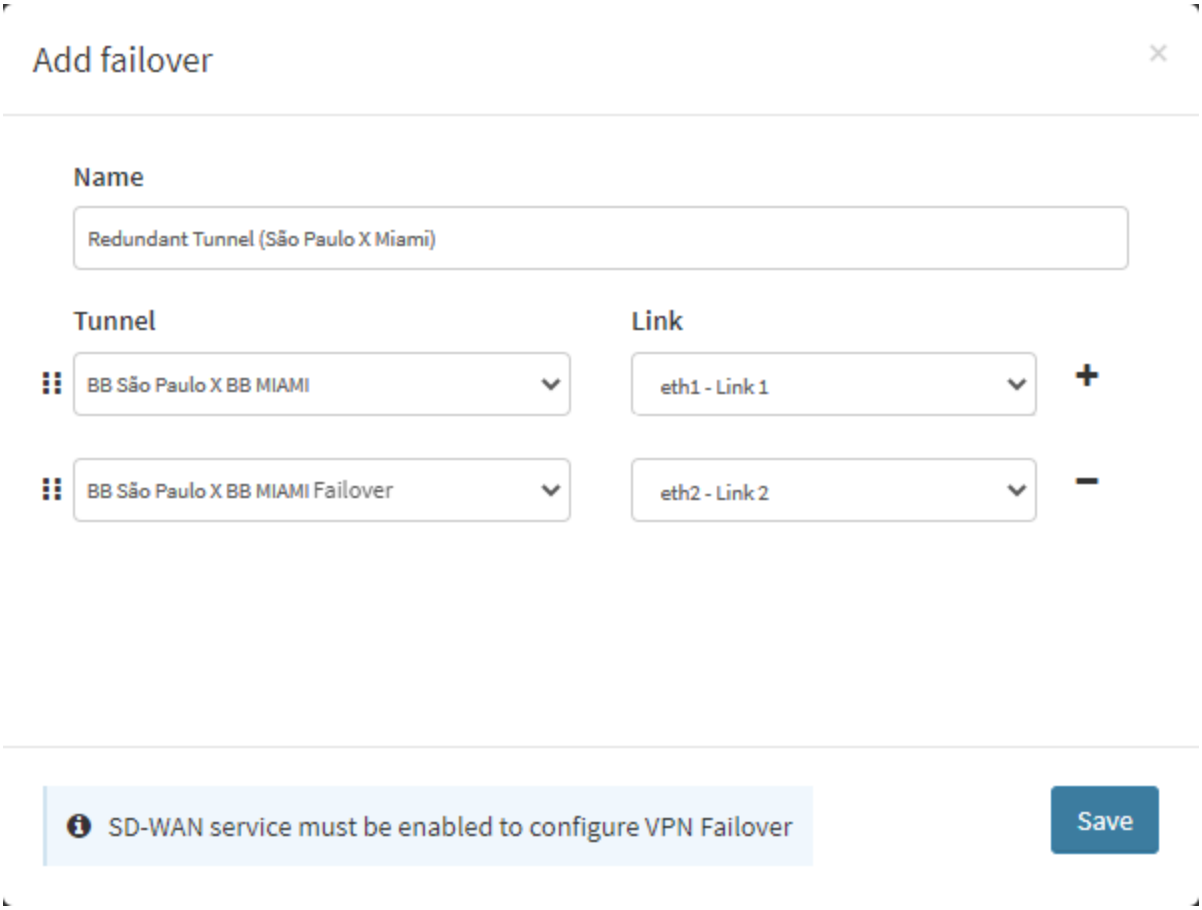
Failover - Add Failover

- ***Tunnel*:** Add the tunnel that was created in the *Tunnel* tab;
- ***Link*:** Add the redundant Link that was enabled in the *SD-WAN Failover*.

Click **[+]** to add more Tunnels and Links or **[−]**.

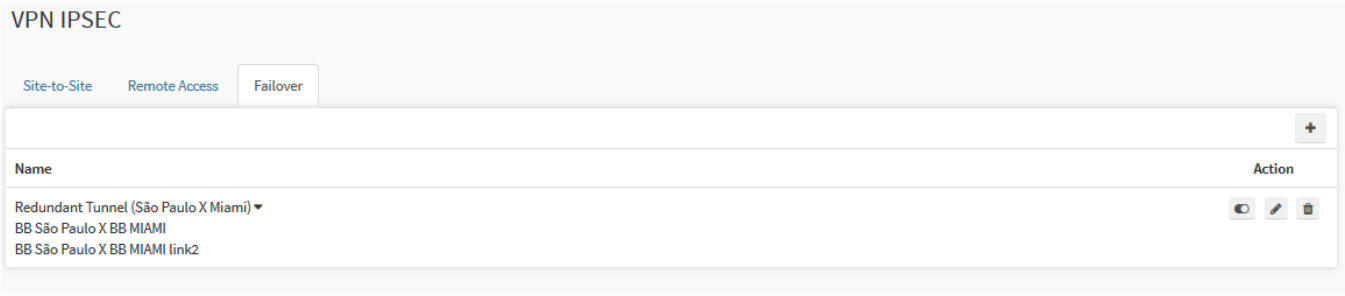
In addition, **[⠿]** allows you to sort them in order of priority.

After completing the addition of the tunnels that will be used to enable the redundancy mode, the form will be similar to the one shown below:



VPN IPSEC - Add failover

When finished, click **[**  **]** to save the settings.



VPN IPSEC - Failover

Blockbit NGFW supports VPN communication with any VPN device that supports Standard, redundant and non-redundant IPSec.

Detailing of the parts of the Head Office and Branch VPN Failover:

When the SD-WAN module detects that the 1st link is off, it automaticaly disables VPN 1, and enables VPN2 by using the 2nd link.

When the 1st link is back on, it will disable VPN 2 and enable VPN 1 back on, by using the 1st link once more.

As to the configuration, the parameters in "Advanced" have to be set in the following way in the Head Office's tunnels:

Tunnel's initialization: **Hold**

- ***DPD Action:*** Clear
- ***DPD Delay:*** 5
- ***DPD Timeout:*** 10

On the Branch side, where the VPN Failover is configured on the tunnels:

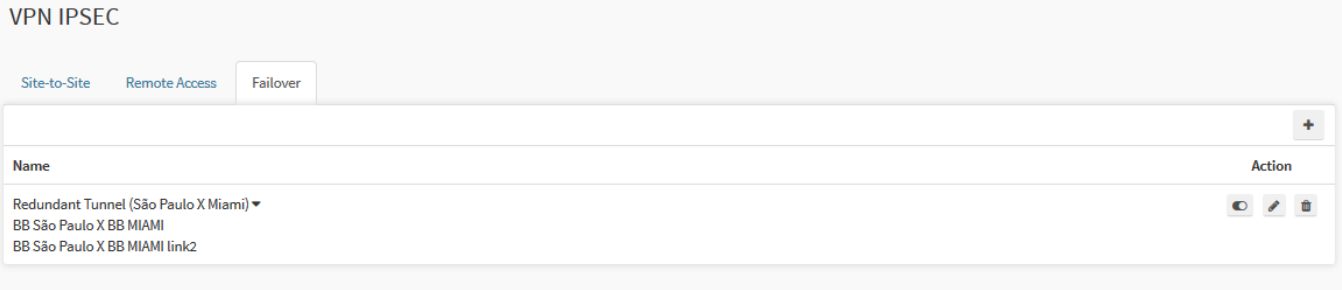
Tunnel's initialization: **Automatic**

- ***DPD Action:*** Clear
- ***DPD Delay:*** 5
- ***DPD Timeout:*** 10

Next, we will analyze the column components of the Failover tab.

Failover - Columns

Next we will analyze each column of the IPSEC VPN screen - Failover tab:



VPN IPSEC - Failover

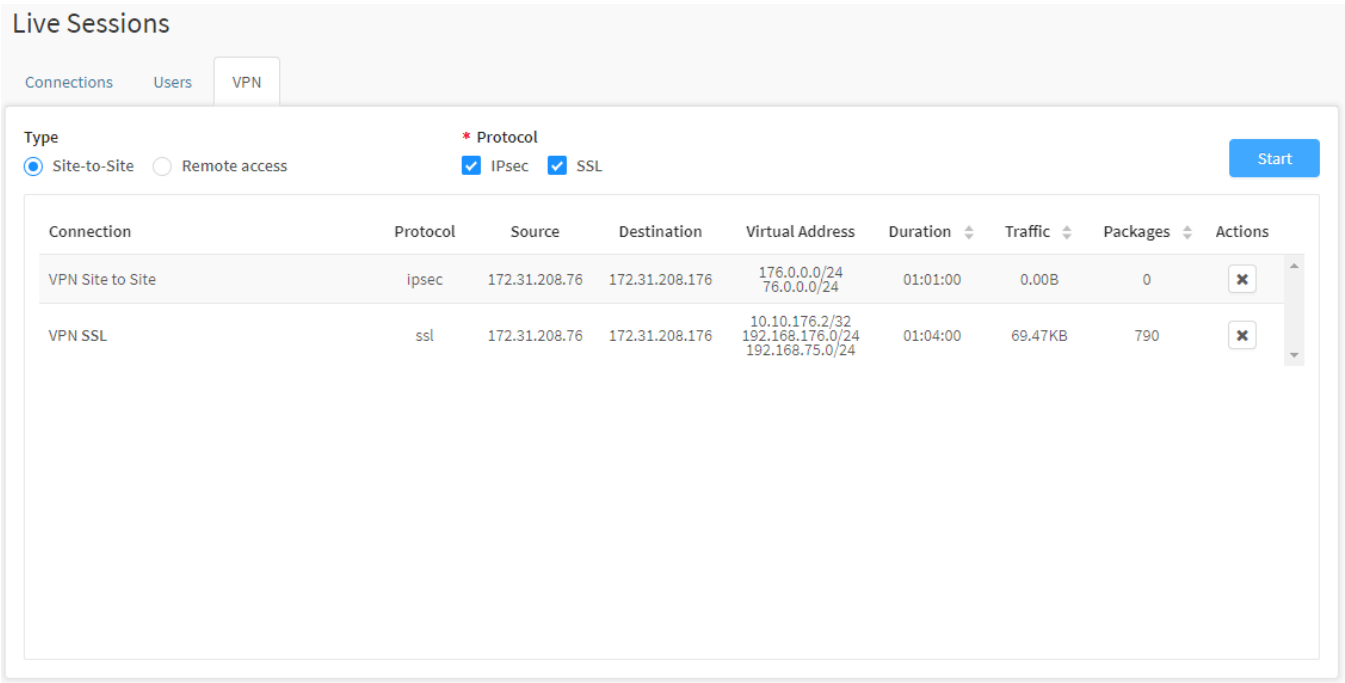
- ***Name*:** Displays the name of the VPN Failover registered during the addition process, in addition to clicking **[ ]**, the added tunnels are displayed;
- ***Action*:** It has a set of essential buttons, these being:
  - ***Enable*[ ]/*Disable*[ ]:** This column enables or disables Failover;
  - ***Edit*[ ]:** This button allows you to edit the Failover settings, it displays a screen similar to the Failover addition screen;
  - ***Delete*[ ]:** Removes Failover.

This concludes the analysis of the Failover tab.

Troubleshooting VPNs

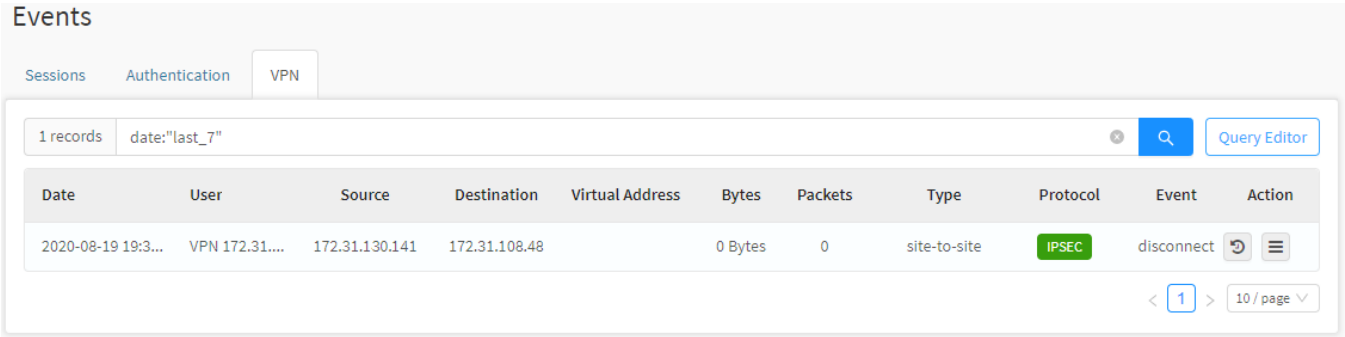
After creating and configuring the VPN tunnels, if it is necessary to validate the configuration or investigate possible problems, you can perform the following procedures:

- Access the *Live Sessions - VPN* tab on the NGFW Monitor. On this screen it is possible to view the current VPN sessions, and it is even possible to drop connections if necessary;



Live Sessions - VPN

- Access the *Security Events - VPN* screen. Where you can search and view VPN logs;



Security Events - VPN

- Access the CLI of your NGFW and enter the command *debug-vpn -t ipsec*. This command is used to display in real time the data on access, source and destination IPs, packet transfer and etc;

```
admin  >debug-vpn -t ipsec
Aug 20 19:17:28.958 05[NET] <tun16|4389> received packet: from 172.31.240.241[500] to 172.31.208.40[500] (36 bytes)
Aug 20 19:17:28.958 05[ENC] <tun16|4389> parsed IKE_SA_INIT response 0 [ N(NO_PROP) ]
Aug 20 19:17:28.958 05[IKE] <tun16|4389> received NO_PROPOSAL_CHOSEN notify error
Aug 20 19:19:28.956 12[CFG] vici initiate 'tun16', me 172.31.208.40, other 172.31.240.241, limits 0
Aug 20 19:19:28.956 12[IKE] <tun16|4390> initiating IKE_SA tun16[4390] to 172.31.240.241
Aug 20 19:19:28.957 12[ENC] <tun16|4390> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(
REDIR_SUP) ]
Aug 20 19:19:28.957 12[NET] <tun16|4390> sending packet: from 172.31.208.40[500] to 172.31.240.241[500] (332 bytes)
Aug 20 19:19:28.960 15[NET] <tun16|4390> received packet: from 172.31.240.241[500] to 172.31.208.40[500] (36 bytes)
Aug 20 19:19:28.960 15[ENC] <tun16|4390> parsed IKE_SA_INIT response 0 [ N(NO_PROP) ]
Aug 20 19:19:28.960 15[IKE] <tun16|4390> received NO_PROPOSAL_CHOSEN notify error
```

Command Line Interface – debug-vpn -t ipsec

- Still in the CLI of your NGFW and enter the command *show-vpn-conn*. This command displays data about the tunnels, connection time, encryption used and etc;

```
admin  >show-vpn-conn
tun1: #1, ESTABLISHED, IKEv1, 46b72d9f1eb1bde4:c90e3afe280a6bcf
  local  '200.200.100.101' @ 200.200.100.101[500]
  remote '200.200.100.102' @ 200.200.100.102[500]
  3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
  established 14s ago, rekeying in 10308s
  tun1: #1, reqid 1, INSTALLED, TUNNEL, ESP:3DES_CBC/HMAC_SHA1_96
    installed 14s ago, rekeying in 3003s, expires in 3586s
    in  ce95e16d,      0 bytes,     0 packets
    out c60db9a6,      0 bytes,     0 packets
    local  192.168.200.0/24
    remote 192.168.210.0/24
```

Command Line Interface – show-vpn-conn

- Finally, it is also possible to consult the data displayed through the CLI command show-vpn-info. The function of this command is to display general information about the VPN.

```
admin  >show-vpn-info
  uptime: 16 seconds, since Mar 15 09:31:28 2018
  malloc: sbrk 2703360, mmap 0, used 576032, free 2127328
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
Listening IP addresses:
  172.16.102.78
  200.200.100.101
  192.168.222.1
Connections:
       tun1:  200.200.100.101...200.200.100.102,0.0.0.0/0,::/0  IKEv1
       tun1:   local:  [200.200.100.101] uses pre-shared key authentication
       tun1:   remote: [200.200.100.102] uses pre-shared key authentication
       tun1:   child:  192.168.200.0/24 === 192.168.210.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
       tun1[1]: ESTABLISHED 16 seconds ago, 200.200.100.101[200.200.100.101]...200.200.100.102[200.200.100.102]
       tun1[1]: IKEv1 SPIs: 46b72d9f1eb1bde4_i* c90e3afe280a6bcf_r, rekeying in 2 hours
       tun1[1]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
       tun1{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ce95e16d_i c60db9a6_o
       tun1{1}:  3DES_CBC/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 50 minutes
       tun1{1}:   192.168.200.0/24 === 192.168.210.0/24
```

Command Line Interface – show-vpn-info

When using the *"vpn-ipsec"* command the following help message will be displayed:

Usage: vpn-ipsec [OPTION] [ID]
Script that start or stop vpn ipsec connection.

Optional Arguments
up, Start vpn ipsec connection
down, Stop vpn ipsec connection
-h, --help Display this help message and exit

Example

vpn-ipsec [option] [tunnel-id]

vpn-ipsec up 1

vpn-ipsec down 2

Where we can check the commands used to activate and deactivate a tunnel:

- ***Activate: admin>vpn-ipsec up <id>***
- ***Deactivate: admin>vpn-ipsec down <id>***
- ***Id:*** It's the id of the tunnel to be activated/deactivated.

```
admin  >vpn-ipsec up 1
[IKE] establishing CHILD_SA tun1{92}
[ENC] generating CREATE_CHILD_SA request 420 [ SA No TSi TSr ]
[NET] sending packet: from 189.108.60.138[4500] to 152.249.126.84[4500] (224 bytes)
[NET] received packet: from 152.249.126.84[4500] to 189.108.60.138[4500] (224 bytes)
[ENC] parsed CREATE_CHILD_SA response 420 [ SA No TSi TSr ]
[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ
[IKE] CHILD_SA tun1{92} established with SPIs c5747035_i cdd098b8_o and TS 172.31.0.0/16 172.32.0.0/16 === 172.25.0.0/24
initiate_completed successfully
```

Command Line Interface - vpn-ipsec up 1

For more information about IPSEC VPN, check this page.

UTM - Services - SSL VPN

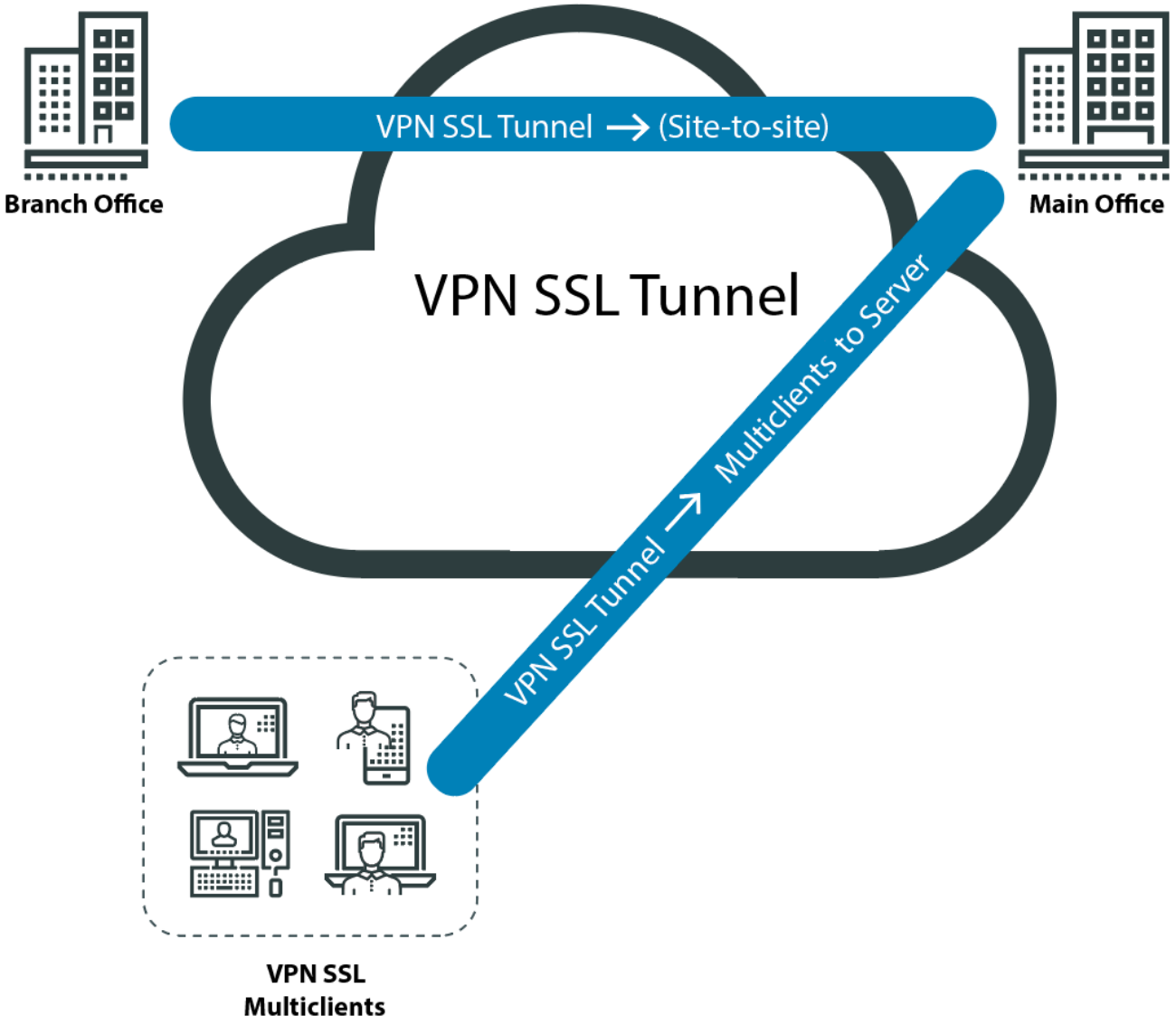
The SSL VPN is the service responsible for managing access of a secure connection under the SSL protocol to network applications and resources.

Unlike IPSEC, it does not establish site-to-site connections. SSL VPN works at layer 7 (OSI model). As SSL is a protocol that is embedded in most Web applications, this type of protocol encapsulation becomes a more compatible VPN solution between applications. It is a VPN modality that uses the resources of a standard WEB browser to establish its connection, works as a WEB portal (a public intranet) used to provide remote users with access to applications and resources on the private network from anywhere in the world.

The SSL VPN service on BLOCKBIT NGFW provides the SSL Tunnel VPN connection service that allows a duly authorized remote user to use a modern Web browser to securely access various services on the private network.

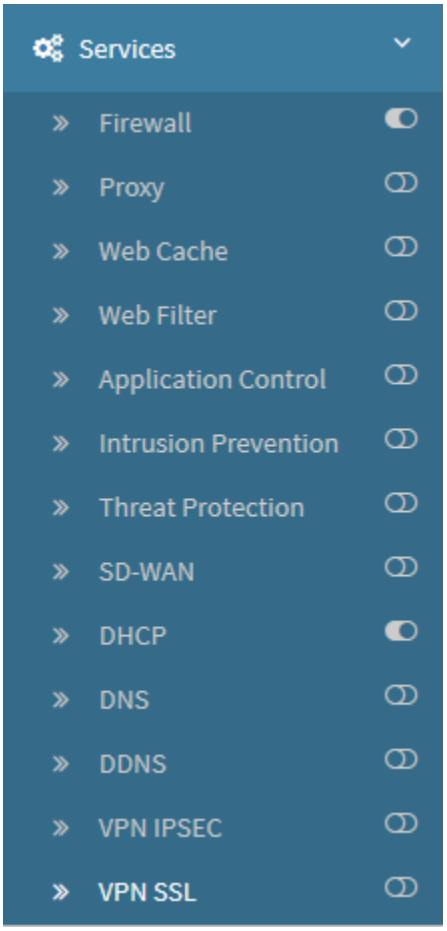
The traffic between the browser and the BLOCKBIT NGFW VPN SSL device is encrypted, offering versatility, ease of use, and specific controls for groups and users in each application mode available through the “Authentication Portal”.

The VPN SSL Tunnel is the service responsible for managing access to a secure connection under the SSL / TLS protocol.



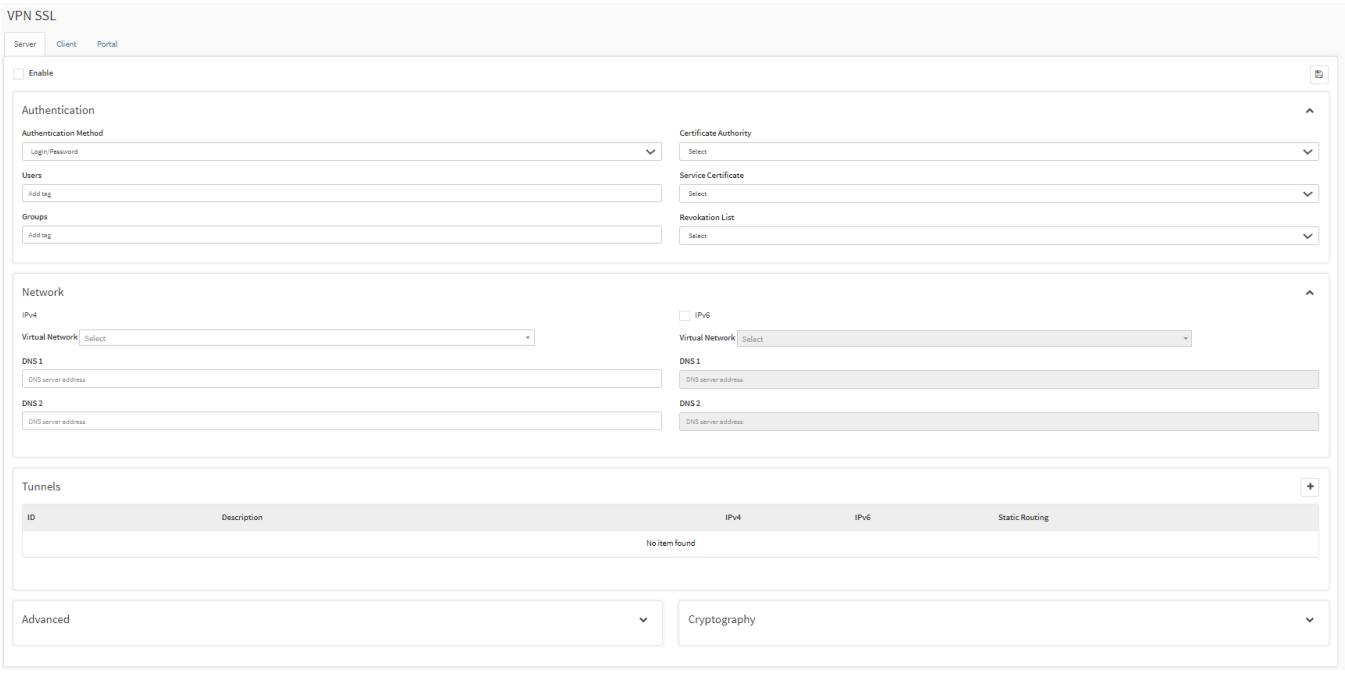
TUNNEL SSL VPN Topology

To access the resources click on the VPN SSL option.



Services - VPN IPSEC

The screen below will appear:



SSL VPN

In this session we will review some technical specifications:

- Encryption and Authentication;
- List of applications on SSL VPN access;
- Establishing SSL Portal VPN Access.

In addition, the SSL VPN screen consists of the tabs:

- *Server tab*;
- *Client tab*;
- *Portal tab*.

Next, we will detail each component of these screens.

VPN SSL - Encryption and Authentication

Even in remote access using a public medium, its access is encapsulated and encrypted using a range of security algorithms and protocols.

SSL VPN provides a high level of security through specific protocols that establish connectivity. Using SSL v3 / TLS v.1.2 that work in layers 4 and 5 of the OSI model (transport layer and Session). Information is encapsulated and encrypted in the presentation and application layers.

It implements a private Certification Authority (CA) to manage access to communication through digital certificates. In this way, only certificates issued by the product are accepted to negotiate the connection with the VPN concentrator.

Uses multi-factor authentication with encryption and a range of security methods to ensure that only authorized users can access the network.

- Shared Key(*PSK*);
- XAuth authentication;
- Digital certificate per user (X.509 certificate).

 The authentication method with (Shared secret keys - PSK) is the simplest, however when combined with X-Auth Authentication + Digital Certificates it becomes the most robust and powerful authentication feature.

It has high levels of security based on multiple encryption and authentication algorithms. (AES; Camellia, DES; IDEA; RC2); (MD5; DAS; RSA; SHA).

VPN SSL - List of applications on SSL VPN access

The SSL VPN service provides users with secure access to applications that are installed on a private network. Through the "Authentication Portal" users once authenticated have access to **[Virtual Office]** a "Bookmark" with the list of applications available for remote access.

The traffic between the browser and the BLOCKBIT NGFW's VPN SSL device is encrypted, offering versatility, ease of use, and specific controls for groups and users in each application mode available through the “Authentication Portal”.

The list of applications available for each user is defined through the VPN SSL management interface, that is, only previously enabled users will have access to the applications available in the SSL VPN access.

The tunneling feature of applications through the Portal basically consists of making a diversion of Port (Port Forward) to the destination application. However, for each type of application, a different method will be used.

Among the list of applications we have:

- **Client / server applications**

They work through a Web Tunnel and require the “Client” of the Server application for traffic through the WEB Tunnel.

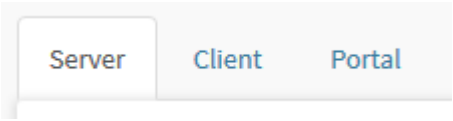
- **Remote access applications:**
  - *RDP* terminal;
  - *VNC terminal*;
  - *SSH terminal*.
- **Web Applications:** Use the Reverse Proxy feature to access the page server;
- **Network shares (*SMB*):** Requires the configuration of a “Storage Point” type “SMB” in BB NGFW, for the network sharing feature.

VPN SSL - Server tab

The BLOCKBIT NGFW Provides two models of VPN Tunnel type VPN implementations

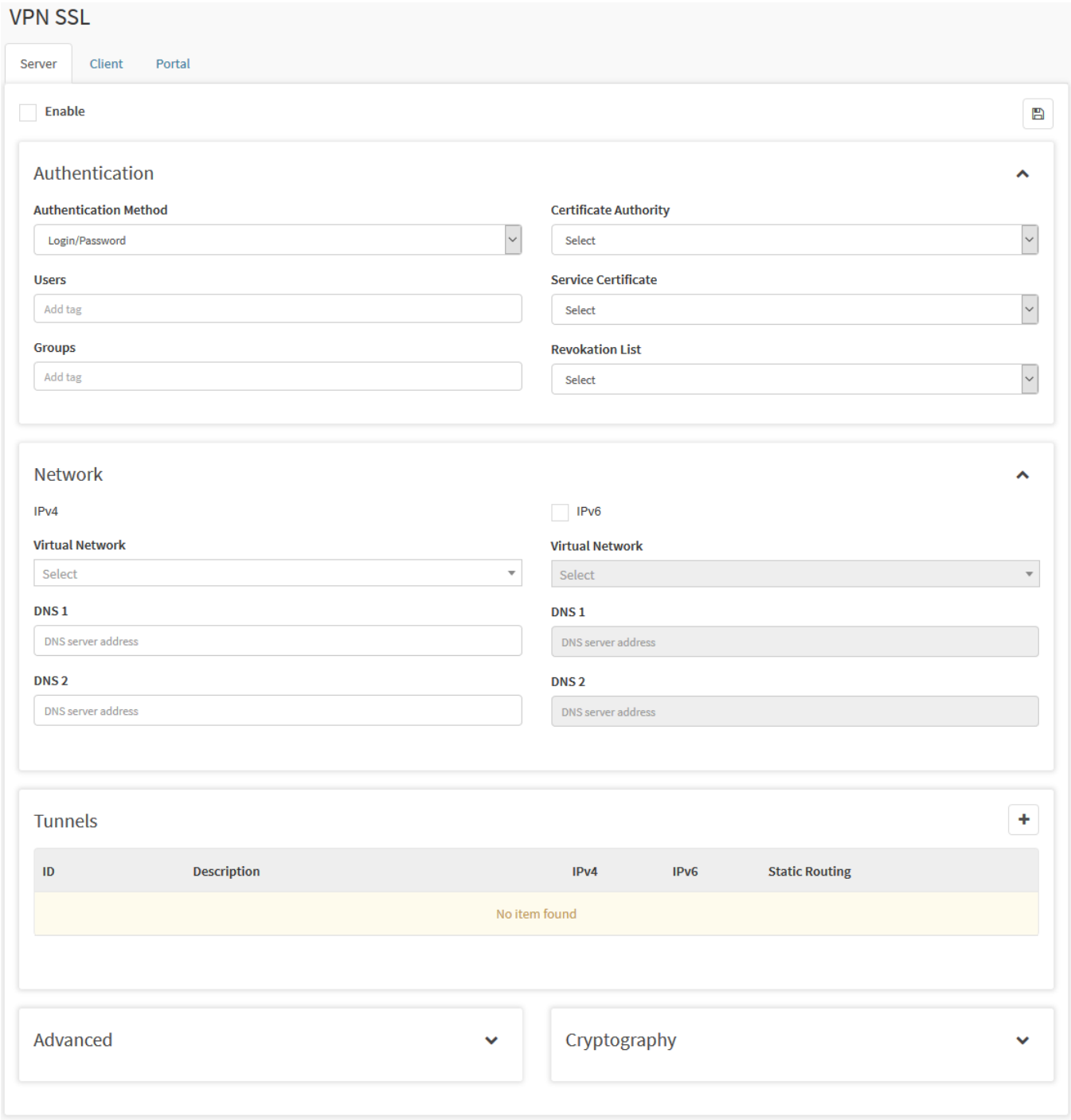
- Multiclients Server;
- Server Server (Site-to-Site).

To configure and enable VPN SSL Server, access the Server tab:



Servers tab

The screen below will appear:



VPN SSL - Servers

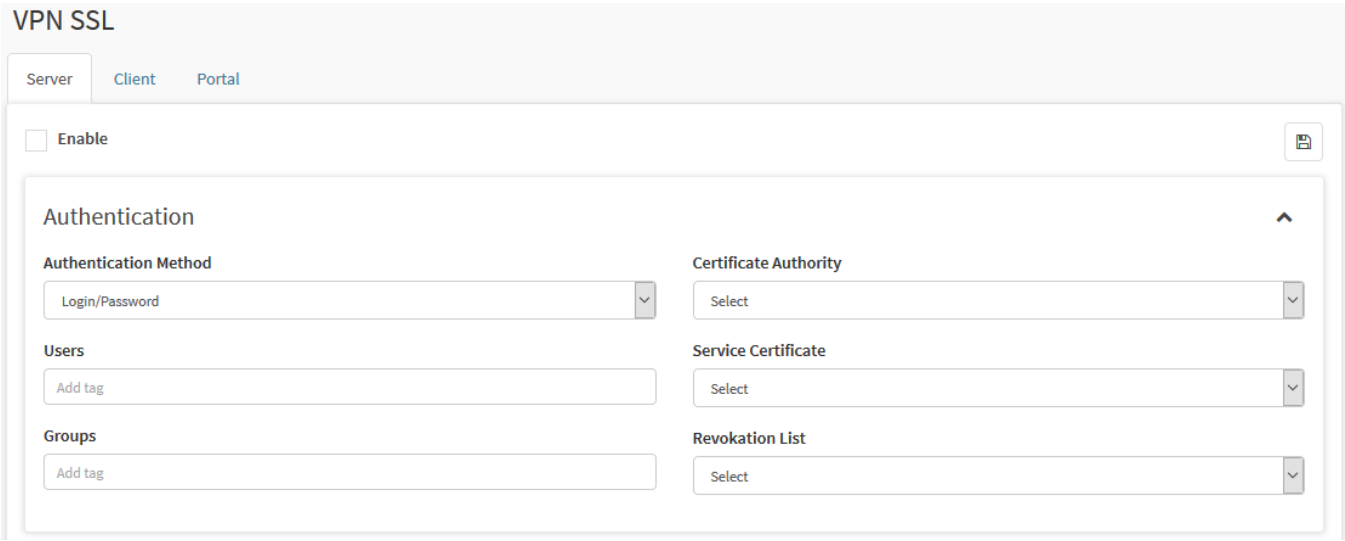
This screen consists of the following panels:

- *Authentication*;
- *Network*;
- *Tunnels*;
- *Advanced*;
- *Cryptography*.

Next we will analyze the components of this screen.

VPN SSL - Authentication

Below we will analyze each component of the Authentication panel:



VPN SSL Server – Authentication

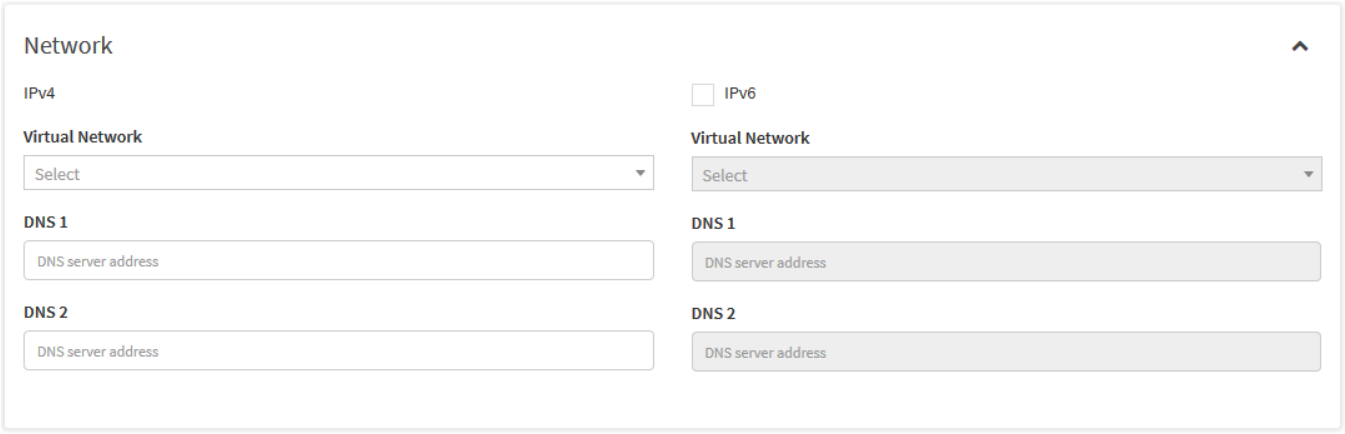
- ***Enable[ ]:*** *By checking this checkbox the SSL VPN will be enabled*;
- ***Authentication Method:*** *Selection of the authentication method. You can choose to select to use a "Login / Password" or a "Login / Password + User Certificate";*
- ***Users:*** Selection of "Users" for permission filters on SSL VPN client access*;*
- ***Groups:*** *Selection of "Groups" for permission filters on SSL VPN client access;*
- ***Certificate Authority:*** *Selection of the certifying entity [C.A.] responsible for validating the authenticity of the "C.S. - Service certificate "for authentication with SSL VPN client access. {Item opting for selecting the authentication method}*;
- ***Service Certificate:*** *Selection of the Digital Certificate used as an authentication method in the SSL VPN client access. {Item opting for selecting the authentication method}*;
- ***Revokation List:*** *Selection of the revoked certificate list to guarantee the exclusive use of valid digital certificates. {Optional item}*

In the Users and Groups fields, if the users or groups are not inserted, the setting will allow any connection to be made. To prevent from any user or group to connect, it is necessary to insert the allowed users or groups in these fields.

Next, we'll look at the *Network* panel.

VPN SSL - Network

Below we will analyze each component of the Network panel:



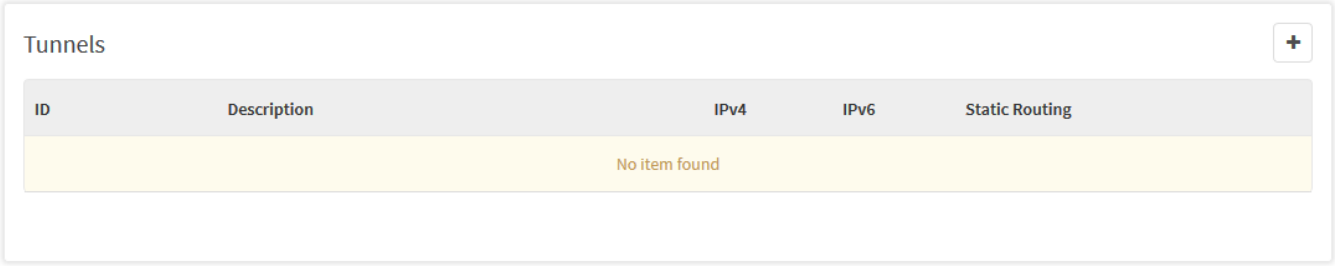
VPN SSL – Network

- ***IPv6[ ]:*** Determines whether the assignment will be for IPv6, selecting this field enables all fields on the right. This field is valid for both IPv4 and IPv6*;*
- ***Virtual Network:*** Defines the virtual network that will be used in the SSL VPN, the items that appear in this field are the address objects registered in *Addresses - Actions Menu - Create Object*. This field is valid for both IPv4 and IPv6;
- ***DNS 1:*** *Determines the address of the primary DNS server. This field is valid for both IPv4 and IPv6*;
- ***DNS 2:*** *Determines the address of the secondary DNS server. This field is valid for both IPv4 and IPv6.*

Next, we'll look at the *Tunnels* panel.

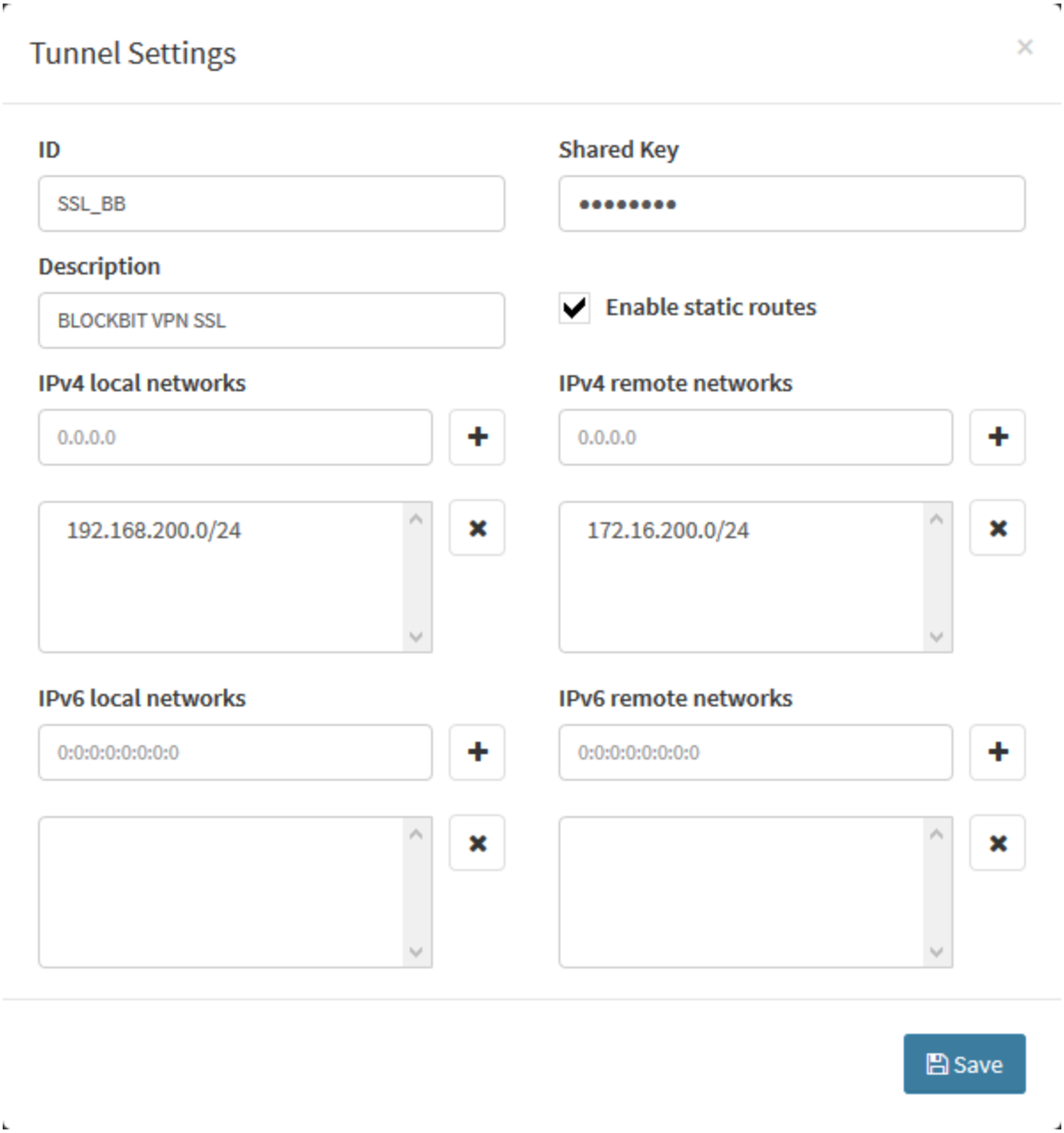
VPN SSL - Tunnels

Below we will analyze each component of the Tunnel panel:



VPN SSL Server – Tunnels

By clicking on the **[ ]** button, the screen below will be displayed.



VPN SSL Server – Tunnel Settings

- ***ID:*** *Local VPN endpoint identification method that will be used at the client endpoint to validate tunnel authentication. Ex.: SSL_BB*;
- ***Shared Key:*** *It is the shared key that will be used for authentication between the client and the server*;
- ***Description:*** *Inform the name of the tunnel. Ex .: BLOCKBIT VPN SSL*;
- ***Enable static routes[ ]:*** *With this option enabled when the tunnel is closed, the system sends routes automatically to networks that have been declared in the tunnel.*;
- ***IPv4 local networks:*** *Declaration of IPv4 network addresses / local subnet "not valid" of the VPN LOCAL site*. Click **[ ]** to add to the list or **[ ]** to remove the IPs already added. Ex.: *"192.168.200.0/24";*
- ***IPv4 remote networks:*** *Declaration of IPv4 network addresses / local subnet "not valid" of the Remote VPN site*. Ex.: *"172.16.200.0/24";*
- ***IPv6 local networks:*** *Declaration of IPv6 network addresses / local subnet "not valid" of the LOCAL VPN site*. Click **[ ]** to add to the list or **[ ]** to remove the IPs already added*;*
- ***IPv6 remote networks:*** *Declaration of IPv6 network addresses / local subnet "not valid" from the Remote VPN site.*

After that click on [Save] the screen below will be displayed.

VPN SSL Server - Tunnels settings

Next we will analyze the Advanced panel.

VPN SSL - Advanced

Below we will analyze each component of the Advanced panel:

VPN SSL Server – Advanced

- ***Compression [ ]:*** *Allows you to enable the Data Compression method. Enabling the compression method is mandatory to enable access to Blockbit Client*;

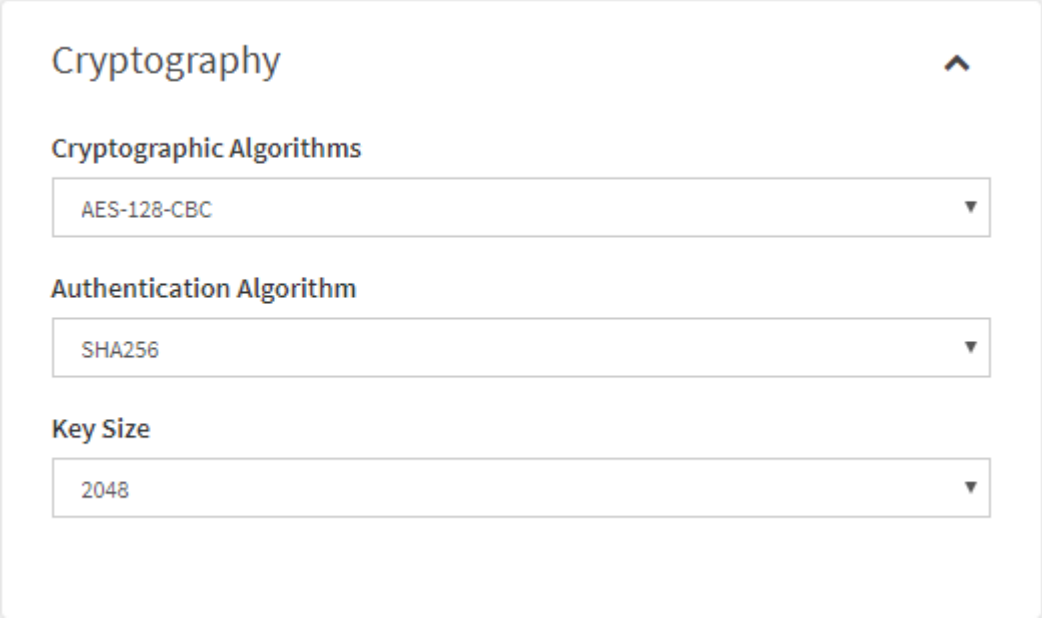
For more information about *Blockbit Client*, see this page.

- ***Key lifetime:*** *Determines the validity time of the successful negotiation key*;
- ***KeepAlive:*** *Determines the time to restart the tunnel N seconds without passing traffic through the tunnel*;
- ***Max Clients:*** *Determines the number of clients connected simultaneously*.

Next, we'll look at the *Cryptography* panel.

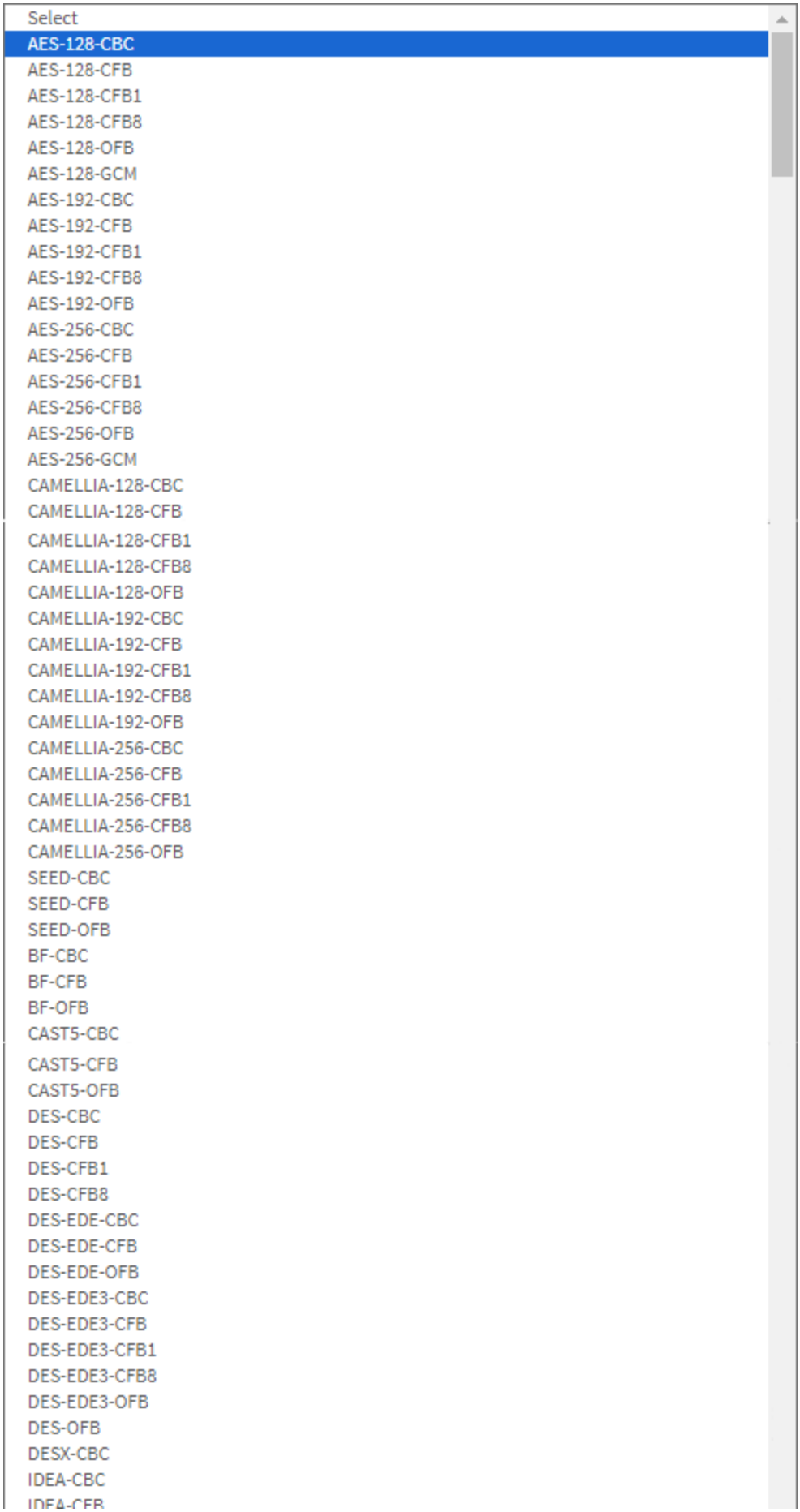
VPN SSL - Cryptography

Below we will analyze each component of the Cryptography panel:



VPN SSL Server – Cryptography

- ***Cryptographic Algorithms:*** *Determines the encryption algorithm for the tunnel. Ex.: AES-128-CBC;*
- ***Authentication Algorithm:*** *Determines the authentication algorithm used by the tunnel. Ex.: SHA254;*
- ***Key Size:*** *Determines the size of the key that will be used in the tunnel. Ex .: 2048*.


Select
AES-128-CBC
AES-128-CFB
AES-128-CFB1
AES-128-CFB8
AES-128-OFB
AES-128-GCM
AES-192-CBC
AES-192-CFB
AES-192-CFB1
AES-192-CFB8
AES-192-OFB
AES-256-CBC
AES-256-CFB
AES-256-CFB1
AES-256-CFB8
AES-256-OFB
AES-256-GCM
CAMELLIA-128-CBC
CAMELLIA-128-CFB
CAMELLIA-128-CFB1
CAMELLIA-128-CFB8
CAMELLIA-128-OFB
CAMELLIA-192-CBC
CAMELLIA-192-CFB
CAMELLIA-192-CFB1
CAMELLIA-192-CFB8
CAMELLIA-192-OFB
CAMELLIA-256-CBC
CAMELLIA-256-CFB
CAMELLIA-256-CFB1
CAMELLIA-256-CFB8
CAMELLIA-256-OFB
SEED-CBC
SEED-CFB
SEED-OFB
BF-CBC
BF-CFB
BF-OFB
CAST5-CBC
CAST5-CFB
CAST5-OFB
DES-CBC
DES-CFB
DES-CFB1
DES-CFB8
DES-EDE-CBC
DES-EDE-CFB
DES-EDE-OFB
DES-EDE3-CBC
DES-EDE3-CFB
DES-EDE3-CFB1
DES-EDE3-CFB8
DES-EDE3-OFB
DES-OFB
DESX-CBC
IDEA-CBC

List of Cryptographic Algorithms

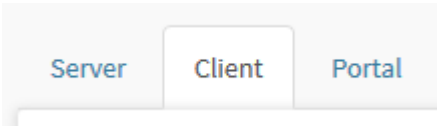
When finishing the settings, click **[**  **]** to save the changes.

After saving, for the settings to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: NGFW - Command queue.

After performing these procedures the SSL VPN will have been successfully configured.

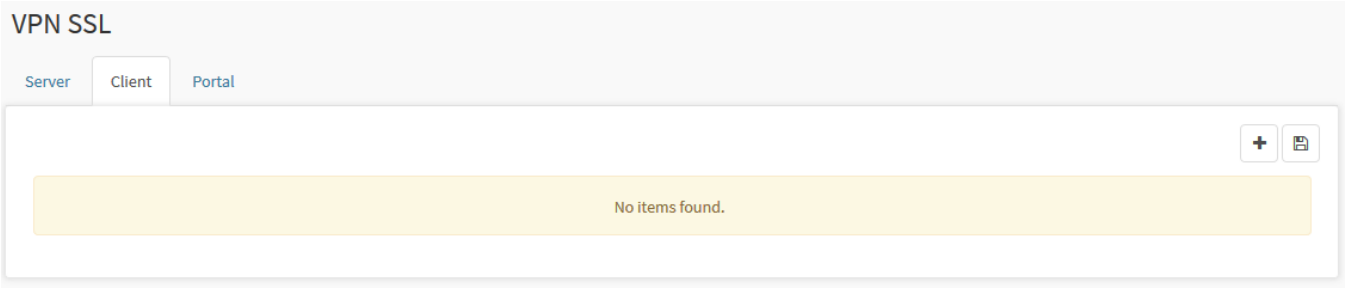
VPN SSL - Client tab

To configure and enable SSL tunnels, access the Client tab:



Client tab

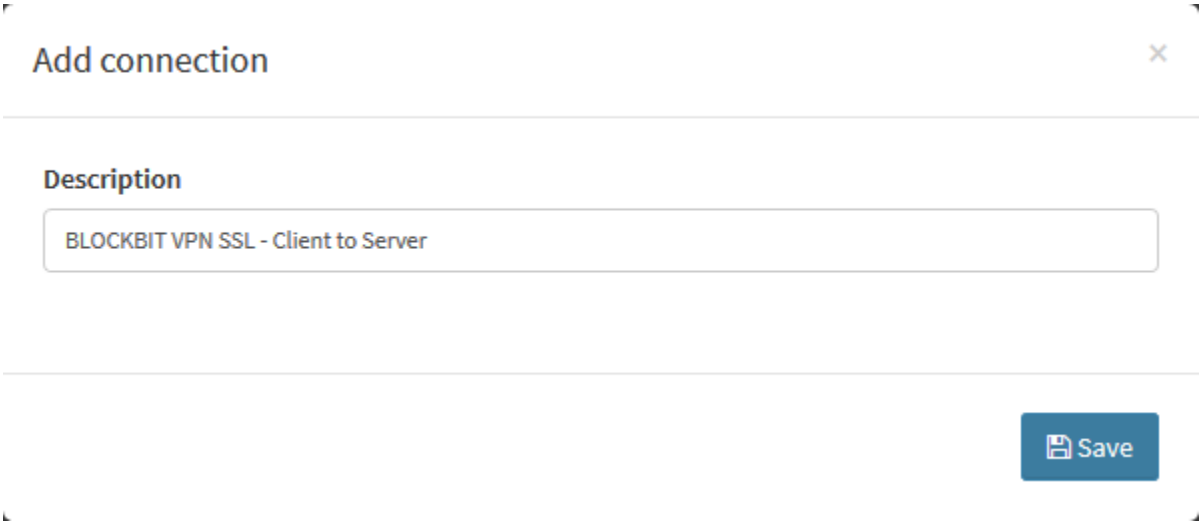
The screen below will appear:



VPN SSL - Client

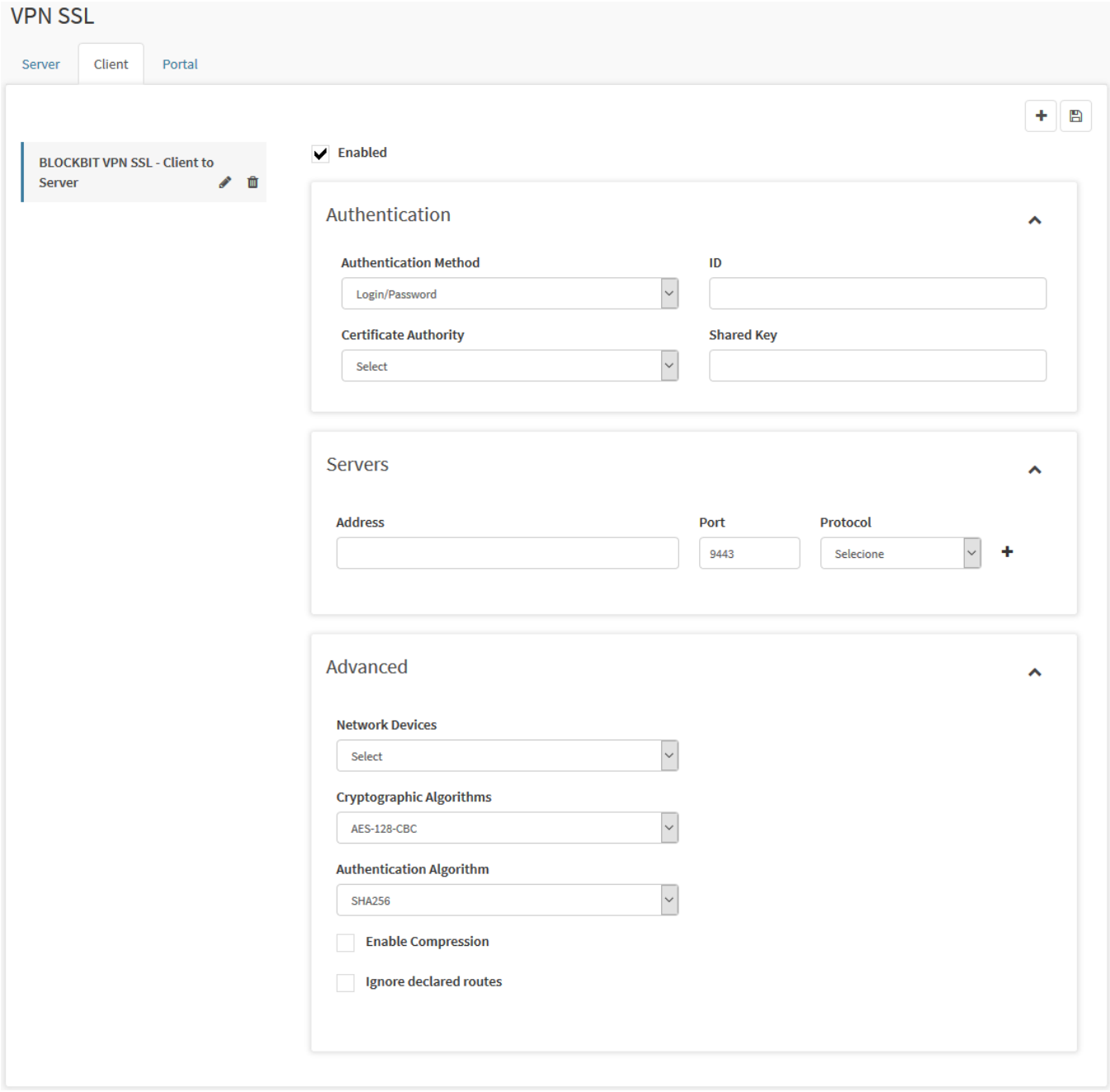
Next we will analyze the components of this screen:

By clicking on the **[**  **]** button, the screen below will be displayed.



VPN SSL Client – Description

After that click on **[**  **]** and the screen below will be displayed.



VPN SSL Client - Settings

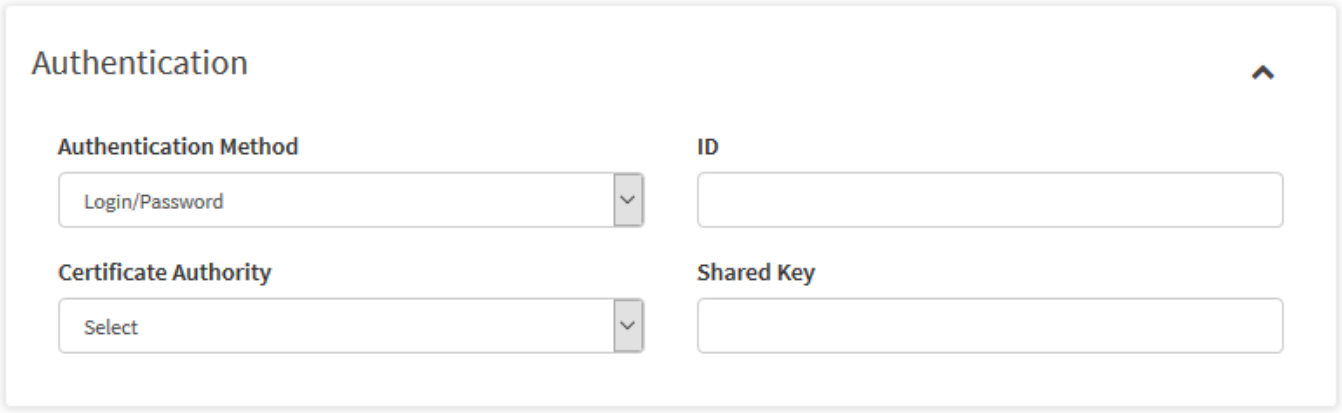
This screen is composed of the following panels:

- *Authentication*;
- *Servers*;
- *Advanced*.

Below we will analyze each of these panels in detail.

Client - Authentication Panel

Next, we'll review each component of the Authentication panel:



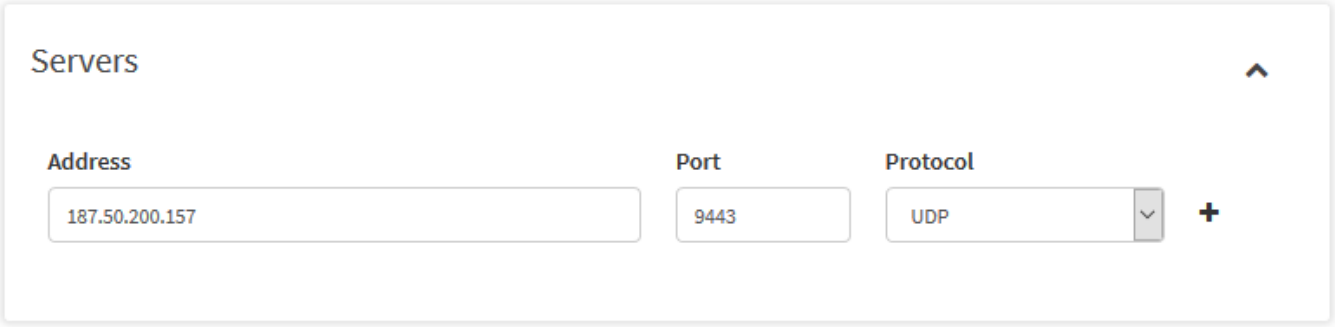
VPN SSL Client - Authentication

- ***Authentication Method:*** *Selection of the authentication method. You can choose to select to use a "Login / Password" or a "Login / Password + User Certificate]";*
- ***Certificate Authority:*** *Selection of the certifying entity [C.A] responsible for validating the authenticity of the "C.S. - Service certificate "for authentication with SSL VPN client access. {Item opting for selecting the authentication method}*;
- ***Service Certificate:*** *Selection of the Digital Certificate used as an authentication method in the SSL VPN client access. {Item opting for selecting the authentication method}*;
- ***ID:*** *Inform the ID that was defined in the Server configuration. Eg SSL_BB*;
- ***Shared Key:*** Informar a *shared key* que foi definido na configuração do *Server*.

A seguir analisaremos o painel *Servers*.

Client - Servers Panel

Next, we'll look at each component of the Servers panel:



VPN SSL Client – Servers

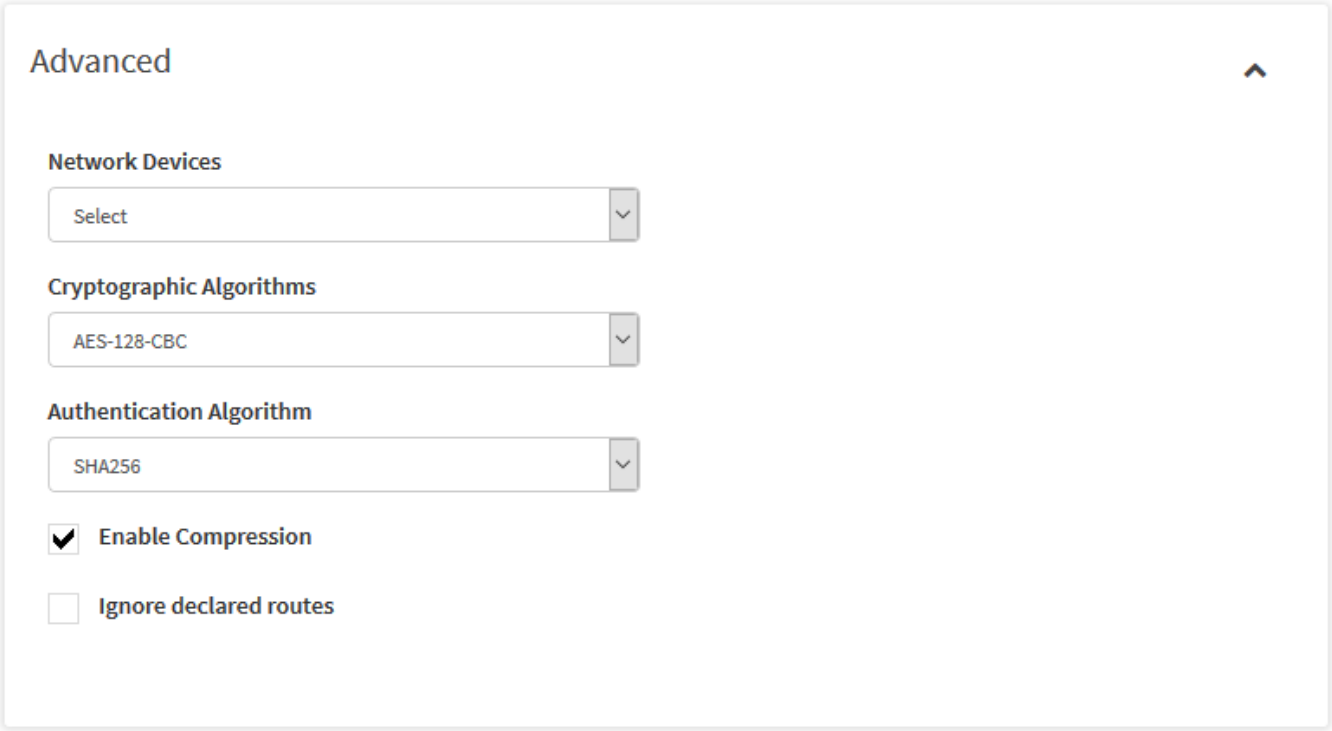
- ***Address:*** *Set the IP address of the SSL VPN Server. Ex.: 187.50.200.157;*
- ***Port:*** *Set the connection port for the SSL VPN Server. Ex.: 9443;*
- **Protocol:** Define the communication protocol with the SSL VPN Server. Ex.: UDP.

By clicking on the **[+]** button, it is possible to add more server addresses if the SSL VPN server has more than one internet link to balance VPN tunnel.

Next we will analyze the *Advanced* panel.

Client - Advanced Panel

Below we will analyze each component of the Advanced panel:



VPN SSL Client – Advanced

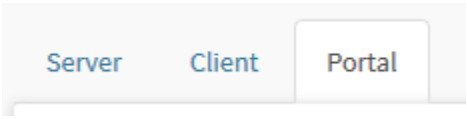
- ***Network Devices:*** *This option defines which internet link the tunnel will be configured on, if not selected, it will be closed via the default gateway link;*
- ***Cryptographic Algorithms:*** *Determines the encryption algorithm for the tunnel that must be the same as that configured on the SSL VPN Server. Ex.: AES-128-CBC*;
- ***Authentication Algorithm:*** *Determines the authentication algorithm used by the tunnel that must be the same as that configured on the SSL VPN Server. Ex.: SHA256;*
- ***Enable Compression*** **[ ]***: Allows you to enable the data compression method;*
- ***Ignore declared routes:*** *This option ignores routes that will be sent by the server.*

When finishing the settings, click **[ ]** to save the changes.

After saving, for the settings to take effect it will be necessary to access the command queue **[ ]** and apply the changes made. For more information on the command queue access the page: NGFW - Command queue.

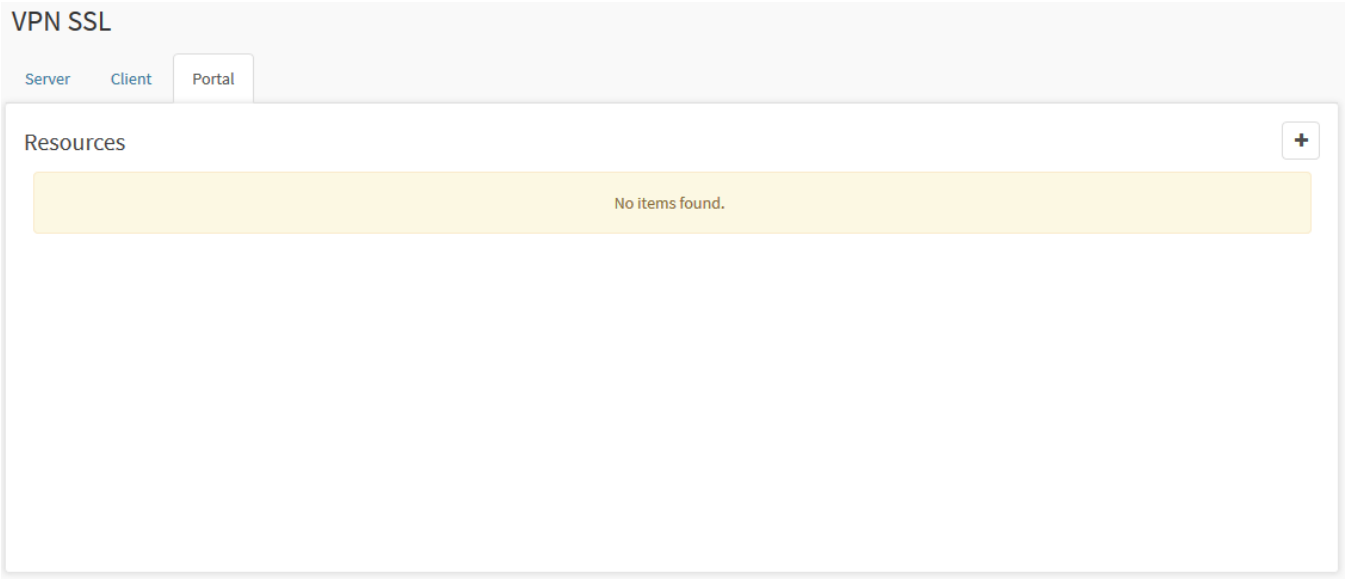
VPN SSL - Portal tab

For configuration, access the Portal tab:



Portal tab

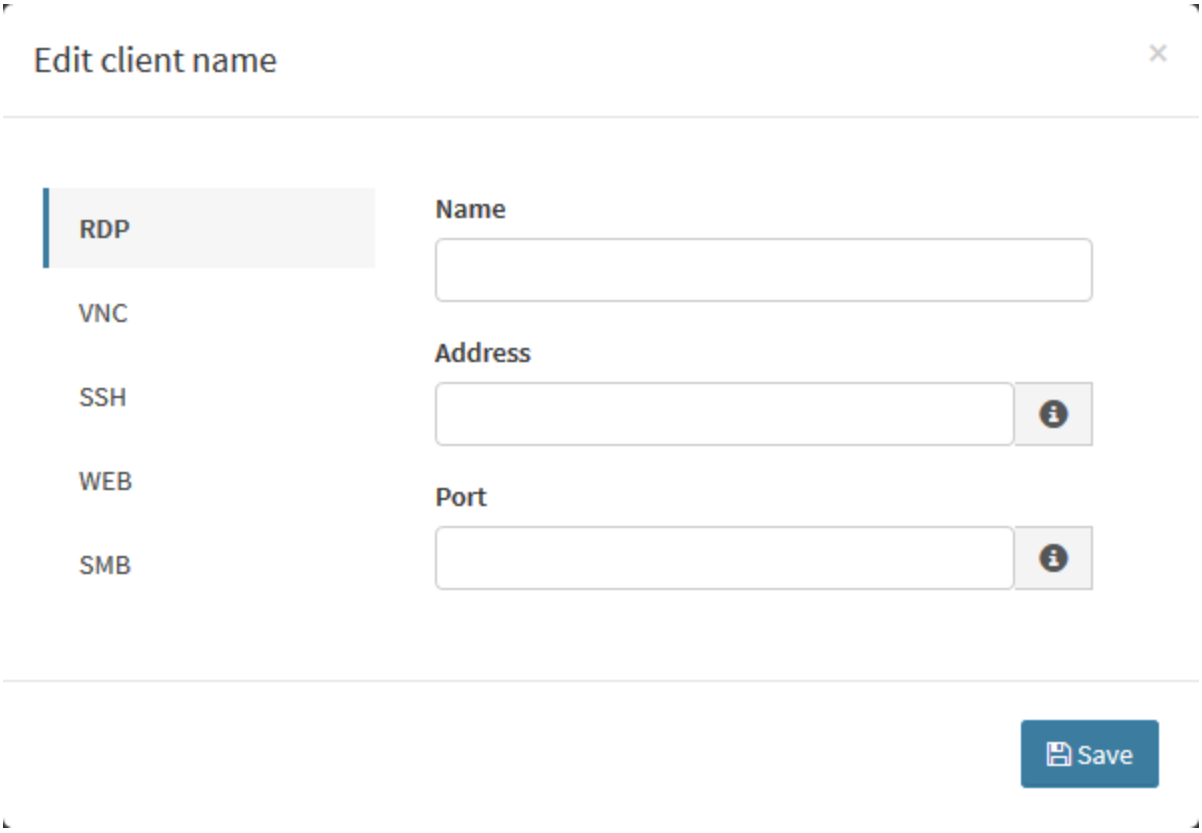
The screen below will appear:



VPN SSL - Portal

Next we will analyze the components of this screen:

By clicking on the **[**  **]** button, the screen below will be displayed.



VPN SSL Portal – Resource

Configure those to be made available and define your access policies respectively, defining which “users / groups” will have access to each application in your network.

This window allows the following configuration possibilities:

- *RDP*;
- *VNC*;
- *SSH*;
- *WEB*;
- *SMB*.

Next, we will analyze each of these options in detail.

Portal - RDP

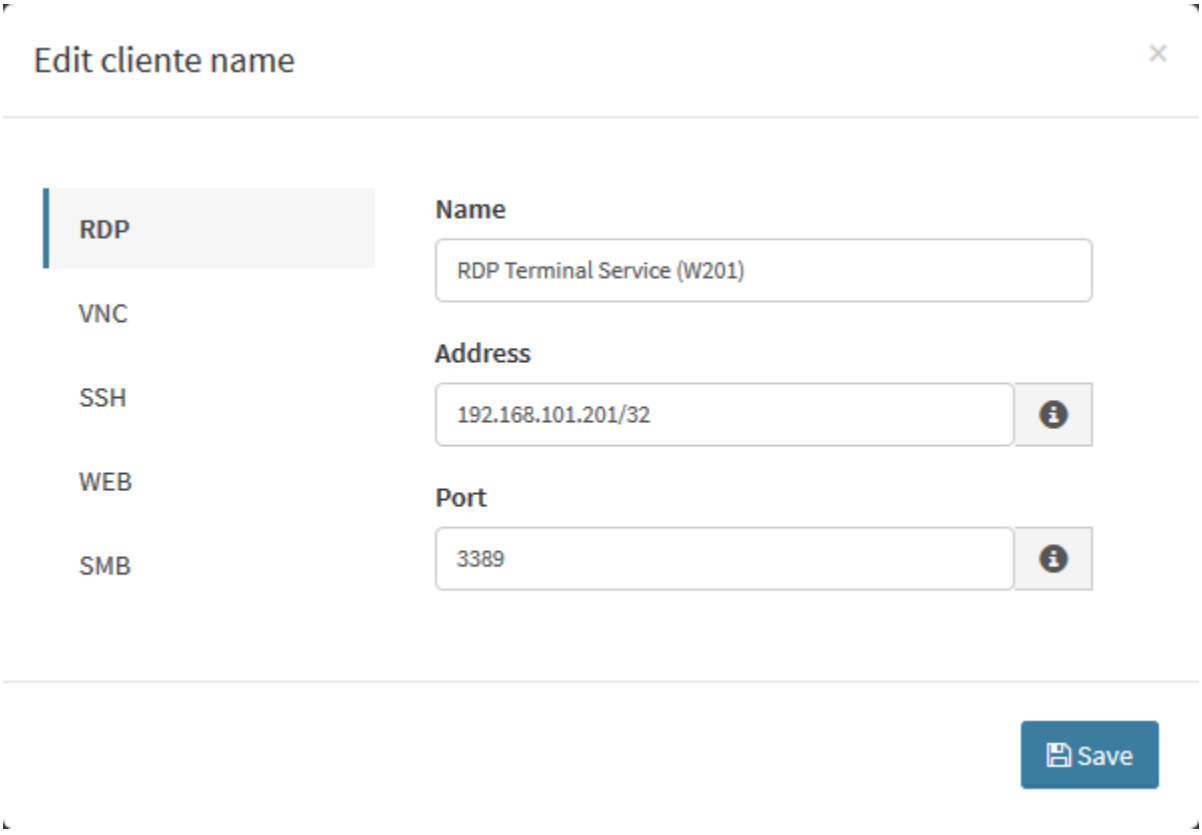
Configure the form according to the specifications for connection to a “Remote Desktop” application.

Let's exemplify by configuring access to the MS-Terminal Service remote desktop service.

VPN SSL - Example 1

Application	***Terminal RDesktop* (*MSTSC*).**
Local IP	192.168.101.201/32
Application port	3389
Description	*RDP Terminal Service* (W201)
Permission (Can be applied by user or groups).	vpn.sup@bbuniversity

Next we will analyze how to make these settings:



VPN SSL - RDP

- ***Authentication Method:*** *Selection of the authentication method. You can choose to select to use a “Login / Password” or a “Login / Password + User Certificate]”;*
- ***Certificate Authority:*** *Selection of the certifying entity [C.A] responsible for validating the authenticity of the “C.S. - Service certificate ”for authentication with SSL VPN client access. {Item opting for selecting the authentication method}*;
- ***Service Certificate:*** *Selection of the Digital Certificate used as an authentication method in the SSL VPN client access. {Item opting for selecting the authentication method}*;

- ***ID:*** *Inform the ID that was defined in the Server configuration. Eg SSL_BB*;
- ***Shared Key:*** *Inform the shared key that was defined in the Server configuration*.

Next, we'll look at how to add *VNC* access.

Portal - VNC

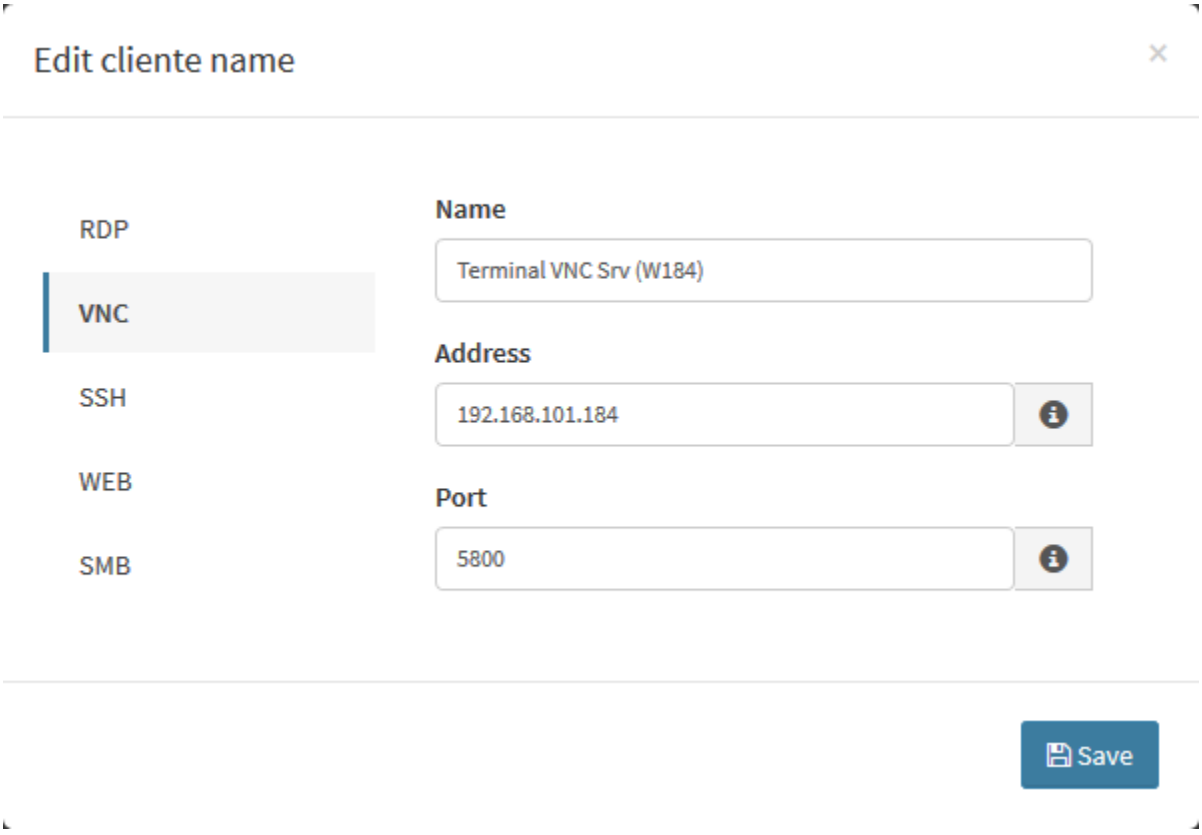
Configure the form according to the specifications for connecting to a remote access application.

Let's exemplify the configuring access to the VNC remote desktop service.

VPN SSL - Example 2

Application	***Terminal VNC RDesktop***
Local IP	192.168.101.184/32
Application port	5800
Description	*Terminal VNC Srv (W184)*
Permission (Can be applied by user or groups).	vpn.sup@bbuniversity.com

Next we will analyze how to make these settings:



VPN SSL - VNC

- ***Name*:** Determines the access' name. Ex.: VNC Srv Terminal (W184);
- ***Address*:** Determines the access' IP address. Ex.: 192.168.101.184;
- ***Port*:** Determines the port to be used. Ex .: 5800.

Next, we'll look at how to set up SSH access.

Portal - SSH

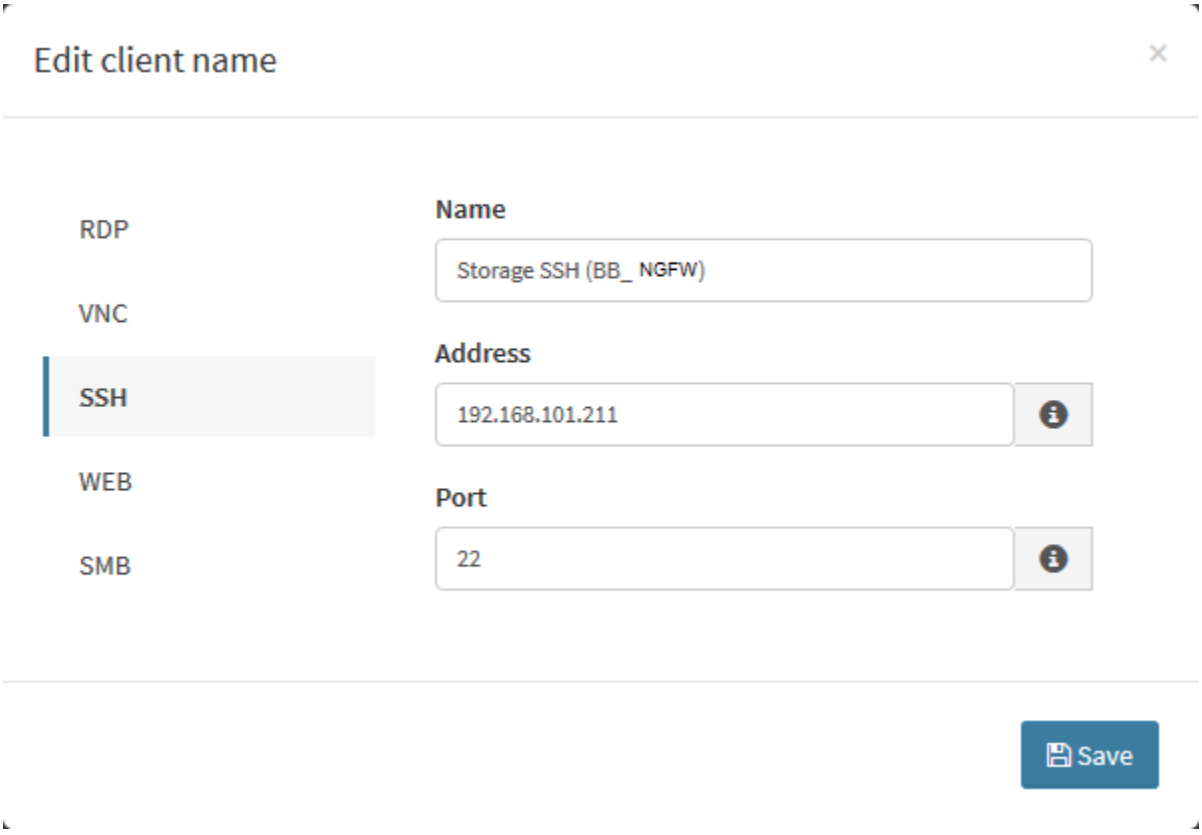
Configure the form according to the specifications for connection to a “Remote SSH” application.

Let's exemplify configuring access to the SSH Server - Storage Backup BLOCKBIT - Remote Desktop.

VPN SSL - Example 3

Application	**Terminal *SSH***
Local IP	192.168.101.211/32
Application port	22
Description	*Storage SSH* (BB-NGFW)
Permission (Can be applied by user or groups).	vpn.sup@bbuniversity

Next we will analyze how to make these settings:



VPN SSL - SSH

- ***Name*:** Determines the name that the access will have. Ex.: *Storage SSH (BB_NGFW)*;
- ***Address*:** Determines the access IP address. Ex.: 192.168.101.211;
- ***Port*:** Determines the port to be used. Ex.: 22;

Next we will analyze how to configure access to the Web Application.

Portal - WEB

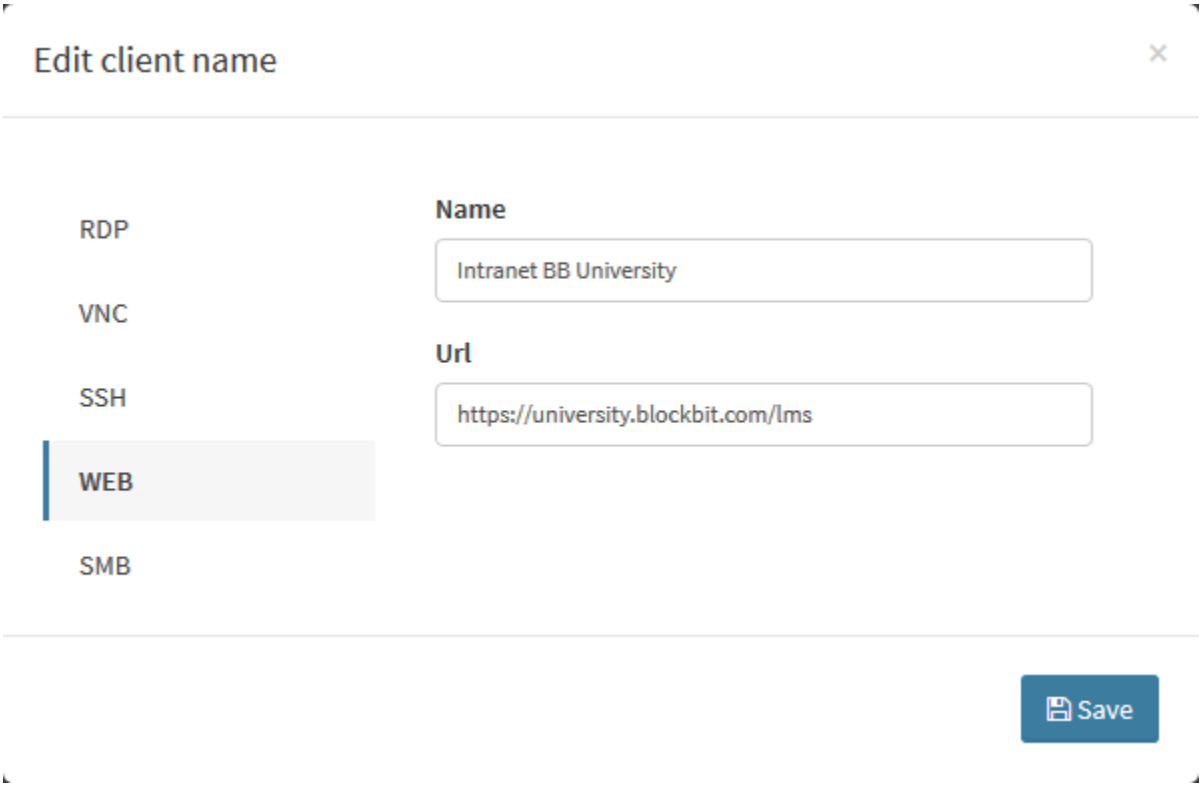
Configure the form according to the specifications for connection to a “WEB” application.

Let's exemplify the configuration of access to an internal WEB application (Intranet).

VPN SSL - Example 4

Application	Local WEB Application - Intranet
URL address	http://intranet.bbuniversity
Local Port (Random high / or user-defined door).	36288
Description	Intranet BB University
Permission (Can be applied by user or groups).	all@bbuniversity

Next we will analyze how to make these settings:



VPN SSL - WEB

- ***Name*:** Determines the name that the access will have. Ex.: BB University Intranet;
- ***Url*:** Determines the address to be used. Ex.: https://university.blockbit.com/lms.

Next, we'll look at how to set up access to the *SMB*.

Portal - SMB

Configure the form according to the specifications for connecting to an “SMB” sharing service.

Let's exemplify the configuration of access to SMB network sharing resources.

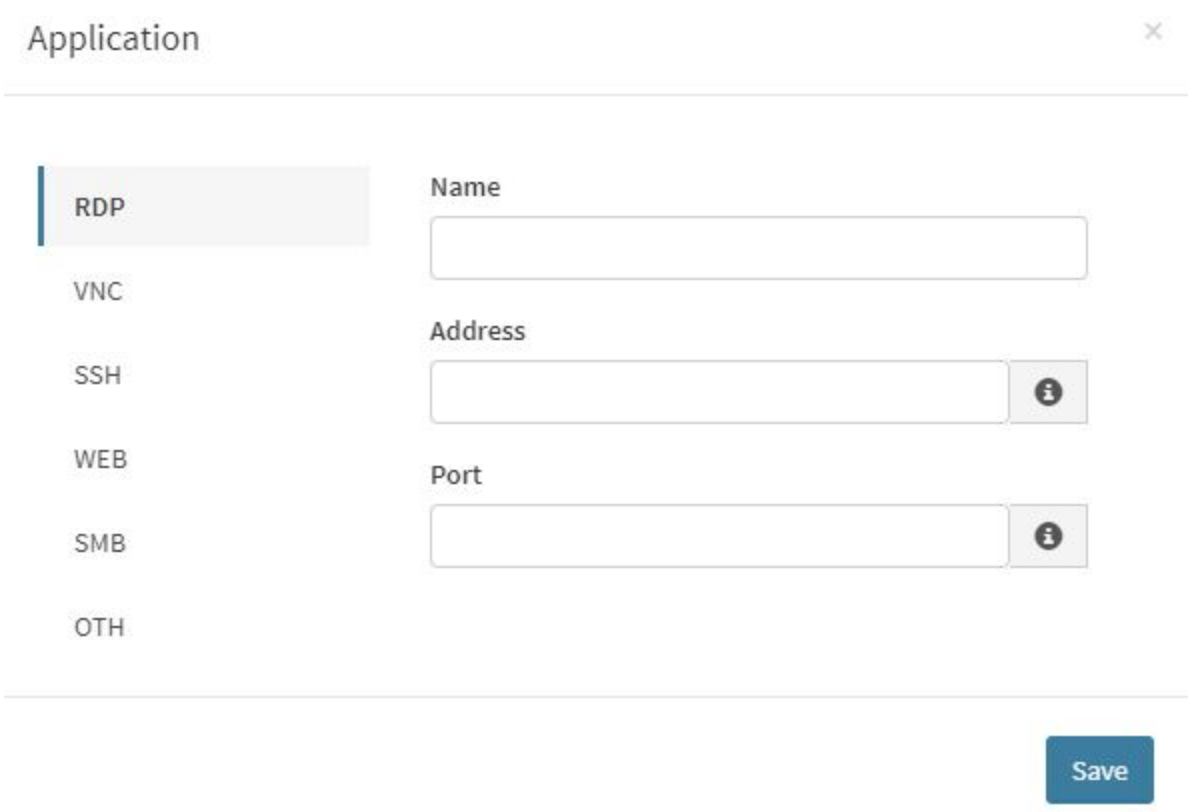
VPN SSL - Example 5

Application	Shared data area (SMB)
SMB Sharing *(Name of the share defined by the OS).*	*SMB - AD*
Description	NGFW Docs
Permission (Can be applyied per user or groups).	vpn.sup@bbuniversity.com

Next we will analyze how to make these settings:

Before configuring the SSL VPN Portal, you need to create an SMB storage in Settings System Storage. For more information see SMB Storage..

In Services VPN SSL Portal, click on [+] add. The following screen will appear:

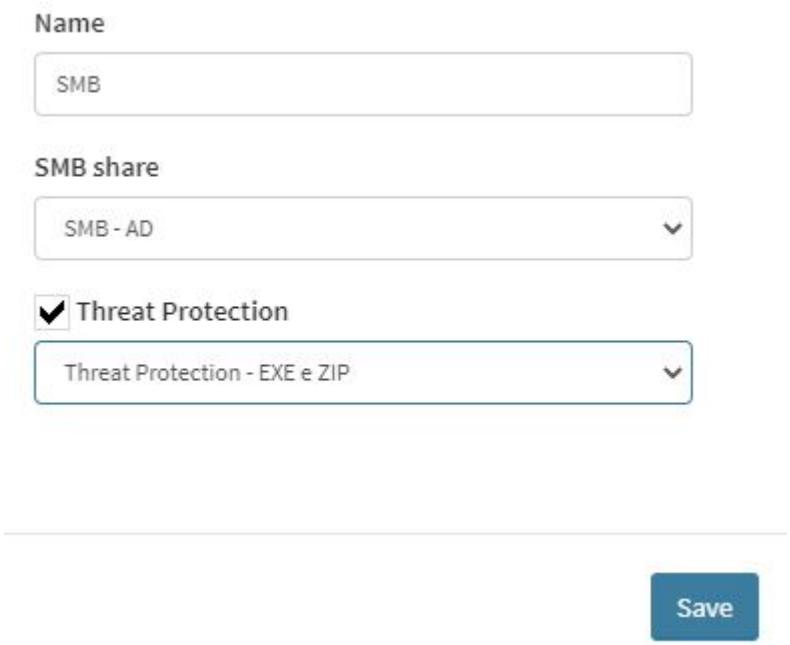


VPN SSL - Portal - Add

Select the SMB application.

VPN SSL - Portal - Add - SMB

Fill in all the fields.

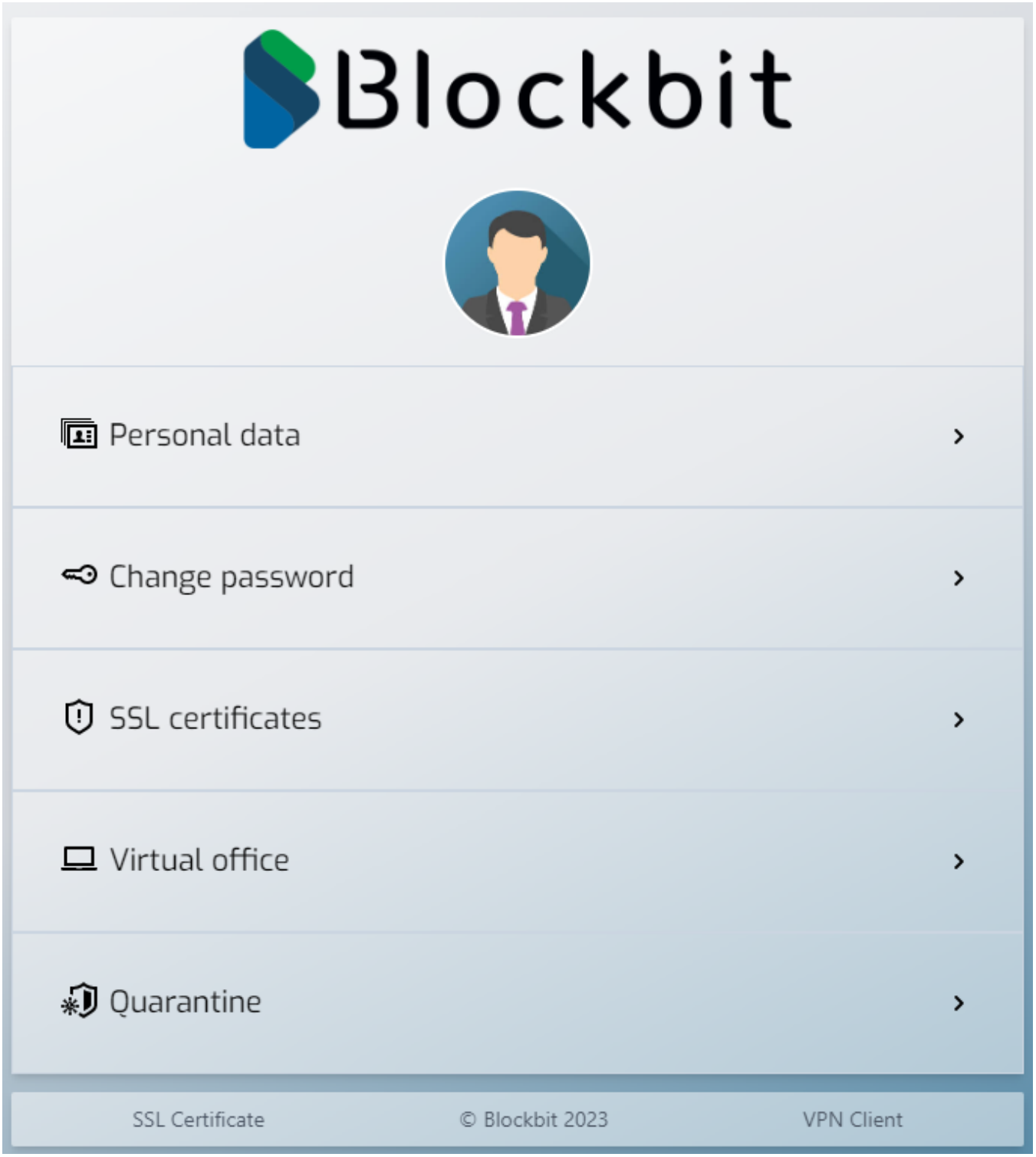


VPN SSL - Portal - Add - SMB

- ***Name*:** Determines the name that the access will have. Ex.: *Storage Blockbit*;
- ***SMB share*:** Determines the name the share will have (check the link below to check how to create an *SMB Storage*). Ex.: *NGFW Document*.
- **Threat Protection:** Determines the threat protection analysis by the ATP service engine. Ex.: Enable ou Disable.
- ***Select Profile:*** After selecting the option to enable the protection against spywares and viruses, the *Advanced Threat Protection*, select a previously created ATP profile (To know more about ATP profiles, click here).

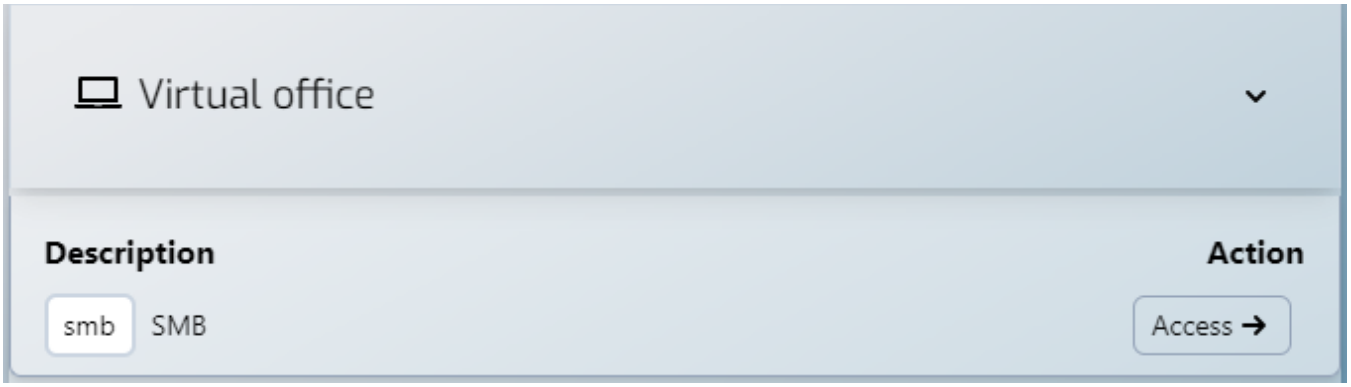
It is necessary to enable the Threat Protection service when creating the SMB type application. Files will only be directed for analysis if a Threat Protection profile is selected.
It is not possible to save the setting without enabling the Threat Protection checkbox.

Access the Authentication Portal (Captive Portal).



Captive Portal

Go to Virtual Office Access



Virtual Office

When uploading/downloading a file, if the file is from the maximum extent and size allowed by the ATP profile, redirect it to the ATP verification, which is similar to the Web Filter's, and validate the block screen.

Name	Tipo	Tamanho	Data	Ação
NovaPasta	-	-	31/12/1969 19:30	
ChromeSetup.exe		1,36 MB	03/10/2022 18:23	
Hardware.Blockbit.jpg		7,21 KB	20/12/2022 09:43	
VirtualBox-7.0.6-155176-OSX.dmg		126,81 MB	30/01/2023 07:09	
VirtualBox-7.0.6-155176-Win.exe		105,34 MB	30/01/2023 07:08	
debian-mac-11.6.0-amd64-netinst.iso		385 MB	30/01/2023 07:07	
eicar_com.zip		184 B	01/11/2022 09:03	
eicarcom2.zip		132 B	08/02/2023 10:43	
node-v16.16.0-x64.msi		27,25 MB	28/01/2023 14:49	
odilon22222		49,3 KB	20/12/2022 09:44	
oga-akerfirewall-NGFW_7.1.1-pt.pdf		32,21 MB	28/01/2023 14:18	
putty.exe		1,57 MB	01/11/2022 09:04	
utweb_installer.exe		1,71 MB	30/01/2023 07:13	

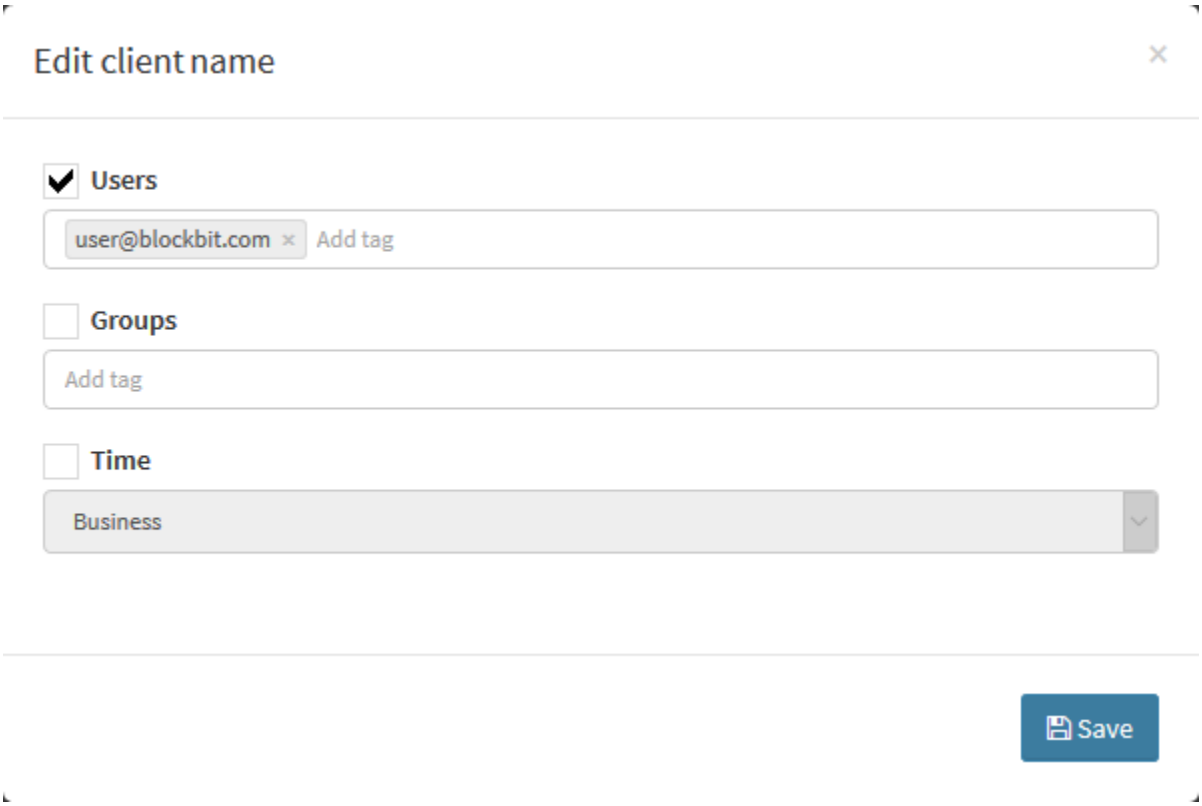
Next, we'll look at management and settings permissions.

Portal - Setting and Managing Permissions

This interface allows you to "Add", "Edit", "Remove" VPN SSL applications and manage the access permissions of each registered application.

VPN SSL - Portal

Now we can Enable the permissions and select “Users / Groups” and “Timetable” with permission to access the respective applications according to the defined policies. Click on **[ ]** for each application in the list and select the "Users" or "Groups" with permission on the application according to the definitions of the applied policies.



After making the settings, click ***[Save]***.

Portal - SSL VPN requirements

For SSL VPN to manage a secure connection, we first need to make sure that we meet some requirements and then make the service available to the network.

1. Define available network applications / applications.

- Web Applications. Ex.: “Intranet Portal Application”;
- Remote access application. Ex.: “SSH terminal; VNC terminal; Terminal Remote Desktop ”;
- *SMB network shares. Ex.: “Common file server area”.*

2. Survey the IP addresses and service ports of each application to pre-configure the objects **[IP address]** and **[Services]**;

3. For SMB sharing. Requires configuring a storage point. Item **[Settings] [System] [Storage]**;

4. Establish “Access Policies” for each application that will be made available;

- Resources (Applications);
- List of “Users / Groups” with right of access.

5. Enable firewall permission for the SSL Portal VPN service “port 922 / TCP” for the respective “network zone (s)” of the address (es) with permission;

6. Go to **[Services] [Firewall] [Zone Protection]** tab;

VPN SSL - Establishing SSL Portal VPN Access

Among the access policies for accessing network resources, the administrator can define that communications with some of these services are only available through a VPN.

One of the means for accessing VPN to network applications is through access to the Authentication portal. Only the portal allows access to applications in a safe and reliable way, as it establishes encrypted and independent accesses, regardless of the “LAN” network classes; "DMZ"; or “WAN”.

To establish communication with the “Virtual Office”, the user must first access the authentication portal.

Once authenticated, if you have permission to access any application, the user will have access to Virtual Office through a "Bookmark" with the list of applications available for their access.

Accessing the authentication portal

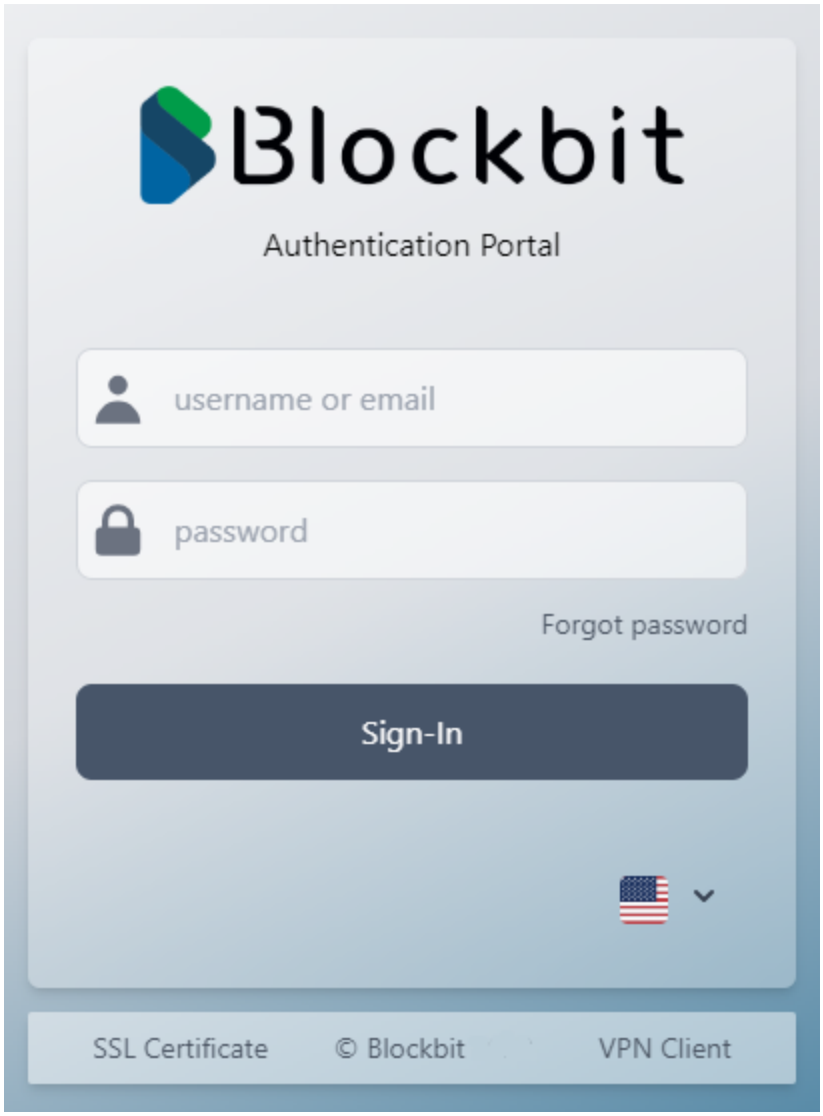
Virtual Office is an integral part of the “Authentication Portal” and its main objective is to offer through a browser. Ex: MS-Edge, Google Chrome or Mozilla Firefox, run "Applications" and "Network resources" over a secure connection, the VPN SSL Portal.

When logging out of the user on the authentication portal, or when the connection is dropped, access to the WEB applications, they have a maximum time limit of up to 5 minutes, after that time, it is necessary to log in again.

The other way is through the authentication portal, it is possible to access it through two modes:

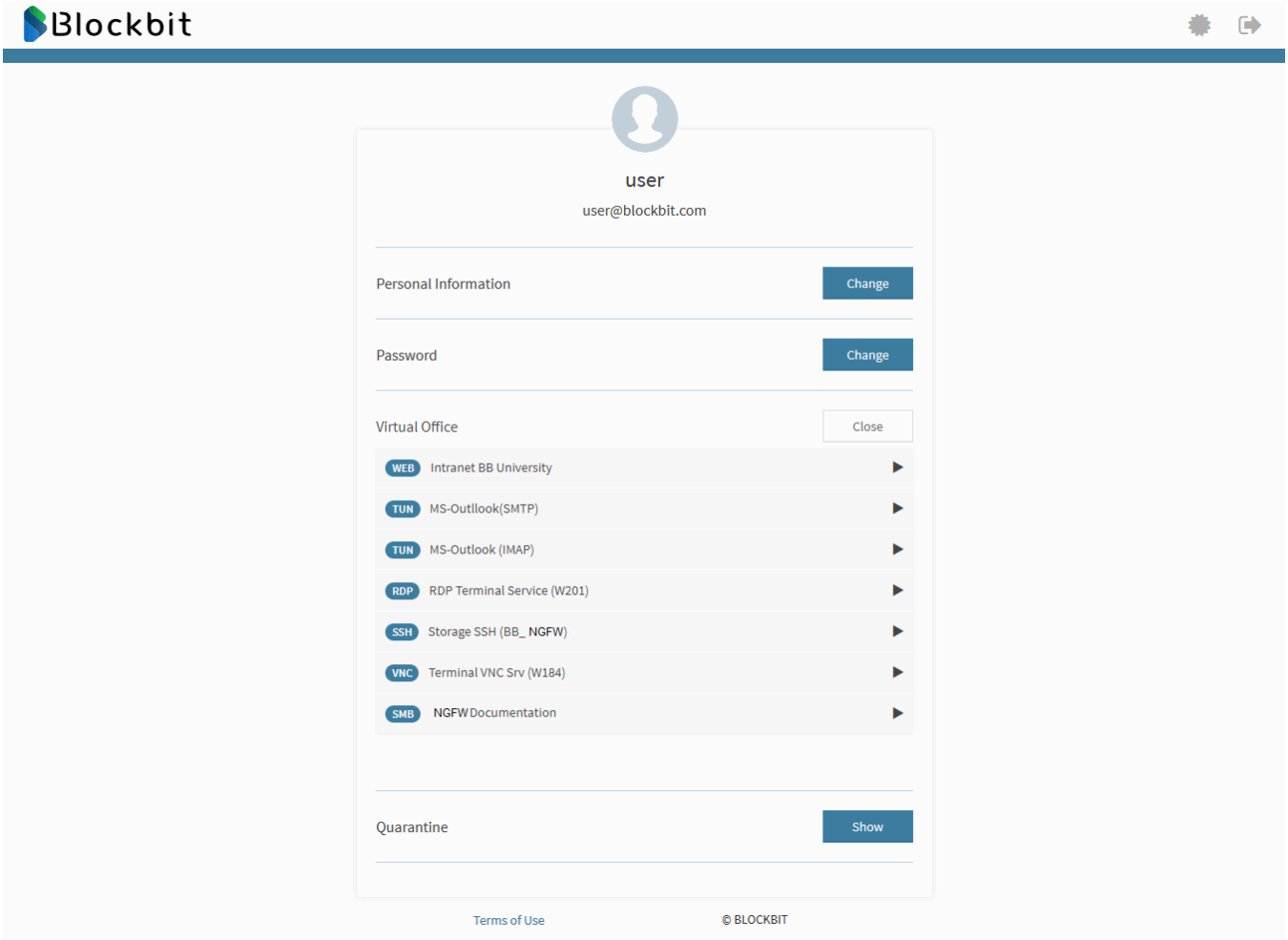
- Your domain host with port 9803 (Ex.: https://host.seudominio.com:9803);
- IP address of your UTM with port 9803 (Ex.: https://172.16.102.130:9803).

We will make an access using a user member of a group with permissions to access VPN SSL Portal.



VPN SSL – Authentication Portal

When you click [Login] the following screen will be displayed:

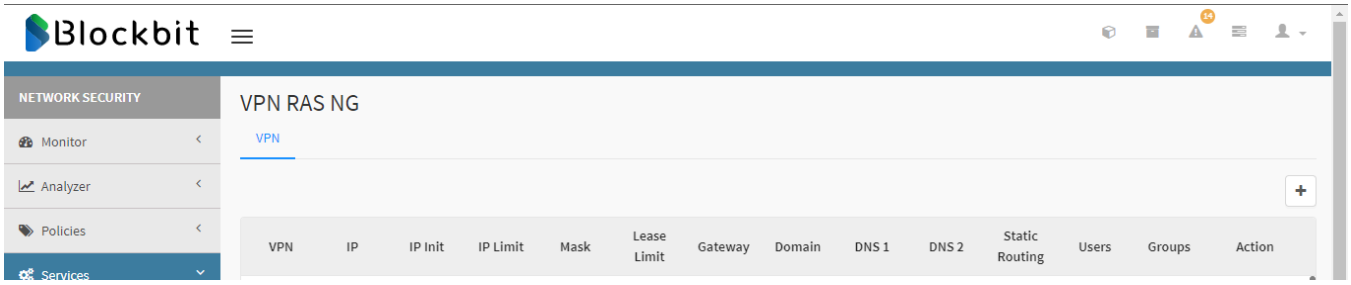


VPN SSL – User Portal

To access any of the applications just click on the icon [▶].

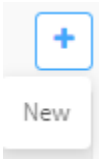
UTM - Services - NG VPN

The NG VPN allows the creation of VPN HUBs through the filling of a form containing the necessary information for the creation of a VPN tunnel.



NG VPN Panel

To configure a new NG VPN's HUB, click the [] button:



New NG VPN HUB creation

The NG VPN's HUBs creation form is divided into 3 sections:

Create

Virtual DHCP Server Setting

VPN's Name

Same names are not allowed

Virtual Host IP Address

Distrbutes IP Address Start

Distrbutes IP Address Limit

Subnet Mask

Lease Limit (seconds)

Options Apllied to Clients (optional)

DNS Server Address 1

DNS Server Address 2

Default Gateway Address

Domain Name

Static Routing

192.168.0.1/255.255.255.0/192.168.0.222

Inserting users and user groups

Users

Please select

Groups

Please select

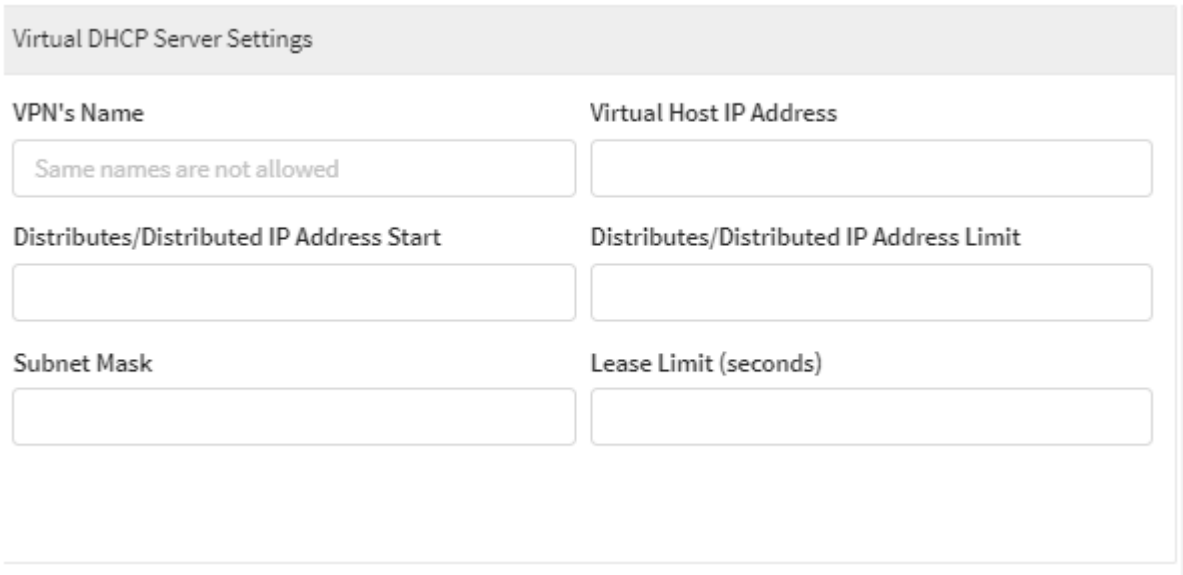
Cancel

Save

NG VPN HUBs creation form

Next, we will analyze each section of the form.

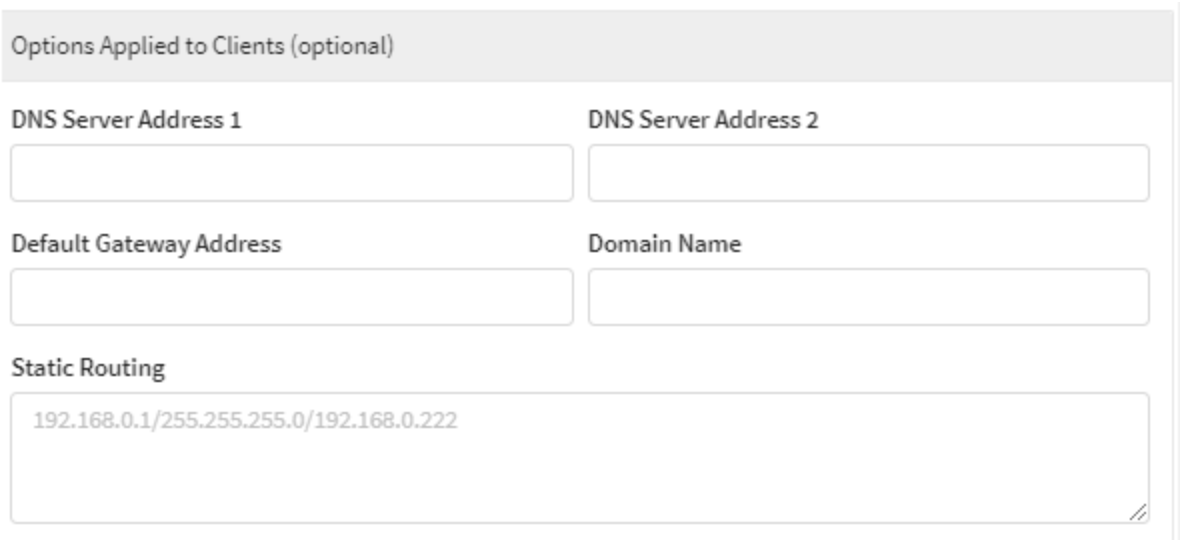
Virtual DHCP Server Settings



NG VPN form

- ***VPN's Name:*** Insert the name of the new NG VPN HUB. Note that it must be different from existing ones.
- ***Virtual Host IP Address:*** Insert the HUB's virtual IP address.
- ***Distributed IP Address Start:*** Insert the beginning of the range of the IPs to be distributed. Ex: 192.168.150.100
- ***Distributed IP Address Limit:*** I*nsert the end of the range of the IPs to be distributed*. Ex: 192.168.150.200
- ***Subnet Mask:*** Insert the subnet mask to be used by the VPN HUB. Ex: 255.255.255.0
- ***Lease Limit (seconds):*** This is the time limit between the lease of IPs for users of the VPN. Ex: 3600

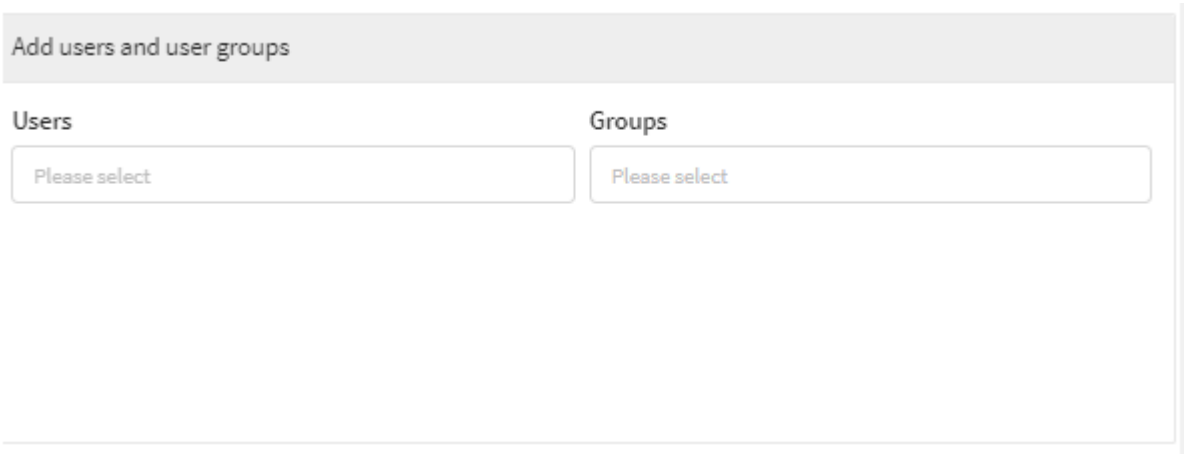
Options Applied to Clients (optional)



NG VPN's Form

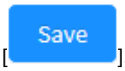
- ***DNS Address 1:*** Enter the main DNS server address. Ex: 171.31.1.2
- ***DNS Address 2:*** Enter the secondary DNS server address.
- ***Default Gateway Address:*** Insert the standard gateway address to be used.
- ***Domain Name:*** Insert the name of the domain. Ex: blockbit.com
- ***Static Routing:*** Insert the static route addresses for the HUBs. Network Address, Network mask, and the HUB's Virtual address (gateway) separated by slashes and when adding more, have them separated by coma. Ex: 173.30.0.0/255.255.255.0/192.168.150.1, 171.29.1.0/255.255.255.0/192.168.150.1.

Adding Users and User Groups



NG VPN's Form

- ***Users:*** Select a user from the NGFW's registered users list.
- ***Groups:*** Select a group from the NGFW's registered groups list.

Save the changes by clickinig the save button [

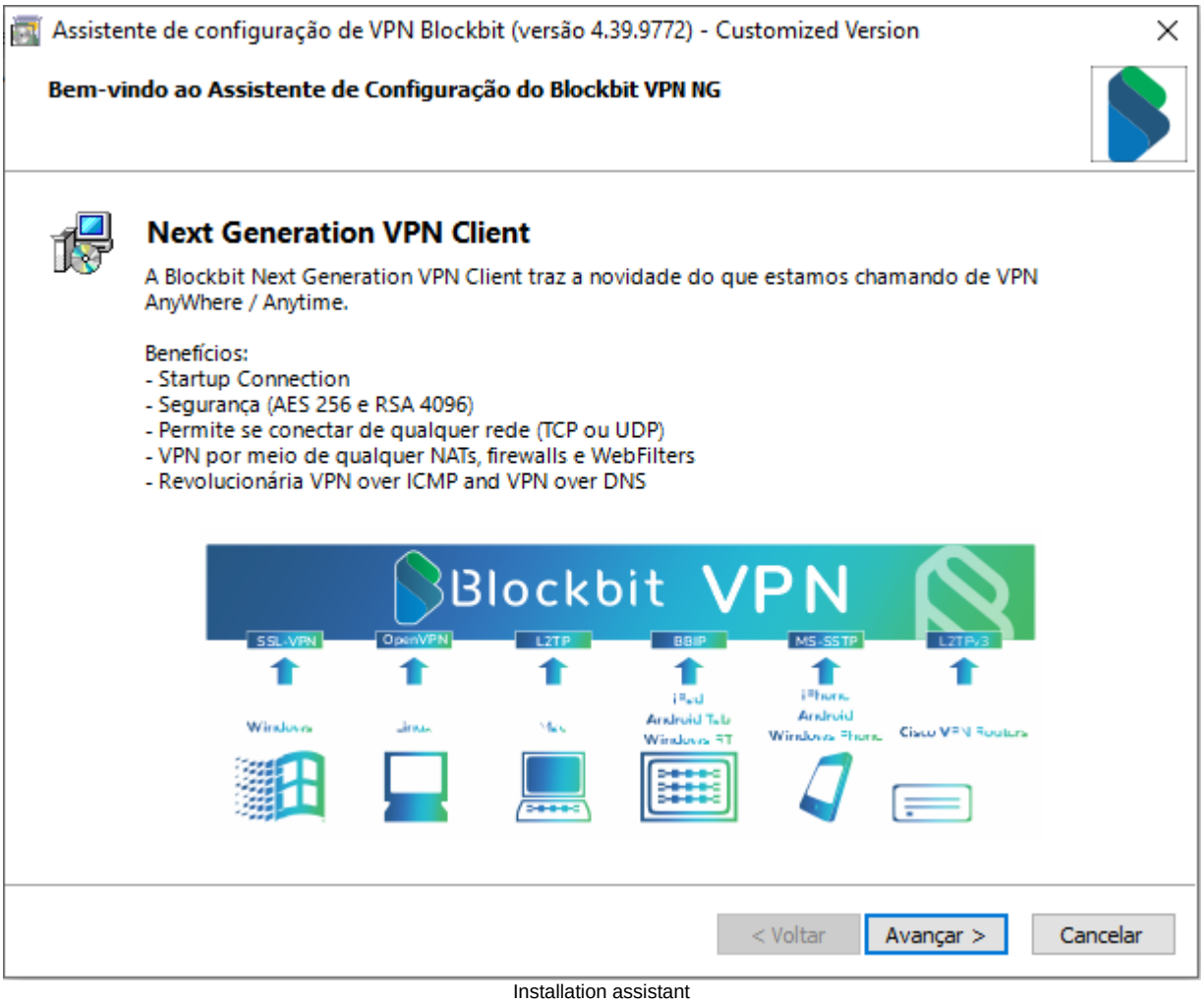
], and the NG VPN HUBs setup will be ready.

NGFW - Services - NG VPN Client

In this section we will see how to install and configure the Blockbit NG VPN.

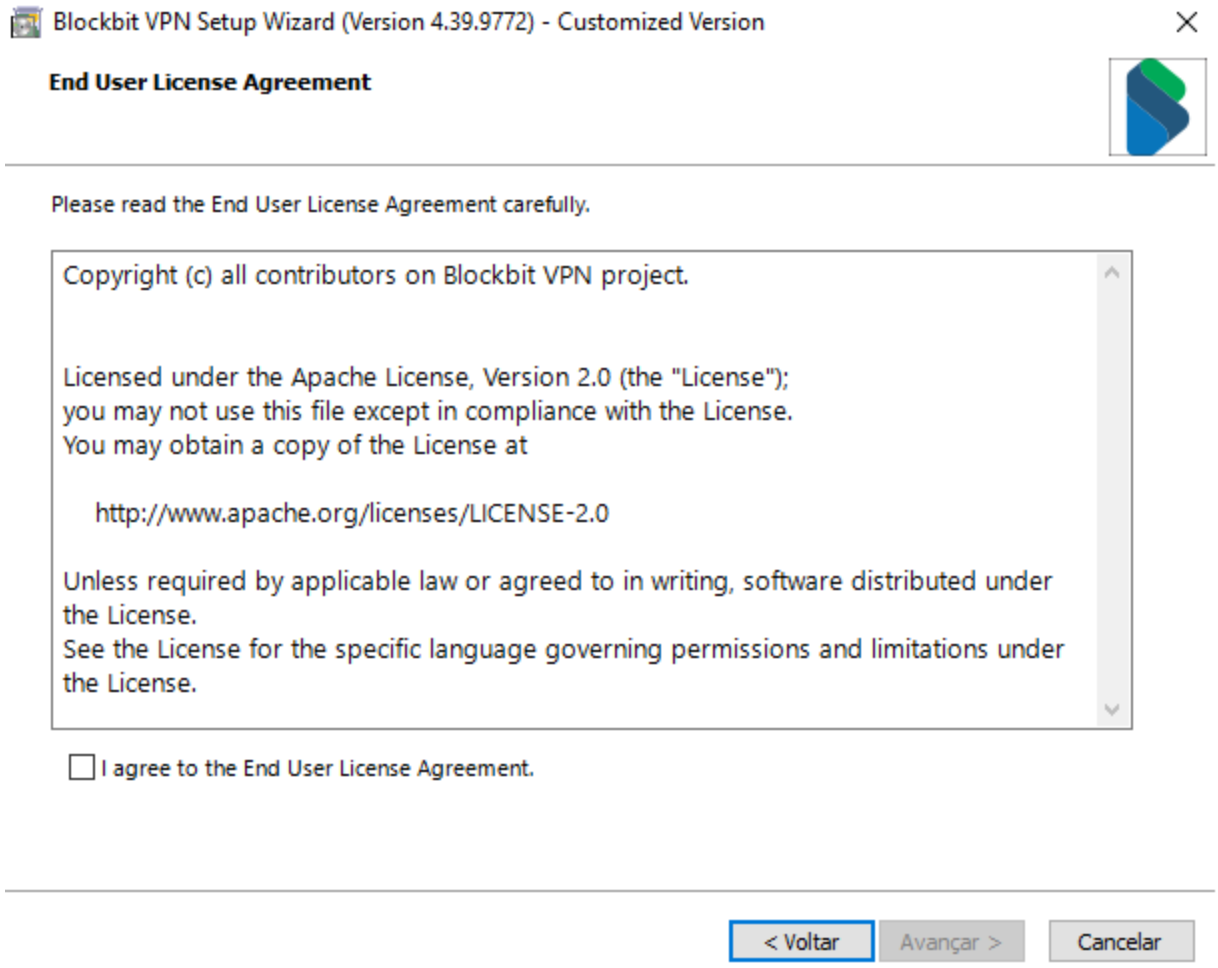
Installation

First, run the Blockbit NG VPN Client configuration assistant. The following screen will be displayed, listing some os the functionalities of the NG VPN:



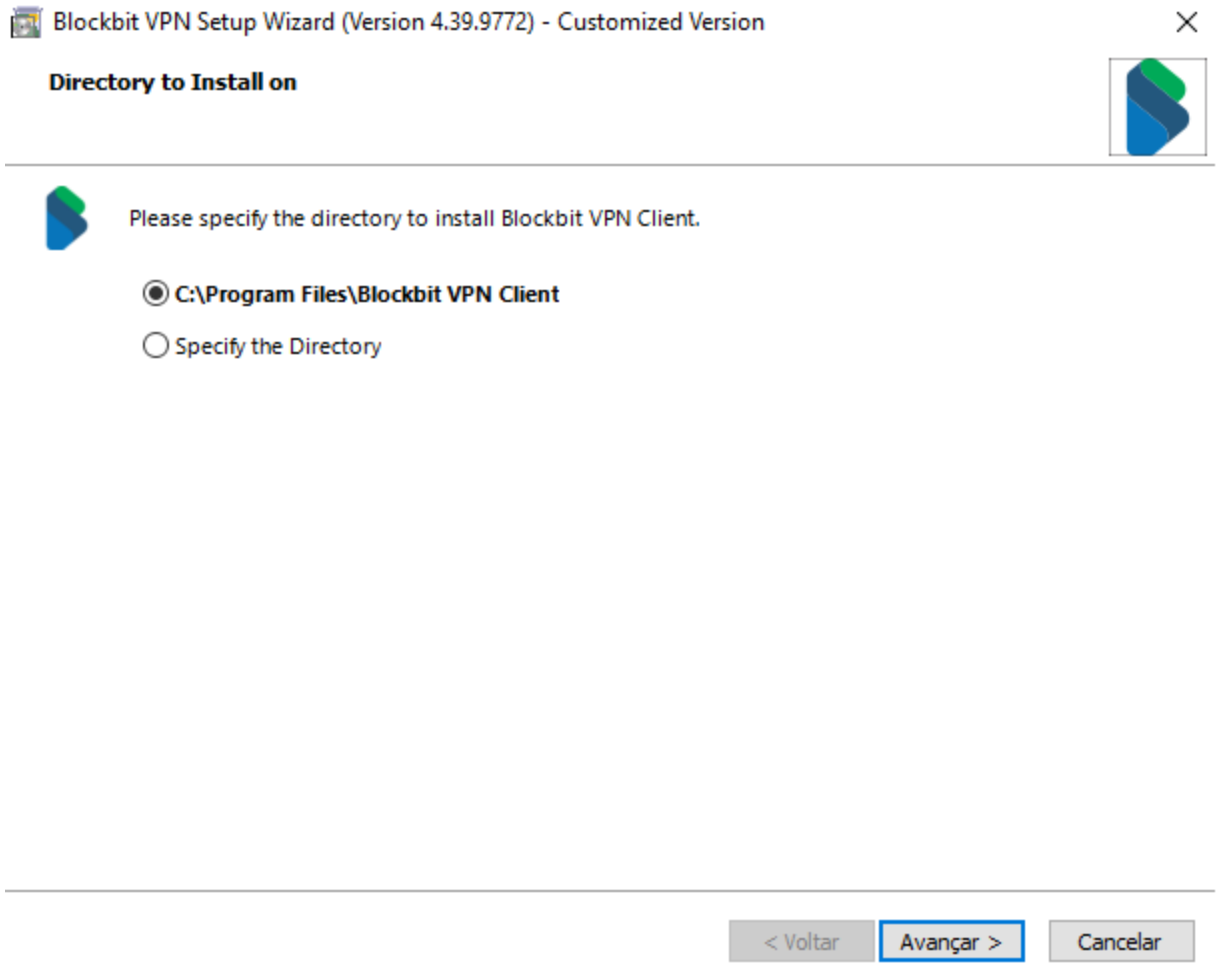
Installation assistant

Then, the final user license contract will be displayed, just agree with the license terms, by marking the option:



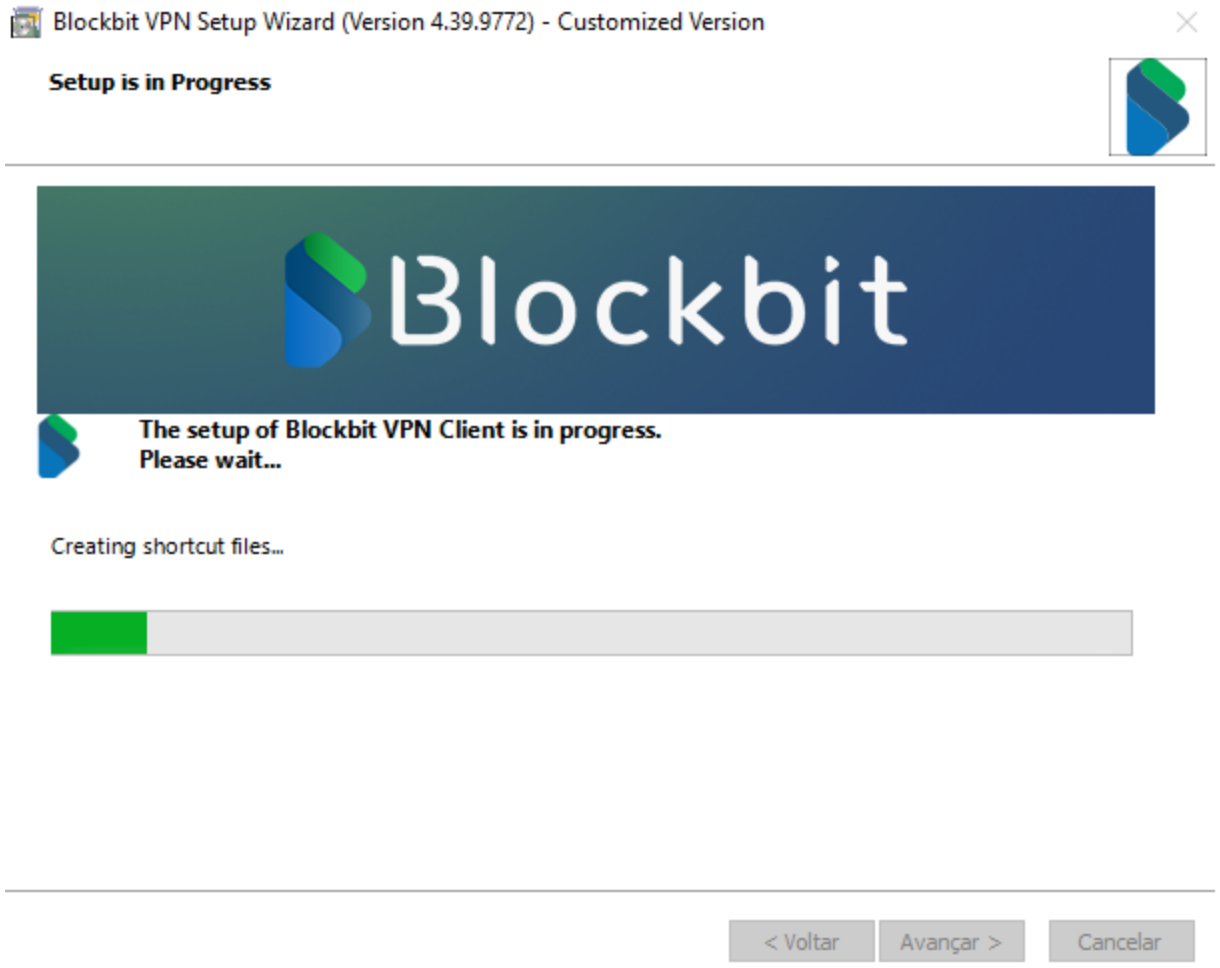
Final User License Contract

On the next screen, it is possible to select where the installation files are going to be stored:



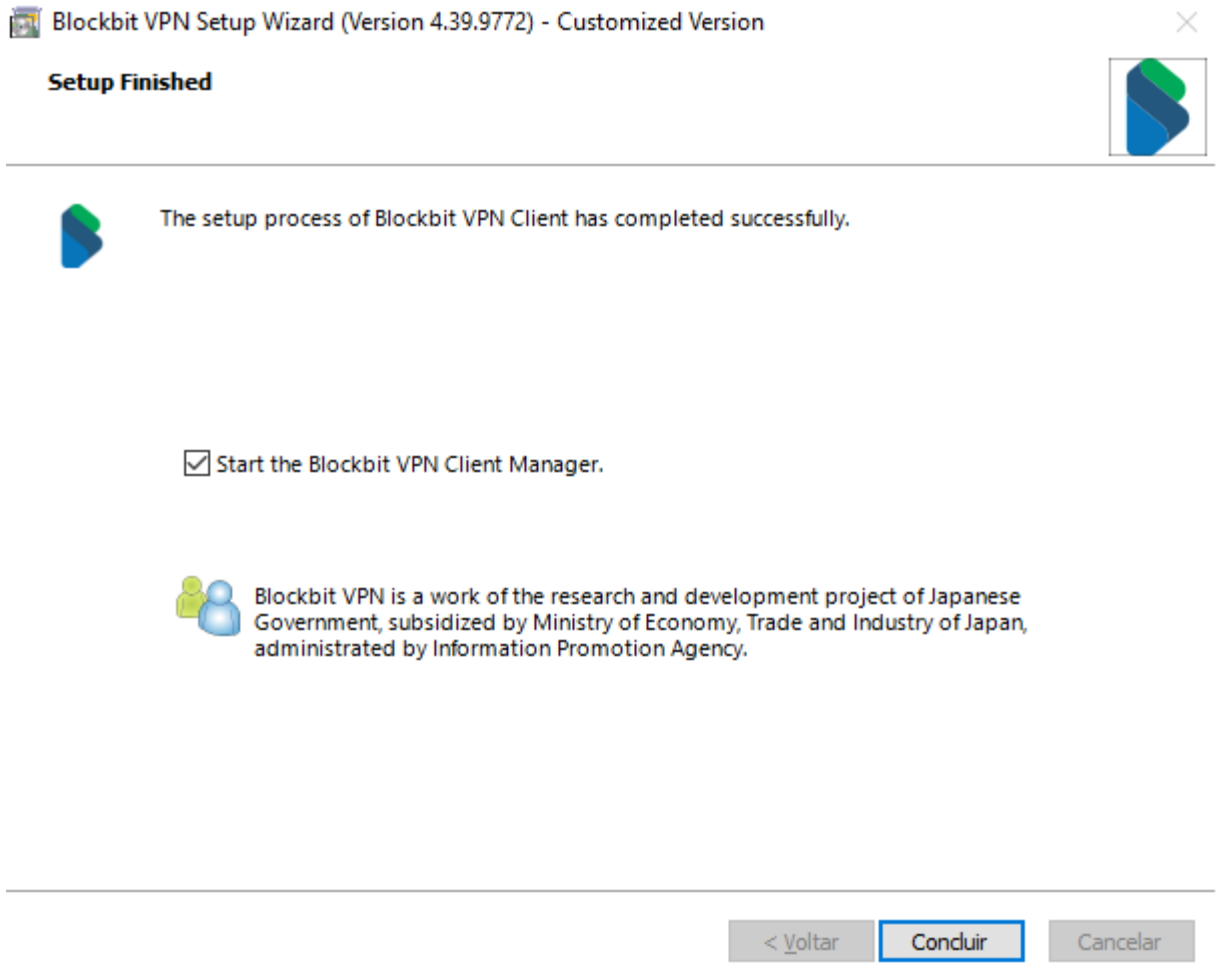
Custom Directory selection

After selecting the folder, click the advance button:



Configuration in Progress

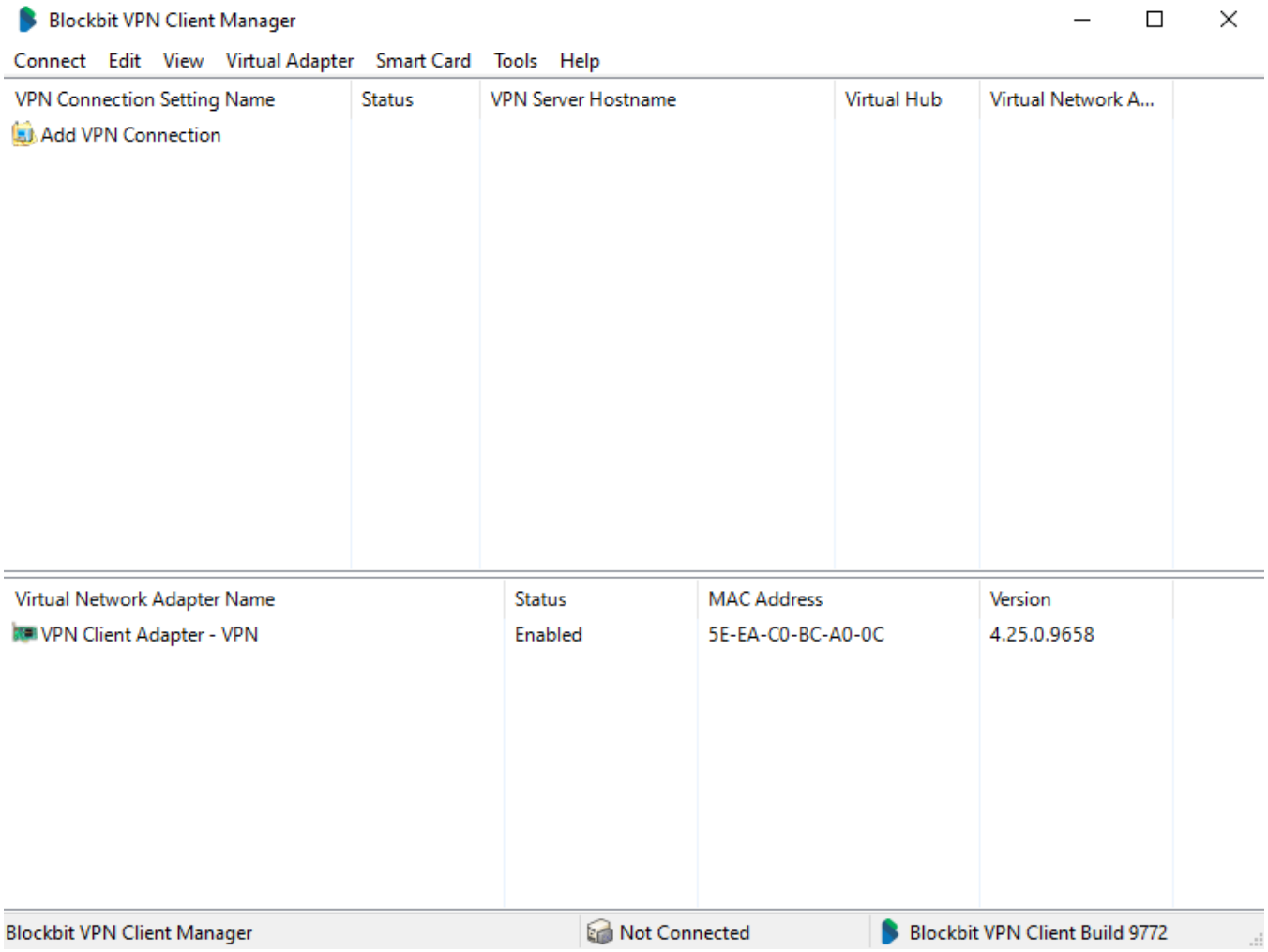
After the installation, check the box displayed and click the "finish" button, should the Blockbit NG VPN be started:



Installation Complete

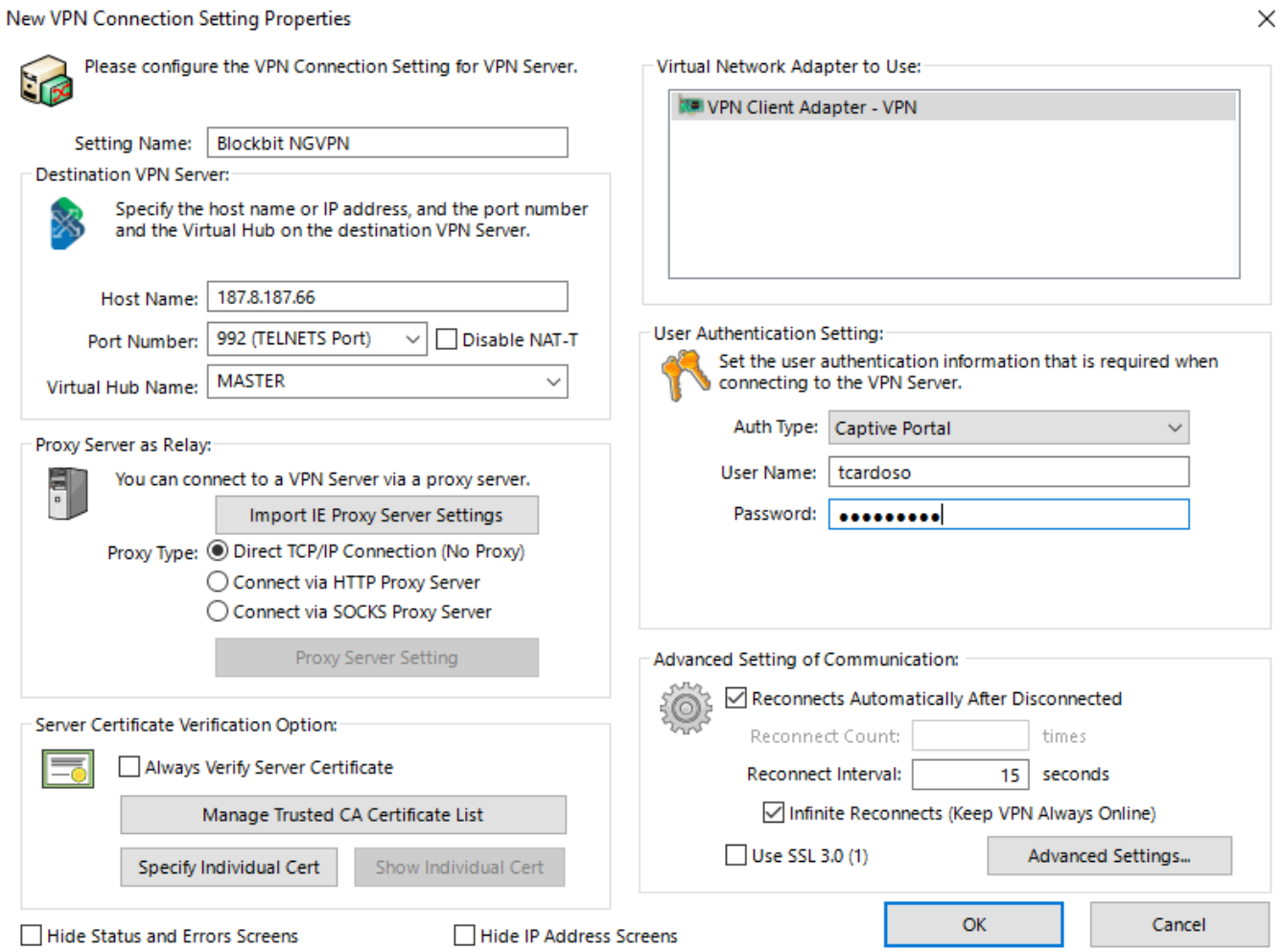
Configuration

After finishing the Client's installation and starting it up, the main screen will be displayed. The following sections will cover the configuration process of your NG VPN connection.



Blockbit NG VPN Client's main page

Click on "Add VPN Connection", and the settings page will be displayed:



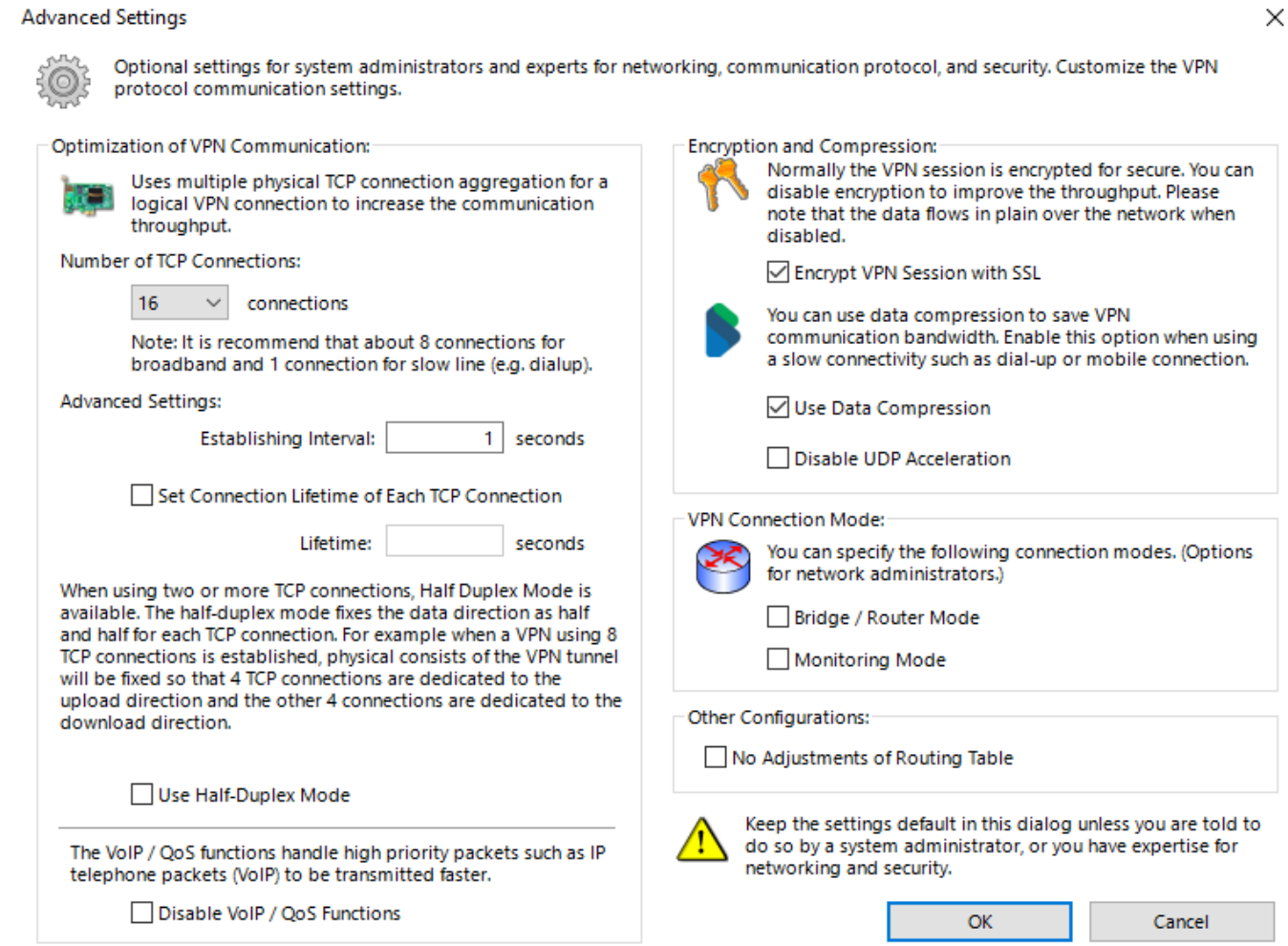
Settings

- ***Setting name:*** Name to be used on the NG VPN's settings.
- ***Host name:*** IP address or name of the host to be used.
- ***Port Number:*** Specify the port to be used.
- ***Virtual HUB name:*** Virtual hub's name, previously configured, to be used in this setting.
- ***Proxy type:*** Select the type of Proxy server to be used.
- ***Server Certificate Verification option:*** In case authority certificates will be used, it is possible to select and configure them in this option.
- ***Virtual Network Adapter to Use:*** Virtual adapter previously configured.
- ***User Authentication Setting:*** Select the authentication type that will be used, from the available options.
- ***Advanced Setting of Communication:*** Automatic reconnetion options in case of connection drop and the number of reconnection attemps are available in this option.

Next, we will analyze the advanced options.

Advanced settings

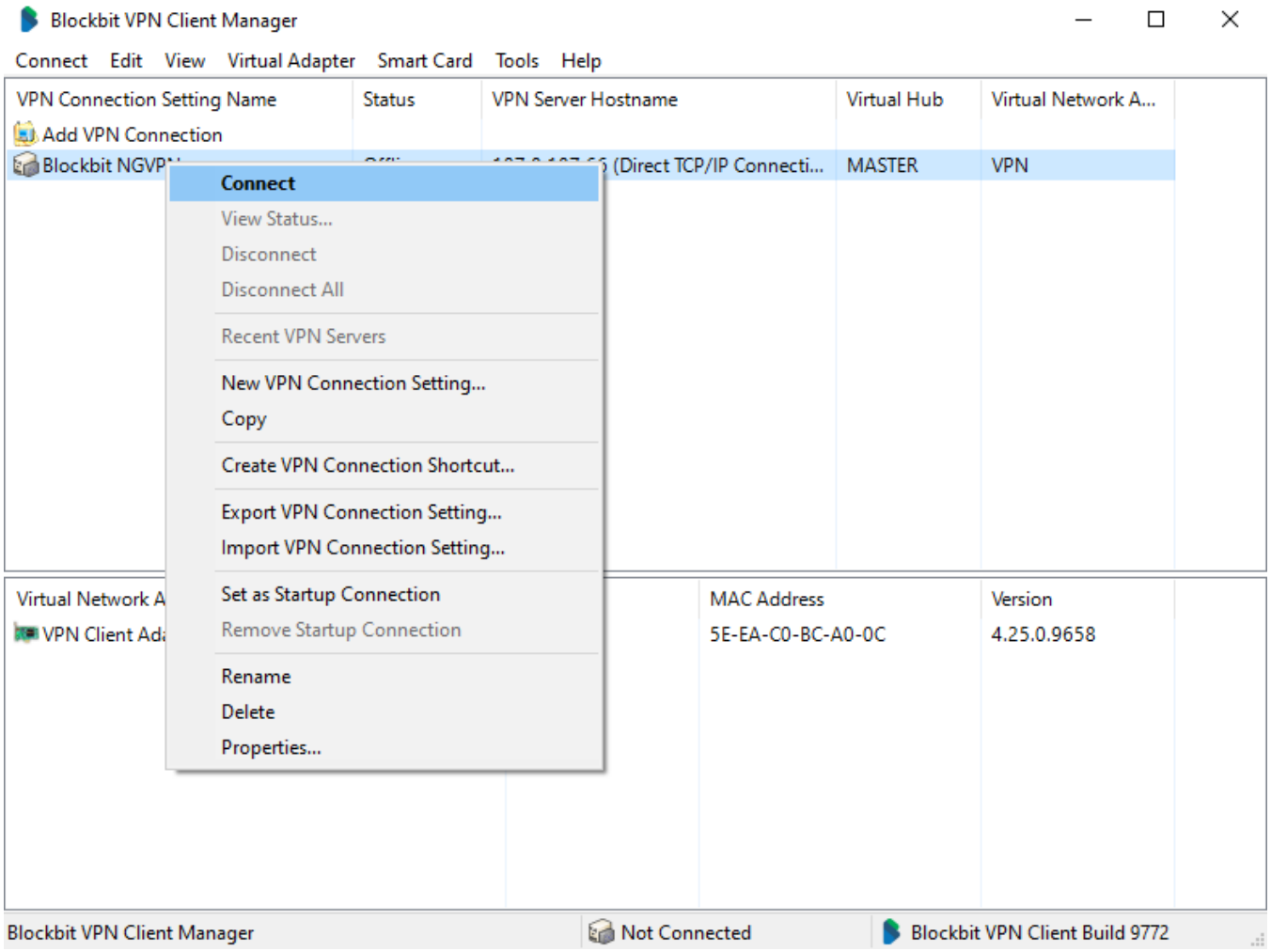
The advanced options allow a better customization of the encryption and communication protocols options of the NG VPN.



Advanced Settings main page

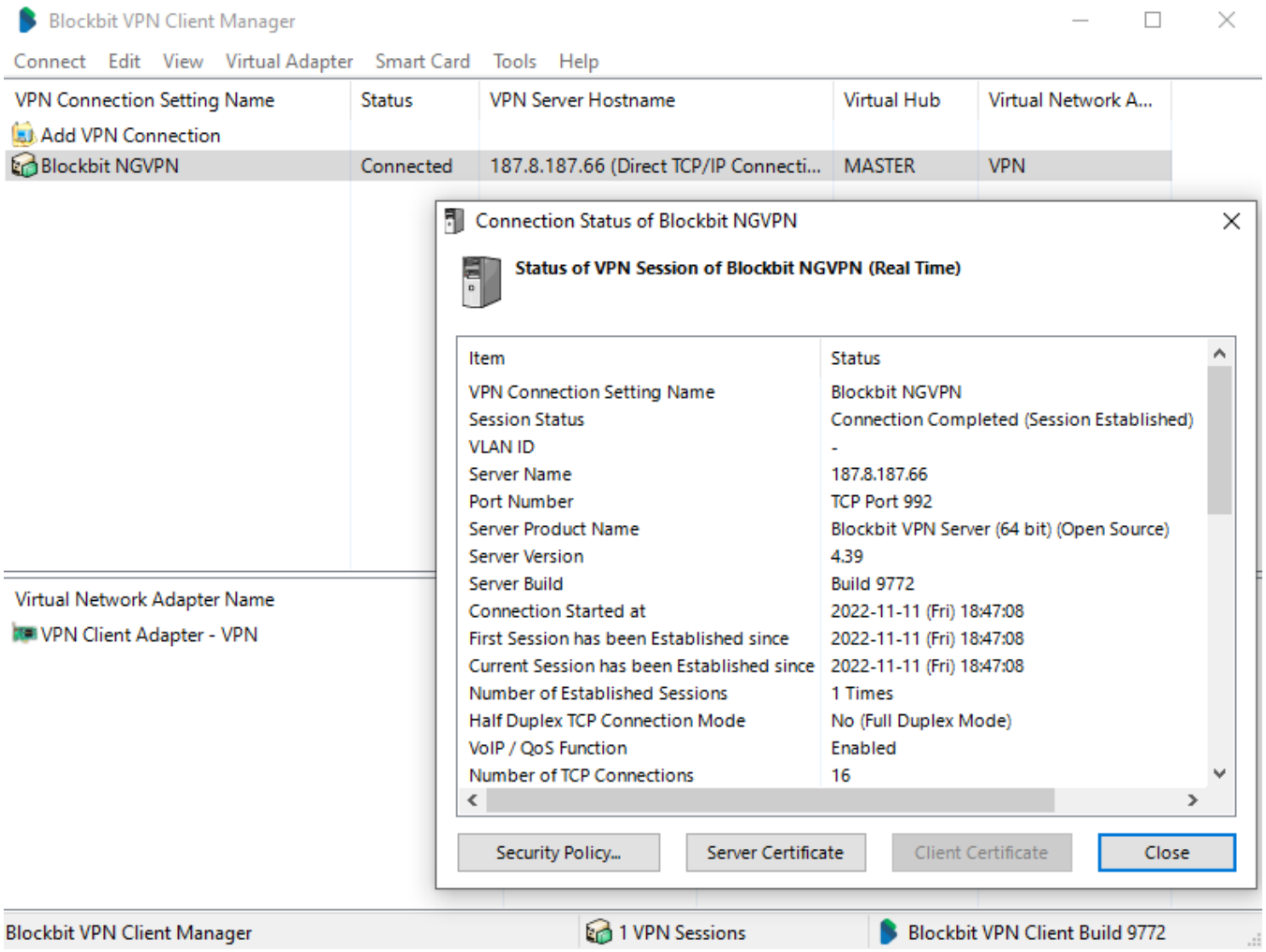
- ***Optimization:*** Allows the increase of the throughput over the use of multiple aggregation of physical TCP connections.
- ***Encryption:*** Allows the SSL encryption of the VPN session to be enabled to increase the connection's communication security. Disabling this option is not recommended, for it can mean a significant drop in the session's security.
- ***VPN Connection mode:*** Select between the Monitoring or Bridge modes (This option is recommended for network administrators).

After selecting the desired options, click "OK" to return to the settings main screen.



Main Screen - NG VPN all set.

By having finished this settings, click in "Connect", and the VPN session will be established just as on the screen bellow:

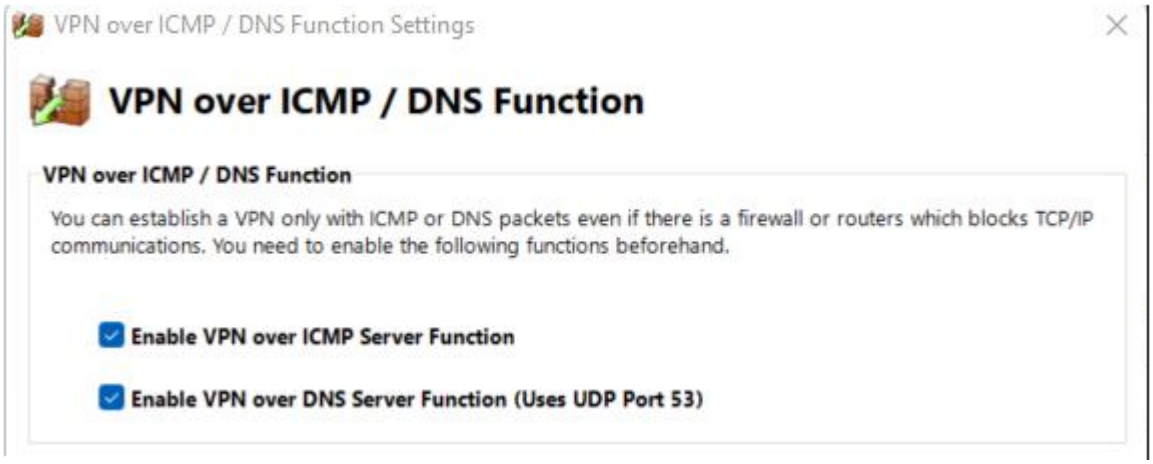


NG VPN - Configured and Connected

It's important to remember that the TCP Ports (bind) used are: 992, 5555, 8888, without the necessity of manually creating Zone Protection.
VPN over ICMP / DNS function settings

It is necessary to observe the possibility of conflict with the internal DNS, it's possible to establish the VPN only with ICMP or DNS packets even if there is a Firewall or routers which blocks the TCP/IP communications. It's necessary to previously enable the following functions:

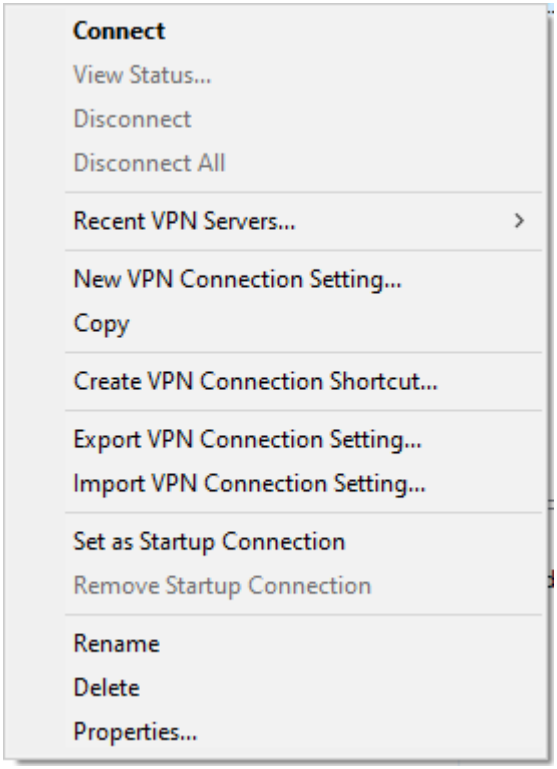
- Enable the VPN over ICMP server function
- Enable the VPN over DNS server function (Uses Port 53). As shown on the image bellow:



VPN Settings - NG VPN Client

Defining a new Startup Connection

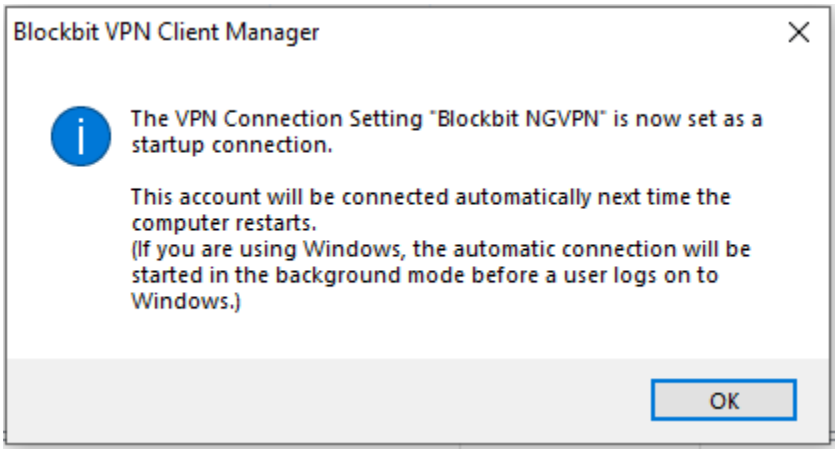
It's possible to define one of the connections of the NG VPN to be established when Windows is starting. On the connections menu, or by selecting a connection with the right click, the following menu is displayed:



NG VPN connection settings

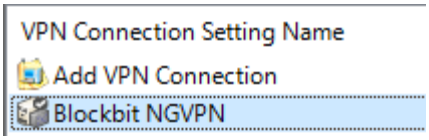
Select the "Set as Startup Connection" option to define a connection as startup connection.

The following message will be displayed, confirming that the connection is now selected as a startup connection. It also informs that the connection will be established on the background even before a user logs in on Windows:



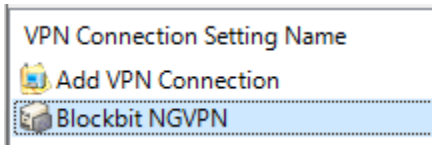
Message confirming the selection of a startup connection

After selecting the option, please note that the icon will change and the connection selected as startup will be marked differently:



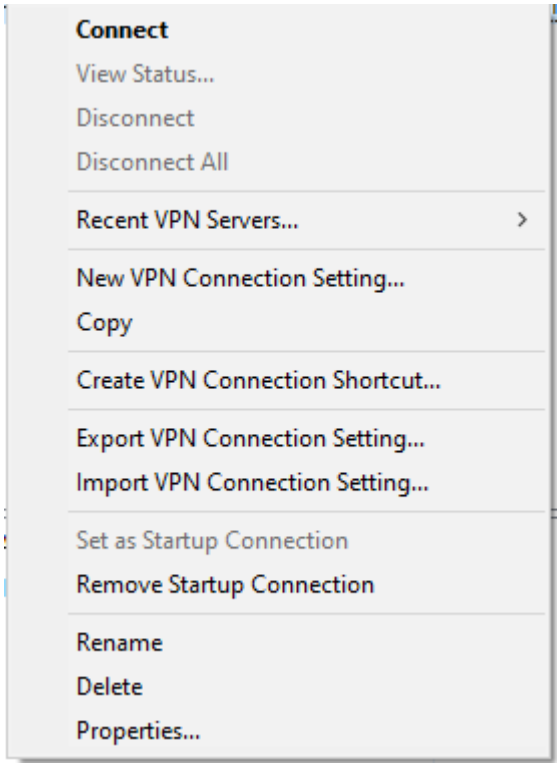
Selected connection

The other connections will not have the [] mark.

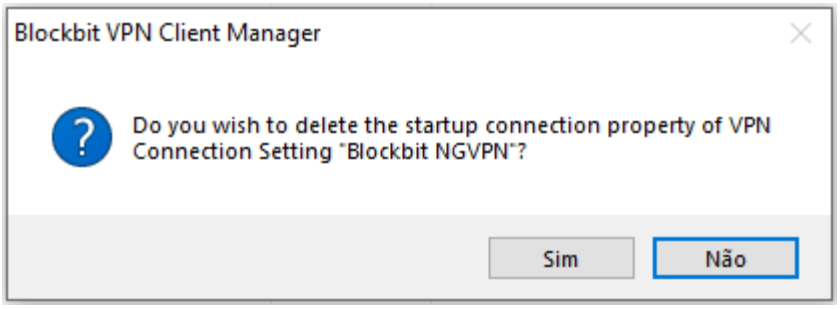


Normal connection

To remove a connection that is selected as startup, just click with the right button on this connection and select the "Remove statup connection" option:



Removal of a startup connection



Confirmation message of the removal of a startup connection

It's important to note that the removal of a startup connection by following the steps shown above, does not mean that the connection will be deleted, it simply will no longer be started at the system's initialization.

If you want to maintain a constant connection to a specific Virtual Hub when the computer is running, set that connection setting to startup connection and enable the [Endless Reconnection (Keeps the VPN Session Always)] option. In this way, VPN Client automatically attempts to connect to VPN Server using the specified connection setting when Windows is started, even if a user is not logged in on Windows.

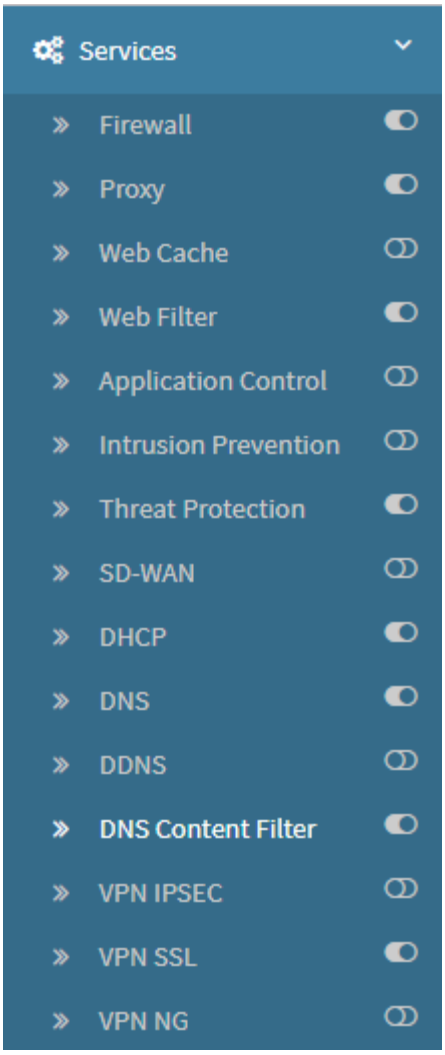
And so, we have configured our NG VPN Connection.

NGFW - Services - DNS Content Filter

DNS Content Filter is a service that prevents a user from being redirected to an innapropriate web address by protecting the translation of a specific domain to an IP address. The DNS Content filter allows access moderation to addresses sorted by their content. Eg: Gaming websites.

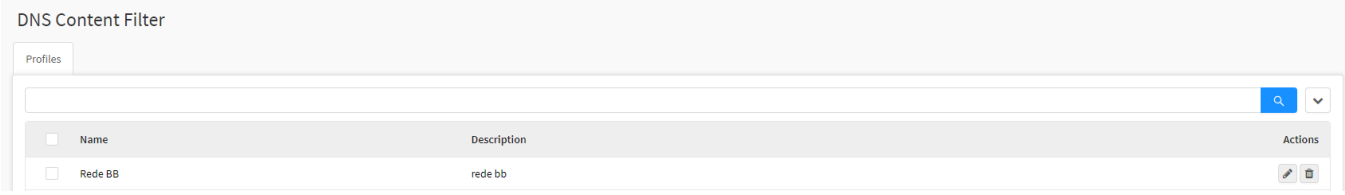
To use with Cluster, the DNS Content Filter has to be configured over an Alias interface (Ex: eth2:0) working as the local gateway.
The DNS Content Filter won´t work with the proxy on explicit mode.

On the menu, select DNS Content Filter:



Services - DNS Content Filter

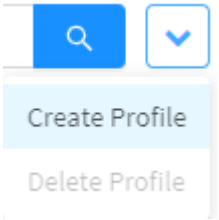
The following screen will be displayed:



Services - Interface DNS Content Filter

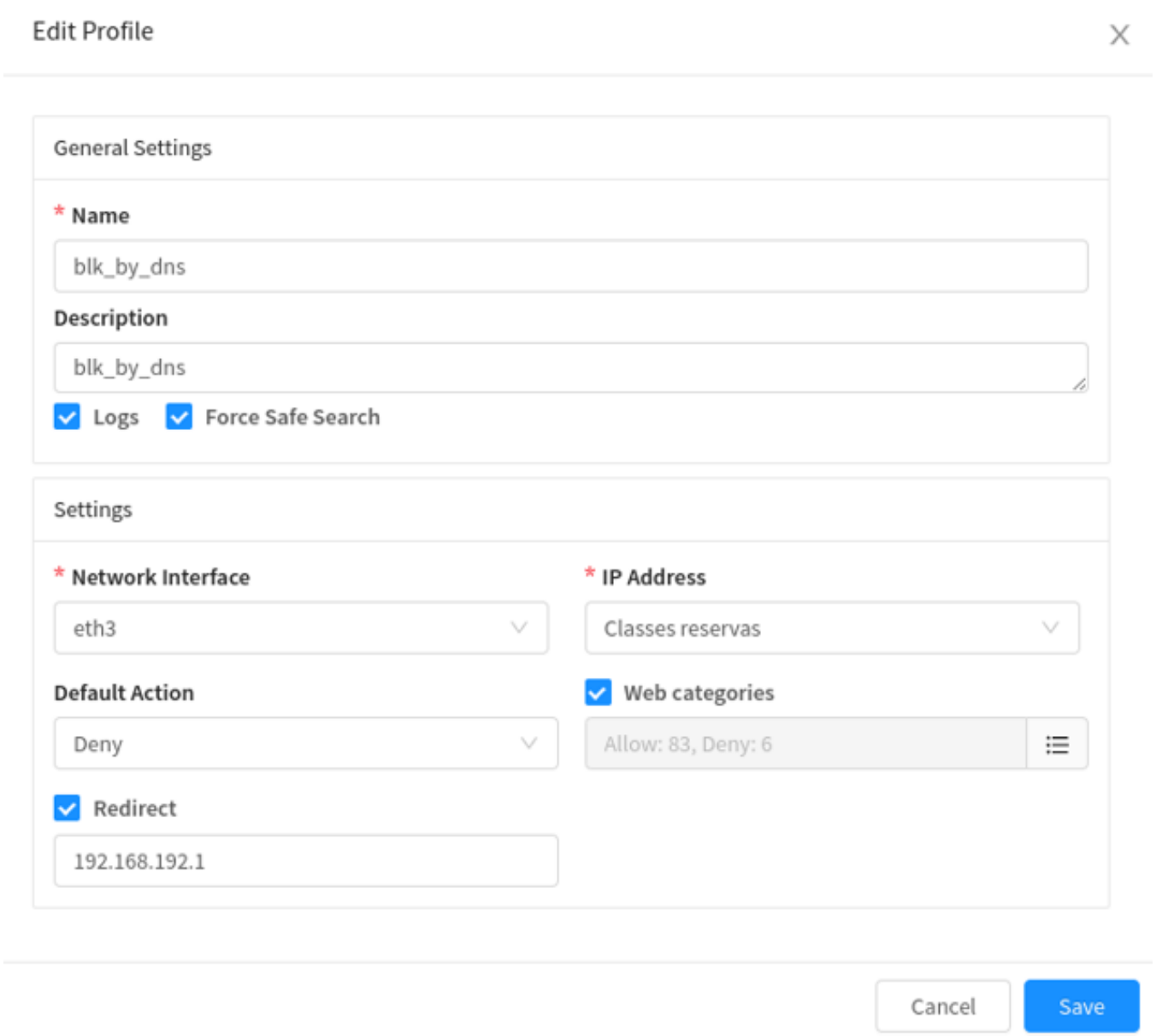
Create Profile

To create a DNS Content Filter Profile, click on Create profile in the actions menu:



DNS Content Filter - Create Profile

The following screen will be displayed:



Create Profile - DNS Content Filter

- **Name:** Profile´s name.
- **Description:** Profile´s description.
- **Logs:** Activates access logs. To check, go to Security Events.

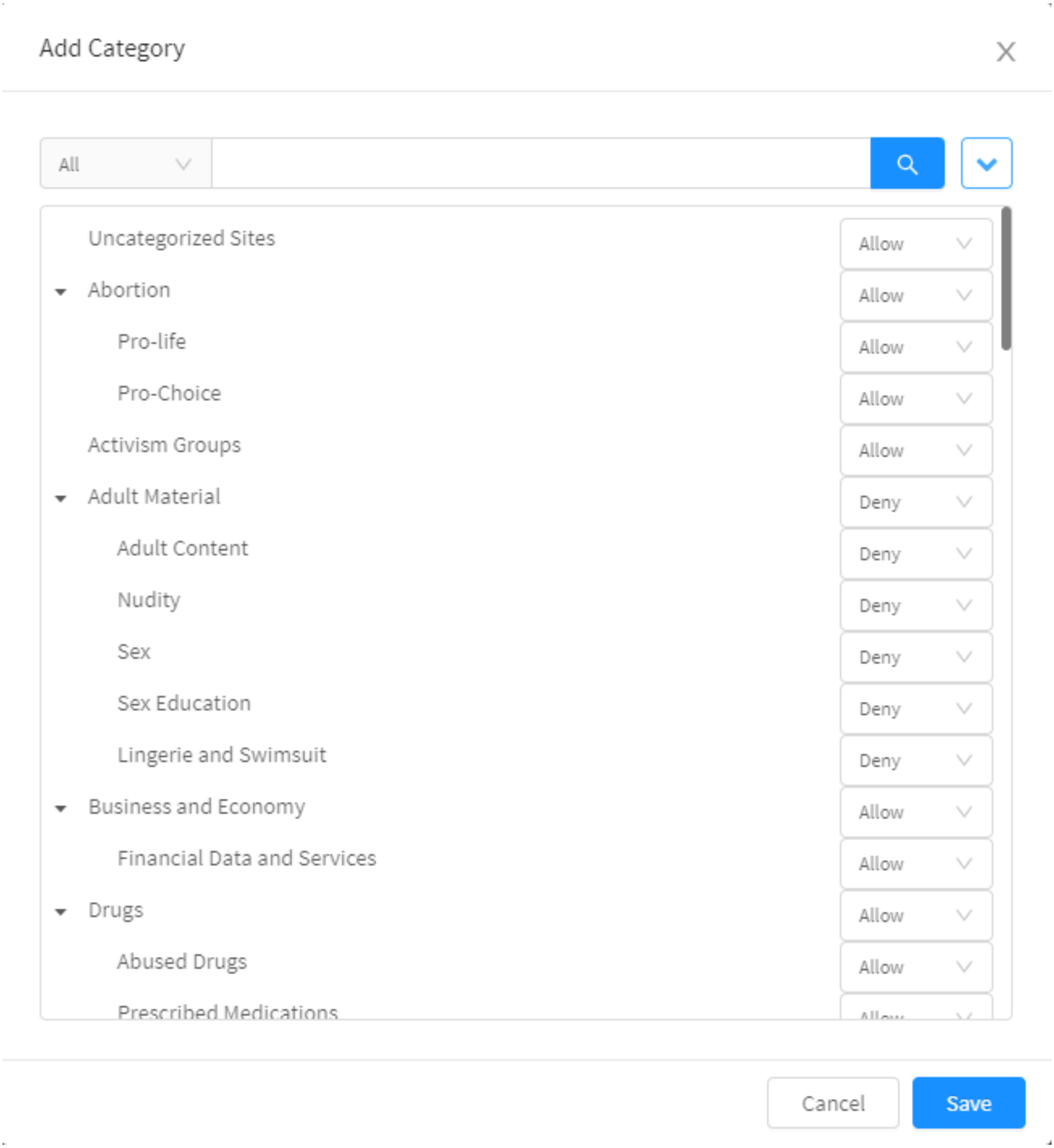
Access attempts can be viewed at Security Events by using the logtype:"dnscontent".

- **Force Safe Search:** Enables content filters automatically on search engines (Google, Bing, Yahoo!, YouTube, etc.).
- **Network Interface:** Selects the profile´s network interface (eth0, eth1, eth2, eth3).
- **IP Address:** Select the IP address with requisitions filtered by the DNS Content Filter.
- **Default Action:** Defines the default action taken by the DNS Content Filter (Allow or Deny) when a category is accessed.
- **Web Categories:** Select the categories with controlled access.
- **Redirect:** Defines the IP a user will be directed when the access is denied.

All stations´ DNS must point to the NGFW IP. Access DNS to configure.

Web Categories

In this screen, it is possible to choose categories to deny access by app, search or website.



Categories List

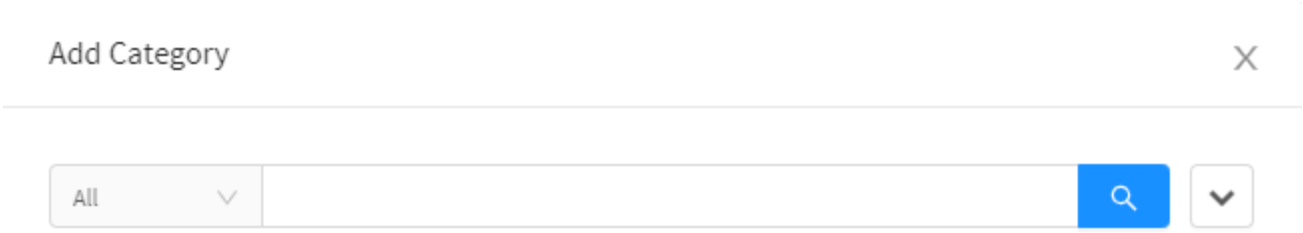
Each category can have sub-categories, whose access can be denied individually or as a group.

In "Uncategorized Sites", it is possible to deny access to domains outside the menu´s categories.

After configuring, press "save".

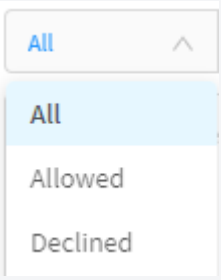
Actions menu

You can search for categories in the Actions menu.



Overview - Actions Menu

Categories display menu:

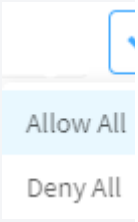


Shows categories according to access:
All
Allowed
Declined

Display Menu - Search bar:

Allows search for a specific category using keywords.

Actions Menu



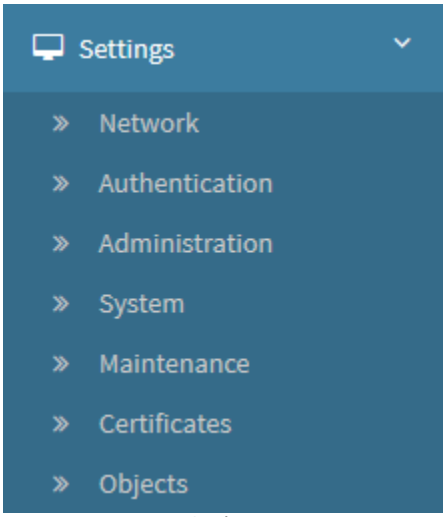
Allows changi the type of access of a category.

After selecting categories/sub-categories, click "save".

After configuring, the DNS Content Filter starts immediately. There is no need to manually bound it to a policy.

UTM - SETTINGS

The “system administration” item allows us to manage access to the WEB administration interface, define and apply the general settings, manage the registration and permissions of the system administrators, audit the accesses and the applied settings, and also manage blocked users by unauthorized access attempts .



Settings

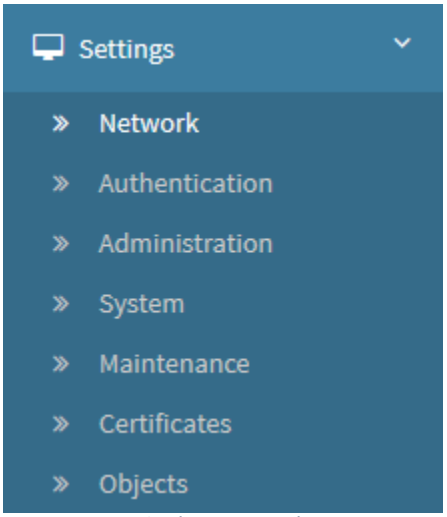
Contains the following options:

- *Network*;
- *Authentication*;
- *Administration;*
- *System;*
- *Maintenance*;
- *Certificates*;
- *Objects*.

UTM - Settings - Network

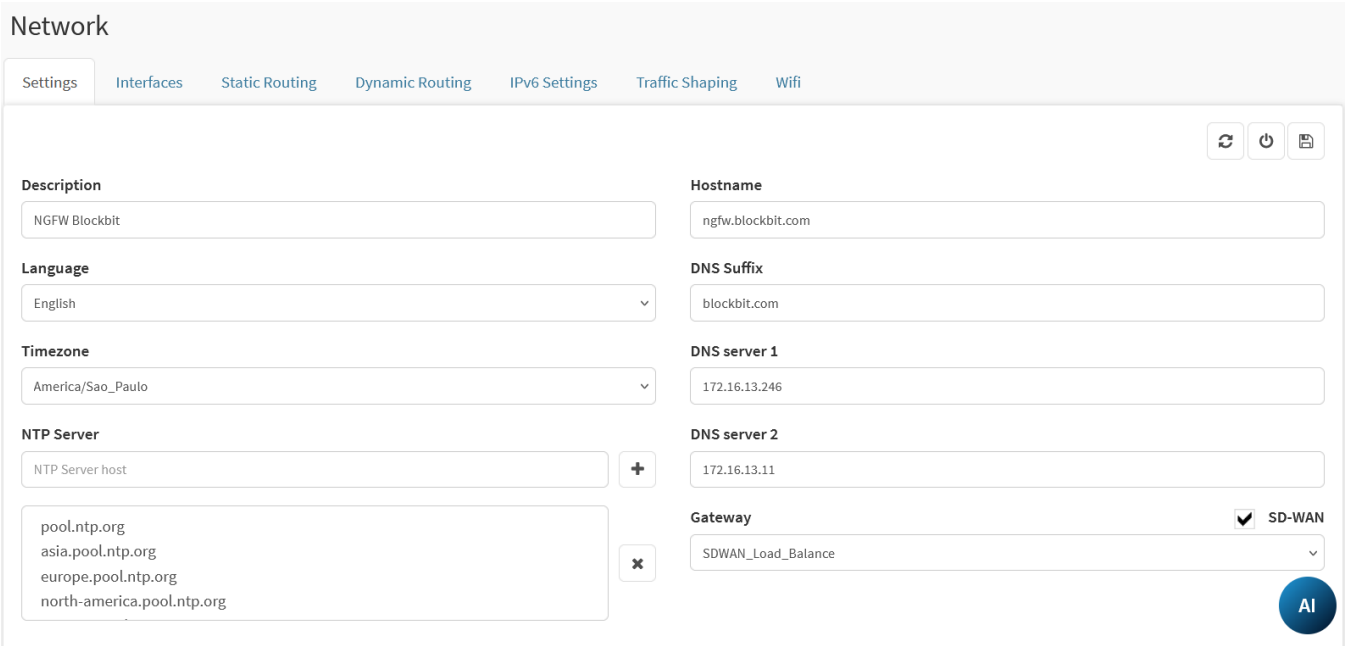
The interface includes an exclusive area for managing and configuring devices from the system information to the settings of the network interfaces and advanced routing.

To access this screen, select the "Network" option.



Settings - Network

The screen below will appear:



Settings - Network - Settings

The Network screen has the following tabs:

- *Settings*;
- *Interfaces*;
- *Static Routing*;
- *Dynamic Routing*;
- *IPv6 Settings*;

- *Traffic Shaping;*
- *WiFi*

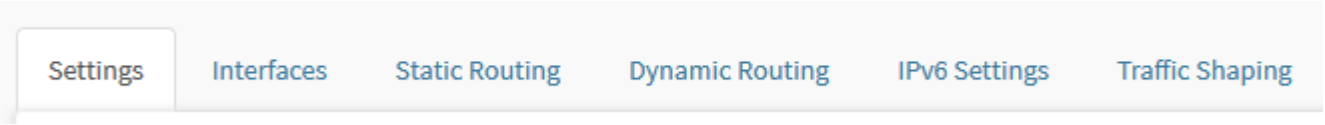
Next we will analyze the components of the *Settings* tab.

Network - Settings

This tab displays the fields related to the Windows AD server where administration credentials are configured.

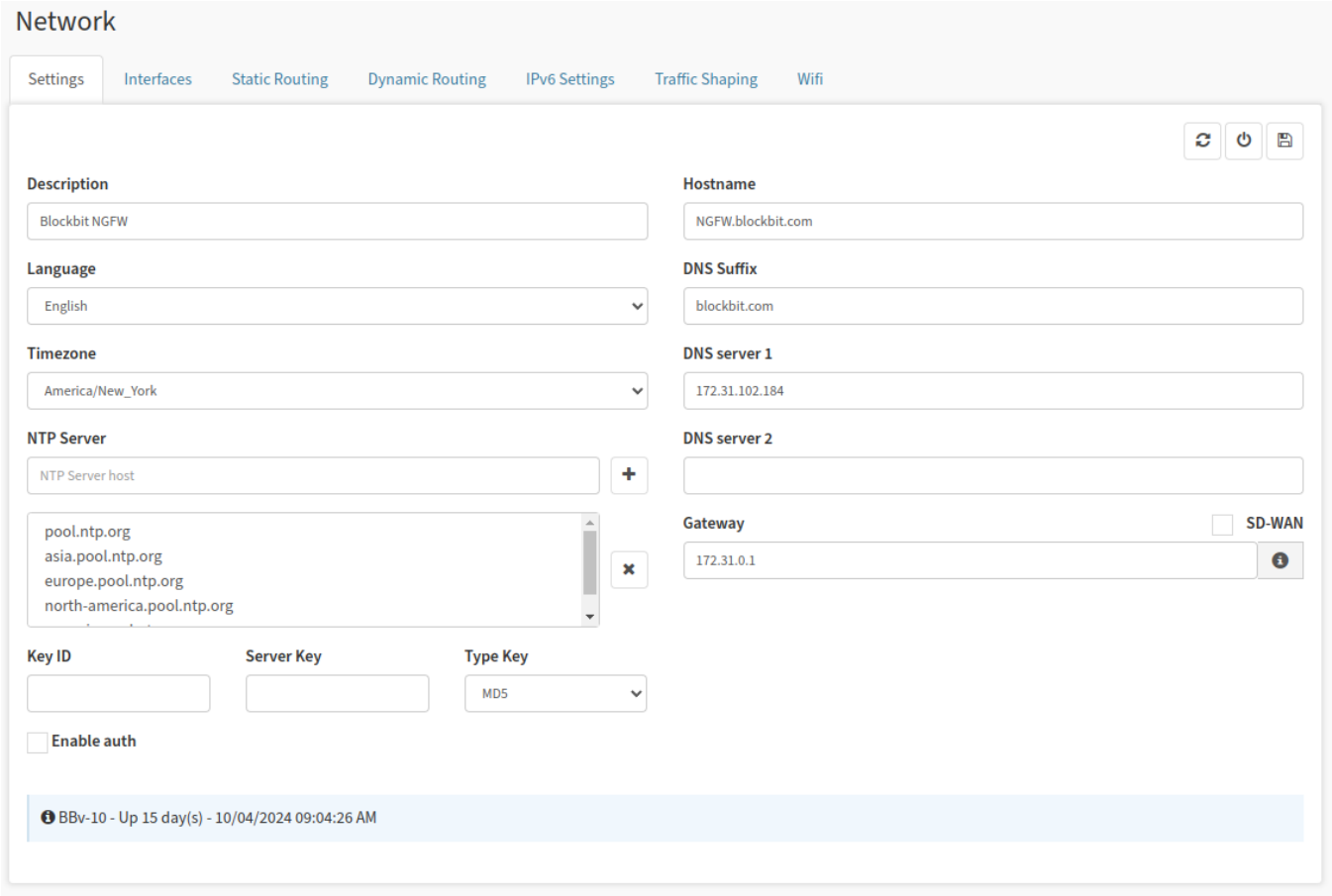
In the **[Settings]** tab, the administrator can change the basic system parameters defined in the Configuration Wizard.

If the tab is not selected, click on the "Settings" tab:



Settings tab

The next screen will appear:



Network - Settings

This panel consists of three action buttons and the following fields:

When configuring the NTP Server field: It is suggested to use the national NTP Server as a.ntp.br

- ***Description*:** Defines a description for the NGFW. Ex.: *Blockbit NGFW*;
- ***Language*:** Sets the interface language; Supported languages: English and Portuguese. Ex.: *English*;
- ***Timezone*:** Sets the time zone. Ex.: America/New_York;
- ***NTP Server*:** *Defines the NTP Server*. Ex.: pool.ntp.org, asia.pool.ntp.org, europeu.pool.ntp.org, north-america.pool.ntp.org, oceania.pool.ntp.org;
  - ***Enable Auth:*** Enables PEERS/Server authentication support;
  - ***Key ID:*** *Enter Peer key;*
  - ***Server Key:*** *Enter Sever key;*
  - ***Type Key:*** *Select key type (MD5, SHA1 or SHA256).*
- ***Hostname*:** Defines the name for the server. Ex.: master.blockbit.com;
- ***DNS Suffix*:** Defines the suffix for the server. Ex.: blockbit.com;
- ***DNS server 1*:** Sets the IP of the primary DNS server. Ex.: 172.16.102.161;
- ***DNS server 2*:** Defines the IP of the secondary DNS server, this field is optional;
- ***Gateway*:** Defines the system gateway. Ex.: 172.16.102.1.
- **SD-WAN:** Checkbox to enable the SD-WAN profile selection mode on the gateway field.

It's important to notice that regardless of the SD-WAN profile mode that is selected, only the "Failover" type is supported by the standard gateway field. Therefore, if the user selects an SD-WAN profile of the "Load Balance" for instance, the system will automatically convert it to "Failover", ignoring the profile's original action.

At the end of the settings click on the **[**  **]** button and apply in the action queue **[**  **]** .

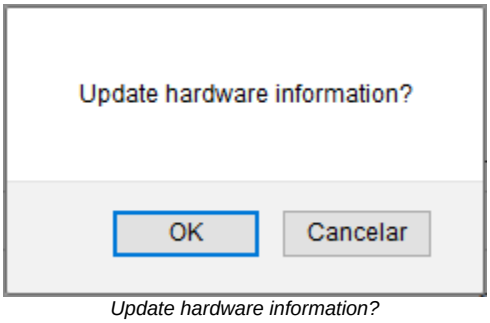
In addition, at the top right of the form you will find 3 icons, for more information visit this page.

Network - Settings - Action Buttons

At the top right of the form you will find 3 icons, with the following functions:

Update Hardware Information

The [ ] button has the function of updating the hardware information. When you click on it, the following notification will be displayed:



Update hardware information?

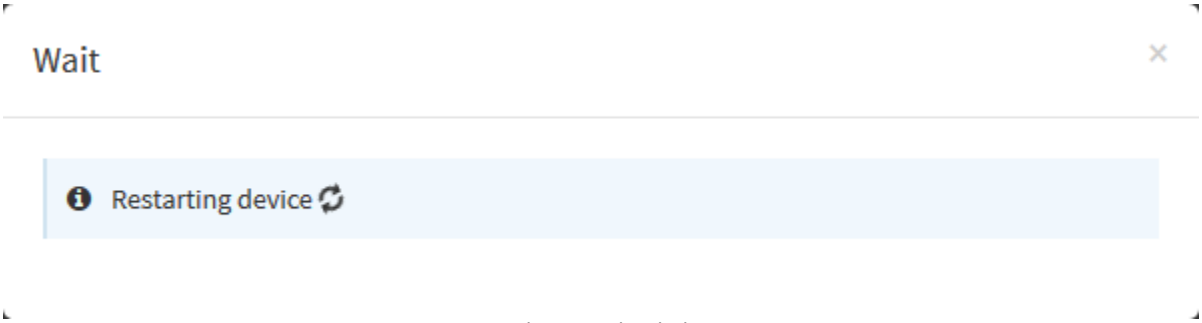
Click on [OK] to complete the update otherwise click on [Cancel] to close this window.

Shutdown/Restart

The [ ] button has the function of turning off or restarting the UTM, it is the equivalent of applying the *shutdown* or *reboot* command on the CLI. When you click on it, the following window will appear:

Shutdown/Restart

To restart the system, select the Reboot option, click the [Save] button and wait for the process to complete, as shown below:

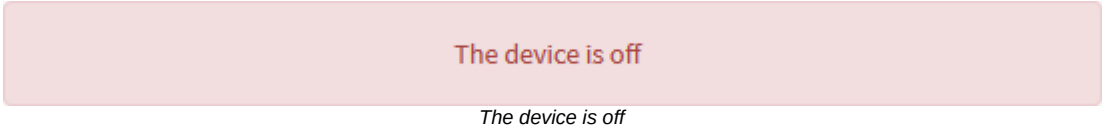


Wait - Restarting device

After this step, you will be redirected to the login screen.

Login screen

To shut down the system, select the Power Off option, click the [Save] button, the shutdown process will be performed and the following message will be displayed:



The device is off

From that point on, the system will be inoperable until it is turned on again.

Save

The [] button allows saving the settings made, however, after clicking on it in the Network panel, it is necessary to apply the changes made in the command queue, as shown on the page: Command queue;

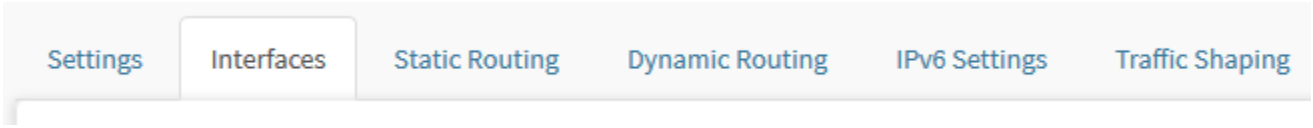
Network - Interfaces

Standard “Ethernet” physical interfaces are automatically identified by the system. For more information on configuring them, check this page: *Interfaces - Interface Ethernet*.

In addition, on this panel it is possible to configure the physical interfaces to support the MPLS protocol.

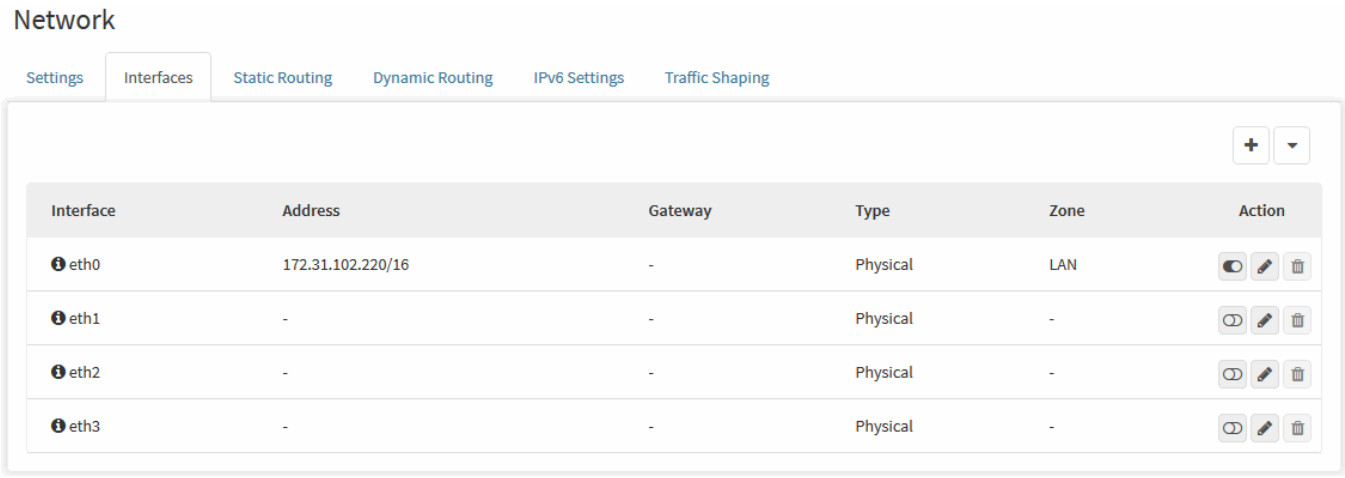
The “Interfaces” tab is made up of six columns: “*Interface*”, "*Address*", "*Gateway*", “*Type*”, “*Zone*” and “*Action*” and in addition, at the top of the screen there is a button for adding interfaces and the actions menu.

Click on the Interfaces tab.



Interfaces tab

The “Interfaces” screen will appear, as shown by the image below:



Network - Interfaces

In this tab we can configure and add physical and virtual interfaces, as listed below:

- ***Ethernet***;
- **3G/4G/LTE**;
- **ALIAS**;
- ***VIRTUAL*;**
- ***VLAN*;**
- ***DSL*;**
- ***LAG*;**
- ***BRIDGE*;**
- ***TUNNEL*.**

This section will cover:

- Registration, Editing and Removal of interfaces;
- Enabling and Disabling Interfaces;
- The particularities of each type of Interface;
- MPLS protocol concept;
- Packet Fragmentation and MTU;
- Etc.

Next, we'll look at the functions located at the top of this panel.

Interfaces - MPLS support

MPLS (Multi Protocol Label Switching) is an efficient way to connect access points through the cloud and reduce the overhead in packet routing.

This technology performs the forwarding of packets using specific labels instead of IP addresses or layer 3 information, virtual links are used instead of endpoints, avoiding checking the routing table which consequently streamlines the data flow.

MPLS works by assigning labels to all routes in the routing table of appliances connected to the network, after this step the LDP (Label Distribution Protocol) automatically shares this information, which in turn is used to build a routing table based on labels. The packet forwarding uses this table as the basis for forwarding the packets, always prioritizing the shortest route, during the process of sending them, when a network router receives the packet, it replaces the current label with that of the next hop in the network and continues, this process is repeated until the package reaches its destination.

MPLS technologies are applicable to any network layer protocol, being able to bridge between access points through cloud service routers in a private tunnel, the method is applicable regardless of the interface, allows communication from one to many (making it possible to determine specifically within the cloud with whom the communication will be made) and thanks to the application of tags contributes to the network's Quality of Service (QoS).

The NGFW provides native network encapsulation support based on the MPLS protocol, which allows it to act as a LER (Label Edge Router) by encapsulating and unpacking the labels, eliminating the need to use a physical router at the end and optimizing traffic.

However, it is noteworthy that it does NOT route MPLS network packets.

The NGFW does not act as an LSR (Label Switch Router). An LSR is characterized by routing packets on the MPLS network using labels as the basis for locating the most performing route.

The NGFW allows the encapsulation of several MPLS network segments through a single link, which allows traffic to be routed on the same link to multiple units, allowing the provision of a private dedicated link for long distance networks to connect to multiple organizational units.

In order to use this feature, the system administrator will need to configure static routes as listed below:

- Target network;
- Destination gateway;
- Destination label (only available on interfaces with MPLS support enabled);
- Output interface.

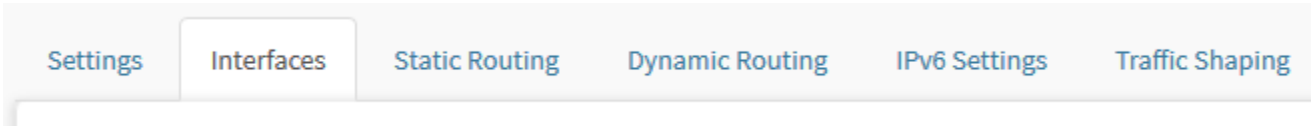
When an MPLS-type interface is identified, the kernel modules are automatically loaded and support is applied to the operating system.

The activation of MPLS is not available in older versions of the NGFW as their version of the Kernel does not support the protocol.

Configuration of Physical Interfaces

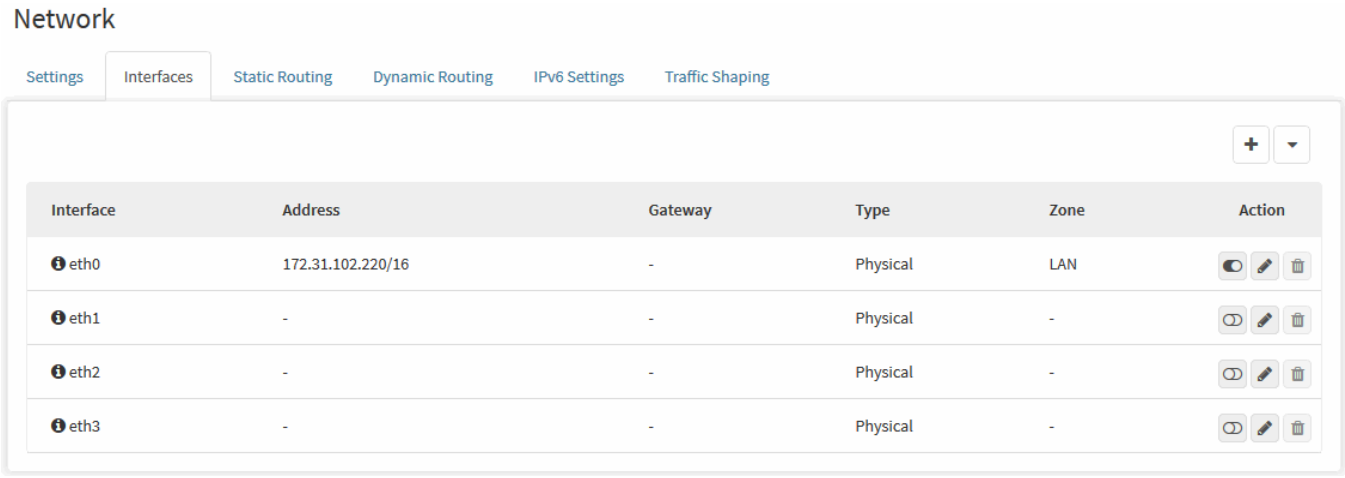
To configure MPLS support, you will need to configure a physical interface, to do so, follow the steps below:

Being in Network, click on the Interfaces tab:



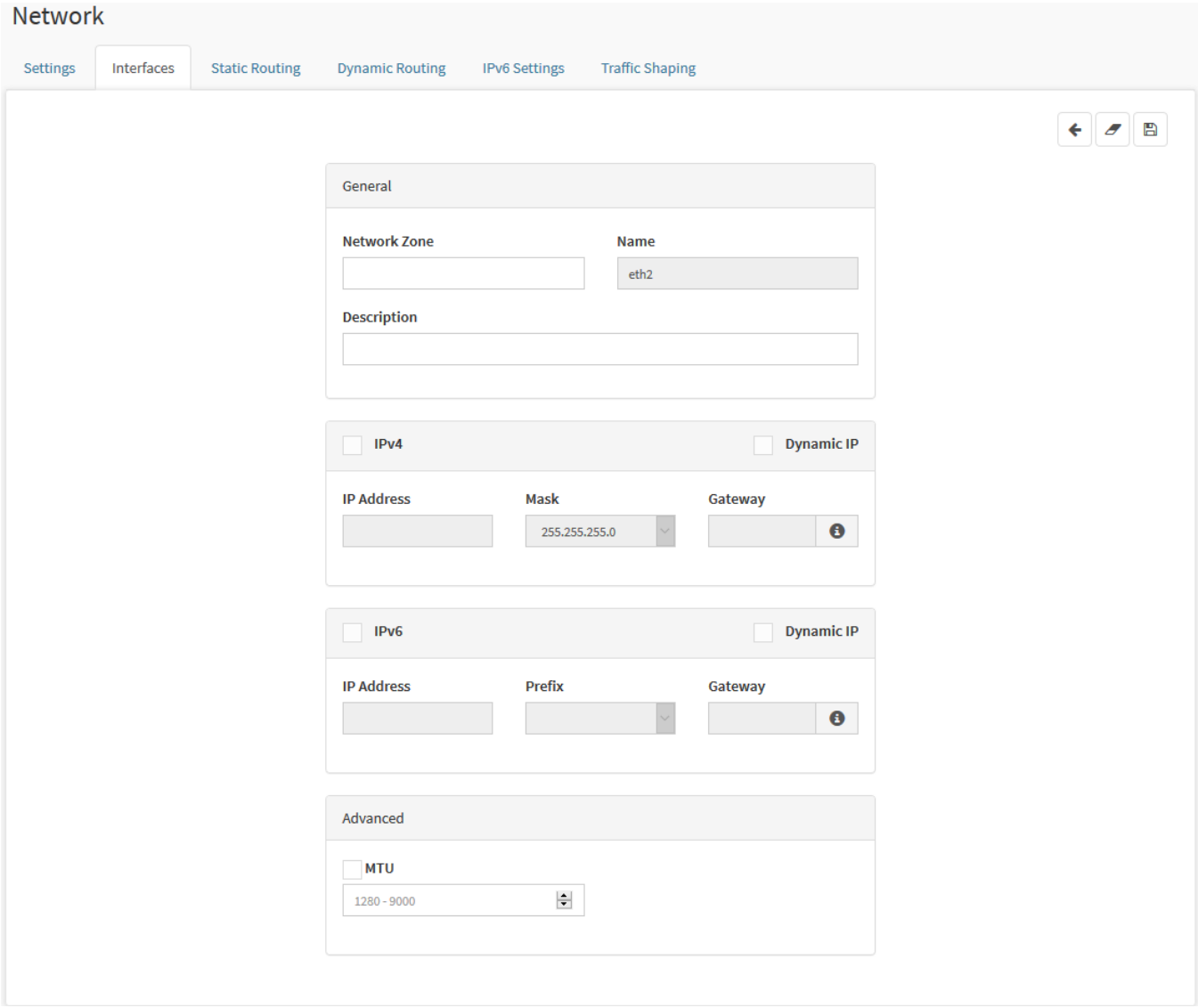
Interfaces tab

The “Interfaces” screen will appear, as shown by the image below:



Network - Interfaces

Initially access a physical interface and click on **edit [** **]**. The following screen will be displayed:

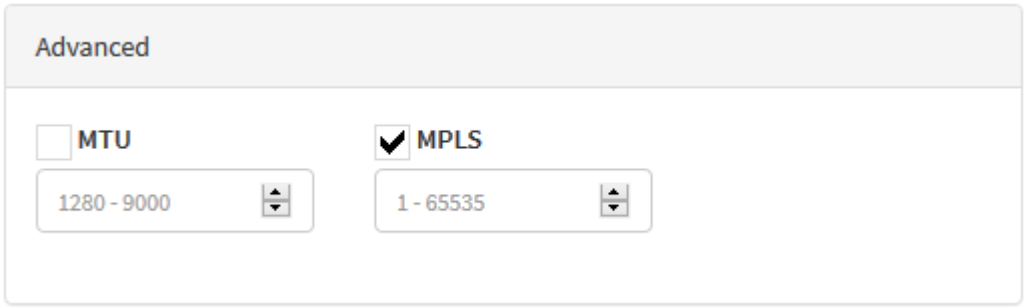


Configure it according to the specifications of the respective fields, as shown on this page.

In the Advanced panel, pay attention to the following settings:

Advanced

More information about the Advanced panel follows:



Interface Ethernet – Advanced

In a Physical interface it is possible to define the MTU (Maximum Transmission Unit), enable and configure the MPLS label:

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

- **MPLS*[ ]*:** When you enable this option, support for the MPLS protocol will be enabled, and you can route packets over both IPv4 and IPv6. When the check box is enabled, the text box below will allow the definition of the local label, and the possible value to be entered in this field is from 1 to 65535.

The activation of MPLS is not available in older versions of UTM as their version of the Kernel does not support the protocol.

If you want to delete all the settings made on this interface, click ***Erase*[ ]**.

WARNING: The ***Erase*[ ]** button will erase all interface settings. Under no circumstances apply the settings in the **command queue [ ]** without first configuring the interface without first, configuring the interface. If it is not displayed on this panel, access the "Settings" tab and click the **Update Software Information [ ]** button to view the interface again and be able to edit it.

To save changes, click ***Save***[ ], otherwise click ***Back***[ ] to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

If a static route using the interface has been configured, when disabling this interface a confirmation message will be displayed. For more information on how to set up static routes, see the next step.

After performing these procedures the interface will have been successfully configured.

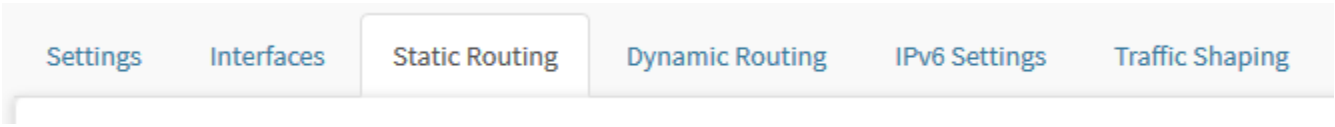
Next, we'll look at how to set up static routes:

Configuration of static routes

The example below shows a in basic terms how to configure a static route with MPLS. Consult this page if you need more detailed information.

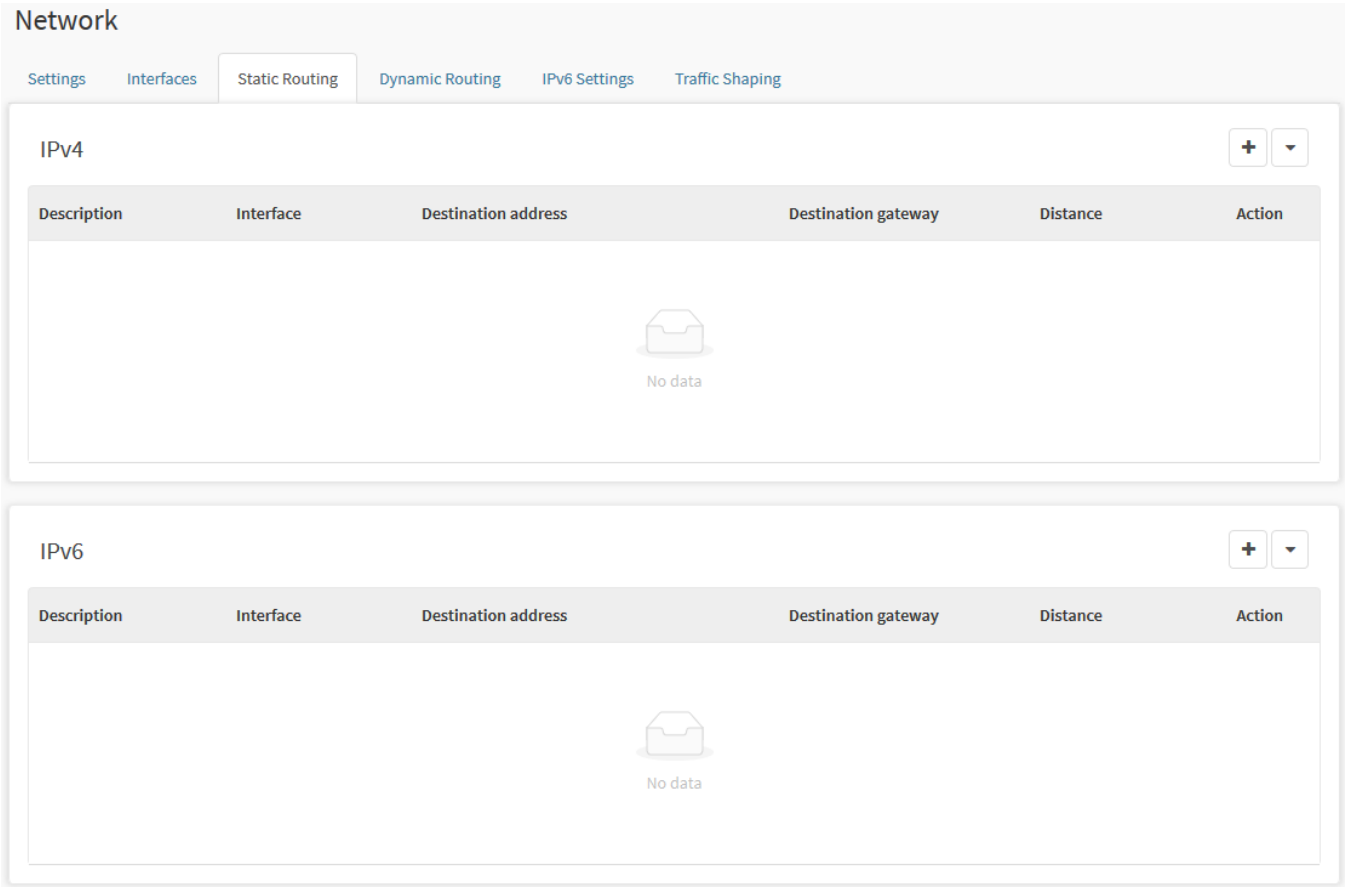
To view the detailed walkthrough of a static route configuration with MPLS, see the example located on this page.

Configure the static routes for MPLS, for that, being in Network, click on the Static Routing tab.



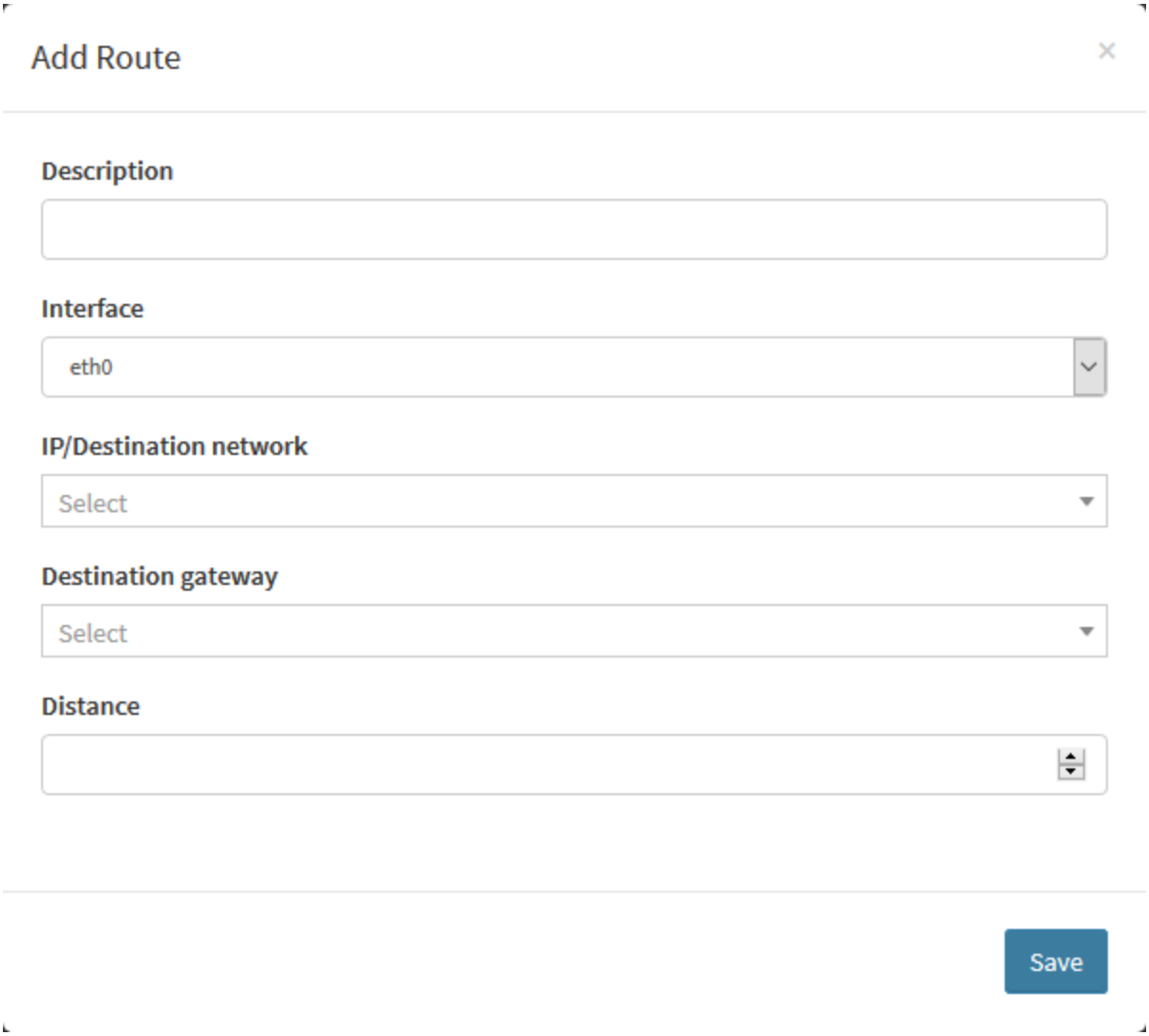
Static Routing tab

The “Static Routing” screen will appear, as shown in the image below:



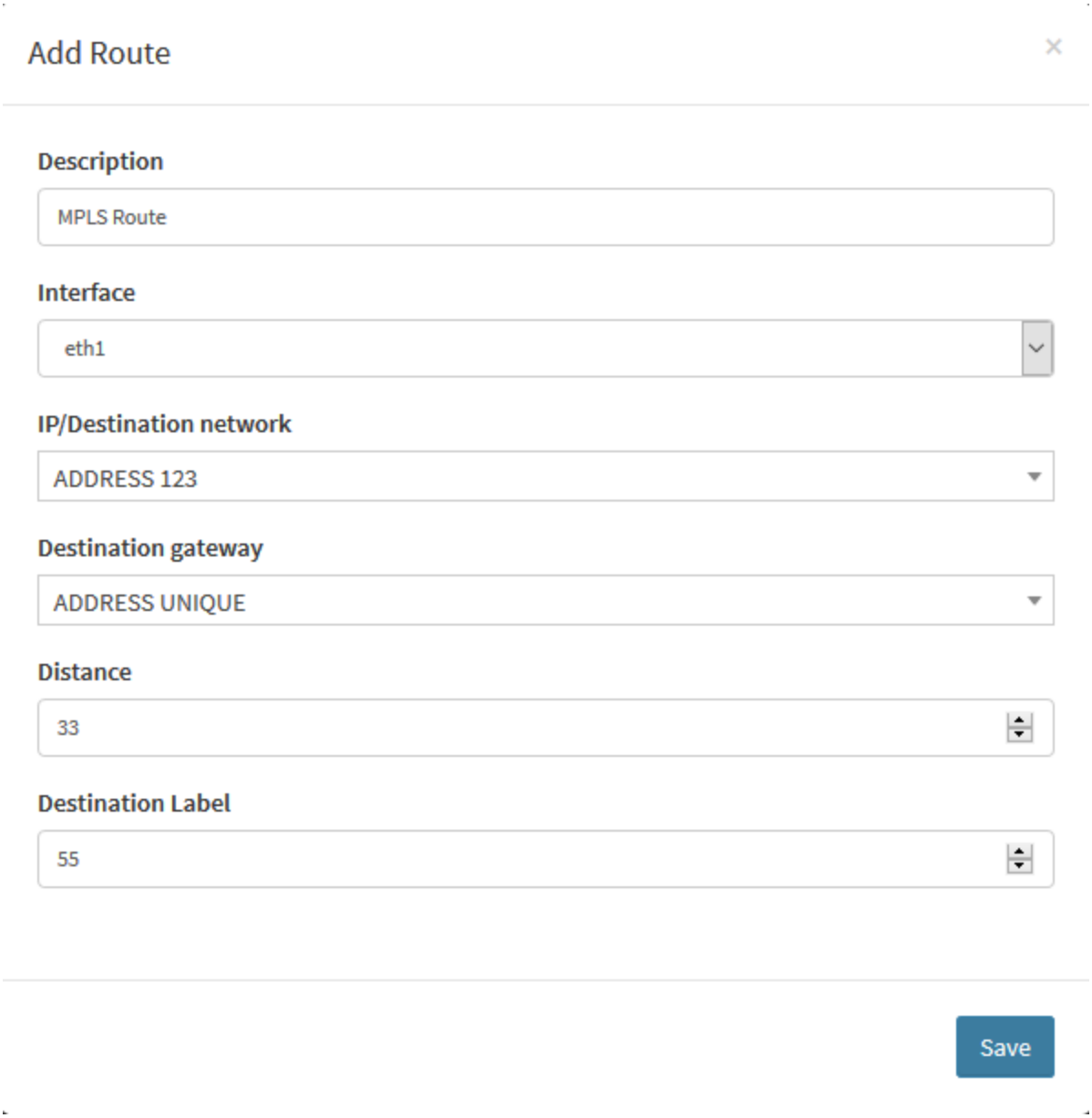
Static Routing

To add a route, click **Add Route [ ]** in **[IPv4]** and / or **[IPv6]** respectively.



Static Routing - Add Route

Configure all fields as described on the page, after completing the settings, pay attention to the Destination Label field, as shown below:



Static Routing - Add route

- ***Destination Label*:** This field will appear ONLY if the selected interface already has MPLS enabled. To configure it on the physical interfaces, just follow the instructions above. Enter the MPLS destination label. The default value accepted in this field is 1, the minimum value is 1 and the maximum value is 65535.

To save the changes, click **Save [** Save **]**, otherwise, click the **[** **]** at the top of the window or click outside it to cancel the procedure.

After saving, you will need to access the **command queue [** **]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

This finalizes the configuration of the MPLS protocol.

For more information on how to configure a physical interface, visit this page.

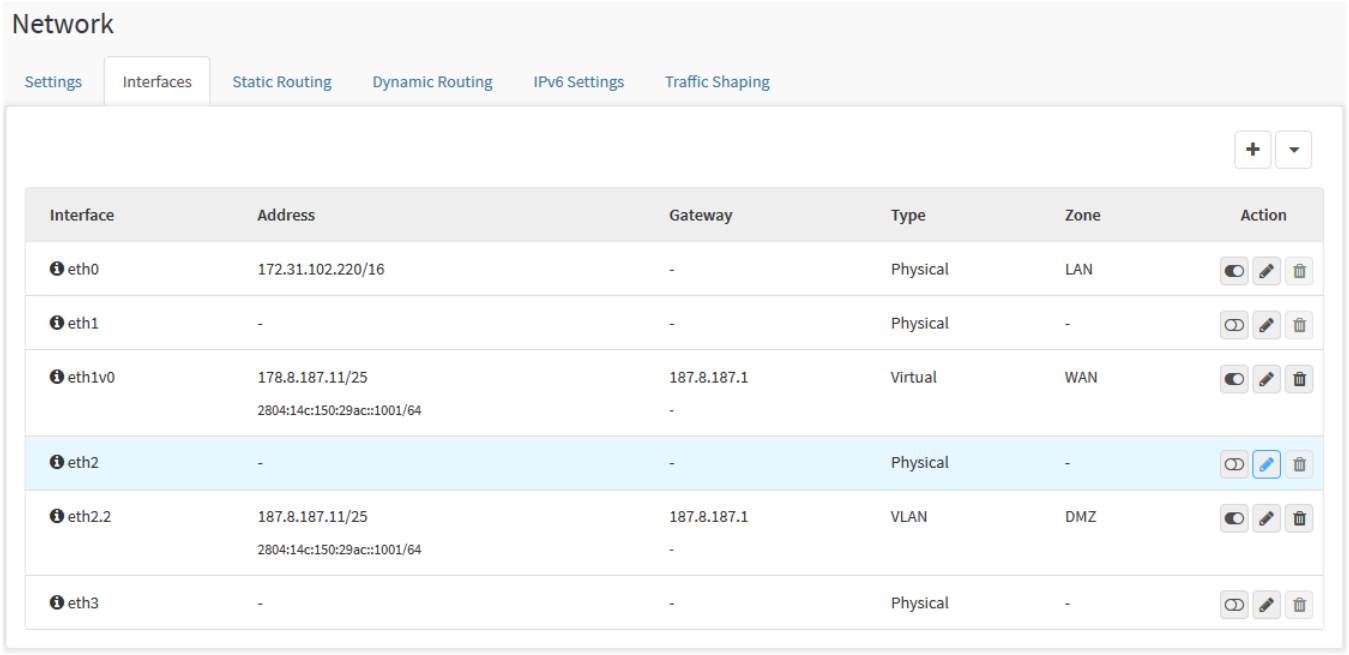
If you want to see how the interface panel is structured, see this page.

Interfaces - Ethernet Interface

Standard “Ethernet” physical interfaces are automatically identified by the system.

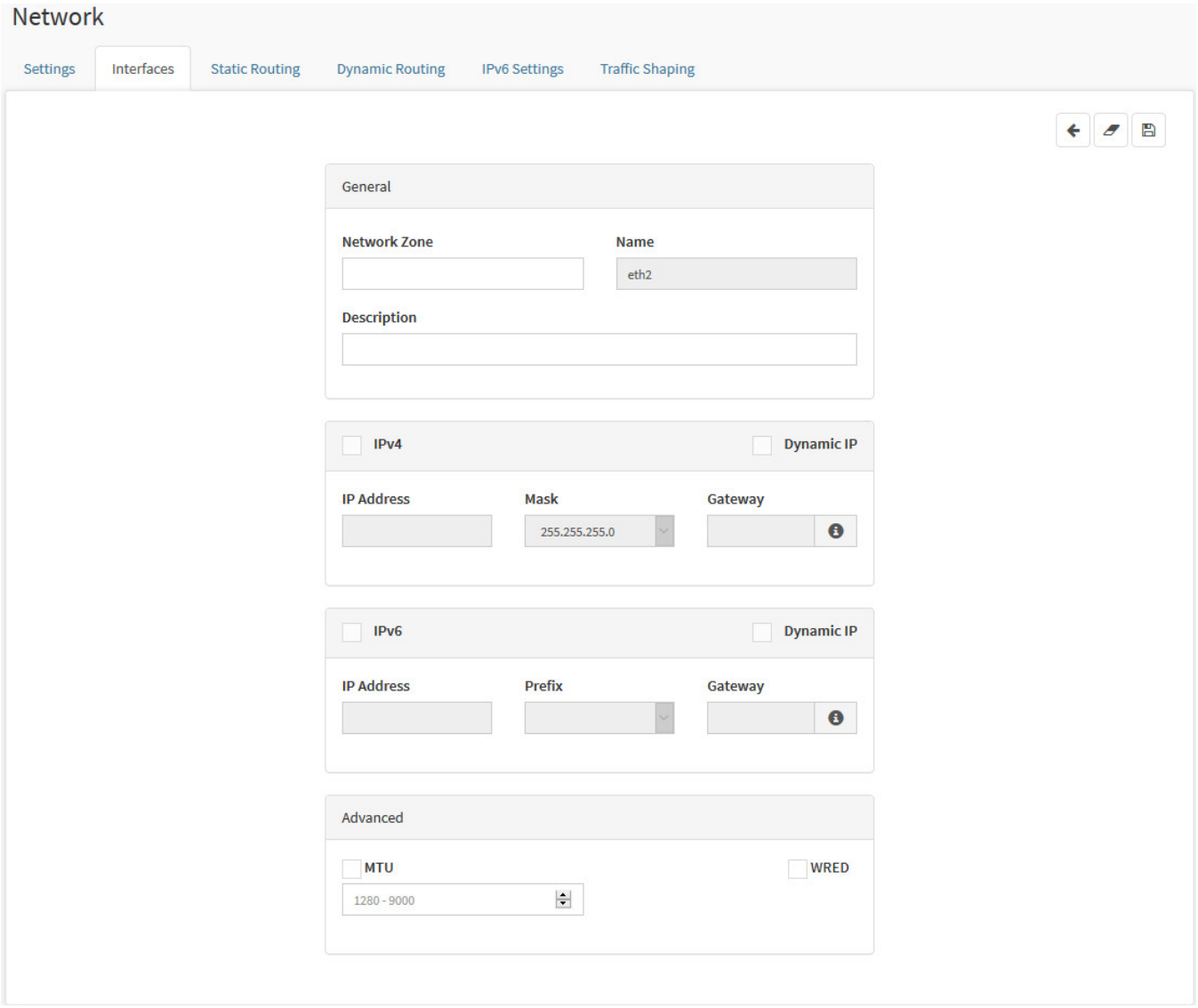
To configure a physical interface, follow the steps below:

Click **edit [ ]** in the corresponding interface. Ex.: *“Eth2”.*



Interfaces - Network edit Interfaces

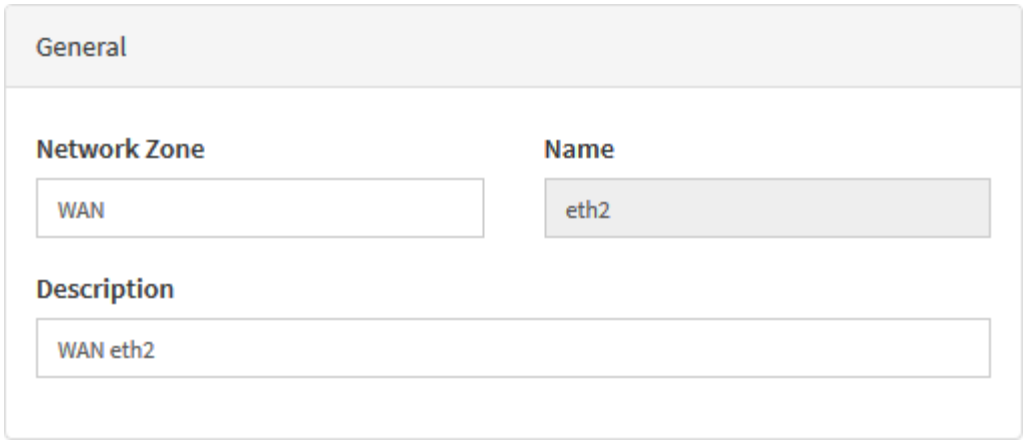
The following screen will appear:



Interface Ethernet - Edit Interfaces

Configure it according to the specifications of the respective fields, as shown below:

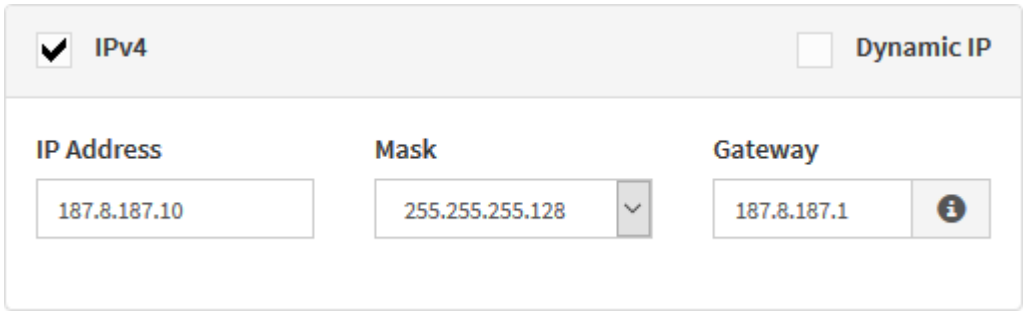
General



Interface Ethernet - General

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Enter “WAN” and select it from the list;
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “[eth2]”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: “WAN eth2”.

IPv4

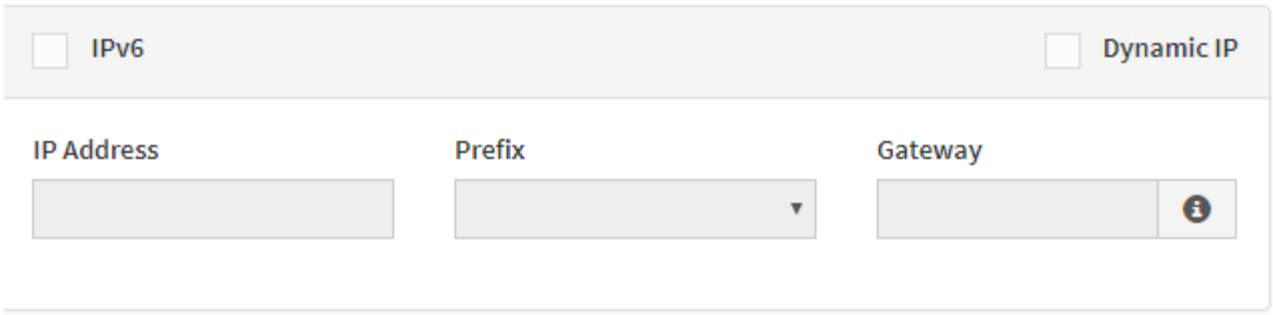


Interface Ethernet – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]*:*** This check box is used to determine whether the IP will be automatically configured by DHCP*;*
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *“187.8.187.10”*;
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is a mandatory requirement*. Ex.: “255.255.255.128”;
- ***Gateway:*** *Defines the gateway address corresponding to the network*. This is a NOT mandatory requirement. Ex.: *“187.8.187.1”.*

IPv6



Interface Ethernet – IPv6

To enable the IPv6 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]*:*** This check box is used to determine whether the IP will be automatically configured by DHCP*;*
- ***IP Address*:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement;
- ***Prefix*:** Select the prefix corresponding to the IPv6 addressing*. This is a mandatory requirement*;
- ***Gateway*:** Defines the gateway address corresponding to the network. This is a NOT mandatory requirement.

Advanced

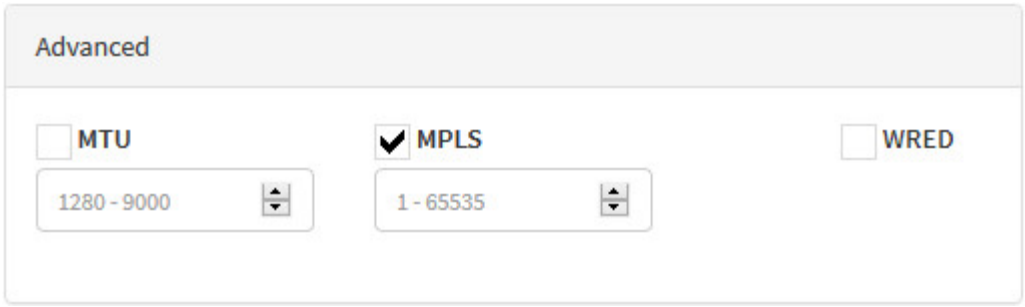
There is a limit on the size of data transmitted over a network that limits the number of bytes that can be transmitted in a single packet. This limit, which is a characteristic of the link layer, is known as MTU ("Maximum Transmission Unit" or "Maximum Transmission Unit") and exists on several types of networks, not just on local Ethernet networks.

Below is a reference table of the standard MTU value for some types of networks.

Network	MTU (in bytes)
***WLAN* 802.11**	7981
Ethernet Jumbo Frames	1501 - 9198
Token *Ring* 802.5	4464
FDDI	4352
Ethernet	1500
IEEE 802.3 / 802.2	1492
PPPoE	1492

Protocol table x MTU

Here is more information about the Advanced panel:



Interface Ethernet – MTU

In a Physical interface it is possible to define the MTU (Maximum Transmission Unit), enable and configure the MPLS label:

- ***MTU[ ]*:** To enable this option, mark the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (*JUMBO FRAME*);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

- **MPLS*[ ]*:** When you enable this option, support for the MPLS protocol will be enabled, and you can route packets over both IPv4 and IPv6. When the check box is enabled, the text box below will allow the definition of the destination label, and the possible value to be entered in this field is from 1 to 65535**.** For more information about MPLS, see this page.

The activation of MPLS is not available in older versions of the NGFW as their version of the Kernel does not support the protocol.

- **WRED*[ ]*:** When enabled, the WRED will selectivelly discard traffic packages before the interface queue is full. This will make band usage more efficient and lessen latency and package loss during peak traffic.

  If you want to delete all the settings made on this interface, click ***Erase*[ ]**.

WARNING: The ***Erase*[ ]** button will erase all interface settings. Under no circumstances should the settings be applied in the **command queue[ ]** without first configuring the interface. If it is not displayed on this panel, access the "Settings" tab and click the ***Update Software Information* [ ]** button to return to viewing the interface and being able to edit it.

Blockbit NGFW will automatically create host and network objects with IPv4, IPv6 and their masks addresses. Those can be configured in their respective fields.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [**  **]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures the interface will have been successfully configured.

For more information on how to configure a 3G / 4G / LTE interface, visit this page.

For more information on MPLS, see this page.

Interfaces - 3G / 4G / LTE connection

In view of the importance of keeping the network always available and operational efficiency, some Blockbit appliances have built-in 3G / 4G / LTE module, providing connectivity to the mobile network infrastructure and allowing compatible appliances to have access. This solution is particularly useful in operations established in regions with unstable network performance, the feature aims to be used as a cost-effective alternative or also serving as a contingency network to guarantee availability in case of any unforeseen or bottleneck in the network.

This feature is available for use in internet access, static, dynamic routing policies, VPN and mainly in SD-WAN. If the appliance has a module installed, the graphical interface will automatically detect it allowing its configuration.

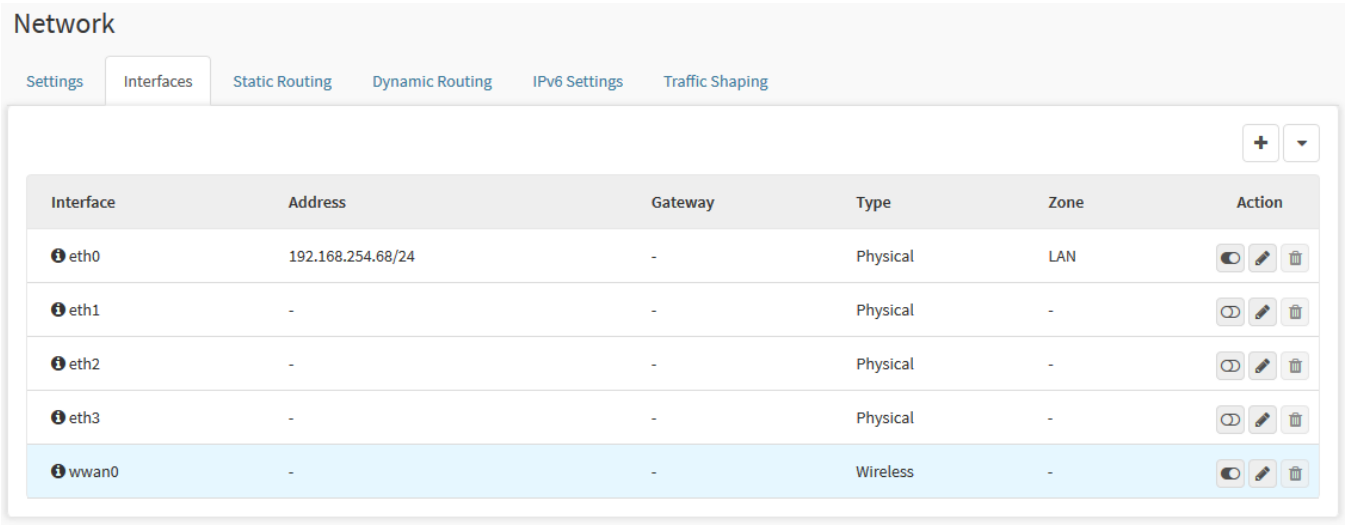
For more information regarding the current status of the 3G / 4G / LTE connection use the [show-wwan] command;

If the Appliance has 3G / 4G / LTE support, the interface will be automatically detected.

Multiple Modems

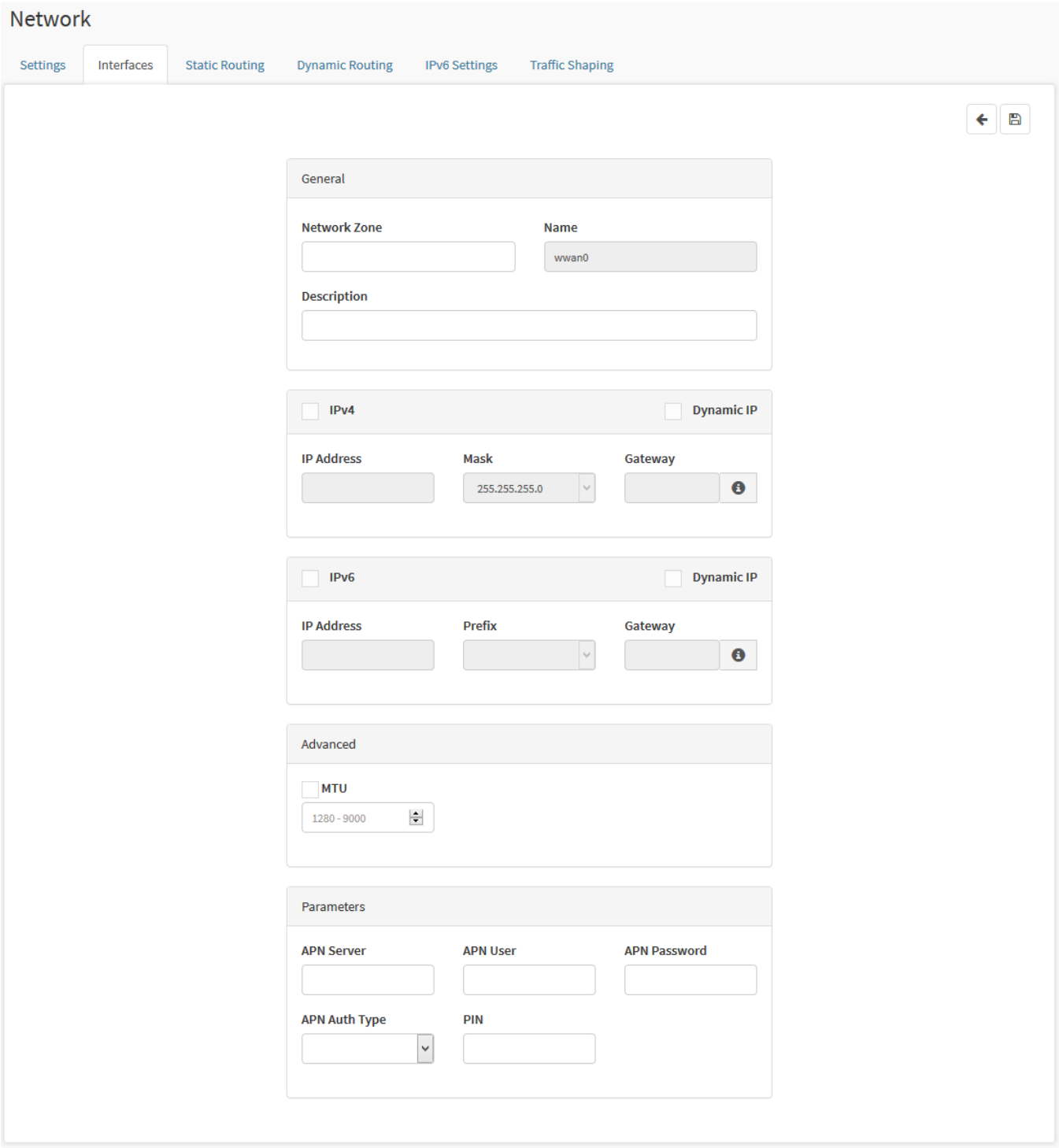
Some of the Blockbit appliances support the use of multiple (2 or more) modems. Those are instantly detected when pluged in, as network interfaces, and are used for a better performance of the internet link.

Click **edit [ ]** on the WWAN0 interface.



Interfaces - Edit network interfaces

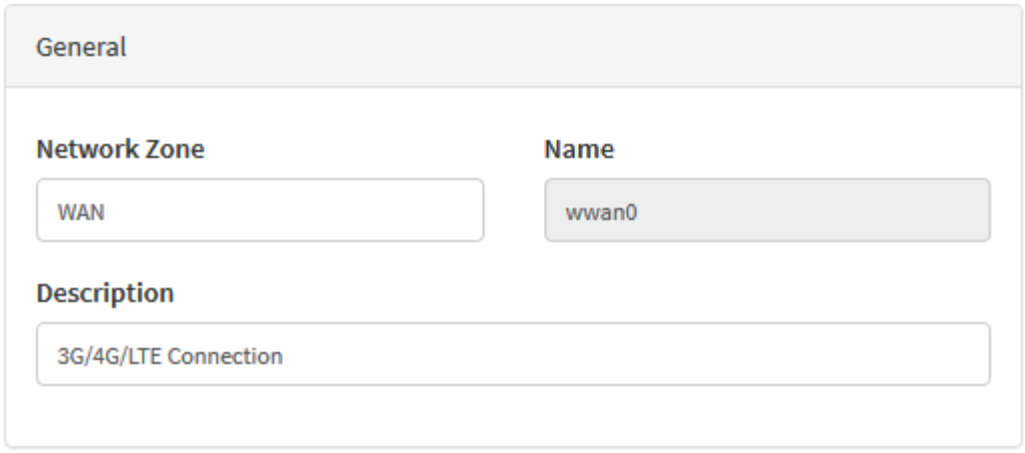
The following screen will appear:



Interface 3G/4G/LTE - Edit Interfaces

Configure it according to the specifications of the respective fields, as shown below:

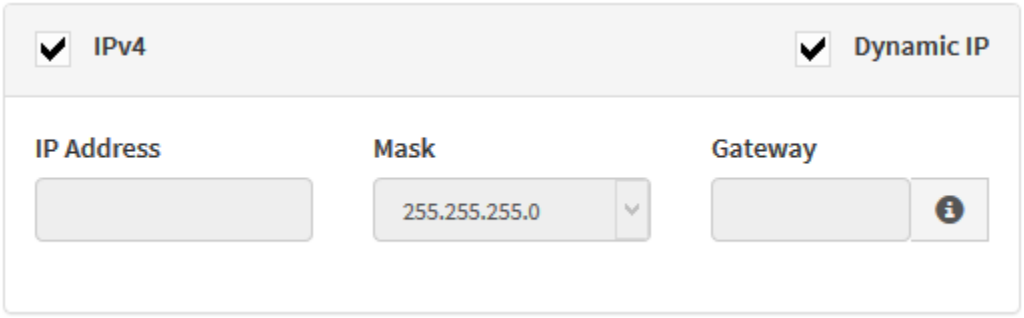
General



Interface 3G/4G/LTE - General

- ***Network Zone*:** This field refers to the definition of the kind of interfaces' grouping . By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Enter “WAN” and select it from the list;
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “wwan0”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. E.g: “3G / 4G / LTE Connection”.

IPv4

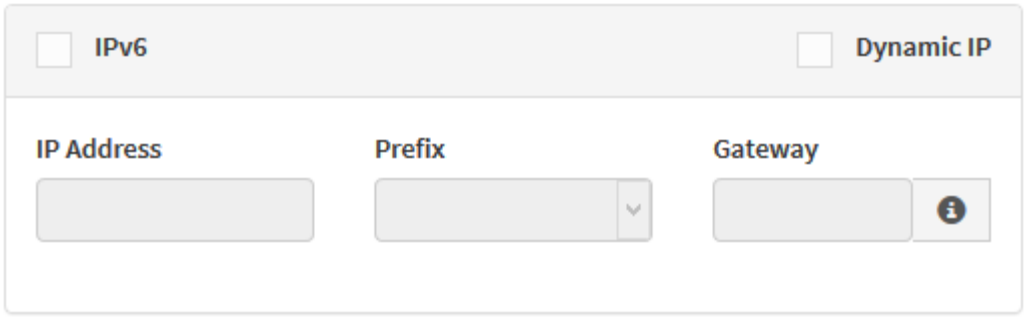


Interface 3G/4G/LTE – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]*:*** This check box is used to determine whether the IP will be automatically configured by the DHCP. *By checking this checkbox, the fields below will be disabled*;
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement;
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is not a mandatory field*;
- ***Gateway:*** Defines the network's gateway address. This is not a mandatory field.

IPv6



Interface 3G/4G/LTE – IPv6

To enable the IPv6 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]*:*** This check box is used to determine whether the IP will be automatically configured by DHCP. *By checking this checkbox, the fields below will be disabled;*
- ***IP Address*:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement;
- ***Prefix*:** Select the prefix corresponding to the IPv6 addressing. *This is a mandatory requirement*;
- ***Gateway*:** Defines the gateway address corresponding to the network. This is a NOT mandatory requirement.

Advanced

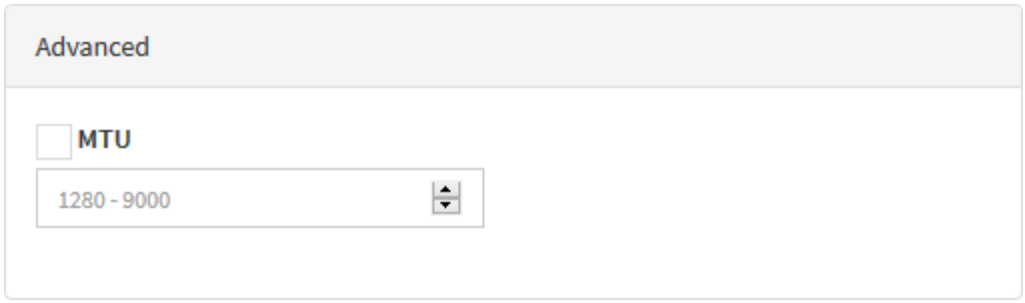
There is a limit on the size of data transmitted over a network that limits the number of bytes that can be transmitted in a single packet. This limit, which is a characteristic of the link layer, is known as MTU ("Maximum Transmission Unit" or "Maximum Transmission Unit") and exists in several types of networks.

Below is a reference table of the standard MTU value for some types of networks.

Network	*MTU* (in bytes)
***WLAN* 802.11**	7981
Ethernet Jumbo Frames	1501 - 9198
Token *Ring* 802.5	4464
FDDI	4352
Ethernet	1500
IEEE 802.3 / 802.2	1492
PPPoE	1492

Protocol table x MTU

Here is more information about the Advanced panel:



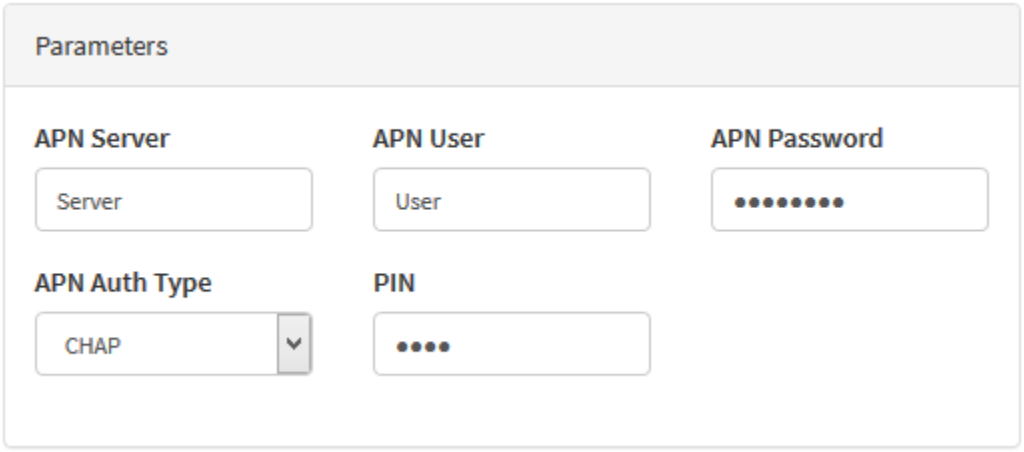
Interface 3G/4G/LTE – MTU

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

Parameters

In this panel the parameters of the 3G / 4G / LTE network are configured. The data in this panel is dynamic, so before configuring these fields, contact your operator for more information.



Interface 3G/4G/LTE – Parameters

Below we will describe the function of each of the fields in this panel.

WARNING: Bearing in mind that the parameters are different according to your access provider, confirm the data with the support of your operator before configuring them in this panel.

- ***APN Server:*** Defines the server name*;*
- ***APN User*:** Determines the user to be used by the server;
- ***APN Password*:** Sets the user password;

- ***APN Auth Type*:** In this field, the type of authentication protocol to be used is determined, which can be:
  - **PAP**;
  - **CHAP**;
  - **MSCHAP**.
- ***PIN*:** Determines the PIN number that will be used by the 3G / 4G / LTE interface.

To see examples of how to register the parameters of the main operators, see this page.

If you want to delete all the settings made on this interface, click ***Erase*[ ]**.

WARNING: The ***Erase*[ ]** button will erase all interface settings. Under no circumstances should the settings be applied in the **command queue [ ]** without first configuring the interface. If it is not displayed on this panel, access the "Settings" tab and click the ***Update Software Information* [ ]** button to return to viewing the interface and being able to edit it.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

By performing these procedures, the interface will have been successfully configured.

For more information on how to configure a physical interface, visit this page.

To see the configuration parameters of the main operators, visit this page.

Examples - 3G / 4G / LTE Connection Parameters

Next, we will exemplify the registration of some examples of parameters for the main Brazilian ISPs. The model presented is intended to serve only as a guide, as these data are dynamic and can be changed.

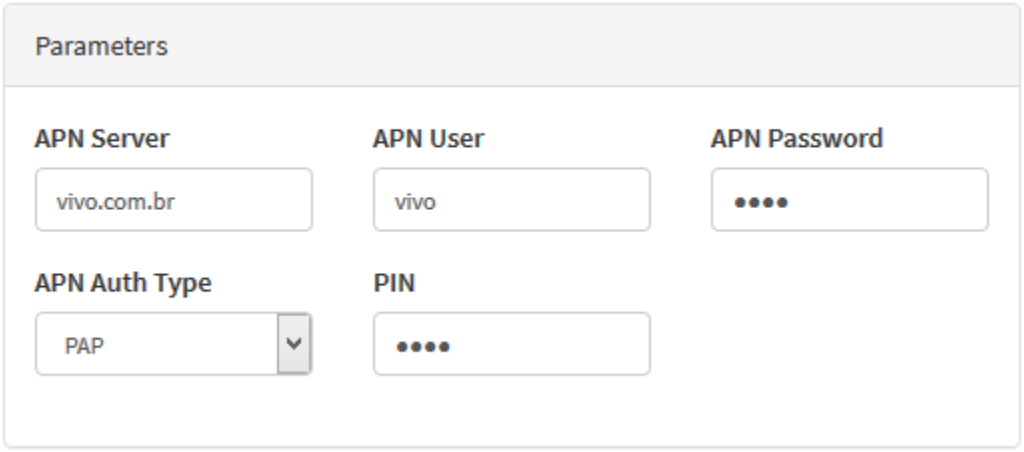
WARNING: Since the parameters are different according to your service provider, confirm the data with the support of your operator before configuring them in the parameters panel.

We will carry out the demonstration using the following Service Providers:

- Example 1 - Vivo;
- Example 2 - Tim;
- Example 3 - Oi;
- Example 4 - Claro.

These parameters were collected on 08/06/2020.

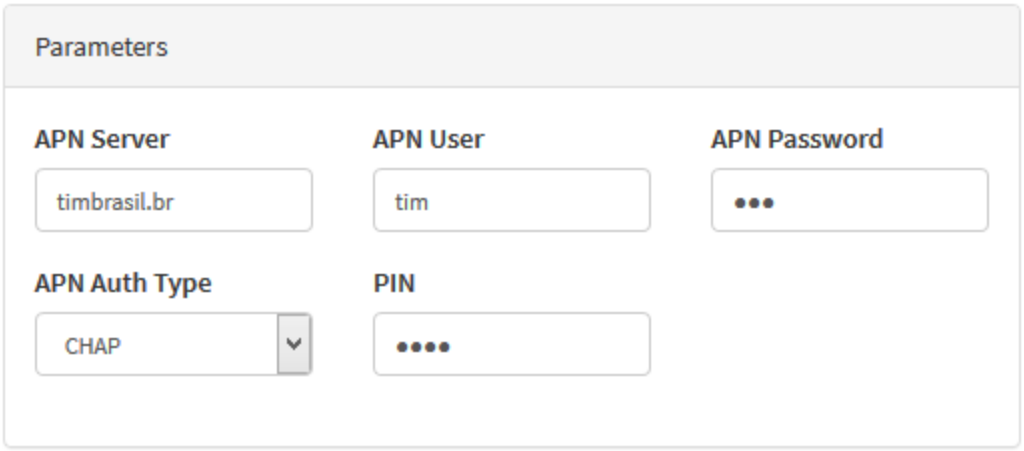
Example 1 - Vivo



Example 1 – Vivo

- ***APN Server:*** vivo.com.br*;*
- ***APN User*****:** vivo;
- ***APN Password*****:** vivo;
- ***APN Auth Type*****:** PAP;
- ***PIN*****:** 1010.

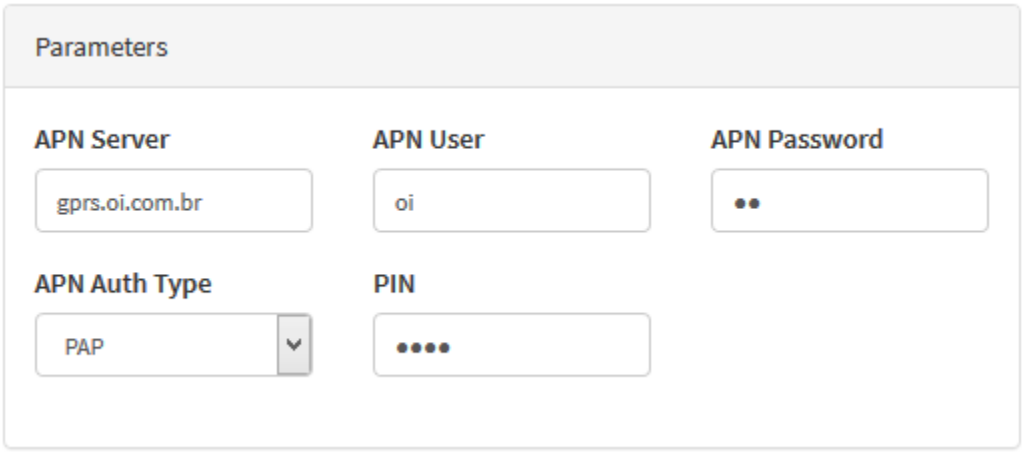
Example 2 - Tim



Example 2 – Tim

- ***APN Server:*** timbrasil.br*;*
- ***APN User*****:** tim;
- ***APN Password*****:** tim;
- ***APN Auth Type*****:** CHAP;
- ***PIN*****:** 1010.

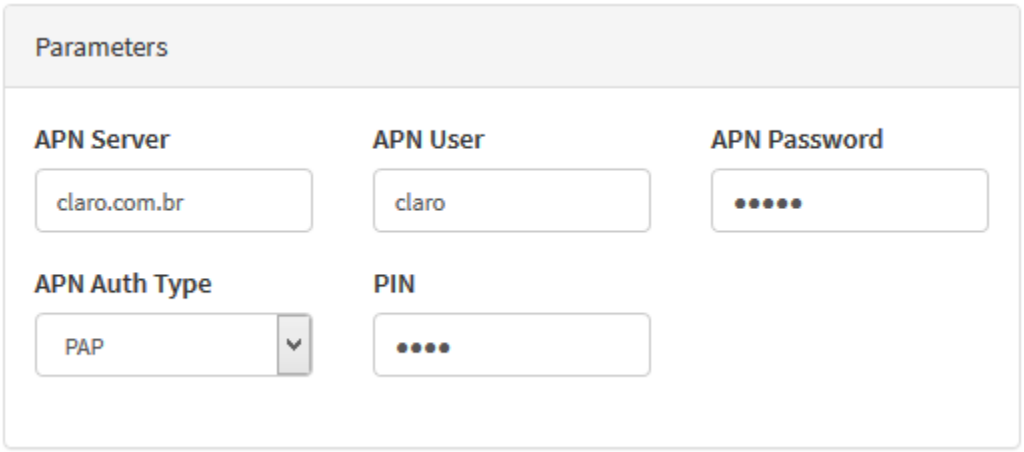
Example 3 - Oi



Example 3 – Oi

- ***APN Server:*** gprs.oi.com.br*;*
- ***APN User*****:** oi;
- ***APN Password*****:** oi;
- ***APN Auth Type*****:** PAP;
- ***PIN*****:** 8888.

Example 4 - Claro



Example 4 – Claro

- ***APN Server:*** claro.com.br*;*
- ***APN User*****:** claro;
- ***APN Password*****:** claro;
- ***APN Auth Type*****:** PAP;
- ***PIN*****:** 3636.

For more information on how to configure the other panels, check this page.

For more information on 3G / 4G / LTE, visit this page.

For more information on adding interfaces, visit this page.

Interfaces - Add Button

A local virtual network usually named VLAN, is a logical independent network. Several VLANs are able to coexist in a single "switch", as to segment a local (physical) network in "N" virtual networks, creating multiple separated broadcast domains. A VLAN also makes it possible to put into a single broadcast domain, hosts with distinct physical locations and connected to different switches. Another purpose of a virtual network is to restrict access to network resources without considering the networks' physical topology.

By many reasons (network organization, performance, privacy, safety, etc.) it is frequently necessary to segment an organization's network into several "networks/sub-networks", in other words, it is necessary to segment the broadcast domains.

The Blockbit NGFW supports the addition of virtual interfaces of the "VLAN" type, and mandatorily requires a free physical interface **[EthX]**, which increases the capacity of your Blockbit NGFW device keeping its performance and the security of your network. The VLANs use ID tags to logicaly separate devices in a network with broadcast domains segmented by a VLAN. These minor domains forward packets only to devices that are a part of this VLAN domain. This reduces the traffic and increases the network security.

Supported VLAN interfaces:

- **DOT.1Q Protocol**: IEEE 802.1Q Standard;
- ***ID Tags*:** ID 0 - 4096;
- ***VLAN ID* 1 – *ID* 4094:** Interval of allowed *ID*s to group up IP addresses of the same network/sub-network;
- ***VLAN ID* 0 (zero):** It is only used for high priority frames;
- ***VLAN ID* 1 (one):** Corresponds to *VLAN default*. Usually used as main or single bus;
- ***VLAN ID* 4095:** *Reserved ID VLAN* . It is used for VLAN grouping;
- ***IEEE 802.1p:*** Used to determine the service class in the Ethernet structure.

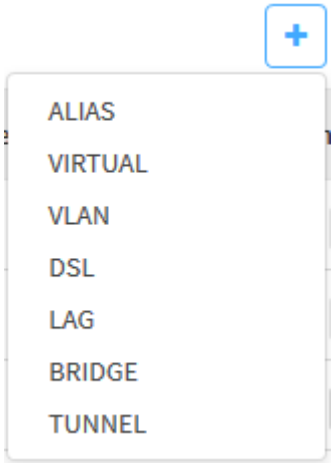
The *VLAN* uses the *IEEE 802.1Q* standard and all the commutation devices (switches) layer 2 and 3 along a route must be compatible with the 802.1 Q protocol, in order to support the VLAN traffic.

In order to configure a VLAN interface, follow the next steps:

At the top right of the screen we have the Add Interface button:

Interfaces – Add Interface button

By clicking on this button the menu below is displayed:



Interfaces – Add Interface button - *Menu*

The menu consists of the options:

- *ALIAS;*
- *VIRTUAL*;
- *VLAN*;
- *DSL*;
- *LAG*;
- *BRIDGE*;
- *TUNNEL*.

Below we will analyze each option in detail.

For more information on how to configure 3G / 4G / LTE interfaces, visit this page.

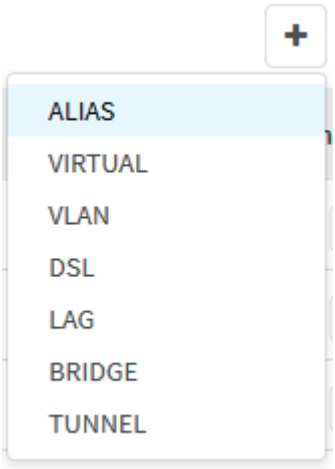
For more information on the action menu, visit this page.

Adding Interfaces - ALIAS

The ALIAS option has the basic function of associating more than one network IP to the same interface, this option basically acts using the settings that have already been made in a network interface as a basis to create the ALIAS.

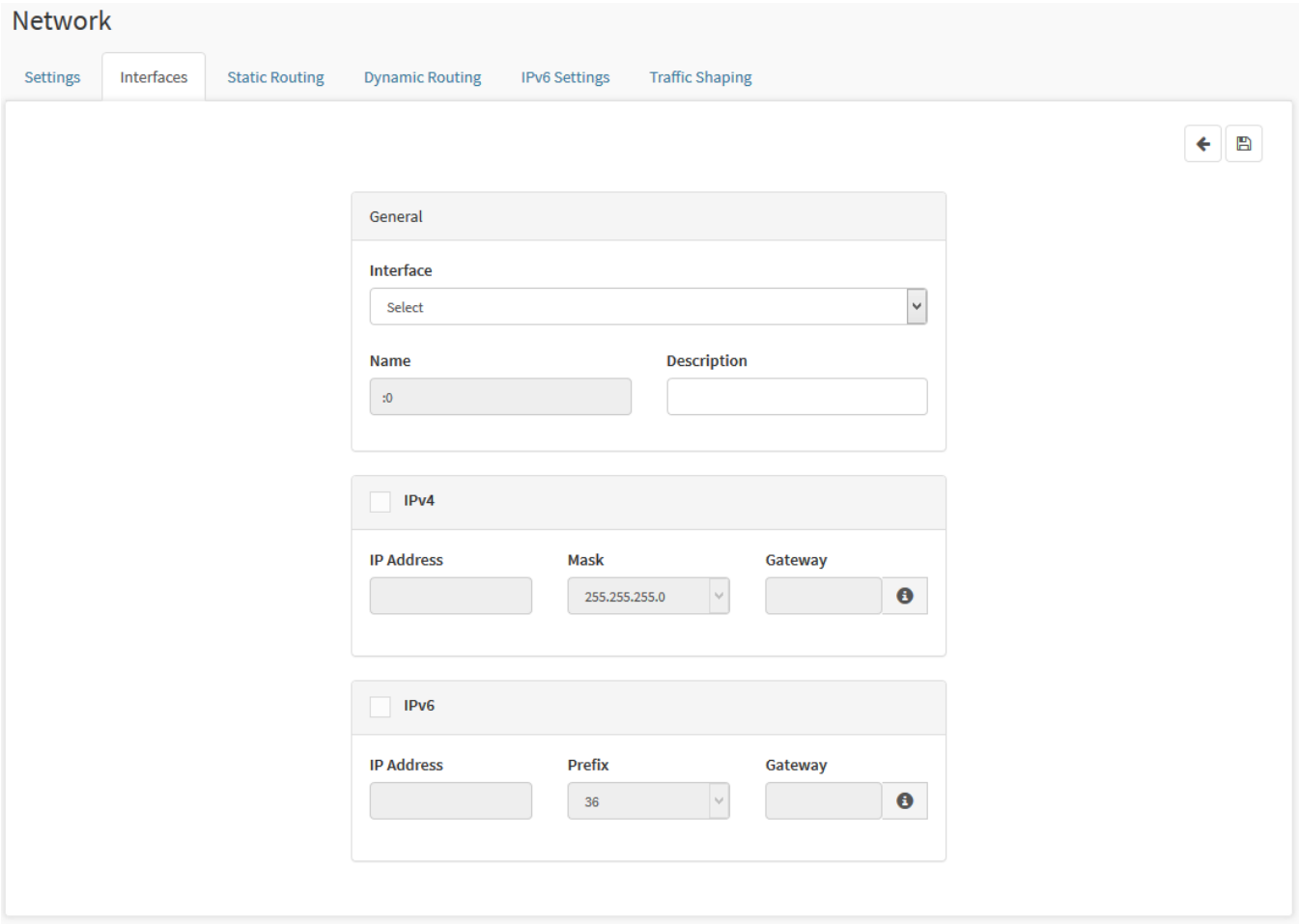
To configure an ALIAS interface, follow the steps below:

Click on **[** **]** and select the **[ALIAS]** option:



Add Interface Interface - Menu - Virtual

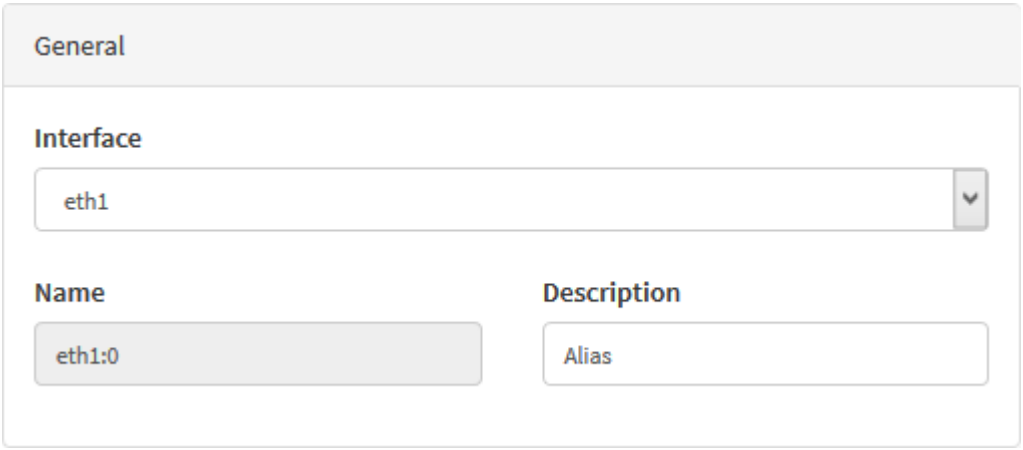
The following screen will appear:



ALIAS Interface - Virtual Interface Creation

Configure it according to the specifications of the respective fields, as shown below:

General

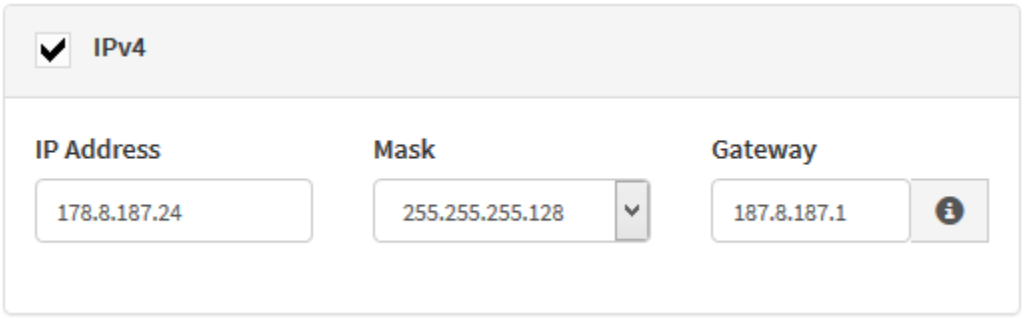


ALIAS of the Interface – General

- **Interface:** In this selection field it is possible to define the desired interface. Ex.: "*eth1"*;

- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: "*Eth1:0*";
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: "*Alias*".

IPv4

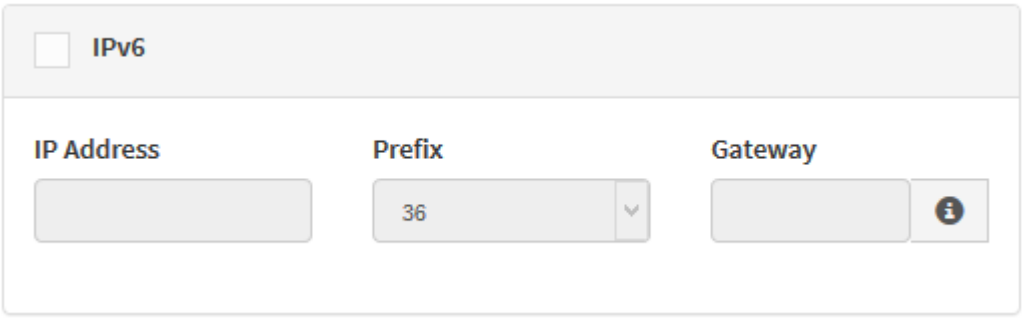


Interface Virtual – *IPv4*

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"187.8.187.24";*
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is a mandatory requirement*. Ex.: *"255.255.255.128";*
- ***Gateway*:** Defines the gateway address corresponding to the network. This is a NOT mandatory requirement. Ex.: *"187.8.187.1".*

IPv6



Interface Virtual – *IPv6*

If you want to enable the IPv6 addressing standard, check the checkbox ***[ ]*** at the top of the panel and configure the form with the corresponding data for each field.

- ***IP Address*:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement;
- ***Prefix*:** Determines the prefix corresponding to the IPv6 addressing. This is a mandatory requirement;
- ***Gateway*:** Defines the gateway address corresponding to the network. This is a NOT mandatory requirement.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [**  **]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures the interface will have been successfully configured.

Next we will analyze how to add a Virtual interface.

For more information on adding other types of interfaces, visit this page.

Adding Interfaces - Virtual (MAC VLAN)

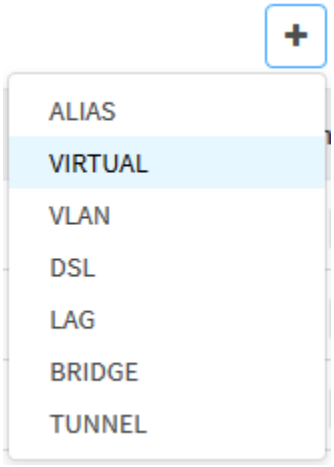
The Blockbit NGFW supports adding virtual interfaces of the “MAC VLAN” type, and requires a physical interface **[*EthX*]**.

A network interface can have several IP addresses, including for different logical network segments, but they do not isolate traffic, which can be "identified" or "intercepted" on this interface.

In a MAC VLAN, a single network interface is assumed and allows the creation of multiple virtual addresses with different MACs, that is, “N for 1”. A MAC VLAN can only see traffic that has a MAC address corresponding to the interface, preventing other virtual interfaces from "identifying" or "intercepting" traffic destined for another MAC VLAN.

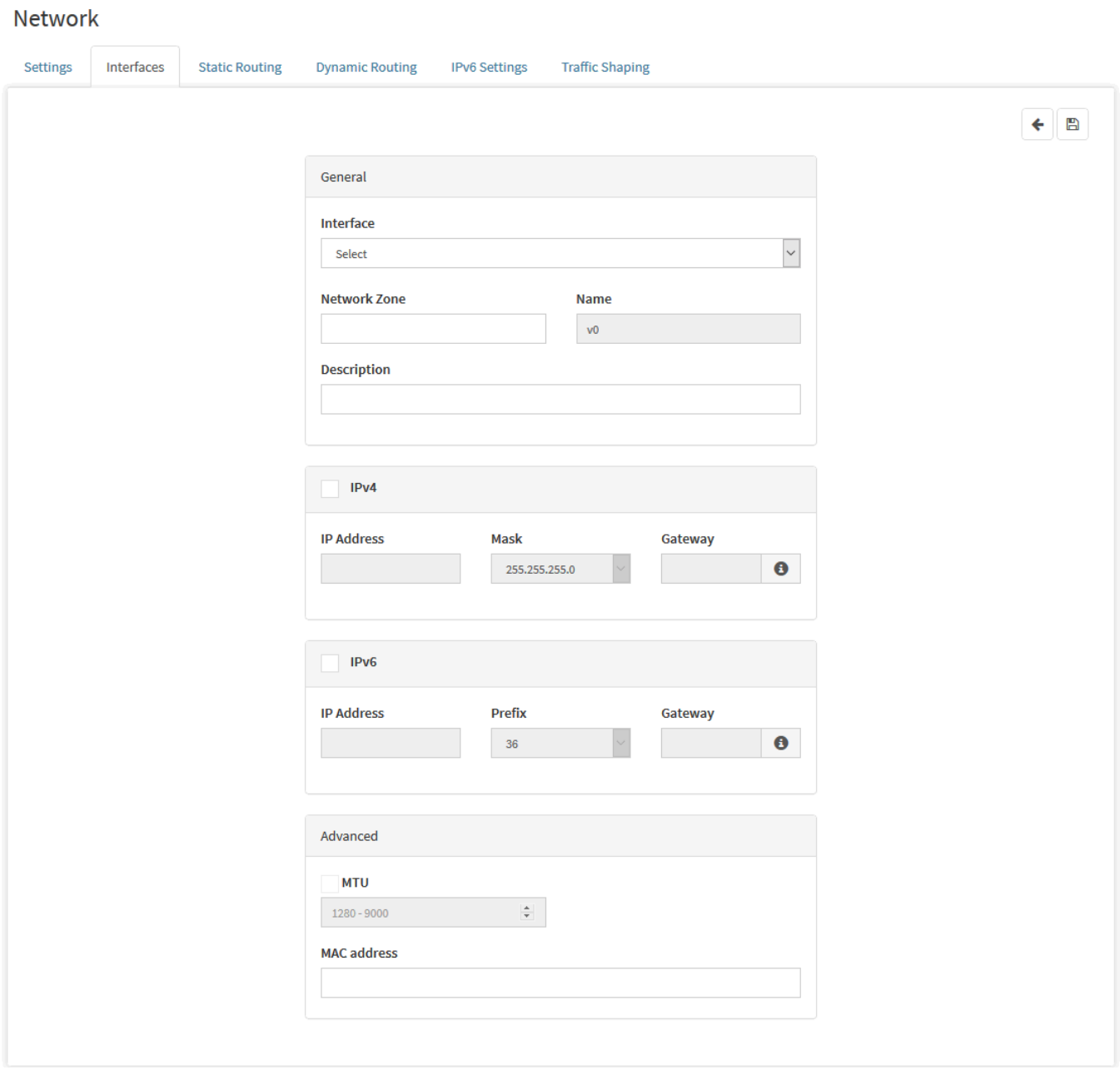
To configure a Virtual interface, follow the steps below:

Click on **[**  **]** and select the **[VIRTUAL]** option:



Add Interface Interface - Menu - Virtual

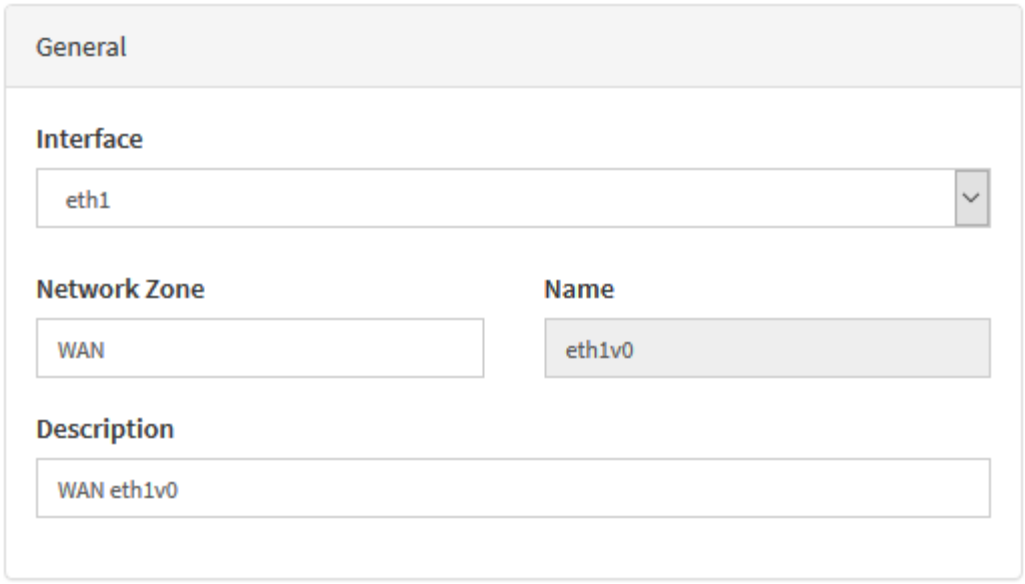
The following screen will be displayed:



Interfaces - Virtual Interface Creation

Configure it according to the specifications of the respective fields, as shown below:

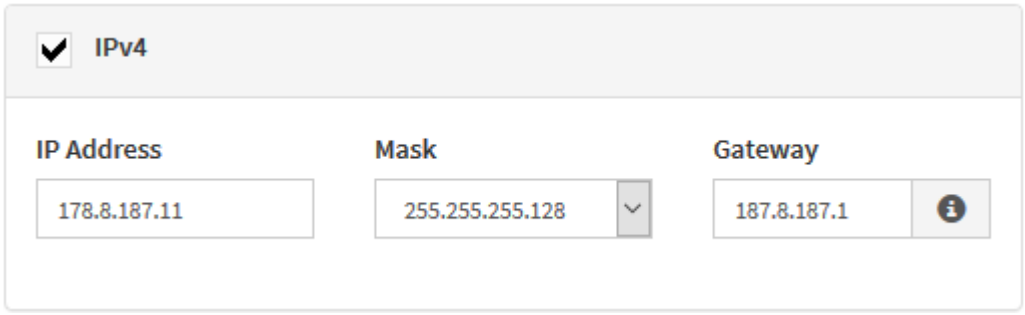
General



Interface Virtual – General

- **Interface:** In this selection field it is possible to define the desired interface. Ex.: *eth1*;
- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the "WAN", "LAN" and "DMZ" zones. This is a mandatory requirement. Ex.: Enter "WAN" and select it from the list*;*
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: "[*Eth1v0*]";
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: "*Wan eth1v0*".

IPv4

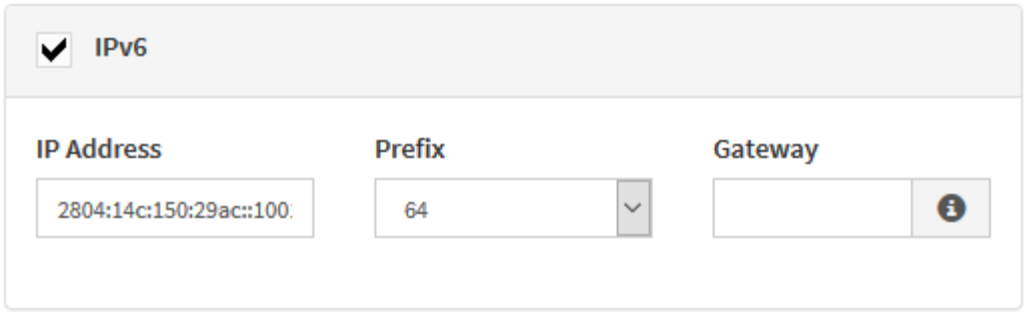


Interface Virtual – *IPv4*

To enable the default for IPv4 addressing, check the checkbox **[ ]** at the top of the panel and configure the form with the corresponding data for each field.

- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"187.8.187.11";*
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing*. This is a mandatory requirement*. Ex.: *"255.255.255.128";*
- ***Gateway*:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement. Ex.: *"187.8.187.1".*

IPv6

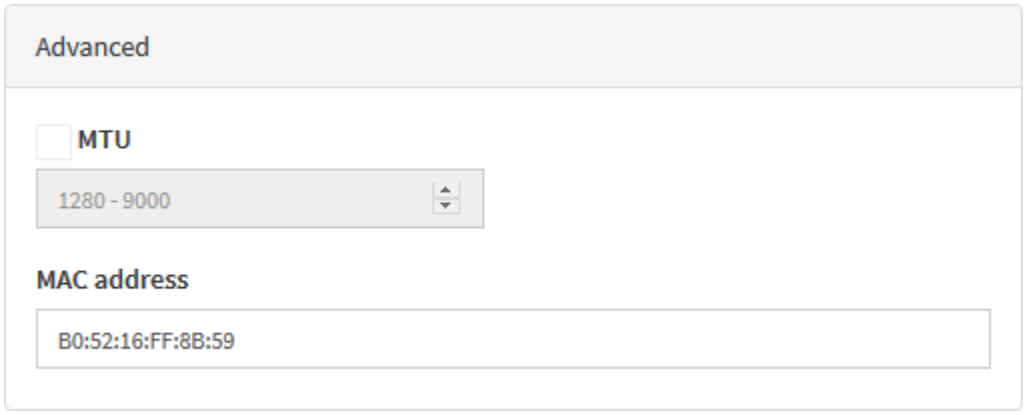


Interface Virtual – *IPv6*

To enable the IPv6 addressing standard, check the ***[ ]*** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***IP Address*****:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement. Ex.: “2804:14c:150:29ac::1001”;
- ***Prefix*****:** Determines the prefix corresponding to the IPv6 addressing. This is a mandatory requirement. Ex.: “64”;
- ***Gateway*****:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement.

Advanced



Interface Virtual – *Advanced*

In a Virtual interface it is possible to define the MTU (Maximum Transmission Unit) and change the MAC address. Following details of each field:

- ***MTU[ ]*****:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

- ***MAC address*****:** In this field it is possible to change the MAC address of the virtual interface, if no address is defined, the system will automatically generate one. *This is a NOT mandatory requirement*.

To save changes, click **Save [ ]**, otherwise click ***Back*****[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [**  **]** and apply the changes made. For more information about the command queue visit the page: UTM - COMMAND QUEUE.

After performing these procedures the interface will have been successfully configured.

Next, we'll look at how to add a VLAN interface.

For more information on adding other types of interfaces, visit this page.

Adding Interfaces - VLAN

A virtual local area network, usually called a VLAN, is an independent logical network. Several VLANs can coexist on the same “switch”, in order to segment a local (physical) network into “N” virtual networks, creating multiple separate broadcast domains. A VLAN also makes it possible to place hosts with different physical locations and connected to different switches in the same broadcast domain. Another purpose of a virtual network is to restrict access to network resources without considering the physical topology of the network.

For various reasons (network organization, performance, privacy, security, etc.) it is often necessary to segment an organization's network into several “networks / subnets”, that is, it is necessary to segment broadcast domains.

The Blockbit NGFW supports the addition of virtual interfaces of the “VLAN” type, and mandatorily requires a free physical [EthX] interface, which increases the capacity of your Blockbit NGFW device while maintaining its performance and the security of your network. VLANs use ID tags to logically separate devices on a network with broadcast domains targeted by the VLAN. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

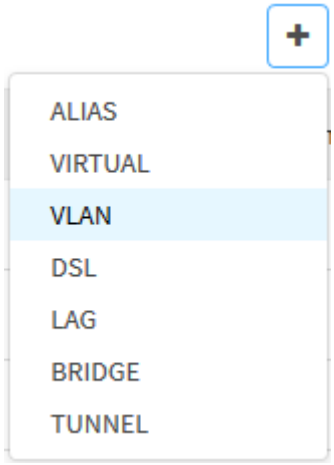
Supported VLAN interfaces:

- **DOT.1Q Protocol**: IEEE 802.1Q standard;
- ***Tags ID*:** ID 0 - 4096;
- ***VLAN ID* 1 – *ID* 4094:** Range of ID’s allowed to group IP addresses of the same network / subnet;
- ***VLAN ID* 0(zero):** It is used only for high priority frames;
- ***VLAN ID* 1(um):** Corresponds to the default VLAN. Usually used as main or single bus;
- ***VLAN ID* 4095:** Reserved VLAN ID. It is used for VLAN teaming.

The VLAN uses the IEEE 802.1Q standard and all layer 2 and 3 switches along a route must be compatible with the 802.1Q protocol to support VLAN traffic.

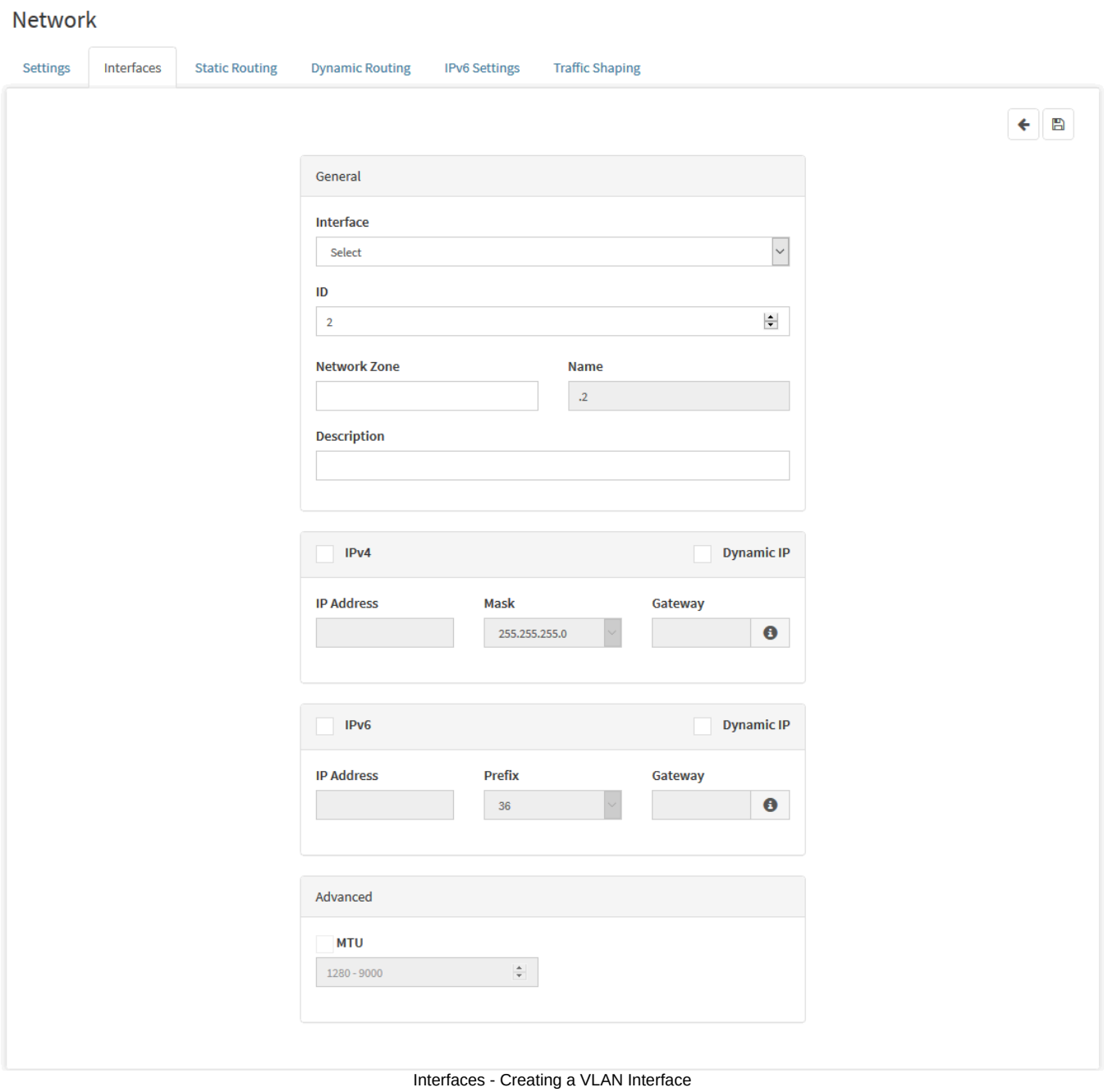
To configure a VLAN interface, follow the steps below:

Click on **[** **+** **]** and select the **[*VLAN*]** option:



Add Interface Interface - Menu - VLAN

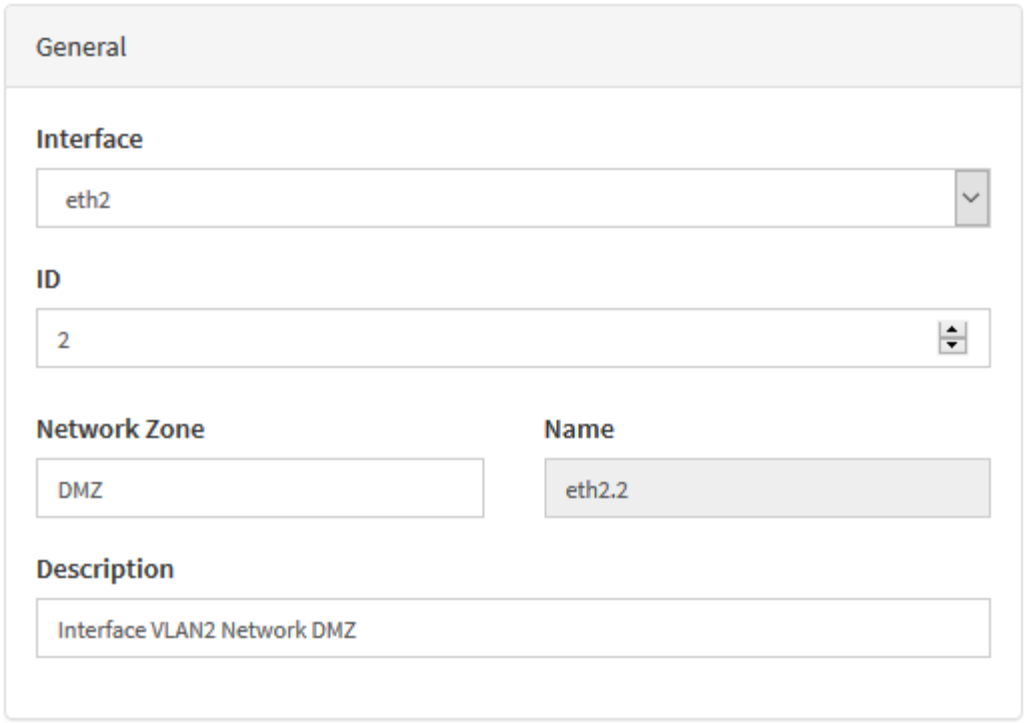
The following screen will appear:



Interfaces - Creating a VLAN Interface

Configure it according to the specifications of the respective fields, as shown below:

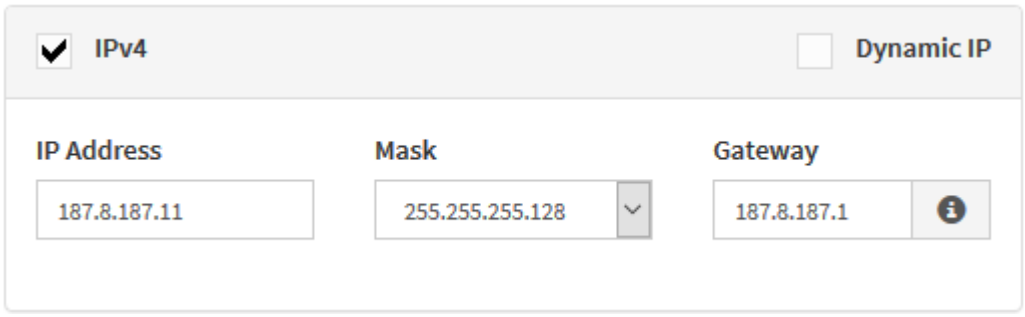
General



VLAN Interface - General

- **Interface:** In this selection field it is possible to define the interface where the VLAN will be configured. Ex.: eth2;
- ***ID*:** Defines the VLAN ID to be configured. Ex.: 2;
- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Enter “WAN” and select it from the list;
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “[eth2.2]”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: “Interface *VLAN2 Network DMZ*”.

IPv4

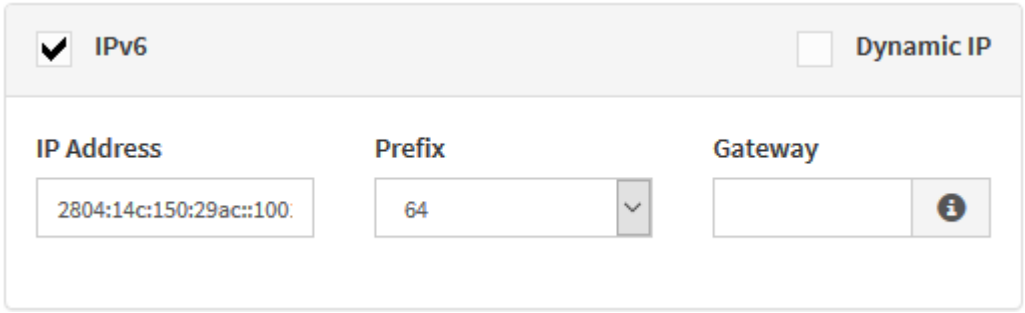


Interface VLAN – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]*:*** This check box is used to determine whether the IP will be automatically configured by DHCP*;*
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *“187.8.187.11”*;
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is a mandatory requirement*. Ex.: “255.255.255.128”;
- ***Gateway:*** *Defines the gateway address corresponding to the network*. This is a NON-mandatory requirement. Ex.: *“187.8.187.1”.*

IPv6

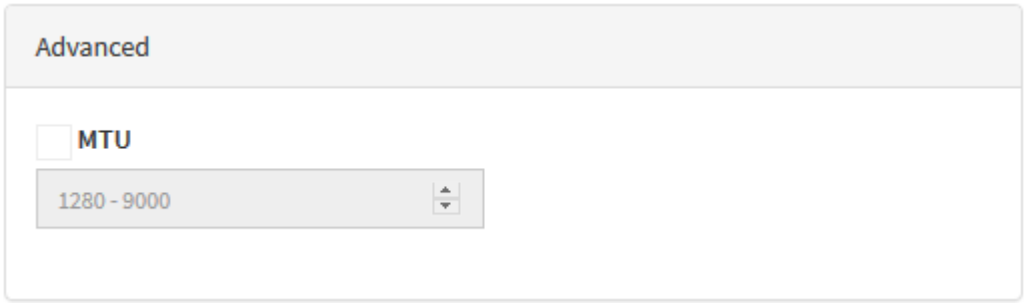


Interface VLAN – IPv6

To enable the IPv6 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*[ ]:** This check box is used to determine whether the IP will be automatically configured by DHCP;
- ***IP Address*:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement. Ex.: “2804:14c:150:29ac::1001”;
- ***Prefix*:** Select the prefix corresponding to the IPv6 addressing. *This is a mandatory requirement.* Ex.: “64”;
- ***Gateway*:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement.

Advanced



Interface VLAN – Advanced

- ***MTU*[ ]:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME).

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information, see this page.

To save changes, click **Save [ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures the interface will have been successfully configured.

Next, we'll look at how to add a DSL interface.

For more information on adding other types of interfaces, visit this page.

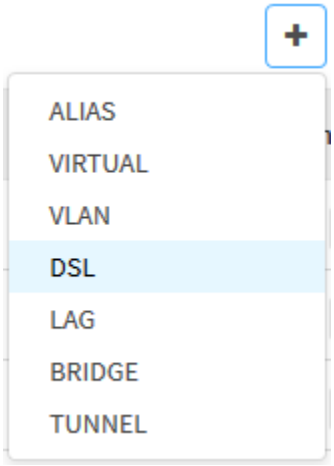
Adding Interfaces - DSL

The DSL (Digital Subscriber Line) interface uses data transmission technology over phone lines, normally installed for internet access.

The Blockbit NGFW is compatible with connections which support both the DSL and PPoE (Point-to-point over Protocol) protocols used to encapsulate PPP frames within Ethernet frames, a solution for tunneling packets over DSL connections to the IP network. PPPoE is typically used for authentication features (username and password).

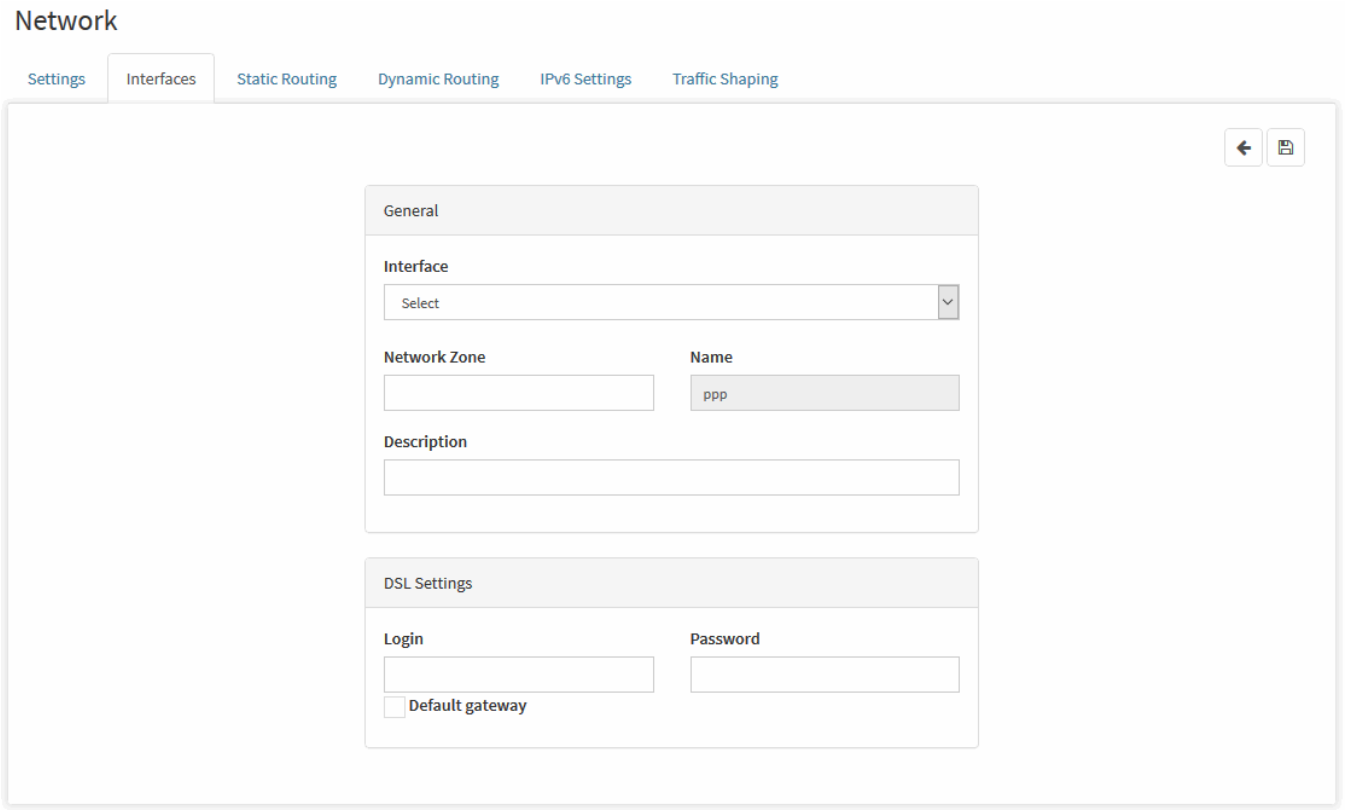
To configure a DSL interface, follow the steps below:

Click on **[**  **]** and select the **[*DSL*]** option:



Add Interface Interface - Menu - DSL

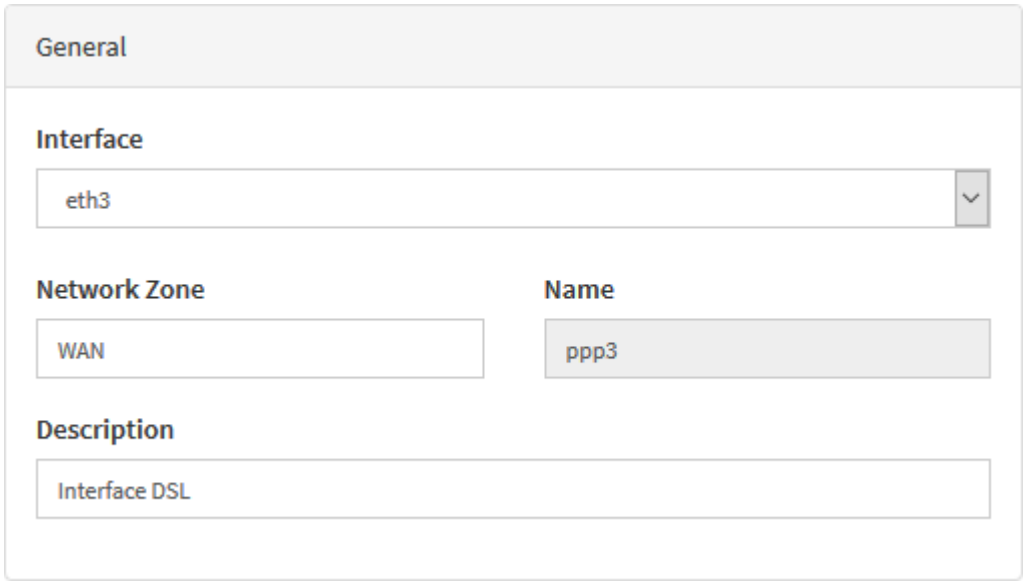
The following screen will appear:



DSL Interface - DSL Interface Creation

Configure it according to the specifications of the respective fields, as shown below:

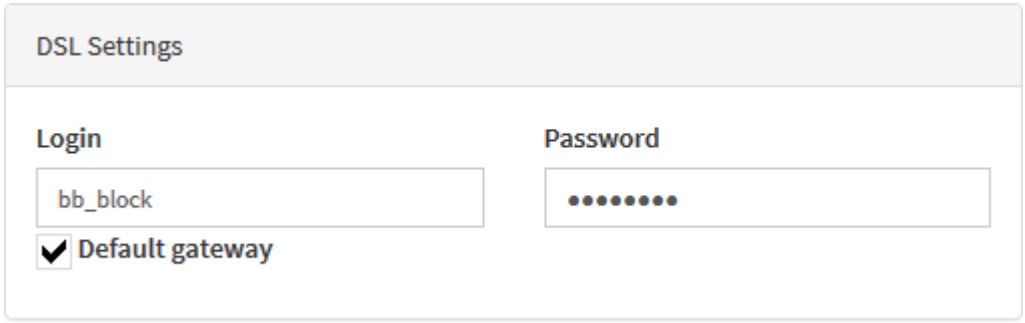
General



DSL Interface - General

- **Interface:** In this selection field it is possible to define the interface where the DSL interface will be configured. Ex.: eth3;
- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Enter “WAN” and select it from the list;
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: *“ppp3”;*
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: *“Interface DSL”.* {mandatory requirement*}.*

DSL Settings



Interface DSL - DSL Settings

The default configuration of the providers requires DSL user authentication under the PPPoE protocol.

- ***Login***: In this field the user name for ADSL authentication is determined, each service provider requires authentication with specific syntax. Ex.: *“user_name” or “user_name@seu_dominio.com”;*
- ***Password*:** This field defines the user's password;
- ***Default Gateway[ ]*:** By enabling this checkbox, the system's “Default Route” will be automatically loaded to the PPP interface. Ex.: *“ppp3”.*

To save changes, click **Save [ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command Queue.

After performing these procedures the interface will have been successfully configured.

Next, we'll look at how to add a LAG interface.

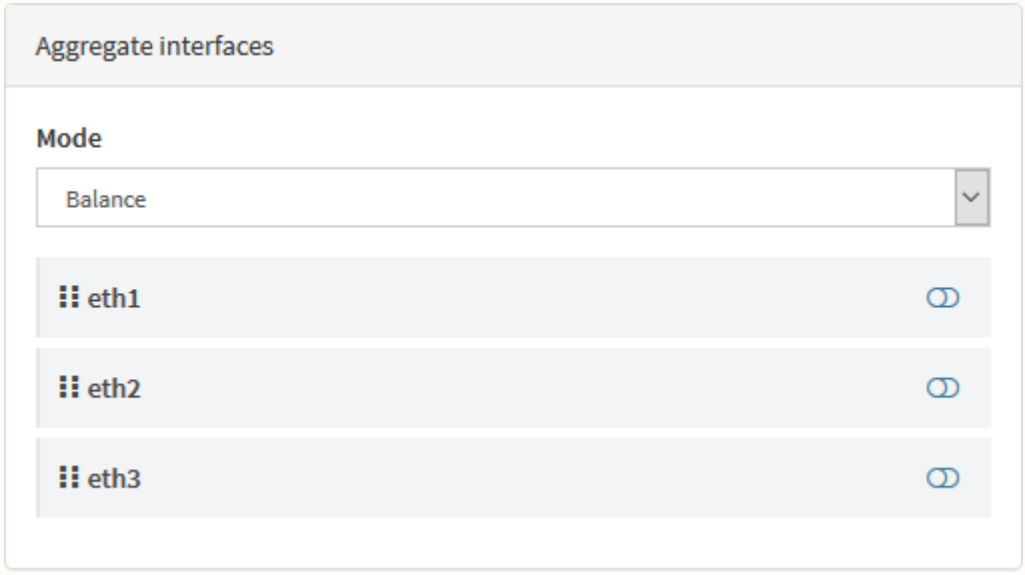
For more information on adding other types of interfaces, visit this page.

Adding Interfaces - LAG (Link Aggregation)

The LAG interface is the resource that combines multiple physical interfaces into a single logical interface, which we call “LAG (Link Aggregation Group)” and one of its main purposes is to increase the bandwidth of the network traffic to the total width bandwidth of the aggregated physical interfaces, providing greater bandwidth as well as link redundancy, in case one of the links fails, automatically maintaining traffic to the other LAG interface(s).

The LACP (Link Aggregation Control Protocol), is a layer 2 negotiation protocol, which provides methods to control the aggregation of multiple physical ports in a single logical group. It allows a network device to negotiate an automatic grouping of links by sending LACP packets to another directly connected device that also implements LACP.

To add any LAG type interface, it is necessary that two or more interfaces are available. Otherwise during the creation process, they will not be displayed in the Aggregate interfaces panel.



The Blockbit NGFW offers this feature in 3 (three) operating modes:

- Aggregation mode;
- Balance Mode;
- Active/Backup mode.

To configure the link aggregation service, we need to create an aggregation group “LAG - Link Aggregation Group”, and define which links “interfaces” will be members of the group.

To configure a “LAG” interface, the interfaces must be “disabled” ***[ ]***.

Next, we'll take a closer look at the operating modes, starting with the Aggregation Mode.

For more information on adding other types of interfaces, visit this page.

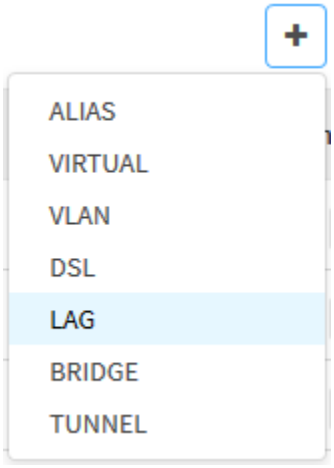
LAG - Aggregation mode

The Aggregation mode is where there is a uniform distribution of traffic over the physical interfaces of the group of aggregated links, thus adding the bandwidth of the network interfaces in the group and increasing the reliability of the connection.

The LAG enabled in “Aggregation” mode requires network switches to support the “LACP - Link Aggregation Control Protocol (802.3ad)” protocol, and be properly configured.

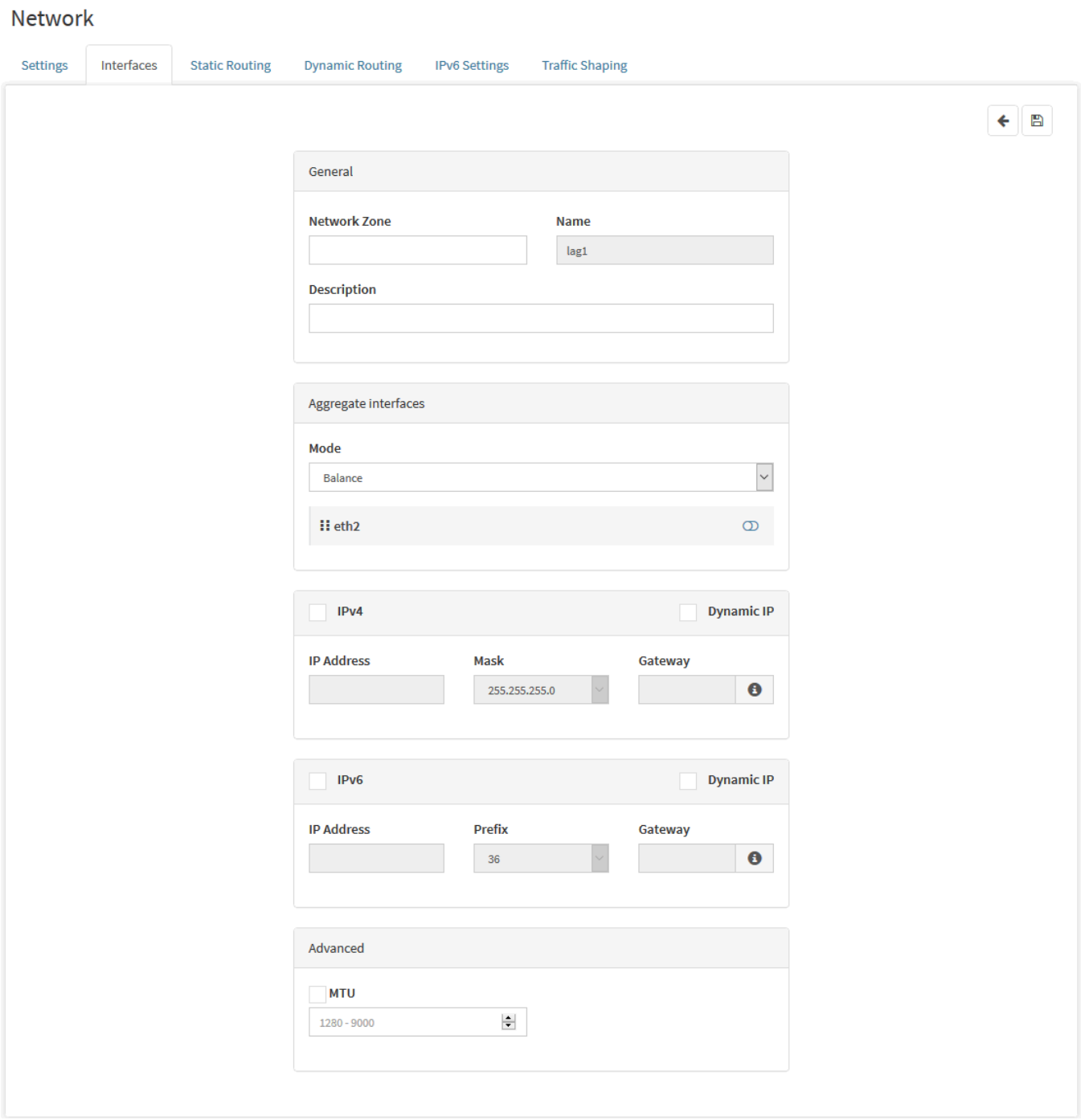
To configure a LAG interface in Aggregation mode, follow the steps below:

Click on **[ ]** and select the **[LAG]** option:



Button for Adding Interfaces - Menu - LAG

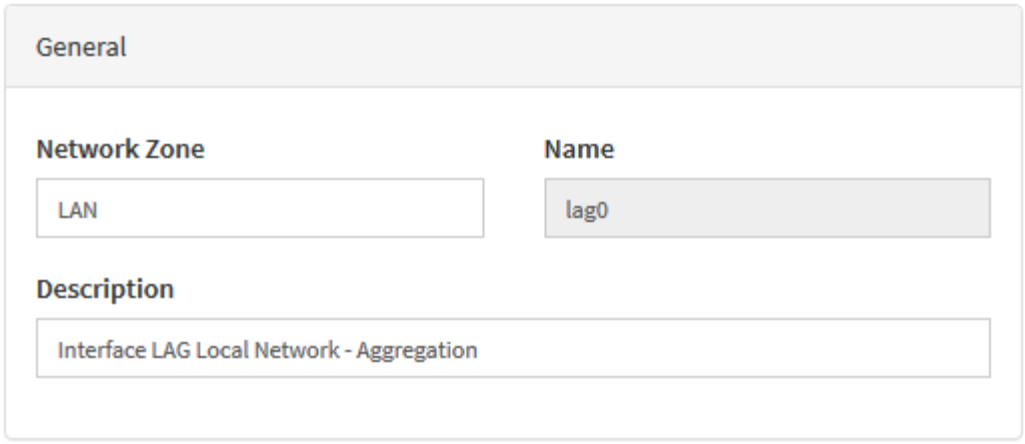
The following screen will appear:



Interfaces - Creation of LAG Interface

Configure it according to the specifications of the respective fields, as shown below:

General



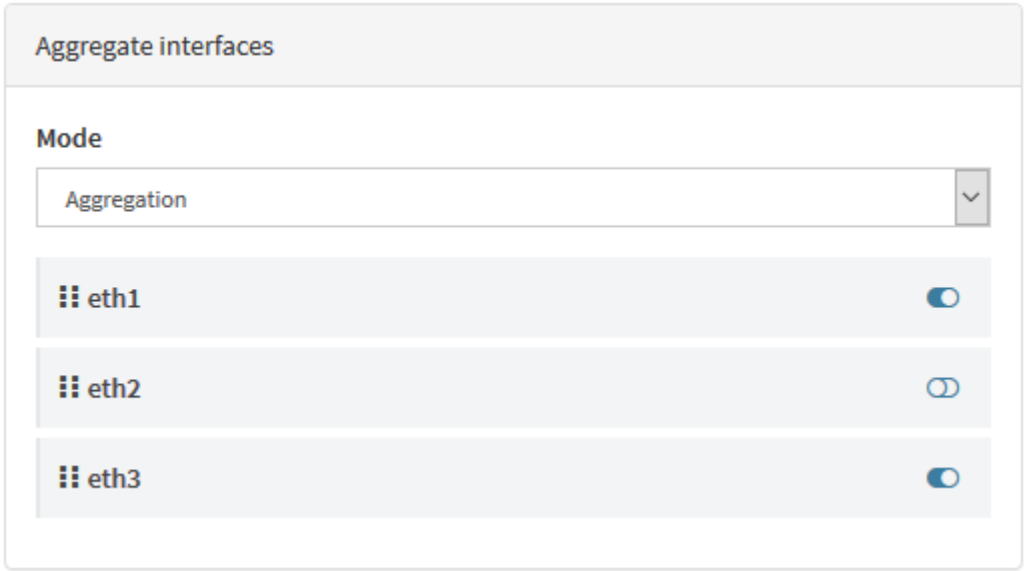
Interface LAG – General

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Type "LAN" and select it from the list*;*
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “[*lag0*]”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: “*LAG - Aggregation*”.

Aggregate Interfaces

To add any LAG type interface, it is necessary that two or more interfaces are available. Otherwise during the creation process, they will not be displayed in the Aggregate interfaces panel.

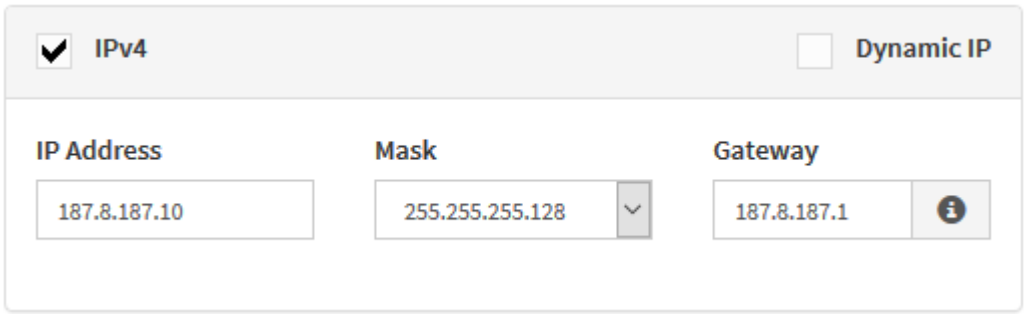
To configure a “LAG” interface, the interfaces must be “disabled” ***[ ]***.



Interface Virtual – Aggregate Interfaces

- ***Mode*:** Determines the operation mode of the LAG interface. By default we have "Balance", "Aggregation" and "Active-Backup" modes. Ex.: "*Aggr egation*";
- ***Interfaces[ ]:*** Activate the interfaces that will be used. Ex.: eth1 and eth3.

IPv4

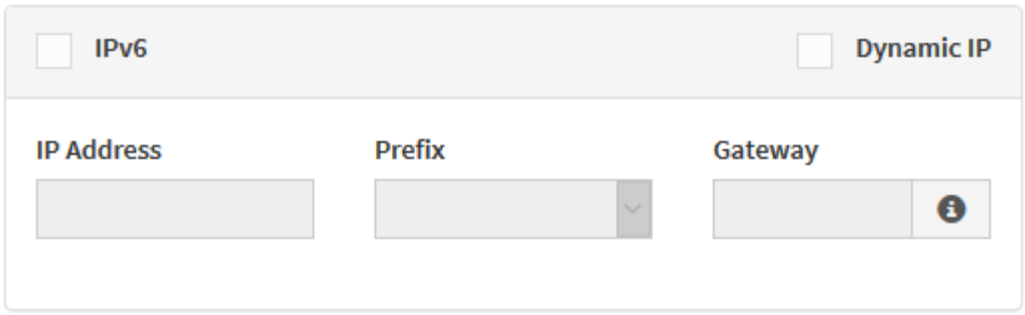


Interface LAG – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"187.8.187.10";*
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is a mandatory requirement*. Ex.: *"255.255.255.128";*
- ***Gateway*:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement. Ex.: *"187.8.187.1".*

IPv6

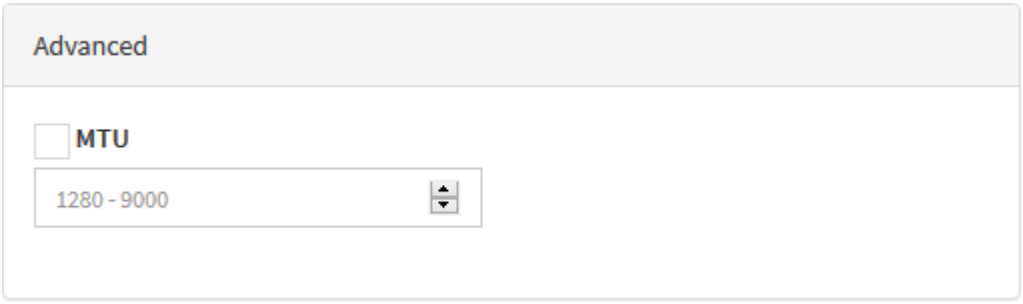


Interface LAG – IPv6

To enable the IPv6 addressing standard, check the ***[ ]*** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** Sets the IPv6 address of the virtual interface;
- ***Prefix*:** Determines the prefix corresponding to the IPv6 addressing;
- ***Gateway*:** Defines the gateway address corresponding to the network.

Advanced



Interface LAG – Advanced

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

- ***MAC address*:** In this field it is possible to change the MAC address of the virtual interface, if no address is defined, the system will automatically generate one.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures the interface will have been successfully configured.

Next, we will delve into how to create a LAG *Balance mode* interface.

For more information on adding other types of interfaces, visit this page.

LAG - Balance Mode

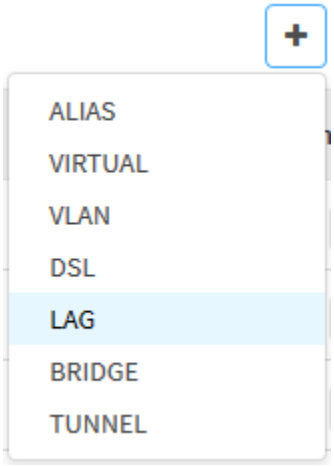
This is where traffic is distributed in sequential order from the first interface of the group to the last, basically the service distributes the load, that is, the packets, alternately between the LAG interfaces. In the same connection, packets are sent to interface 1, then to interface 2 and so on from the first interface to the last.

It is the only way that sends packets from the same TCP / IP connection through multiple interfaces.

When using multiple sends and multiple incoming connections, packets can often be received out of order and result in retransmission.

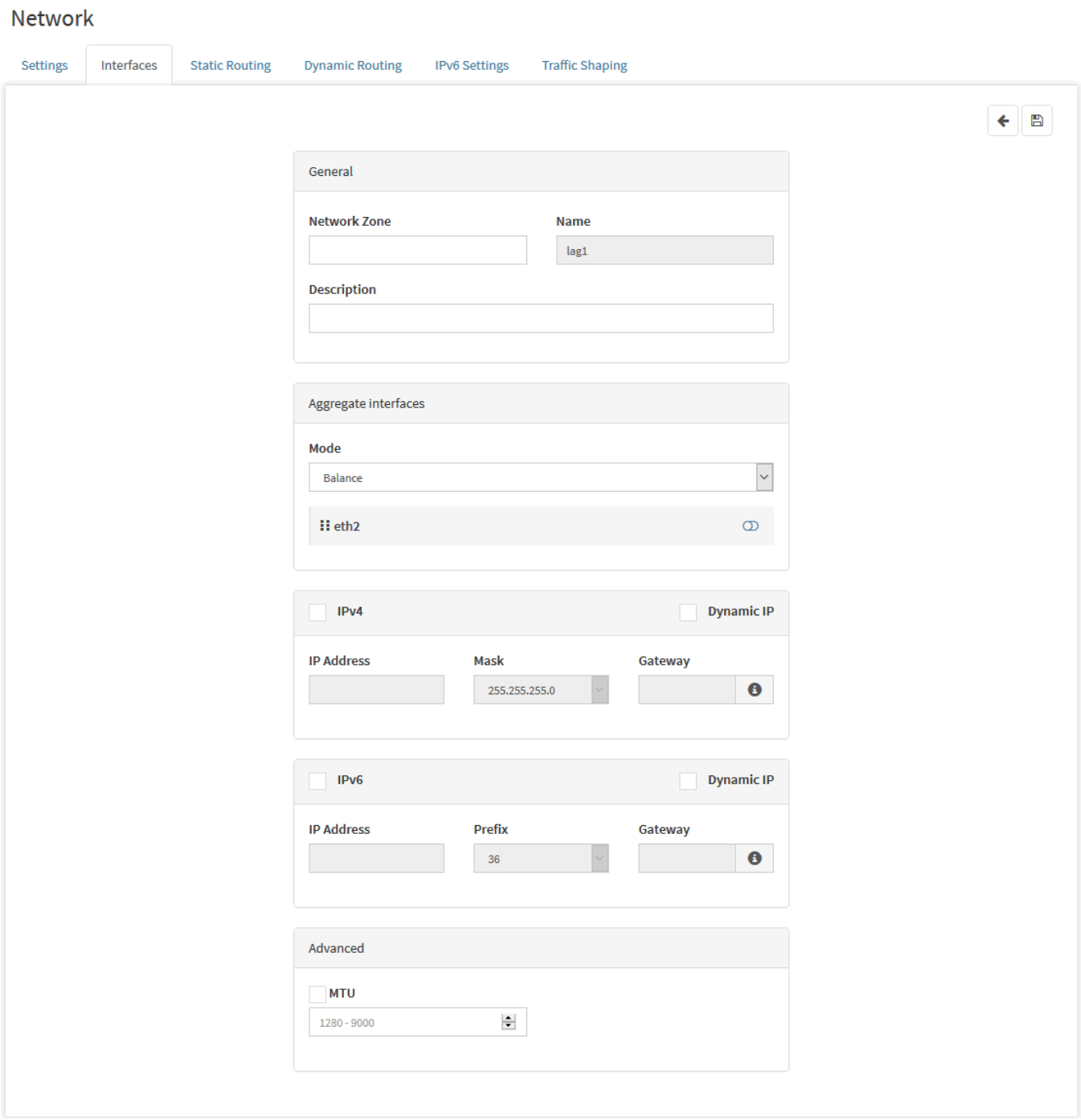
To configure a LAG interface in Balance mode, follow the steps below:

Click on **[ ]** and select the **[LAG]** option:



Button for Adding Interfaces - Menu - LAG

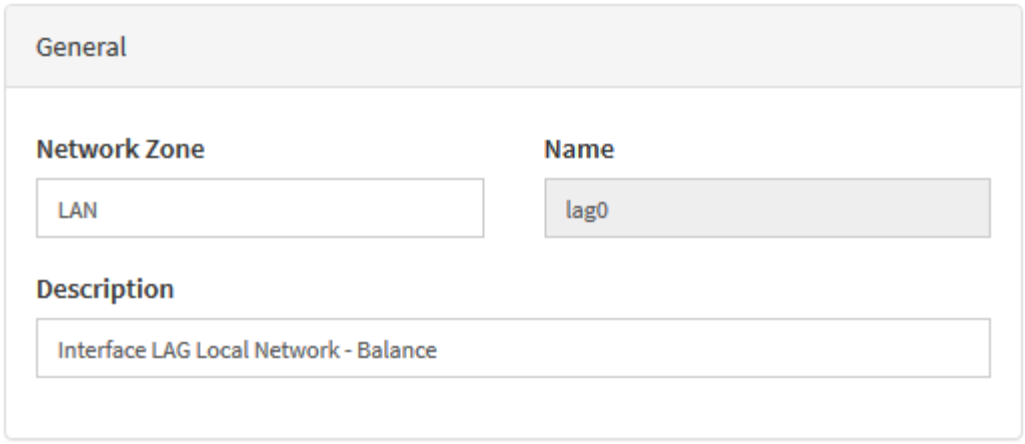
The following screen will appear:



Interfaces - Creation of a LAG Interface

Configure it according to the specifications of the respective fields, as shown below:

General



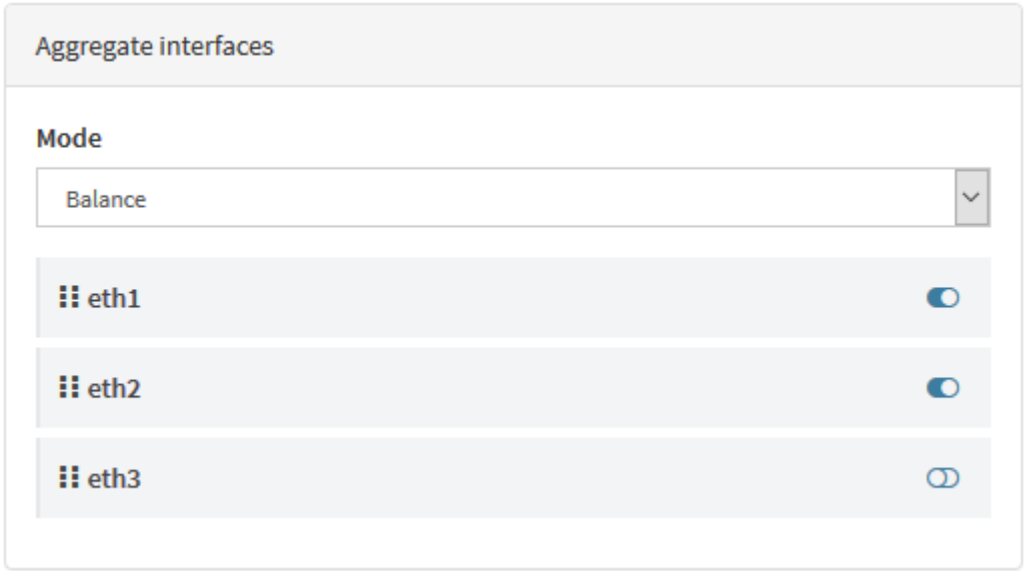
Interface LAG – General

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Type "LAN" and select it from the list*;*
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “[*lag0*]”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: “*LAG - Balance*”.

Aggregate Interfaces

To add any LAG type interface, it is necessary that two or more interfaces are available. Otherwise during the creation process, they will not be displayed in the Aggregate interfaces panel.

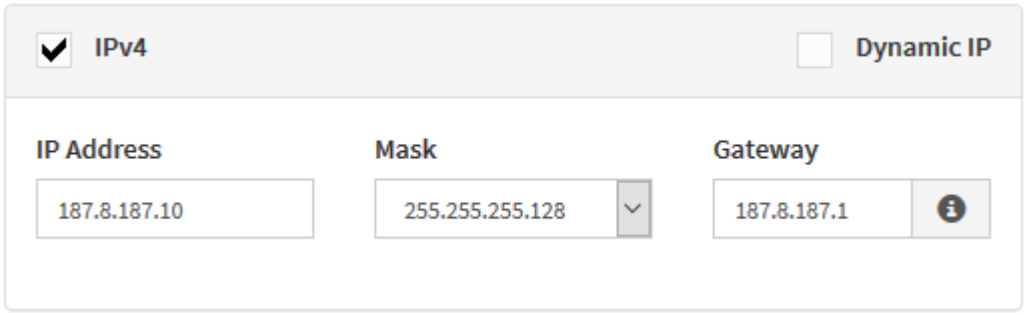
To configure a “LAG” interface, the interfaces must be “disabled” ***[ ]***.



Interface Virtual – Aggregate Interfaces

- ***Mode*:** Determines the operation mode of the LAG interface. By default we have "Balance", "Aggregation" and "Active-Backup" modes. Ex: "Balance";
- ***Interfaces[ ]:*** Activate the interfaces that will be used. Ex.: eth1 and eth2.

IPv4

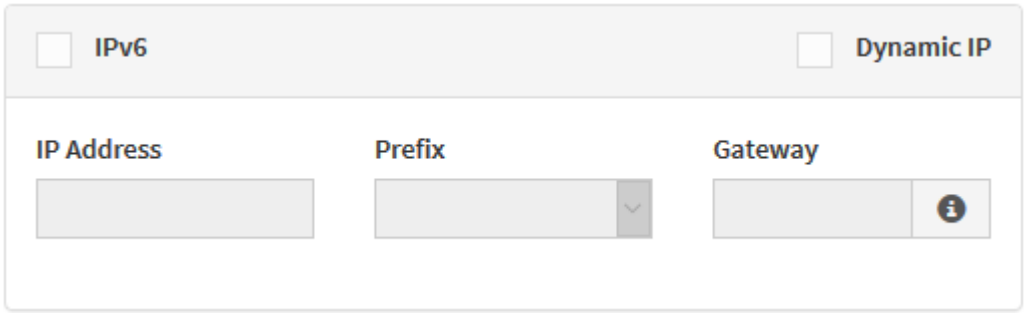


Interface LAG – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"187.8.187.10";*
- ***Mask*:** This check box determines the mask corresponding to the IPv4 addressing**.** *This is a mandatory requirement.*Ex.: *"255.255.255.128";*
- ***Gateway*:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement. Ex.: *"187.8.187.1".*

IPv6



Interface LAG – IPv6

To enable the IPv6 addressing standard, check the ***[ ]*** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** the IPv6 address of the virtual interface;
- ***Prefix*:** Determines the prefix corresponding to the IPv6 addressing;
- ***Gateway*:** Defines the gateway address corresponding to the network.

Advanced

Interface LAG – Advanced

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME).

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information, see this page.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

After performing these procedures the interface will have been successfully configured.

Next, we will delve into how to create an *Active Backup mode* LAG interface.

For more information on adding other types of interfaces, visit this page.

LAG - Active / Backup mode

In this mode, the system enables only one interface as "active" and packets traffic is sent through only one interface. Additional network interfaces work in “Standby” mode and only become active if the main interface fails.

Active / backup mode is the best option for exclusive “High availability” configuration with multiple interconnected switches.

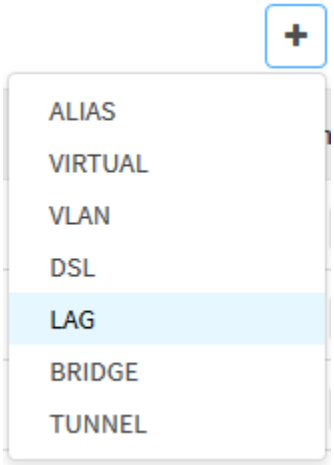
For all operating modes, the LAG supports the redundancy service. *If one of the links on the aggregate interface becomes unavailable, traffic will continue to flow over to any available interface(s) in the group.*

This mode supports interfaces of the type:

- ***Ethernet*;**
- ***VLAN*.**

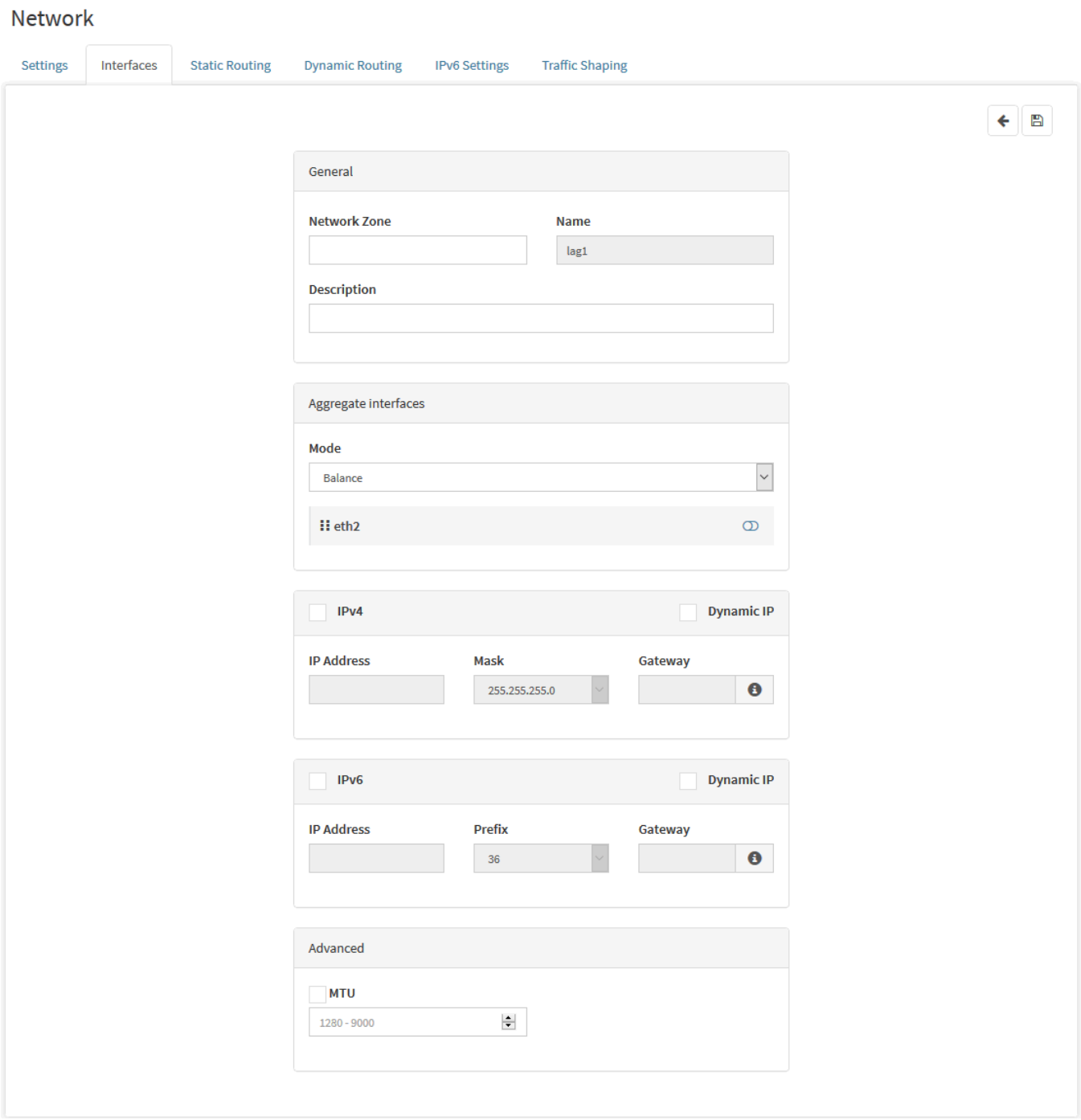
To configure a LAG interface in Balance mode, follow the steps below:

Click on **[** **]** and select the **[LAG]** option::



Button for Adding Interfaces - Menu - LAG

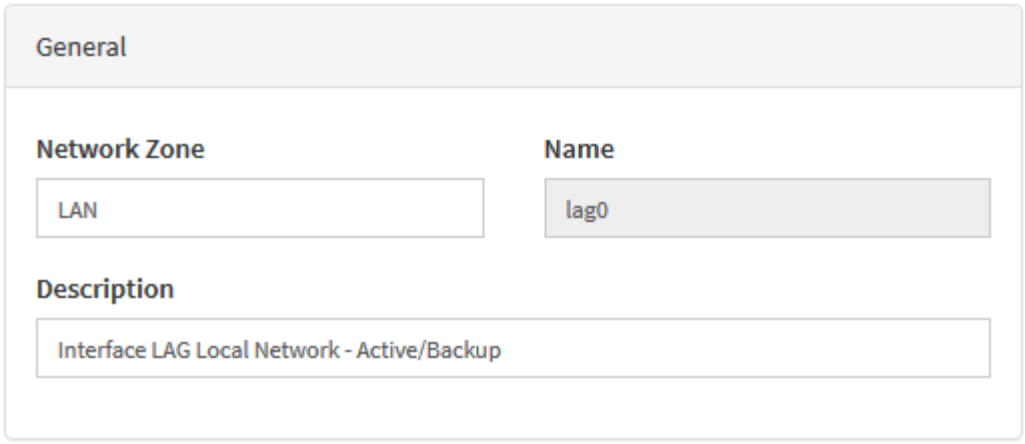
The following screen will be displayed:



Interfaces - Creation of LAG Interface

Configure it according to the specifications of the respective fields, as shown below:

General



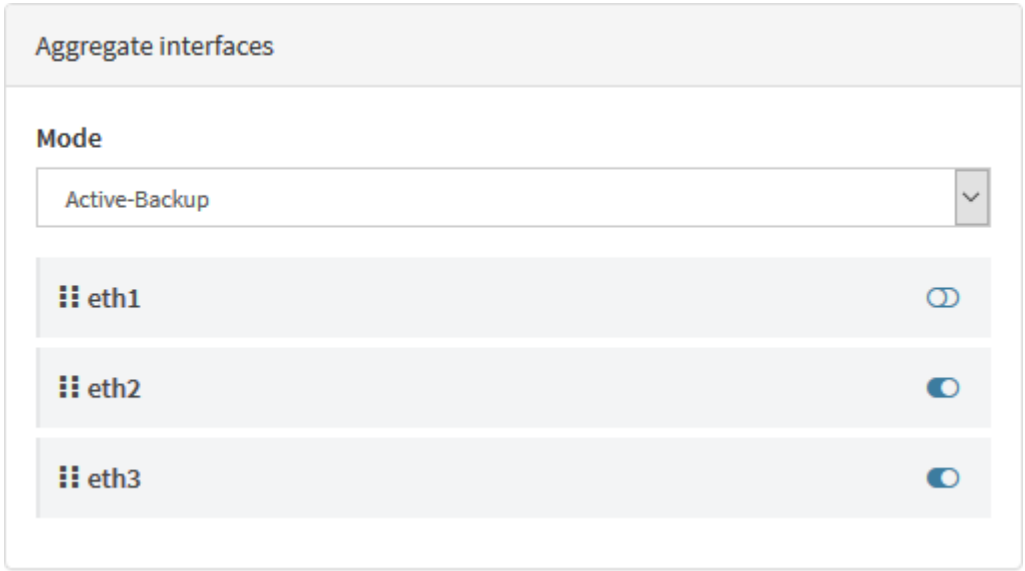
LAG Interface - General - Active / Backup

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Type "LAN" and select it from the list*;*
- ***Name*:** Refers to the identification of the network interface that was selected for editing. Ex.: “[*lag0*]”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: “*LAG - Active/Backup*”.

Aggregate Interfaces

To add any LAG type interface, it is necessary that two or more interfaces are available. Otherwise during the creation process, they will not be displayed in the Aggregate interfaces panel.

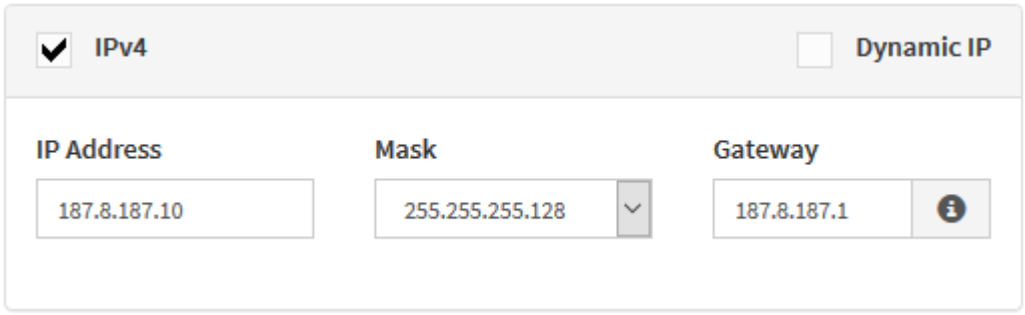
To configure a “LAG” interface, the interfaces must be “disabled” ***[ ]***.



LAG Interface - Aggregate Interfaces

- ***Mode*:** Determines the operating mode of the LAG interface. By default we have "Balance", "Aggregation" and "Active-Backup" modes. Ex.: "*Activ e-Backup*";
- ***Interfaces[ ]:*** Activate the interfaces that will be used. Eg: eth2 and eth3.

IPv4

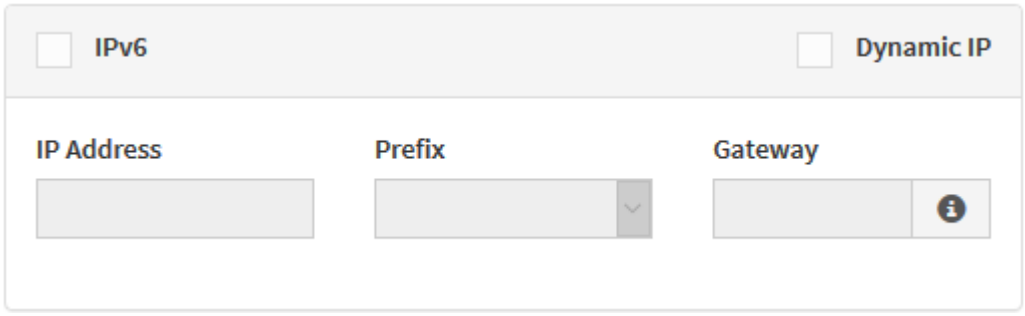


LAG Interface – IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"187.8.187.10";*
- ***Mask*:** This checkbox determines the mask corresponding to the IPv4 addressing. *This is a mandatory requirement*. Ex.: *"255.255.255.128";*
- ***Gateway*:** Defines the gateway address corresponding to the network. This is a NOT mandatory requirement. Ex.: *"187.8.187.1".*

IPv6



LAG interface - IPv6

To enable the IPv6 addressing standard, check the ***[ ]*** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*:** Sets the IPv6 address of the virtual interface;
- ***Prefix*:** Determines the prefix corresponding to the IPv6 addressing;
- ***Gateway*:** Defines the gateway address corresponding to the network.

Advanced

LAG Interface – Advanced

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command Queue.

After performing these procedures the interface will have been successfully configured.

Next, we will analyze how to create a *Bridge* type interface.

For more information on adding other types of interfaces, visit this page.

Adding Interfaces - Bridge

A "bridge" is a logical network interface composed of one or more physical network interfaces operating at layer 2 (link) which is sending packets through MAC addresses.

Interfaces in "bridge" mode have well-defined purposes, and when it comes to Firewall it is very important to understand its features, characteristics and applicability.

Characteristics

The "bridges" are used to interconnect several networks that are in different segments or have different protocols, thus creating an extended network, its operation is transparent in the network, and can be used as a switch / firewall.

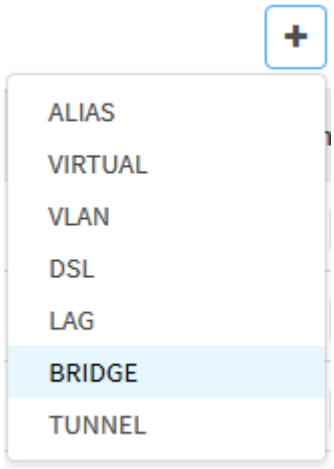
Applicability

This implementation model allows you to offer a superior layer of security for your network, optimizing the features and performance of your Blockbit NGFW device.

It also serves to define a network layout that allows two protection barriers using DMZ, determine a configuration pattern and well-applied policies and allows a high degree of monitoring and detection of attacks.

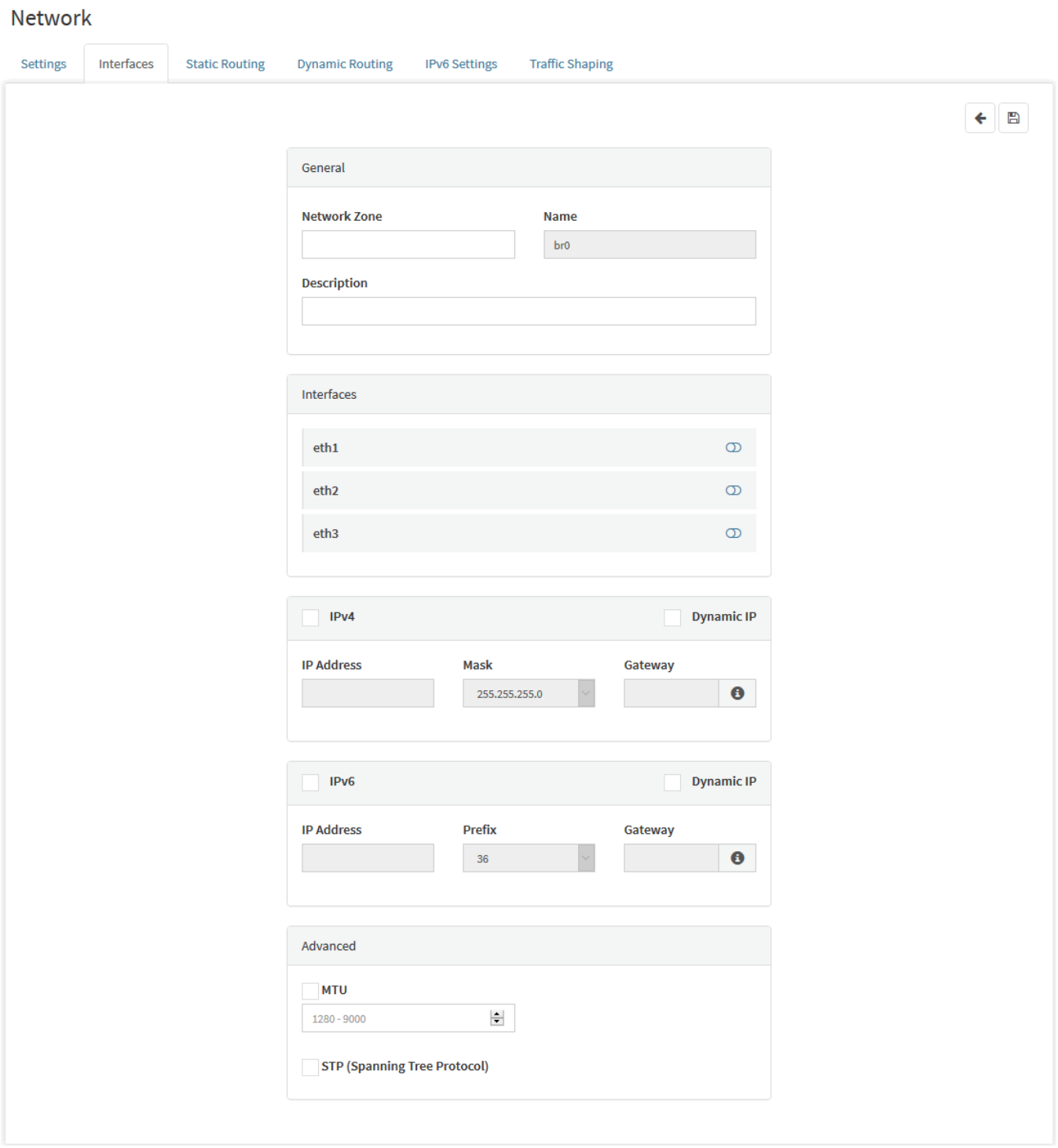
To configure a Bridge interface, follow the steps below:

Click on **[** + **]** and select the **[*BRIDGE*]** option:



Add Interface button - Menu - Bridge

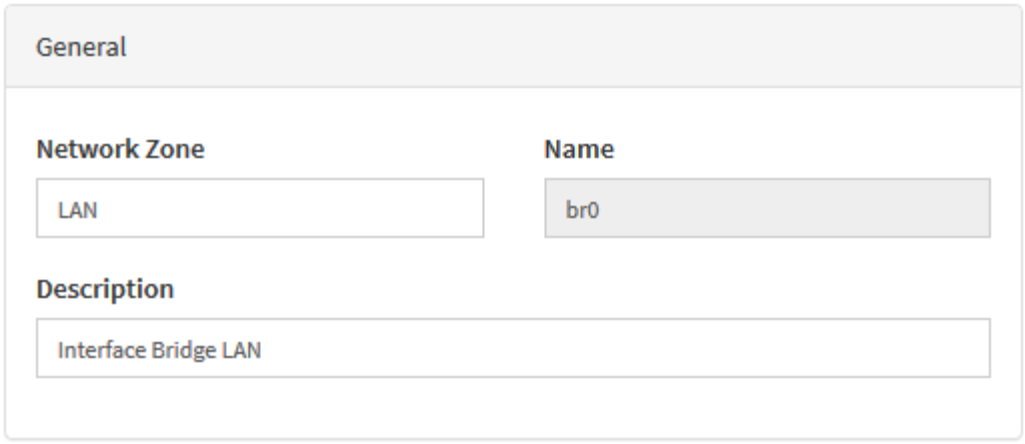
The following screen will appear:



Interfaces - Bridge Interface Creation

Configure it according to the specifications of the respective fields, as shown below:

General



Interface Bridge – General

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Type "LAN" and select it from the list;
- ***Name*:** *Refers to the identification of the network interface selected for editing*. Ex.: *“br0”;*
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: *“Interface Bridge LAN”.*

Interfaces

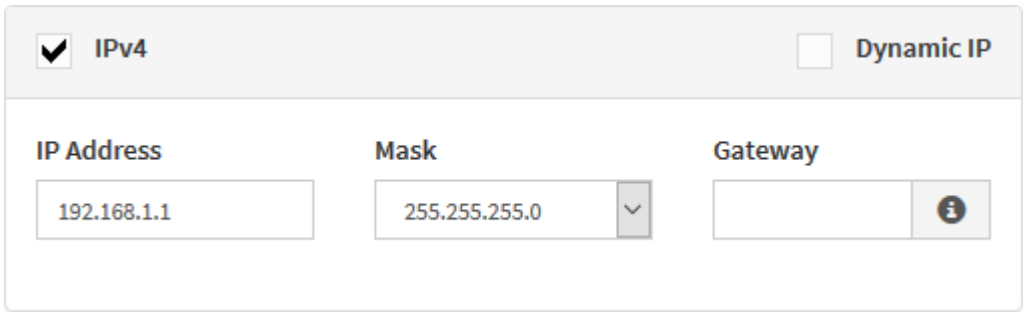
To add any Bridge type interface, it is necessary that two or more interfaces are available. Otherwise during the creation process, they will not be displayed in the Interfaces panel.

Bridge Interface - Interfaces

This is the selection panel for the corresponding interfaces in order to enable them as bridge interfaces.

- ***Interfaces[ ]:*** *Activate the interfaces that will be used. Ex: eth1 and eth3.*

IPv4

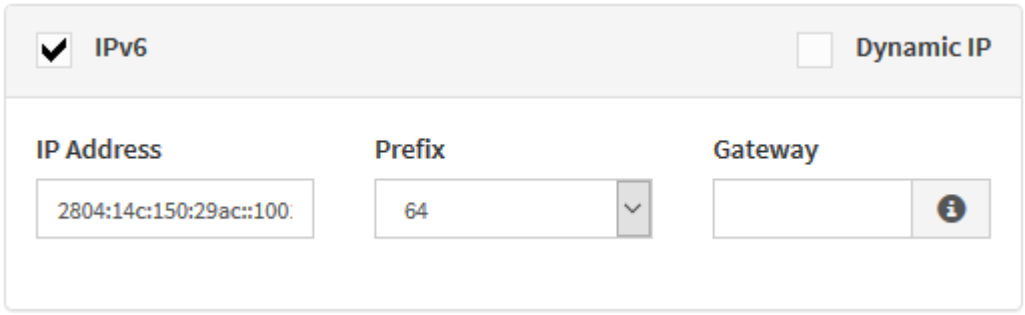


Virtual Interface - IPv4

To enable the IPv4 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP[ ]:*** *This check box is used to determine whether the IP will be automatically configured by DHCP*;
- ***IP Address*****:** Defines the IPv4 address of the virtual interface. This is a mandatory requirement. Ex.: *"192.168.1.1".*
- ***Mask*****:** This checkbox determines the mask corresponding to the IPv4 addressing*. This is a mandatory requirement*. Ex.: *"255.255.255.0";*
- ***Gateway*****:** Defines the gateway address corresponding to the network. This is a NON-mandatory requirement. Ex.: *"187.8.187.1".*

IPv6

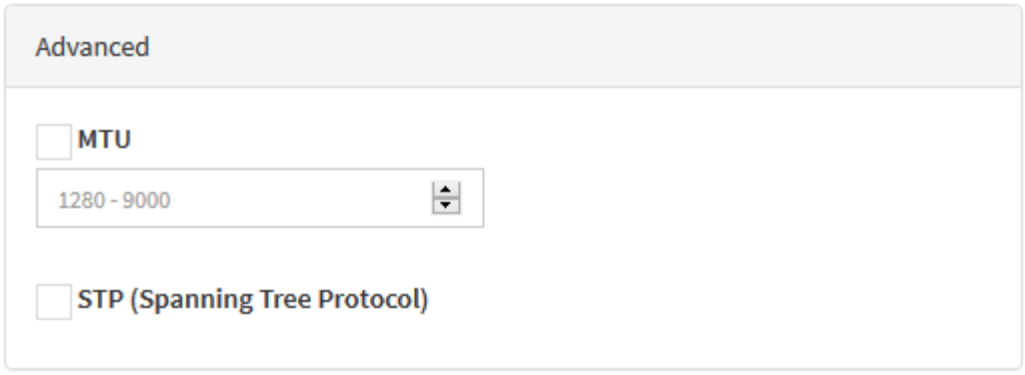


Bridge Interface - IPv6

To enable the IPv6 addressing standard, check the **[ ]** checkbox at the top of the panel and configure the form with the corresponding data for each field.

- ***Dynamic IP*****[ ]*:*** This check box is used to determine whether the IP will be automatically configured by DHCP*;*
- ***IP Address*****:** Sets the IPv6 address of the virtual interface. This is a mandatory requirement. Ex.: "*2804:14c:150:29ac::1001*;
- ***Prefix*****:** Select the prefix corresponding to the IPv6 addressing*. This is a mandatory requirement.* Ex.: "64";
- ***Gateway*****:** Defines the gateway address corresponding to the network. This is NOT a mandatory requirement.

Advanced



Interface Bridge – Advanced

In a Bridge interface it is possible to define the MTU (Maximum Transmission Unit) and activate the STP (Spanning Tree Protocol)

- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME);

  Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

- ***STP (Spanning Tree Protocol)*[ ]:** This check box is used to activate the use of the Spanning Tree Protocol in the interface.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After performing these procedures, the interface will have been successfully configured.

Next, we'll look at how to add a Tunnel interface.

For more information on adding other types of interfaces, visit this page.

Adding Interfaces - Tunnel

Tunnel interfaces are firewall interfaces that define a point-to-point connection to remote routers on private networks, and / or route-based VPN tunnels.

Any traffic routed to a tunnel interface that is allowed by the Firewall access rules, tends to be commonly configured between an incoming and outgoing router, in addition, this traffic is sent to the tunnel.

The header encapsulation referring to standard network protocols is performed on packets whose function is to be sent through the tunnel interface, this encapsulation through a new header is called GRE (Generic Routing Encapsulation).

The GRE protocol is intended to encapsulate a variety of network layer protocols within a specific IP tunnel, creating a private point-to-point connection between remote routers.

This protocol is quite functional in several scenarios, normally used in VPN for encapsulating packets sent through a tunnel over the Internet, works transparently to the user, in order to interconnect remote networks as if they were directly connected.

GRE is not considered a secure protocol, the information transmitted through the tunnel is not encrypted, as the GRE does not have this function, to correct this gap, in order to ensure information's integrity, it is possible to use the GRE protocol alogside the IPSec protocol .

Operation of the GRE protocol

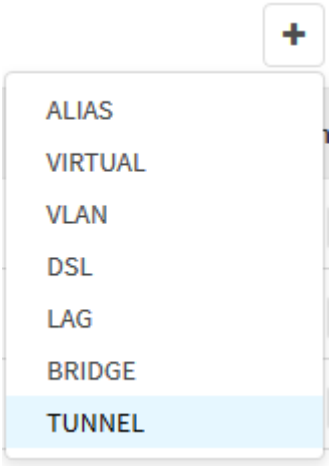
The GRE protocol works by encapsulating network layer protocols within virtual connections through an external IP packet. Therefore, the encapsulated packets are transported through both points of the tunnel, being forwarded through IP networks. During this route, the other routers only check the external IP, with no analysis of the internal packet until it is forwarded to the destination of the GRE tunnel. Only when it reaches its recipient in the tunnel, the package has its encapsulation removed and is finally dispatched to its goal.

GRE protocol features:

- Encapsulation of multiple protocols using only a single backbone;
- Multicast and IPv6 traffic;
- Connecting discontinuous subnets;
- VPN over WAN networks.

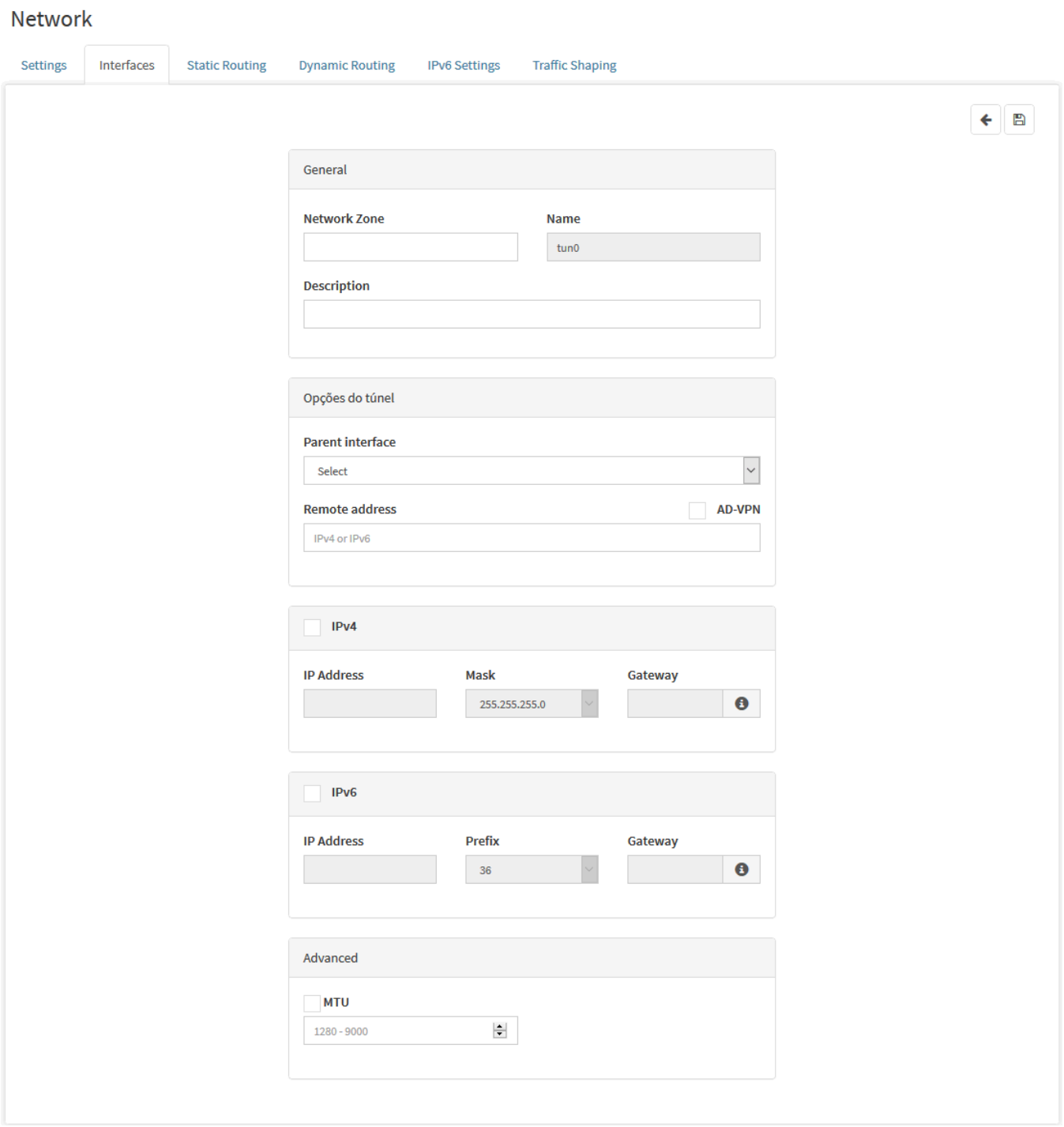
To configure a Tunnel interface, follow the steps below:

Click on **[**  **]** and select the **[TUNNEL]** option:



Add Interface Interface - Menu - Tunnel

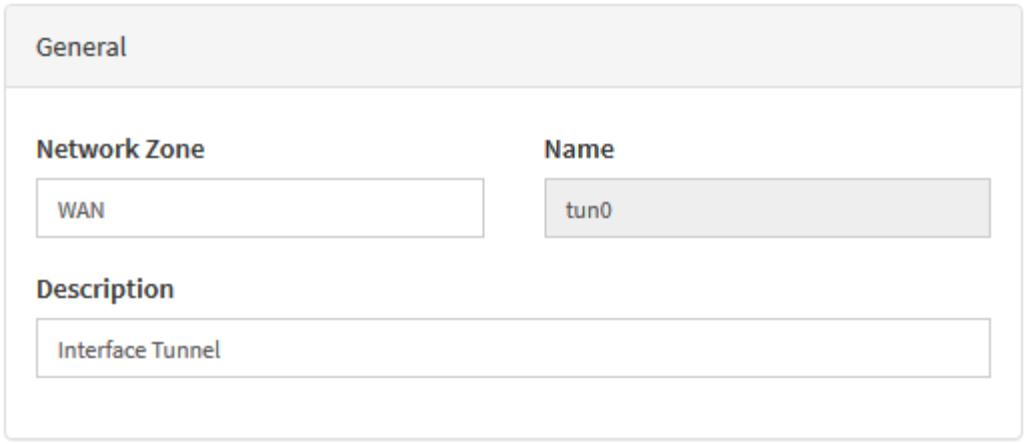
The following screen will appear:



Interfaces - Tunnel Interface Creation

Configure it according to the specifications of the respective fields, as shown below:

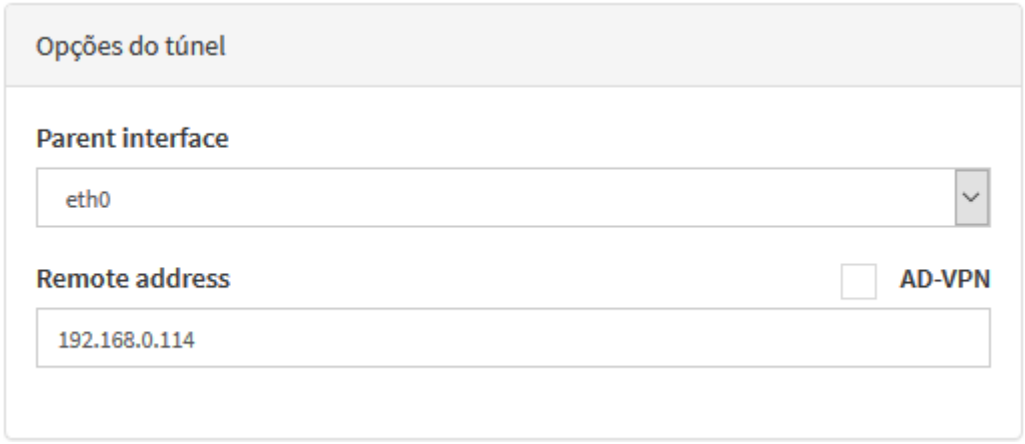
General



Tunnel Interface - General

- ***Network Zone*:** This field refers to the definition of the type of interface grouping. By default we have the “WAN”, “LAN” and “DMZ” zones. This is a mandatory requirement. Ex.: Enter “WAN” and select it from the list;
- ***Name*:** Refers to the identification of the network interface selected for editing. Ex.: “tun0”;
- ***Description*:** Define a description to identify the configured interface. This is a mandatory requirement. Ex.: *Interface Tunnel.*

Tunnel options



Tunnel Interface - Tunnel Options

- ***Parent Interface*:** Selection of the corresponding "physical" ethernet interface for loading the "tunnel" interface. It usually refers to the communication interface between the routers of the point-to-ready connection (“point-to-point”). Ex.: “[tun0]”;
- **Remote Address:** IP address of the remote point to establish the GRE tunnel connection*. This IP address refers to the address of the BB-NGFW, or router, or remote end*. Ex.: *“192.168.0.114”;*
- ***AD-VPN[ ]:*** When activating this option, the "Remote Address" field will be disabled. If this checkbox is checked, the interface will use the VPN Auto-Discovery feature.

The **IPv4/IPv6** “addressing” and “MTU treatment” tables **[advanced]** are based on the configuration profile of your network environment and therefore are optional items.

You can optionally add **IPv4** and / or **IPv6** addresses to a Tunnel Interface. This addressing will serve as a “Gateway” for the destination network of the remote point of the GRE tunnel.

Adding an IP address allows you to define the source of traffic sent from the node **[BB-NGFW]**. Ex.: An IP is recommended, to provide a source address for dynamic routing daemons, and for the Independent Multicast Protocol Configuration - Sparse-Mode (PIM-SM).

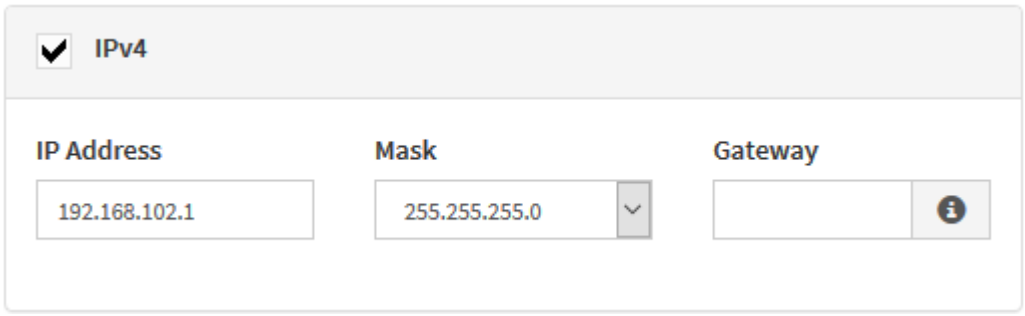
If no IP address is added, traffic from “from” and “to” Tunnel Interface will automatically use the Default Firewall IP, both for outbound traffic and for its origin address.

The mapping of the **[*TUNNEL*]** interfaces to the physical network interfaces of the “node” itself are based on the routing configuration.

Here is a demonstration:

IPv4 configuration example

[TUNEL] interfaces can only have static IP addresses.



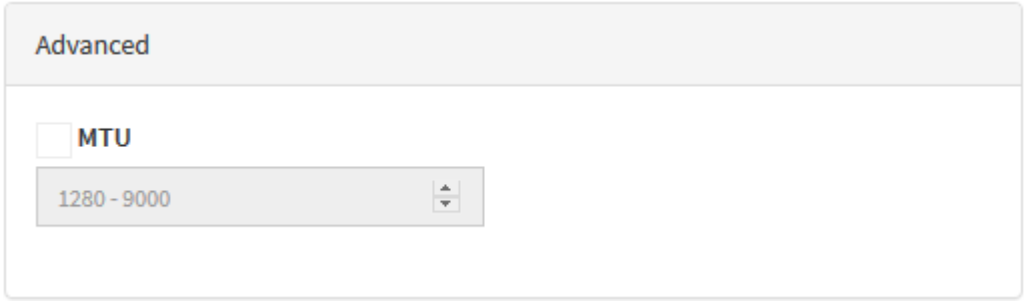
Tunnel Interface - IPv4

- **IPv4 address:** Enter the IPv4 address of the network that will serve as the gateway to the GRE tunnel. This is a mandatory requirement. Ex.: *“192.168.102.1”;*
- **Mask:** Select the mask corresponding to the IP address of the network. This is a mandatory requirement. Ex.: *“255.255.255.0”;*
- ***Gateway*:** Inform the gateway that will be used. This is a NON-mandatory requirement.

The GRE tunnel requires the configuration of Route (s) for the destination network (s). *The routes can be of the type: “static”, “dynamic” or “multicast”.*

It also requires the creation of security policies of the type "Forwarding" or "Forward" between the local network (s) of (origin) and the remote network (s) of (destination).

Advanced



- ***MTU[ ]*:** To enable this option, check the checkbox. This field defines the MTU of the virtual interface, the possible values are between 1280 to 9000 (JUMBO FRAME).

Attention, to avoid fragmentation, it may be necessary to increase the MTU values. For more information on this, see this page.

To save changes, click ***Save*[ ]**, otherwise click ***Back*[ ]** to return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information about the command queue visit the page: UTM - Command Queue.

After performing these procedures, the interface will have been successfully configured.

Below we will detail the components of the action menu.

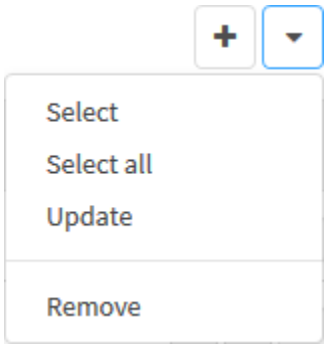
For more information on adding other types of interfaces, visit this page.

Interfaces - Actions menu

At the top right of the screen, next to the Add Interface button we have the actions menu:

Interfaces – Actions menu button

By clicking on this button the menu below is displayed:



Interfaces - Actions menu

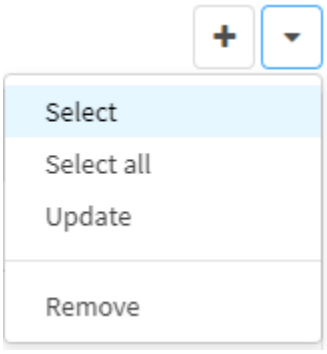
The menu consists of the following options:

- *Select;*
- *Select All*;
- *Update*;
- *Remove*.

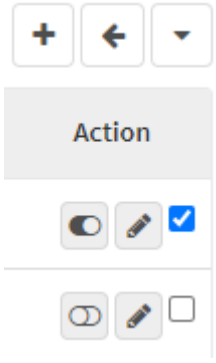
Next, each action menu option will be detailed.

Interfaces - Actions menu - Select

By clicking on “Select” in the action menu, a selection box will be shown next to each interface, allowing them to be selected to receive specific changes:



Interfaces – Select

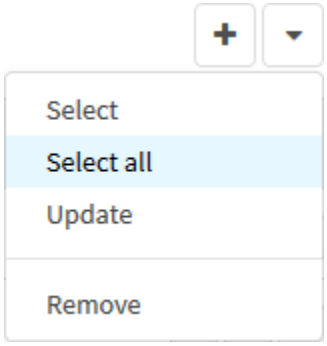


Select interface action

This allows the user to select which interfaces will receive specific changes.

Interfaces - Actions menu - Select All

By clicking on “Select All” in the action menu all interfaces will be selected.

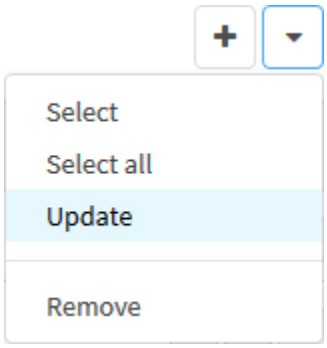


Interfaces – Select All

This allows changes that affect all interfaces to be easily implemented.

Interfaces - Actions menu - Update

By clicking on “Update” in the action menu, all information related to the interfaces will be updated.



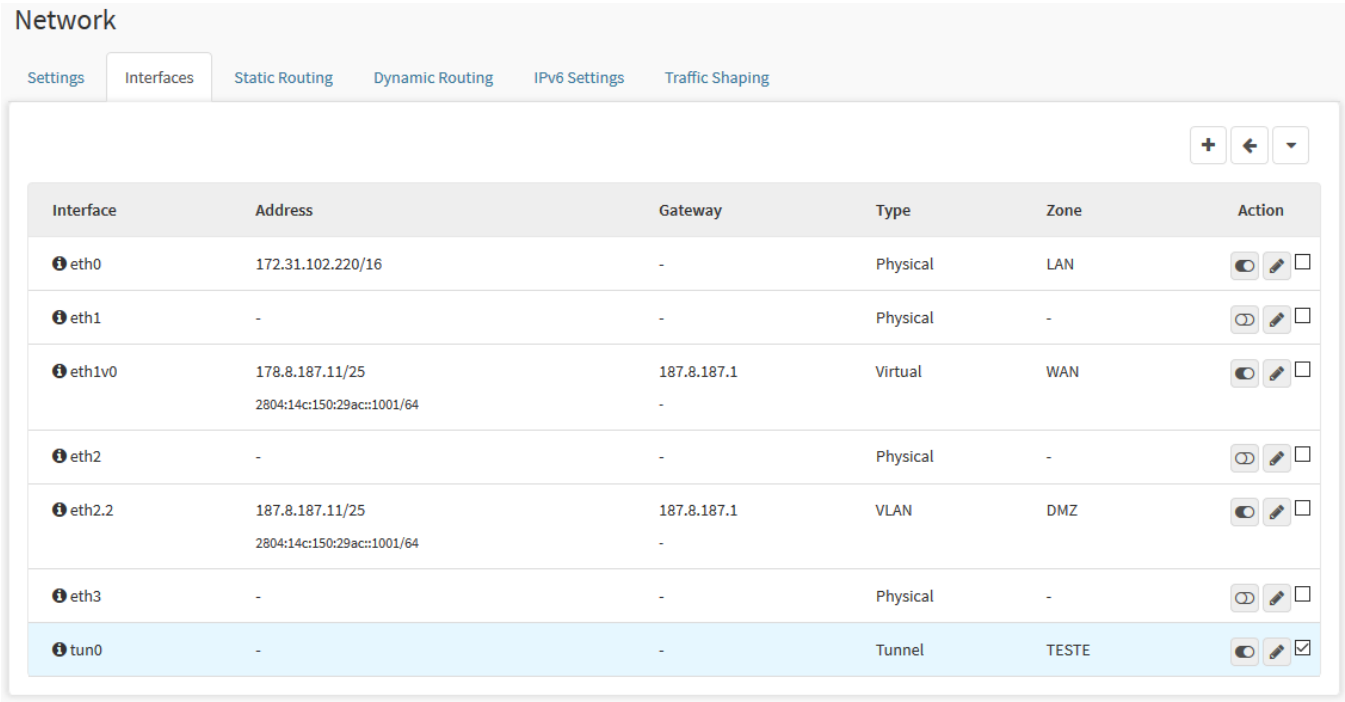
Interfaces – Update

This allows changes that affect all interfaces to be easily implemented.

Interfaces - Actions Menu - Remove

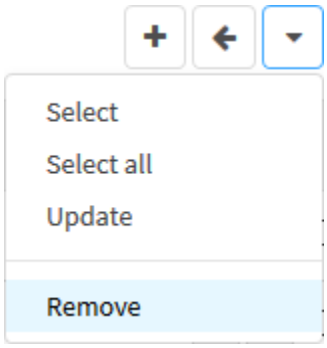
Through the action menu it is possible to delete several interfaces at the same time. Follow these steps:

1. Select the interfaces you want to delete by clicking on the **checkbox [ ]**;



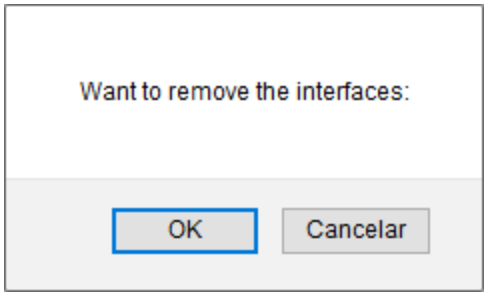
Interfaces - Selected interfaces

2. Click on the **Actions Menu [ ]** and select the option “Remove”;



Interfaces - Actions menu - Remove

3. A screen will appear asking if you want to delete the selected device:



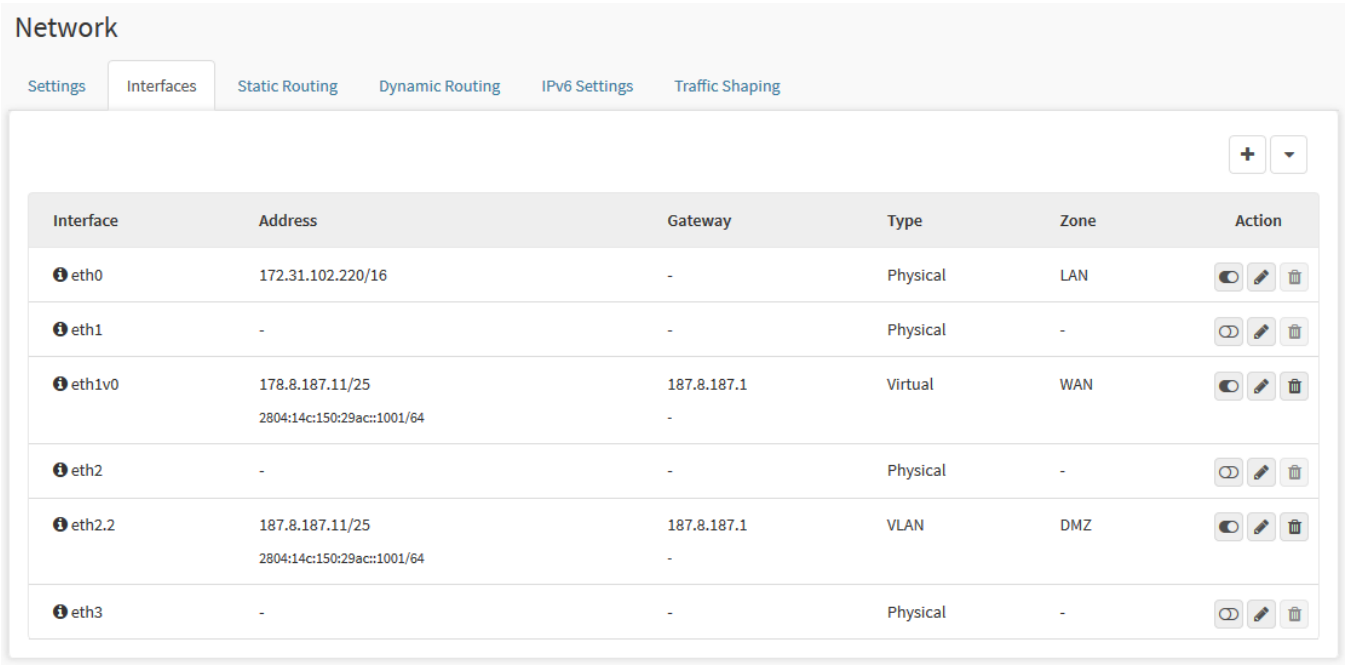
Interfaces – Remove interfaces

If you want to cancel, click the **[** Cancel **]** button. To complete the deletion click on the **[** OK **]** button.

The interface has been successfully deleted.

Interfaces - Columns

Below we will explain each column of the Interfaces tab:



Interfaces

- **Select [ ]:** Allows you to select an Interface*;*
- ***Interface*:** Displays the interface, in addition, when placing the mouse under the **[ ]** icon, the description of the interface will be displayed in a drop-down menu;
- ***Address*:** Displays addresses for the interface;
- ***Gateway*:** Displays the registered interface gateway;
- ***Type*:** Displays the type of interface, can be *physical* (represents physical ethernet interfaces), *Virtual*, *VLAN*, *DSL*, *Aggregation* (represents LAG interfaces), *Bridge and Tunnel*;
- ***Zone*:** Displays the registered zone, by default, it can be LAN, WAN or DMZ;
- ***Actions*:** Provides the following essential actions:
    - ***Enable*[ ]/*Disable*[ ]:** Allows you to enable or disable the interface;
    - ***Edit*[ ]:** It allows to edit the settings of the interface added in the Interface Add Button;
    - ***Delete*[ ]:** Allows you to remove an interface, it is equivalent to the *Remove* option in the actions menu.

Packet Fragmentation and MTU

In this session we will delve into how fragmentation works and address its harms, detail MTU and other related resources, its influence on MPLS, IPSEC, GRE packet transport and some recommendations to ensure the correct transmission of datagrams. Topics covered:

- Packet fragmentation;
- MTU, Jumbo Frame and MSS;
- Fragmentation, MTU and Baby Giants in MPLS;
- Fragmentation in IPSEC and GRE.

We will start by detailing the fragmentation of packages.

Package Fragmentation

By convention, whenever a host forwards an IPv4 packet (datagram) over the network, it cannot be larger than the maximum size supported by the network in question. The maximum acceptable limit is stipulated not only by the network data link, but also by the MTU (Maximum transmission unit), according to RFC 894, most ethernet devices use a maximum value of 1500 bytes, but several factors can interfere with transmission making these values smaller, for example, ethernet networks that are using SNAP (Subnetwork Access Protocol), passing through the LLC layer (Logical link control) or PPPoE (Point-to-Point Protocol over Ethernet) networks have an MTU of 1492 bytes, taking into account that the maximum size of an IPv4 datagram is 65535 bytes, when the packet reaches a point in the network where the MTU is smaller than its size, it is necessary to fragment packets.

Below is a reference table of the standard MTU value for some types of networks.

MTU x Protocol table

Network	MTU (in bytes)
***WLAN* 802.11**	7981
Ethernet Jumbo Frames	1501 - 9198
Token *Ring* 802.5	4464
FDDI	4352
Ethernet	1500
IEEE 802.3 / 802.2	1492
PPPoE	1492

IP fragmentation is a procedure that segments packets into parts that have an equal or minor size than that established on the limits, thus making it possible to carry out their transfer over a transmission link that has an MTU smaller than the original packet. This process allows the fragments to be forwarded independently, which generates a better use of the network resources, in addition, thanks to fragmentation, very large packets can be transported without causing losses in performance and also facilitating transport to the destination host, if the packet is not fragmented then it will be discarded.

For more information regarding the fragmentation process, refer to RFC 791.

During the process of transferring the fragments to their recipient, the receiving host stores the received parts in a buffer while waiting for the transfer to be completed, if the transmission takes too long, the destination host may issue a timeout message and discard the fragments, however if the transfer is successful, the fragmented parts of the packet are recomposed by the receiving host using as base certain fields of the IPv4 protocol header, at the end of this process the recipient results in the original packet reconstituted concluding the communication between the hosts.

For more information on the package recomposition process, refer to RFC 815.

The fragmentation process has several negative aspects that cause it to be considered harmful:

- If a single fragment is lost during the transfer to the destination host, all fragments stored in the buffer are discarded, requiring retransmission of all fragments until the host has the necessary fragments to successfully reassemble the original package.;
- Packet fragmentation does not send the fragments in a defined order, being characterized by allowing the parts to be sent independently, this requires the receiving host to order the fragments once they are received;
- The IPv4 fragmentation process generates a small drop in the CPU and memory performance of all devices that perform this process;
- The receipt of fragments by the receiving host also generates a drop in performance because it requires that it allocate part of its memory to store the fragments and then recreate the original package;
- There are several devices that inspect the packets during transport, but thanks to fragmentation, only the first fragment of the packet will have the IPv4 header, which ends up causing conflicts with these devices.

Next we will detail the MTU and define Jumbo Frames and MSS.

MTU, Jumbo Frames and MSS

As denoted by the name, the function of the MTU is to define the maximum size of the data blocks to be manipulated in layer 3 of the OSI model. Effectively the MTU establishes a size limit for the IP packets to be sent in a single transaction of the network layer without having to reduce the packet size (fragmentation), the higher the value, the less the overhead, however as smaller MTUs end up increasing the need for fragmentation, network delays are consequently reduced.

If it is necessary to exceed the maximum transmission capacity of the MTU (1500 bytes), it is possible to enable Jumbo Frames. The latter are a data unit capable of transmitting up to a maximum of 9000 bytes, used over Ethernet links, the use of Jumbo Frames automatically causes more data to be transferred using a smaller amount of packets and precisely because it reduces the need for fragmentation a performance improvement causing less protocol overhead. Despite the positives, Jumbo Frames are configured differently according to the specifications of each manufacturer, so it is necessary to analyze whether all devices on the network are in agreement, if at some point the MTU is limited to 1500 bytes, the package will be discarded or fragmentation will occur, invalidating the benefits of the Jumbo Frame.

Another way to deal with an increase in MTU is to configure the MSS (Maximum Segment Size), it is a parameter of the TCP header whose purpose is to define the maximum data that will be transferred in a single segment. The MSS defines the maximum amount of data that a host is willing to accept in a single IPv4 packet without considering the TCP and IP header, it is also characterized by being negotiated during the handshake process and cannot exceed the limit established by the MTU.

 For more information about the MSS, refer to RFC 879 (for IPv4) and RFC 2460 (for IPv6).

Next we will detail the MPLS influence on the MTU and define Baby Giants.

Fragmentation, MTU and Baby Giants in MPLS

Thanks to the particular characteristics of how MPLS works, it ends up impacting the way traffic is routed: Effectively, MPLS adds labels that are used to create its own routing table, since each of these labels is equivalent to 4 bytes in length, there is interference in the size of the Ethernet frames. In normal use situations, this increase does not interfere negatively in the transmission of the packets, however, in the use of IPSEC VPN tunnels for example, the header of the data packets has its size increased even more.

Taking into account a scenario where the IP packet is already using the maximum possible size established by the MTU (1500 bytes), but it is not large enough to justify the use of Jumbo Frames (the packet is less than 1600 bytes), it is classified like a Baby Giant. Most of the time, switches and routers ignore the fact that packets of this type have exceeded the MTU limit and allow communication normally, but this depends on the specifications of each appliance on the network.

Considering this scenario, a way to prevent conflicts is to reduce the MTU of the IP, the MTU of the MPLS itself and the maximum size of the TCP segment (MSS) to transfer a maximum of 1500, so that the packets already with the added labels will not exceed the standard limit.

Considering a scenario where the size of the packages is large enough not to be considered a Baby Giant, it is recommended to use Jumbo Frames to increase the limit to 9000 bytes.

 For more information about MPLS, see this page.

Next, we will detail fragmentation in GRE and IPSEC tunnels.

Fragmentation in GRE and IPSEC tunnels

According to RFC 2784, GRE tunnels add 20 bytes in an IPv4 header and an additional 4 bytes in a GRE header, in addition, when encapsulating packets in another protocol, the frame in general ends up increasing in size and causing overhead in the header, which impairs transport by devices using a standard MTU, in the case of IPSEC, about 80 bytes (ESP and IP header) are added to perform the encapsulation, in addition, the encryption algorithms used in VPN tunnels can add more bytes to the transported datagrams (in the practice of padding for example) and finally, another impact factor is whether IPSEC is using the mode of transport or tunnel which can also cause more overload factors.

Thanks to all the points previously mentioned, it is very likely that there will be fragmentation in the packets sent and consequently lose in the performance of the VPN tunnel.

Considering this scenario where the size of the packets is always tending to exceed the MTU limits because of encapsulation, encryption and other factors, it is recommended: Adjust the MTU of the physical interface where the IPSEC was configured, set an MSS value in order to reduce the size of the transported segments and, if necessary, consider changing the encryption algorithm of your tunnel.

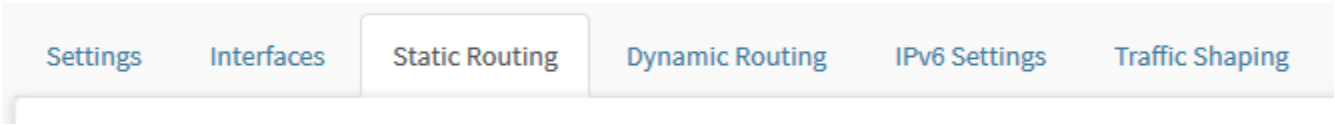
Network - Static Routing

Routing is a network layer resource, the purpose of which is to define the path taken by the packets to the destination. The device responsible for this activity is the router, and it has tables with the necessary information to determine the destination of the packets it receives.

This routing can be static being carried out through local routes defined by directly connected interfaces, or through address of gateways with the purpose of reaching a specific network or subnet.

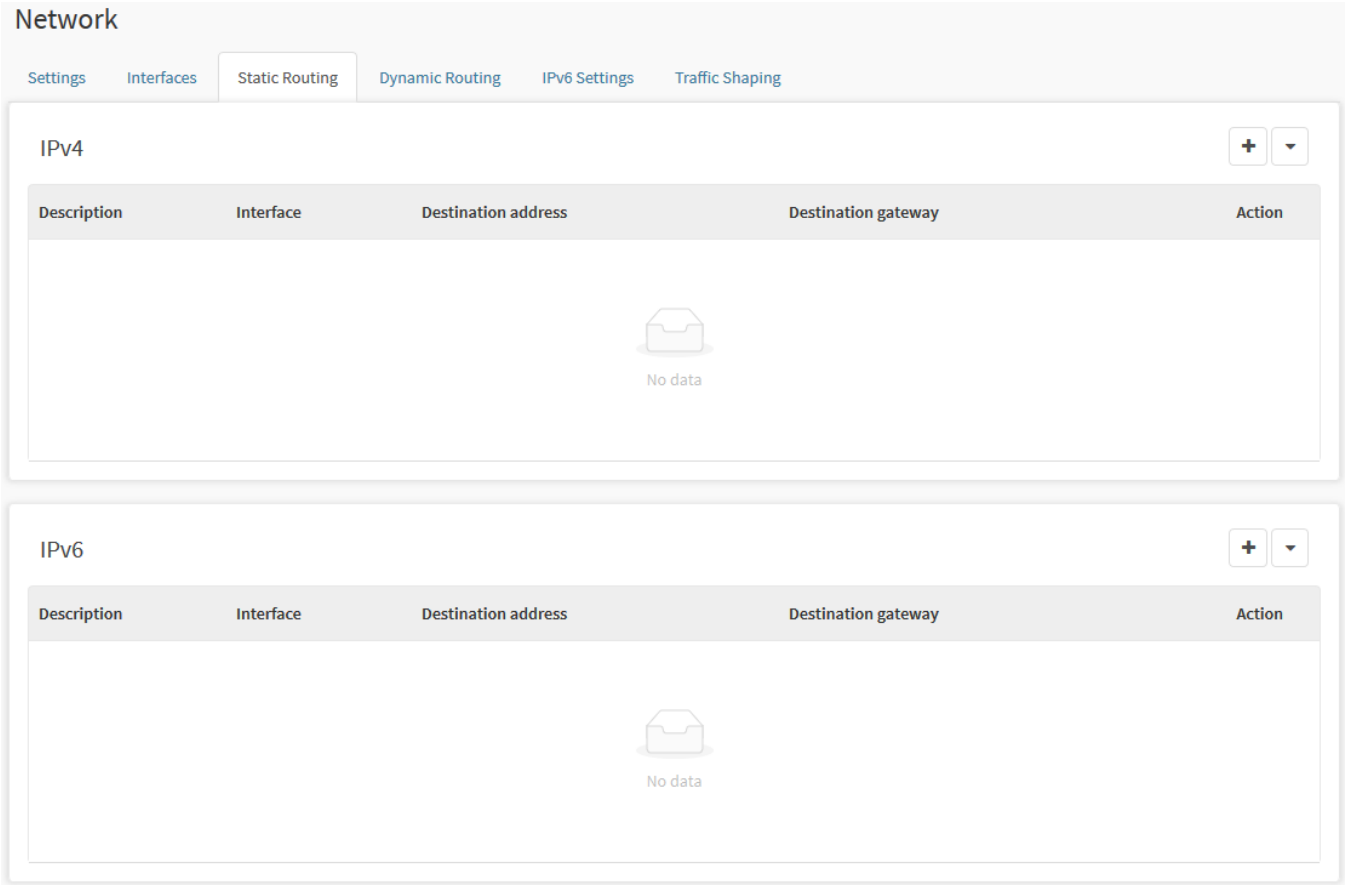
You can optionally add **IPv4** and / or **IPv6** addressing routes based on the configuration profile of your network environment.

Click on the Static Routing tab.



Static Routing tab

The “Static Routing” screen will appear, as shown by the image below:



Static Routing

This section will cover:

- Adding, editing and removing routes;

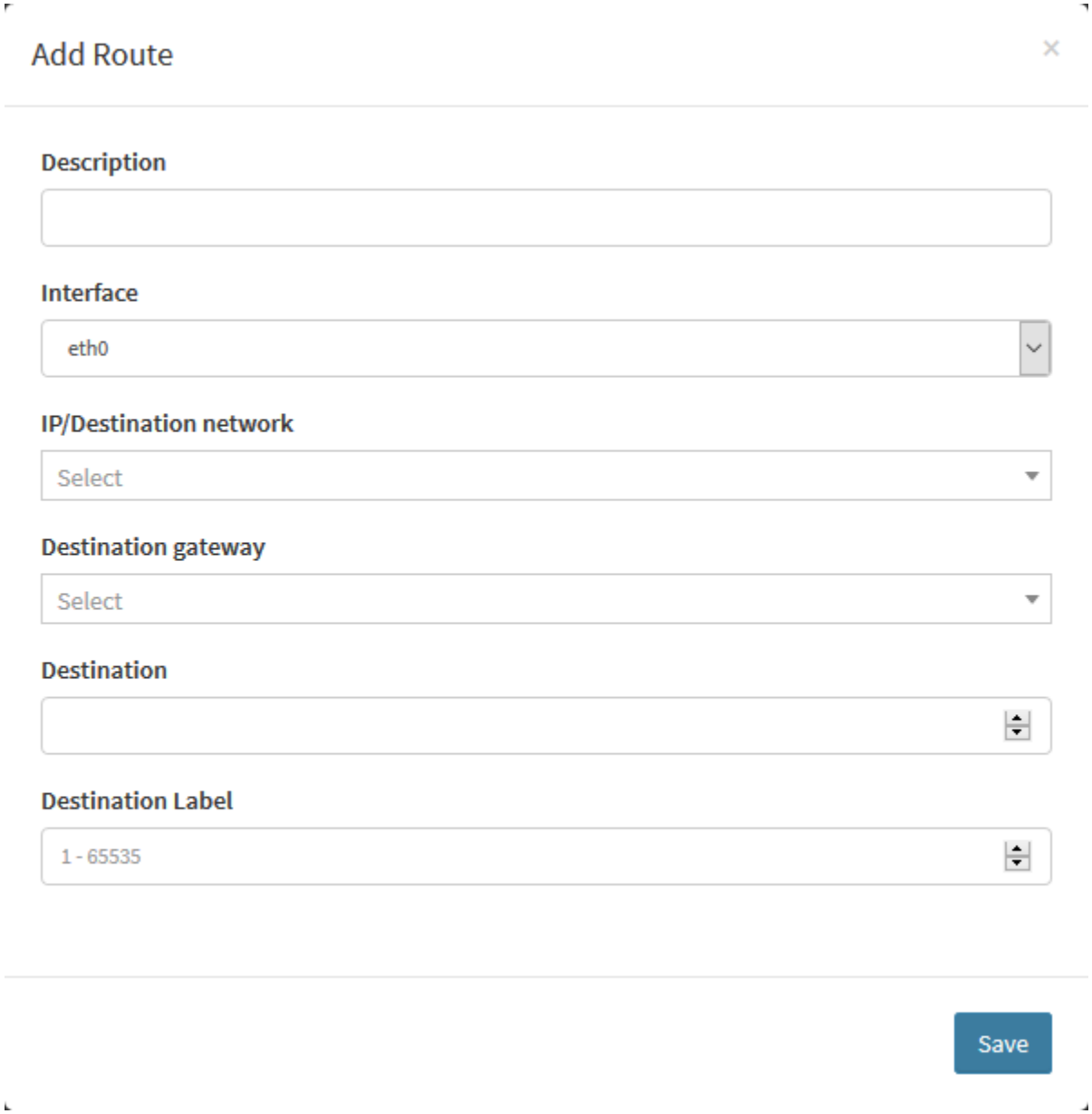
- Example of configuring Static Routes with MPLS support;
- Configuration example with ECMP support;

Next, we'll look at the add button at the top of this screen.

Static Routing - Add Button

To add a route, click **Add Route [+]** respectively for each **[*IPv4*]** and / or **[*IPv6*]** frame.

Next, we will exemplify the configuration according to the specifications of the form and the data of the fields for definition of the static routing for the destination network of the remote point of the “GRE tunnel” in the standard [IPv4]:



Add Route

- ***Description*:** Defines a description for identifying the configured static route. This is a required field. Ex.: “*Route Network*”;
- ***Interface***: Selection of the network interface corresponding to the device [ethX / tunX] that is connected to the outbound gateway device of the packet for the destination network. Usually refers to the communication interface between routers. Ex.: “[tun0]”;
- ***IP/ Destination network*:** Enter or select from the list the destination IP address / Network / Subnet to be reached. This is a required field. Ex.: “Class B network”;
- ***Destination gateway*:** Enter or select the gateway address from the list to access the destination network. This is a required field. Ex.: “172.31.0.1 /32”;

- ***Destination*:** Enter the "Administrative Distance" of the route to access the destination Gateway. The default value accepted in this field is 1, the minimum value is 1 and the maximum value is 225;
- ***Destination Label*:** This field will appear ONLY if the selected interface already has MPLS enabled. For more information, see the page. Enter the administrative distance label. The minimum value is 16 and the maximum value is 1048575.

Note that in the IP / Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If not, they will not appear in the list. For more information on creating an IP-type object, see this page.

To save changes, click [Save], otherwise, click the [ ] at the top of the window or click outside it to cancel the procedure.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

This same procedure applies to the configuration of an IPv6 route.

After performing these procedures the interface will have been successfully configured.

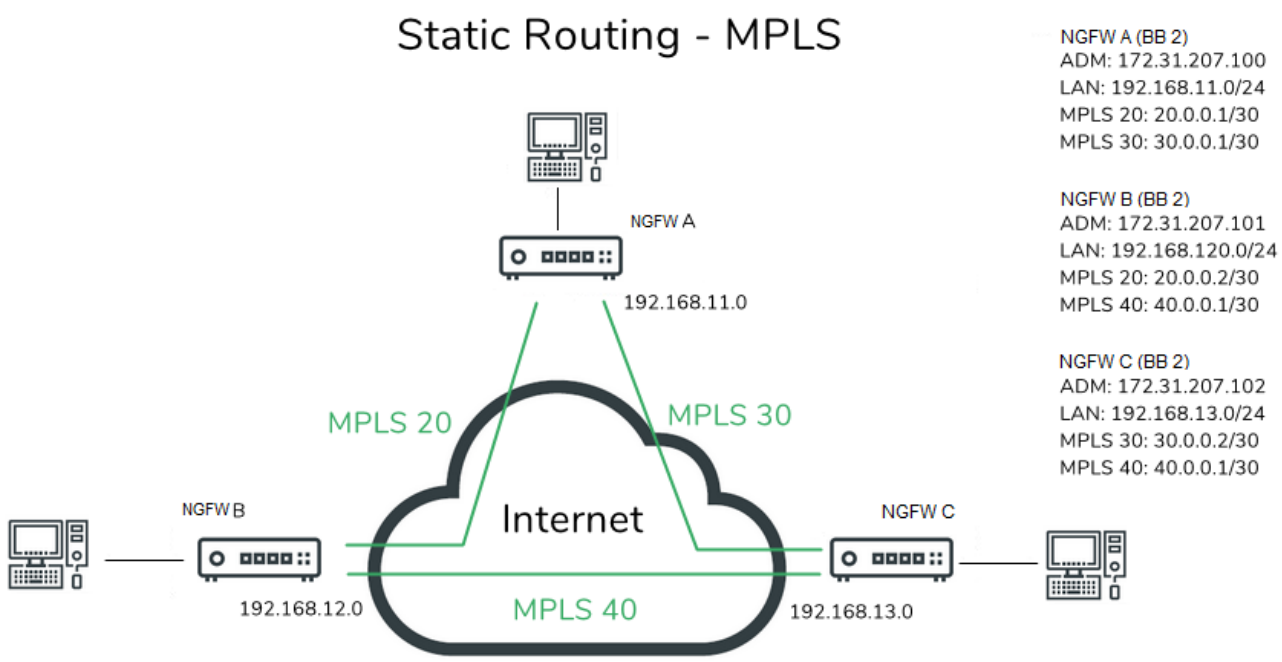
Access this page, to see an example of how to connect between two NGFWs using ECMP to perform dynamic routing.

Static Routing - MPLS

This section will present the step by step to configure a static route with MPLS.

For more information about MPLS, see this page.

This demonstration will take into account the following structure:



Dynamic Routing - Structure

In this structure, three NGFWs connected by MPLS will be interconnected. The following IPs will be used in this example:

ECMP - IP addressing

Name	LAN IP address	Links
NGFW A	192.168.11.1/24	20.0.0.1/30
		30.0.0.1/30
NGFW B	192.168.12.1/24	20.0.0.2/30
		40.0.0.1/30
NGFW C	192.168.13.1/24	30.0.0.2/30
		40.0.0.1/30

The steps we will take in this demonstration will be:

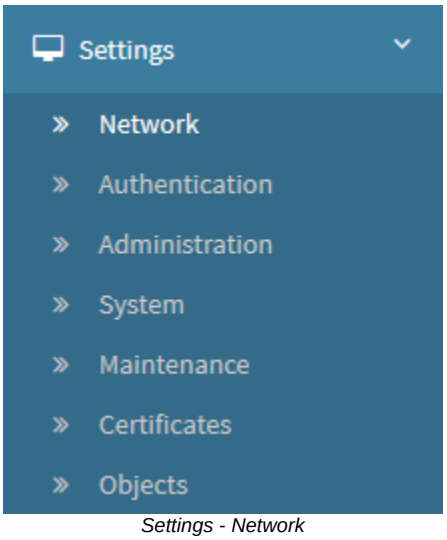
1. Configuring Interfaces on NGFW A;
2. Configuration of static routes in NGFW A;

3. Configuring the Interfaces on NGFW B;
4. Configuration of static routes in NGFW B;
5. Configuration of Interfaces in NGFW C;
6. Configuration of Interfaces in NGFW C;
7. Validation of Static Routing Configuration

We will start the demo by configuring the NGFW A interfaces.

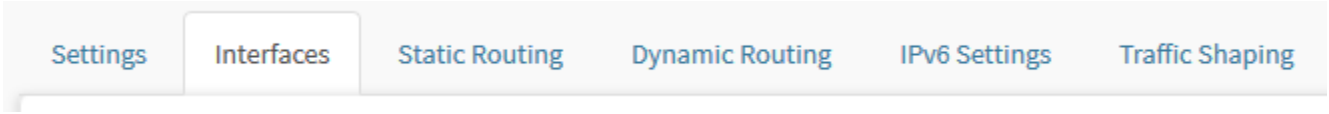
Static Routing - MPLS - Configuring Interfaces on UTM A

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab

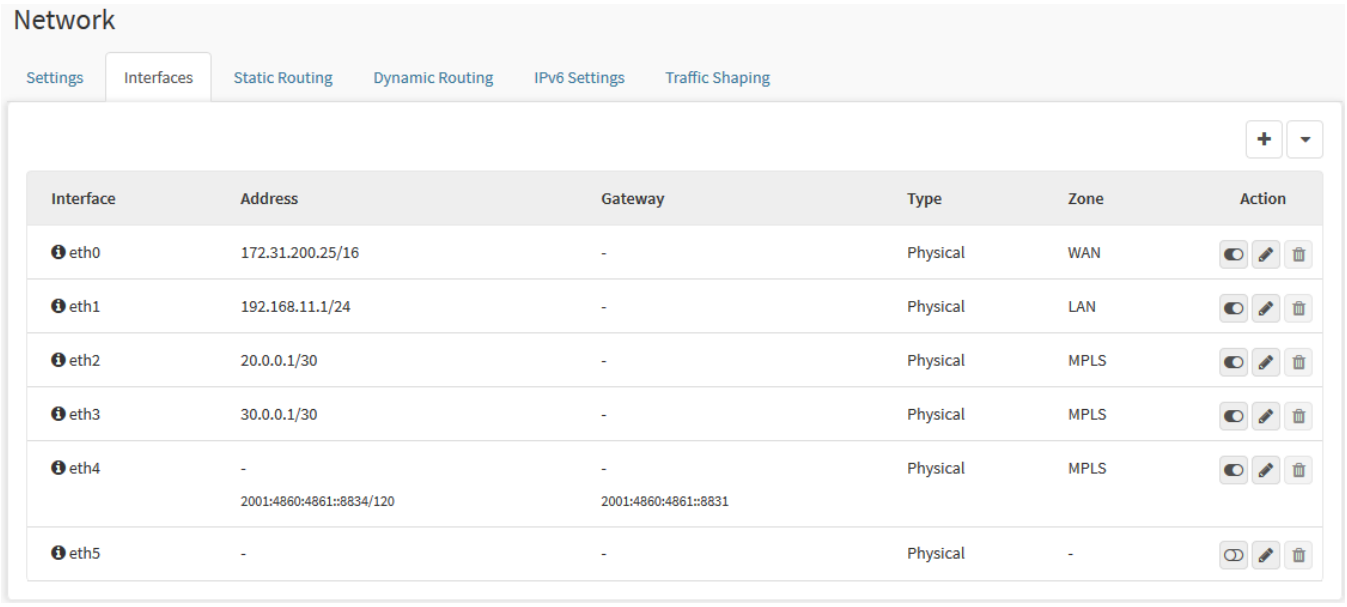
We will make the following settings in this step:

- Initially we will need to configure the NGFW A LAN (to serve as the destination of NGFW B and NGFW C);
- Configure the physical interfaces that will be used by MPLS:
  - MPLS20 Link;
  - MPLS30 Link.

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

For more information on MPLS interfaces, visit this page.

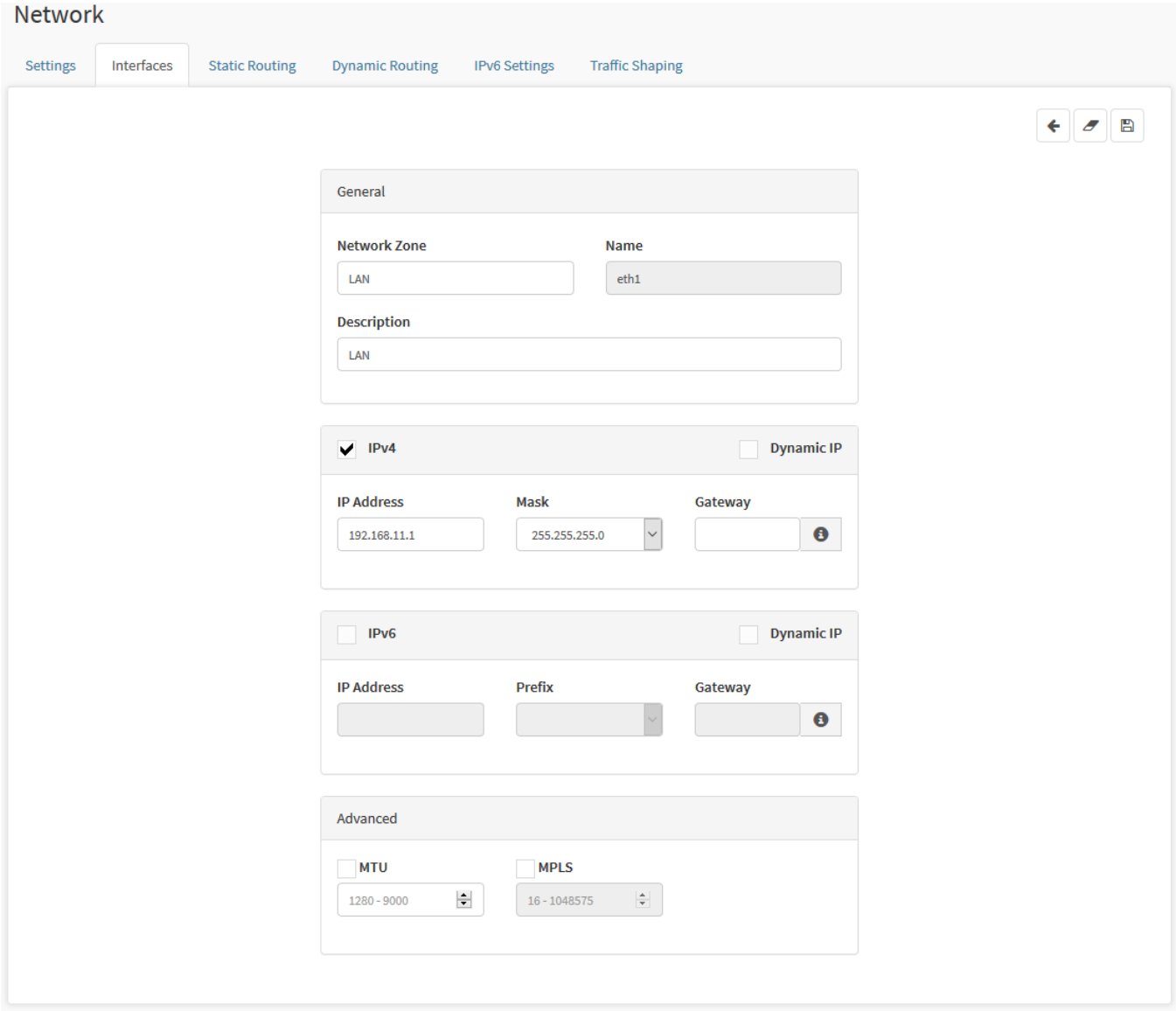
Below are the NGFW A interface configurations:



Network - Interfaces

LAN configuration of NGFW A

Access the physical interface you will use and click [ ]. A seguinte tela será exibida:

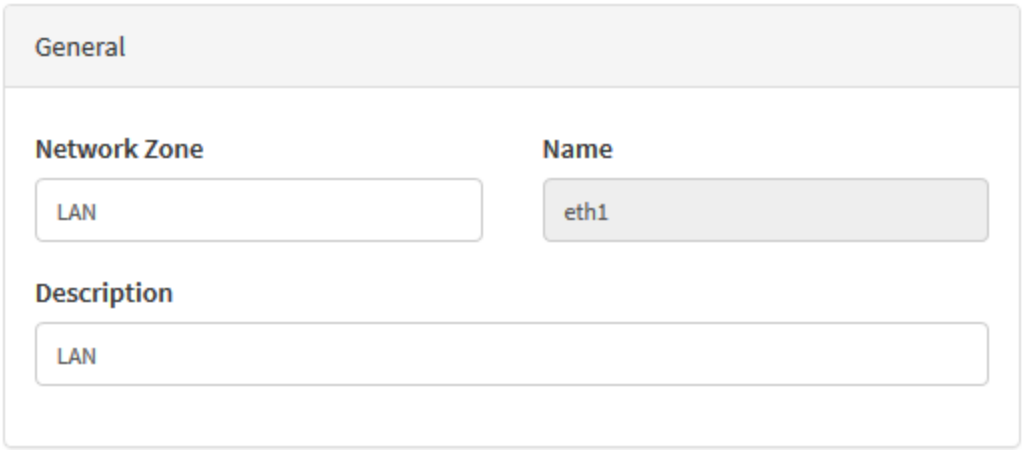


Interfaces - eth1

Next we will detail the panels that we will need to configure.

General - Panel

Complete the form as shown below:

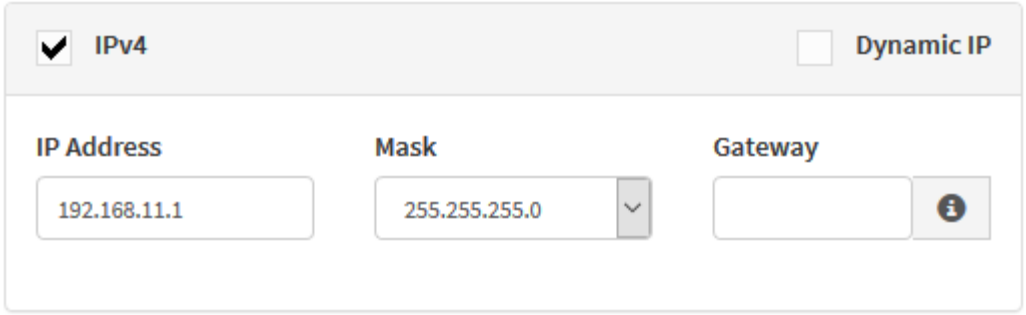


Interfaces - General Panel

- ***Network Zone*:** In this example we will name the zone "LAN";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: LAN.

IPv4

Complete the form as shown below:



Interfaces - IPv4

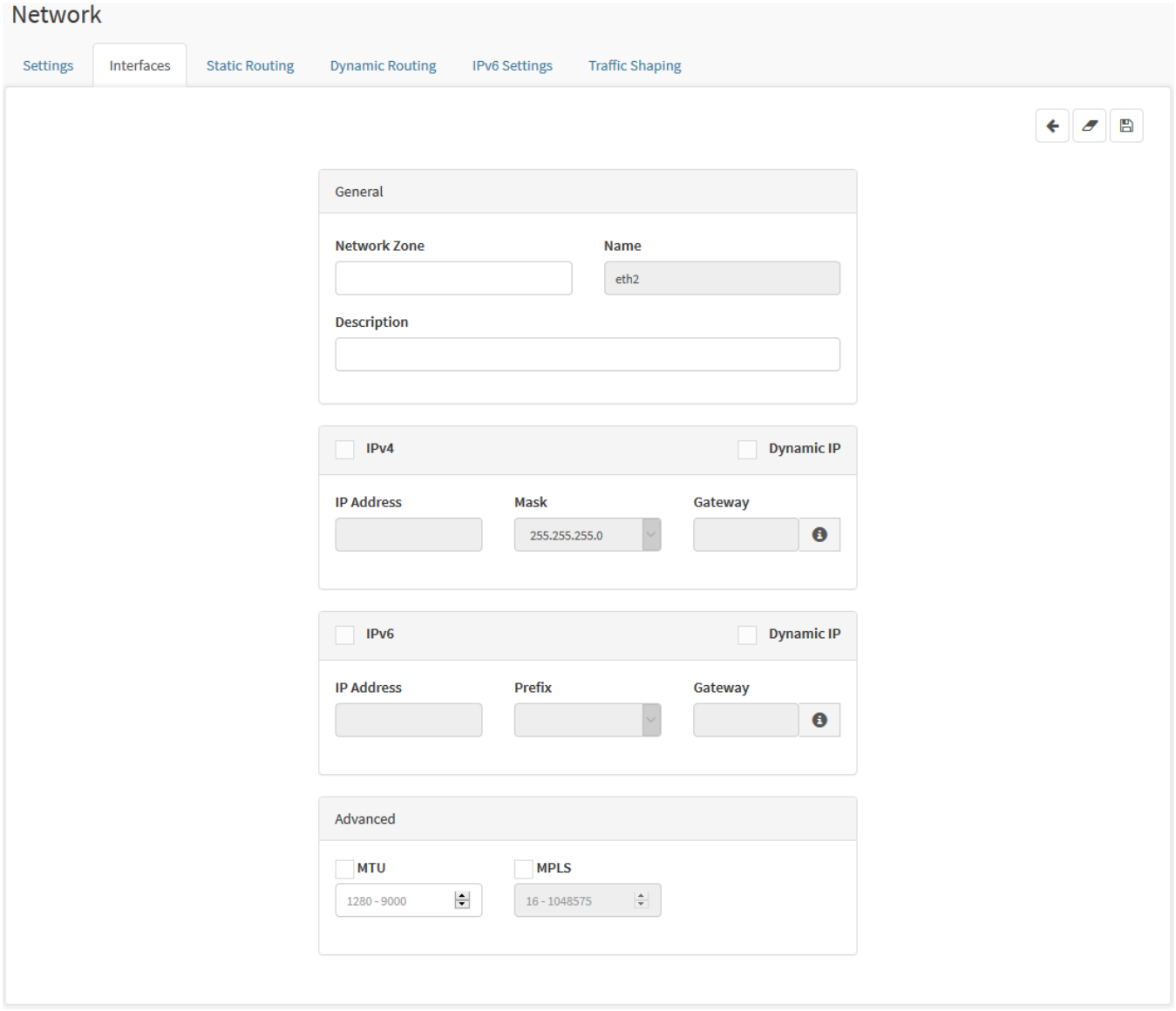
- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW A, in this case, it will be: 192.168.11.1;
- **Mask:** Select the netmask to be used by NGFW A.

To save, click **[ ]**.

This completes the LAN configuration of NGFW A. Next we will configure the interfaces that will be used by MPLS.

Link MPLS20

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

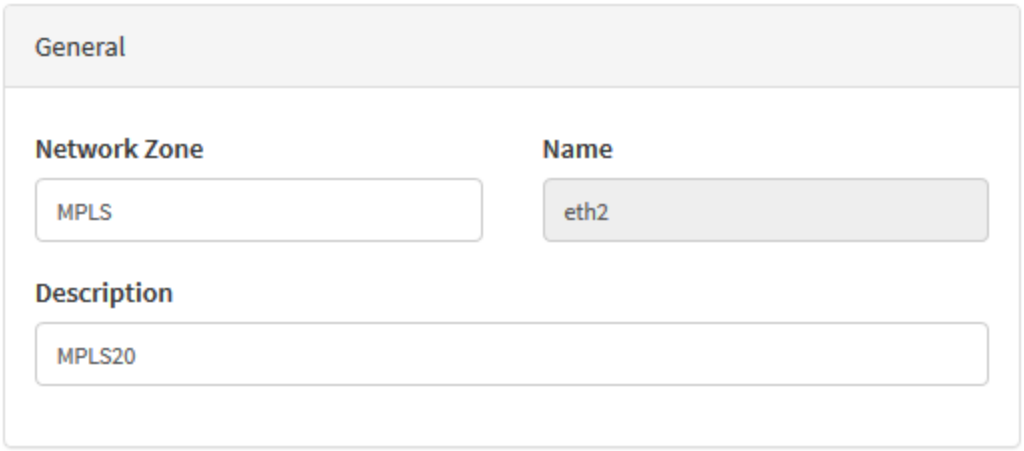


Interfaces - eth2

Next we will detail the panels that we will need to configure.

General - Panel

Complete the form as shown below:

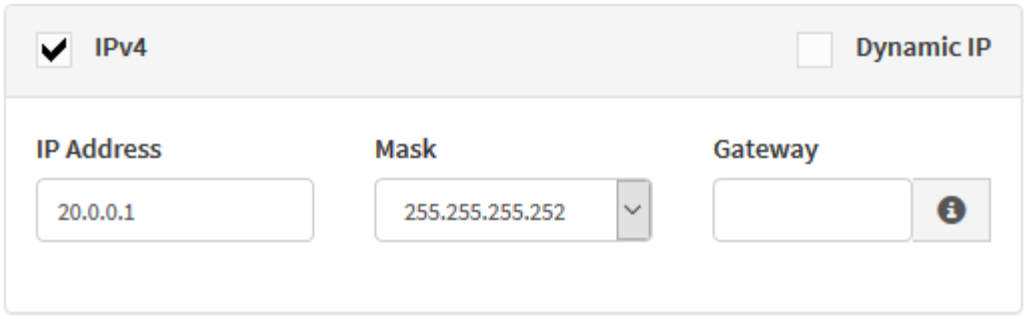


Interfaces - General Panel

- ***Network Zone*:** To organize, we will name the zones that we will use as "MPLS";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: MPLS20.

IPv4

Complete the form as shown below:

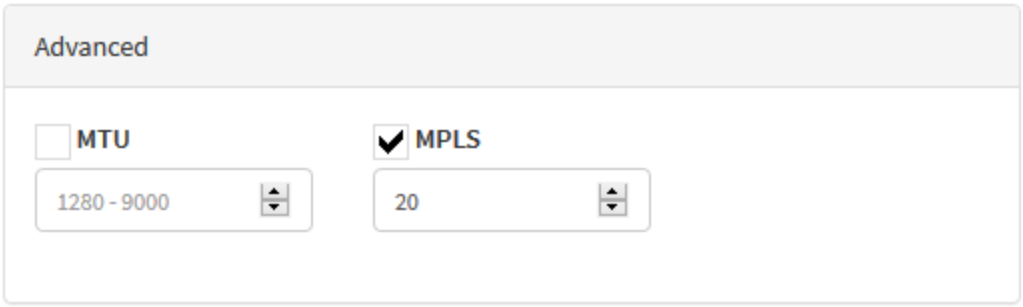


Interfaces - IPv4

- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by MPLS, in this case, it will be: 20.0.0.1;
- **Mask:** Select the netmask to be used.

Advanced

Complete the form as shown below:



Interfaces - Advanced

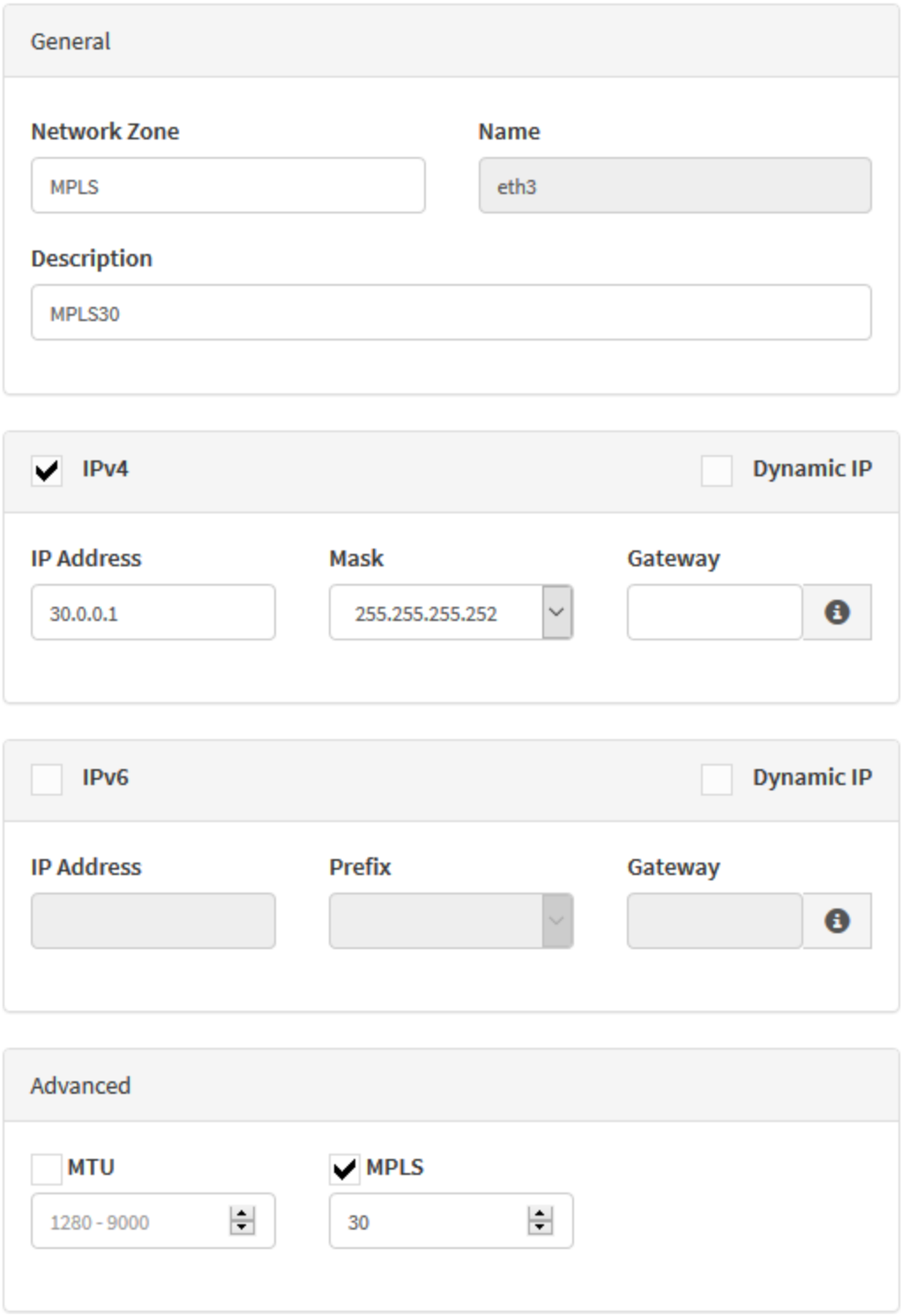
- ***MPLS[ ]:*** *Enable this option for MPLS to be activated*. In this example we will use as a label the value: "20".

To save, click **[ ]**.

This completes the configuration of the MPLS20 interface. Follow the same steps to configure the other links*:*

Link MPLS30

Below, an image demonstrating how the MPLS30 link should be configured:



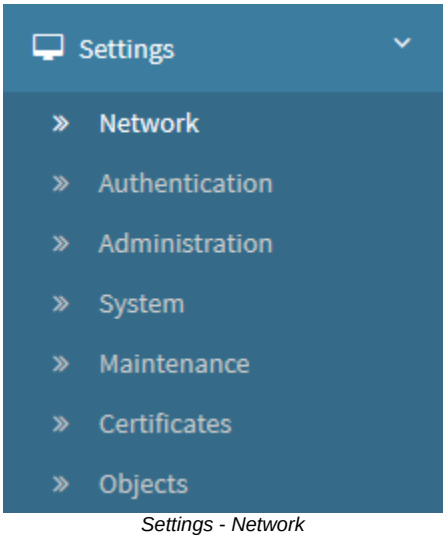
Interfaces - MPLS30 Config

This finalizes the configuration of the Interfaces in NGFW A, next we will configure the static routes.

Static Routing - MPLS - Configuration of static routes in UTM A

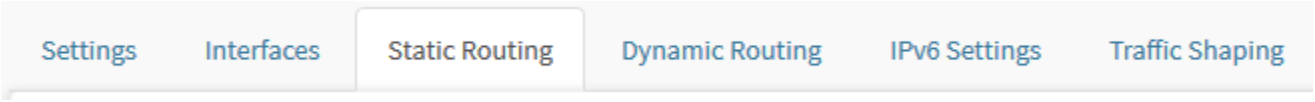
After configuring the interfaces, follow the steps below:

Still in Settings, in the Network option:



Settings - Network

Click on the Static Routing tab:

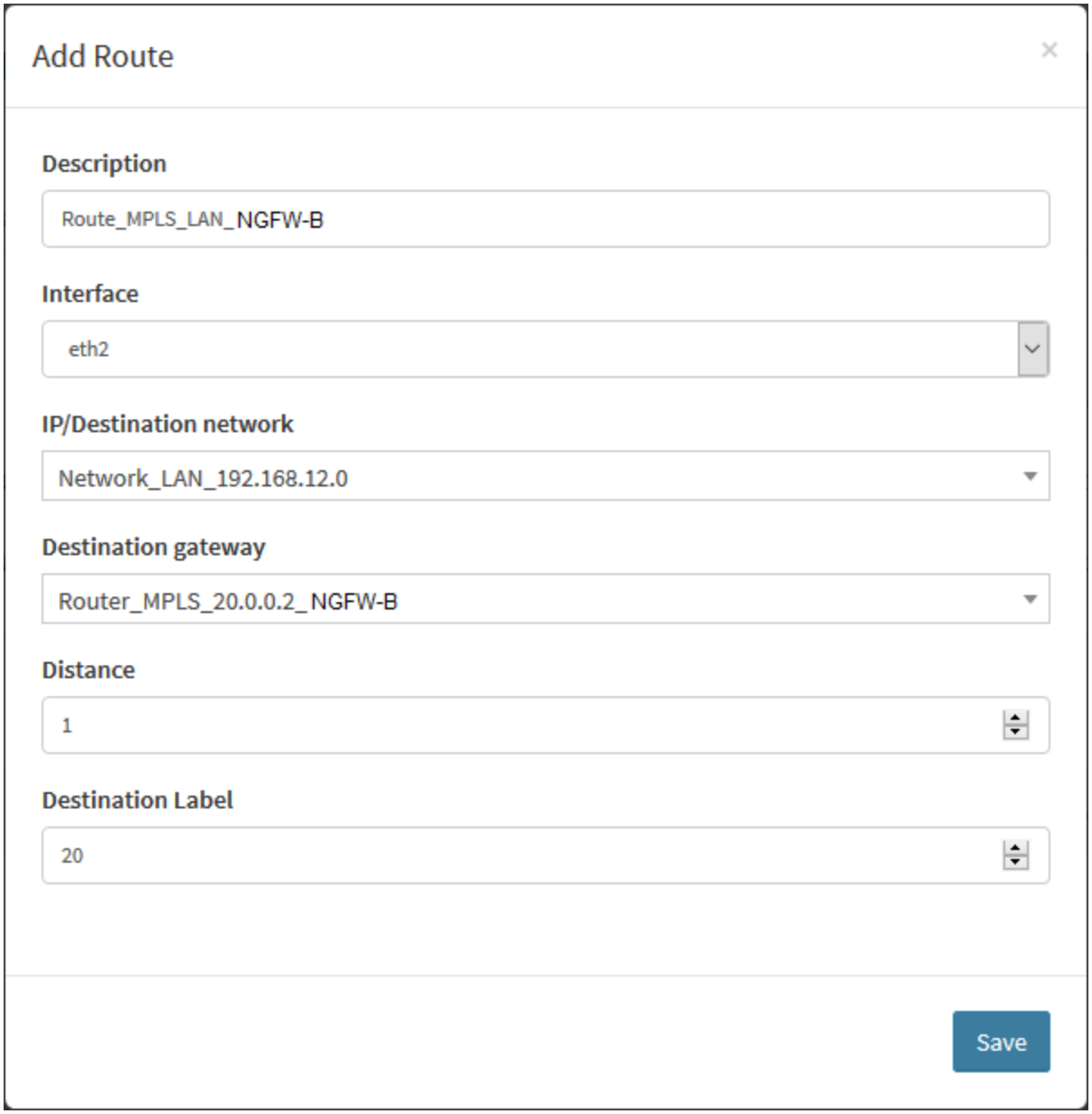


Static Routing tab

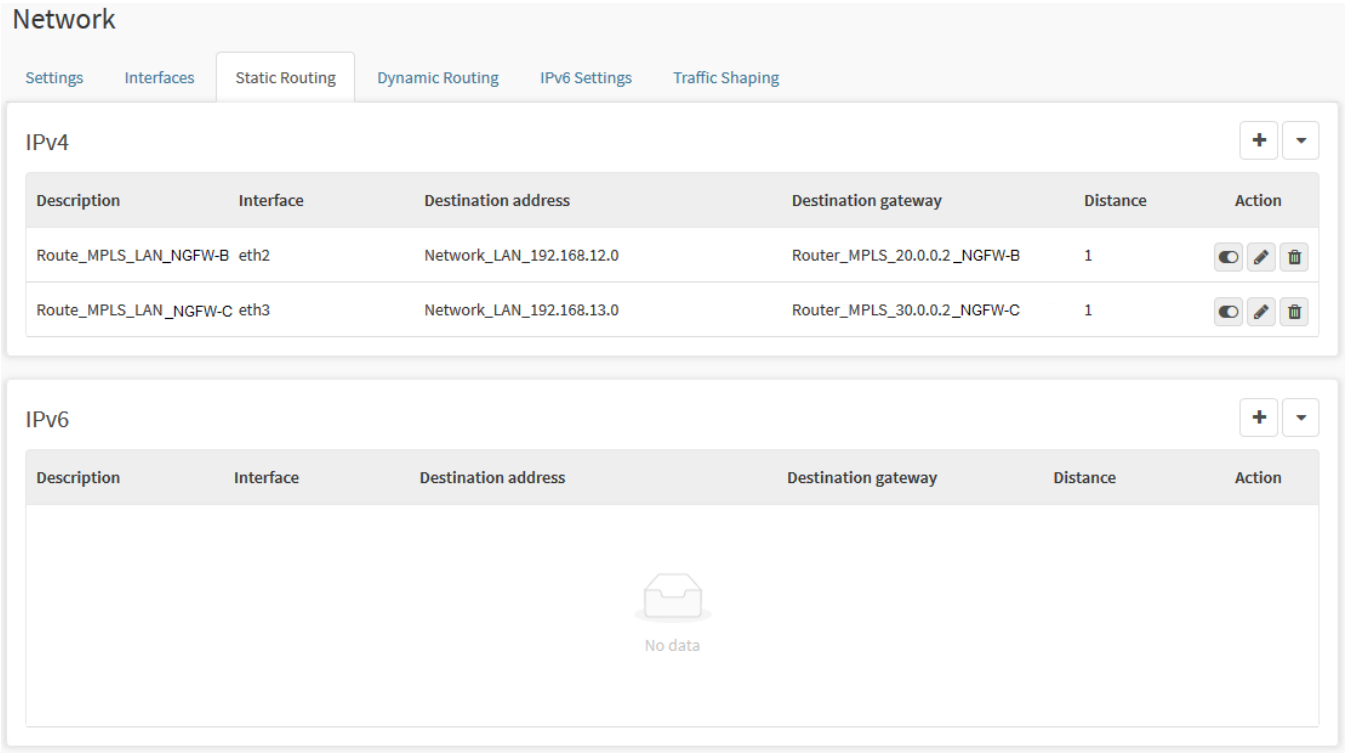
In this step, we will configure the static route using the IP of NGFW B and NGFW C as destination.

Some details of the static routing tab will not be considered in this example, if you want more information, see this page.

Below are the NGFW A interface configurations:



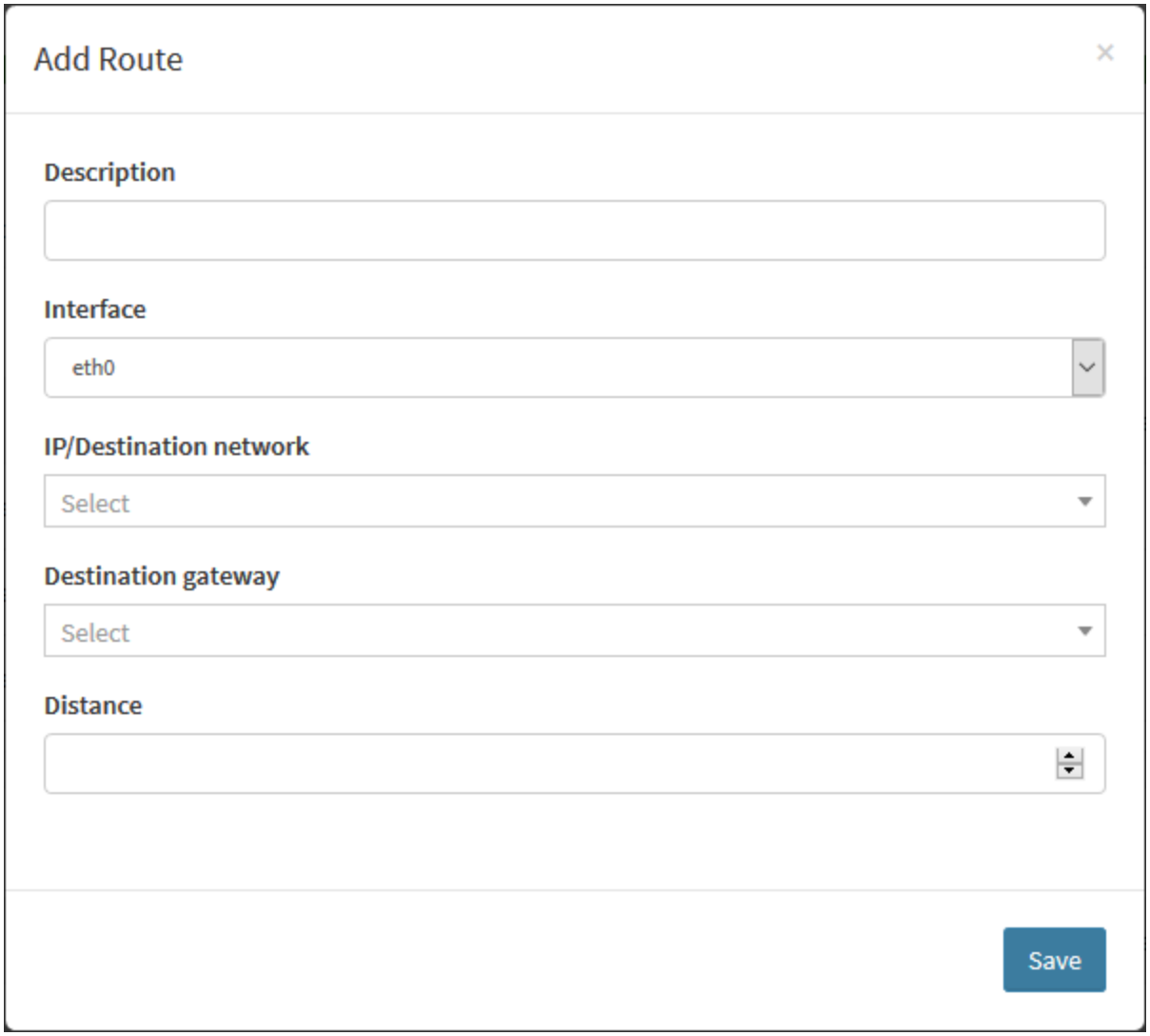
Route settings



Network - Static Routing

LAN MPLS route to NGFW B

Click **[**  **]** to create a new route. The following window will be displayed:

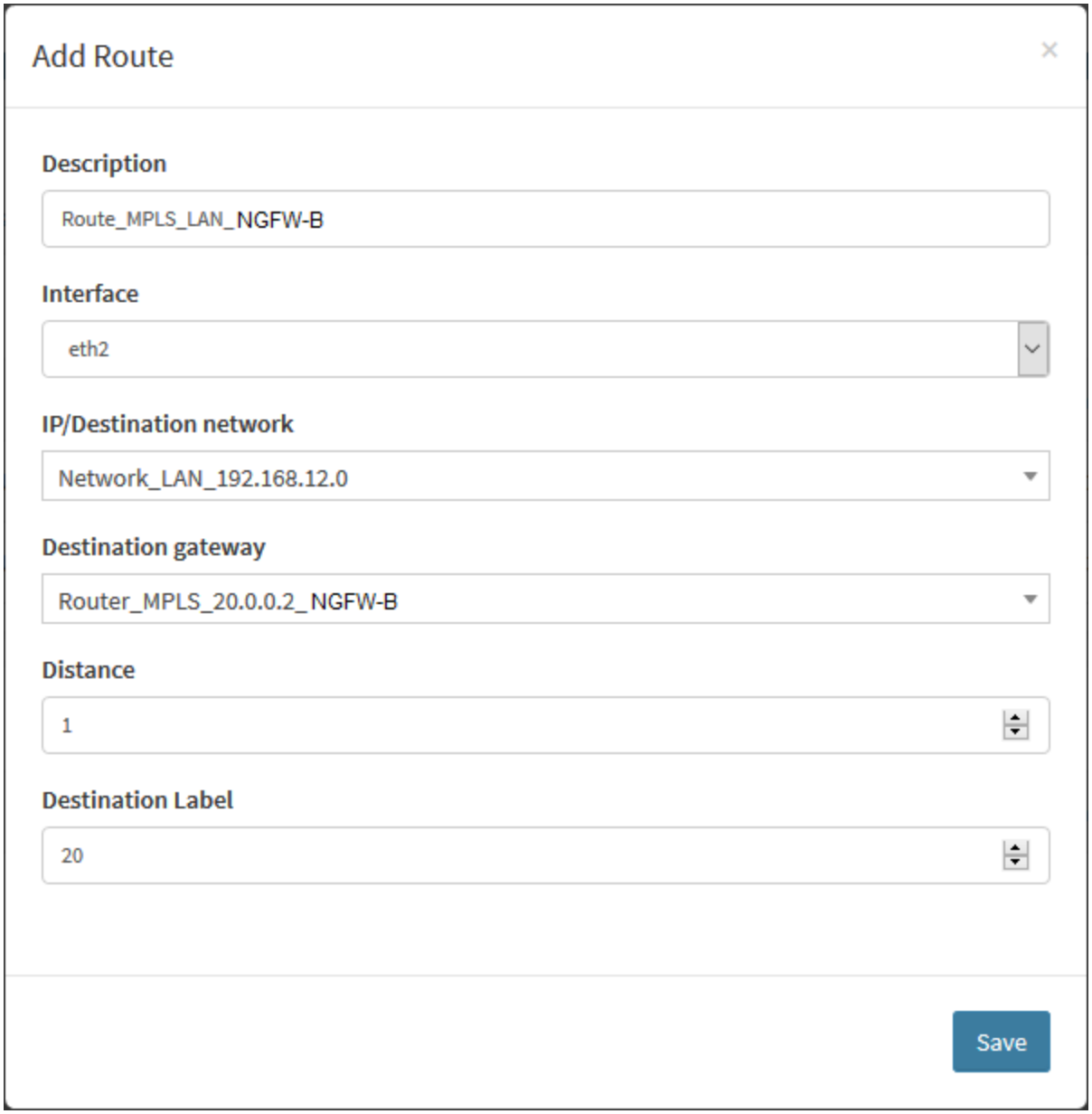


Static Routing - Add Route

- ***Description*:** To organize, we will name the routes using the syntax: "Route_MPLS_LAN_NGFW-B";
- ***Interface*:** Define the same interface that was used to configure the MPLS link with NGFW-B, in this case it will be "eth2", thanks to this interface having MPLS, the Destination Label field will be displayed;
- ***IP/Destination Network:*** *Configure using the NGFW B IP as the destination, in this case we will use a single IP object containing the address: 192.168.12.0, we name this object as "Network_LAN_192.168.12.0"*;
- ***Destination Gateway*:** Determine the router as the destination gateway, in this case we will use a single IP object containing the address: 20.0.0.2, we name this object "Router_MPLS_20.0.0.2_NGFW-B";
- ***Distance*:** Set the administrative distance, in this example, we will use the value "1";
- ***Destination Label*:** As the destination label we will use the value: "20".

Note that in the IP / Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If not, they will not appear in the list. For more information on creating an IP-type object, see this page.

When finished, the static route must be configured this way:



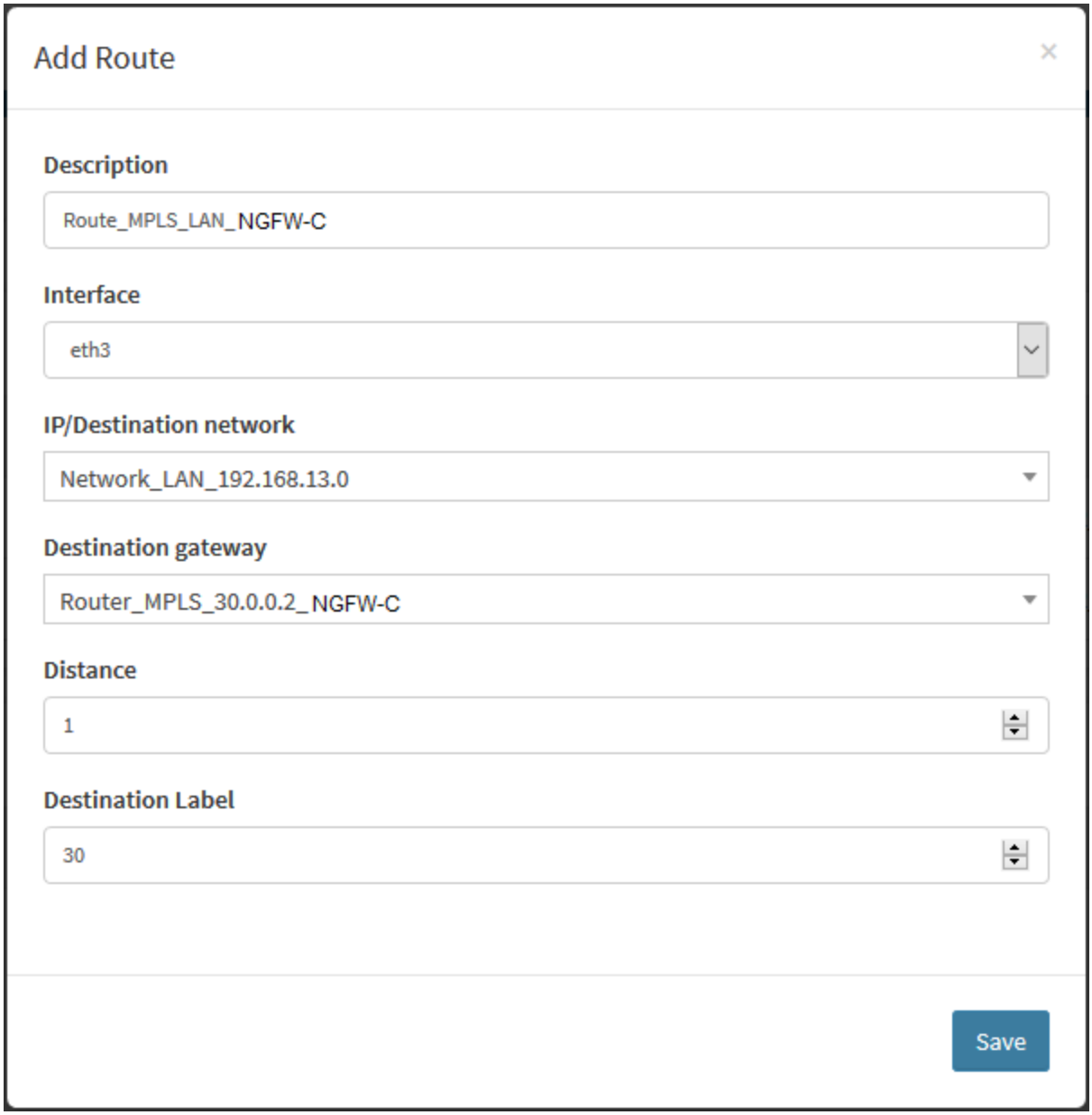
Static Routing - Add Route - Route_MPLS_LAN_NGFW-B

To finish the settings, click [Save].

This completes the configuration of the static route from NGFW A to NGFW B. Follow the same steps to configure the route from NGFW A to NGFW C*:*

LAN MPLS route to NGFW C

Below, an image demonstrating how the NGFW C route should be configured:



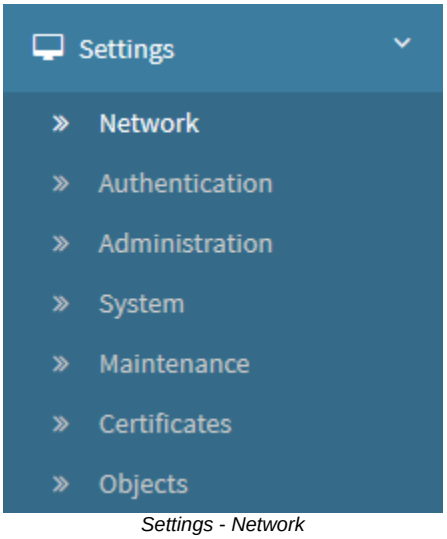
Static Routing - Add Route - Route_MPLS_LAN_NGFW-C

This finalizes the configuration of the static routes in NGFW A, next we will configure NGFW B.

Static Routing - MPLS - Configuring the Interfaces on UTM B

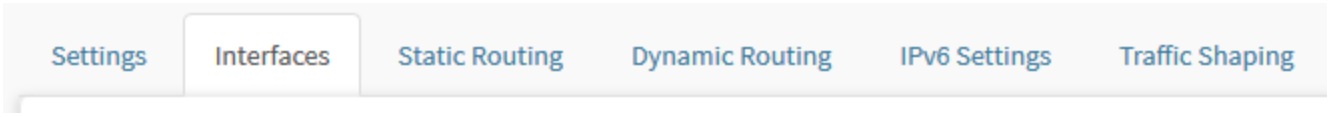
The procedures we will do here will be identical to the ones we did in NGFW A, but referring to NGFW B.

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab

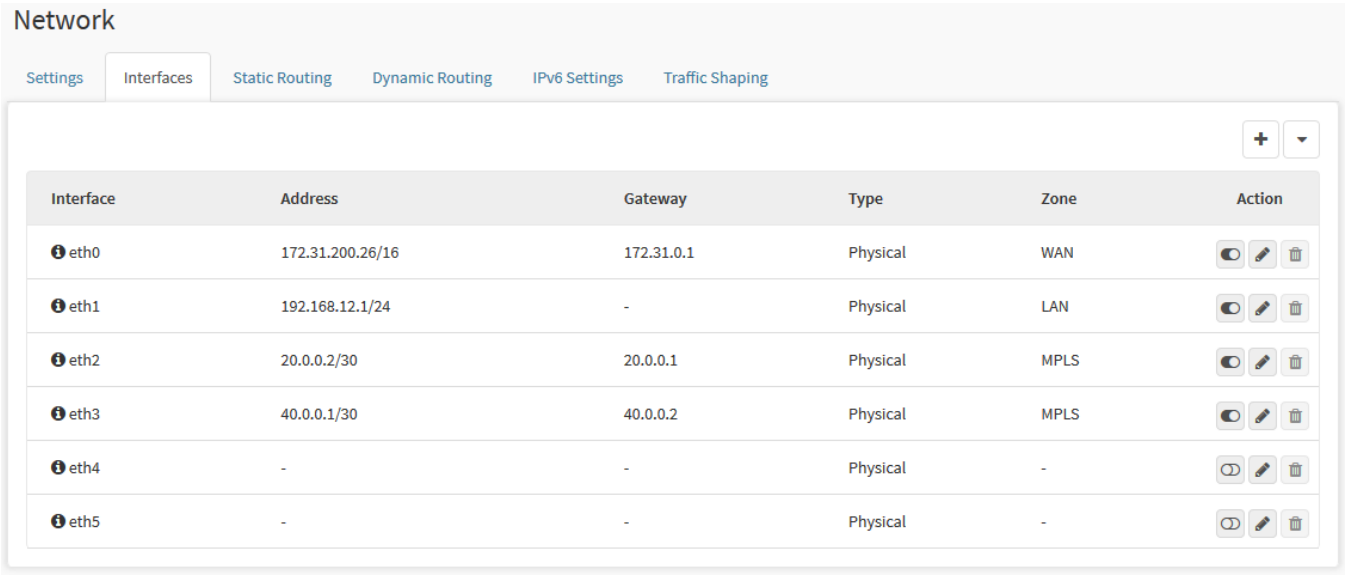
We will make the following settings in this step:

- Initially we will need to configure the NGFW B LAN (to serve as the destination of NGFW A and NGFW C);
- Configure the physical interfaces that will be used by MPLS:
  - *Link* MPLS21;
  - *Link* MPLS40.

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

For more information on MPLS interfaces, visit this page.

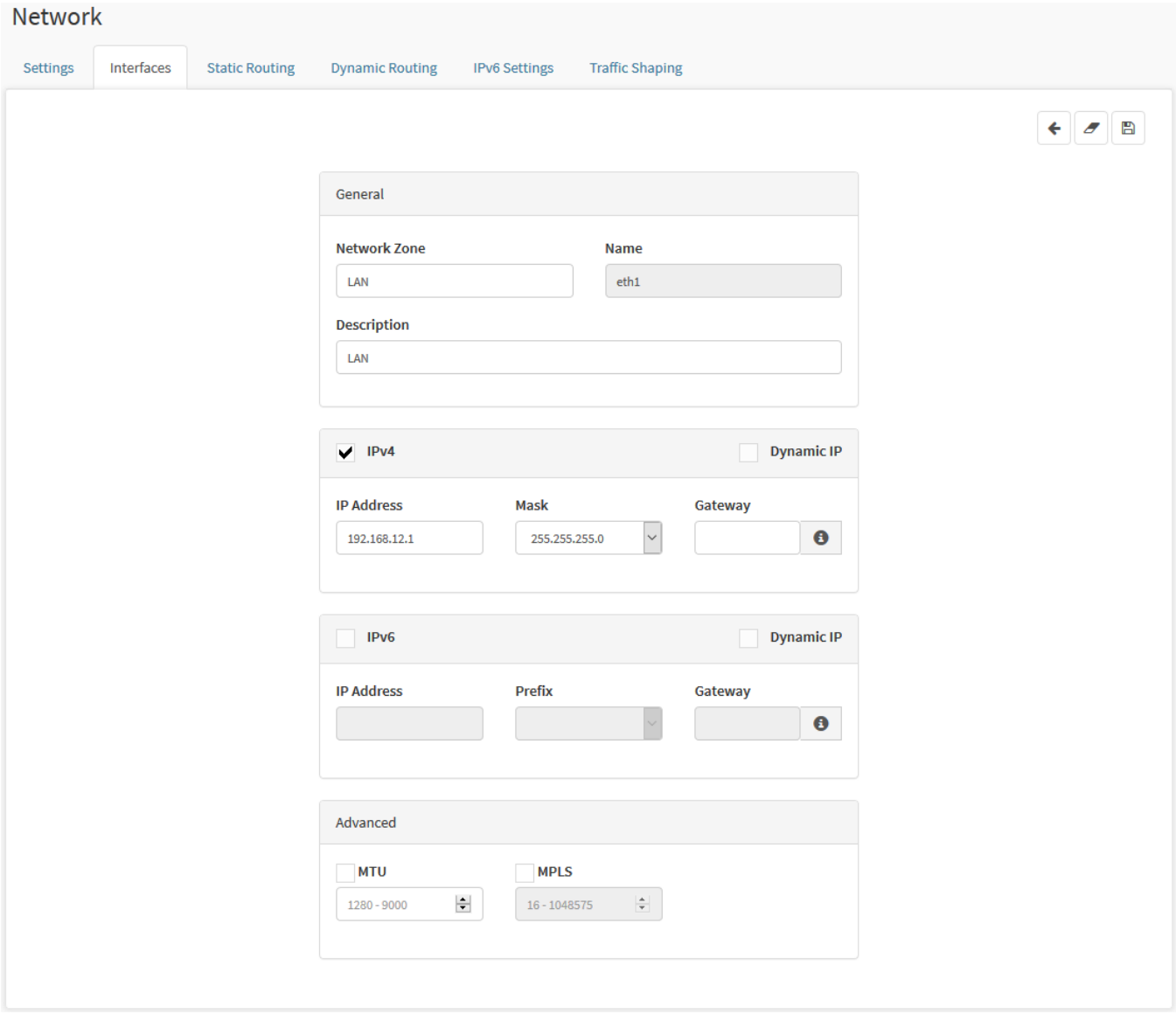
Below are the NGFW B interface configurations:



Network - Interfaces

LAN configuration of the NGFW B

Access the physical interface you will use and click [ ]. The following screen will be displayed:

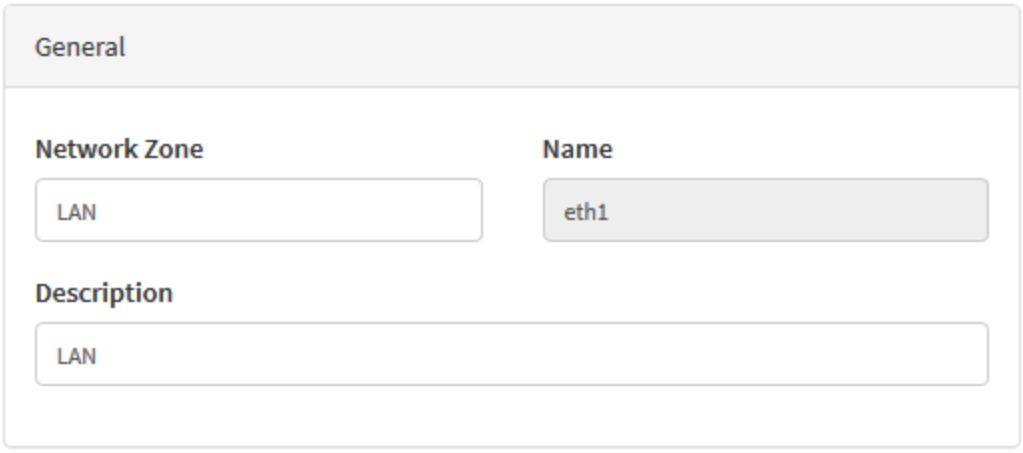


Interfaces - eth1

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

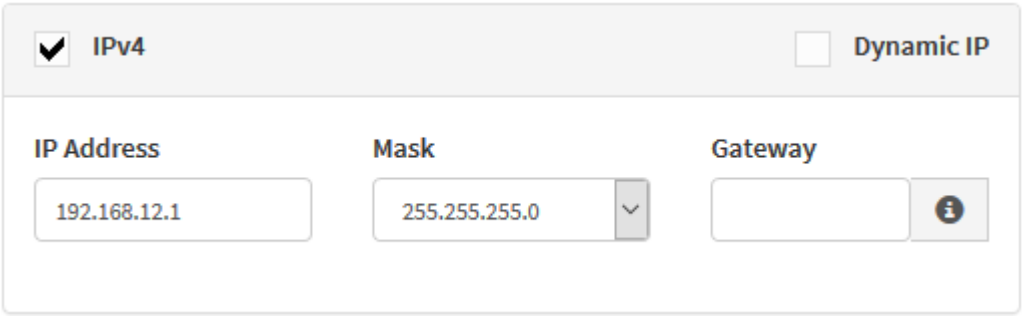


Interfaces – General Panel

- ***Network Zone*:** In this example we will name the zone "LAN";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: LAN.

IPv4

Complete the form as shown below:



Interfaces - IPv4

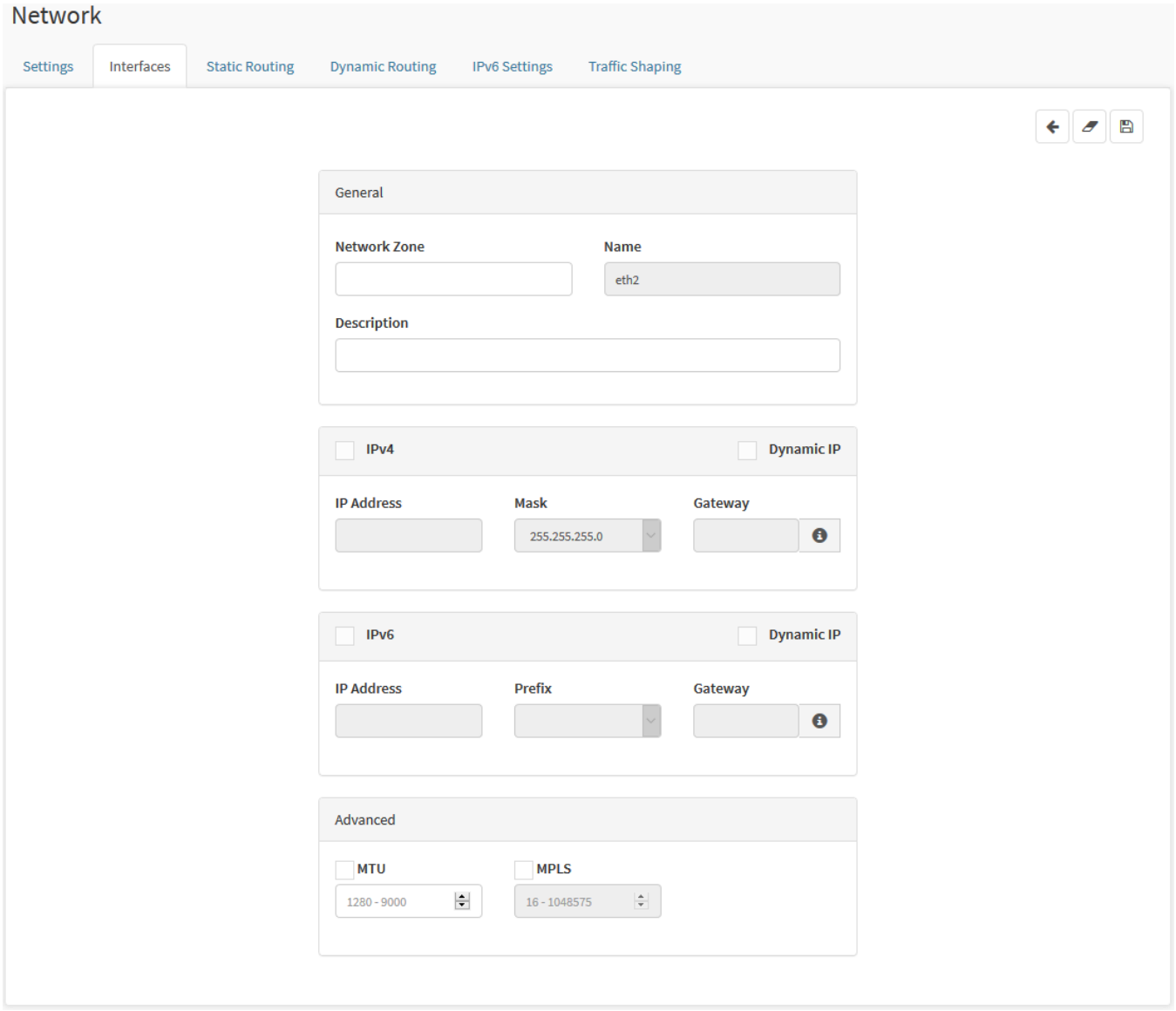
- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW B, in this case, it will be: 192.168.12.1;
- **Mask:** Select the netmask to be used by NGFW B.

To save, click **[ ]**.

This completes the NGFW B LAN configuration. Next we will configure the interfaces that will be used by MPLS.

Link MPLS21

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

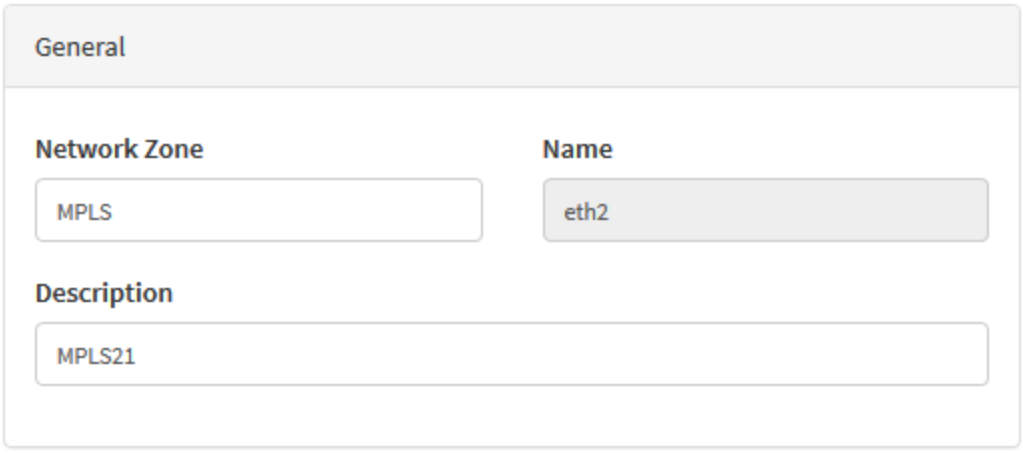


Interfaces - eth2

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

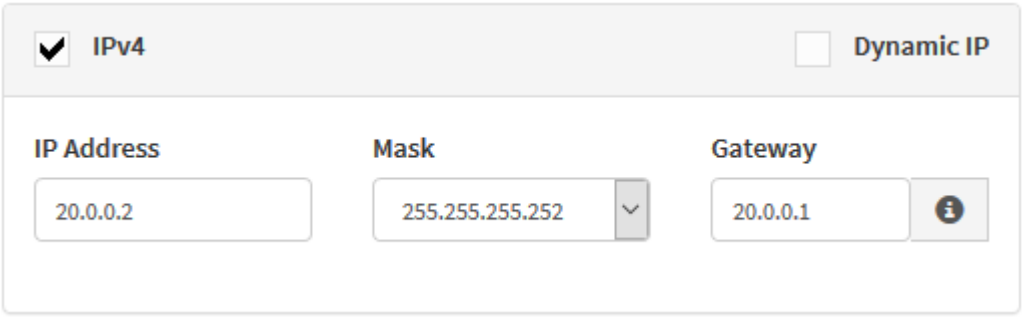


Interfaces – General Panel

- ***Network Zone*:** To organize, we will name the zones that we will use as "MPLS";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: MPLS21.

IPv4

Complete the form as shown below:

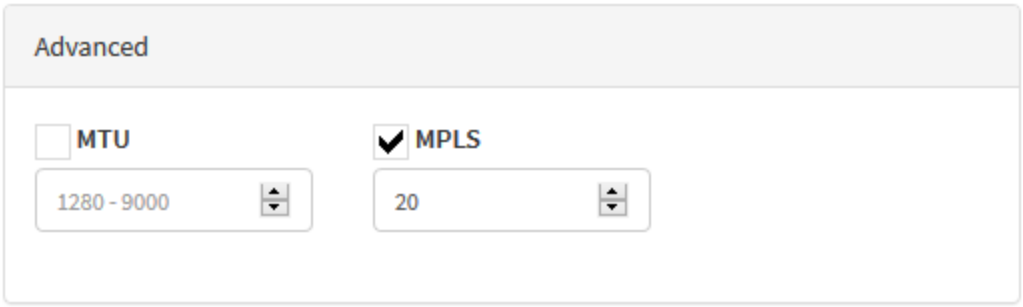


Interfaces - IPv4

- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by MPLS, in this case, it will be: 20.0.0.2;
- **Mask:** Select the netmask to be used.

Advanced

Complete the form as shown below:



Interfaces - Advanced

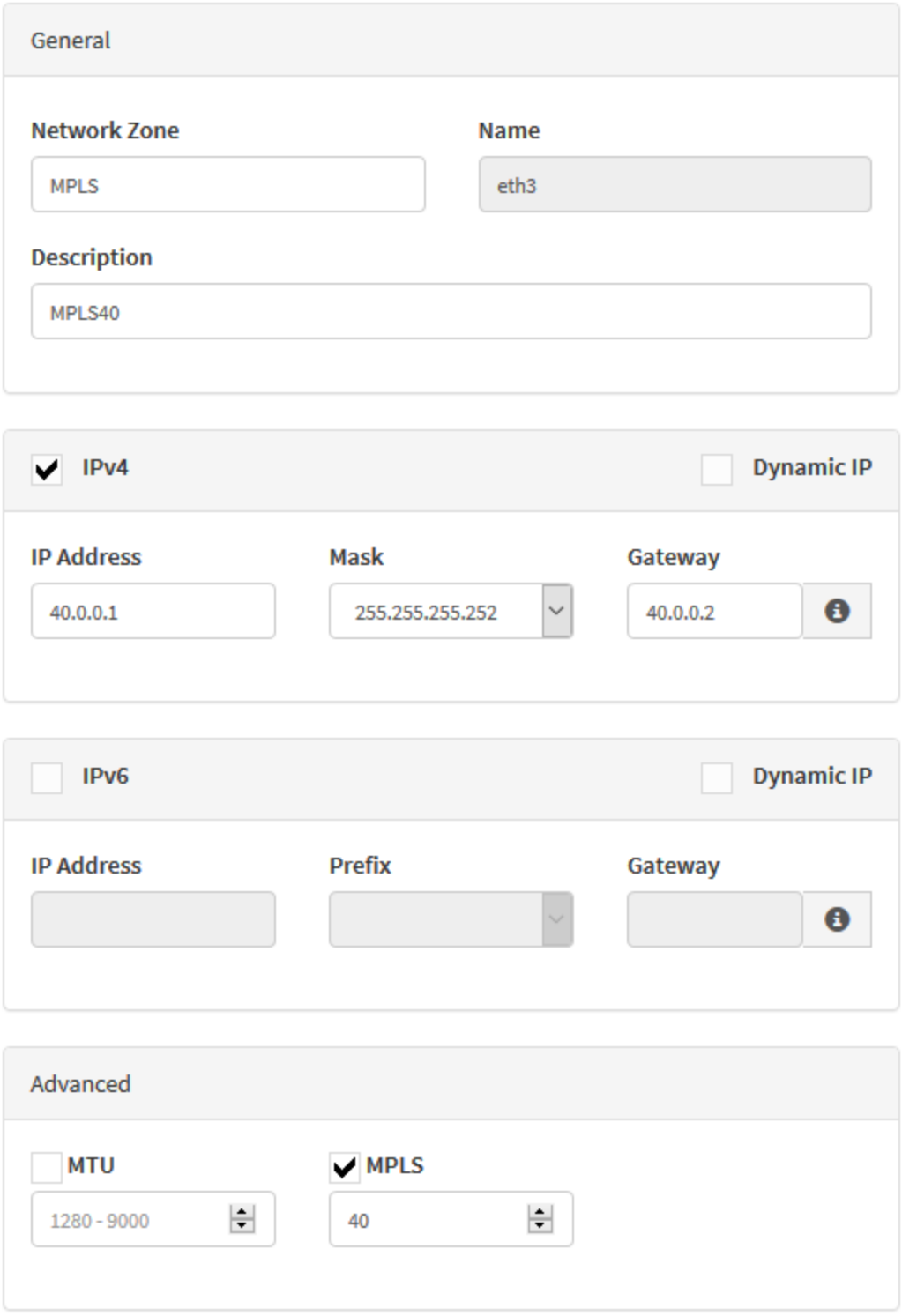
- ***MPLS[ ]:*** *Enable this option for MPLS to be activated*. In this example we will use as a label the value: "20".

To save, click **[ ]**.

This completes the configuration of the MPLS21 interface. Follow the same steps to configure the other links*:*

Link MPLS40

Below, there's an image demonstrating how the MPLS40 link should be configured:



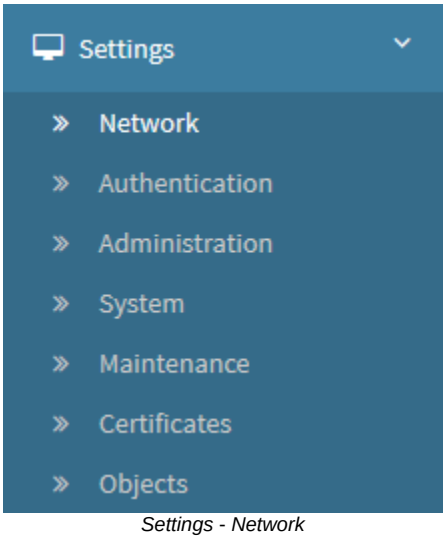
Interfaces - MPLS40 Config

This finalizes the configuration of the Interfaces in NGFW B, next we will configure the static routes.

Static Routing - MPLS - Configuration of static routes in UTM B

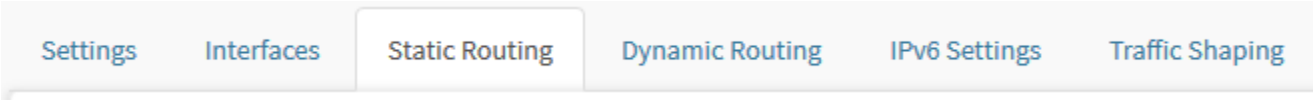
After configuring the interfaces, follow the steps below:

Still in Settings, in the Network option:



Settings - Network

Click on the Static Routing tab:

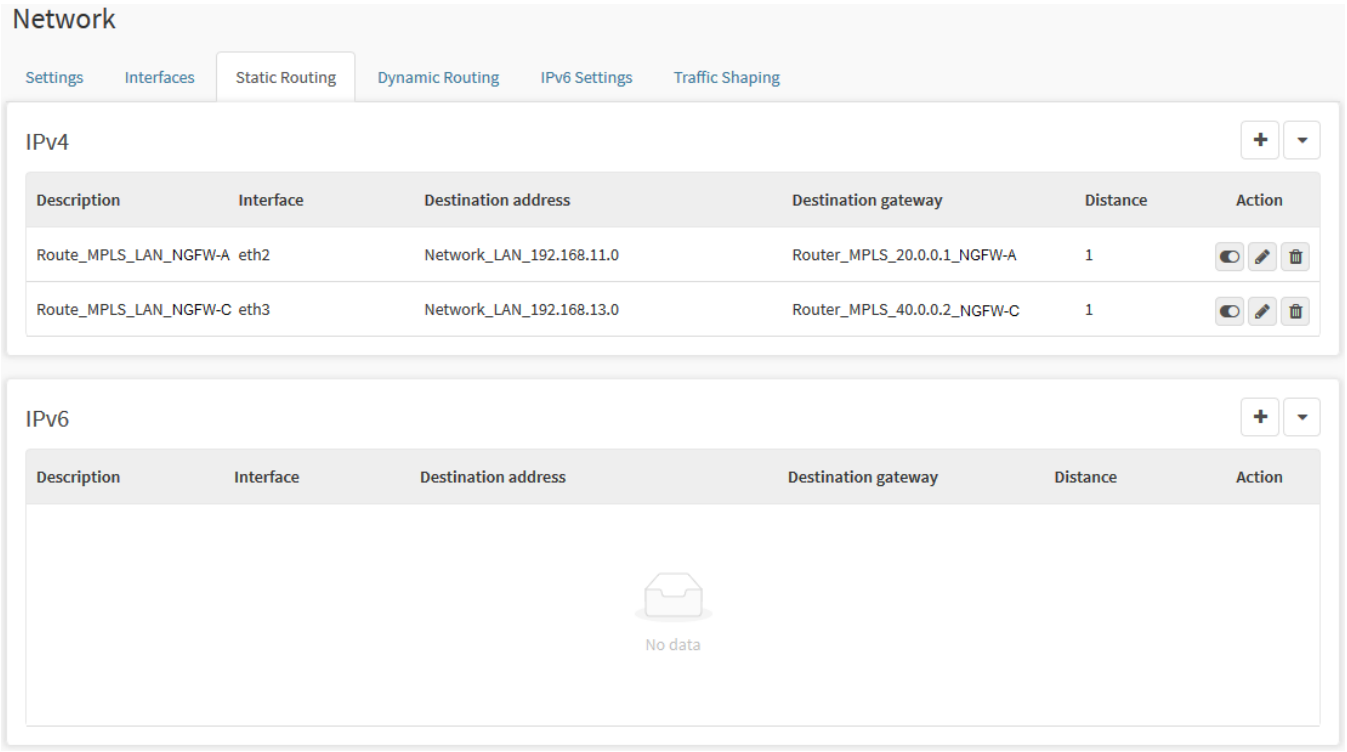


Static Routing tab

In this step, we will configure each static route using the IP of NGFW A and NGFW C as destination.

Some details of the static routing tab will not be considered in this example, if you want more information, see this page.

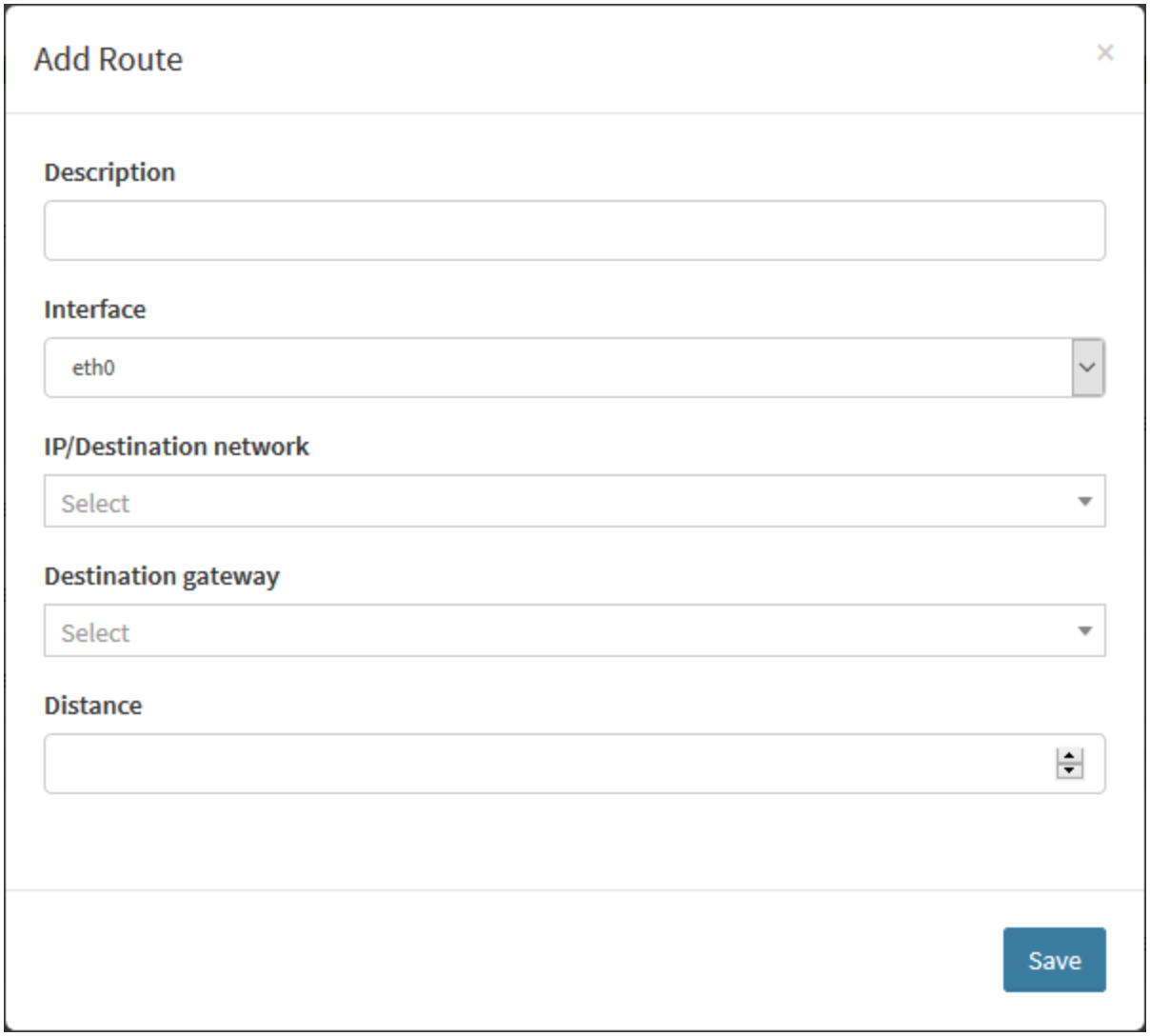
Below are the NGFW B interface configurations:



Network - Static Routing

LAN MPLS route to NGFW A

Click **[**  **]** to create a new route. The following window will be displayed:

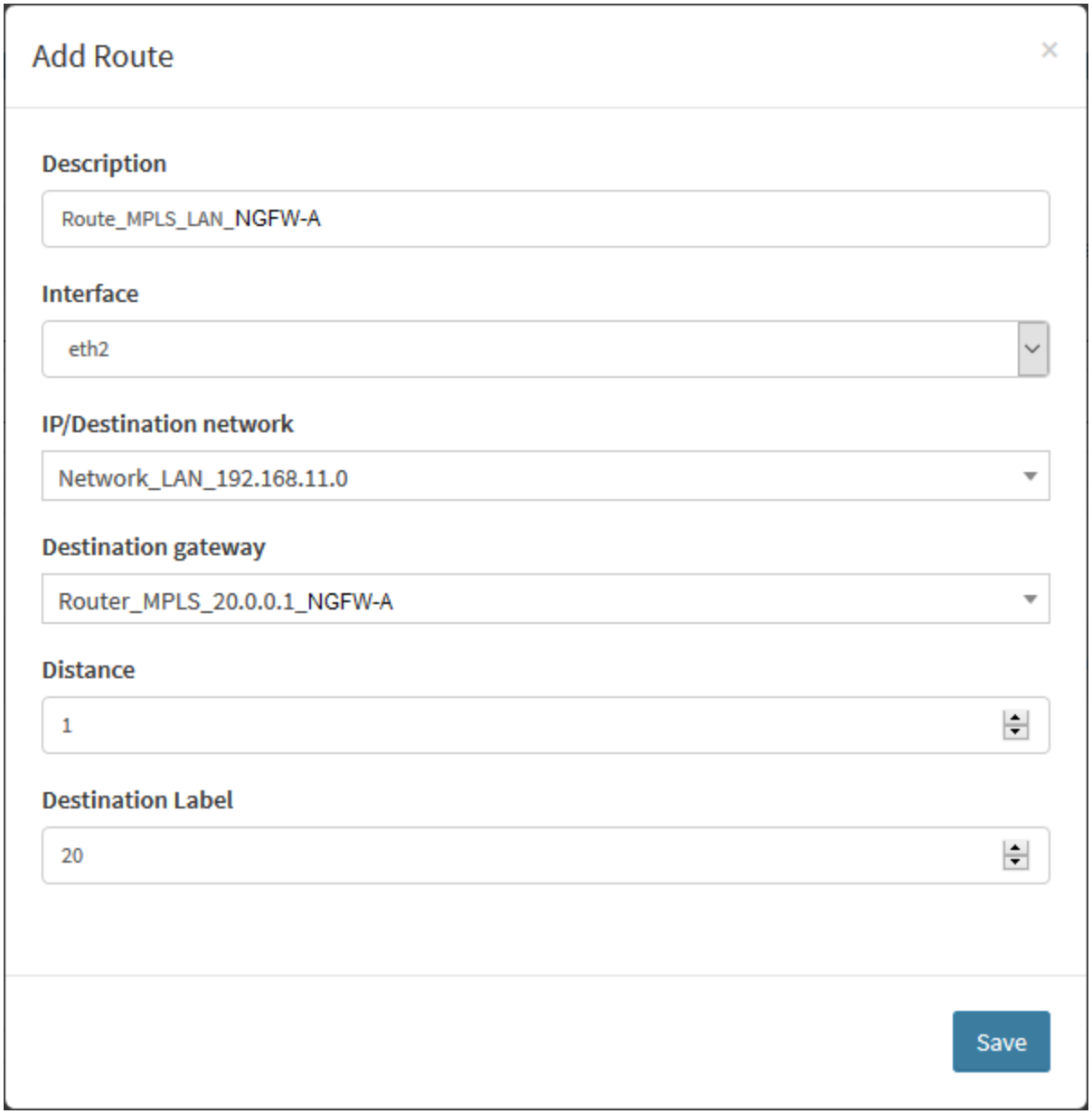


Static Routing - Add Route

- ***Description*:** To organize, we will name the routes using the syntax: "Route_MPLS_LAN_NGFW-A";
- ***Interface*:** Define the same interface that was used to configure the MPLS link with the NGFW-A, in this case it will be "eth2", thanks to this interface having MPLS, the Destination Label field will be displayed;
- ***IP/Destination Network:*** *Configure using the NGFW B IP as the destination, in this case we will use a single IP object containing the address: 192.168.11.0, we name this object as "Network_LAN_192.168.12.0"*;
- ***Destination Gateway*:** Determine the router as the destination gateway, in this case we will use a unique IP object containing the address: 20.0.0.2, we name this object "Router_MPLS_20.0.0.1_NGFW-A";
- ***Distance*:** Defines the administrative distance, in this example, we will use the value "1";
- ***Destination Label*:** As the destination label we will use the value: "20".

Note that in the IP / Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If not, they will not appear in the list. For more information on how to create an IP type object, see this page.

When finished, the static route must be configured this way:



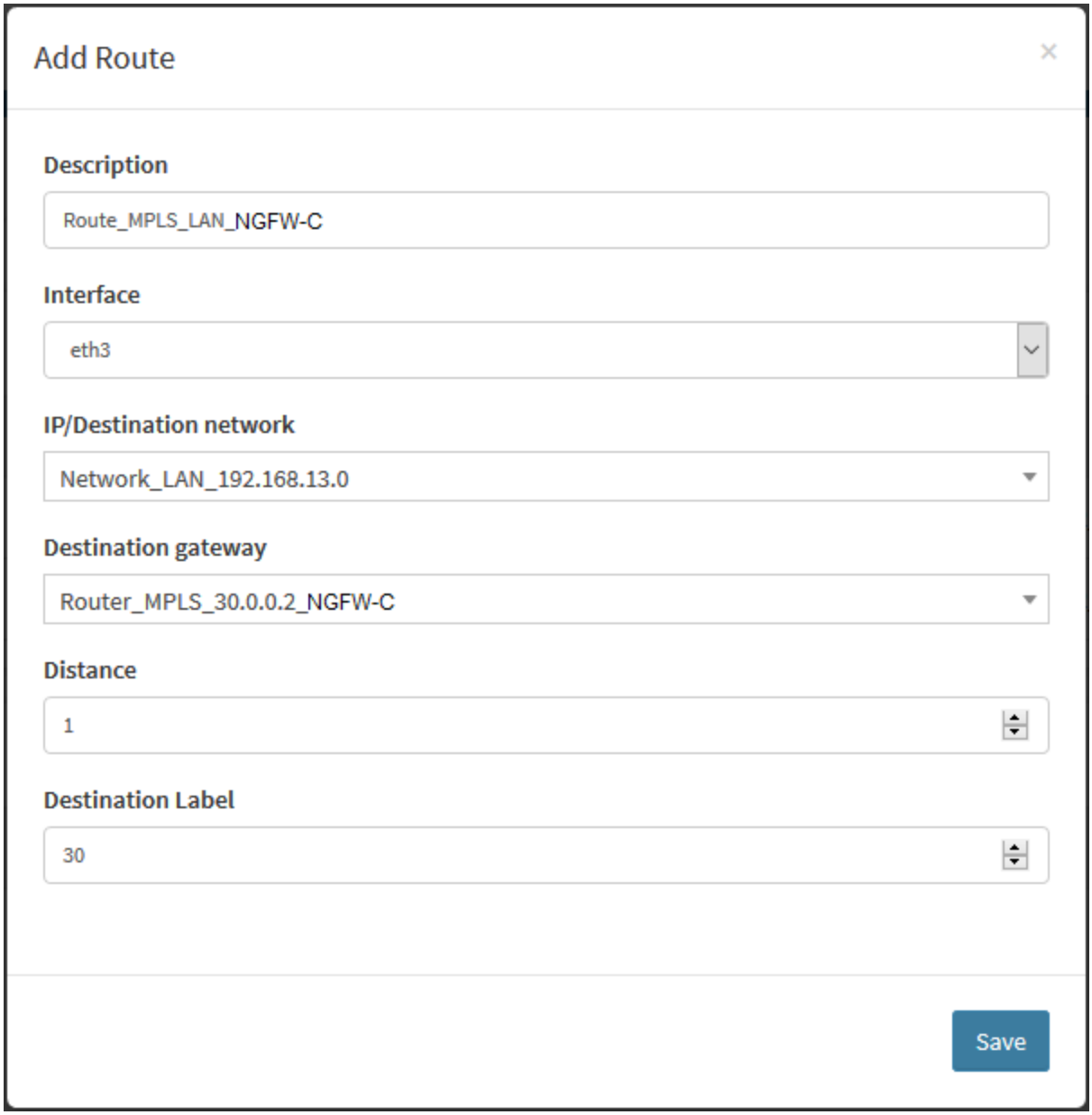
Static Routing - Add Route - Route_MPLS_LAN_NGFW-A

To finish the settings, click [Save].

This completes the configuration of the static route from *NGFW* B to *NGFW* A. Follow the same steps to configure the route from *NGFW* B to *NGFW* C*:*

LAN MPLS route to *NGFW* C

Below, an image demonstrating how the *NGFW* C route should be configured:



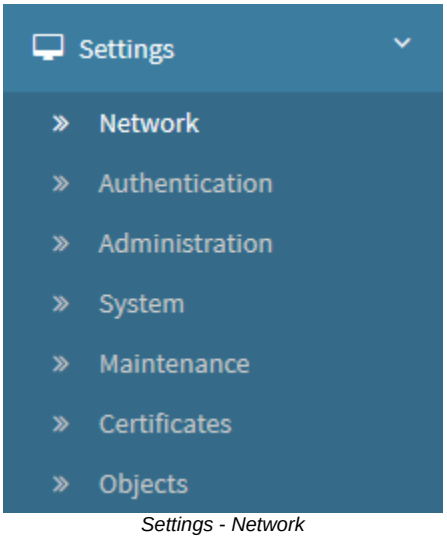
Static Routing - Add Route - Route_MPLS_LAN_NGFW-C

This finalizes the configuration of the static routes in *NGFW* B, next we will configure NGFW C.

Static Routing - MPLS - Configuration of Interfaces in UTM C

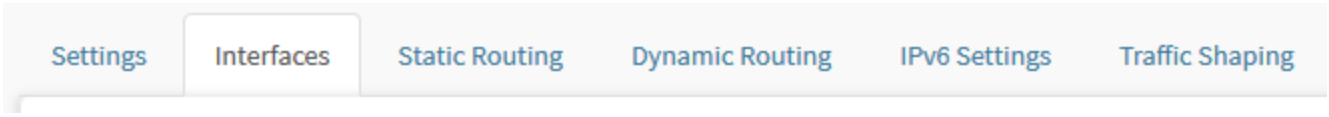
The procedures we will do here will be identical to the ones we did in NGFW A and NGFW B, but referring to the NGFW C.

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab

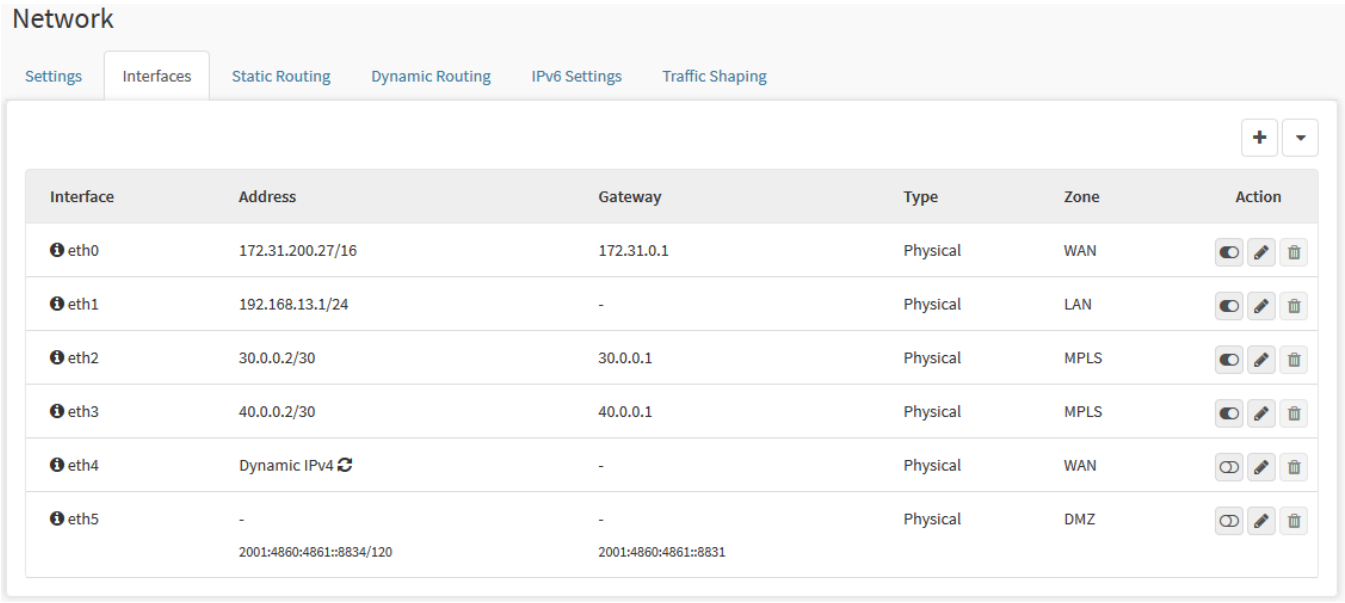
We will make the following settings in this step:

- Initially we will need to configure the NGFW C *LAN* (to serve as the destination of the NGFW A and NGFW B);
- Configure the physical interfaces that will be used by MPLS:
  - *Link* MPLS31;
  - *Link* MPLS41.

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

For more information on MPLS interfaces, visit this page.

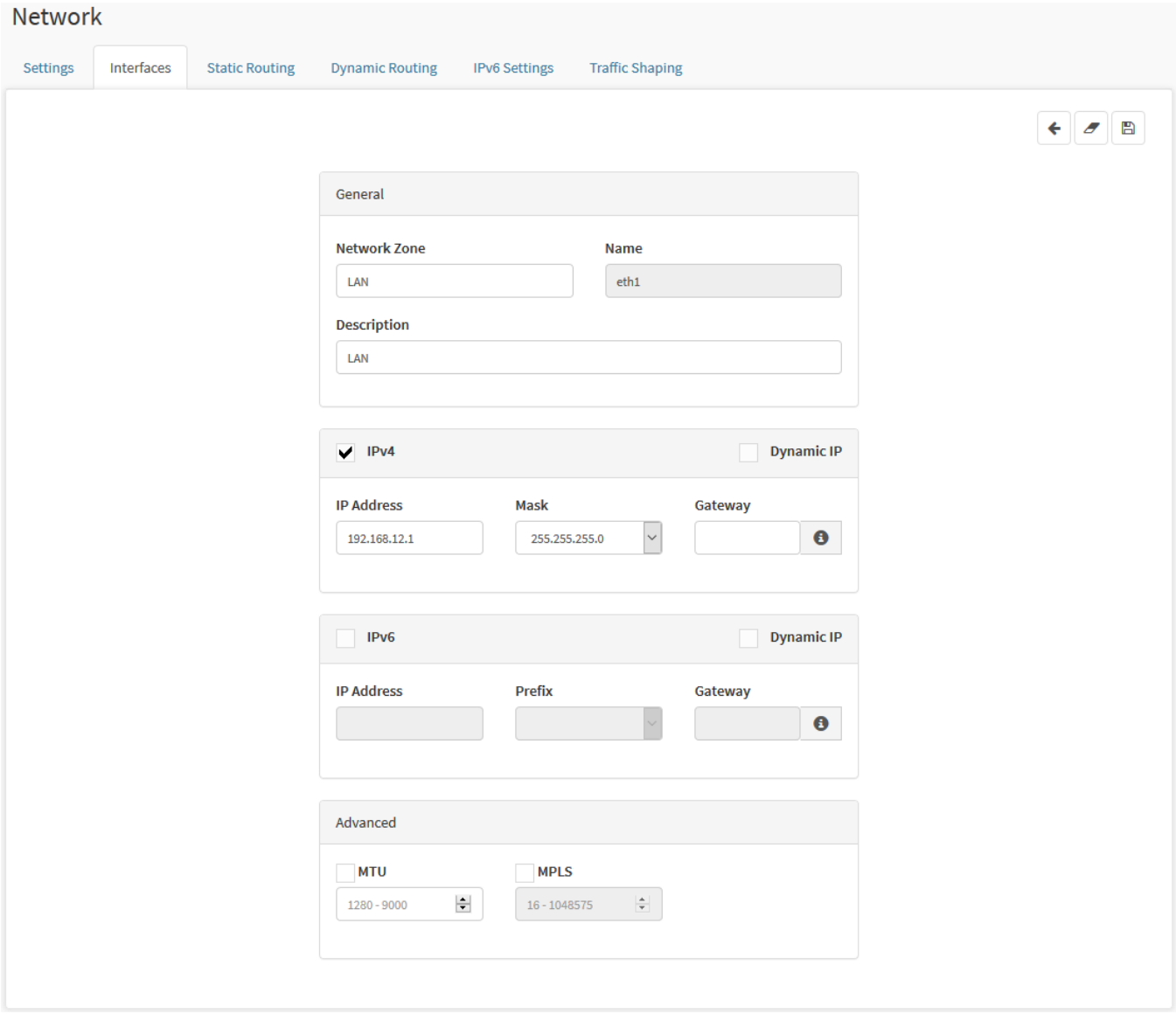
Below are the NGFW C interface's settings:



Network - Interfaces

NGFW C LAN configuration

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

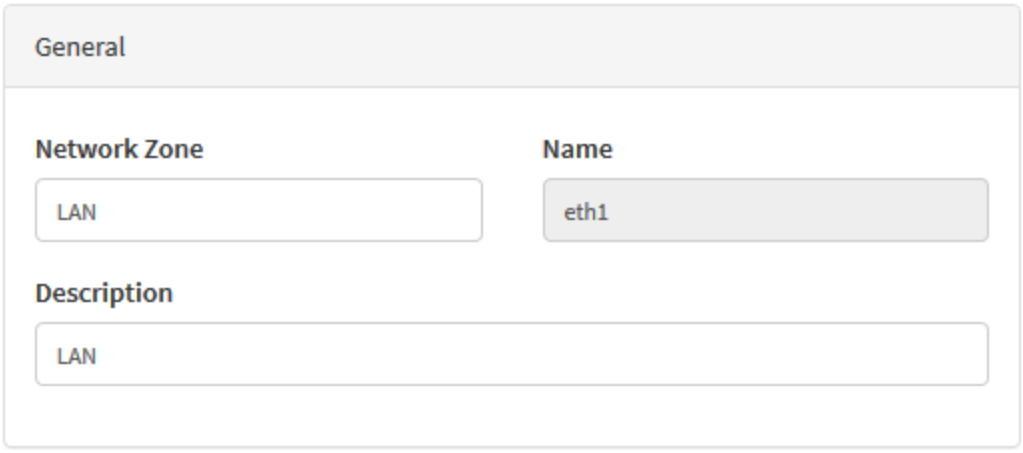


Interfaces - eth1

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

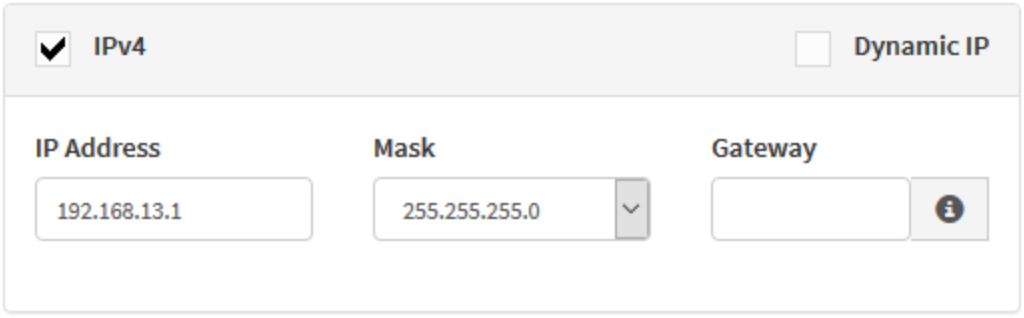


Interfaces – General Panel

- ***Network Zone*:** In this example we will name the zone "LAN";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: LAN.

IPv4

Complete the form as shown below:



Interfaces - IPv4

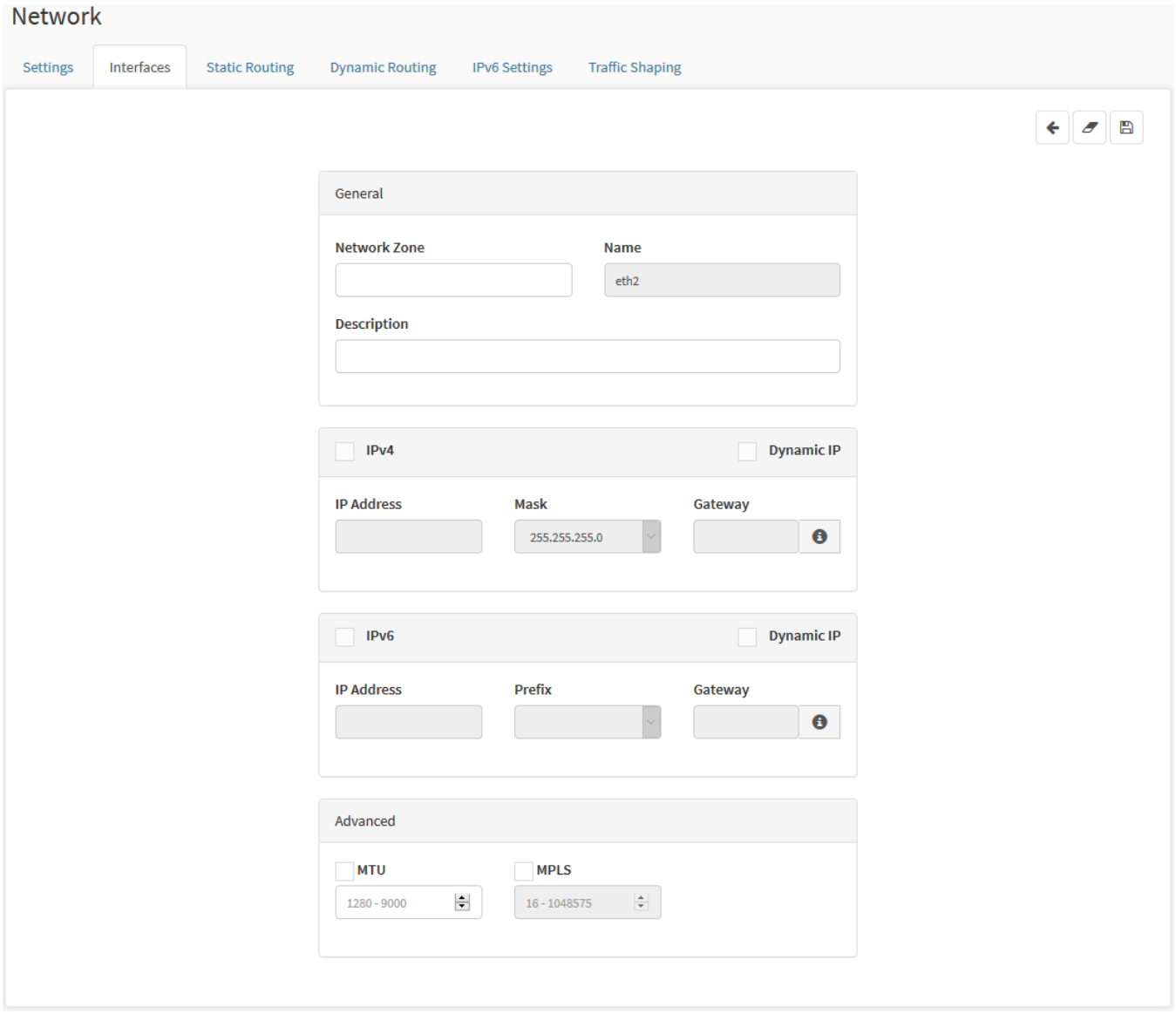
- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW C, in this case, it will be: 192.168.13.1;
- **Mask:** Select the netmask to be used by NGFW C.

To save, click **[ ]**.

This completes the NGFW C LAN configuration. Next we will configure the interfaces that will be used by MPLS.

Link MPLS31

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

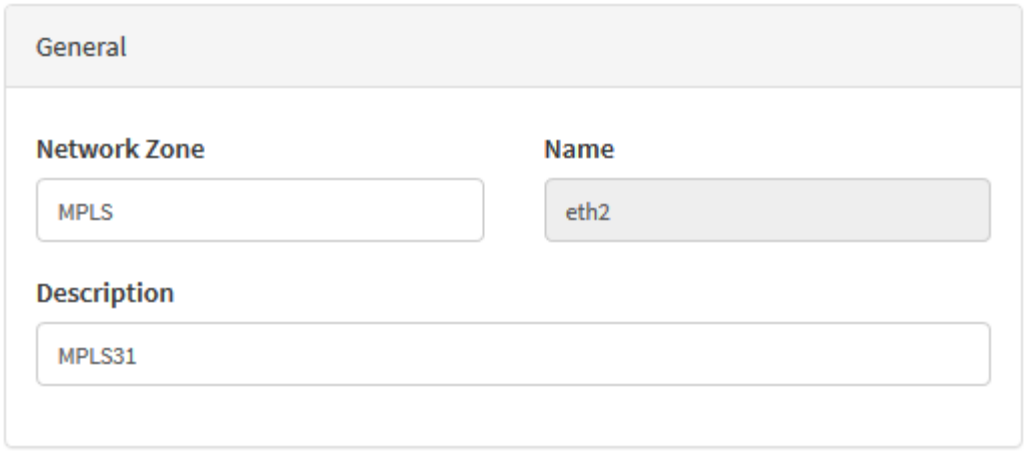


Interfaces - eth2

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

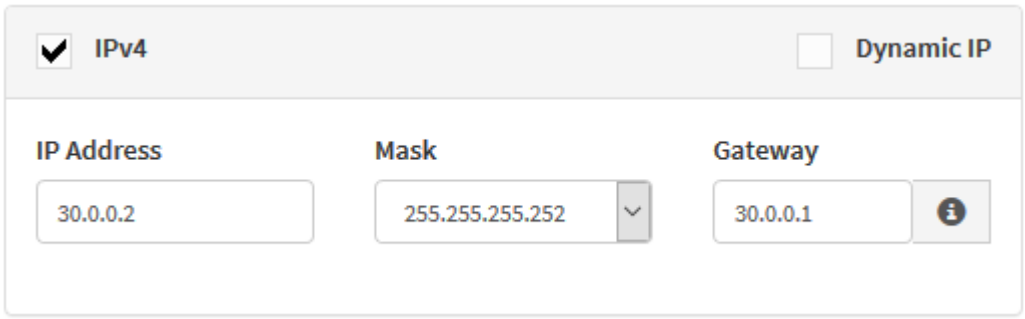


Interfaces – General Panel

- ***Network Zone*:** To organize, we will name the zones that we will use as "MPLS";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: MPLS31.

IPv4

Complete the form as shown below:

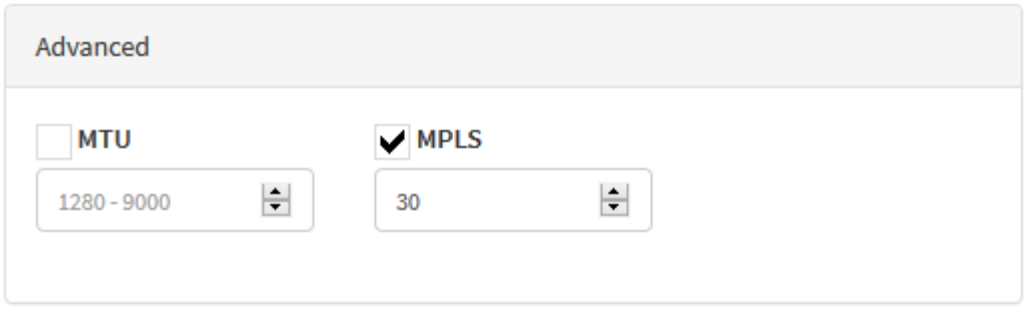


Interfaces - IPv4

- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by MPLS, in this case, it will be: 30.0.0.2;
- **Mask:** Select the netmask to be used.

Advanced

Complete the form as shown below:



Interfaces - Advanced

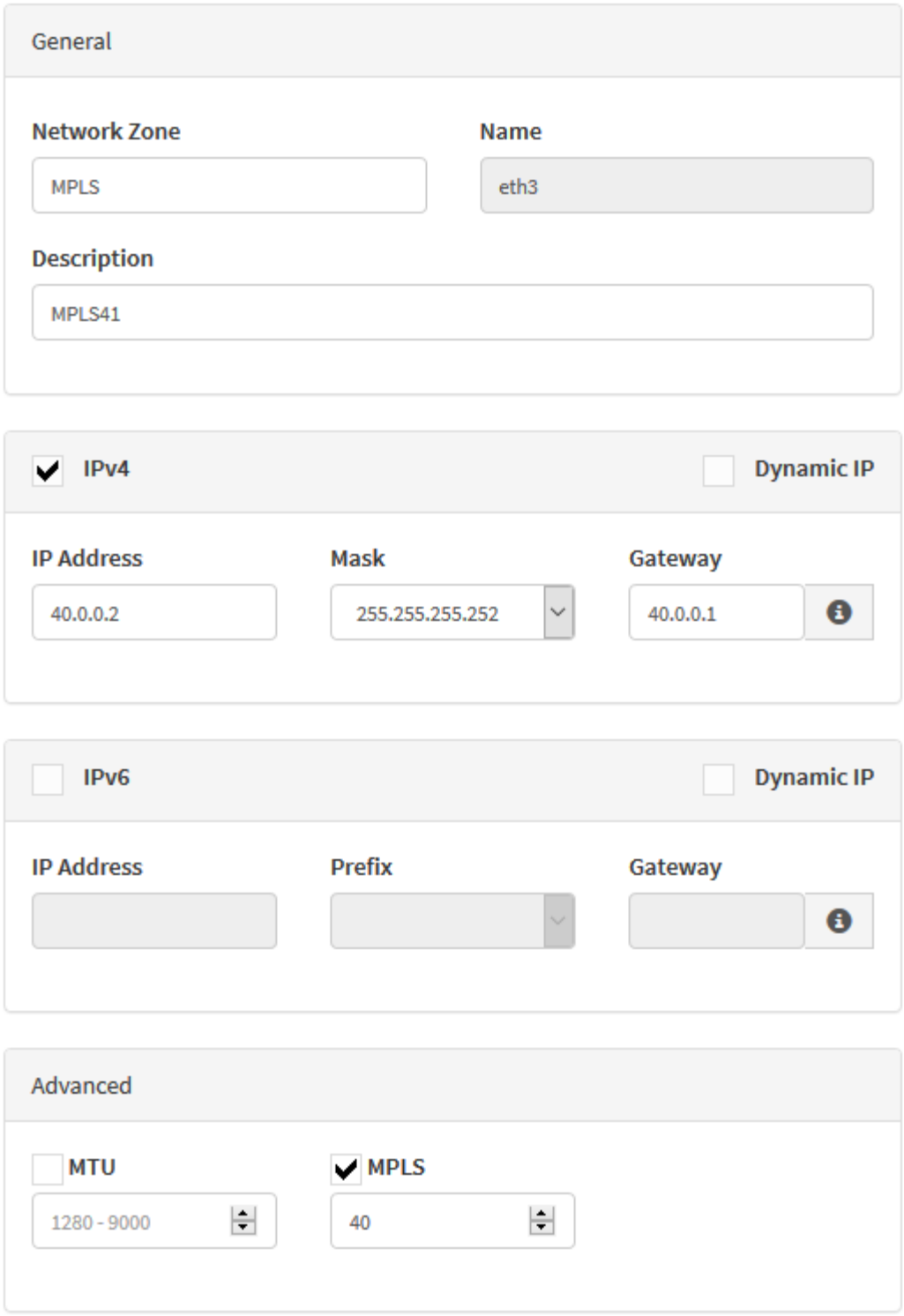
- ***MPLS[ ]:*** *Enable this option for MPLS to be activated*. In this example we will use as a label the value: "30".

To save, click **[ ]**.

This completes the configuration of the MPLS31 interface. Follow the same steps to configure the other links*:*

Link MPLS41

Below, an image demonstrating how the MPLS41 link should be configured:



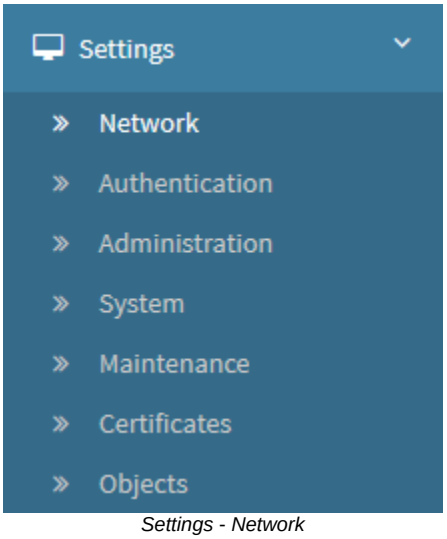
Interfaces - MPLS41 Config

This ends the configuration of the Interfaces in NGFW C, next we will configure the static routes.

Static Routing - MPLS - Configuration of static routes in UTM C

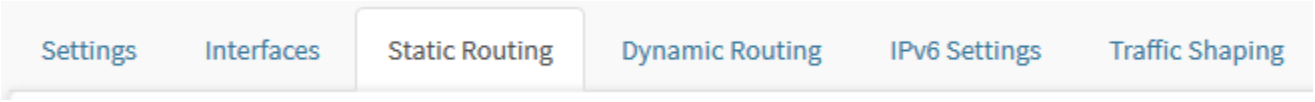
After configuring the interfaces, follow the steps below:

Still in Settings, in the Network option:



Settings - Network

Click on the Static Routing tab:

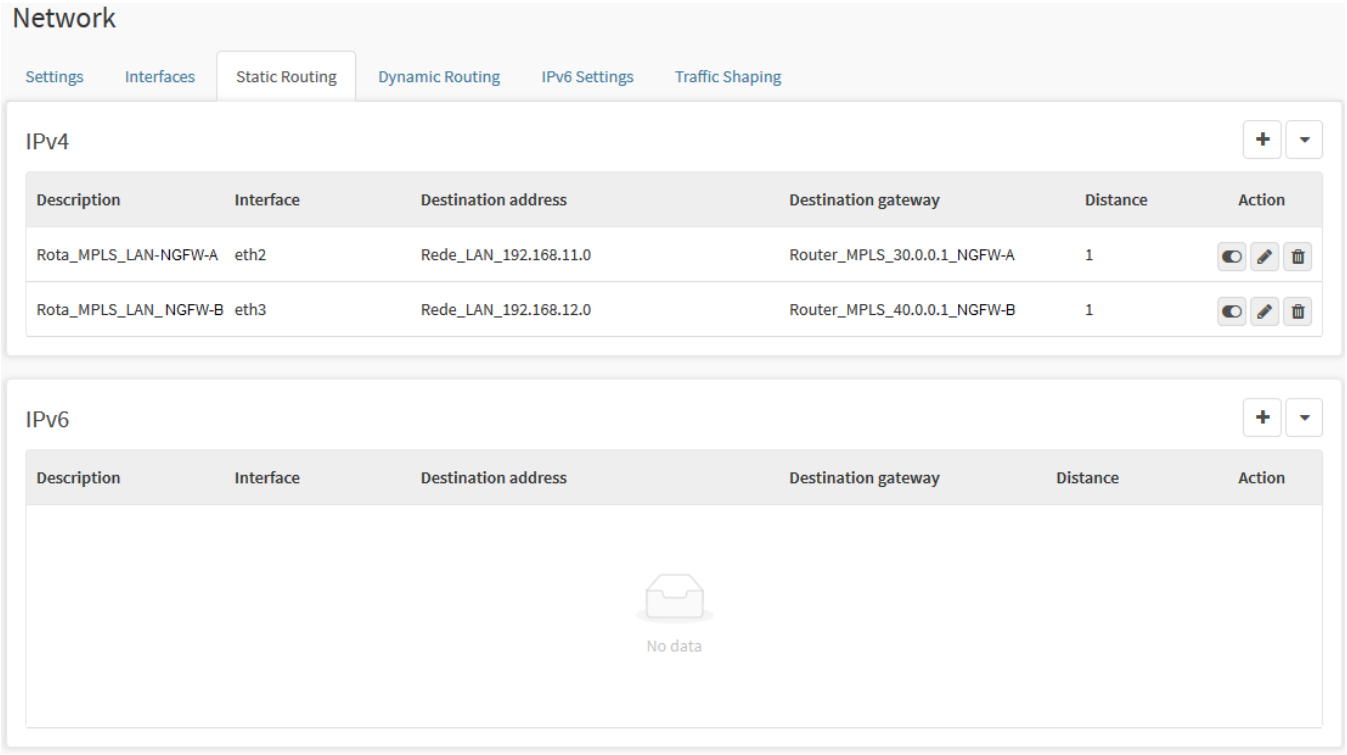


Static Routing tab

In this step, we will configure each static route using the IP of NGFW A and NGFW C as the destination.

Some details of the static routing tab will not be considered in this example, if you want more information, see this page.

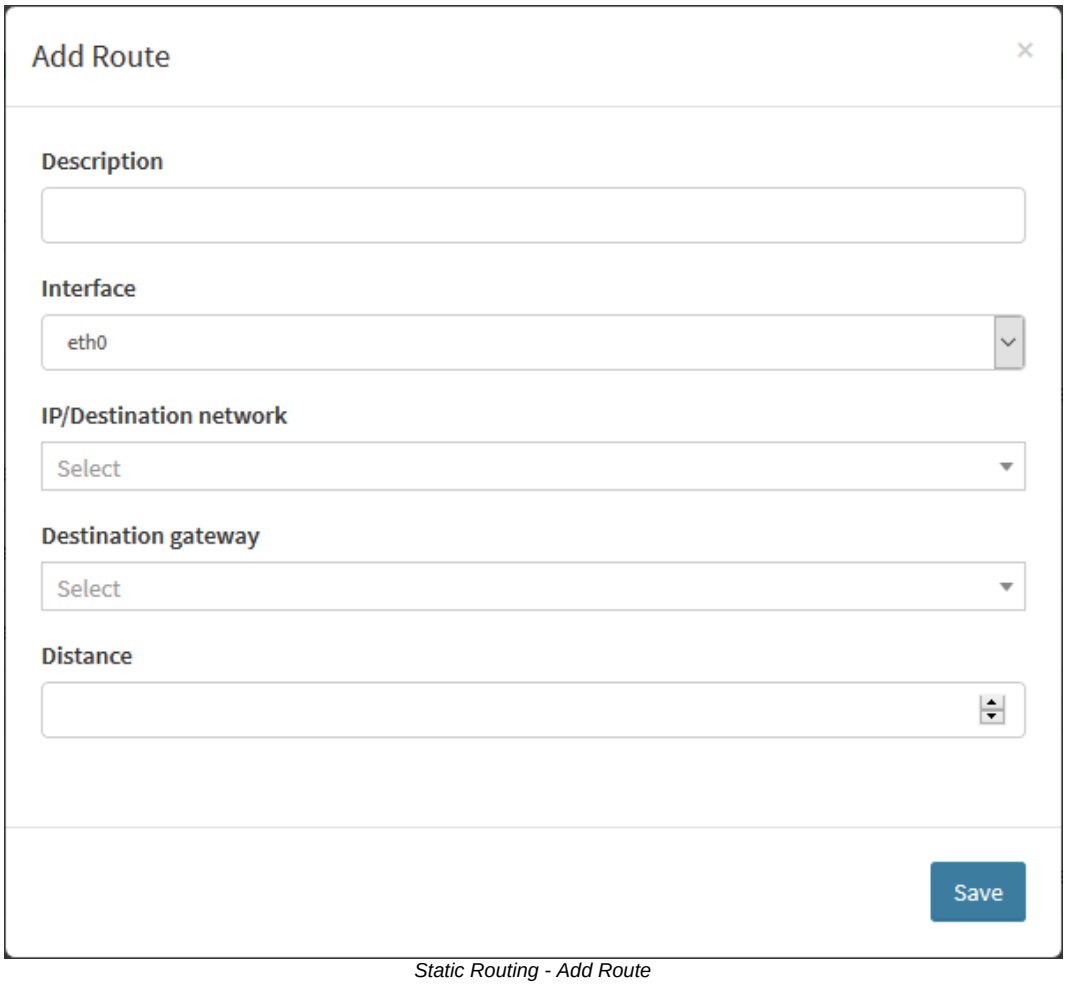
Below are the NGFW C interface settings:



Network - Static Routing

LAN MPLS route to NGFW A

Click **[**  **]** to create a new route. The following window will be displayed:

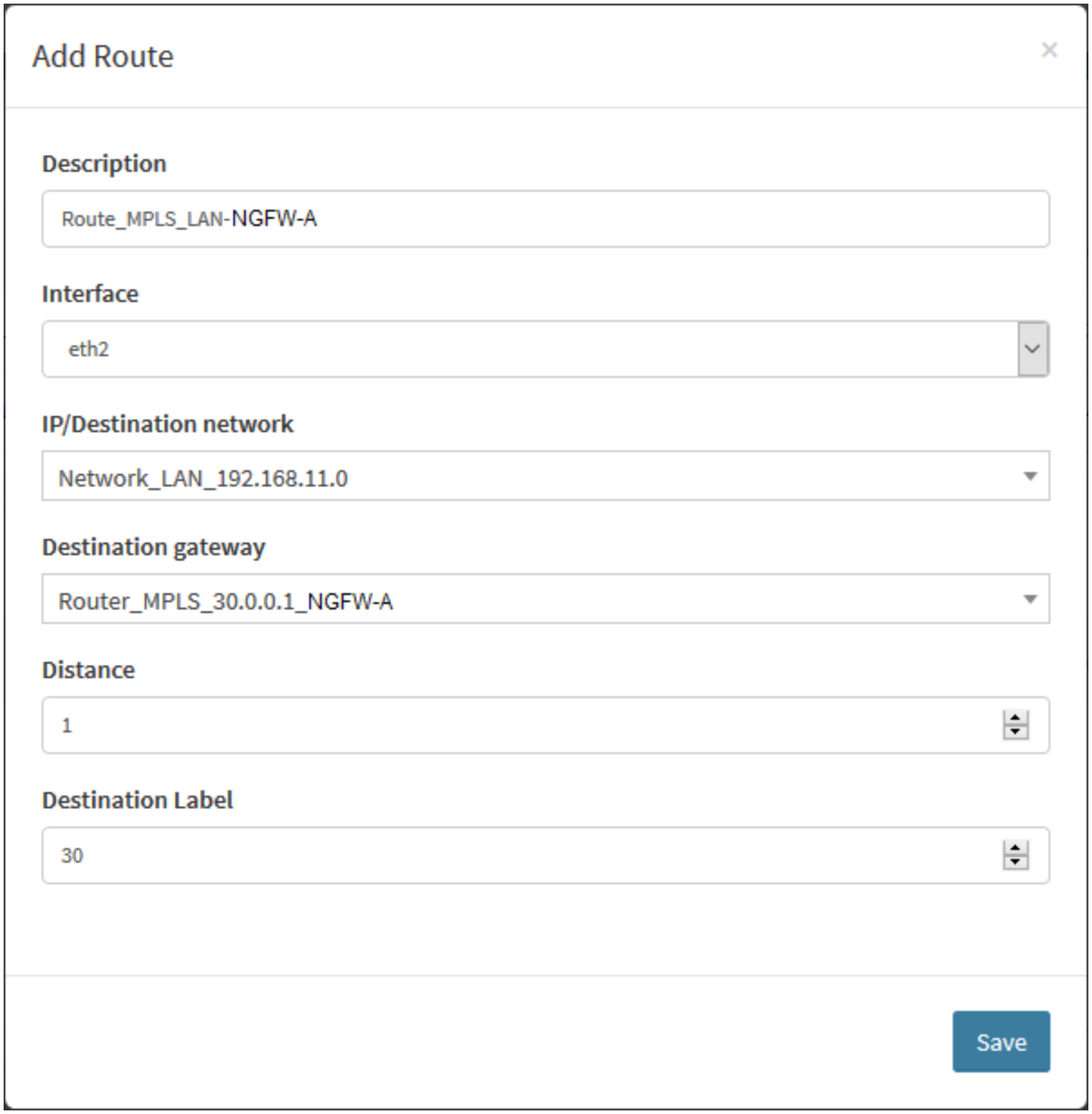


Static Routing - Add Route

- ***Description*:** To organize, we will name the routes using the syntax: "Route_MPLS_LAN_NGFW-A";
- ***Interface*:** Define the same interface that was used to configure the MPLS link with NGFW-A, in this case it will be "eth2", thanks to this interface having MPLS, the Destination Label field will be displayed;
- ***IP/Destination Network:*** *Configure using the NGFW A IP as the destination, in this case we will use a unique IP object containing the address*: 192.168.11.0*, we named this object "Network_LAN_192.168.11.0"*;
- ***Destination Gateway*:** Determine the router as the destination gateway, in this case we will use a single IP object containing the address: *30.0.0.1, we named this object "Router_MPLS_30.0.0.1_NGFW-A"*;
- ***Distance*:** Defines the administrative distance, in this example, we will use the value "1";
- ***Destination Label*:** As the destination label we will use the value: "30".

Note that in the IP / Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If not, they will not appear in the list. For more information on creating an IP-type object, see this page.

When finished, the static route must be configured this way:



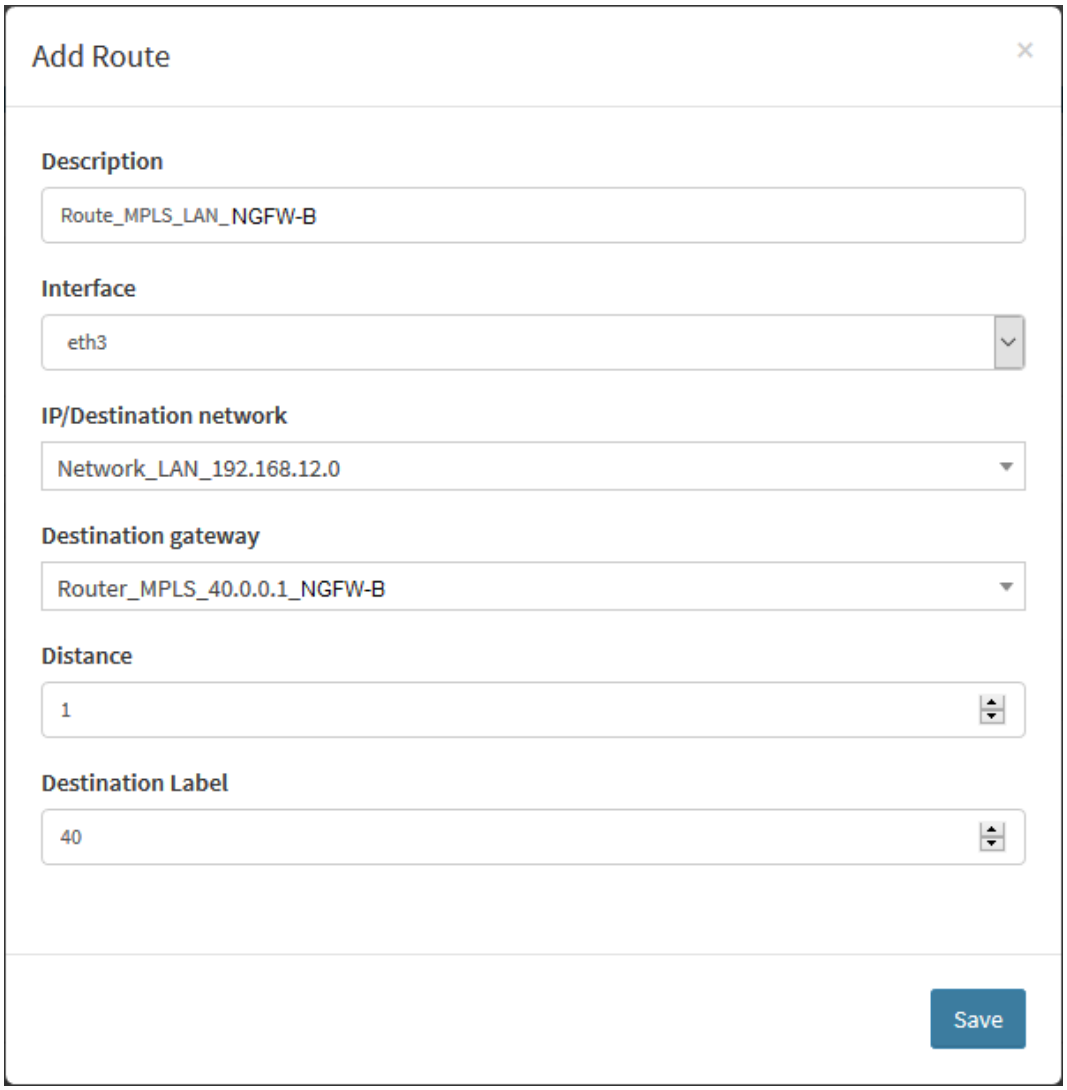
Static Routing - Add Route - Route_MPLS_LAN_NGFW-A

To finish the settings, click [Save].

This completes the configuration of the static route from NGFW C to NGFW A. Follow the same steps to configure the route from NGFW C to NGFW B:

LAN MPLS route to NGFW B

Below, an image demonstrating how the route to NGFW B should be configured:



Static Routing - Add Route - Route_MPLS_LAN_NGFW-B

This ends the configuration of the static routes in NGFW C, the last step is to validate all the configurations we have made.

Static Routing - MPLS - Settings Validation

To perform the validation, we will access the NGFW A CLI and run some commands, if you need more information about it, see this page.

One of the simplest tests to validate the operation of the routes is to *ping* NGFW A (172.31.200.25) to NGFW B (172.31.200.26) and check for an answer, as shown in the image below:

```
admin  >ping 172.31.200.26
PING 172.31.200.26 (172.31.200.26) 56(84) bytes of data.
64 bytes from 172.31.200.26: icmp_seq=1 ttl=63 time=1.67 ms
64 bytes from 172.31.200.26: icmp_seq=2 ttl=64 time=0.233 ms
64 bytes from 172.31.200.26: icmp_seq=3 ttl=64 time=0.623 ms
64 bytes from 172.31.200.26: icmp_seq=4 ttl=64 time=0.512 ms
64 bytes from 172.31.200.26: icmp_seq=5 ttl=64 time=0.533 ms
64 bytes from 172.31.200.26: icmp_seq=6 ttl=64 time=0.397 ms

--- 172.31.200.26 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5119ms
rtt min/avg/max/mdev = 0.233/0.662/1.676/0.470 ms
admin  >
```

CLI - Validation of communication from the NGFW A to the NGFW B by Ping

Next, the ping from NGFW A (172.31.200.25) to NGFW C (172.31.200.27):

```
admin  >ping 172.31.200.27
PING 172.31.200.27 (172.31.200.27) 56(84) bytes of data.
64 bytes from 172.31.200.27: icmp_seq=1 ttl=63 time=1.78 ms
64 bytes from 172.31.200.27: icmp_seq=2 ttl=64 time=0.582 ms
64 bytes from 172.31.200.27: icmp_seq=3 ttl=64 time=0.993 ms
64 bytes from 172.31.200.27: icmp_seq=4 ttl=64 time=0.301 ms
64 bytes from 172.31.200.27: icmp_seq=5 ttl=64 time=0.620 ms

--- 172.31.200.27 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.301/0.856/1.787/0.515 ms
admin  >
```

CLI - Validation of communication from the NGFW A to the NGFW C by Ping

In addition, if you want to list all the routes that NGFW A is currently using, just run the *ip route list* command and check if the created routes were listed:

```
admin  >ip route list
default via 172.31.0.1 dev eth0
20.0.0.0/30 dev eth2 proto kernel scope link src 20.0.0.1
30.0.0.0/30 dev eth3 proto kernel scope link src 30.0.0.1
120.0.0.0/24 dev tun0 proto kernel scope link src 120.0.0.1
120.0.0.2  encap mpls  20 via 20.0.0.2 dev eth2
172.31.0.0/16 dev eth0 proto kernel scope link src 172.31.200.25
192.168.11.0/24 dev eth1 proto kernel scope link src 192.168.11.1
192.168.12.0/24  encap mpls  20 via 20.0.0.2 dev eth2
192.168.13.0/24  encap mpls  30 via 30.0.0.2 dev eth3
192.168.15.0/24 dev eth5 proto kernel scope link src 192.168.15.15
admin  >
```

CLI - ip route list do NGFW A

It is also possible to perform these same steps at the other ends, following a demonstration using the *ping* command to check the communication from NGFW B (172.31.200.26) to NGFW A (172.31.200.25):

```
admin  >ping 172.31.200.25
PING 172.31.200.25 (172.31.200.25) 56(84) bytes of data.
64 bytes from 172.31.200.25: icmp_seq=1 ttl=64 time=0.429 ms
64 bytes from 172.31.200.25: icmp_seq=2 ttl=64 time=0.376 ms
64 bytes from 172.31.200.25: icmp_seq=3 ttl=64 time=0.472 ms
64 bytes from 172.31.200.25: icmp_seq=4 ttl=64 time=0.427 ms
64 bytes from 172.31.200.25: icmp_seq=5 ttl=64 time=0.463 ms

--- 172.31.200.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.376/0.433/0.472/0.038 ms
admin  >
```

CLI - Validation of communication with NGFW B to NGFW A by Ping

Next, ping from the NGFW B (172.31.200.26) to the NGFW C (172.31.200.27):

```
admin  >ping 172.31.200.27
PING 172.31.200.27 (172.31.200.27) 56(84) bytes of data.
64 bytes from 172.31.200.27: icmp_seq=1 ttl=63 time=1.68 ms
64 bytes from 172.31.200.27: icmp_seq=2 ttl=64 time=0.640 ms
64 bytes from 172.31.200.27: icmp_seq=3 ttl=64 time=0.533 ms
64 bytes from 172.31.200.27: icmp_seq=4 ttl=64 time=0.654 ms
64 bytes from 172.31.200.27: icmp_seq=5 ttl=64 time=0.404 ms

--- 172.31.200.27 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4063ms
rtt min/avg/max/mdev = 0.404/0.782/1.681/0.458 ms
admin  >
```

CLI - Validation of communication from the NGFW B to the NGFW C by Ping

Below the NGFW B IP route list:

```
admin  >ip route list
default via 172.31.0.1 dev eth0
20.0.0.0/30 dev eth2 proto kernel scope link src 20.0.0.2
40.0.0.0/30 dev eth3 proto kernel scope link src 40.0.0.1
120.0.0.0/24 dev tun0 proto kernel scope link src 120.0.0.2
120.0.0.1  encap mpls  20 via 20.0.0.1 dev eth2
172.31.0.0/16 dev eth0 proto kernel scope link src 172.31.200.26
192.168.11.0/24  encap mpls  20 via 20.0.0.1 dev eth2
192.168.12.0/24 dev eth1 proto kernel scope link src 192.168.12.1
192.168.13.0/24  encap mpls  40 via 40.0.0.2 dev eth3
admin  >
```

CLI - ip route list from the NGFW B

Then, ping from the NGFW C (172.31.200.27) to the NGFW A (172.31.200.25).

```
admin  >ping 172.31.200.25
PING 172.31.200.25 (172.31.200.25) 56(84) bytes of data.
64 bytes from 172.31.200.25: icmp_seq=1 ttl=64 time=0.936 ms
64 bytes from 172.31.200.25: icmp_seq=2 ttl=64 time=0.605 ms
64 bytes from 172.31.200.25: icmp_seq=3 ttl=64 time=0.600 ms
64 bytes from 172.31.200.25: icmp_seq=4 ttl=64 time=0.566 ms

--- 172.31.200.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.566/0.676/0.936/0.153 ms
admin  >
```

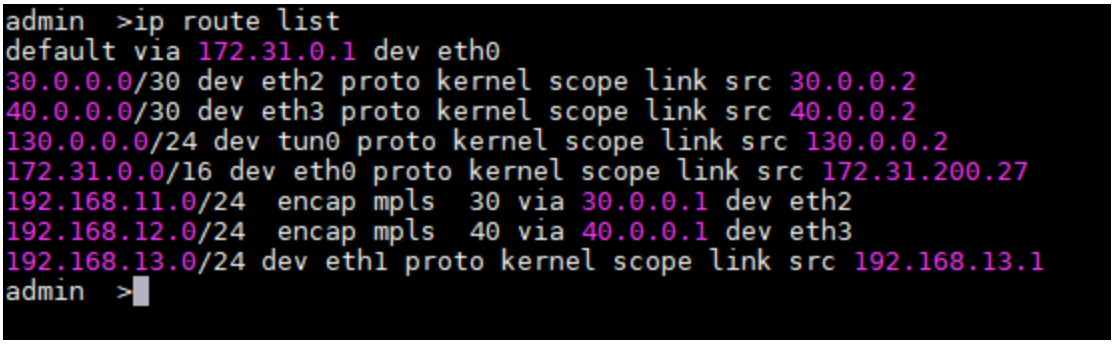
CLI - Validation of communication from the NGFW C to the NGFW A by Ping

Below, ping from the NGFW C (172.31.200.27) to NGFW B (172.31.200.26).

```
admin  >ping 172.31.200.26
PING 172.31.200.26 (172.31.200.26) 56(84) bytes of data.
64 bytes from 172.31.200.26: icmp_seq=1 ttl=63 time=132 ms
64 bytes from 172.31.200.26: icmp_seq=2 ttl=64 time=0.614 ms
64 bytes from 172.31.200.26: icmp_seq=3 ttl=64 time=0.495 ms
64 bytes from 172.31.200.26: icmp_seq=4 ttl=64 time=0.739 ms
64 bytes from 172.31.200.26: icmp_seq=5 ttl=64 time=0.689 ms

--- 172.31.200.26 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.495/27.097/132.948/52.925 ms
admin  >
```

CLI - Validation of communication from the NGFW C to the NGFW B by Ping

And finally, listing the NGFW C routes through the *ip route list*:



CLI - ip route list from the NGFW C

This concludes the demo, for more information regarding Static Routing, see this page.

If you want to see more details about the columns on the Static Routing tab, visit this page.

Dynamic Routing - ECMP

The acronym ECMP stands for Equal-Cost Multi-Path, it is a multipath routing method that allows the balancing of network traffic, effectively allowing the traffic of packets to a specific destination to be done by several equal routes priority. ECMP has methods to define the best path, making the distribution of the packages according to which of the routes has the best performance. In this way, it is possible to add 2 or more static routes, to the same destination, with the same distance and the system will execute load balance, based on the IP of origin of the connection, ECMP will use its algorithms to choose the shortest distance to reach the destination.

It is important to note that for the ECMP to act correctly, the same value for "Administrative Distance" must be registered in the multiple static routes registered.

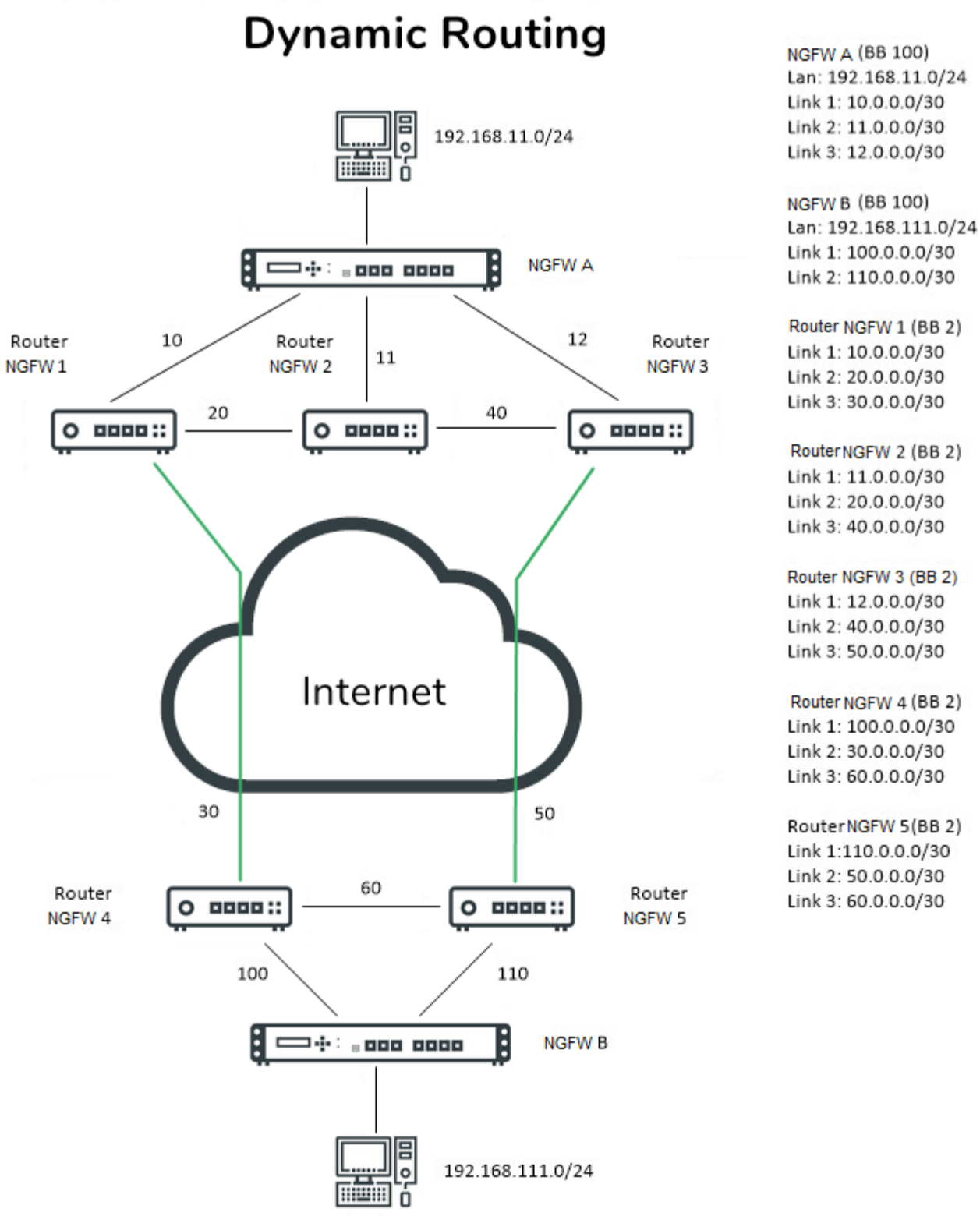
If several routes with different distances are registered, routes that have a shorter distance value will have priority.

Taking into account the prioritization according to the distance value, it is possible to use it to determine the priority of the services according to their static or dynamic routing.

If the NGFW loses communication with the Gateway, routing is automatically interrupted by this path until this link is reestablished. Drop and return detection occurs through ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol).

Regarding SD-WAN, although similar, the options available in static routing do not interfere with policies based on SD-WAN, however, the latter has higher priority than static routing rules regardless of what is defined in Administrative Distances.

Below we will demonstrate a step by step how to connect two NGFWs using ECMP to perform dynamic routing. This demonstration will take into account the following structure:



Dynamic Routing - Structure

In this structure, two NGFWs will be interconnected with multiple links connected through several routers. The following IPs will be used in this example:

ECMP - IP addressing

Name	LAN IP address	Links
NGFW A	192.168.11.0/24	10.0.0.0/30
		11.0.0.0/30
		12.0.0.0/30
NGFW B	192.168.111.0/24	100.0.0.0/30
		110.0.0./30

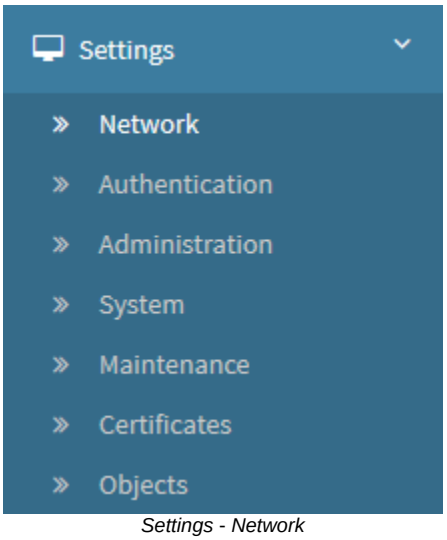
The steps we will take in this demonstration will be:

1. Configuring the Interfaces on NGFW A;
2. Configuration of static routes in NGFW A;
3. Configuration of Interfaces on NGFW B;
4. Configuration of static routes in NGFW B;
5. Validation of Static Routing Configuration.

We will start the demo by configuring the NGFW A interfaces.

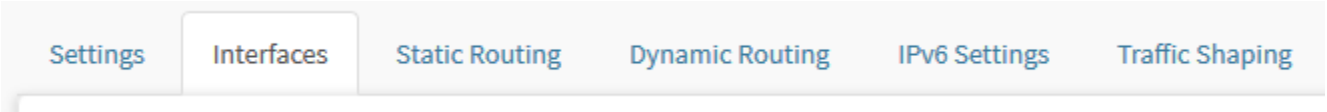
Dynamic Routing - ECMP - Configuring Interfaces on UTM A

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



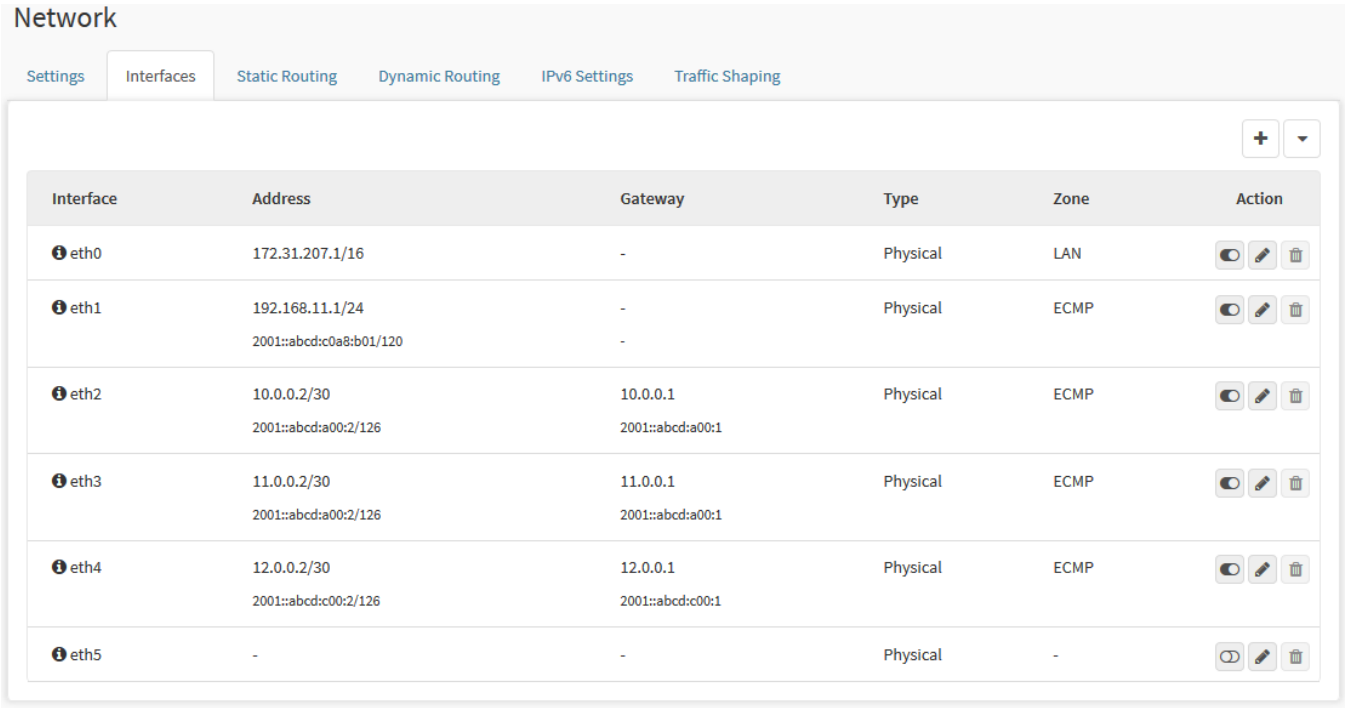
Interfaces tab

We will make the following settings in this step:

- Initially we will need to configure the NGFW A LAN (to serve as the NGFW B destination);
- Configure the physical interfaces that will be used to connect to the routers that will be used as a link by NGFW A being them:
  - NGFW 1;
  - NGFW 2;
  - NGFW 3.

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

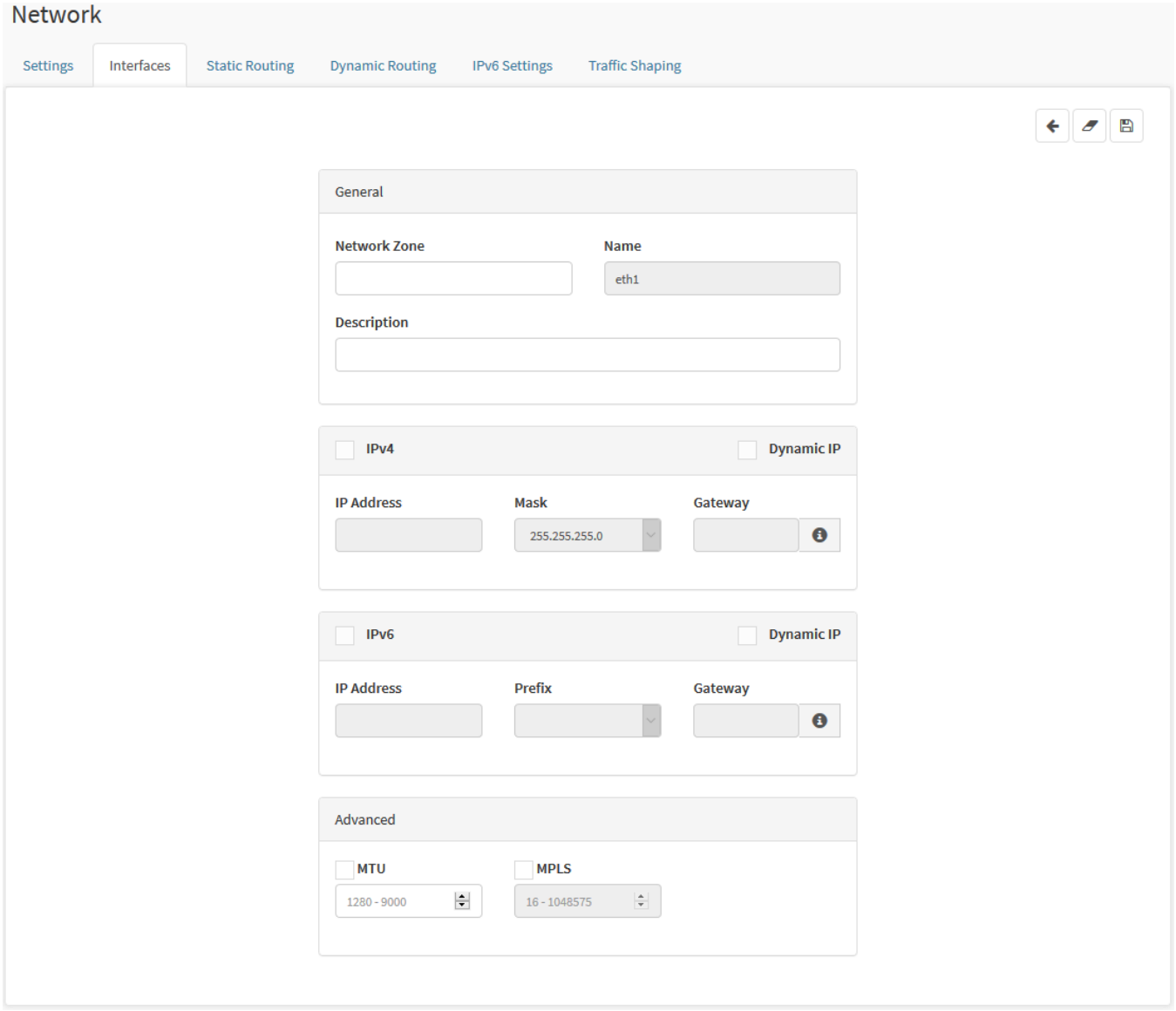
Below are the NGFW A interface settings:



Network - Interfaces

LAN configuration of NGFW A

Access the physical interface you will use and click **[**  **]**. The following screen will be displayed:

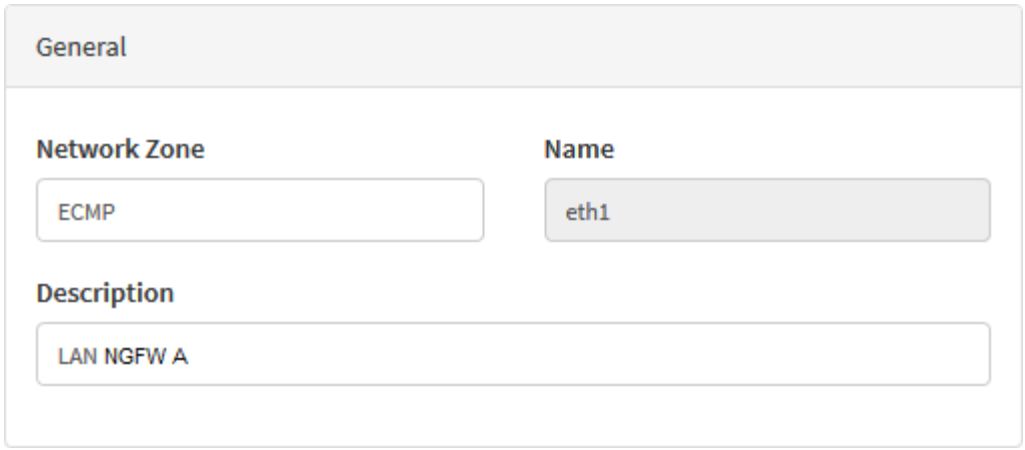


Interfaces - eth1

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

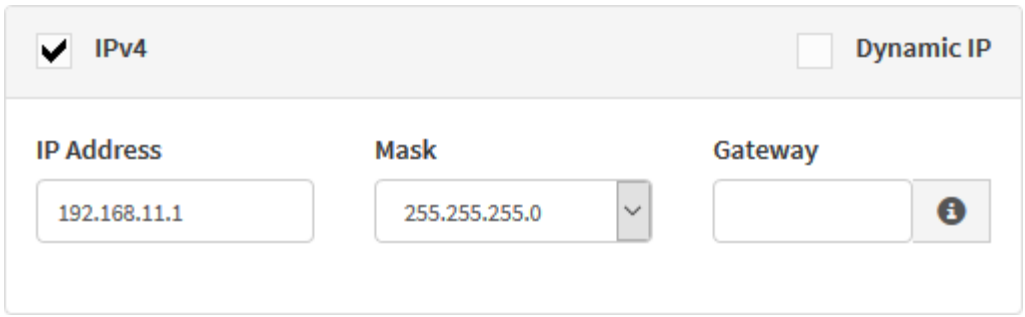


Interfaces - General Panel

- ***Network Zone*:** To organize, we name the Zones of all the interfaces that we will use "ECMP";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex .: LAN NGFW A.

IPv4

Complete the form as shown below:



Interfaces - IPv4

- **IPv4[ ]:** Mark this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW A, in this case, it will be: 192.168.11.1;
- **Mask:** Enter the netmask to be used by NGFW A.

IPv6

Complete the form as shown below:

Interfaces - IPv6

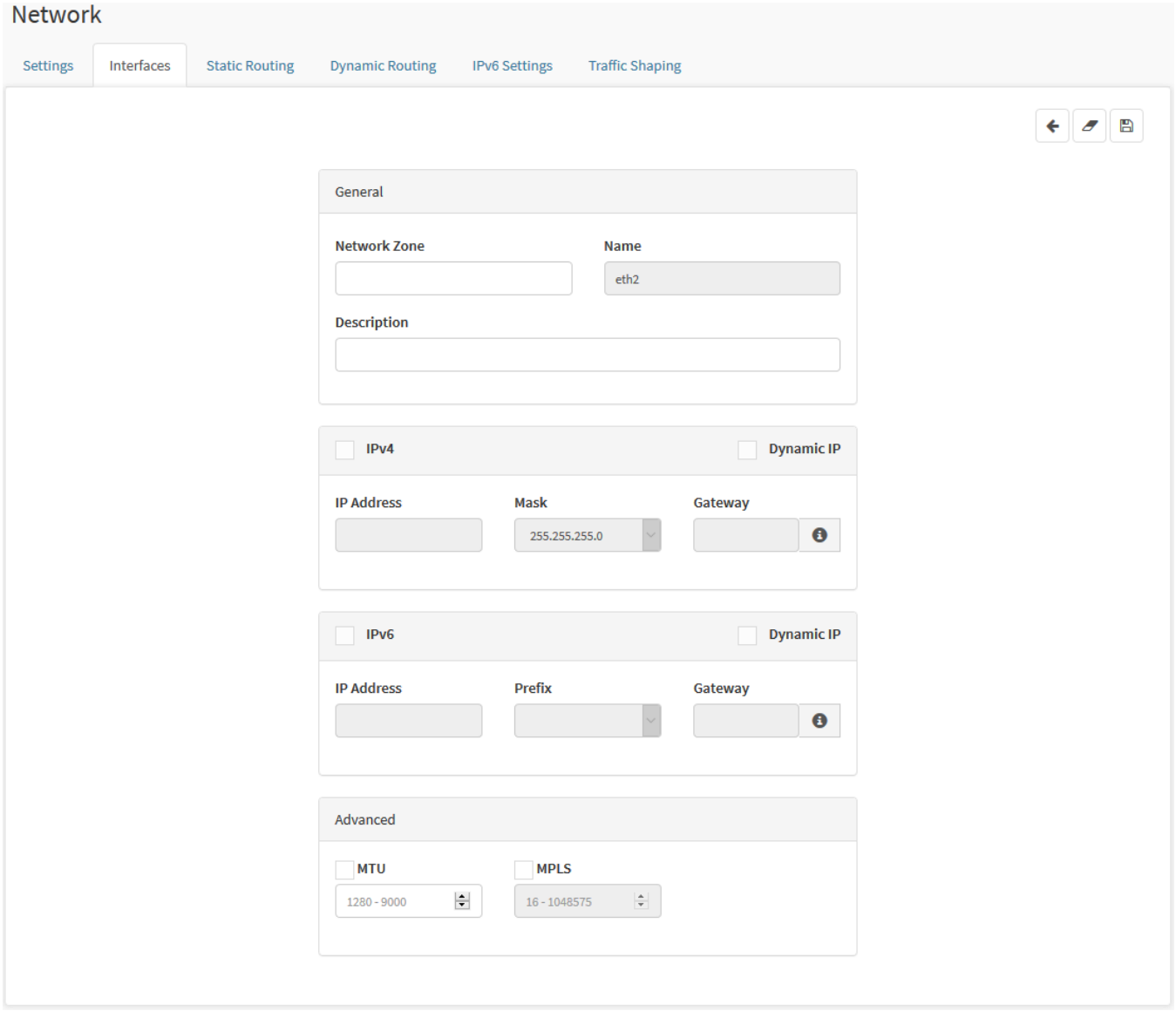
- **IPv6[ ]:** Mark this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW A, in this case, it will be: 2001 :: abcd: c0a8: b01;
- **Prefix:** Select the prefix "120".

To save, click **[ ]**.

This completes the LAN configuration of NGFW A. Next we will configure the interfaces that will be used by the routers.

Link with the NGFW router 1

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

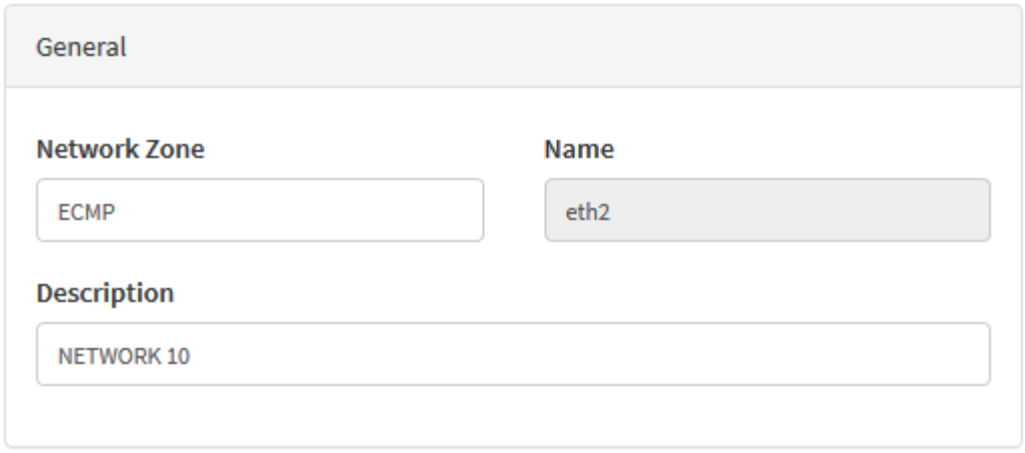


Interfaces - eth2

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

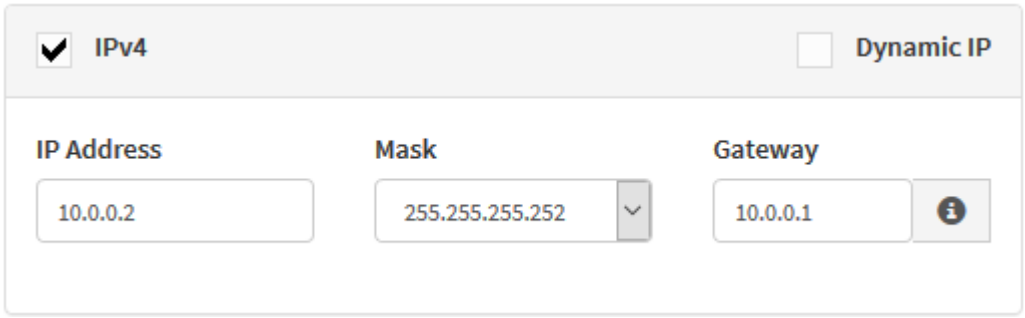


Interfaces - General Panel

- ***Network Zone*:** To organize, we name the Zones of all the interfaces that we will use "ECMP";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: NETWORK 10.

IPv4

Complete the form as shown below:



Interfaces - IPv4

- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by the router, in this case, it will be: 10.0.0.2;
- **Mask:** Enter the netmask that will be used by the router;
- **Gateway:** Define the gateway that will be used by the router, being: 10.0.0.1.

IPv6

Complete the form as shown below:

Interfaces - IPv6

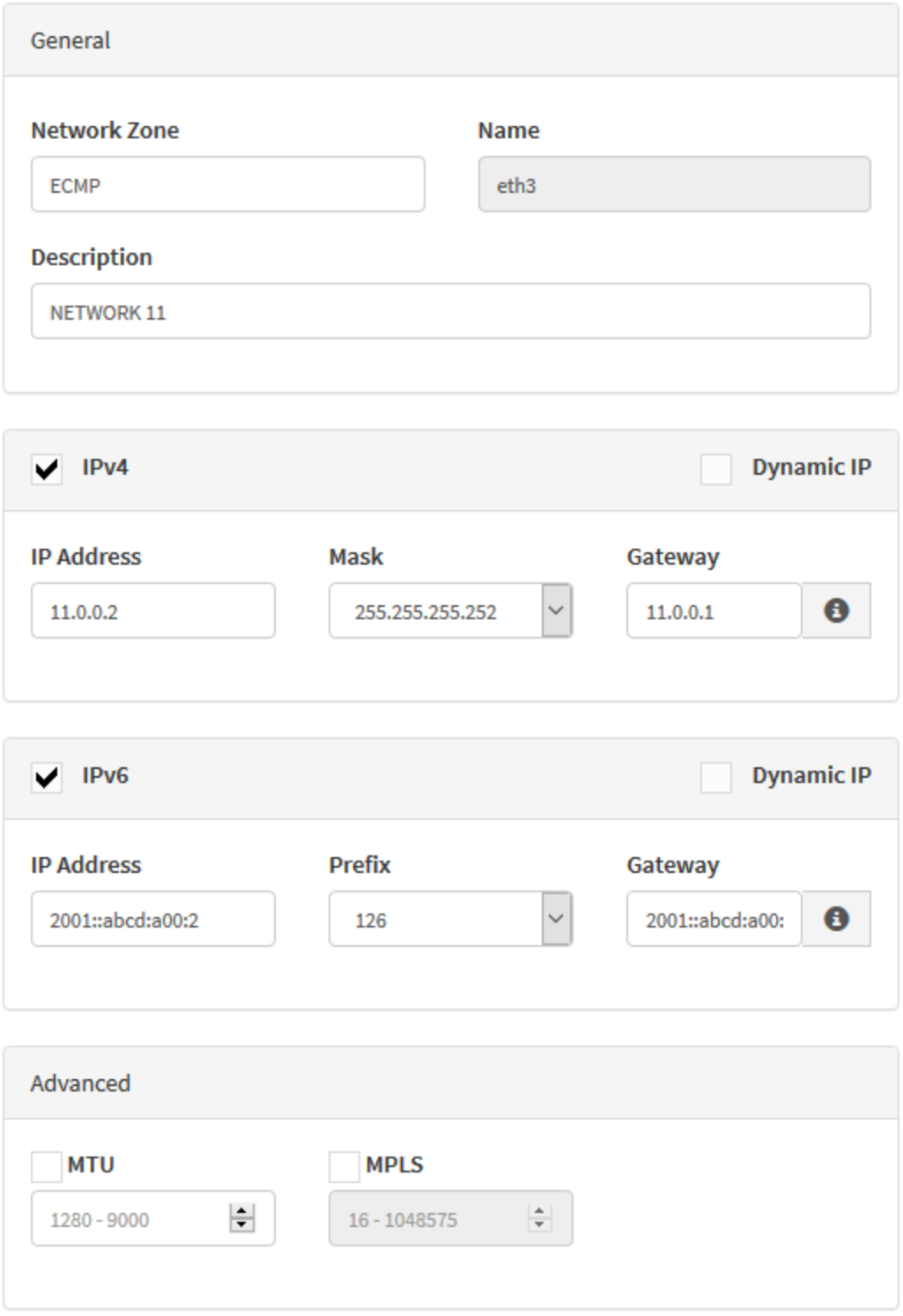
- **IPv6[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by the router, in this case, it will be: 2001 :: abcd: a00: 2;
- **Prefix:** Select the prefix "126";
- **Gateway:** Define the gateway that will be used by the router, we will use: 2001 :: abcd: a00: 1.

To save, click **[ ]**.

This completes the configuration of the interface of one of the routers. Follow the same steps to configure the other links*:*

Link to the NGFW 2 router

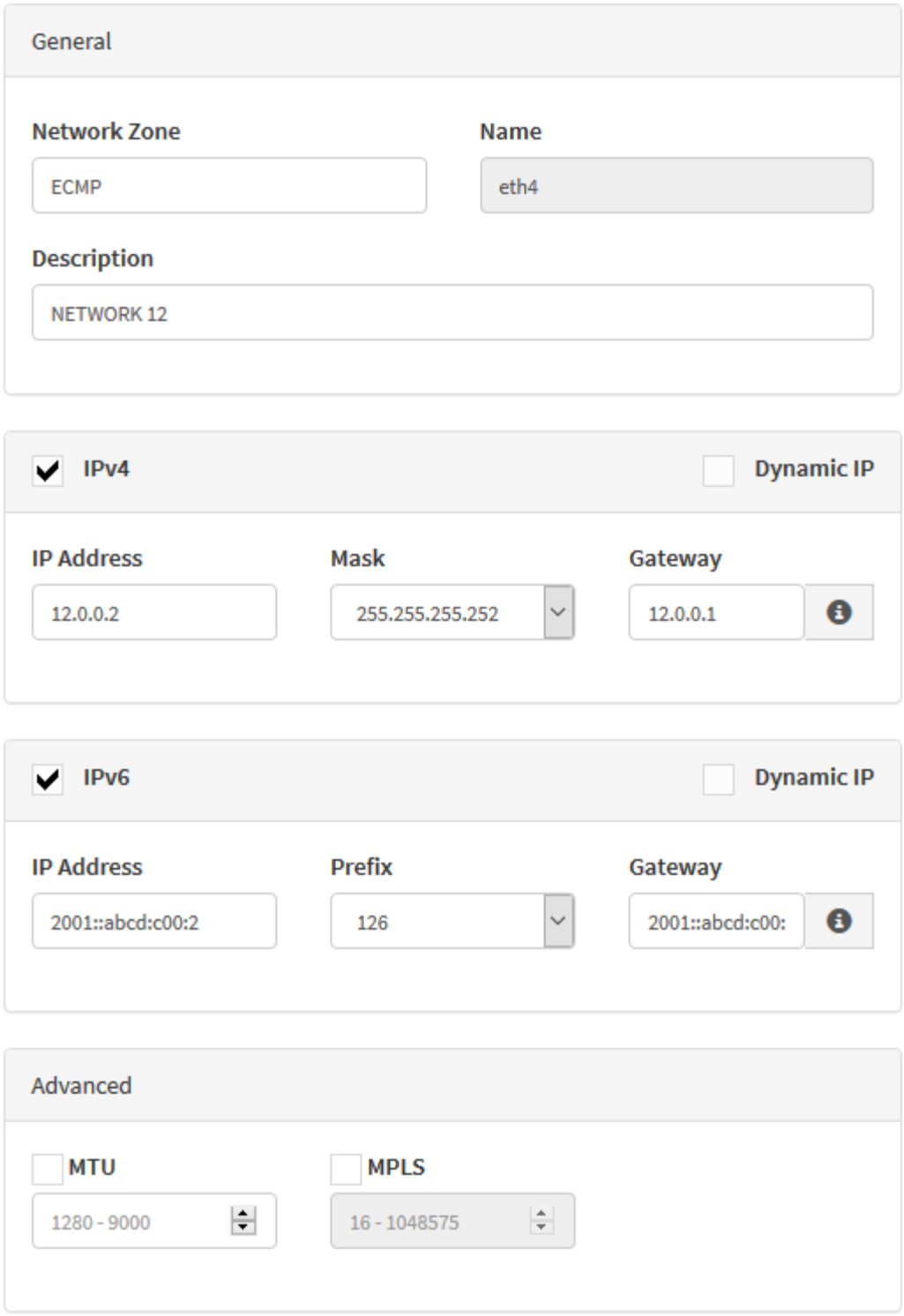
Below, an image demonstrating how the NGFW 2 Router link should be configured:



Interfaces - NGFW 2 Config

Link with the NGFW 3 router

Below, an image demonstrating how the link with the NGFW 3 Router should be configured:



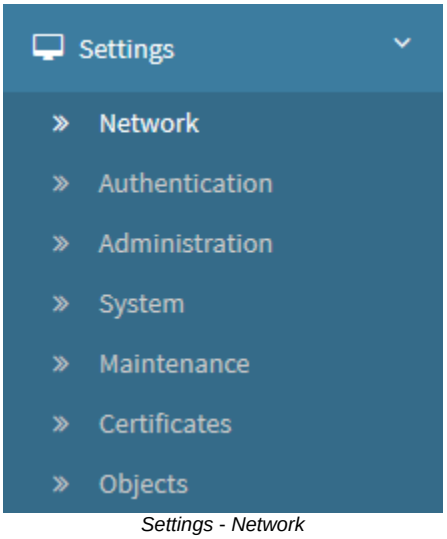
Interfaces - NGFW 3 Config

This finalizes the configuration of the Interfaces in NGFW A, next we will configure the static routes.

Dynamic Routing - ECMP - Configuration of static routes in UTM A

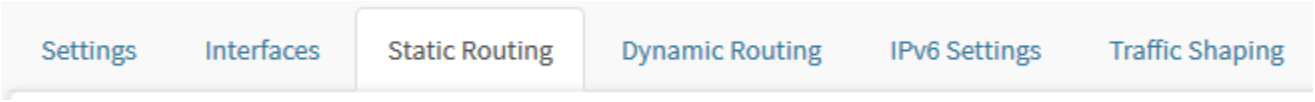
After configuring the interfaces, follow the steps below:

Still in Settings, in the Network option:



Settings - Network

Click on the Static Routing tab:

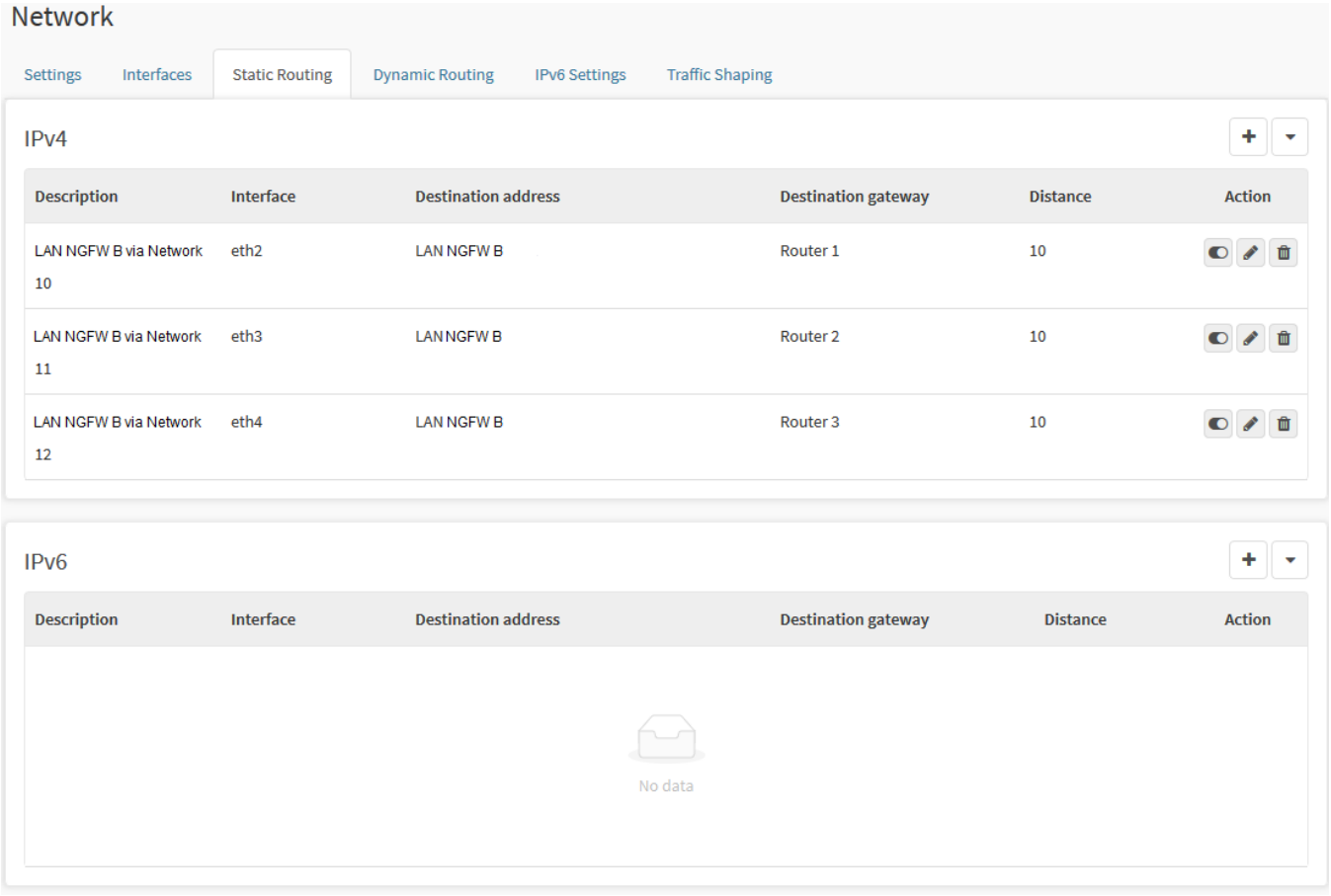


Static Routing tab

In this step, we will configure each static route using the IP of NGFW B as the destination, determining the routers as the gateway and placing them all in the same administrative distance. In this way, Static Routing will load balance using the source IP of the connection as a base.

Some details of the static routing tab will not be considered in this example, if you want more information, see this page.

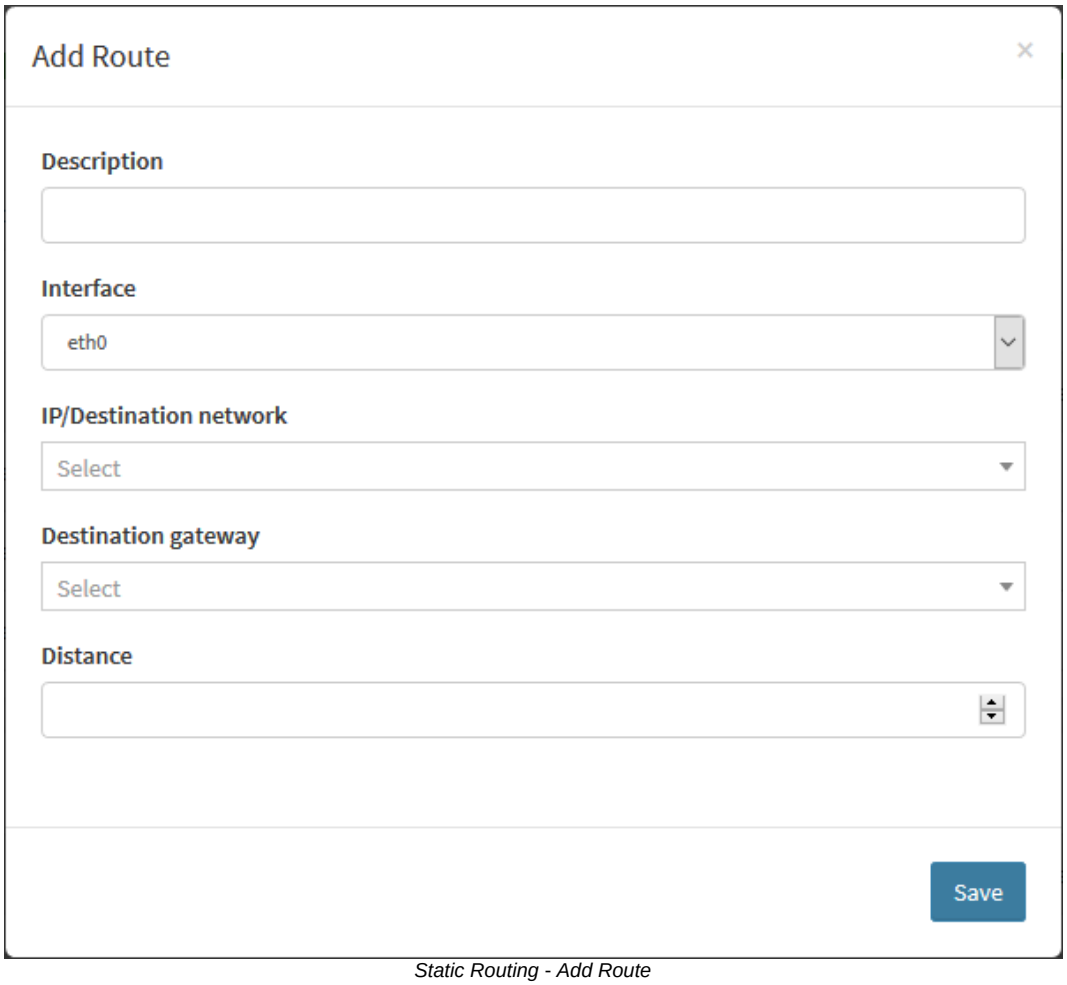
Below are the NGFW A interface configurations:



Network - Static Routing

Router 1

Click **[**  **]** to create a new route. The following window will be displayed:

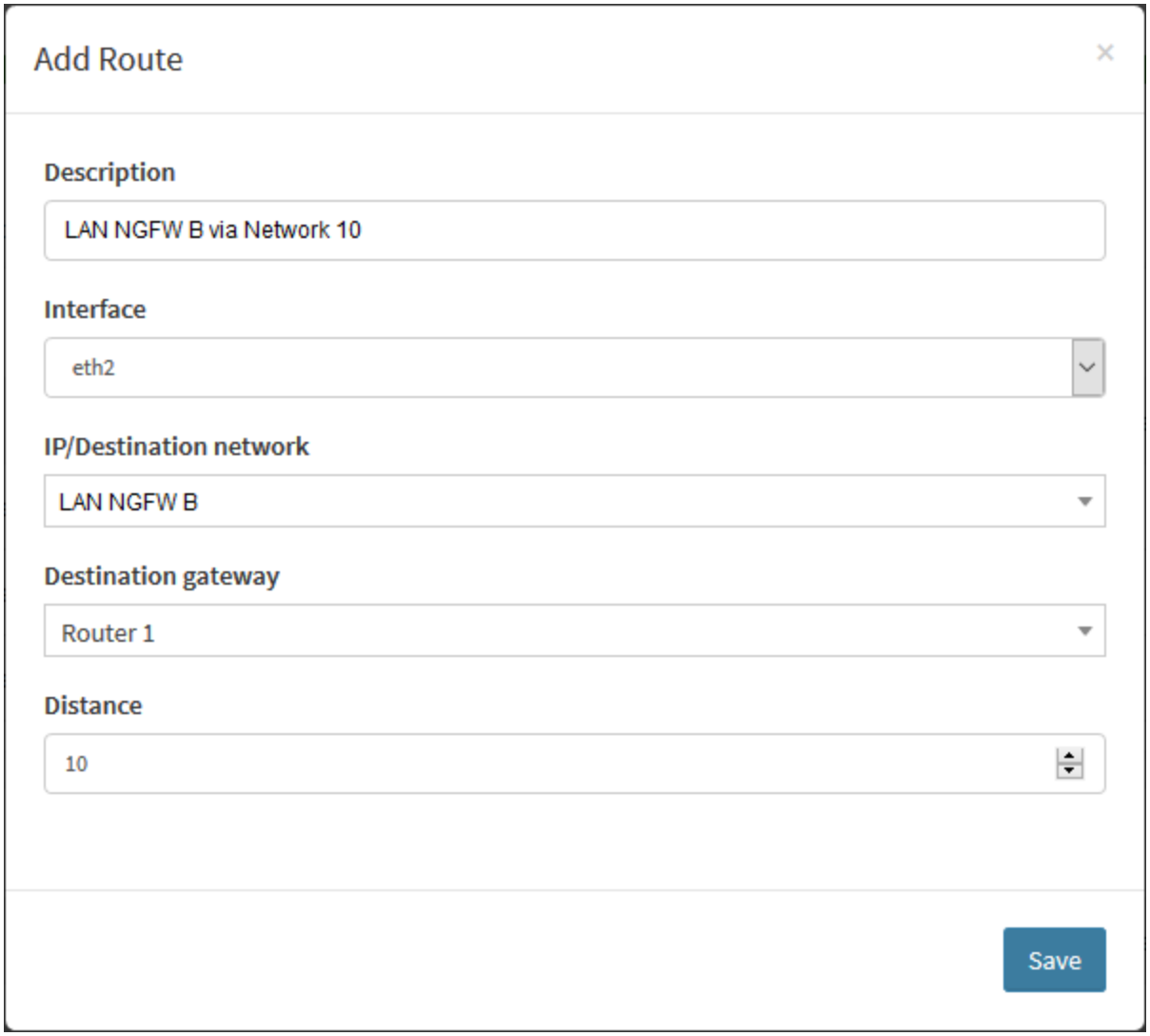


Static Routing - Add Route

- ***Description*:** To organize, we name the descriptions of all the interfaces that we will use "LAN NGFW B" and we will determine which IP range the route will use "via Network 10";
- ***Interface*:** Define the same interface that was used to configure the link with the router, in this case it will be "eth2";
- ***IP/Destination Network:*** *Configure using the NGFW B IP as a destination*;
- ***Destination Gateway*:** Determine the router as the destination gateway, in this case we will use "Router 1";
- ***Distance*:** Defines the administrative distance, note that all routers must use the same value, in this example, we will use the distance "10".

Note that in the IP/Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If not, they will not appear in the list. For more information on how to create an IP type object, see this page.

When finished, the static route must be configured this way:



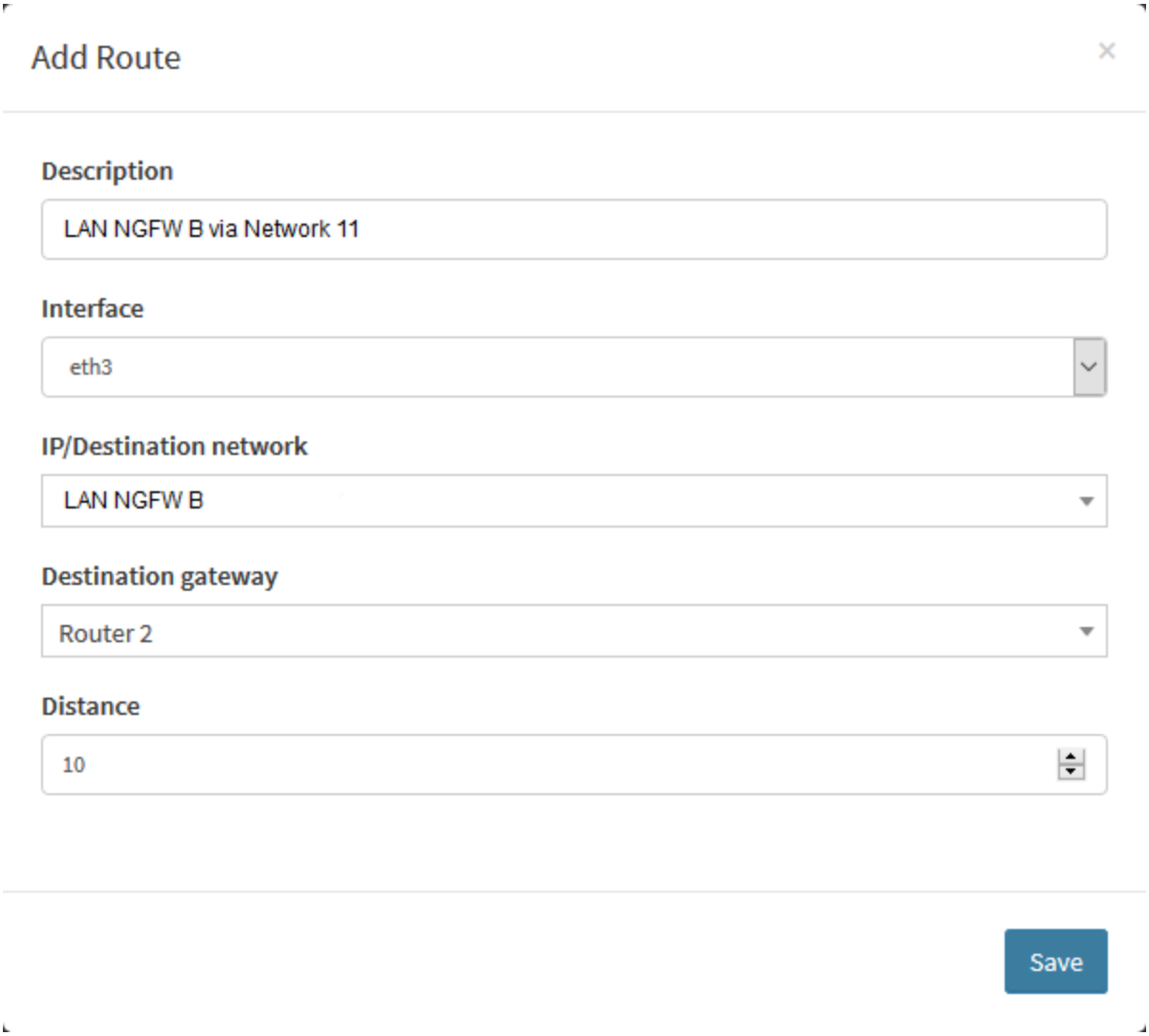
Static Routing - Add Route - Router 1

To finish the settings, click [Save].

This completes the configuration of the NGFW router 1 static route. Follow the same steps to configure the other routers:

Router 2

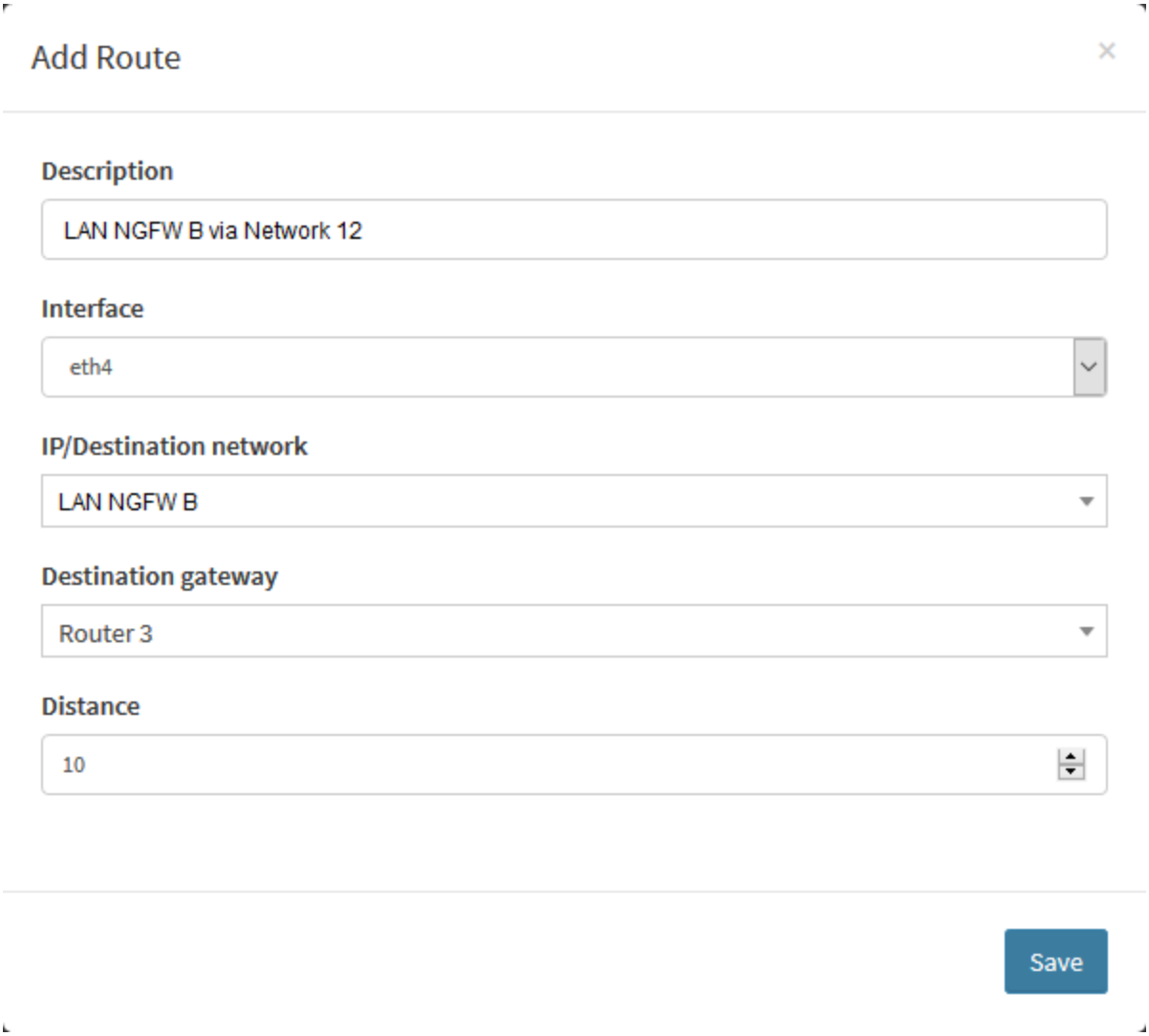
Below, an image demonstrating how the NGFW Router 2 should be configured:



Static Routing - Add Route - Router 2

Router 3

Below, there's an image demonstrating how the NGFW 3 Router should be configured:



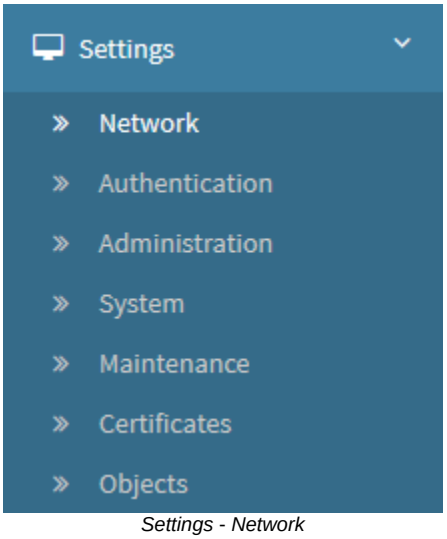
Static Routing - Add Route - Router 3

This finalizes the configuration of the static routes in NGFW A, next we will configure NGFW B.

Dynamic Routing - ECMP - Configuring the Interfaces on UTM B

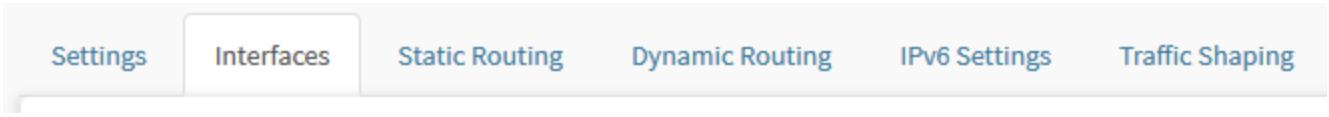
The procedures we will do here will be identical to the ones we did in NGFW A, but referring to NGFW B.

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



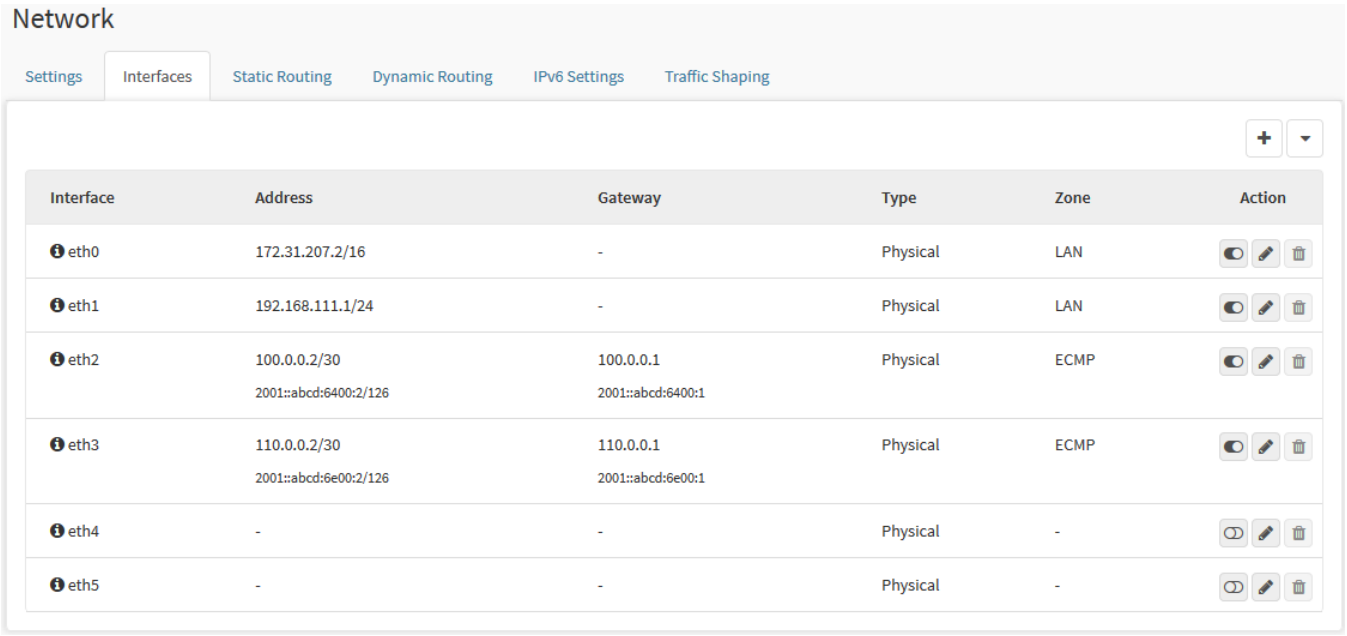
Interfaces tab

We will make the following settings in this step:

- Initially we will need to configure the NGFW B LAN (to serve as the NGFW A destination);
- Configure the physical interfaces that will be used to connect with the routers that will be used as a link by NGFW B:
  - NGFW 4;
  - NGFW 5.

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

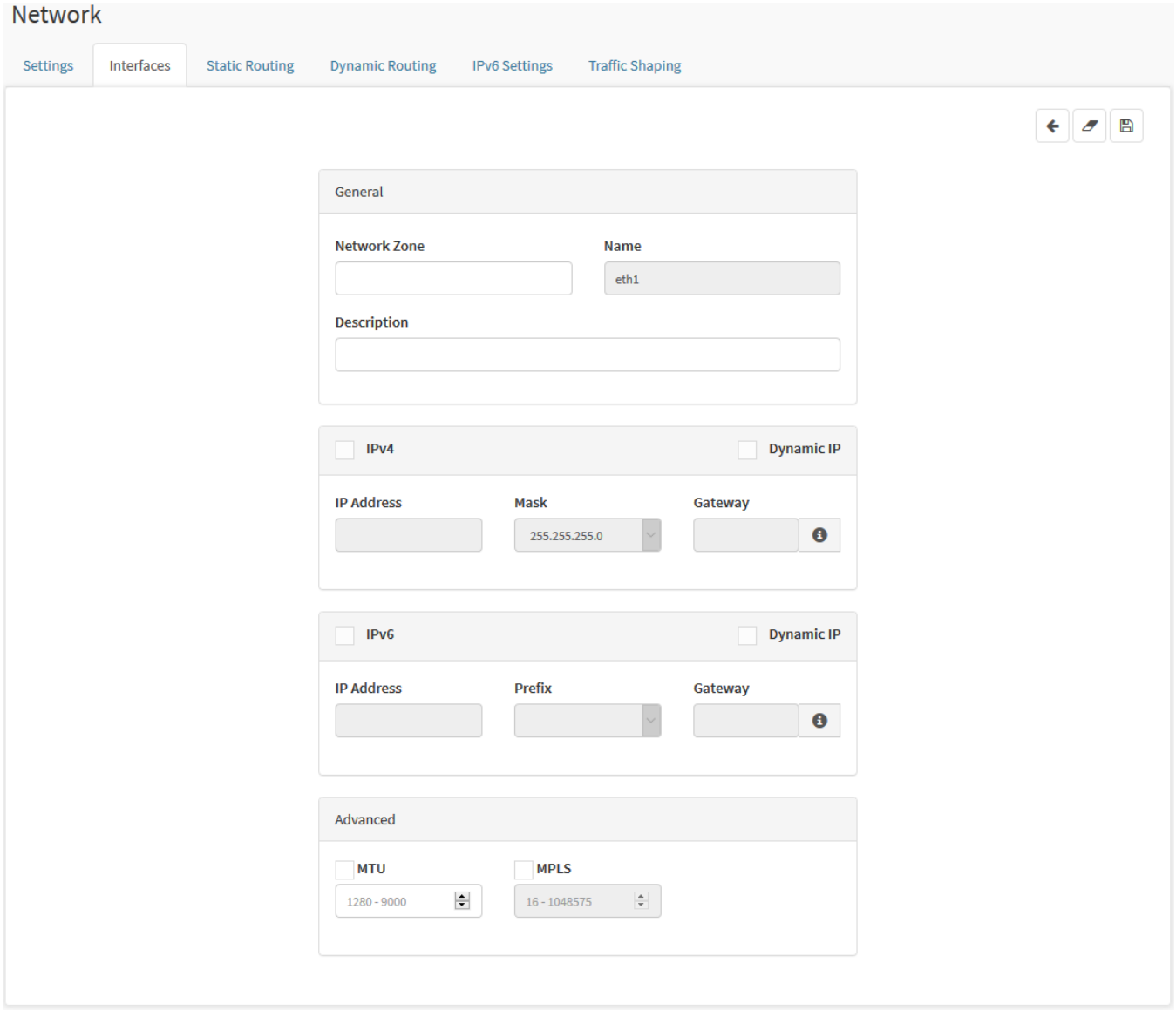
Below are the NGFW B interface configurations:



Network - Interfaces

LAN configuration of NGFW B

Access the physical interface you will use and click **[**  **]**. The following screen will be displayed:

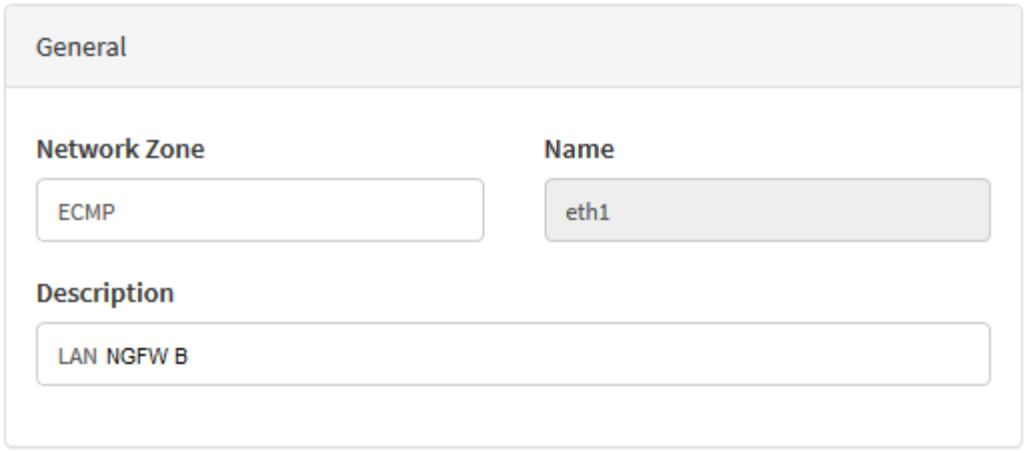


Interfaces - eth1

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

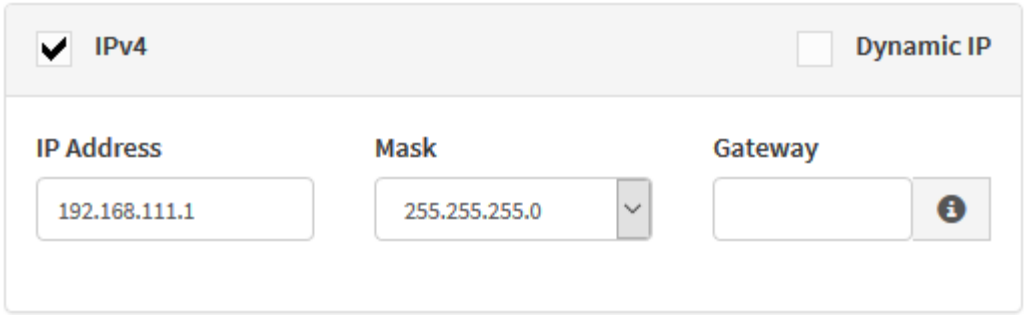


Interfaces – Painel *General*

- ***Network Zone*:** To organize, we name the Zones of all the interfaces that we will use "ECMP";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: LAN NGFW B.

IPv4

Complete the form as shown below:



Interfaces - IPv4

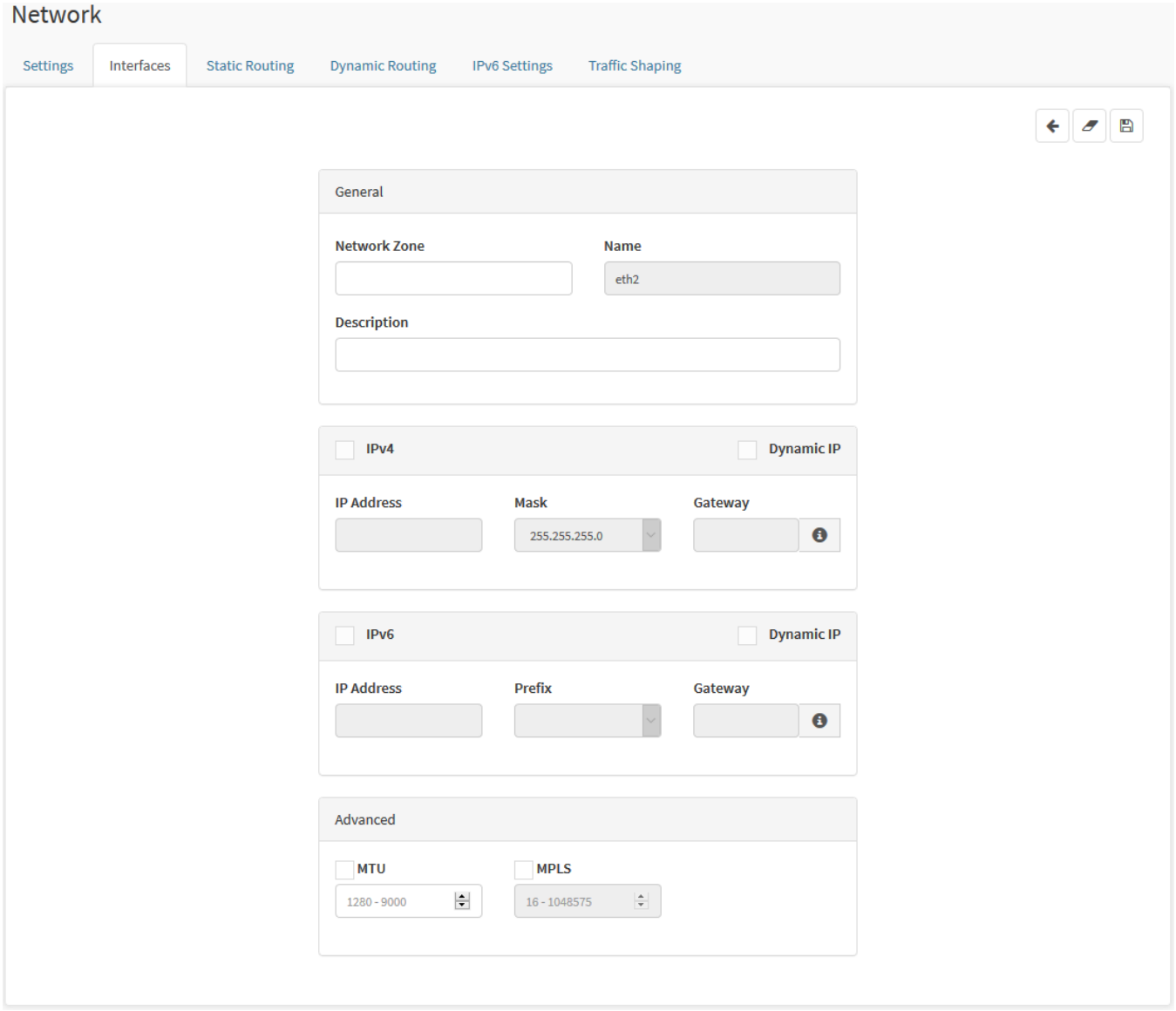
- **IPv4[ ]:** Mark this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by NGFW A, in this case, it will be: 192.168.11.1;
- **Mask:** Enter the netmask to be used by NGFW B.

To save, click **[ ]**.

Next we will configure the interfaces that will be used by the routers.

Link with the NGFW 4 router

Access the physical interface you will use and click **[ ]**. The following screen will be displayed:

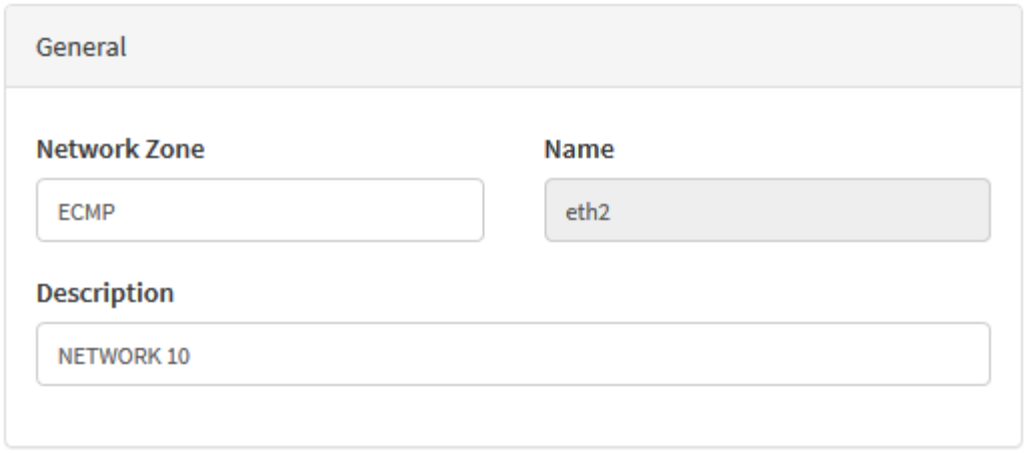


Interfaces - eth2

Next we will detail the panels that we will need to configure.

General Panel

Complete the form as shown below:

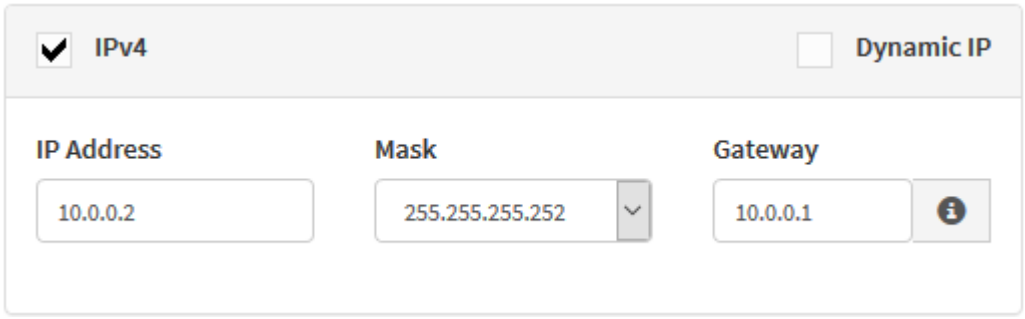


Interfaces – Painel *General*

- ***Network Zone*:** To organize, we name the Zones of all the interfaces that we will use "ECMP";
- ***Description*:** Insert the desired description in order to facilitate the identification of the interface later. Ex.: NETWORK 10.

IPv4

Complete the form as shown below:



Interfaces - IPv4

- **IPv4[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by the router, in this case, it will be: 10.0.0.2;
- **Mask:** Enter the netmask that will be used by the router;
- **Gateway:** Define the gateway that will be used by the router, being: 10.0.0.1.

IPv6

Complete the form as shown below:

Interfaces - IPv6

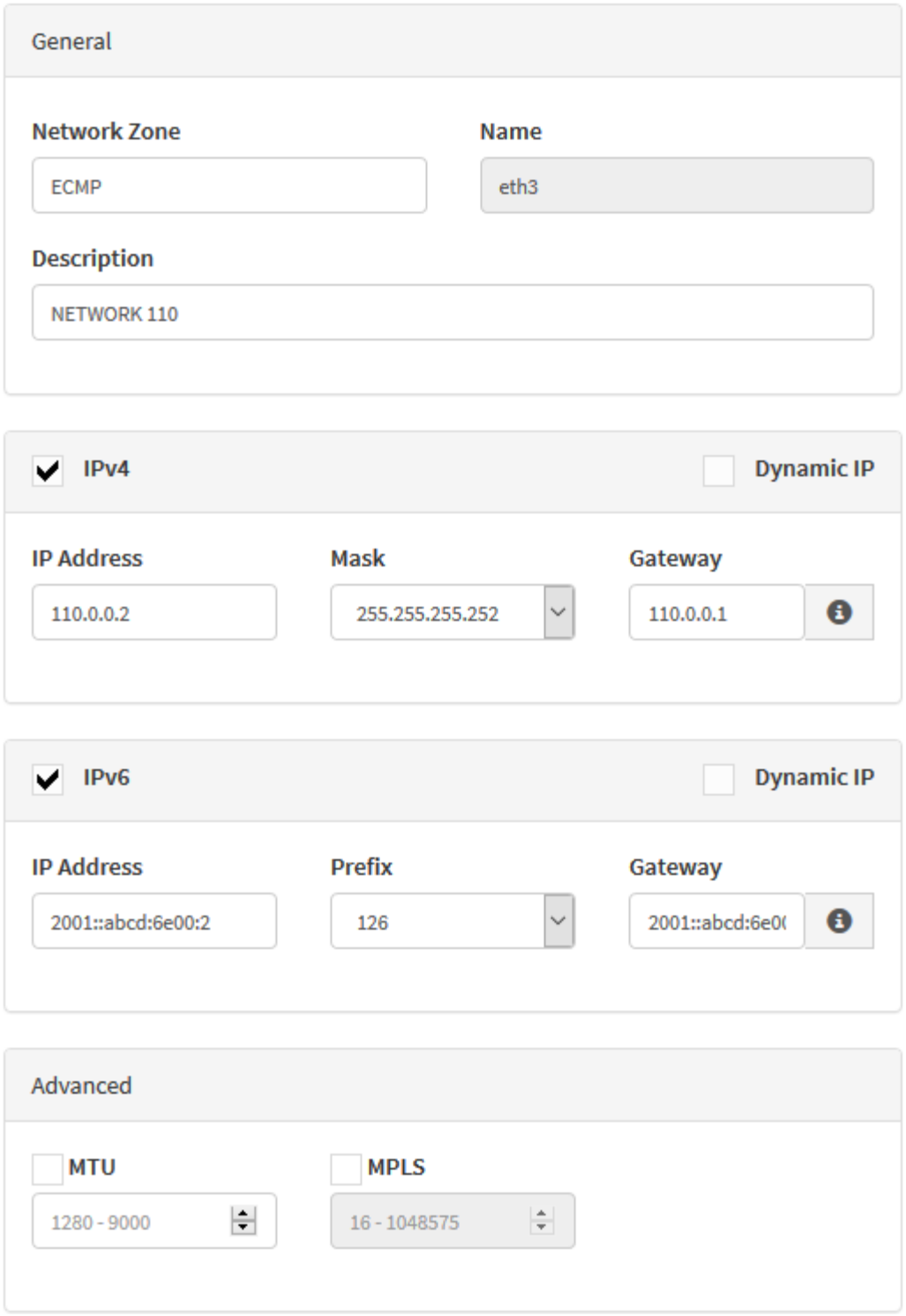
- **IPv6[ ]:** Check this checkbox to enable the form;
- **IP Address:** Add the IP that will be used by the router, in this case, it will be: 2001 :: abcd: 6400: 2;
- **Prefix:** Select the prefix "126";
- **Gateway:** Define the gateway that will be used by the router, we will use: 2001 :: abcd: 6400: 1.

To save, click **[ ]**.

This completes the configuration of the interface of one of the routers. Follow the same steps to set up the other link:

Link with the NGFW 5 router

Below, an image demonstrating how the NGFW 5 Router link should be configured:



Interfaces - NGFW 5 Config

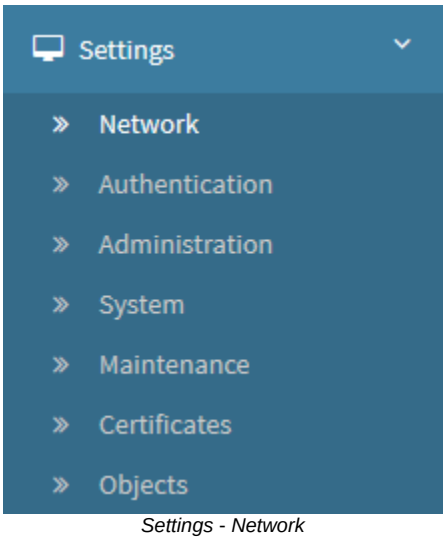
This finalizes the configuration of the Interfaces in NGFW B, next we will configure the static routes.

Dynamic Routing - ECMP - Configuration of static routes in UTM B

As in the previous step, the procedures that we will do here will be identical to the ones we did at the NGFW A, but referring to NGFW B.

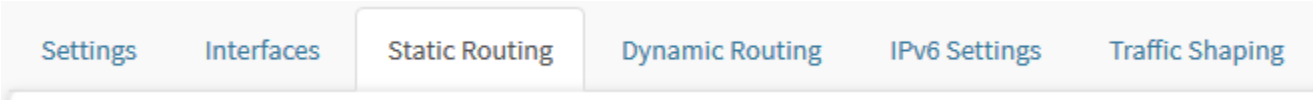
After configuring the interfaces, follow the steps below:

Still in Settings, in the Network option:



Settings - Network

Click on the Static Routing tab:

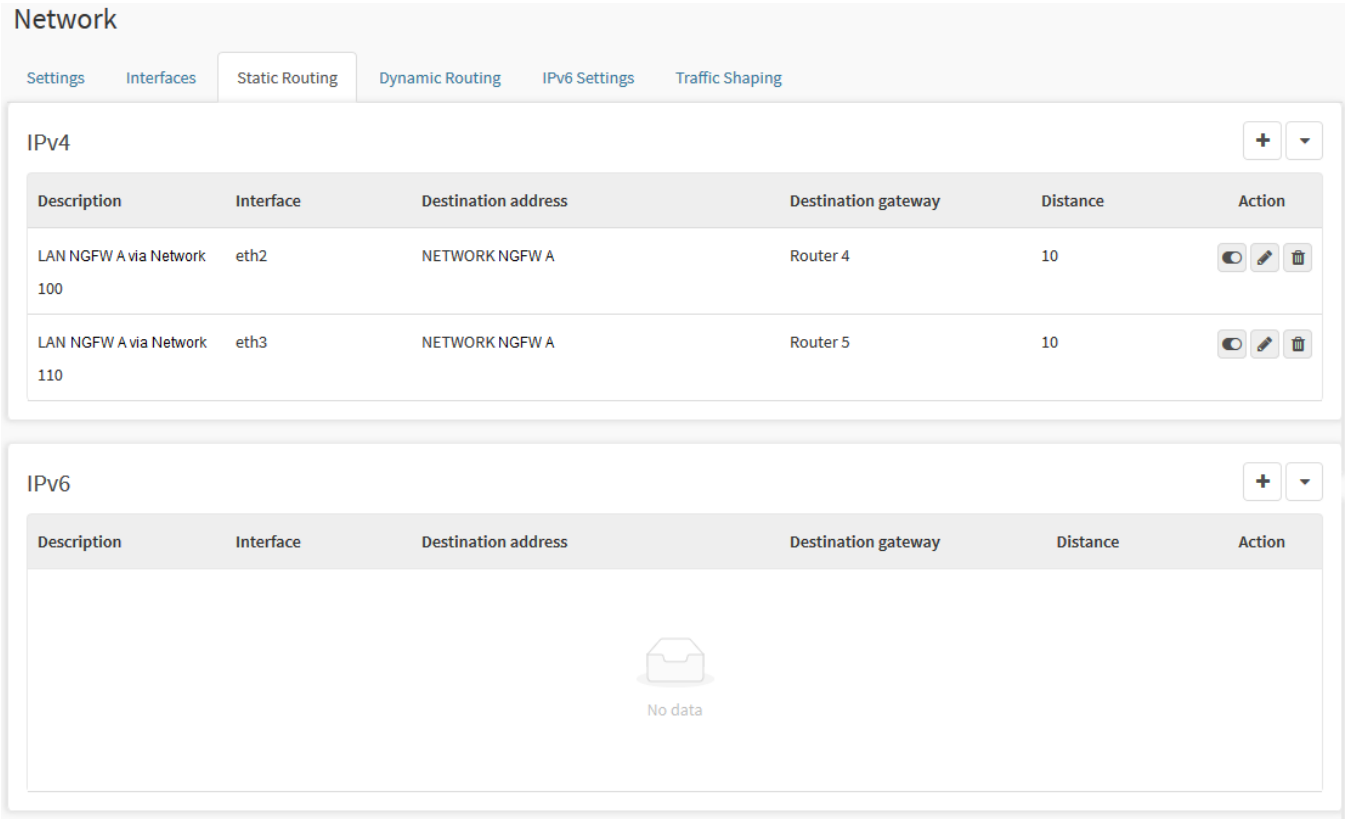


Static Routing Tab

In this step, we will configure each static route using the IP of NGFW A as the destination, determining the routers as the gateway and placing all of them in the same administrative distance. In this way, Static Routing will load balance using the source IP of the connection as a base.

Some details of the static routing tab will not be considered in this example, if you want more information, see this page.

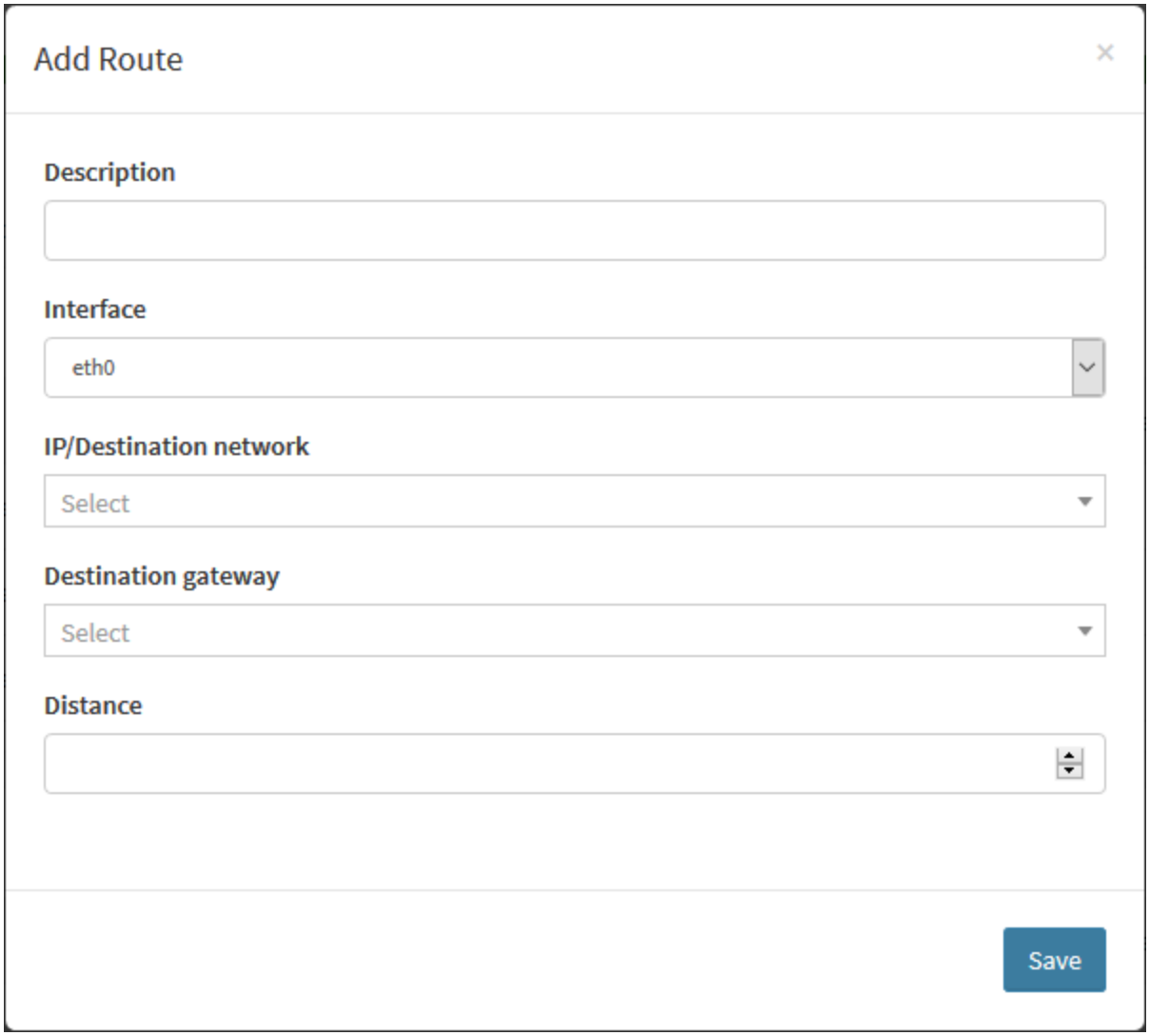
Below are the NGFW B interface settings:



Network - Static Routing

Router 4

Click **[**  **]** to create a new route. The following window will appear:

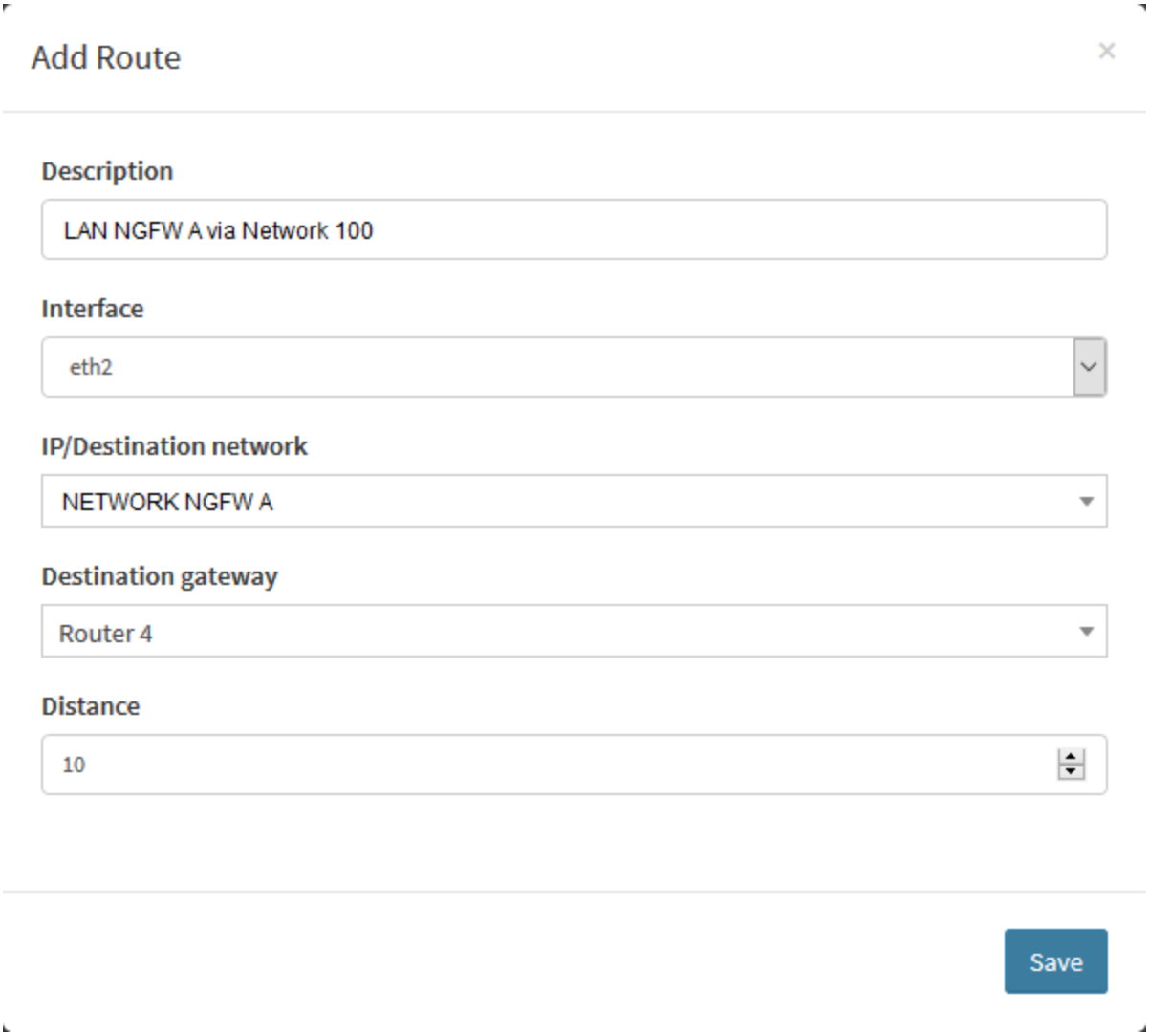


Static Routing - Add Route

- ***Description*:** To organize, we will name the descriptions of all the interfaces that we will use "LAN NGFW A" and we will determine which IP range the route will use "via Network 100";
- ***Interface*:** Define the same interface that was used to configure the link with the router, in this case it will be "eth2";
- ***IP/Destination Network:*** *Configure using the NGFW A IP as a destination*;
- ***Destination Gateway*:** Determine the router as the destination gateway, in this case we will use "Router 4";
- ***Distance*:** Defines the administrative distance, note that all routers need to use the same value, in this example, we will use the distance "10".

Note that in the IP / Destination Network and Destination Gateway fields, the listed objects are of the unique type, so it is necessary to create them in advance. If this is not done, they will not appear in the list. For more information on how to create an IP-type object, see this page.

When finished, the static route must be configured in this way:



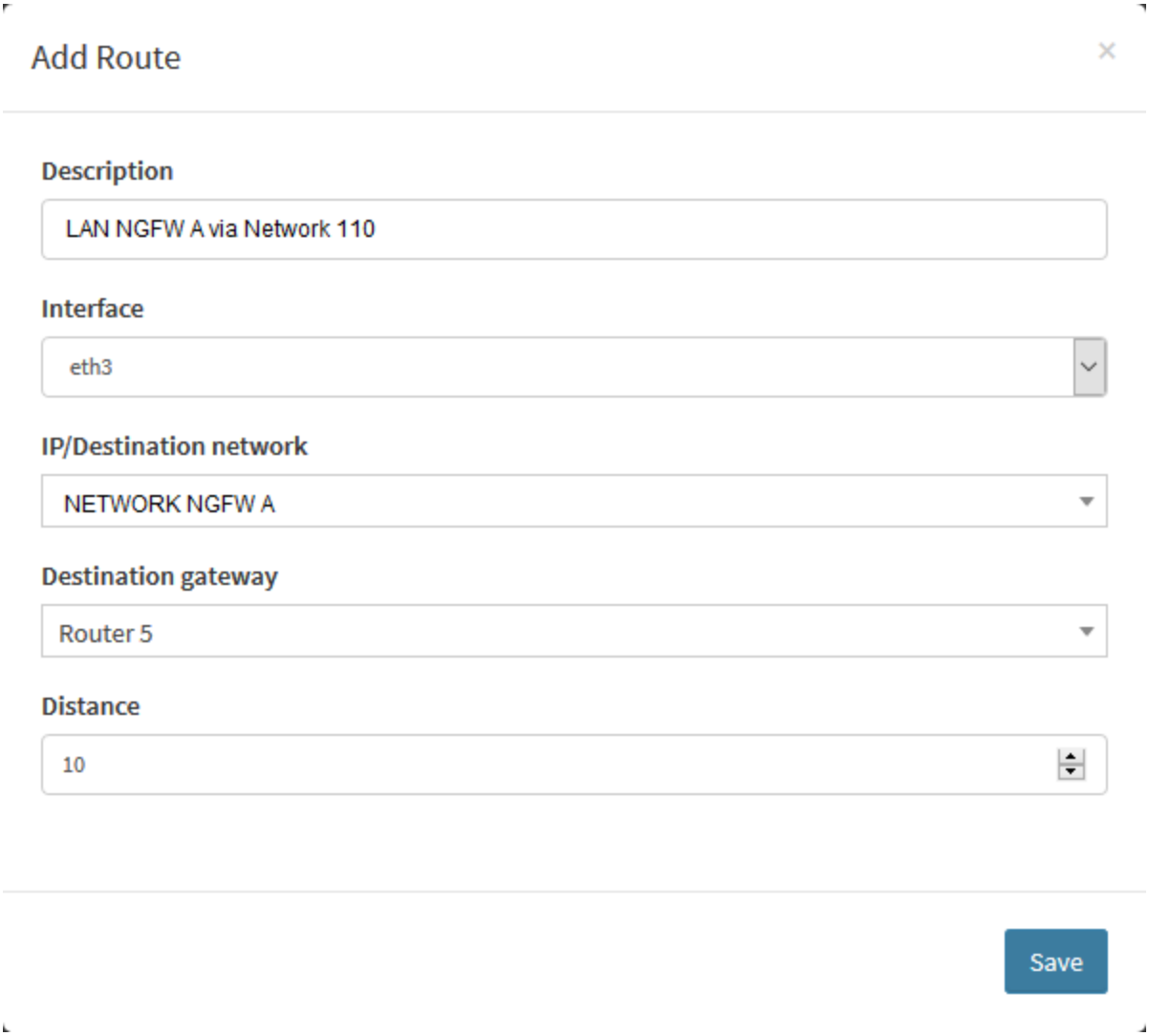
Static Routing - Add Route - Router 4

To finish the settings, click [Save].

This completes the configuration of the NGFW 4 router static route. Follow the same steps to configure the other routers:

Router 5

Below, an image demonstrating how the NGFW 5 Router should be configured:



Static Routing - Add Route - Router 5

This finalizes the configuration of the static routes in NGFW B, the last step is to validate all the configurations that we have made.

Dynamic Routing - ECMP - Configuration Validation

To carry out the validation, we will access the NGFW A's CLI and run some commands, if you need more information about this, see this page.

One of the simplest tests to validate the operation of the routes is to *ping* from the NGFW A (172.31.207.1) to the NGFW B (172.31.207.2) and check for an answer, as shown on the image below:

```
admin  >ping 172.31.207.2
PING 172.31.207.2 (172.31.207.2) 56(84) bytes of data.
64 bytes from 172.31.207.2: icmp_seq=1 ttl=64 time=1.47 ms
64 bytes from 172.31.207.2: icmp_seq=2 ttl=64 time=0.640 ms
64 bytes from 172.31.207.2: icmp_seq=3 ttl=64 time=0.651 ms
64 bytes from 172.31.207.2: icmp_seq=4 ttl=64 time=0.523 ms
64 bytes from 172.31.207.2: icmp_seq=5 ttl=64 time=0.600 ms
64 bytes from 172.31.207.2: icmp_seq=6 ttl=64 time=0.570 ms
admin  >
```

CLI - Validation of communication with NGFW B by Ping

In addition, if you want to list all the routes that NGFW A is currently using, just run the *ip route list* command and check if the created routes were listed:

```
admin  >ip route list
default via 172.31.0.1 dev eth0
10.0.0.0/30 dev eth2 proto kernel scope link src 10.0.0.2
11.0.0.0/30 dev eth3 proto kernel scope link src 11.0.0.2
12.0.0.0/30 dev eth4 proto kernel scope link src 12.0.0.2
172.31.0.0/16 dev eth0 proto kernel scope link src 172.31.207.1
192.1.1.0/24 dev dummy1 proto kernel scope link src 192.1.1.1
192.168.11.0/24 dev eth1 proto kernel scope link src 192.168.11.1
192.168.111.0/24
        nexthop via 10.0.0.1 dev eth2 weight 10
        nexthop via 11.0.0.1 dev eth3 weight 10
        nexthop via 12.0.0.1 dev eth4 weight 10
admin  >
```

CLI - ip route list do NGFW A

It is also possible to carry out these same steps at the other end, following a demonstration using the *ping* command to verify the communication status with the NGFW A:

```
admin  >ping 172.31.207.1
PING 172.31.207.1 (172.31.207.1) 56(84) bytes of data.
64 bytes from 172.31.207.1: icmp_seq=1 ttl=64 time=0.599 ms
64 bytes from 172.31.207.1: icmp_seq=2 ttl=64 time=0.534 ms
64 bytes from 172.31.207.1: icmp_seq=3 ttl=64 time=0.356 ms
64 bytes from 172.31.207.1: icmp_seq=4 ttl=64 time=0.488 ms
64 bytes from 172.31.207.1: icmp_seq=5 ttl=64 time=0.499 ms
admin  >
```

CLI - Validation of communication with NGFW A by Ping

And finally, listing the NGFW B routes through the *ip route list*:

```
admin  >ip route list
default via 172.31.0.1 dev eth0
100.0.0.0/30 dev eth2 proto kernel scope link src 100.0.0.2
110.0.0.0/30 dev eth3 proto kernel scope link src 110.0.0.2
172.16.10.0/24 via 172.31.0.1 dev eth0
172.16.12.0/23 via 172.31.0.1 dev eth0
172.16.20.0/24 via 172.31.0.1 dev eth0
172.16.100.0/24 via 172.31.0.1 dev eth0
172.16.101.0/24 via 172.31.0.1 dev eth0
172.16.102.0/24 via 172.31.0.1 dev eth0
172.16.103.0/24 via 172.31.0.1 dev eth0
172.25.0.0/16 via 172.31.0.1 dev eth0
172.30.0.0/30 via 172.31.0.1 dev eth0
172.31.0.0/16 dev eth0 proto kernel scope link src 172.31.207.2
172.32.0.0/16 via 172.31.0.1 dev eth0
192.168.11.0/24
        nexthop via 100.0.0.1 dev eth2 weight 10
        nexthop via 110.0.0.1 dev eth3 weight 10
192.168.100.0/24 via 172.31.0.1 dev eth0
192.168.105.0/24 via 172.31.0.1 dev eth0
192.168.111.0/24 dev eth1 proto kernel scope link src 192.168.111.1
192.168.200.0/24 via 172.31.0.1 dev eth0
192.168.253.0/24 via 172.31.0.1 dev eth0
192.168.254.0/24 via 172.31.0.1 dev eth0
admin  >
```

CLI - ip route list do NGFW B

This concludes the demonstration, for more information on Static Routing, see this page.

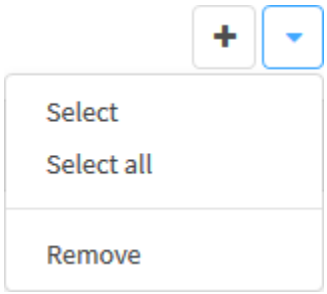
If you want to see more details about the columns on the Static Routing tab, visit this page.

Static Routing - Actions Menu

At the top right of the screen, next to the Add Routes button we have the actions menu:

Static Routing – Actions menu button

By clicking on this button the menu below is displayed:



Static Routing – Actions menu

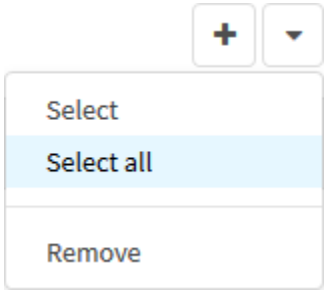
The menu consists of the following options:

- *Select;*
- *Select All*;
- *Remove*.

Next, each action menu option will be detailed.

Static Routing - Actions Menu - Select All

By clicking on “Select All” in the action menu all routes will be selected.



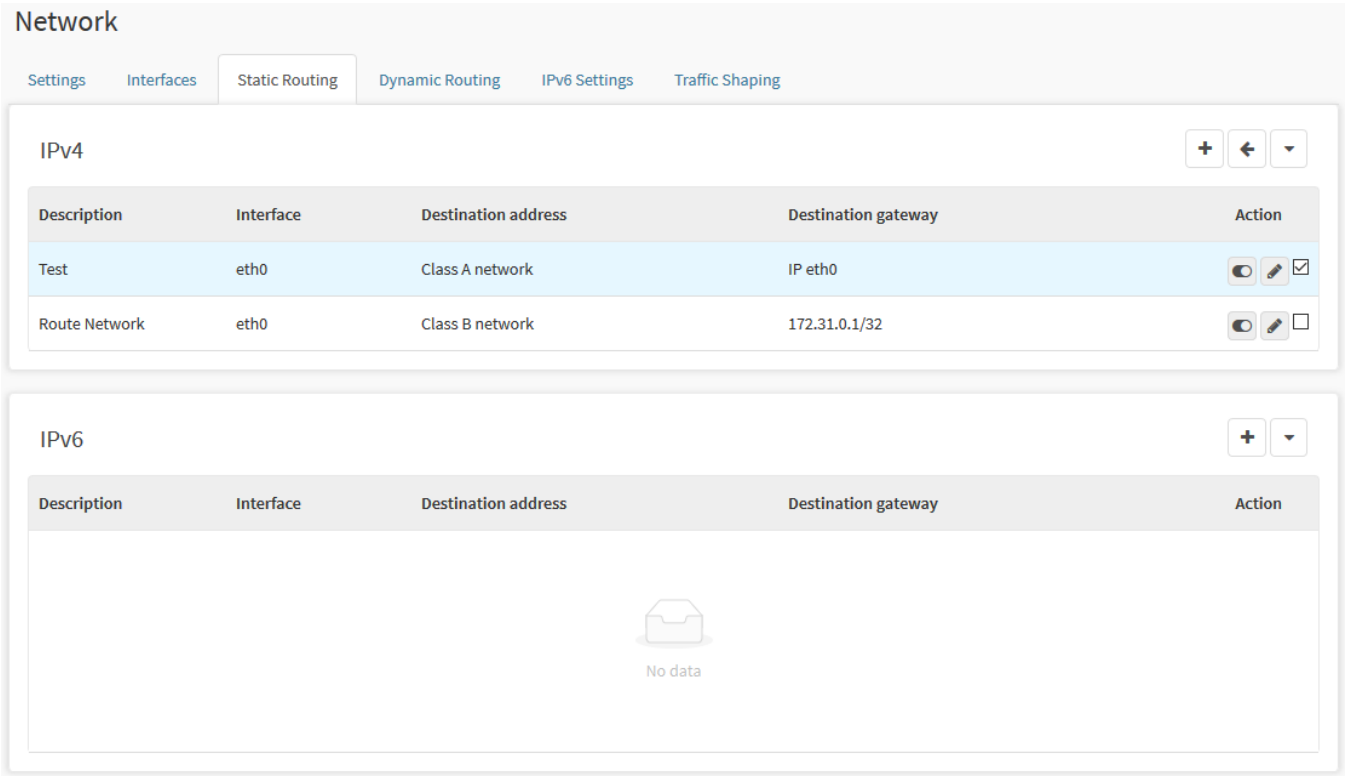
Interfaces – Select All

This allows changes that affect all routes to be easily implemented.

Static Routing - Actions Menu - Remove

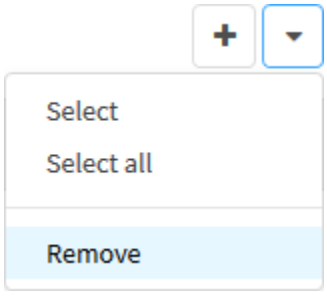
Through the action menu it is possible to delete several routes at the same time. Follow the steps below:

1. Select the routes you want to delete by clicking the checkbox **[ ]**;



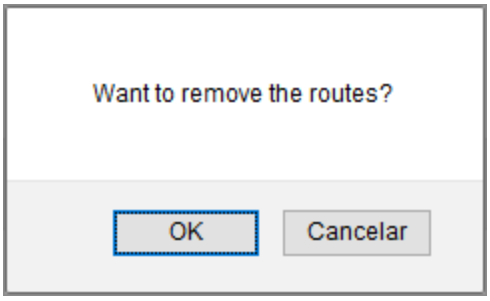
Static Routing – Selected routes

2. Click on the Actions menu **[ ]** and select the option “Remove”;



Static Routing – Actions Menu – *Remove*

4. A screen will appear asking if you want to delete the selected route:



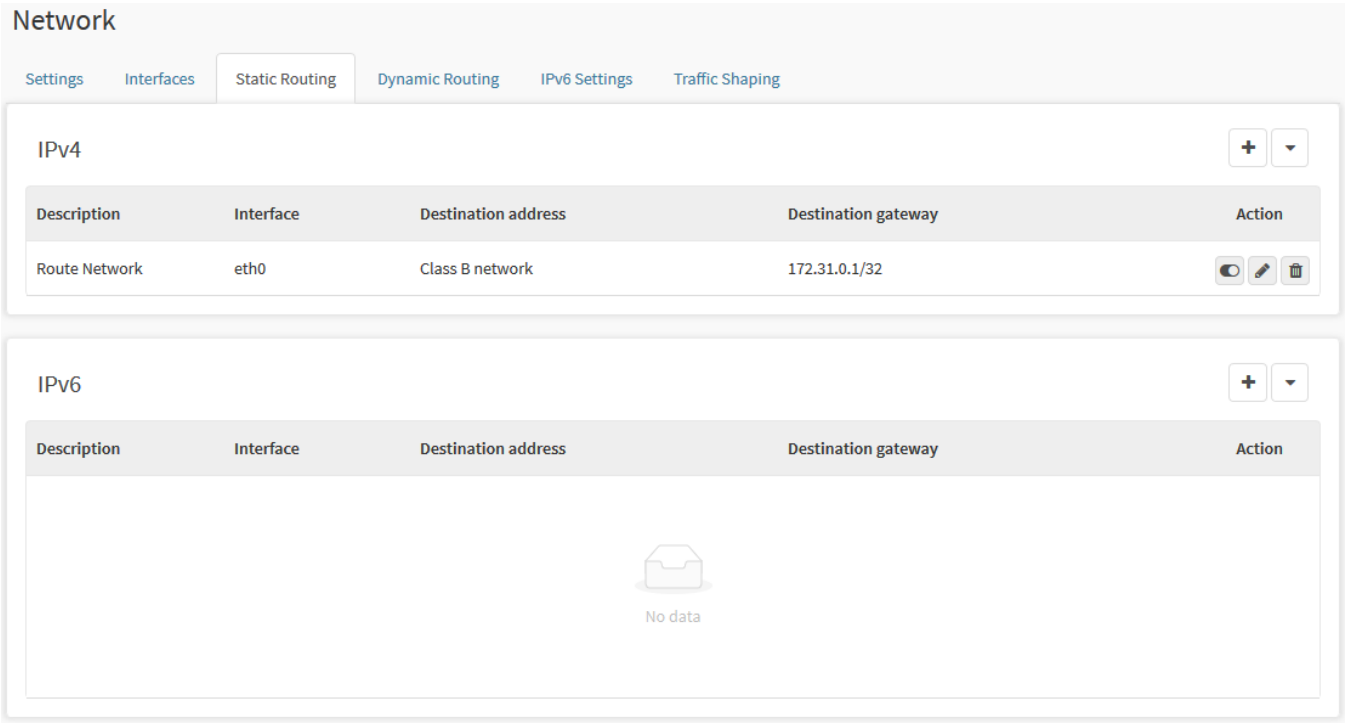
Static Routing –Routes deletion confirmation

If you want to cancel, click the **[** Cancel **]** button. To finish removing the route, click the **[** OK **]** button.

The route has been successfully deleted.

Static Routing - Columns

Below we will explain each column of the Static Routing tab:



Static Routing

- ***Description*:** Displays the route description;
- ***Interface*:** Displays the interface for the route;
- ***Destination address*:** Displays the destination address of the registered route;
- ***Destination gateway*:** Displays the destination gateway of the registered route;
- ***Actions*:** Provides the following essential actions:
    - ***Enable*[ ]/*Disable*[ ]:** Allows you to enable or disable routes;
    - ***Edit*[ ]:** Allows you to edit the route settings added in the Add Button;
    - ***Delete*[ ]:** Allows you to remove an interface.

For more information on Static Routing, visit this page.

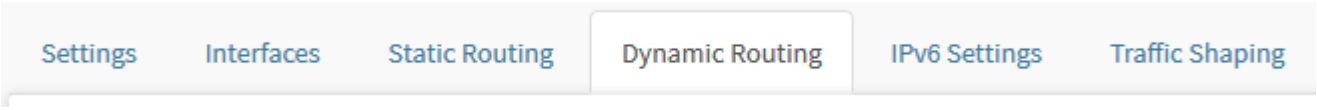
Network - Dynamic Routing

Many routing concepts apply to static routing. However, without understanding these basic concepts, it is difficult to understand the more complex dynamic advanced routing.

The dynamic routing protocol is capable of balancing packets of the same flow between multiple links simultaneously. Unlike static routing, it acts in reaction to damage to the structure of the logical network seeking the best routes, according to their availability, allowing the availability of the maximum valid routes in the event of any eventuality.

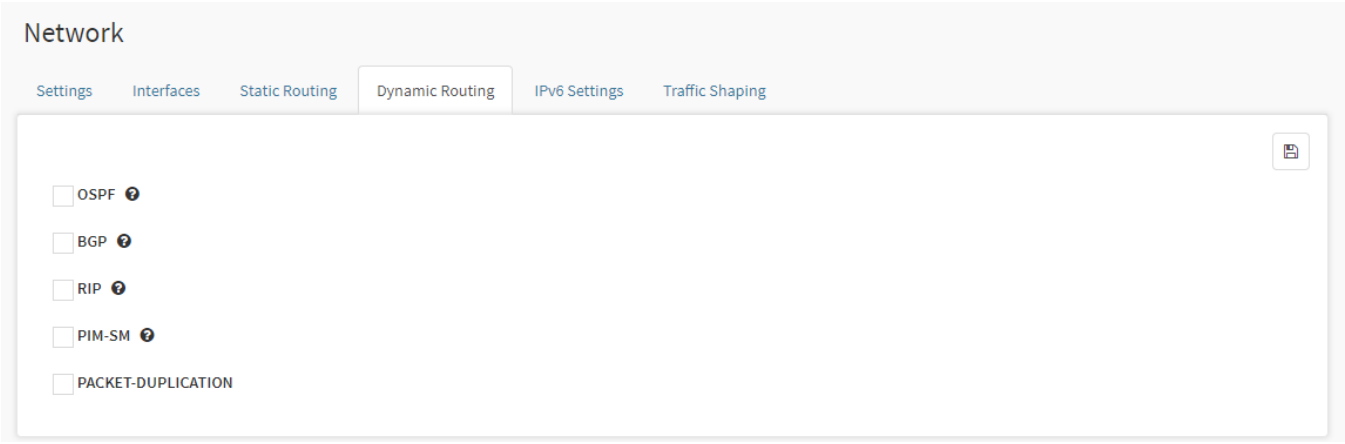
 This chapter of the document is not intended to cover the “Advanced features of dynamic routing”, it only aims to present which protocols are supported by Blockbit NGFW. *For more information regarding “dynamic routing” and each supported protocol, the administrator should look for complementary documentation, for his knowledge and technical improvement.*

Click on the Dynamic Routing tab.



Dynamic Routing tab

The “Dynamic Routing” screen will appear, as shown by the image below:



Dynamic Routing

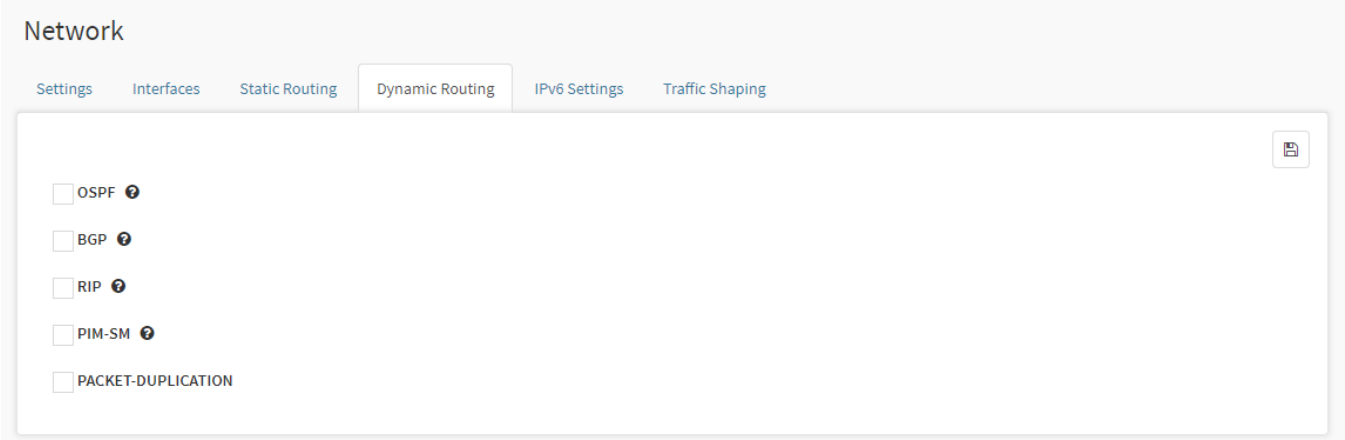
Blockbit NGFW offers dynamic routing with support for protocols:

- **OSPF;**
- **BGP;**
- **RIP;**
- **PIM-SM;**
- **Packet - Duplication.**

Dynamic Routing - Enabling and Configuration

Enable dynamic protocols, based on the characteristics of each protocol and its network structure, its function is to optimize its routing tables, improve the performance of network traffic and the performance of packet handling.

To enable dynamic routing protocols, consider the following information:



Dynamic Routing

- **[ ] *Dynamic Routing - Enabling and Configuration#OSPF*:** By marking the checkbox **[ ]**, OSPF will be enabled. Open Shortest Path First is a protocol that uses LSR (Link State Routing) to perform the routing. Basically the routers communicate and disclose the current state of their link to each other, using this information, a database is created and through it the routers determine and prioritize the shortest path available between themselves and another router;
- **[ ] *BGP*:** By marking the checkbox **[ ]**, BGP will be enabled. The Border Gateway Protocol acts through the determinations configured by a network administrator, manages the routing of packets and directs them between Autonomous Systems (AS). It is one of the standard protocols for external gateway and routing between domains;
- **[ ] *RIP*:** By marking the checkbox [ ], RIP will be enabled. The Routing Information Protocol is a distance vector routing protocol that acts by communicating with the nearest routers and sending information about the distance from the network constantly, through these periodic updates, convergence to a given topology is made;
- **[ ] *Dynamic Routing - Enabling and Configuration#PIM-SM*:** By marking the checkbox [ ], PIM-SM will be enabled. It means Protocol Independent Multicast - Sparse Mode, does not have natively means of discovering topologies and does not create routing tables, however it is able to use information from other routing protocols for this purpose and creates shared multicast traffic trees, being able to use them to define the shortest path by origin. PIM-SM, uses reverse path forwarding (RPF) to communicate with multicast groups and its packages are subdivided as new nodes are introduced to the group, no forwarding is done without request and to find another source of multicast traffic a meeting point in the network (RP - Redezvous Point).
- [ ] ***Packet Duplication***: When checking the check box [ ] the Packet Duplication will be activated. Packet duplication consists in the sending of identical data packets by alternative ways, as to avoid data loss. When a packet is lost, a copy is sent to the server, in replacement.

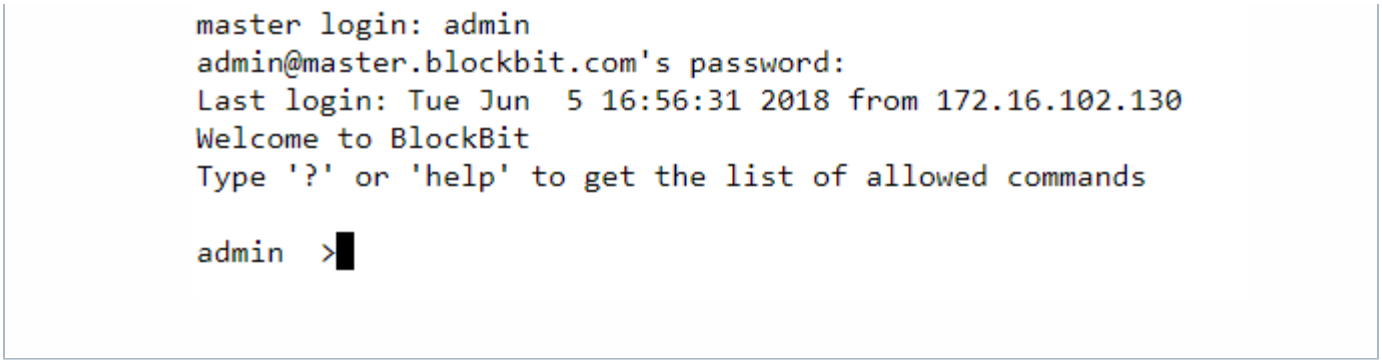
To view configuration **[Examples]**, in the dynamic routing enable interface, click HELP **[ ]** for each protocol respectively.

To configure dynamic routing protocols, access the SSH console through the “Web” interface or through an SSH client. Ex: “Putty”, “MobaXterm”. In the “Web” interface, click on **[*Terminal*]**.

To access the terminal, use the user “admin” and the personalized “password”.

Login: [admin]

Password: [admin]



Here are the examples for each protocol:

[•] *OSPF*

```
Configuration example: OSPF  admin >configure-ospf

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname ngfw-bb
ngfw-bb(config)# router ospf
ngfw-bb(config-router)# network 192.168.10.0/24 area 0
ngfw-bb(config-router)# network 172.16.0.0/24 area 0
ngfw-bb(config-router)# network 192.168.20.0/24 area 0
ngfw-bb(config-router)# exit
ngfw-bb(config)# do wr
ngfw-bb# exit
Connection closed by foreign host
```

[•] *BGP*

```
Configuration example: BGP

admin >configure-bgp

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname ngfw-bb
ngfw-bb(config)# bgp multiple-instance
ngfw-bb(config)# router bgp 180
ngfw-bb(config)# bgp router-id 0.0.0.180
ngfw-bb(config-router)# network 172.16.0.0/24
ngfw-bb(config-router)# timers bgp 1 5
ngfw-bb(config-router)# neighbor 192.168.20.2 remote-as 181
ngfw-bb(config-router)# neighbor 172.15.0.1 remote-as 181
```

```
ngfw-bb(config-router)# do wr
ngfw-bb(config)# exit
Connection closed by foreign host
```

[•] *RIP*

```
Configuration example: RIP

Admin >configure-rip

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname ngfw-bb
ngfw-bb(config)# router rip
ngfw-bb(config-router)# version 2
ngfw-bb(config-router)# network 10.0.0.0/8
ngfw-bb(config-router)# passive-interface eth0
ngfw-bb(config-router)# interface eth0
ngfw-bb(config-if)# no ip rip authentication mode text
ngfw-bb(config-if)# exit
ngfw-bb(config)# do wr
ngfw-bb# exit
Connection closed by foreign host
```

[•] *PIM-SM*

```
Configuration example: PIM

admin >configure-pim

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname ngfw-bb
ngfw-bb(config)# interface eth0
ngfw-bb(config-if)# ip pim ssm
ngfw-bb(config-if)# ip igmp
ngfw-bb(config-if)# interface eth1
ngfw-bb(config-if)# ip pim ssm
ngfw-bb(config-if)# ip igmp
ngfw-bb(config-if)# exit
ngfw-bb(config)# ip multicast-routing
ngfw-bb(config)# do wr
ngfw-bb# exit
Connection closed by foreign host
```

After having finished the settings, click on the [] button and apply to the action queue [].

We will analyze some of the OSPF's properties further, in the following section: OSPF Graceful Restart.

OSPF Graceful Restart

Graceful restart is a function that allows the restart of a router from an OSPF Network by sending TTL packets as “messages” to its adjacent routers, requesting them to enter help mode while it’s off.

Available Configuration:

The following configurations are available under the router ospf/graceful restart node:

Disable disabling the status enable

Enabling the status helper-disable disabling the support helper-enable enabling the support helper-strict-lsa-checking.

Restart helper-strict-lsa-checking option no-strict-lsa-checking.

Disabling helper-strict-lsa-checking option reason.

Restart Reason restart-duration.

Restart interval time.

Graceful Helper mode

The graceful helper mode holds the adjacency of the gracefully restarting neighbour till the grace period expires.

Graceful Restart mode

The gracefully restarting router informs the peers the reason for the graceful restart, the grace period, to the peer using the type 9 opqaue lsas. When the router restarts successfully again it flushes the grace-lsa in a way that the adjacent routers can exit helper mode.

Patch Detail

OSPF Command: **no max-metric router-lsa [on-startup|on-shutdown|administrative]**

This enables RFC3137, OSPF Stub Router Advertisement support, where the OSPF process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach networks through the router.

This support may be enabled administratively (and indefinitely) or conditionally. Conditional enabling of max-metric router-lsas can be for a period of seconds after startup and/or for a period of seconds prior to shutdown.

Enabling this for a period after startup allows OSPF to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable. Enabling this for a period in advance of shutdown allows the router to gracefully excuse itself from the OSPF domain.

Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.

Configured state of this feature as well as current status, such as the number of second remaining till on-startup or on-shutdown ends, can be viewed with the show ip ospf command.

Command: **show ip ospf**

Show information on a variety of general OSPF and area state and configuration information.

Command: **show ip ospf interface [INTERFACE]**

Show state and configuration of OSPF the specified interface, or all interfaces if no interface is given.

Command: **show ip ospf neighbor**

Command: **show ip ospf neighbor INTERFACE**

Command: **show ip ospf neighbor detail**

Command: **show ip ospf neighbor INTERFACE detail**

Command: **show ip ospf database**

Command: **show ip ospf database asbr-summary**

Command: **show ip ospf database external**

Command: **show ip ospf database network**

Command: **show ip ospf database asbr-router**

Command: **show ip ospf database summary**

Command: **show ip ospf database … *link-state-id***

Command: **show ip ospf database … *link-state-id* adv-router *adv-router***

Command: **show ip ospf database … adv-router *adv-router***

Command: **show ip ospf database … *link-state-id* self-originate**

Command: **show ip ospf database … self-originate**

Command: **show ip ospf database max-age**

Command: **show ip ospf database self-originate**

Command: **show ip ospf route**

Show the OSPF routing table, as determined by the most recent SPF calculation.

OSPF Router

To start OSPF process you must specify the OSPF router. As of this writing, ospfd does not support multiple OSPF processes.

Command: **router ospf**

Command: **no router ospf**

Enable or disable the OSPF process. ospfd does not yet support multiple OSPF processes. So, you can not specify an OSPF process number.

OSPF Command: **ospf router-id a.b.c.d**

OSPF Command: **no ospf router-id**

This sets the router-ID of the OSPF process. The router-ID may be an IP address of the router but does not need to be - it can be any arbitrary 32bit number. However, it MUST be unique within the entire OSPF domain to the OSPF speaker - bad things will happen if multiple OSPF speakers are configured with the same router-ID! If one is not specified, then ospfd will obtain a router-ID automatically from zebra.

OSPF Command: **ospf abr-type type**

OSPF Command: **no ospf abr-type type**

type can be cisco|ibm|shortcut|standard. The "Cisco" and "IBM" types are equivalent.

The OSPF standard for ABR behaviour does not allow an ABR to consider routes through non-backbone areas when its links to the backbone are down, even when there are other ABRs in attached non-backbone areas which still can reach the backbone - this restriction exists primarily to ensure routing-loops are avoided.

With the "Cisco" or "IBM" ABR type, the default has been changed, this restriction is lifted, allowing an ABR to consider summaries learnt from other ABRs through non-backbone areas, and hence route via non-backbone areas as a last resort when, and only when, backbone links are down.

Note that areas with fully-adjacent virtual-links are considered to be "transit capable" and can always be used to route backbone traffic, and hence are unaffected by this setting.

Quote: "Though the definition of the ABR (Area Border Router) in the OSPF specification does not require a router with multiple attached areas to have a backbone connection, it is actually necessary to provide successful routing to the inter-area and external destinations. If this requirement is not met, all traffic destined for the areas not connected to such an ABR or out of the OSPF domain, is dropped. This document describes alternative ABR behaviors implemented in Cisco and IBM routers."

OSPF Command: **ospf rfc1583compatibility**

OSPF Command: **no ospf rfc1583compatibility**

RFC2328, the successor to RFC1583, suggests according to section G.2 (changes) in section 16.4 a change to the path preference algorithm that prevents possible routing loops that were possible in the old version of OSPFv2. More specifically it demands that inter-area paths and intra-area backbone path are now of equal preference but still both preferred to external paths.

This command should NOT be set normally.

OSPF Command: **log-adjacency-changes [detail]**

OSPF Command: **no log-adjacency-changes [detail]**

Configures ospfd to log changes in adjacency. With the optional detail argument, all changes in adjacency status are shown. Without detail, only changes to full or regressions are shown.

OSPF Command: **passive-interface interface**

OSPF Command: **no passive-interface interface**

Do not speak OSPF interface on the given interface but do advertise the interface as a stub link in the router-LSA (Link State Advertisement) for this router.

This allows one to advertise addresses on such connected interfaces without having to originate AS-External/Type-5 LSAs (which have global flooding scope) - as would occur if connected addresses were redistributed into OSPF. This is the only way to advertise non-OSPF links into stub areas.

OSPF Command: **timers throttle spf delay initial-holdtime max-holdtime**

OSPF Command: **no timers throttle spf**

This command sets the initial delay, the initial-holdtime and the maximum-holdtime between when SPF is calculated and the event which triggered the calculation. The times are specified in milliseconds and must be in the range of 0 to 600000 milliseconds.

The delay specifies the minimum amount of time to delay SPF calculation (hence it affects how long SPF calculation is delayed after an event which occurs outside of the holdtime of any previous SPF calculation and serves as a minimum holdtime).

Consecutive SPF calculations will always be separated by at least 'hold-time' milliseconds. The hold-time is adaptive and initially is set to the initial-holdtime configured with the above command. Events which occur within the holdtime of the previous SPF calculation will cause the holdtime to be increased by initial-holdtime, bounded by the maximum-holdtime configured with this command. If the adaptive hold-time elapses without any SPF-triggering event occuring then the current holdtime is reset to the initial-holdtime. The current holdtime can be viewed with show ip ospf, where it is expressed as a multiplier of the initial-holdtime.

router ospf timers throttle spf 200 400 10000

In this example, the delay is set to 200ms, the initial holdtime is set to 400ms and the maximum holdtime to 10s. Hence there will always be at least 200ms between an event which requires SPF calculation and the actual SPF calculation. Further consecutive SPF calculations will always be separated by between 400ms to 10s, the hold-time increasing by 400ms each time an SPF-triggering event occurs within the hold-time of the previous SPF calculation.

This command supersedes the timers spf command in previous releases.

OSPF Command: **max-metric router-lsa [on-startup|on-shutdown] <5-86400>**

OSPF Command: **max-metric router-lsa administrative**

OSPF Command: **no max-metric router-lsa [on-startup|on-shutdown|administrative]**

This enables RFC3137, OSPF Stub Router Advertisement support, where the OSPF process describes its transit links in its router-LSA as having infinite distance so that other routers will avoid calculating transit paths through the router while still being able to reach networks through the router.

This support may be enabled administratively (and indefinitely) or conditionally. Conditional enabling of max-metric router-lsas can be for a period of seconds after startup and/or for a period of seconds prior to shutdown.

Enabling this for a period after startup allows OSPF to converge fully first without affecting any existing routes used by other routers, while still allowing any connected stub links and/or redistributed routes to be reachable. Enabling this for a period in advance of shutdown allows the router to gracefully excuse itself from the OSPF domain.

Enabling this feature administratively allows for administrative intervention for whatever reason, for an indefinite period. Note that if the configuration is written to file, this administrative form of the stub-router command will also be written to file. If ospfd is restarted later, the command will then take effect until manually deconfigured.

Configured state of this feature as well as current status, such as the number of second remaining till on-startup or on-shutdown ends, can be viewed with the show ip ospf command.

OSPF Command: **auto-cost reference-bandwidth <1-4294967>**

OSPF Command: **no auto-cost reference-bandwidth**

This sets the reference bandwidth for cost calculations, where this bandwidth is considered equivalent to an OSPF cost of 1, specified in Mbits/s. The default is 100Mbit/s (i.e. a link of bandwidth 100Mbit/s or higher will have a cost of 1. Cost of lower bandwidth links will be scaled with reference to this cost).

This configuration setting MUST be consistent across all routers within the OSPF domain.

OSPF Command: **network a.b.c.d/m area a.b.c.d**

OSPF Command: **network a.b.c.d/m area <0-4294967295>**

OSPF Command: **no network a.b.c.d/m area a.b.c.d**

OSPF Command: **no network a.b.c.d/m area <0-4294967295>**

This command specifies the OSPF enabled interface(s). If the interface has an address from range 192.168.1.0/24 then the command below enables ospf on this interface so router can provide network information to the other ospf routers via this interface.

router ospf network 192.168.1.0/24 area 0.0.0.0

Prefix length in interface must be equal or bigger (ie. smaller network) than prefix length in network statement. For example, statement above doesn't enable ospf on interface with address 192.168.1.1/23, but it does on interface with address 192.168.1.129/25.

Note that the behavior when there is a peer address defined on an interface changed has changed. Currently, if a peer prefix has been configured, then we test whether the prefix in the network command contains the destination prefix. Otherwise, we test whether the network command prefix contains the local address prefix of the interface.

In some cases, it may be more convenient to enable OSPF on a per interface/subnet basis.

OSPF Area

OSPF Command: **area a.b.c.d range a.b.c.d/m**

OSPF Command: **area <0-4294967295> range a.b.c.d/m**

OSPF Command: **no area a.b.c.d range a.b.c.d/m**

OSPF Command: **no area <0-4294967295> range a.b.c.d/m**

Summarize intra area paths from specified area into one Type-3 summary-LSA announced to other areas. This command can be used only in ABR and ONLY router-LSAs (Type-1) and network-LSAs (Type-2) (ie. LSAs with scope area) can be summarized. Type-5 AS-external-LSAs can't be summarized - their scope is AS. Summarizing Type-7 AS-external-LSAs isn't supported yet by Blockbit.

router ospf network 192.168.1.0/24 area 0.0.0.0 network 10.0.0.0/8 area 0.0.0.10 area 0.0.0.10 range 10.0.0.0/8

With configuration above one Type-3 Summary-LSA with routing info 10.0.0.0/8 is announced into backbone area if area 0.0.0.10 contains at least one intra-area network (ie. described with router or network LSA) from this range.

OSPF Command: **area a.b.c.d range IPV4_PREFIX not-advertise**

OSPF Command: **no area a.b.c.d range IPV4_PREFIX not-advertise**

Instead of summarizing intra area paths filter them - ie. intra area paths from this range are not advertised into other areas. This command makes sense in ABR only.

OSPF Command: **area a.b.c.d range IPV4_PREFIX substitute IPV4_PREFIX**

OSPF Command: **no area a.b.c.d range IPV4_PREFIX substitute IPV4_PREFIX**

Substitute summarized prefix with another prefix.

router ospf network 192.168.1.0/24 area 0.0.0.0 network 10.0.0.0/8 area 0.0.0.10 area 0.0.0.10 range 10.0.0.0/8 substitute 11.0.0.0/8

One Type-3 summary-LSA with routing info 11.0.0.0/8 is announced into backbone area if area 0.0.0.10 contains at least one intra-area network (ie. described with router-LSA or network-LSA) from range 10.0.0.0/8. This command makes sense in ABR only.

OSPF Command: **area a.b.c.d virtual-link a.b.c.d**

OSPF Command: **area <0-4294967295> virtual-link a.b.c.d**

OSPF Command: **no area a.b.c.d virtual-link a.b.c.d**

OSPF Command: **no area <0-4294967295> virtual-link a.b.c.d**

OSPF Command: **area a.b.c.d shortcut**

OSPF Command: **area <0-4294967295> shortcut**

OSPF Command: **no area a.b.c.d shortcut**

OSPF Command: **no area <0-4294967295> shortcut**

Configure the area as Shortcut capable. See RFC3509. This requires that the 'abr-type' be set to 'shortcut'.

OSPF Command: **area a.b.c.d stub**

OSPF Command: **area <0-4294967295> stub**

OSPF Command: **no area a.b.c.d stub**

OSPF Command: **no area <0-4294967295> stub**

Configure the area to be a stub area. That is, an area where no router originates routes external to OSPF and hence an area where all external routes are via the ABR(s). Hence, ABRs for such an area do not need to pass AS-External LSAs (type-5s) or ASBR-Summary LSAs (type-4) into the area. They need only pass Network-Summary (type-3) LSAs into such an area, along with a default-route summary.

OSPF Command: **area a.b.c.d stub no-summary**

OSPF Command: **area <0-4294967295> stub no-summary**

OSPF Command: **no area a.b.c.d stub no-summary**

OSPF Command: **no area <0-4294967295> stub no-summary**

Prevents an ospfd ABR from injecting inter-area summaries into the specified stub area.

OSPF Command: **area a.b.c.d default-cost <0-16777215>**

OSPF Command: **no area a.b.c.d default-cost <0-16777215>**

Set the cost of default-summary LSAs announced to stubby areas.

OSPF Command: **area a.b.c.d export-list NAME**

OSPF Command: **area <0-4294967295> export-list NAME**

OSPF Command: **no area a.b.c.d export-list NAME**

OSPF Command: **no area <0-4294967295> export-list NAME**

Filter Type-3 summary-LSAs announced to other areas originated from intra- area paths from specified area.

router ospf network 192.168.1.0/24 area 0.0.0.0 network 10.0.0.0/8 area 0.0.0.10 area 0.0.0.10 export-list foo!access-list foo permit 10.10.0.0/16access-list foo deny any

With example above any intra-area paths from area 0.0.0.10 and from range 10.10.0.0/16 (for example 10.10.1.0/24 and 10.10.2.128/30) are announced into other areas as Type-3 summary-LSA’s, but any others (for example 10.11.0.0/16 or 10.128.30.16/30) aren’t.

This command is only relevant if the router is an ABR for the specified area.

OSPF Command: **area a.b.c.d import-list NAME**

OSPF Command: **area <0-4294967295> import-list NAME**

OSPF Command: **no area a.b.c.d import-list NAME**

OSPF Command: **no area <0-4294967295> import-list NAME**

Same as export-list, but it applies to paths announced into specified area as Type-3 summary-LSAs.

OSPF Command: **area a.b.c.d filter-list prefix NAME in**

OSPF Command: **area a.b.c.d filter-list prefix NAME out**

OSPF Command: **area <0-4294967295> filter-list prefix NAME in**

OSPF Command: **area <0-4294967295> filter-list prefix NAME out**

OSPF Command: **no area a.b.c.d filter-list prefix NAME in**

OSPF Command: **no area a.b.c.d filter-list prefix NAME out**

OSPF Command: **no area <0-4294967295> filter-list prefix NAME in**

OSPF Command: **no area <0-4294967295> filter-list prefix NAME out**

Filtering Type-3 summary-LSAs to/from area using prefix lists. This command makes sense in ABR only.

OSPF Command: **area a.b.c.d authentication**

OSPF Command: **area <0-4294967295> authentication**

OSPF Command: **no area a.b.c.d authentication**

OSPF Command: **no area <0-4294967295> authentication**

Specify that simple password authentication should be used for the given area.

OSPF Command: **area a.b.c.d authentication message-digest**

OSPF Command: **area <0-4294967295> authentication message-digest**

Specify that OSPF packets must be authenticated with MD5 HMACs within the given area. Keying material must also be configured on a per-interface basis.

MD5 authentication may also be configured on a per-interface basis. Such per-interface settings will override any per-area authentication setting.

OSPF Interface

Interface Command: **ip ospf area AREA [ADDR]**

Interface Command: **no ip ospf area [ADDR]**

Enable OSPF on the interface, optionally restricted to just the IP address given by ADDR, putting it in the AREA area. Per interface area settings take precedence to network commands.

If you have a lot of interfaces, and/or a lot of subnets, then enabling OSPF via this command may result in a slight performance improvement.

Interface Command: **ip ospf authentication-key AUTH_KEY**

Interface Command: **no ip ospf authentication-key**

Set OSPF authentication key to a simple password. After setting AUTH_KEY, all OSPF packets are authenticated. AUTH_KEY has length up to 8 chars.

Simple text password authentication is insecure and deprecated in favour of MD5 HMAC authentication.

Interface Command: **ip ospf authentication message-digest**

Specify that MD5 HMAC authentication must be used on this interface. MD5 keying material must also be configured. Overrides any authentication enabled on a per-area basis.

Note that OSPF MD5 authentication requires that time never go backwards (correct time is NOT important, only that it never goes backwards), even across resets, if ospfd is to be able to promptly re-establish adjacencies with its neighbours after restarts/reboots. The host should have system time be set at boot from an external or non-volatile source (eg battery backed clock, NTP, etc.) or else the system clock should be periodically saved to non-volative storage and restored at boot if MD5 authentication is to be expected to work reliably.

Interface Command: **ip ospf message-digest-key KEYID md5 KEY**

Interface Command: **no ip ospf message-digest-key**

Set OSPF authentication key to a cryptographic password. The cryptographic algorithm is MD5.

KEYID identifies secret key used to create the message digest. This ID is part of the protocol and must be consistent across routers on a link.

KEY is the actual message digest key, of up to 16 chars (larger strings will be truncated) and is associated with the given KEYID.

Interface Command: **ip ospf cost <1-65535>**

Interface Command: **no ip ospf cost**

Set link cost for the specified interface. The cost value is set to router-LSA’s metric field and used for SPF calculation.

Interface Command: **ip ospf dead-interval <1-65535>**

Interface Command: **ip ospf dead-interval minimal hello-multiplier <2-20>**

Interface Command: **no ip ospf dead-interval**

Set number of seconds for RouterDeadInterval timer value used for Wait Timer and Inactivity Timer. This value must be the same for all routers attached to a common network. The default value is 40 seconds.

If ’minimal’ is specified instead, then the dead-interval is set to 1 second and one must specify a hello-multiplier. The hello-multiplier specifies how many Hellos to send per second, from 2 (every 500ms) to 20 (every 50ms). Thus, one can have 1s convergence time for OSPF. If this form is specified, then the hello-interval advertised in Hello packets is set to 0 and the hello-interval on received Hello packets is not checked, thus the hello-multiplier need NOT be the same across multiple routers on a common link.

Interface Command: **ip ospf hello-interval <1-65535>**

Interface Command: **no ip ospf hello-interval**

Set number of seconds for HelloInterval timer value. Setting this value, Hello packet will be sent every timer value seconds on the specified interface. This value must be the same for all routers attached to a common network. The default value is 10 seconds.

This command has no effect if ip ospf dead-interval minimal is also specified for the interface.

Interface Command: **ip ospf network (broadcast|non-broadcast|point-to-multipoint|point-to-point)**

Interface Command: **no ip ospf network**

Set explicitly network type for specified interface.

Interface Command: **ip ospf priority <0-255>**

Interface Command: **no ip ospf priority**

Set RouterPriority integer value. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0, makes the router ineligible to become Designated Router. The default value is 1.

Interface Command: **ip ospf retransmit-interval <1-65535>**

Interface Command: **no ip ospf retransmit interval**

Set number of seconds for RxmtInterval timer value. This value is used when retransmitting Database Description and Link State Request packets. The default value is 5 seconds.

Interface Command: **ip ospf transmit-delay**

Interface Command: **no ip ospf transmit-delay**

Set number of seconds for InfTransDelay value. LSAs' age should be incremented by this value when transmitting. The default value is 1 seconds.

Redistribute Routes to OSPF

OSPF Command: **redistribute (kernel|connected|static|rip|bgp)**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) route-map**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric-type (1|2)**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric-type (1|2) route-map word**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric <0-16777214>**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric <0-16777214> route-map word**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric-type (1|2) metric <0-16777214>**

OSPF Command: **redistribute (kernel|connected|static|rip|bgp) metric-type (1|2) metric <0-16777214> route-map word**

OSPF Command: **no redistribute (kernel|connected|static|rip|bgp)**

Redistribute routes of the specified protocol or kind into OSPF, with the metric type and metric set if specified, filtering the routes using the given route-map if specified. Redistributed routes may also be filtered with distribute-lists.

Redistributed routes are distributed as into OSPF as Type-5 External LSAs into links to areas that accept external routes, Type-7 External LSAs for NSSA areas and are not redistributed at all into Stub areas, where external routes are not permitted.

Note that for connected routes, one may instead use *passive-interface*.

OSPF Command: **default-information originate**

OSPF Command: **default-information originate metric <0-16777214>**

OSPF Command: **default-information originate metric <0-16777214> metric-type (1|2)**

OSPF Command: **default-information originate metric <0-16777214> metric-type (1|2) route-map word**

OSPF Command: **default-information originate always**

OSPF Command: **default-information originate always metric <0-16777214>**

OSPF Command: **default-information originate always metric <0-16777214> metric-type (1|2)**

OSPF Command: **default-information originate always metric <0-16777214> metric-type (1|2) route-map word**

OSPF Command: **no default-information originate**

Originate an AS-External (type-5) LSA describing a default route into all external-routing capable areas, of the specified metric and metric type. If the ' always' keyword is given then the default is always advertised, even when there is no default present in the routing table.

OSPF Command: **distribute-list NAME out (kernel|connected|static|rip|ospf**

OSPF Command: **no distribute-list NAME out (kernel|connected|static|rip|ospf**

Apply the access-list filter, NAME, to redistributed routes of the given type before allowing the routes to redistributed into OSPF.

OSPF Command: **default-metric <0-16777214>**

OSPF Command: **no default-metric**

OSPF Command: **distance <1-255>**

OSPF Command: **no distance <1-255>**

OSPF Command: **distance ospf (intra-area|inter-area|external) <1-255>**

OSPF Command: **no distance ospf**

Network - IPv6 Settings

The IPv6 address is 128 bits long, being separated into 8 groups of 4 hexadecimal characters. In addition, IPv6 is logically divided into two 64-bit parts, the first for the network prefix and the second for interface identification.

An IPv6 address can be of three specific types:

- ***Unicast:*** For a single device, packet traffic occurs via the shortest route to the device;
- ***Multicast:*** Refers to a grouping of devices, when the data packet is sent to the recipient, each member of the group receives a copy of the packet;
- ***Anycast:*** Refers to a grouping of devices that have the same prefix, the data packet is only delivered to the nearest sender.

One of the main differences between IPv6 and IPv4 is the multiple extension headers, generating greater efficiency thanks to the possibility to adjust their size, in addition to being able to add new headers in order to meet new needs. There are six types of predefined extension header, they are:

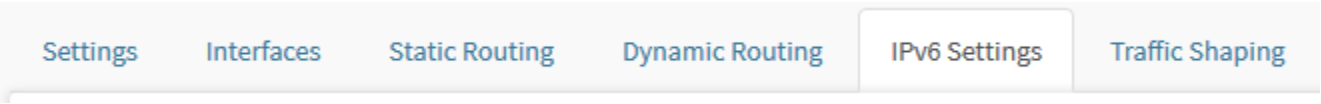
- *Hop-by-hop*;
- *Destination Options*;
- *Routing*;
- *Fragmentation*;
- *Authentication*;
- *Encrypted security payload*.

A host generally has two types of IPv6 unicast: the Local Link Address and the Global Unicast Address. A global address can be obtained using the following auto-configuration methods:

- ***SLAAC*:** It means Stateless Address Auto Configuration, through this method the host uses the *Router Advertising* prefix to generate two Unicast Global Addresses*. In this method the interface ID is unique on the local network thanks to the use of the MAC address or a random value*;
- ***Stateless DHCPv6*:** Through this method, the host uses the Router Advertising prefix to generate two Global Unicast Addresses and uses any available DHCPv6 server to obtain information relevant to the configuration, for example DNS, Gateway and NTP;
- ***Stateful DHCPv6*:** In this method, the host is unable to obtain the prefix through *Router Advertising*, in order to mitigate this, a broadcast is made requesting the Global Unicast Address and any other necessary configuration of an available DHCPv6 server;
- **Stateful DHCPv6 and SLAAC combined:** In this alternative, simply apply the first and penultimate method simultaneously.

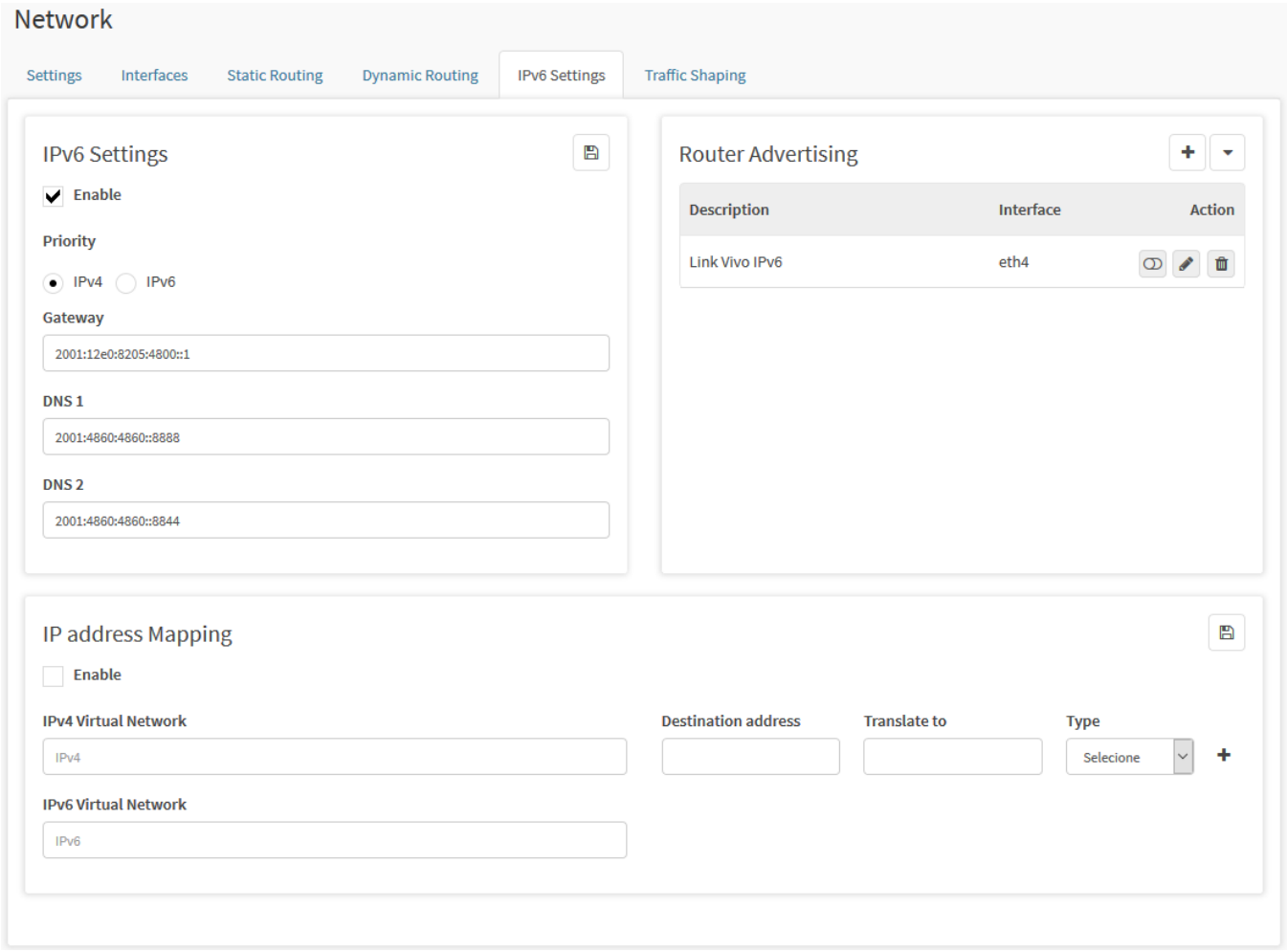
In the system, it is possible to enable and configure IPv6, define how *Router Advertising* will be carried out and perform the conversion from IPv4 to IPv6 through IP mapping.

To make these settings, click on the IPv6 Settings tab, as shown below:



IPv6 Settings tab

The following screen will appear:



IPv6 Settings

This screen consists of the following panels:

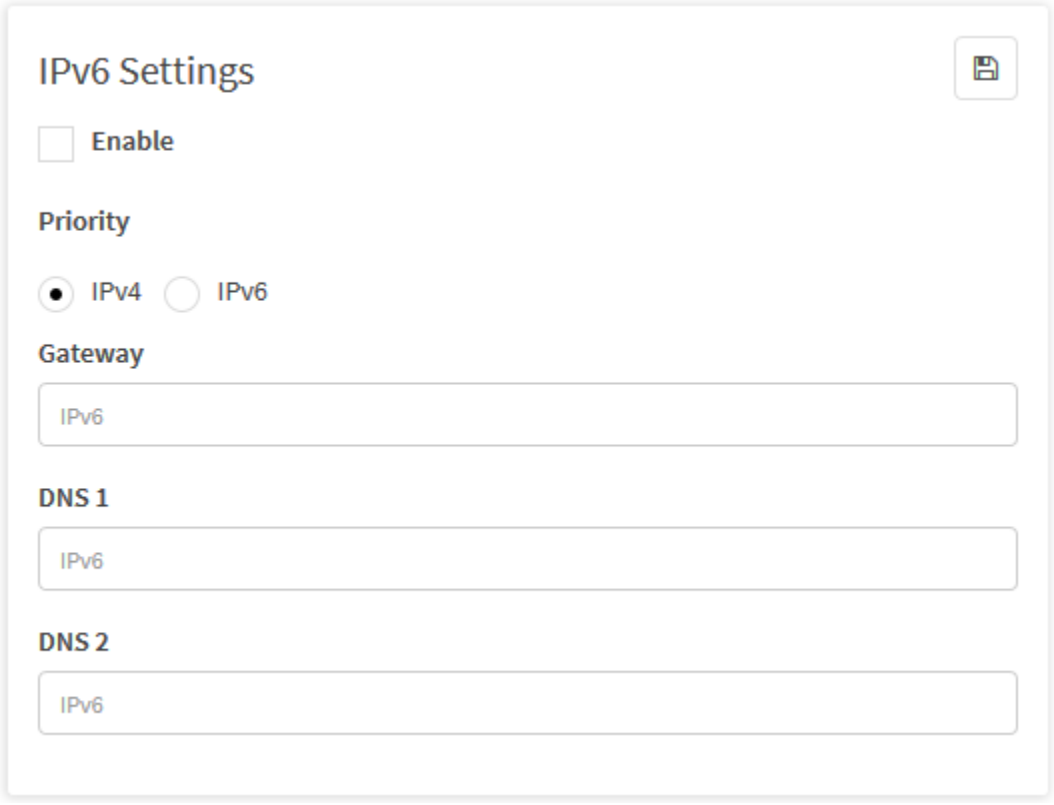
- *IPv6 Settings*;
- *Router Advertising*;
- *IP address Mapping*.

Next, we will analyze each panel in detail.

IPv6 Settings - IPv6 Settings

In this panel are shown general IPv6 settings done on the system.

To do so, complete the fields in this panel:



IPv6 Settings - IPv6 Settings

- ***Enable*[ ]:** If this checkbox is enabled, IPv6 will be enabled;
- ***Priority*:** Determines which type of IP will have priority, the possible options are:
  - ***IPv4*[ ]:** If the checkbox is checked, IPv4 will be selected as a priority;
  - ***IPv6*[ ]:** If the checkbox is checked, IPv6 will be selected as a priority.
- ***Gateway*:** Defines which gateway will be used. *Ex.*: 3178:bbe5:4c9f:7b6f:aecb:6f91:7d06:547d;
- ***DNS1*:** Defines the primary DNS to be used. *Ex.*: 35fb:8841:9b40:af9e:1daa:deee:ad45:f17f;
- ***DNS2*:** Defines the secondary DNS to be used. *Ex.*: f7ee:c742:3864:863e:bd59:85e7:ec38:b0c6.

When finished configuring click on **[ ]** to save the changes.

IPv6 Settings - Router Advertising

Router Advertising is a process where a device sends a request to immediately obtain the settings arranged on the router, for example: routes, hop limit and MTU. During this process, the router broadcasts this data to all nodes in the link and this request acts so that the router quickly responds to the device from which it originated.

The following is an example of the composition of the Router Advertising data package:

- *Source address*;
- *Destination address*;
- *ICMP type*;
- *Hop limit*;
- *Prefix length*;
- *Prefix.*

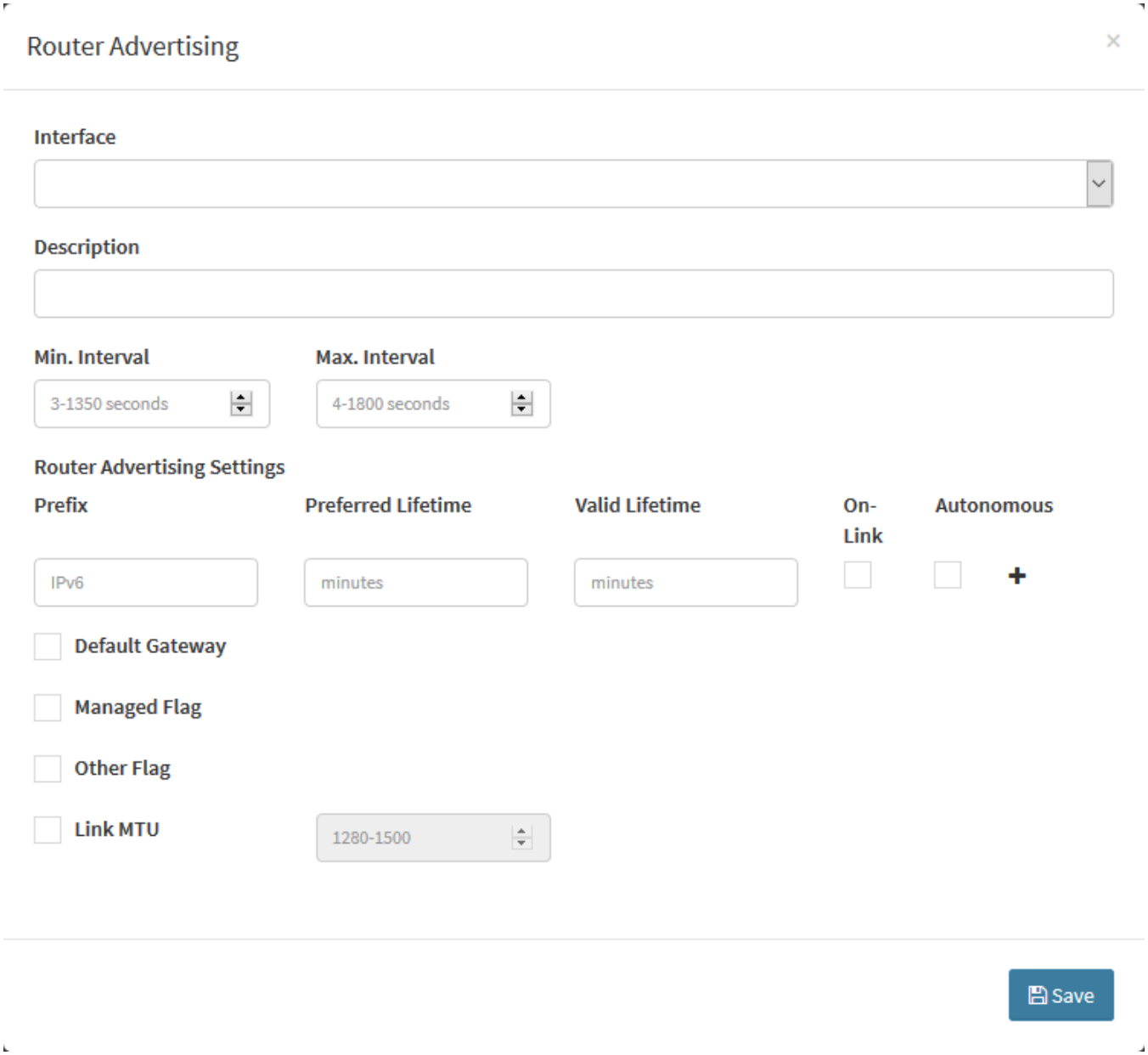
In Router Advertising there are 4 flags whose function is to determine the automatic configuration method applied to the addresses, these are:

- ***M***: It refers to the configuration of the managed address, in this case the host will obtain its IP address from the DHCPv6 server;
- ***O***: Regarding other configurations, the host obtains other configurations (DNS, Gateway, NTP, etc.) from the DHCPv6 server;
- ***A***: Refers to the Standalone Address Configuration, determines whether the autoconfiguration should be processed for the entered prefix;
- ***L***: Refers to the On-Link feature, it is used to determine if the addresses of this prefix can be accessed without needing a router.

Through the combinations of these options it is possible to configure which self-configuration method will be used by the host.

For more information on the autoconfiguration method, check this page.

Next, we'll look at how to configure Router Advertising settings at UTM. To do so, complete the fields in this panel, as shown below:



IPv6 Settings - Router Advertising

- ***Interface*:** In this checkbox, the interface that will be used to perform the Router Advertising is determined, the interfaces that are shown in this list must have been configured with IPv6;

For more information on adding IPv6 interfaces check this page.

- ***Description:*** This field defines the description that the Router Advertising will have;
- ***Min. Interval*:** Sets the minimum interval in seconds for the router to broadcast the Router Advertising;
- ***Max. Interval*:** Sets the maximum interval in seconds for the router to broadcast the Router Advertising;
- ***Prefix*:** Determines the IPv6 prefix (the network address);
- ***Preferred Lifetime*:** Determines the time interval in minutes at which the specified prefix is advertised by the router advertising as preferred;
- ***Valid Lifetime*:** Defines the time interval in minutes for which the specified prefix is advertised by the router advertising as valid;
- ***On-Link* [ ]:** By checking this checkbox, it indicates whether the addresses of this prefix can be reached on that link without having to go through a router. It is equivalent to the L flag, mentioned above;
- ***Autonomous* [ ]:** By checking this checkbox, it allows the automatic address configuration to use the prefix specified in the automatic configuration of IPv6 addresses for hosts on the local link. It is the equivalent of flag A, mentioned above;
- ***Default Gateway* [ ]:** When enabling this field, it is determined that the default Gateway defined in IPv6 settings will be used;

- ***Managed Flag* [ ]:** If this check box is enabled, the host will obtain its IP address from the DHCPv6 server. It is the equivalent of the M flag, mentioned above;
- ***Other Flag* [ ]:** If this check box is enabled, the host will obtain other settings (for example: DNS) from the DHCPv6 server. It is the equivalent of the O flag, mentioned above;
- ***Link MTU* [ ]:** This field determines the Maximum Transmission Unit of the Link, which can be from 1280 to 1500.

When finished configuring click on **[** 

] to save the changes.

IPv6 Settings - IP address Mapping

This panel has the function of enabling and configuring how the conversion from IPv4 to IPv6 will be carried out through IP mapping.

Through the conversion of packets, it is possible to communicate between devices that use IPv6 and equipment that use IPv4.

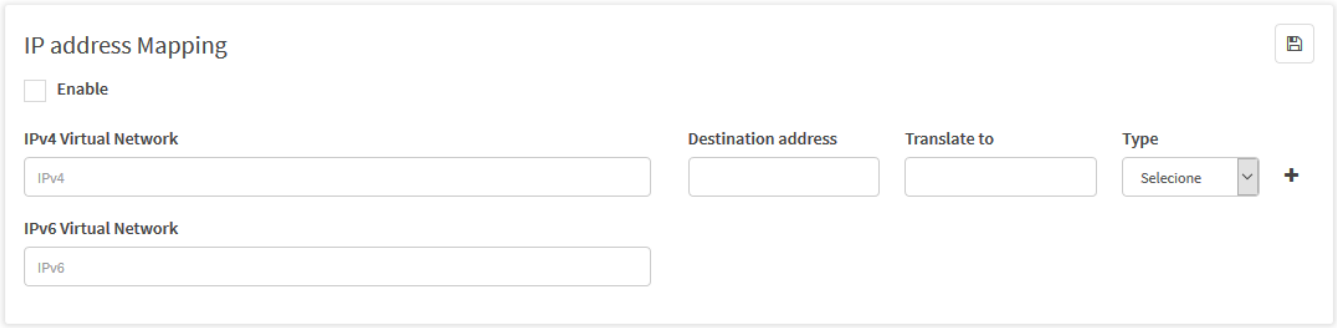
Here are some considerations regarding the functionality of IP conversion methods:

***Dual Stack*:** This method considers that IPv6 and IPv4 will be used natively together on the same device.

Tunnels: Through tunneling, it is possible to communicate between IPv4 and IPv6 networks or vice versa.

- ***6over4*:** It means "IPv6-over-Ipv4", this technique encapsulates the IPv6 packet in an IPv4 packet by adjusting the source / destination header and addresses according to IPv4 standards;
- ***GRE*:** The Generic Routing Encapsulation (RFC 2784) technique creates a static tunnel between two nodes and serves to encapsulate various types of protocol;
- ***NAT64* e *DNS64*:** This technique applies specifically when IPv6 nodes access the internet, the use of DNS64 (RFC 6147) to perform DNS conversion is inevitable.

Below we will analyze how to configure the IP mapping to convert IPv4 addresses to IPv6 and vice versa:



IPv6 Settings - IP address Mapping

- ***Enable*[ ]:** When you enable this check box, the mapping is activated;
- ***IPv4 Virtual Network*:** In this field, IPv4 of the virtual network is added;
- ***Destination address*:** The destination IP address. Depending on the type of transcription that will be done, it determines the type of IP to be added in this field. If it is NAT64, add IPv6, if it is NAT46, add IPv4;
- ***Translate to*:** The IP address that will be translated. Depending on the type of transcription that will be done, it determines the type of IP to be added in this field. If it is NAT64, add IPv4, if it is NAT46, add IPv6;
- ***Type*:** Determines the transcription mechanism that will be used for the network conversion, the possible types are:
  - ***NAT46***;
  - ***NAT64***.
- Click **[ ]** to add additional addresses, or click **[ ]** to remove an address already added.
- ***IPv6 Virtual Network*:** In this field, IPv6 of the virtual network is added.

Click the **[ ]** button to save the settings.

Network - Traffic Shaping

Here we have band management and traffic control, the integration of this service is fundamental in the treatment and prioritization of network services. It has the purpose of allowing and specializing networks in order to significantly improve connection quality.

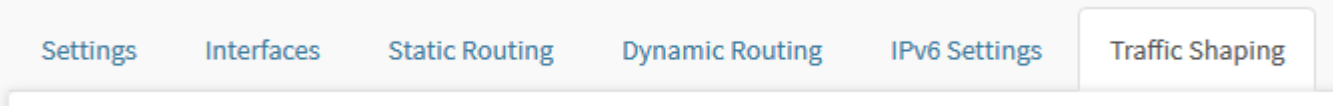
Traffic Shaping Specifications and Features:

- Priority queue control;
- Maximum speed control and guaranteed speed amount per priority level (configurable item);
- Enabling speed control allowing specifying the bandwidth or downstream (download) and upstream (upload) speed of each interface.

The service is pre-configured with 5 (five) priority levels defined by the system:

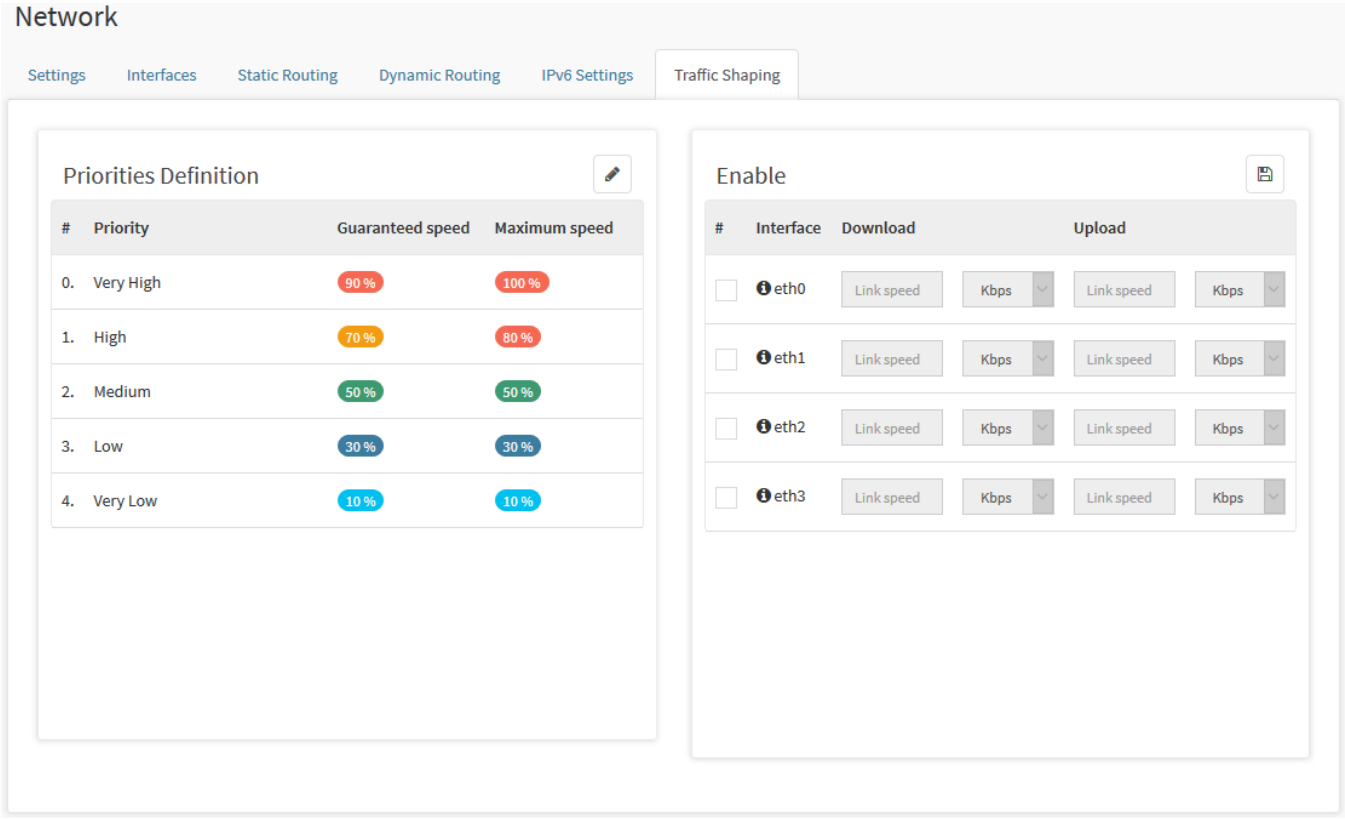
- Very High;
- High;
- Medium;
- Low;
- Very Low.

For enabling and configuring access the Dynamic Routing tab.



Traffic Shaping tab

The screen shown by the image below will appear:



Traffic Shaping

This section will cover:

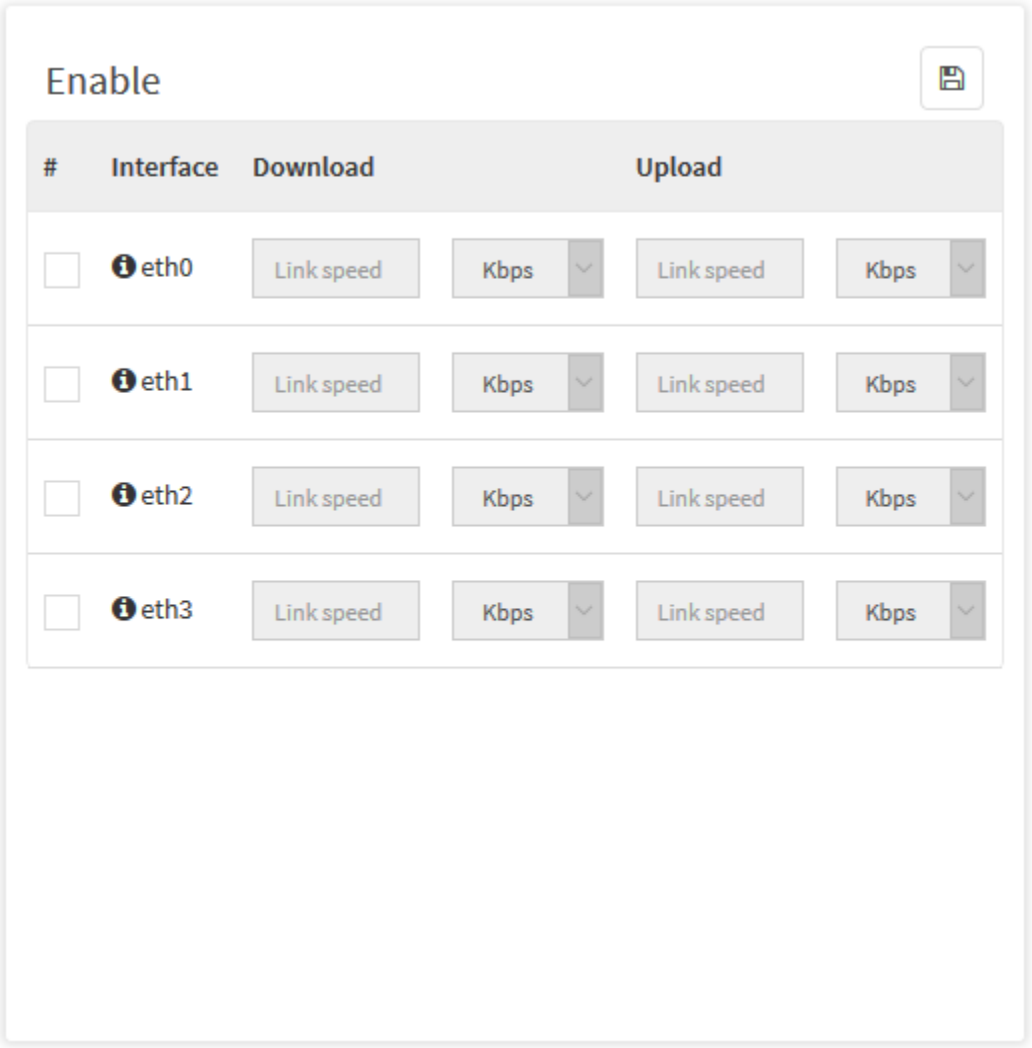
- Setting priorities;
- Download and Upload speed setting;

Next, we will analyze the panels on this screen.

Traffic Shaping - Download and Upload Speed

In the **[Enable]** table, the download and upload speeds specified by the operator of each link are defined, respectively.

This information is used as a basis for applying the “% -percentual” control of each priority level defined in the system.



Traffic Shaping - Enable

Select the network interfaces and parameterize the Download and Upload speeds respectively, according to the link specifications of each operator.

- **Checkbox[ ]**: Enables any of the interfaces for editing;
- **Interface:** It determines the name of the interface, moreover, when hovering over the info icon **[ ]** the description of the interface will be displayed in a drop-down menu;
- **Download:** Defines the speed of the download link in the text box and the unit that will be used in the drop-down list just ahead, the available options are: Kbps, Mbps and Gbps;
- **Upload:** Defines the speed of the upload link in the text box and the unit that will be used in the drop-down list just ahead, the available options are: Kbps, Mbps and Gbps.

The QoS action "Bandwidth control" is applied as "Control filters" in "Security policies".

When finishing the settings click on the [] button and apply to the action queue [].

Next, we'll look at an example of how to do this setup.

Traffic Shaping - Download and Upload Speed - DSL and IP Link Example

Here is an example of how to set the Download and Upload speed:

DSL Link

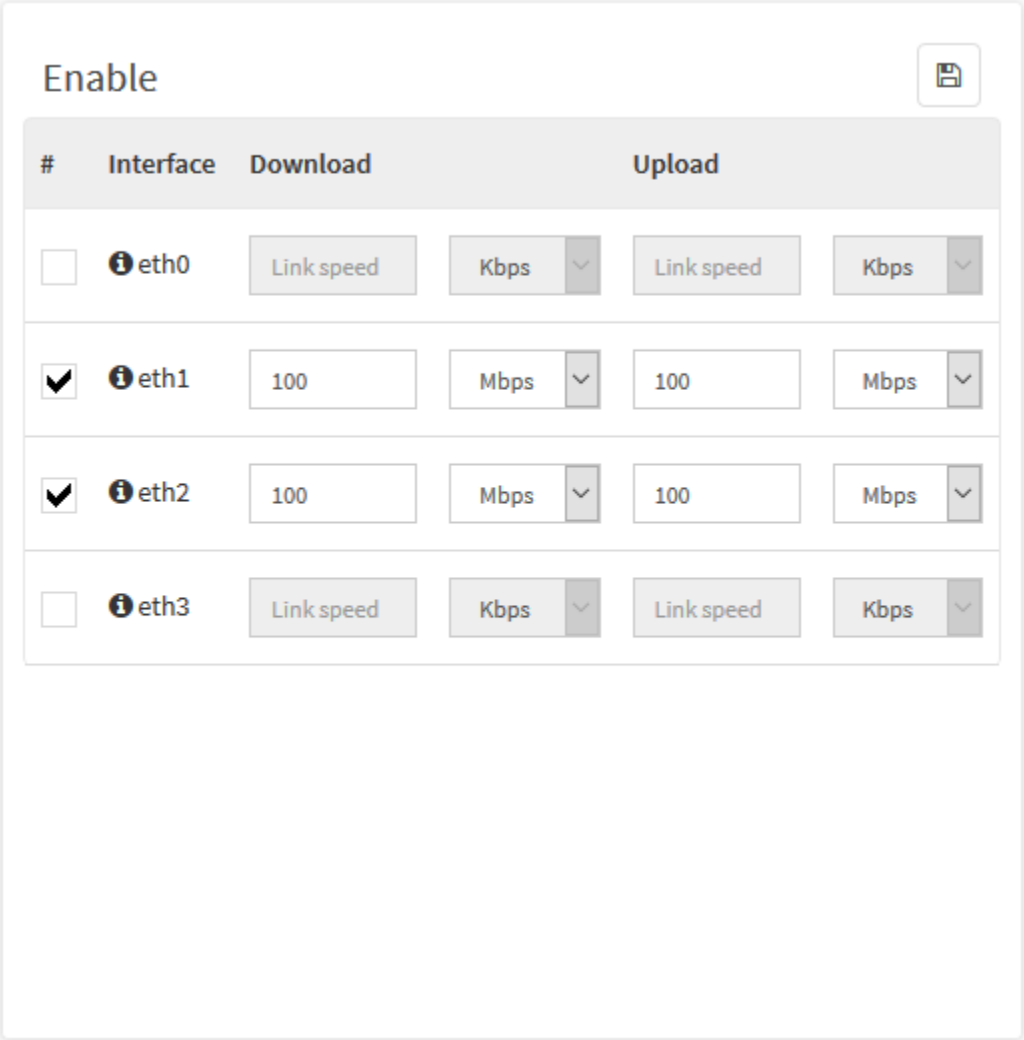
Eth1 interface link:

- 100 Mbps - [*Download*];
- 100 Mbps - [*Upload*].

IP Link

Eth2 interface link:

- 100 Mbps - [*Download*];
- 100 Mbps - [*Upload*].



Traffic Shaping - Enable - Edited

The QoS action "Bandwidth control" is applied as "Control filters" in "Security policies".

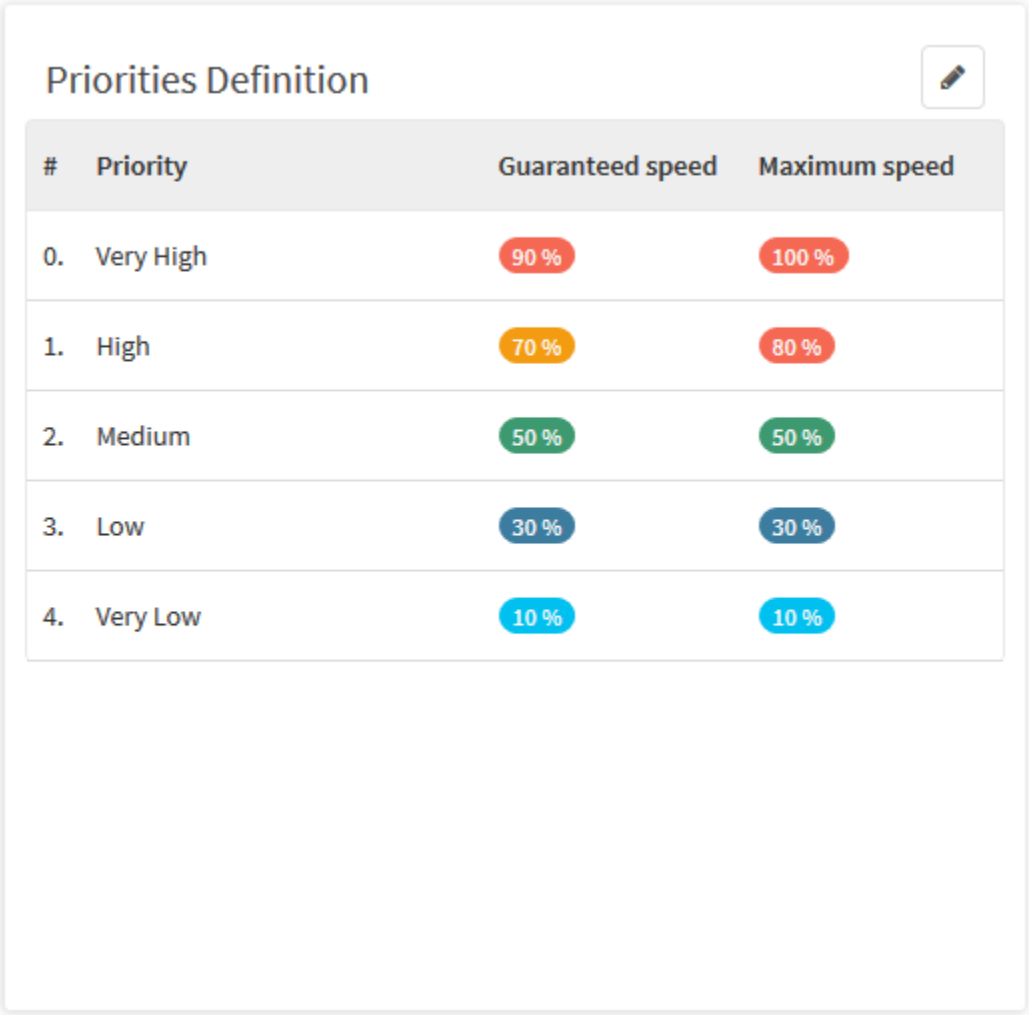
When finishing the settings click on the **[**  **]** button and apply to the action queue **[**  **].**

Traffic Shaping - Priorities Definition

Next, we will analyze the Traffic Shaping panels:

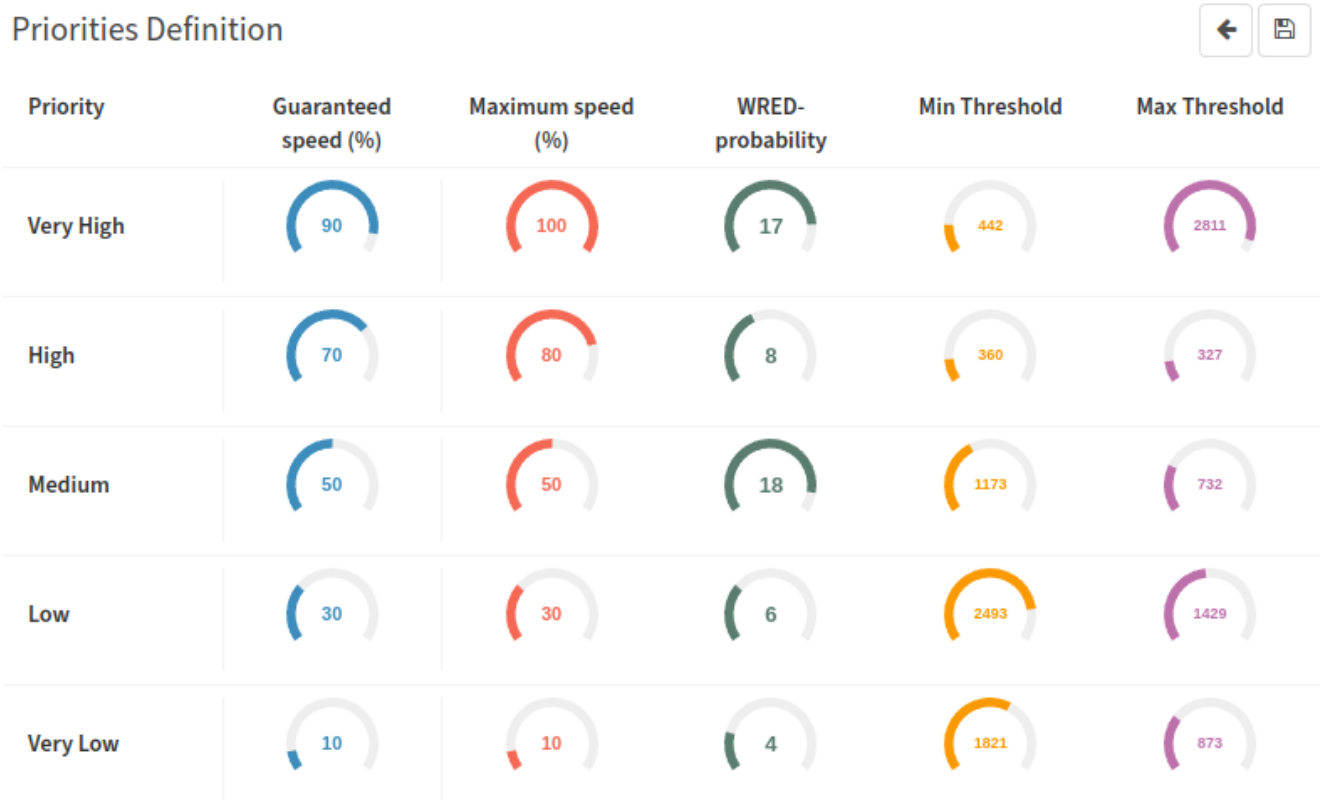
Priorities Definition

The **[*Priorities Definition*]** table has the function of determining the maximum and guaranteed speed of Traffic Shaping.



Traffic Shaping - Priorities Definition

The administrator has the option to redefine the (%) percentages of each priority level “Traffic Shaping” according to the standards and policies of quality of service adopted. To do so, click the Edit **[ ]** button, the following screen will be displayed:



Traffic Shaping - Priorities Definition - Edit

To edit the percentage of priorities, select any of the values and type a new number or click and drag the bar on the graph until you reach the desired result:

Priorities Definition - Edited

Guaranteed speed (%): Percentage of guaranteed band;

Maximum speed (%): Max percentage of avaliable bandl;

WRED-probability: WRED (WeightedRandom Early Drop) allowed band: 0 - 20. Default: 0, without package drop.

Min Threshold: Defines the smallest package queue before WRED acts. Allowed band: 3 - 3000. Default: 100. Default 100;

Max Threshold: Defines the largest package queue before WRED acts. Allowed band: 3 - 3000. Default: 100. Default 100;

Ex.:

Define WRED-probability as 5 means discarding packages when the queue reach "**Min Threshold**" . When the queue reaches "**Max Threshold**", it discards 5% of packages.

Observations:

1. If the queue is below "**Min Threshold",** 0% of packages are discarded.
2. If the queue reaches "**Min Threshold",** it starts discarding packages.
3. If the queue is between "**Min Threshold**" and "**Max Threshold**", it discards proportionally between 0 and 5% of packages.
4. If the mean size of queue is over "**Max Threshold",** 100% of packages will be discarded.

To cancel the changes, click **[** **]** otherwise, when finishing the settings click the **[** **]** button and apply in the action queue **[** **]**.

Next we will analyze the content of the *Enable* panel.

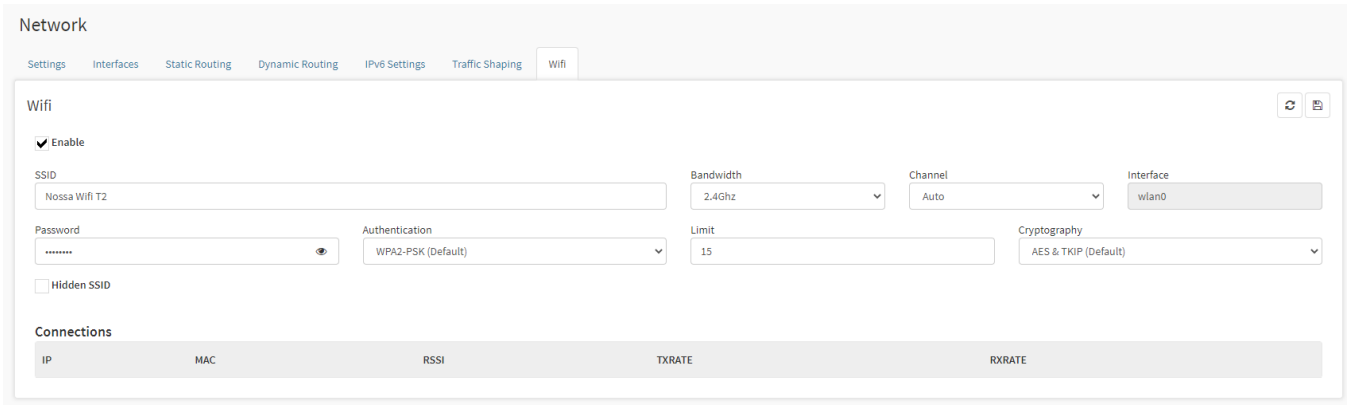
Network - WiFi

In this section we will analyze the wireless network settings (*WiFi*).

It's important to remember that, these options **are only available for physical appliances with the module installed.** In case a virtual appliance is been used, the options on this tab will be faded.

Screen displayed when selecting the *WiFi tab on virtual appliances*

First, we must configure our connection with the required information:



WiFi Settings, now accessed from a physical appliance

- ***Enable:*** Enables/disables the wireless connection (WiFi). This option turns on/shuts down the wireless connection.
- ***SSID:*** Name of the wireless network (*WiFi).* This is where the network's name will be configured by the user.
- ***Bandwidth:*** Choose between 2.4Ghz or 5Ghz. The band capacity determines the connection speed in Ghz. To use it with *5Ghz* make sure of the equipment's compatibility.
- ***Channel:*** The options are Auto, and between 1-32. The number of channels to be made available in the chosen frequency. In "auto" the connection will adapt to the number of channels requested, limited to 32. However it's possible to limit this number, by choosing a limit (1-32).
- ***Interface:*** Sets up the network interface. Up to four interfaces can be set up and used. Select between: *wlan0*, *wlan1*, *wlan2* and *wlan3*.
- ***Password:*** Security password to be used in the WiFi login. Click on the [] button to display the password.
- ***Authentication:*** When disabling the authentication by selecting the "Disabled" option it won't be necessary to use the validation options (Login and Password) to log in to the WiFi network. The other options are WEP *(Wired Equivalent Privacy)*, *WPA-PSK* and *WPA2-PSK (WiFi Protected Access - Pre Shared Key)* the later being set as standard.
- ***Limit:*** Choose the limit number of users that can be logged in simmultaneously.

- ***Cryptography:*** Choose between the following cryptography modes: *AES (Advanced Encryption Standard)*, *TKIP (Temporal Key Integrity Protocol)* or *AES & TKIP,* this last option being set as standard.
- ***Hide SSID:*** Checkbox to hide/display the *SSID*.

UTM - Settings - Authentication

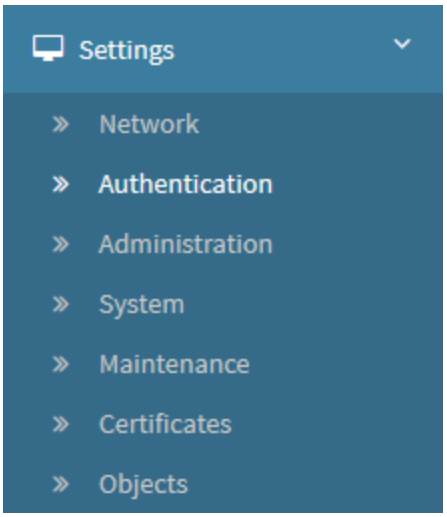
The Blockbit NGFW authentication service is responsible for recognizing users and validating their identification, creating usage sessions, authorizing masked and web access, these being defined in security policies.

The system was developed and prepared to manage the authentication of local and integrated users.

In this session we will analyze:

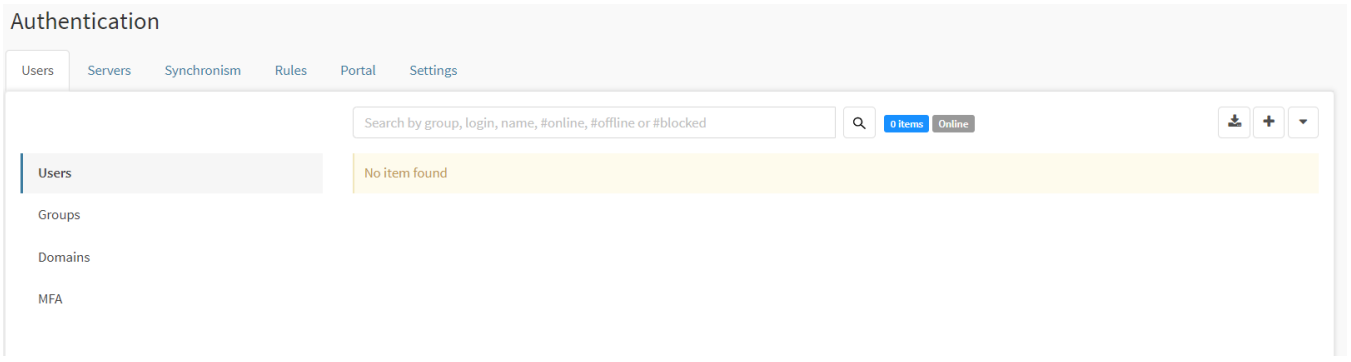
- Authentication - General Concepts;
- Authentication types;
- Sync Types.

To access this screen, just select the “Authentication” option.



Settings - Authentication

The screen below will appear:



Settings - Authentication - Users

The Authentication screen has the following tabs:

- *Users*;
- *Servers*;
- Synchronism;
- Rules;
- *Portal*;

- *Settings*.

Next, we will analyze the components of the *Users* tab.

UTM - Authentication - General Concepts

In this item, the administrator defines which authentication standards will be used.

There are 5 (five) **types** of authentication:

- ***Local***;
- ***Windows AD LDAP***;
- ***LDAP* (*AD*, *Unix*, *Linux*)**;
- ***TACACS+* (*Terminal Access Controller Access-Control System Plus*)**;
- ***Radius* (*Remote Authentication Dial in User Service*)**.

The Authentication Service supports 5 (five) Authentication Methods:

- *Portal WEB*;
- Windows Authentication Client (Agent);
- 2FA - Two Factor Authentication - Digital Certificate;
- *SSO* (*Single Sign On - Windows*);
- *RSSO* (*Radius Single Sign On - Radius*).

The NGFW will use the first server on which it can perform the user, password and domain validation, otherwise it will repeat the same process on the next server until it is successful. The order of authentication priority is respectively: Windows, LDAP, TACACS + and RADIUS Server.

Authentication types

- **Local Authentication**

Local authentication consists of a base of (exclusive) users, registered manually or by importing a list in the “txt” or “.csv” format.

- **Windows authentication client (Agent)**

It is a standard Windows authentication AGENT (.msi - Windows installer) - with support for versions 7+ (and higher).

- **2FA - Two Factor Authentication - Digital Certificate**

The standard login requires a username and password. This is a single factor authentication, and your password is information that you must know in order to gain access to the system.

Two-factor authentication adds the requirement for additional information for your login. The two factors used by the Blockbit NGFW are:

    - (user + password);
    - (digital user certificate - SSL).
- ***Windows AD***

Windows AD server-based authentication requires the Blockbit NGFW server to be integrated into the domain.

- ***LDAP***

LDAP server-based authentication authenticates directly to the LDAP database, requiring no domain integration.

- ***TACACS+***

Authentication based on TACACS + uses connection-oriented transport based on TCP and complete encryption of data packets. Authentication is performed by comparing the login request with the user ID registered in the authentication server's database, which in turn uses the TACACS + protocols to determine whether to guarantee or deny access.

- ***RADIUS***

Authentication based on the RADIUS server, functions as an authentication proxy, where authentication is redirected to the RADIUS server that recognizes the integrated network/domain authentication basis.

There are two RADIUS authentication methods:

- *RSSO* (*Radius Single Sign ON*);
- *Account Client Radius*.

RADIUS allows multiple authentication domains, being:

- [N] domains of the local type;
- [N] integrated domains:
    - *Base Windows* [1];
    - *Base LDAP* [1];

    - *Base RADIUS* [N].
- **Integrated authentication**

The Integrated Authentication Service requires the synchronization of the user base of the respective remote servers. The administrator has the option to synchronize the user base and groups from remote servers to the user base on Blockbit NGFW.

Sync Types

- **Windows *AD/LDAP***

The synchronization process on “Windows AD / LDAP” servers centralizes the registration administration of all users and / or groups on the respective LDAP servers, this synchronization process updates the user base (new or removed) in the Blockbit NGFW user base.

- **TACACS + integration**

TACACS + integrates through "automatic registration" of users already registered on the remote base for one (1) or more (+) user groups for the Blockbit NGFW user base, in this process it is not possible to identify users removed from the server In this case, the network administrator will have the responsibility to manage the user base and manually update the Blockbit NGFW when there are cases of removal of users from the TACACS + base.

- **Radius integration**

The synchronization method using “Radius” servers, performs a “self registration” of the new authenticated users in the remote base for one (1) or more (+) user groups for the Blockbit NGFW user base, in this process it is not possible to identify users removed from the remote server, in which case the network administrator will be responsible for managing the user base and manually updating the Blockbit NGFW when there are cases of removing users from the remote Radius server base.

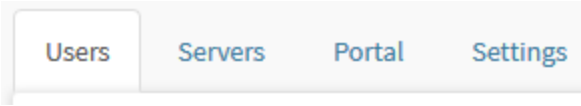
Next we will analyze the components of the users tab.

UTM - Authentication - Users Tab

The system allows the management of users of the local base with the options of "Search", "Import", "Add" or "Remove" a user from the system, it also makes it possible to define which groups they participate in. It is even possible to enable or disable the user, which directly implies the login action.

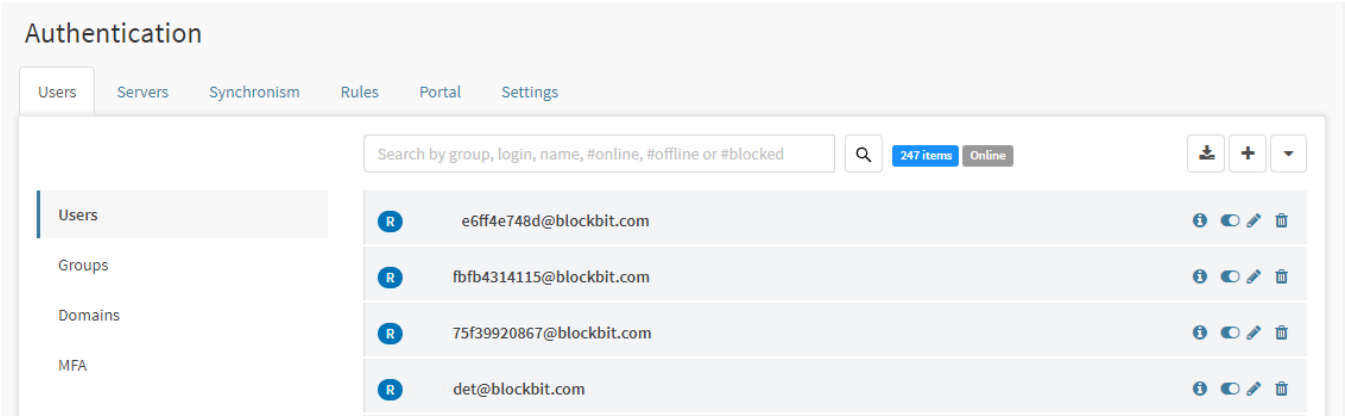
We have “Local” and “Remote” users, and it is worth remembering that the management of remote users is the responsibility of the “Windows AD” or “LDAP” synchronization servers.

For managing the local or remote user base, click Users:



Users tab

The screen will appear, as shown by the image below:



Users tab - Authentication

This screen has 4 side tabs:

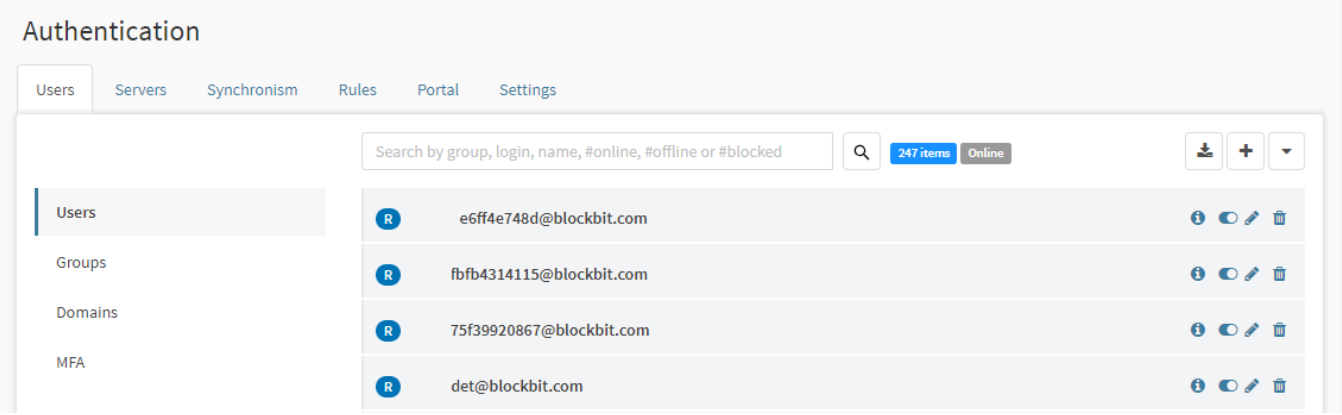
- *Users;*
- *Groups;*
- *Domains;*
- *MFA.*

Next, each component of this screen will be analyzed.

UTM - Users - Users

Through this screen it is possible to add, import and manage users that have already been added.

To visualize the authenticated users, run a search using the #online filter.



Users - Users

This screen comprises the following features:

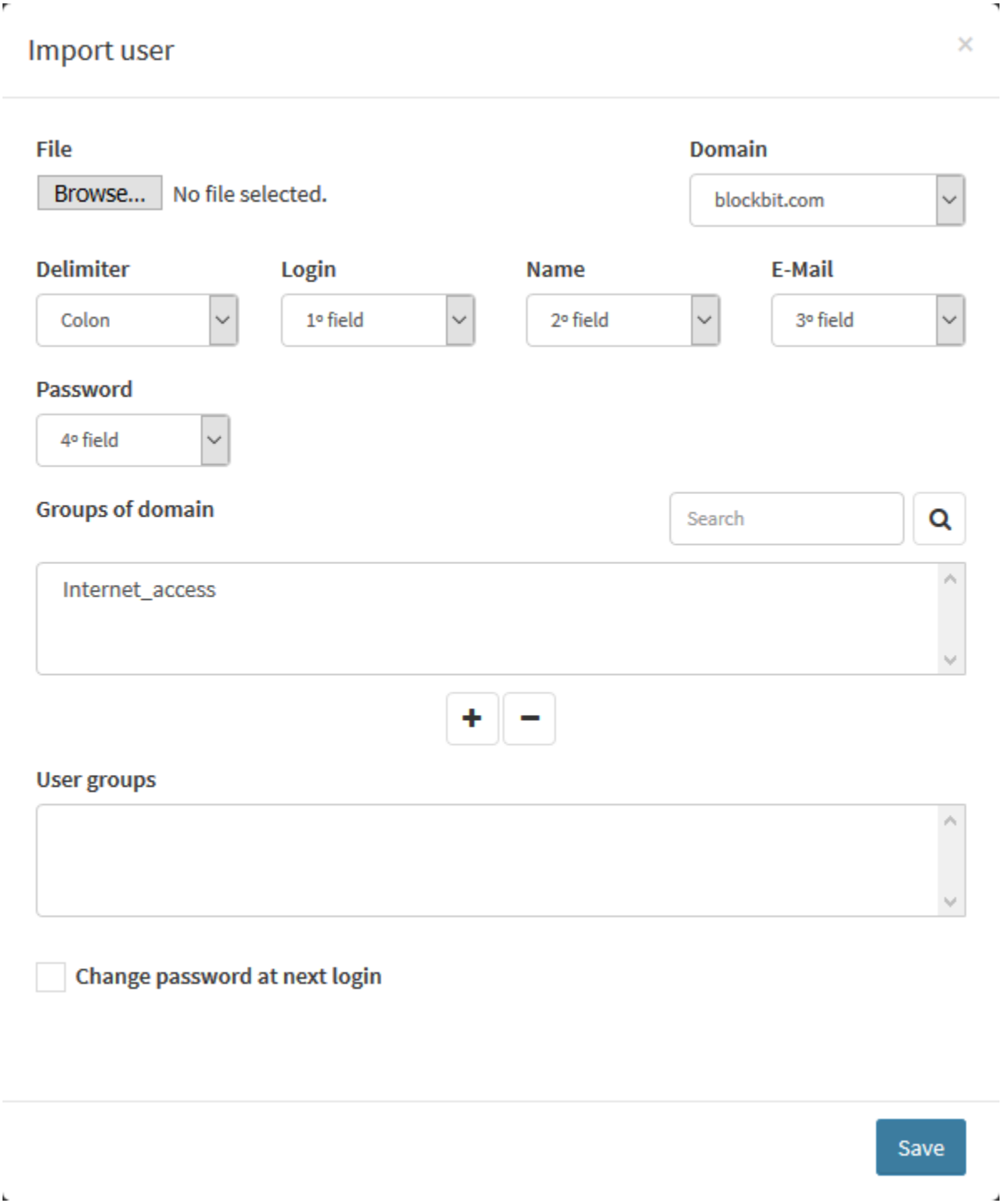
- *Import User*;
- *Add User*;
- *Actions Menu*;
- *Edit User*;
- *Remove User*.

Next, we will analyze each component of this screen.

UTM - Users - Users – Import User

To import users, click on the [ ] button.

This interface allows the administrator to import users from a list file, with standard field delimiters (.csv). Fill in the form according to the import file standard, select the corresponding “domain” and “groups” (if there are groups), then click [Save].



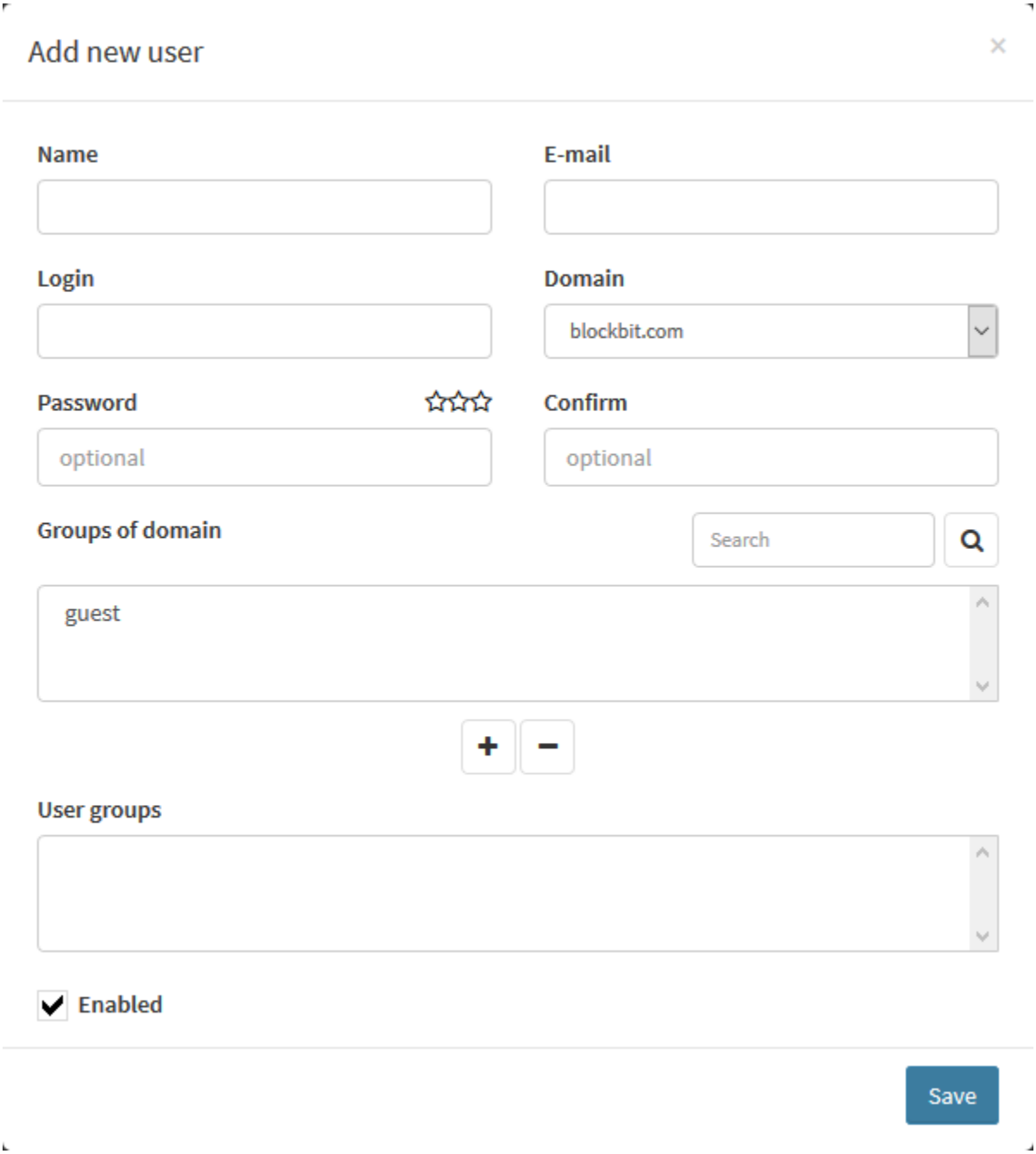
Users - Import Users

- ***File*:** Click the [Browse...] button and select the location of the file that was created to be imported. Ex.: users_local_doc_ngfw14;
- ***Domain*:** Enter the domain to which the users list will be imported. Ex.: blockbit.com;
- ***Delimiter*:** Inform which delimiter was used in the file containing the users. Ex.: *Colon*;
- ***Login*:** Inform the order where the “Login” field is found in the file containing the users. Ex.: 1º *field*;
- ***Name*:** Inform the order that where the “Name” field is found in the file containing the users. Ex.: 2º *field*;
- ***E-mail*:** Inform the order where the “E-mail” field is found in the file containing the users. Ex.: 3º *field*;
- ***Password*:** Inform the order where the “Password” field is found in the file containing the users. Ex.: 4º *field*;
- ***Group of domain*:** Domain groups are available to be selected in order to add synchronized users;
- ***Users groups*:** Groups are selected to add previously imported users;
- ***Change password at next login*[☑]:** By selecting this checkbox, it will be mandatory to change the password at the next login.

 It is common in a process of importing users by list, to set a default password for all users on the same list. For this reason it is important to keep the option “Change password at next login” enabled.

UTM - Users - Users – Add User

To add a new user, click **[+]** button, the following window will be displayed:



Users – *Add New User*

Fill in the fields with the respective data:

- ***Name*:** Enter the user name. Ex.: *user*;
- ***E-mail*:** Inform the user. Ex.: user@blockbit.com;
- ***Login*:** Enter the user's login credentials. Ex.: *userlogin*;
- ***Domain*:** Enter the domain to which the user will belong. Ex.: blockbit.com;
- ***Password*:** Enter the password that the user should use to log in, the stars at the top of the field represent the level of password complexity;
- ***Confirm*:** It is the field where the password entered in the “password” field is confirmed.;

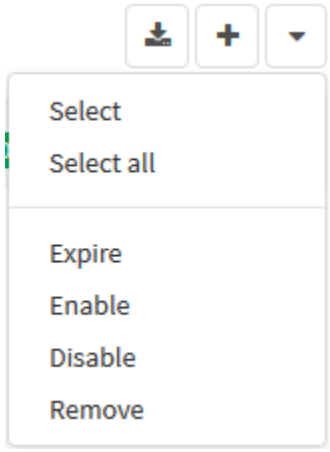
- ***Groups of Domain*:** Determine the domain groups to which the user will be included, the search box on the right allows the search of a specific group;
- ***User Groups*:** This option is used to include the user in any group;
- **Enabled[ ]:** Determines whether the user will be enabled or not.

After completing the necessary changes, click the **[** 

] button to keep the changes.

UTM - Users - Users – Actions Menu

At the top right of the "Users" panel, we have the actions menu, which can be displayed by clicking on the **[ ]**, as illustrated by the image below:



Users – Actions Menu

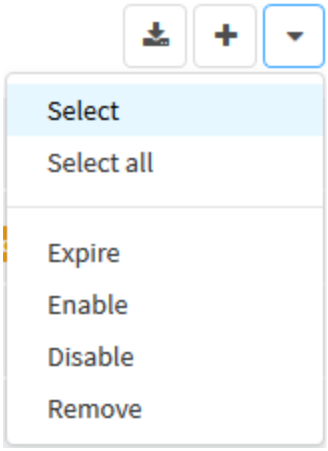
The menu consists of the following options:

- *Select and Select all*;
- *Expire*;
- *Enable;*
- *Disable*;
- *Remove*.

Next, we'll look at each of these options.

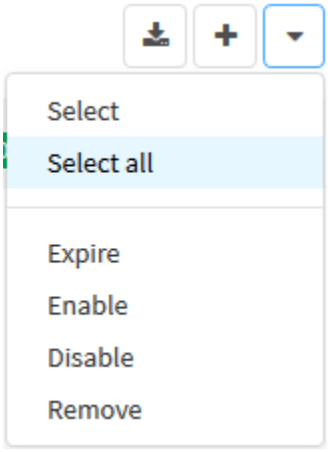
UTM - Users - Actions Menu - Select and Select All

When clicking on the “Select” option, the removal icons will be replaced by checkboxes that can be used to make a mass deletion through the actions menu.



Users - Select

By clicking on “Select All” in the action menu all items will be selected.



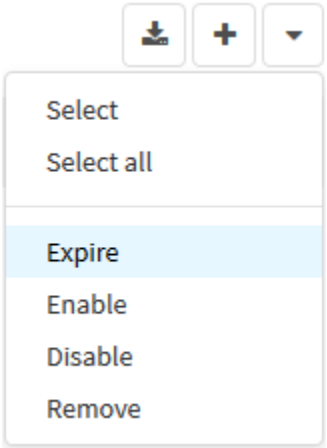
Users – Select All

This allows changes that affect all items to be easily implemented.

UTM - Users - Actions Menu - Expire

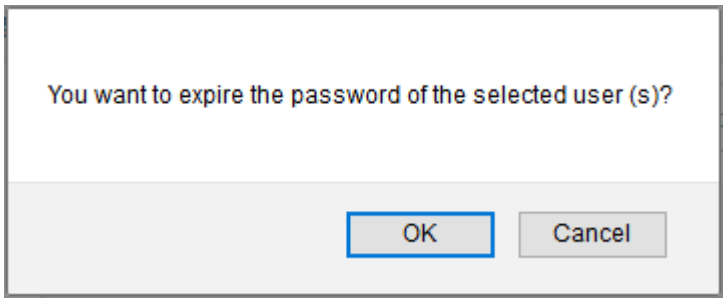
To force the user's password to expire and they have to create a new password at the next login, use the “Expire” function.

To do so, select the desired user and click on the action menu [ ], the menu below will be displayed;



Actions Menu - Expire

After selecting "Expire", the window below will appear:



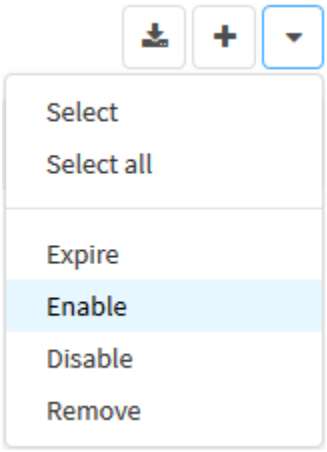
Users – Expire User Password

Click [OK] to force the password to expire, otherwise click [Cancel].

UTM - Users - Actions Menu - Enable

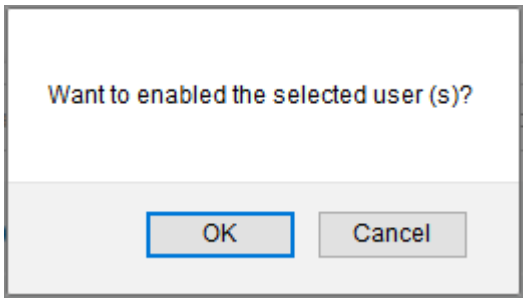
To activate selected users, use the “Enable” function.

To do so, click on the action menu [ ], the menu below will be displayed;



Actions Menu - Enable

After selecting "Enable". The following confirmation message will appear:



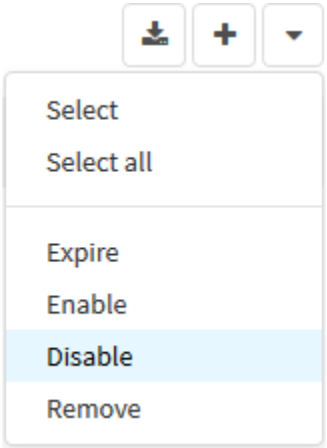
Users – *Enable Users*

Click [OK] to activate the user, otherwise click [Cancel].

UTM - Users - Actions Menu - Disable

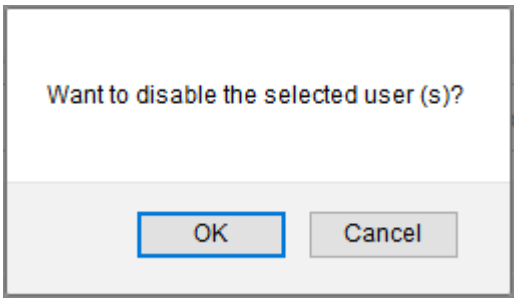
To disable selected users, use the “Disable” function.

To do so, click on the action menu **[ ]**, the menu below will be displayed;



Actions Menu - Disable

After selecting "Disable". The following confirmation message will appear:



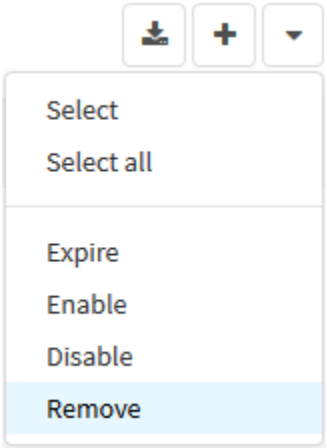
Users – *Disable Users*

Click **[** OK **]** to disable the user, otherwise, click **[** Cancel **]**.

UTM - Users - Actions Menu - Remove

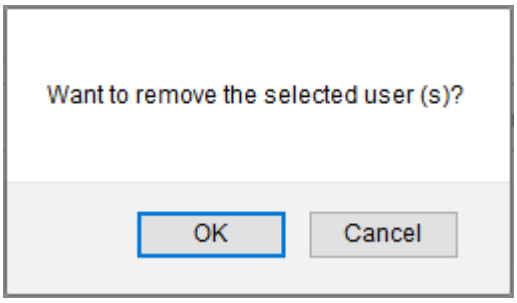
To delete the desired users, use the “Remove” option.

To do so, click on the action menu **[**  **]**, the menu below will be displayed

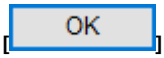
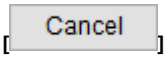


Actions Menu - Remove

The following confirmation message will be displayed:



Users – Remove Users

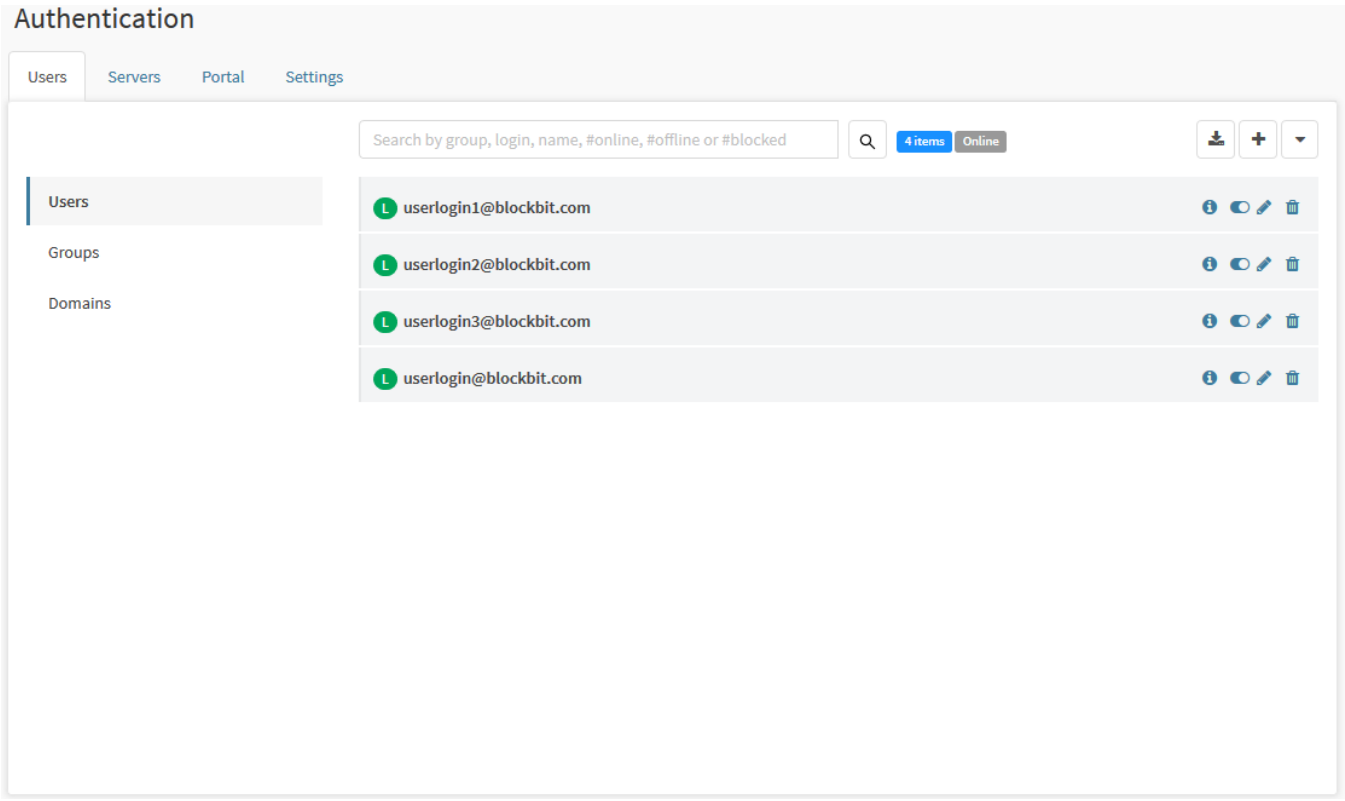
Click **[**  **]** to delete, otherwise, click **[**  **]** to not remove users.

Finally, to see the delete icons **[**  **]** again, click on “Groups” in the left side menu.

UTM - Users - Users - Columns

Below we will explain each column of the Users tab:

To visualize the authenticated users, run a search using "#online" as a filter.

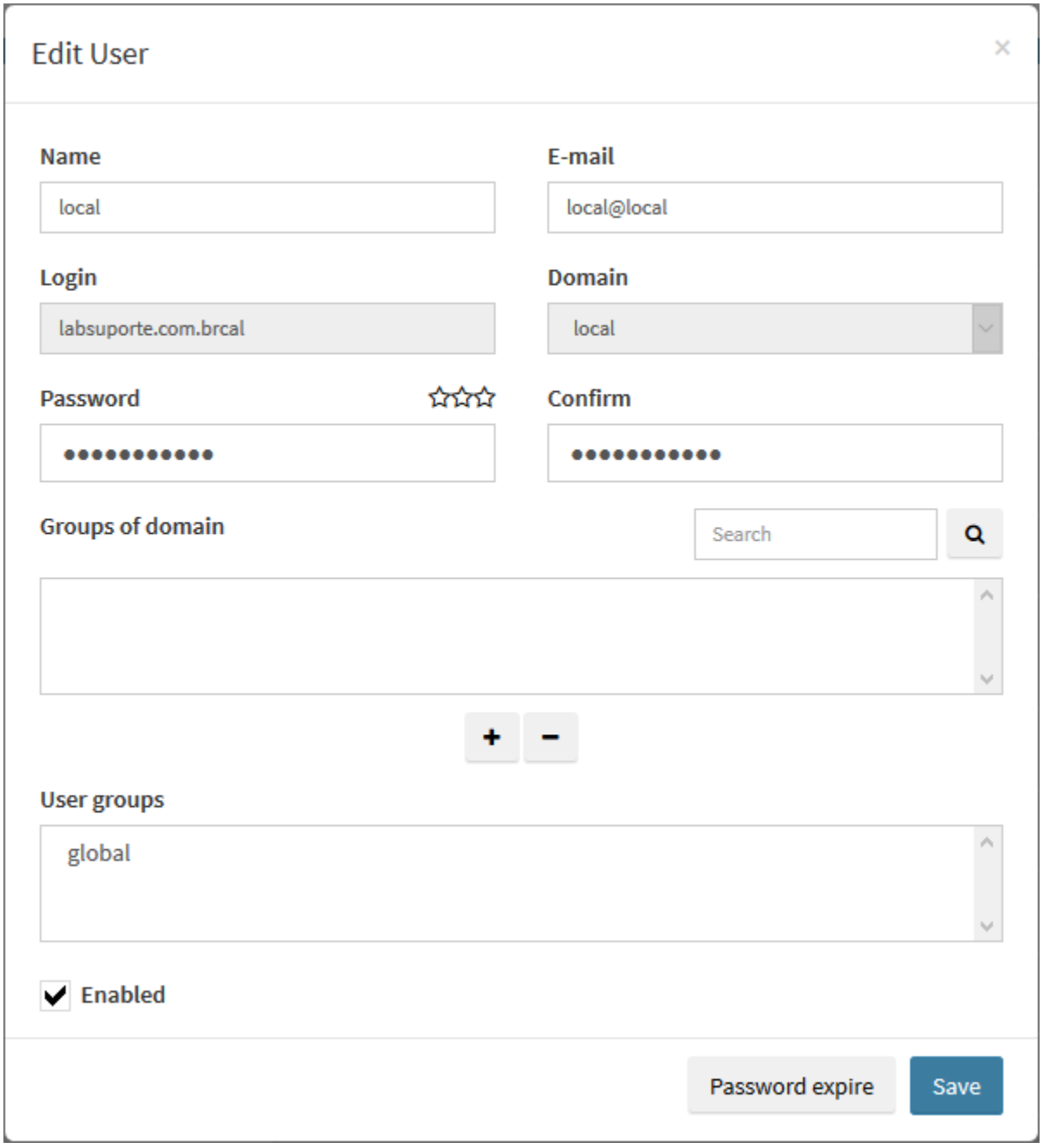


Users

- ***Status:*** *After registering / importing local users, displays the following statuses*:
  - [L]: It means that this is a local user;
  - [R]: It means that this is a remote user, synchronized with a Windows, LDAP or TACACS + database;
  - [Online]: It means that this user is currently logged on;
  - [Bloqueado]: It means that this user was blocked for exceeding the limit of attempts to login;
  - [Expired]: It means that this user's password has expired. In the next “logon” a password change will be required;
- ***Select*** **[ ]:** Allows you to select a user*;*
- ***Login*****:** Displays the user's login and domain, for more information on how to add domains, check this page;
- ***Info [ ]*****:** Displays the registered user's name;
- ***Enabled [ ]/Disabled [ ]*****:** When enabling, it activates the selected user. If the user is disabled he will have his account registered normally, but it will be impossible for him to log in or use it;
- **Edit *[ ]*:** Allows the editing of the settings of the added user, for more information about this option, check this page;
- **Excluir [ ]:** Deletes the selected user, it is the equivalent of the *Remove* option from the actions menu.

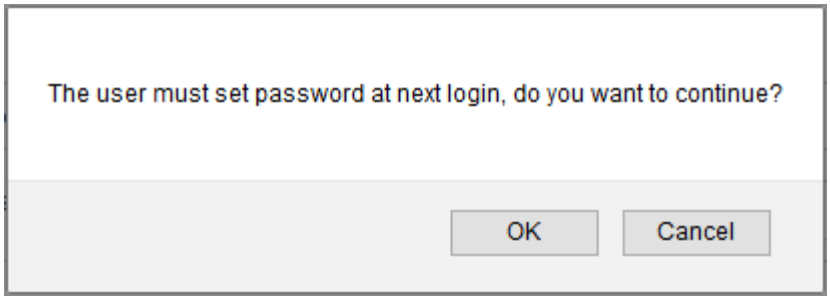
UTM - Users - Columns – Edit User

By clicking on the **[** **]** button it is possible to edit the information located on the selected user.



Users – Add New User

The **[** Password expire **]** button allows the user to determine a password at the next login. When you click this button, the following message will be displayed:



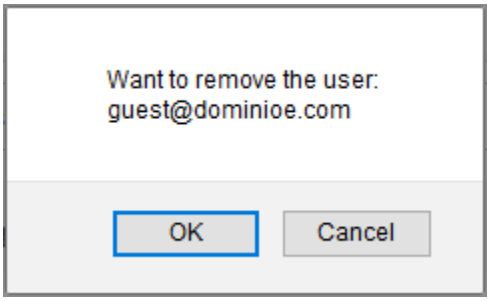
Users – Password Expiration Confirmation.

Click **[** OK **]** to force the user to determine a password at the next login, otherwise, click **[** Cancel **]**.

After completing the necessary changes, click the **[** Save **]** button to save them.

UTM - Users - Columns - Remove User

If you want to remove any of the created users, click on the delete icon **[** **]**, a confirmation message will be displayed, as illustrated by the image below:



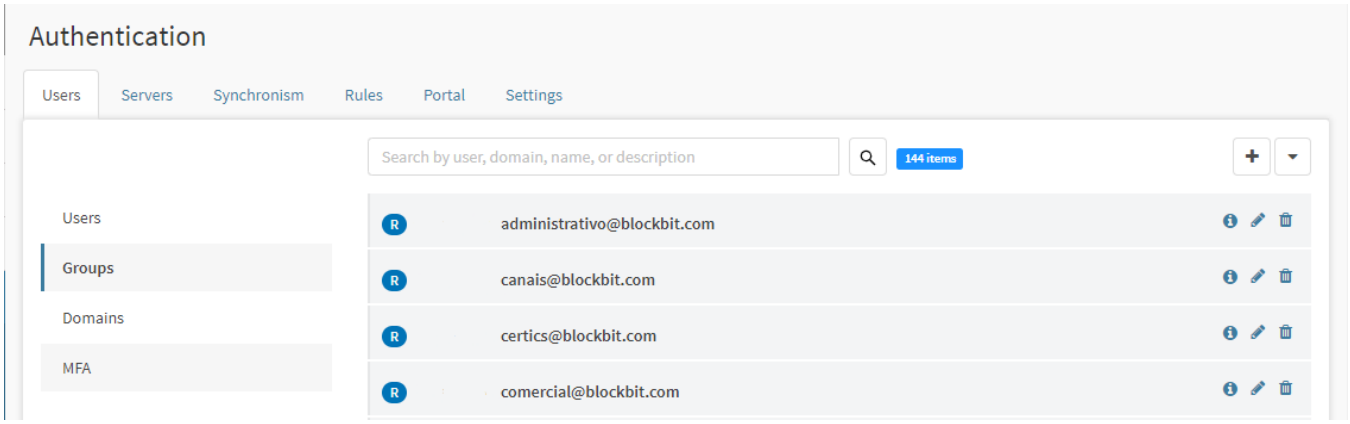
Users – Remove User

Click **[** OK **]** to delete, otherwise, click **[** Cancel **]** to not remove the group.

UTM - Users - Groups

Through this screen it is possible to create user domain groups.

At the top of the "Groups" panel, we have the search bar, through which it is possible to perform a search by user, domain, name or description.



Users - Groups

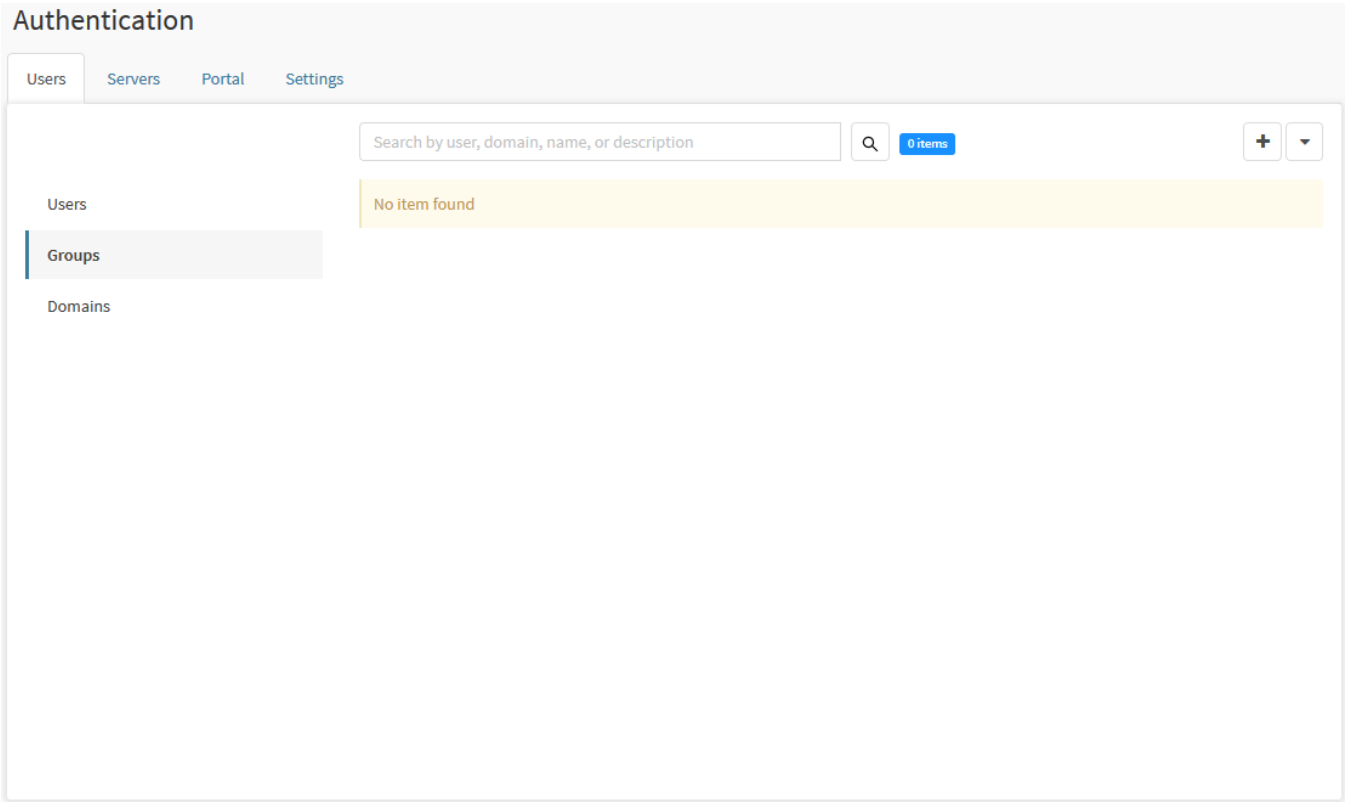
This screen comprises the following features:

- *Add Group*;
- *Edit Group*;
- *Remove Groups*;
- *Actions Menu*.

Next, we will analyze each component of this screen.

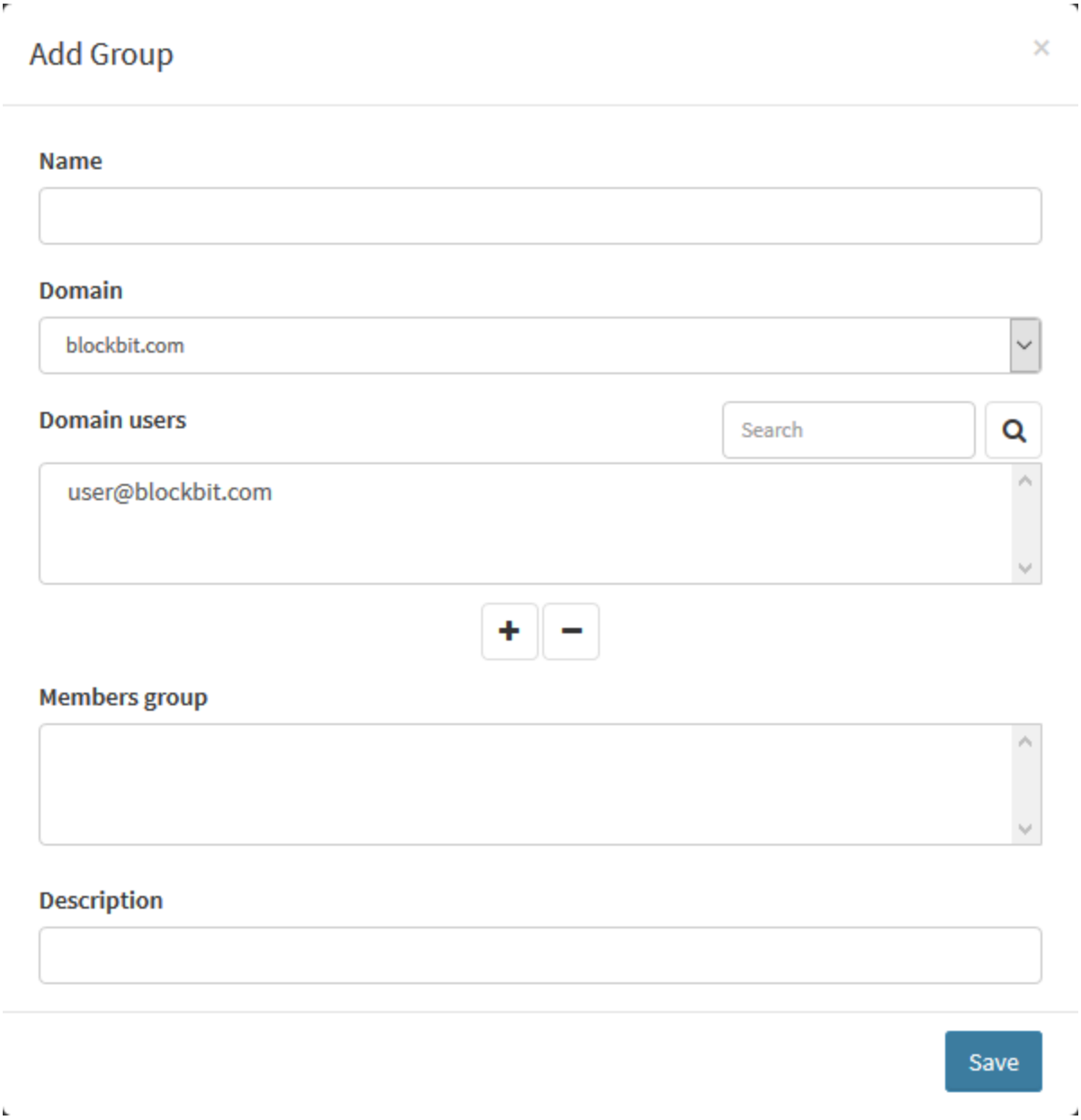
UTM - Users - Groups – Add Group

For cases in which local “domains” are used, it is recommended by good administration practices, also to define “groups” of domain users, this resource aims to facilitate management and simplify the definition of compliance policies that will be applied later.



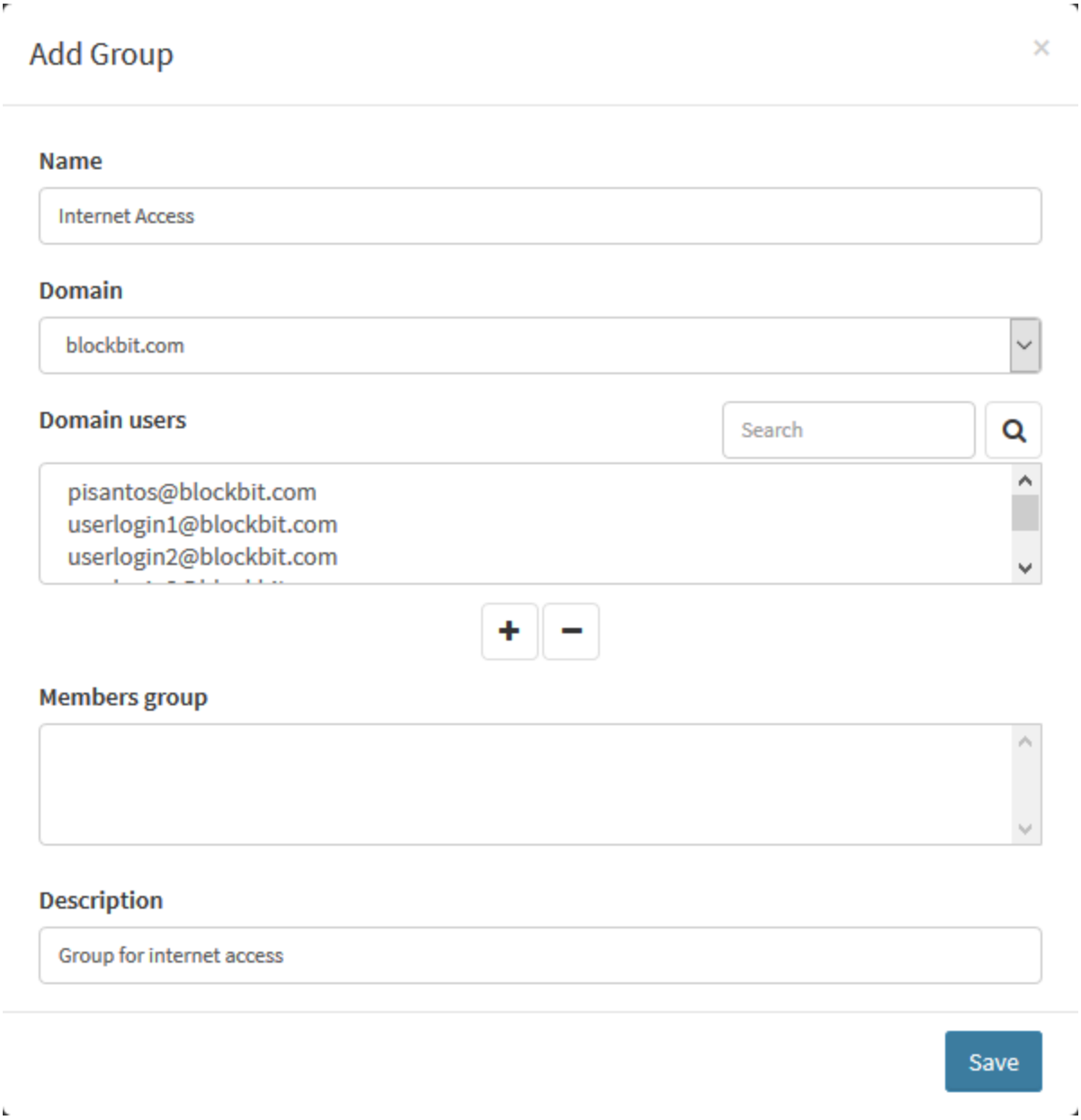
Groups - Add Local Groups

Click on **[** **+** **]** fill in the fields with the respective data:



Groups - Add Groups

- ***Name*:** Enter the group name. Ex.: internet_acess@blockbit.com;
- ***Domain*:** Enter the domain that the created group will be part of. Ex.: blockbit.com;
- ***Domainusers*:** List of users available to be added to the group;
- ***Membersgroup*:** User list group member;
- ***Description*:** Enter the group description. Ex.: Group for an internet access.

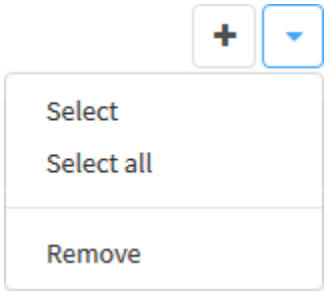


Groups - Add Group - Example

After completing the necessary changes, click the **[**  **]** button to save the changes.

UTM - Users - Groups – Actions Menu

At the top right of the “Groups” panel, we have the actions menu, which can be displayed by clicking the **[ ]** button, as illustrated by the image below:



Groups – Action Menu

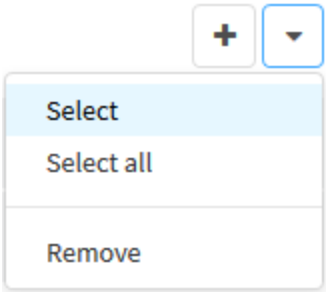
The menu consists of the following options:

- *Select and Select all*;
- *Remove*.

Next, we'll look at each of these options.

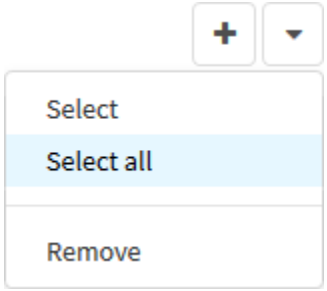
UTM - Groups – Actions Menu - Select and Select All

When clicking on the “Select” option, the removal icons will be replaced by checkboxes that can be used to make a mass deletion through the actions menu.



Groups – Select

By clicking on “Select All” in the action menu all items will be selected.



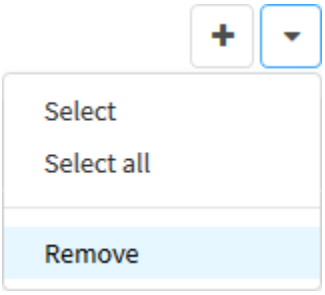
Groups – Select All

This allows changes that affect all items to be easily implemented.

UTM - Groups – Actions Menu - Remove

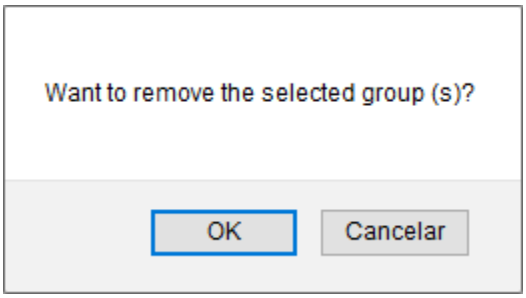
To delete the desired users, use the “Remove” option.

To do so, click on the action menu **[ ]**, the menu below will be displayed;



Actions Menu - Remove

The following confirmation message will be displayed:



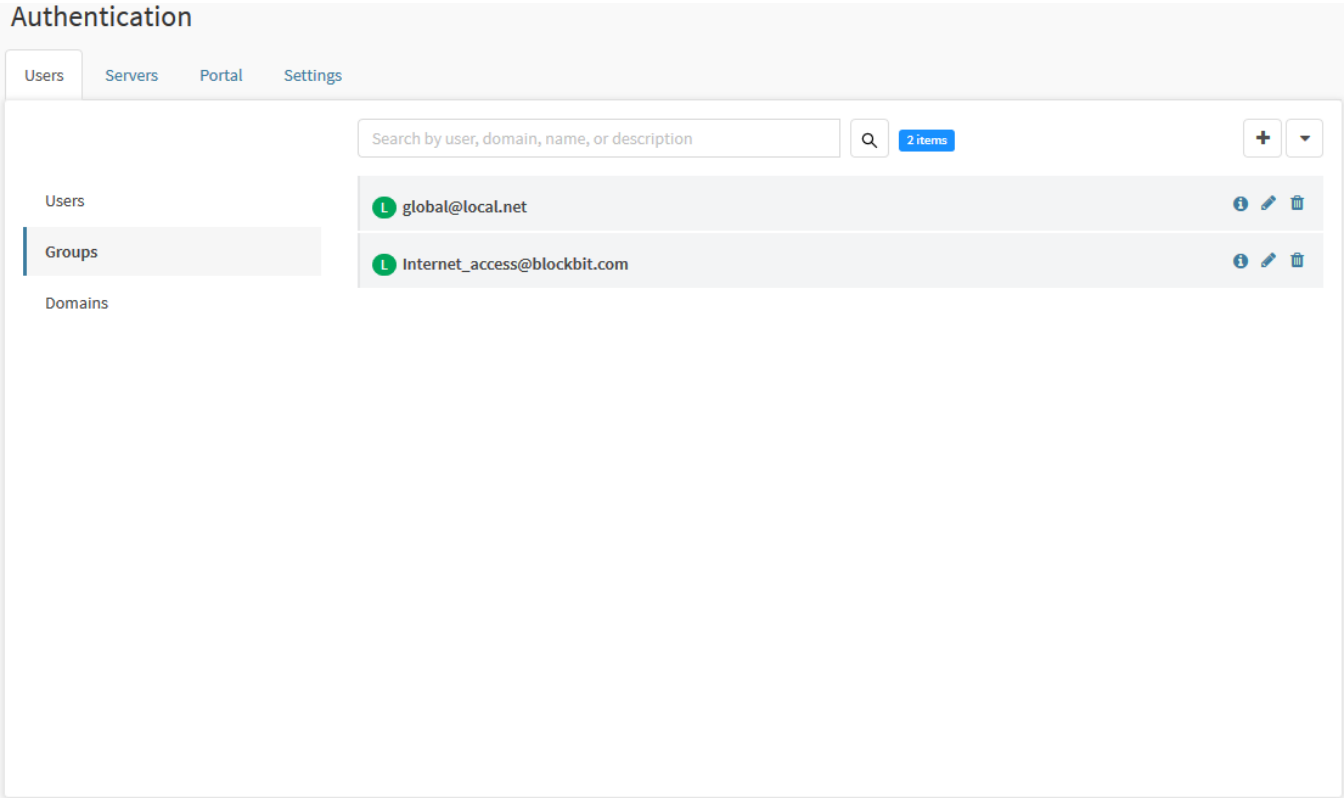
Groups – Remove Groups

Click **[** OK **]** to delete, otherwise, click **[** Cancel **]** to not remove users

Finally, to see the delete **[ ]** icons again, click on “Groups” in the left side menu.

UTM - Users - Groups - Columns

Below we will explain each column of the Users tab:

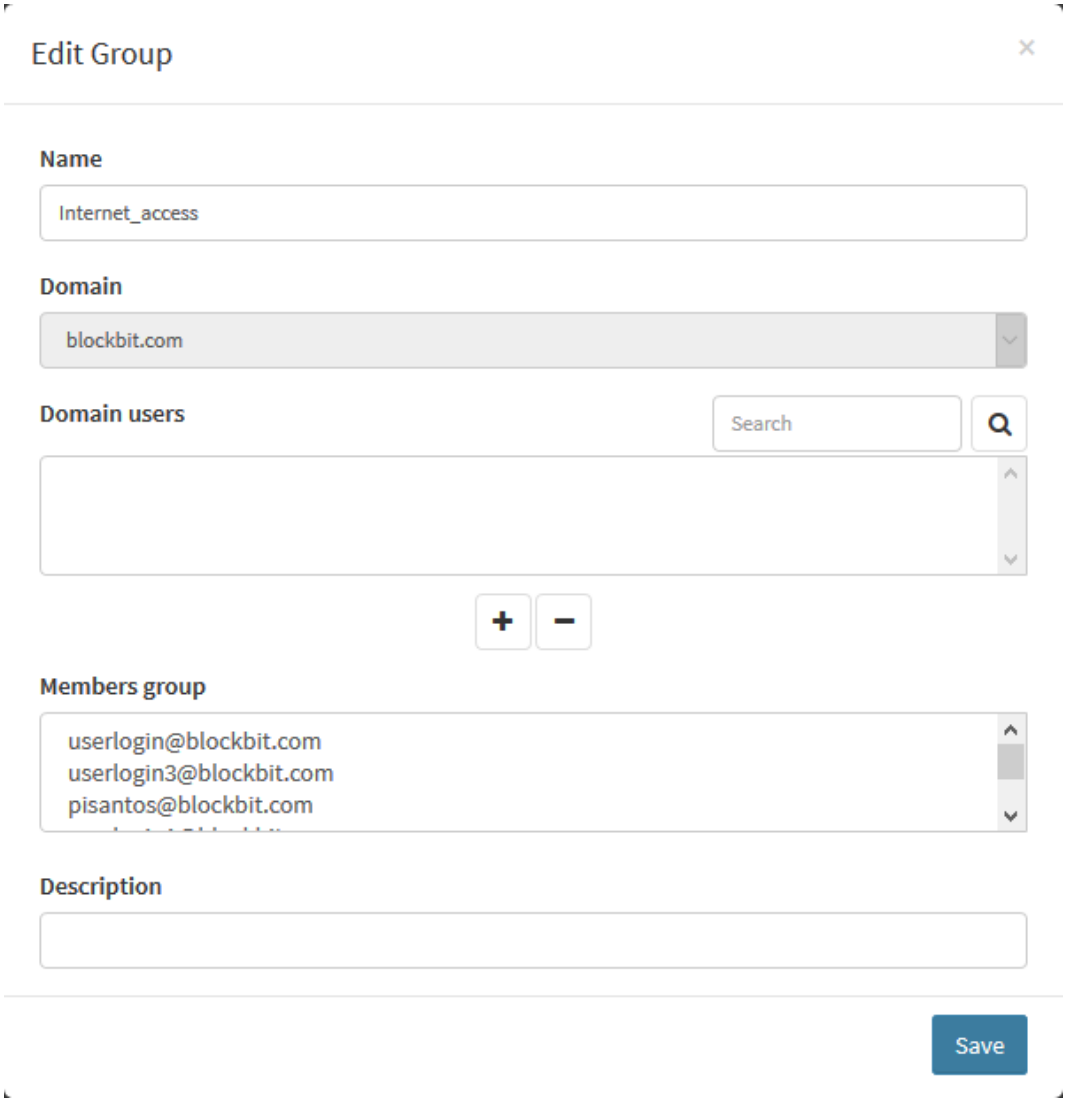


Groups

- ***Status:*** *After registering / importing local users, displays the following statuses*:
  - **[L]:** It means that this group is of the local type;
  - **[R]:** It means that this group is of the remote type;
- ***Select*** **[ ]:** Allows you to select a group*;*
- ***Name*****:** Displays the name of the registered group;
- ***Info [ ]*****:** Displays the description that was added when registering the group;
- **Editar *[ ]*:** Allows you to edit the settings of the added group, for more information about this option, check this page;
- **Excluir [ ]:** Delete the group, it is the equivalent of the *Remove* option in the action menu.

UTM - Groups – Edit Group

By clicking on the edit [ ] button it is possible to edit the information located in the selected group.

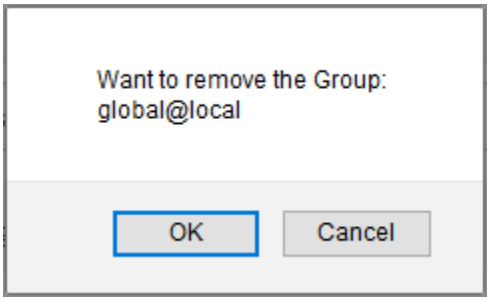


Groups – Edit Group

After completing the necessary changes click on the [Save] button to save the changes.

UTM - Groups – Remove Group

If you want to remove any of the groups created, click on the delete **[** **]** icon, a confirmation message will be displayed, as illustrated by the image below:



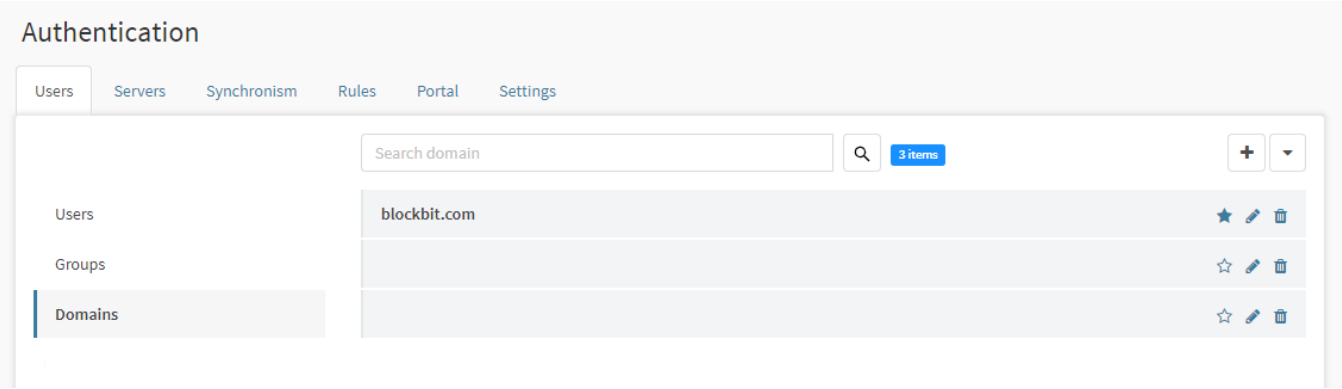
Groups – Delete Domain.

Click **[** OK **]** to delete, otherwise, click **[** Cancel **]** to not remove the group.

UTM - Users - Domains

To add a user, you will first need to add a domain, on this screen you can make these additions.

At the top of the "Domains" panel, we have the search bar, through which it's possible to search the domains that are added:



Users - Authentication Domains

This screen comprises the following features:

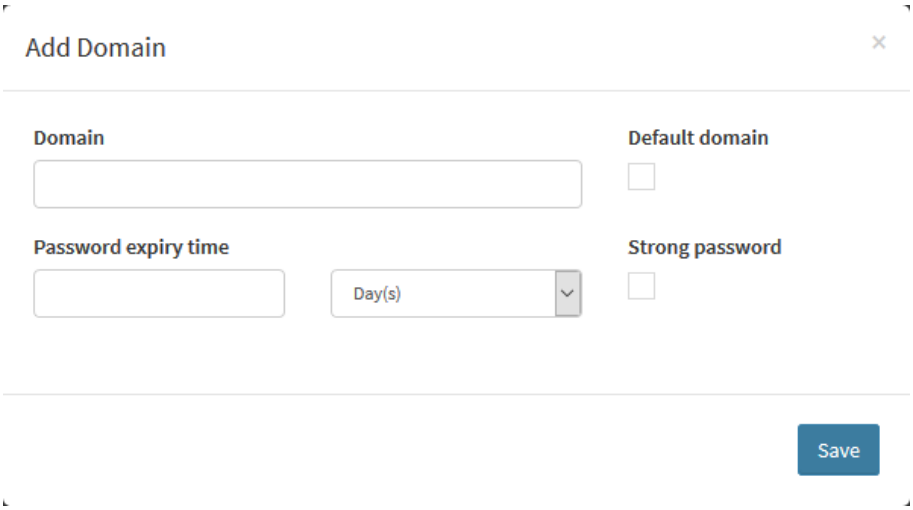
- *Add Domain*;
- *Edit Domain*;
- *Remove Domain*;
- *Actions Menu*.

Next, we will analyze each component of this screen.

UTM - Users - Domains - Add Domain

To add a domain, follow the steps below:

When you click [+] the following window will be displayed:



Domains - Add Domain

- ***Domain:*** Enter the domain name;
- ***Default domain [ ]:*** When checking this checkbox, this domain will be determined as the default domain;
- ***Password expiry time:*** Determines the time required for the password to expire;
- ***Strong password [ ]:*** If this checkbox is enabled, it requires users to use a strong password.

Finally, click [Save] to save the domain.

Check an example of how to add domains on this page.

UTM - Example: Adding Domains

To exemplify, we will add 3 (three) domains of the local type:

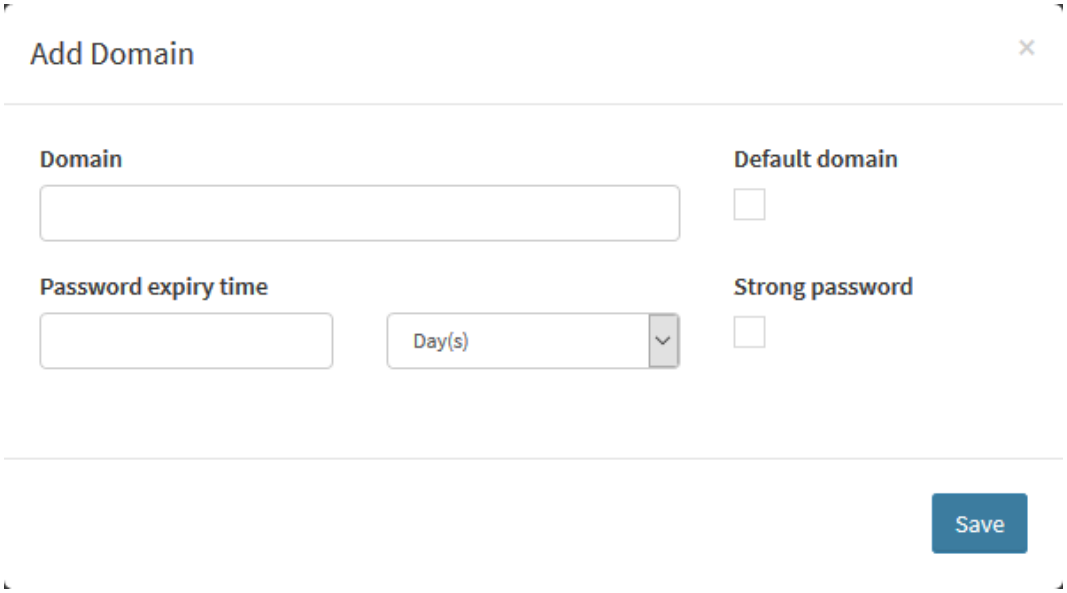
- Domain 1 to “blockbit.com”;
- Domain 2 to “local.net”;
- Domain 3 to “guest.com”.

Then we move on to the user import / add process. The **Import** [ ] or **Add** [ ] users actions are only valid for local domains.

Adding “local” domains - Example 1

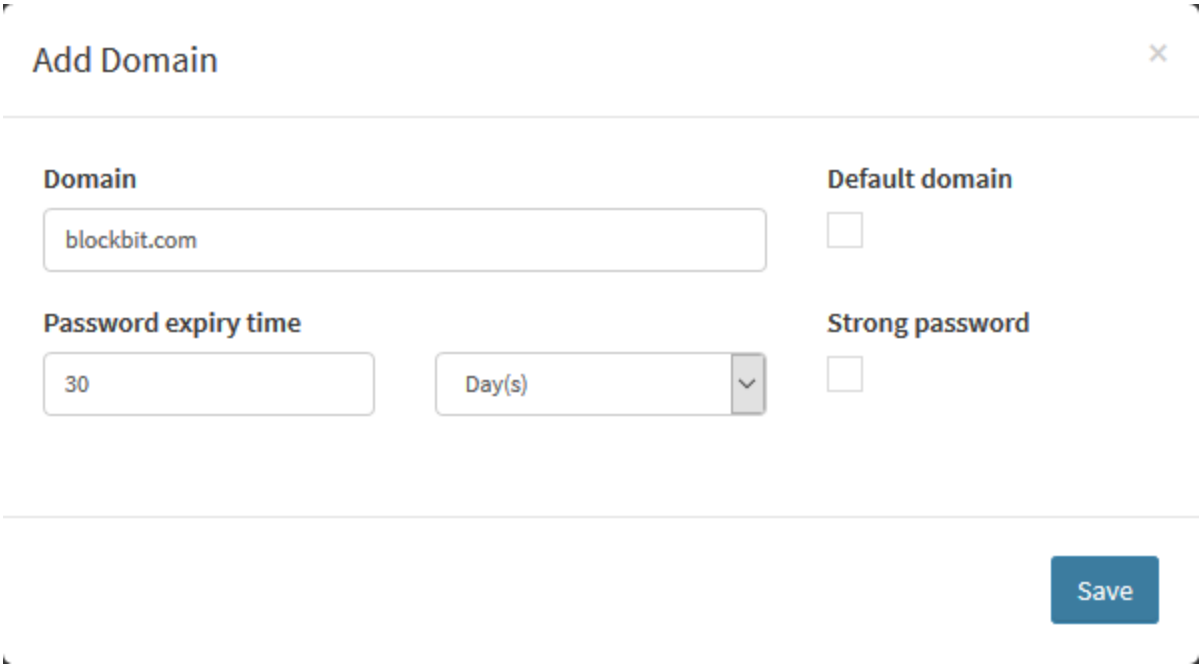
To add domains, on the Users tab click on the Domains side tab.

Click on ***Add*** [ ], the following window will be displayed:



Domains - Authentication Domains

Fill in the fields with the respective data:



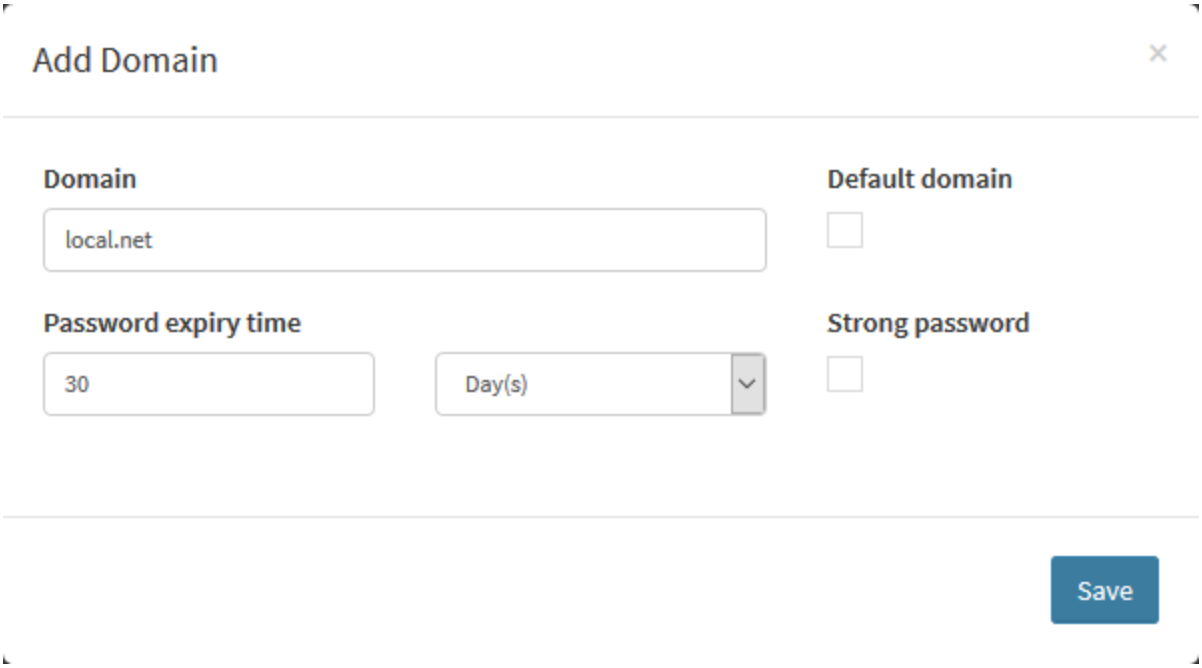
Domains - Add Domain - Example 1

- ***Domain*:** blockbit.com;
- ***Password expiry time*:** 30 days.

Fill in the fields with the respective data and click **[Save]**.

Example 2

Click on **Add [+]**, and fill in the fields with the respective data:



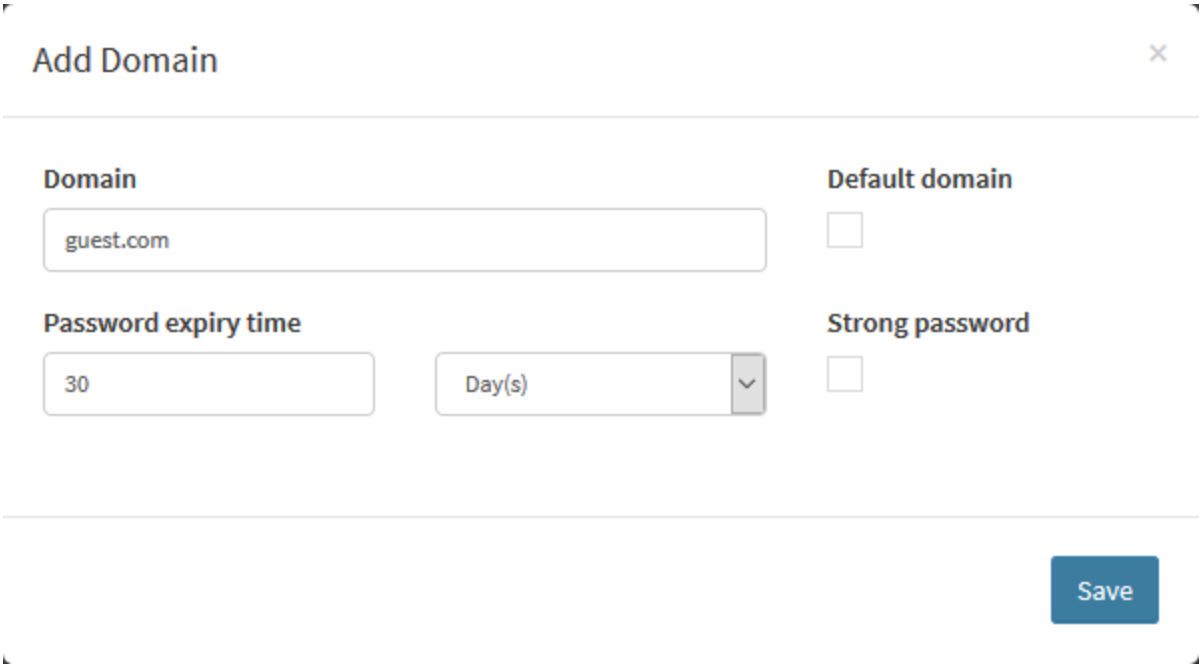
Domains - Add Domain - Example 2

- ***Domain*:** local.net;
- ***Password expiry time*:** 30 days.

Fill in the fields with the respective data and click on [Save].

Example 3

Click on ***Add*** [+], and fill in the fields with the respective data:



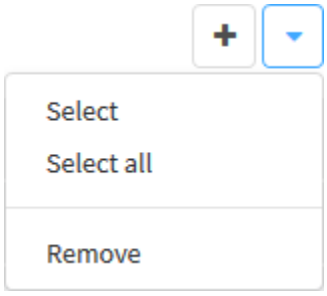
Domains - Add Domain - Example 3

- ***Domain*:** guest.com;
- ***Password expiry time*:** 30 days.

Fill in the fields with the respective data and click on [Save].

UTM - Users - Domains – Actions Menu

At the top right of the "Domains" panel, we have the actions menu, which can be displayed by clicking **[ ]**, as illustrated by the image below:



Domains - Actions Menu

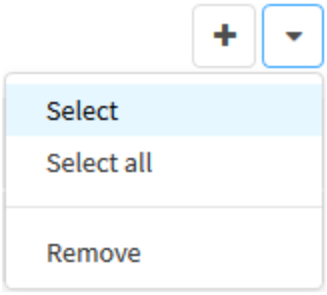
The menu consists of the following options:

- *Select and Select all*;
- *Remove*.

Next, we'll look at each of these options.

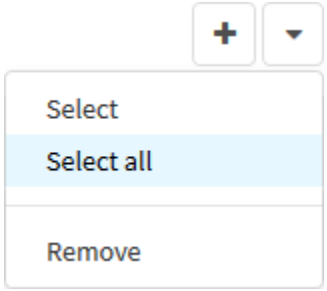
UTM - Domains – Actions Menu - Select and Select All

When clicking on the “Select” option, the removal icons will be replaced by checkboxes that can be used to make a mass deletion through the actions menu.



Domains – Select

By clicking on “Select All” in the action menu all items will be selected.



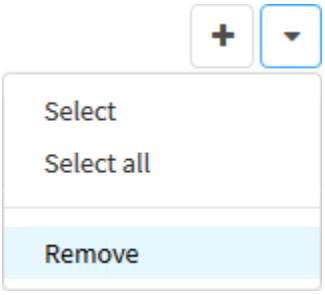
Domains – Select All

This allows changes that affect all items to be easily implemented.

UTM - Domains – Actions Menu - Remove

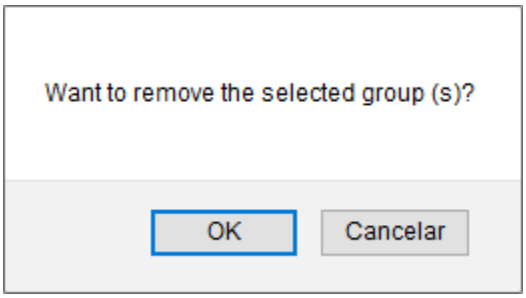
To delete the desired domains, use the “Remove” option.

To do so, click on the action menu [ ], the menu below will be displayed;



Actions Menu - Remove

The following confirmation message will be displayed:



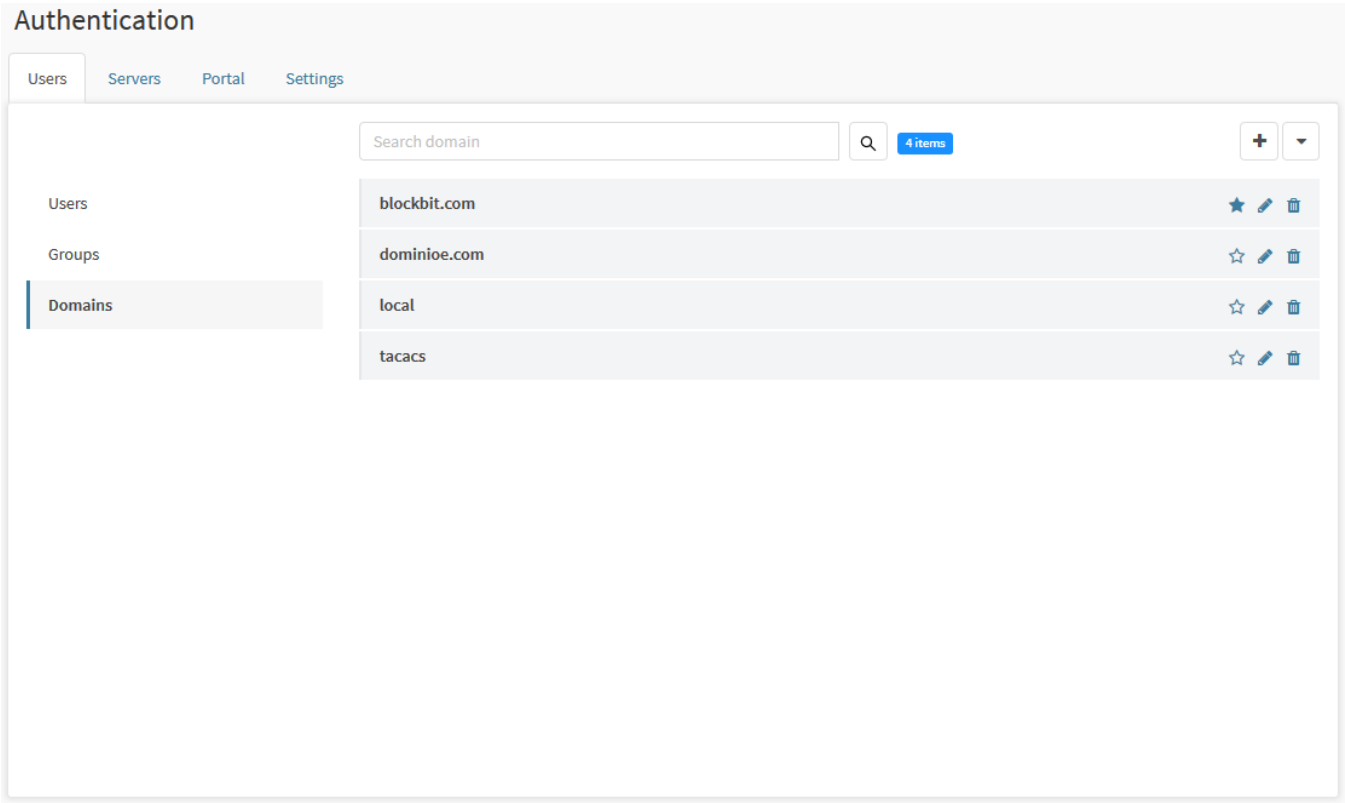
Domains – Remove Groups

Click [OK] to delete, otherwise, click [Cancel] to not remove the domains.

Finally, to see the delete [ ] icons again, click on “Domains” in the left side menu.

UTM - Users - Domains - Columns

Below we will explain each column of the Users tab:



Authentication - Domains

- ***Select* [ ]:** Allows you to select a group;
- ***Name*:** Displays the name of the registered domain;
- **Default[ ]**: Enable to select a default domain, for more information about this option, check this page;
- **Editar *[ ]*:** Allows you to edit the settings of the domain added, for more information about this option, check this page;
- **Excluir [ ]:** Deletes the domain, it is equivalent to the *Remove* option in the actions menu.

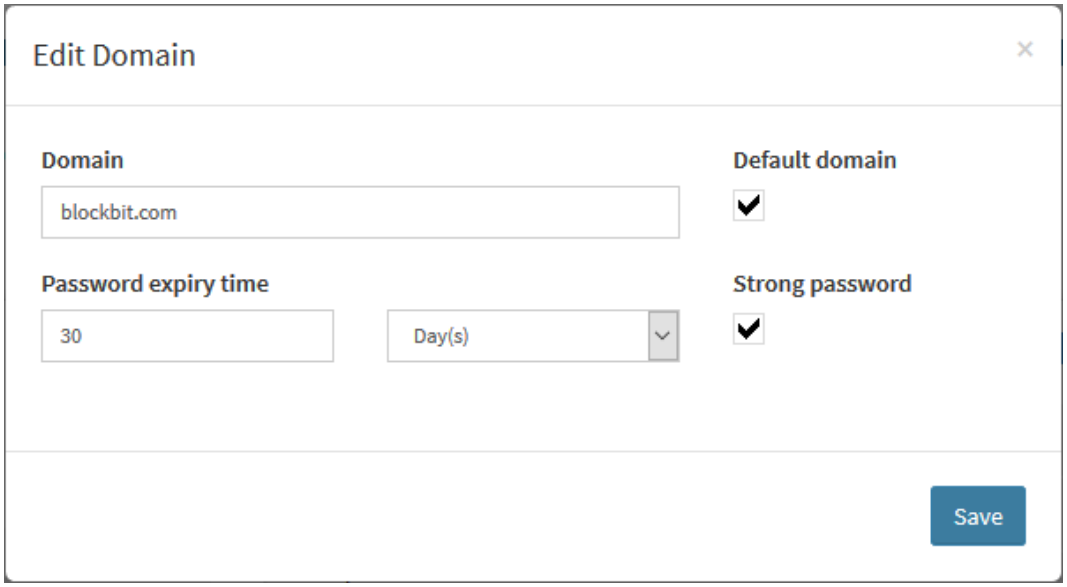
UTM - Users - Domains - Set as Default Domain

After adding the Domain, by clicking on the ***default*** **[ ]** icon, it is possible to configure it as the default domain, there can only be a single default domain. This means that all operations applied to the authentication panel, will consider this domain as the main one. If it is necessary to log in to a domain, other than the default, it will be necessary to inform it in front of the login.

Domains – Default Domain

UTM - Users - Domains – Edit Domain

By clicking on the edit [ ] button it is possible to edit the settings of the selected domain.

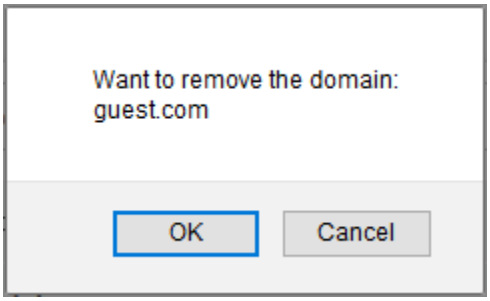


Domains – Edit Domain

After completing the necessary changes click on the [Save] button to save the changes.

UTM - Users - Domains – Remove Domain

If you want to remove any of the created domains, click on the delete **[ ]** icon, a confirmation message will be displayed, as illustrated by the image below:



Domains – Delete Domain.

Click **[** OK **]** to delete, otherwise, click **[** Cancel **]** to not remove the domain.

NGFW - Users - Multi-Factor Authentication (MFA)

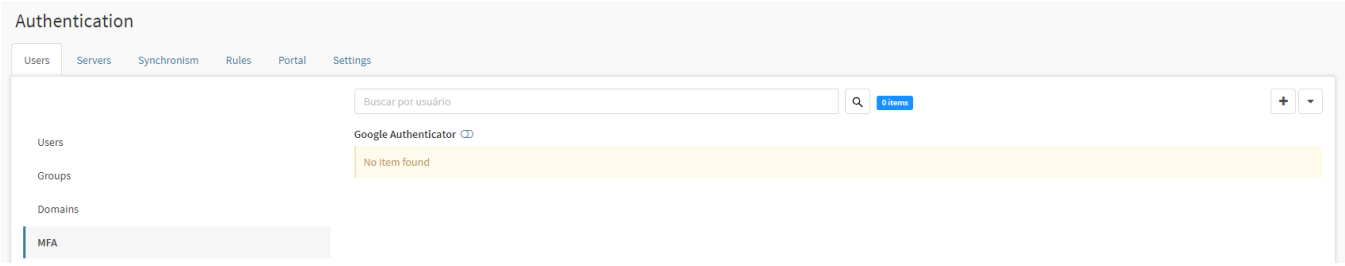
Through this screen it is possible to activate the MFA (Multi-Factor Authentication) method. The *Multi-Factor Authentication* is a method that requires the verification of two or more factors to validate a user. The importance of using an authentication method that goes beyond the mere use of a username and password, are gains in terms of security (increased resistance to Brute Force, and other forms of attacks that aim at stealing the users' credentials). This validation method works as a means for accessing both the NG VPN and the Captive Portal.

About the *Multi-Factor Authentication*

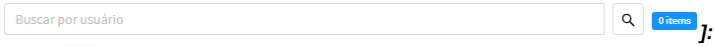
The method consists on a combination of factors for the user's validation. The concept is to validate the identity based on the following elements:

Knowledge (things the user knows): Username and password, answers to preset security questions;

Possession (things the user possesses): Devices like a smartphone or a laptop, to which an OTP (One-time Password) is sent. It can be a password, a PIN, a certificate or a software-generated token, usually sent by e-mail or SMS to the device that is trying to be validated, and can be used only once, generated to provide access for every new login attempt.



Users - Multi-Factor Authentication

- ***Search [***  ***]:*** Searches a user by the name.
- ***Generate key [***  ***]:*** Allows the selection of a registered user and the creation of a validation key for this one. This validation key, or *token*, will be used alongside the password when logging in.
- ***Select [***  ***]:*** Allows the selection of a user or all of them.

 To visualize the online authenticated users, use the "#online" filter on the search bar.

 *On the Blockbit NGFW's features, MFA can only be enabled for local users. Therefore,* ***users of remote servers*** *such as the* ***Windows AD or LDAP are not supported****.*

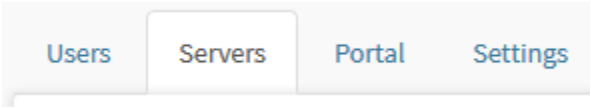
Along the next sections, we will analyze other features that use the MFA as a validation means.

UTM - Authentication - Servers tab

In this screen it is possible to configure the servers for user authentication.

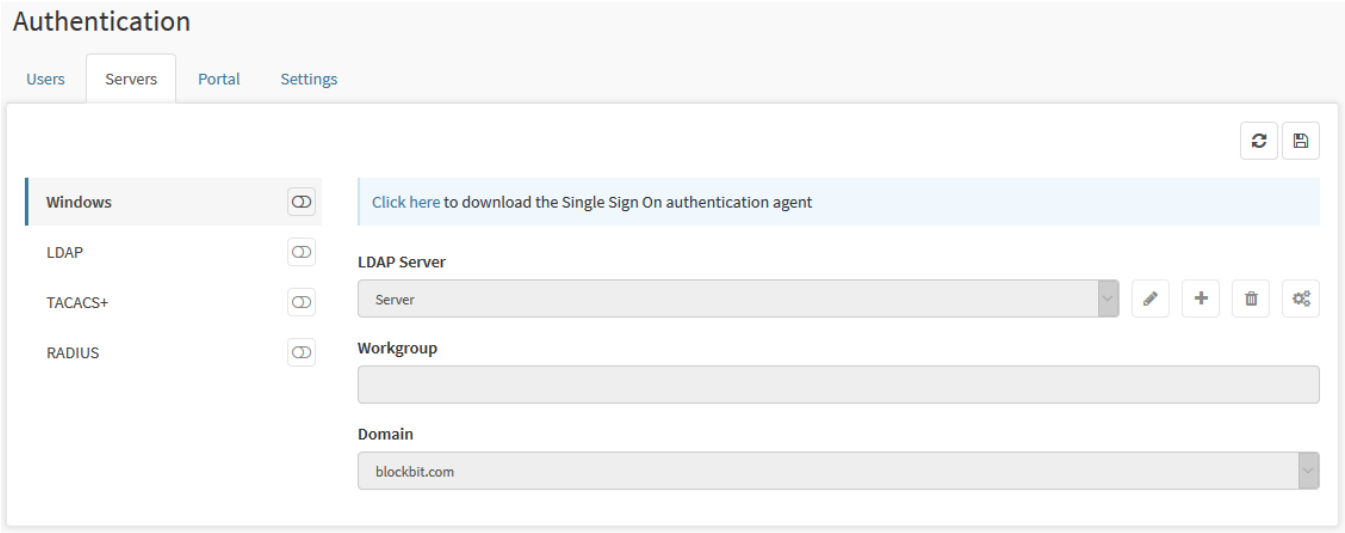
The configuration of the servers is simple, but requires some care not to generate errors or failures in the synchronism in the forest of your Windows AD server.

To make these settings, click on the Servers tab:



Servers tab

The screen will appear, as shown by the image below:



Authentication - Servers

This screen has the following side tabs:

- *Windows Server;*
- *LDAP Server;*
- *TACACS+ Server;*
- *RADIUS Server.*

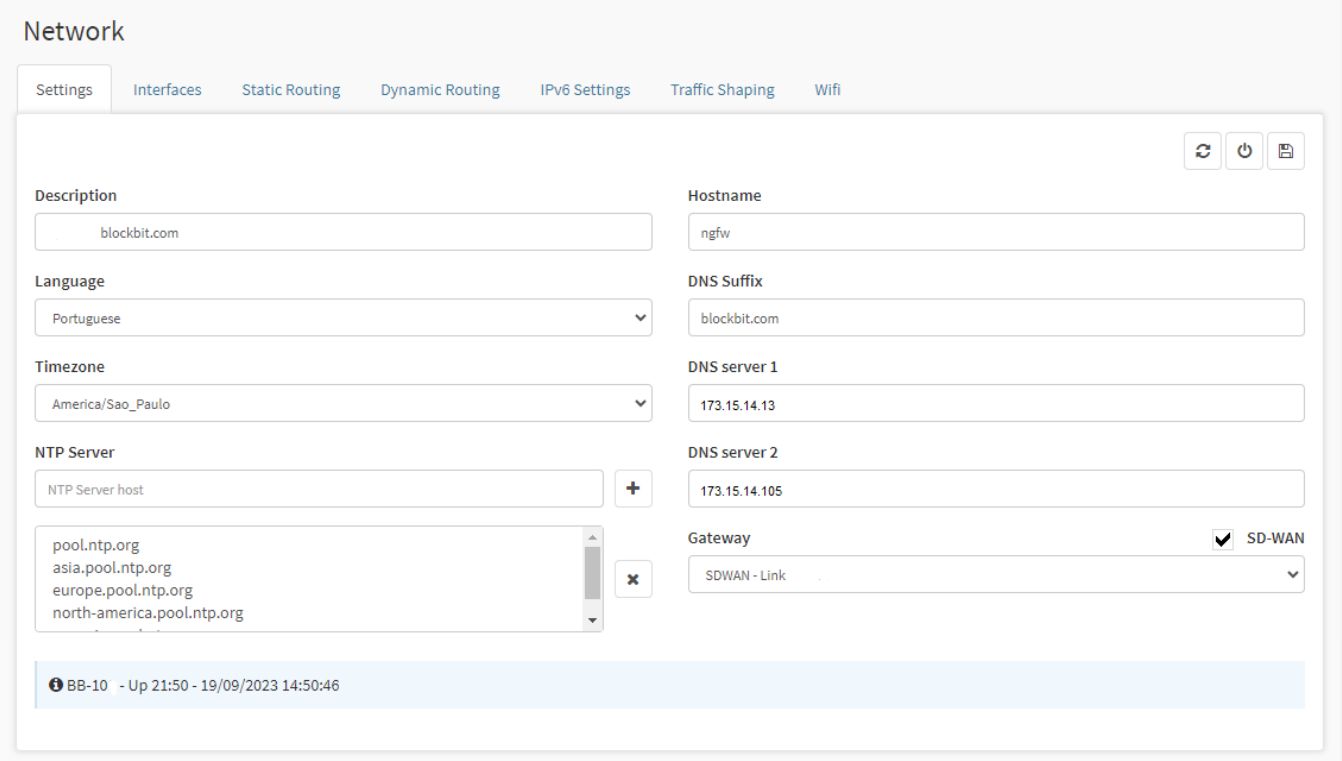
Next, each component of this screen will be analyzed.

UTM - Servers - Windows AD / LDAP domain integration and timing

Integrated authentication supports **Windows AD** and/or **LDAP** authentication and is based on user base synchronization. Windows AD synchronization-based authentication requires the BLOCKBIT NGFW server to be integrated into the domain. Finally, authentication based on authentic LDAP synchronism directly on the LDAP basis, without requiring integration to the domain.

For the domain integration process, it is necessary to ensure that the server is properly configured for joining the Windows server domain controller.

Initially, go to Network - Settings.

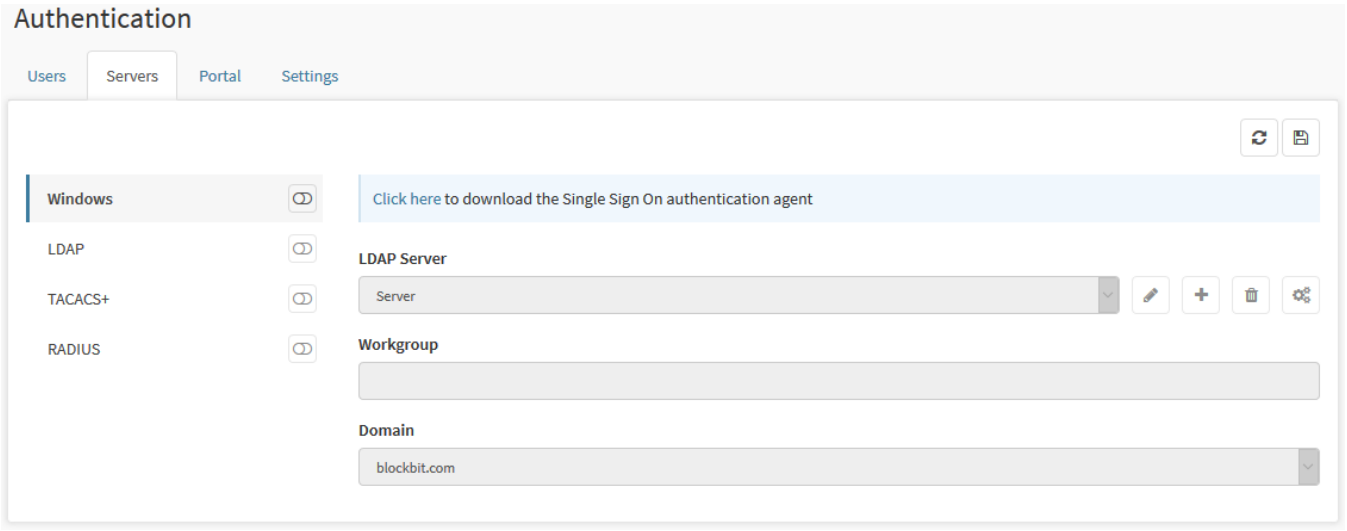


Settings - Network Settings

In the Settings tab, make sure that the address of the DNS server 1 field is set to the IP address of the domain controller of your Windows server, where user synchronism is meant to be applied.

We can configure the user authentication item.

Back to Authentication - Servers.

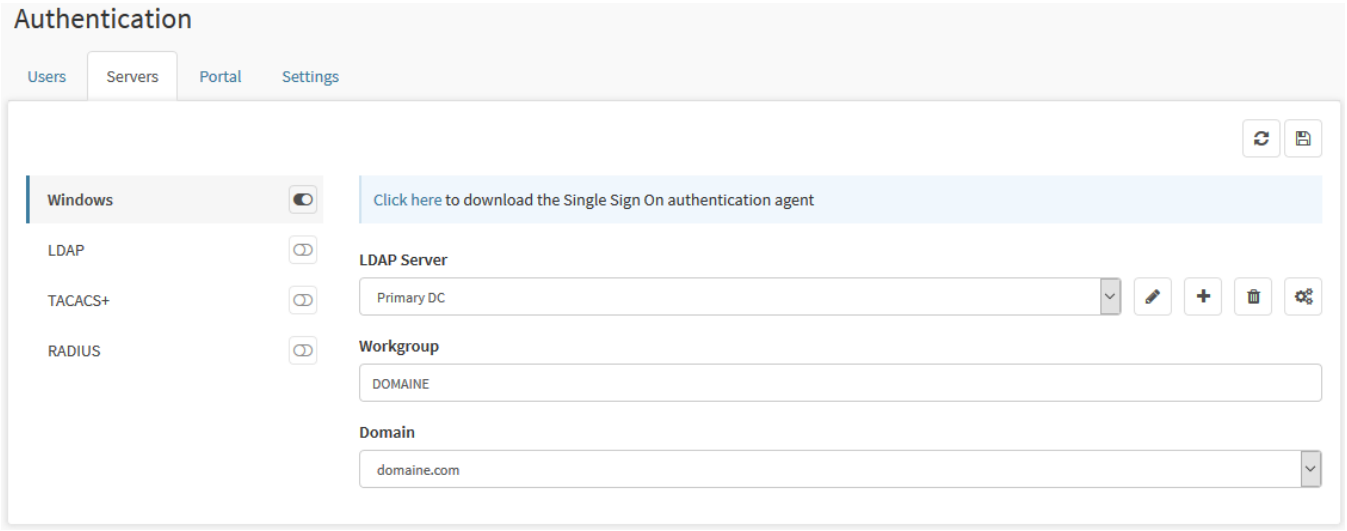


Authentication - Servers

For user authentication we have the Windows and LDAP side tabs**.**

The configuration is simple, but requires some care not to generate errors or failures in the synchronism in the *forest* of your Windows AD server.

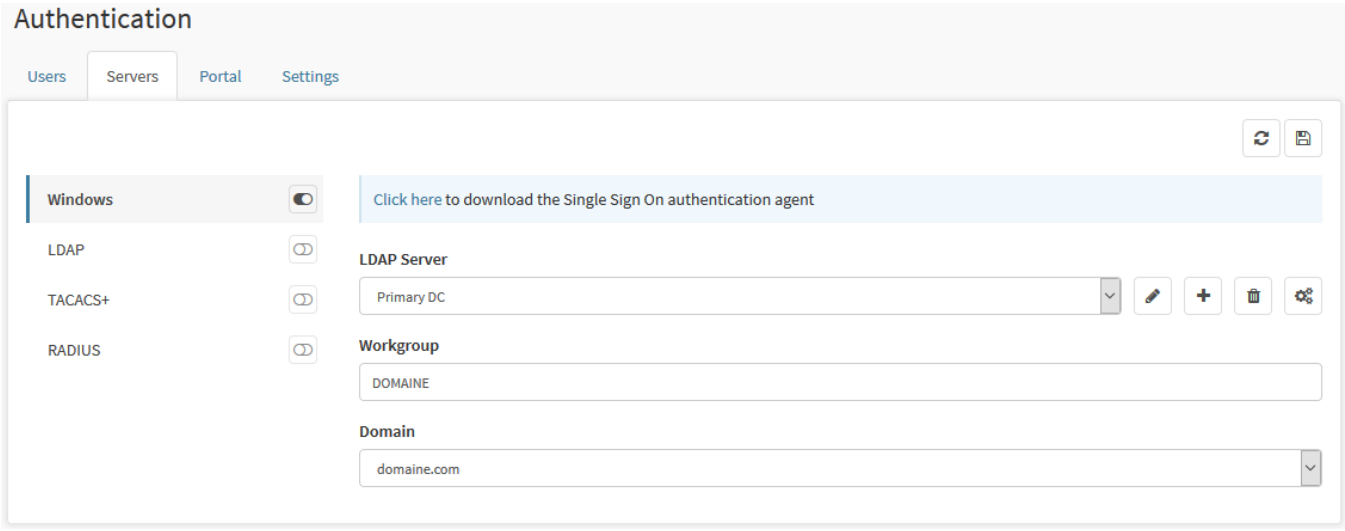
Below we will specify some fields:



Authentication - Windows Server

If the fields are unavailable, enable them using the **[**  **]** option located in front of the left side tabs.

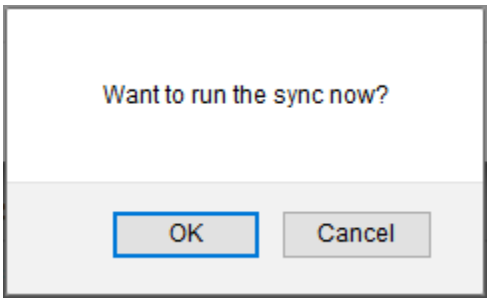
- ***LDAP Server*:** Select the ldap profile that was created using the **[**  **]** button on this same screen. For more information, check the Windows Server page or the LDAP server page. Ex.: *Primary DC*;
- ***Workgroup*:** Defines the domain controller workgroup. E.x. DOMAINE;
- ***Domain*:** Defines the domain to which users will be imported. E.x.: **domaine.com**.



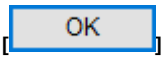
Authentication - Windows Server

Fill in the fields and click **[**  **]** to save the settings.

After saving, by clicking on the [] button and clicking on “Synchronize” it is possible to perform the synchronism manually (for more information, see Windows Server - Sync Interval).



Authentication - Want to run the sync now?

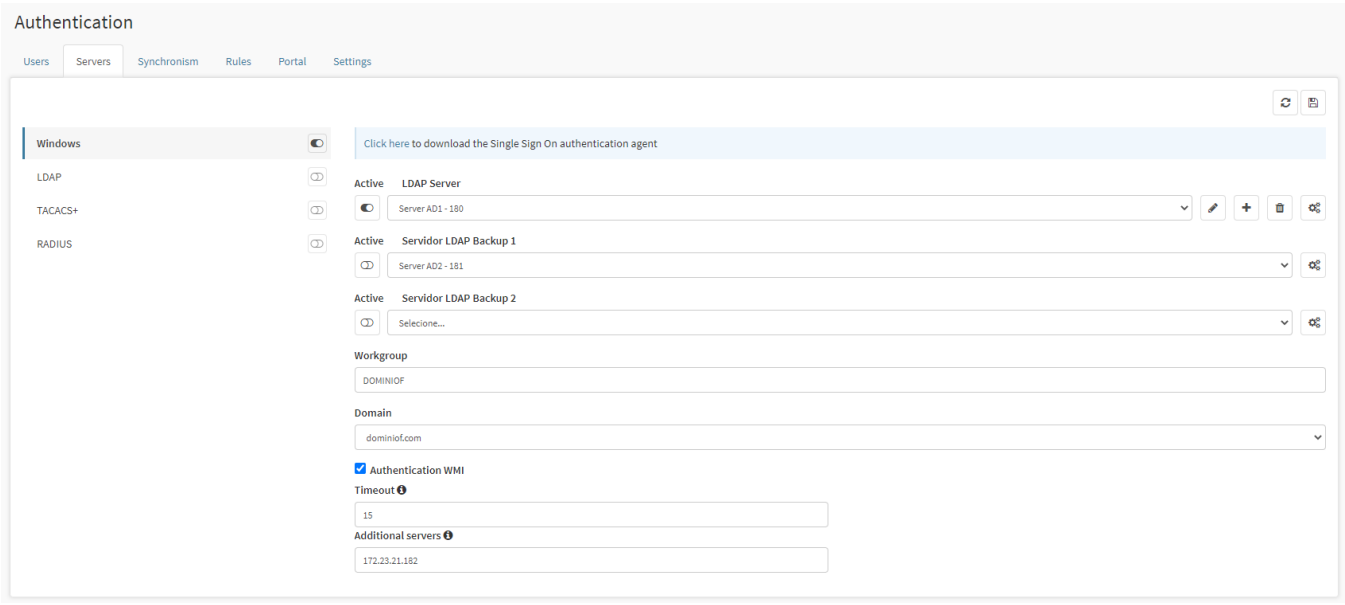
After clicking the **[**  **]** button, the system will start synchronizing with the remote server.

After confirming, it will be necessary to access the command queue **[**  **]** and apply for the synchronism to happen. For more information on the command queue access the page: UTM - Command queue.

The principle of configuring the synchronism of an LDAP base is the same. However, it is important to consider that the filter and search base settings on an LDAP server are created by those who implement the directory service and it is necessary to have this information to be successful in the configuration.

UTM - Servers - Windows Server

Through this screen it is possible to configure the Windows authentication server.



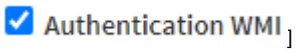
Authentication - Faded Windows Server field

If all options are grayed out as in the image above, select the **[**  **]** icon, located on the right side of the “Windows Server” option. Click on it to activate it, it should look like this: **[**  **]**. Once this is done, the options will be available for editing and the Windows Server server can be configured correctly.

It is possible to set up a maximum of 3 Windows servers this way, in case the primary server becomes unavailable, the authentication will happen in the second and the same way in case both are off, it will be held in the third. In case the first server comes back on, the authentication then will be done on it.

To register more servers, just proceed the same way done to register the first one.

Below we will specify some fields:

- ***LDAP Server*:** Select the LDAP profile that was created by clicking the add **[**  **]** button. Ex.: *Primary DC*;
- ***Workgroup*:** Defines the domain controller workgroup. E.x. DOMINIOC;
- ***Domain*:** Defines the domain into which users will be imported. Ex.: *dominioc.com*.
- ***WMI Authentication***: Mark this option [] to use this type of authentication;
- ***Timeout***: Configure the time the session will take to logout due to inactivity, with a minimum of 10 seconds and a maximum of 600 seconds of inactivity;
- ***Additional Servers***: Field menat for the insertion of aditional authentication servers. In case of more than one, they must be separated by comas.

After filling in the fields, in the upper right corner, next to the sync button, you can see the **[**  **]** button, it has the function of saving the changes made in the "servers" of the "Windows Server" panel.

To add a Windows Server, check this *Windows Server - Add Server* page.

Single Sign On Authentication

This procedure is approved for Windows Server 2012, Windows Server 2008 and Windows Server 2016.

The BLOCKBIT NGFW SSO agent does not need to be distributed among Windows domain devices (workstations). It is an agent that needs to be made available only on the Windows server that owns the domain controller and maintains the AD (Active Directory) on your network, with the role of integrating and synchronizing users.

The SSO client acts integrated with AD login events. Therefore, any device that logs into AD will have its session authenticated at NGFW, this includes other operating systems that somehow join AD.

Windows Management Instrumentation - WMI (Agentless Authentication)

Windows Management Instrument (WMI), consists into specifications for devices and applications management consolidation in Windows Server corporate networks.

These specifications are factory set in the W10, W8, Millenium, 2000, XP and Server 2003, 2012, 2016 and 2019 Windows versions. For previous systems, like Windows 98 and NT 4.0 it can be downloaded and installed.

Warning

In the Blockbit NGFW, the WMI service is similar to the SSO Agent, however IT IS NOT necessary to install the Agent in the AD (Active Directory).

It's necessary to enable the checkbox in the authentication screen - servers - Windows, "WMI Authentication", and insert the timeout right bellow, that is the time within which the NGFW will check the user's sessions with the AD (Active Directory).

Note: The WMI service works only in the Windows authentication method.

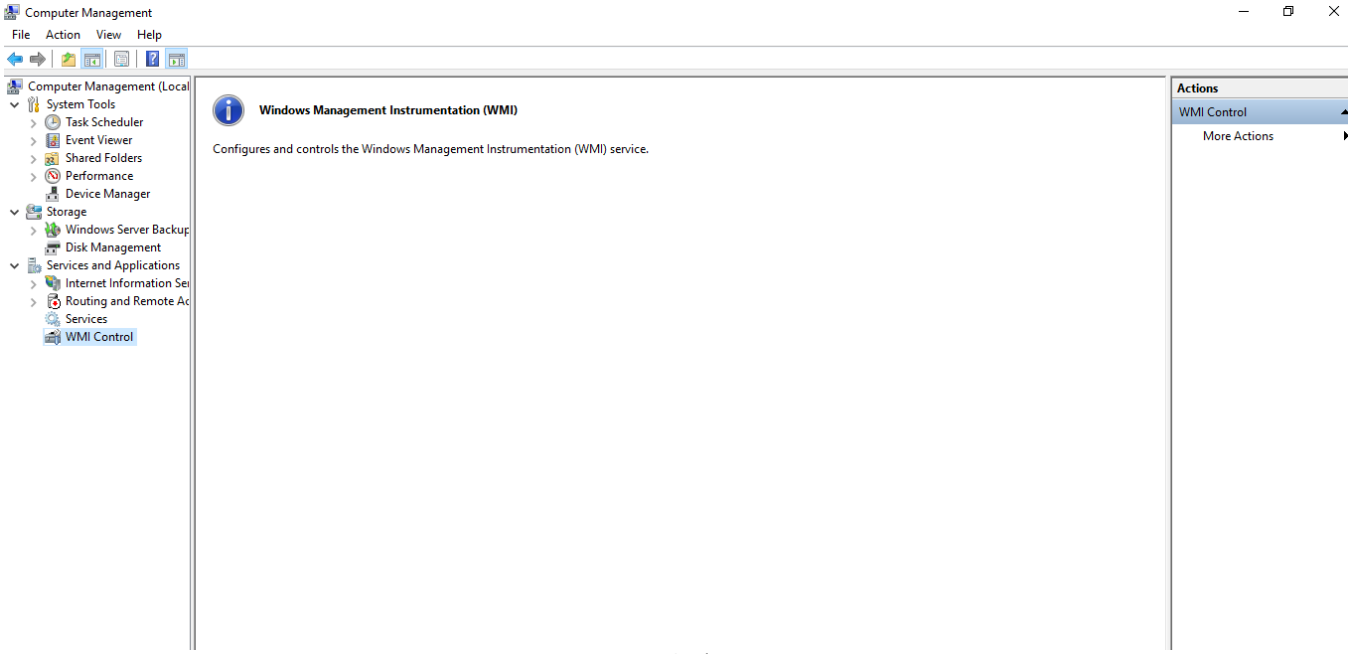
Timeout data:

Default timeout: 15 seconds
Minimum timeout: 10 seconds
Maximum timeout: 600 seconds

WMI - Checkbox and Timeout field

The AD's manager users are set from default with all of the necessary permissions for the WMI to work. In case it's necessary to allow another user who's not a manager, for the WMI to work, follow the steps bellow:

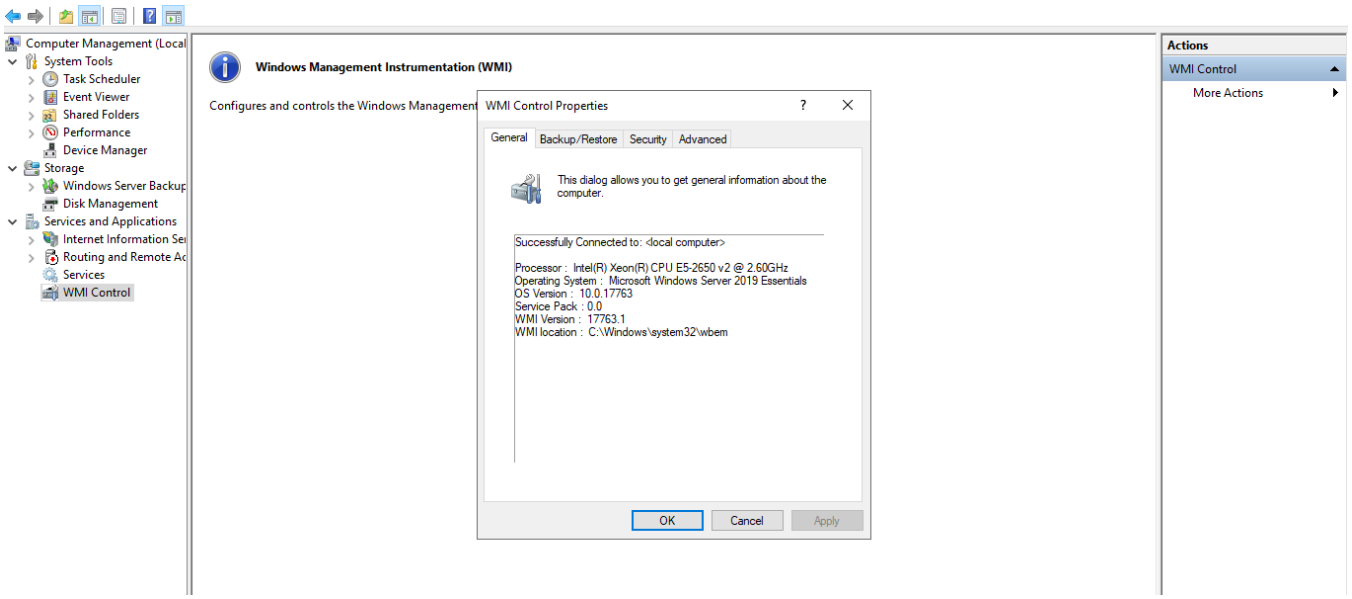
1. In the target server, go to Administrative Tools Computer Management.



WMI - Settings

2. Expand Services and Applications.

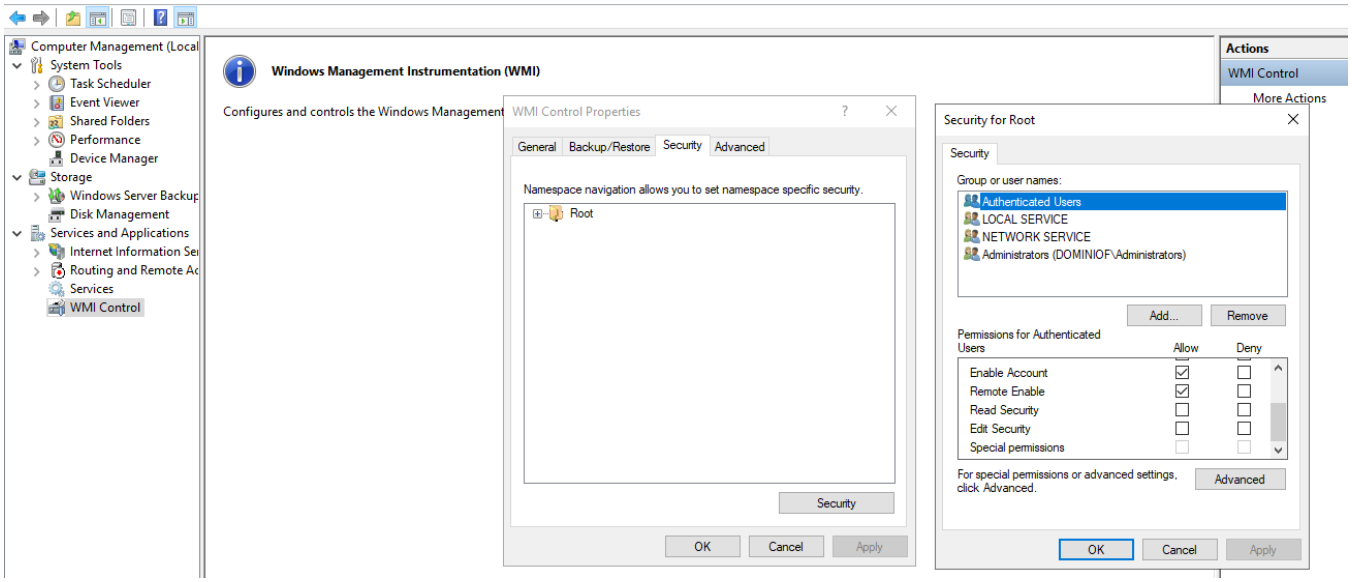
3. Right-click in WMI control and select properties.



WMI - Properties

4. In the WMI control properties window, select the Security tab.
5. Click security.

6. Click "Add" in case of adding a user like a monitor.



WMI - Remote Enable

7. Mark "Remote Enable" for the user or group of users that requires the WMI data.
8. Check if the connection has been successfuly done.

Requirements for running the SSO agent

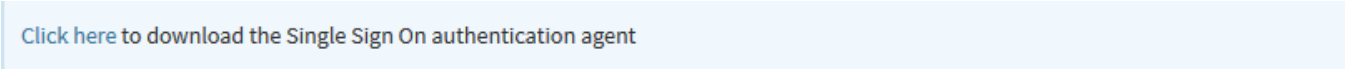
For the BLOCKBIT SSO agent to work and integrate with the scheduling and login event service, the system requires the installation of the **.NET Framework version 3.5** application on the Windows server.

To install **.NET version 3.5**, use the installation features available in the **"Server Manager"** panel, item **[Add roles and features]** of your Windows server.

Download the SSO agent file from your network's Windows AD server and save it to a local directory.

In BLOCKBIT NGFW access the *Windows Server* Menu

Click the link to download the Single Sign On authentication agent. As shown below:

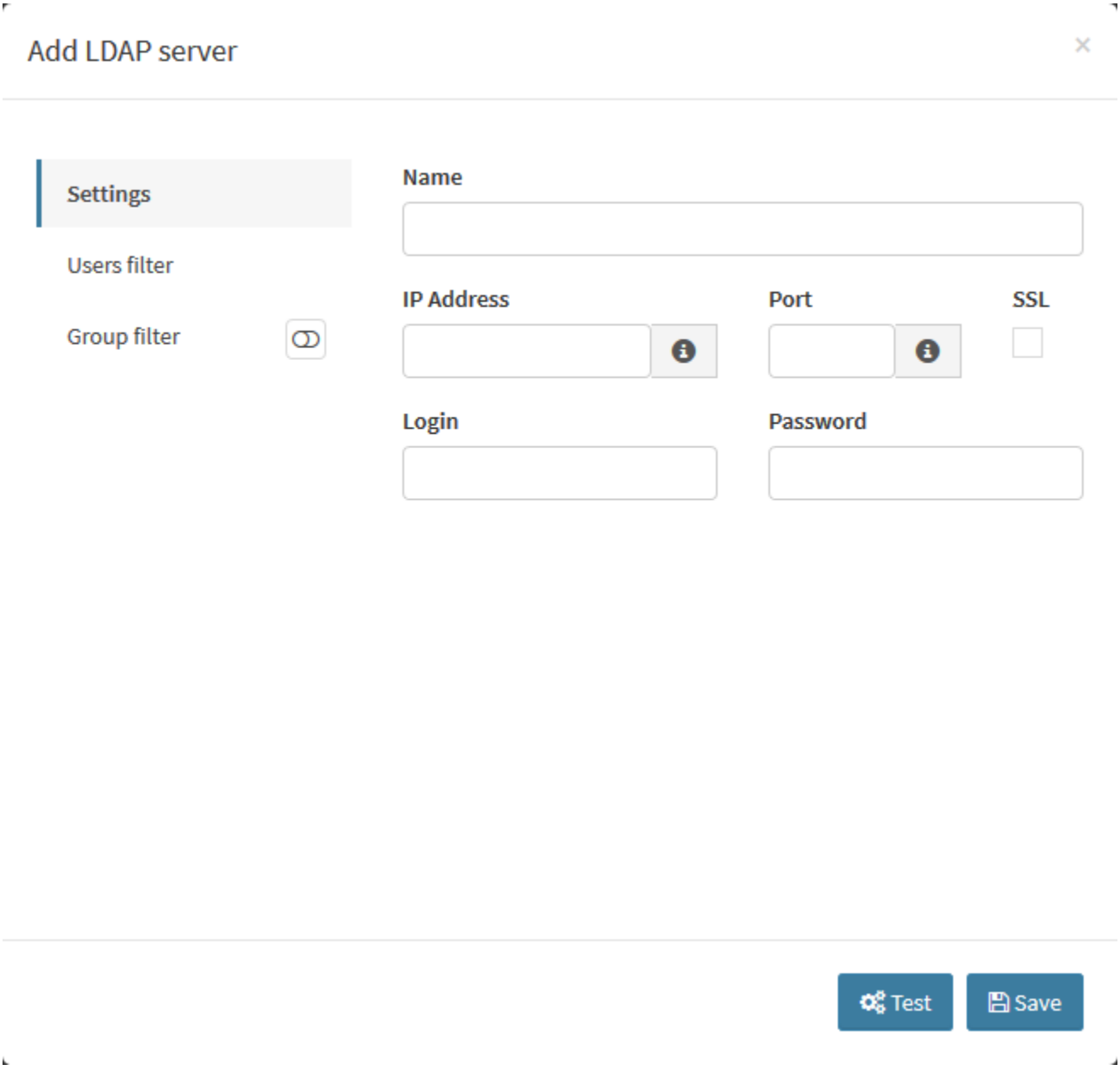


Click here to download the Single Sign On authentication agent

For the SSO agent installation and configuration procedure - follow the setup tutorial procedures on our website (or click here).

UTM - Windows Server - Add Server

To add a new server click on the [+] button. And the screen below will be displayed:



Authentication - Add Windows Server

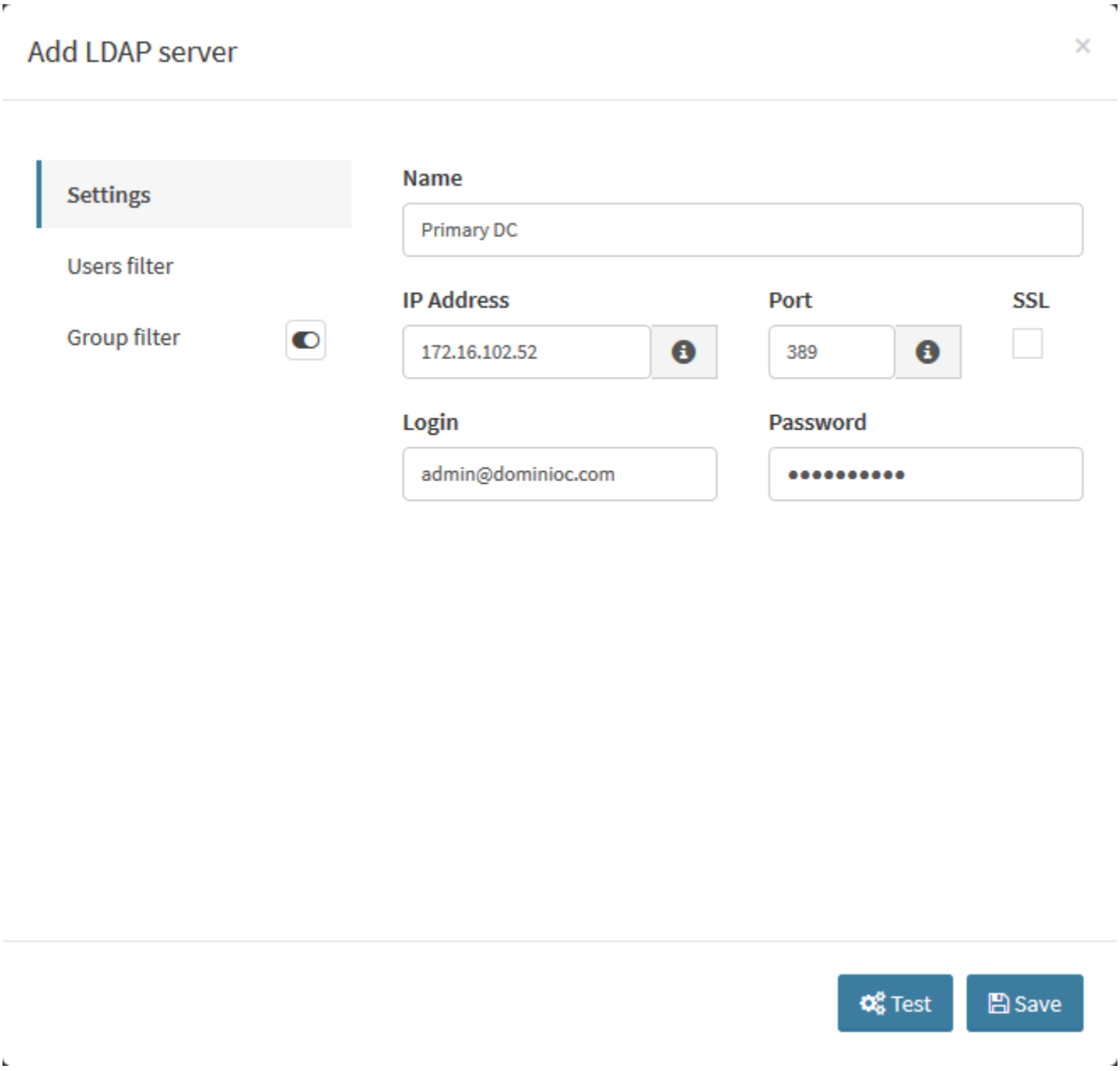
This window contains the following side tabs:

- *Settings;*
- *Users filter;*
- *Group filter*.

Next we will analyze each component of this window.

UTM - Windows Server - Add Server – Settings tab

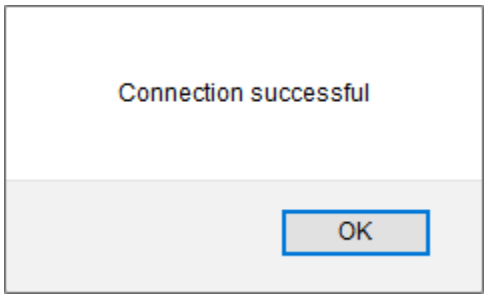
In this tab the fields that refer to the Windows AD server administration credentials can be configured.



Authentication - Add Windows Server – Settings

- ***Name*:** Set a name for the sync connection. Ex.: *Primary* DC;
- ***IP Address*:** Set the IP address of the domain controller. Ex.: 172.16.102.191;
- ***Port*:** Set the port to connect to the domain controller, if the service is running on SSL, check the SSL option **[ ]**. Ex.: 389;
- ***Login*:** Define a Windows server user with LDAP search rights, usually a member of the administrators group. Ex: "administrador@dominioc.com";
- ***Password*:** Set user password.

By clicking on the **[Test]** button, the system will validate the credentials of access to the Windows server.

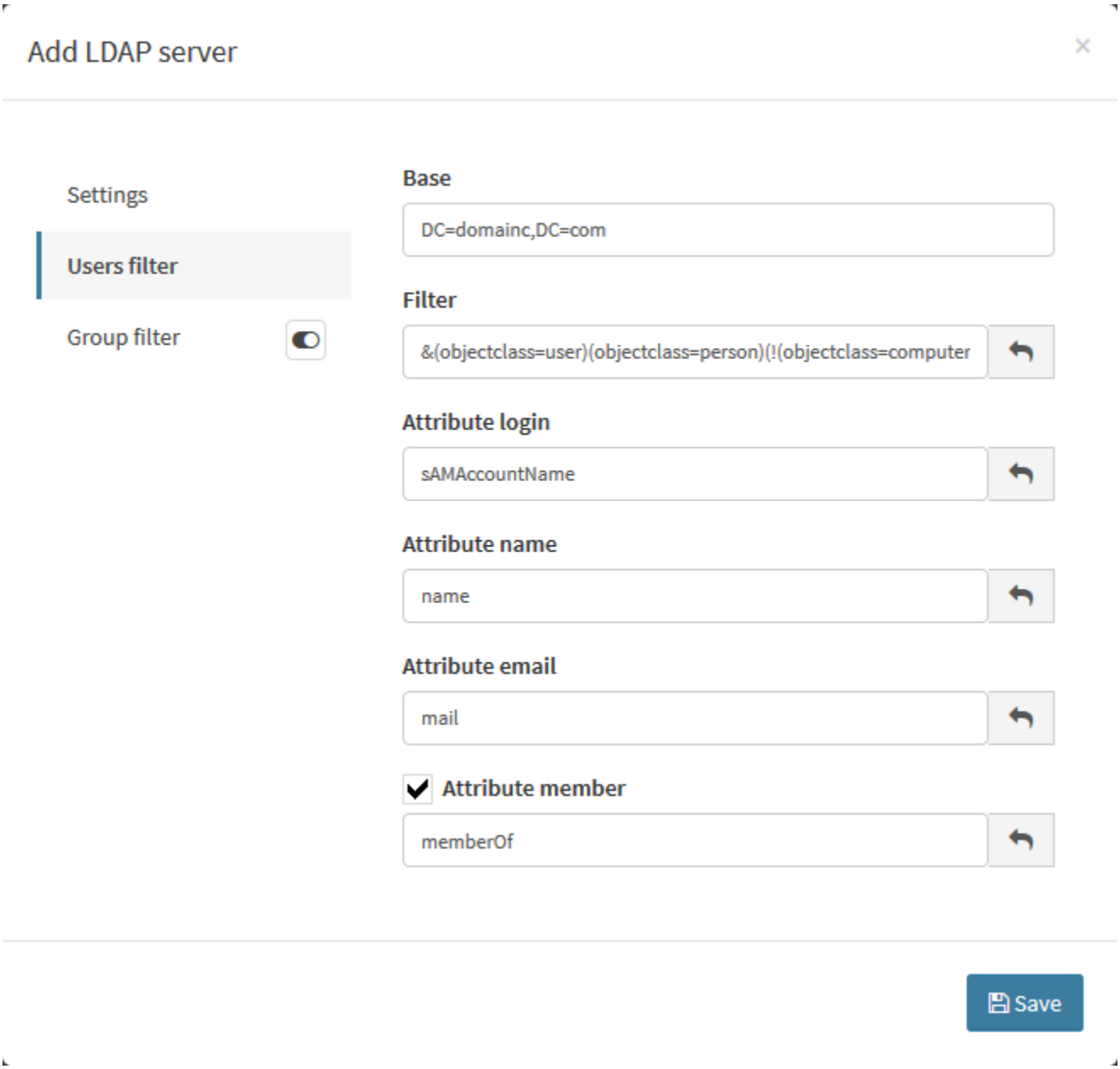


Authentication – Connection Successful

To continue configuring, access the next side tab: *Users filter*.

UTM - Windows Server - Add Server – Users filter tab

In this tab, the fields referring to the user search base and their respective filters in the LDAP base of the Windows AD server are configured.



Authentication – Add Windows Server – User filter

Configure the “Base”, “Filter”, “Attribute login”, “Attribute name”, “Attribute email” and “Attribute member” fields according to the LDAP database of the respective Windows server.

These fields are filled in automatically when you click the **[ ]** button.

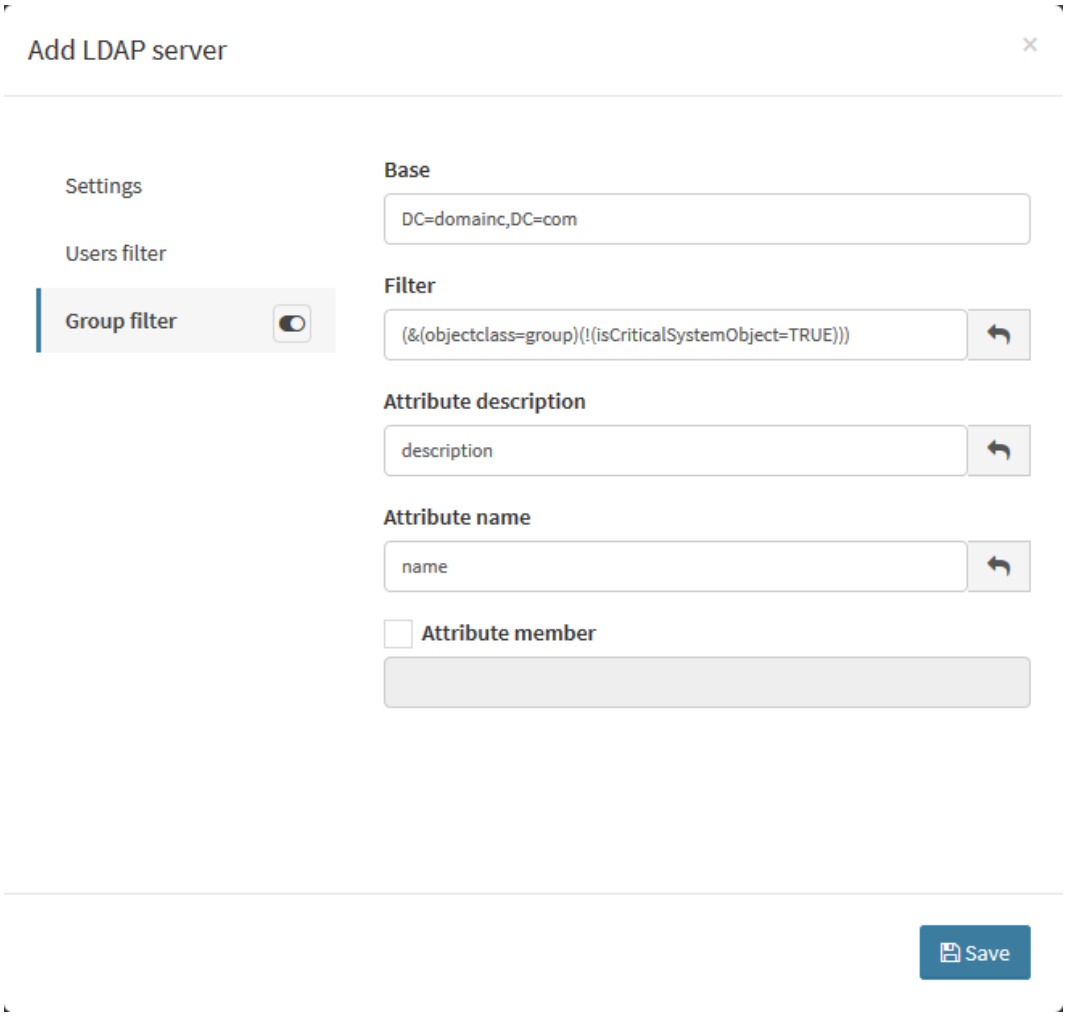
For the configuration of a Windows AD server with LDAP, it is necessary to manually change the fields to have the values below:

- ***Filter:*** *(&(objectclass=user)(objectclass=person)(!(objectclass=computer)))*
- ***Attribute login:*** *userPrincipalName*

To continue configuring, access the next side tab: Group Filter.

UTM - Windows Server - Add Server – Group filter tab

In this tab it is possible to enable group synchronism by clicking on the [ ] button. Configure the fields “Base”, “Filter”, “Description attribute” and “Member attribute” according to the LDAP database data of the respective Windows server.



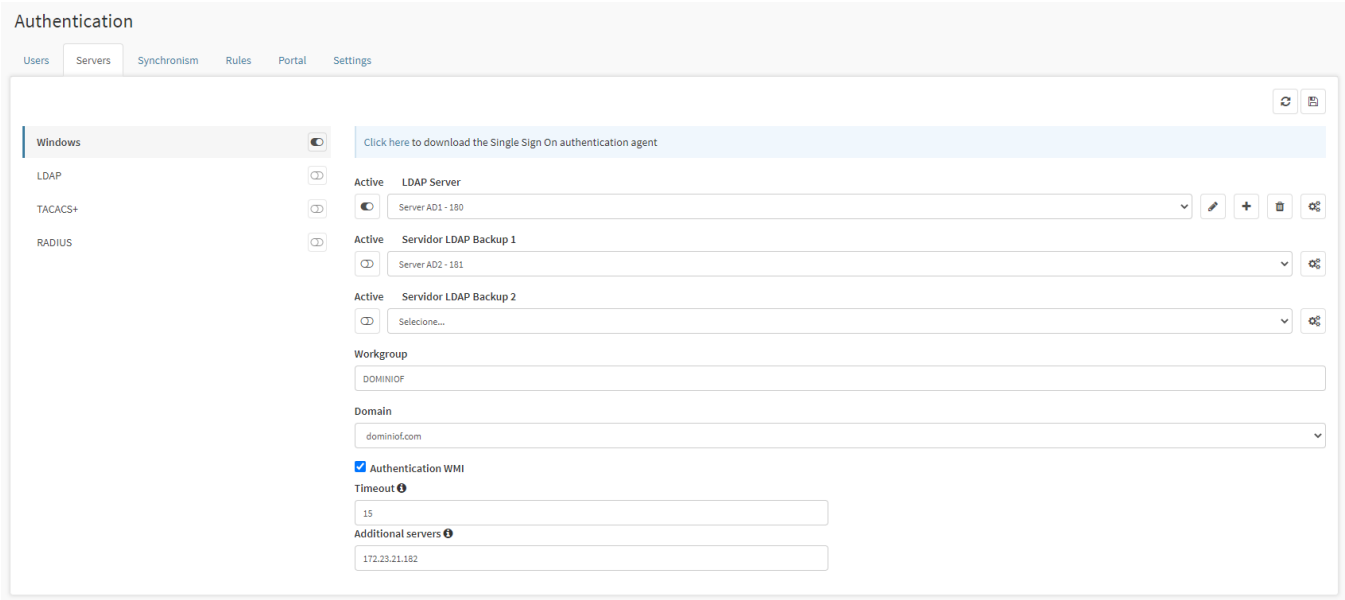
Authentication – Add Windows Server – Group filter

These fields are filled in automatically when you click the [ ] button

Fill in the fields and click on [Save], the “servers” tab will be automatically displayed.

The principle of configuring the synchronism of an LDAP base is the same. However, it is important to consider that the settings of filters and search base on an LDAP server, are created by those who implement the directory service and therefore, it is necessary to be in possession of this information to be successful in the configuration.

After saving and completing the set up, you will be redirected to the main page, and if you need to set up additional servers, just follow the same steps you did for the first server.

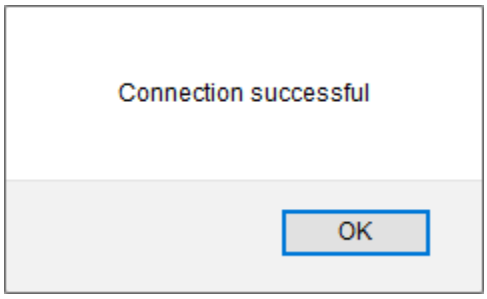


Authentication - Windows Server

UTM - Windows Server – Connection Test

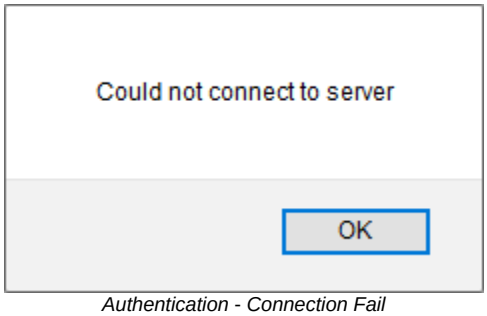
After adding a connection, it is possible to perform a connection test by clicking on the connection test [ ] icon, it is equivalent to the [Test] button on the addition panel.

If the connection was successful, the following window will be displayed:



Authentication – Connection Successful

If the connection fails, the following window will be displayed:

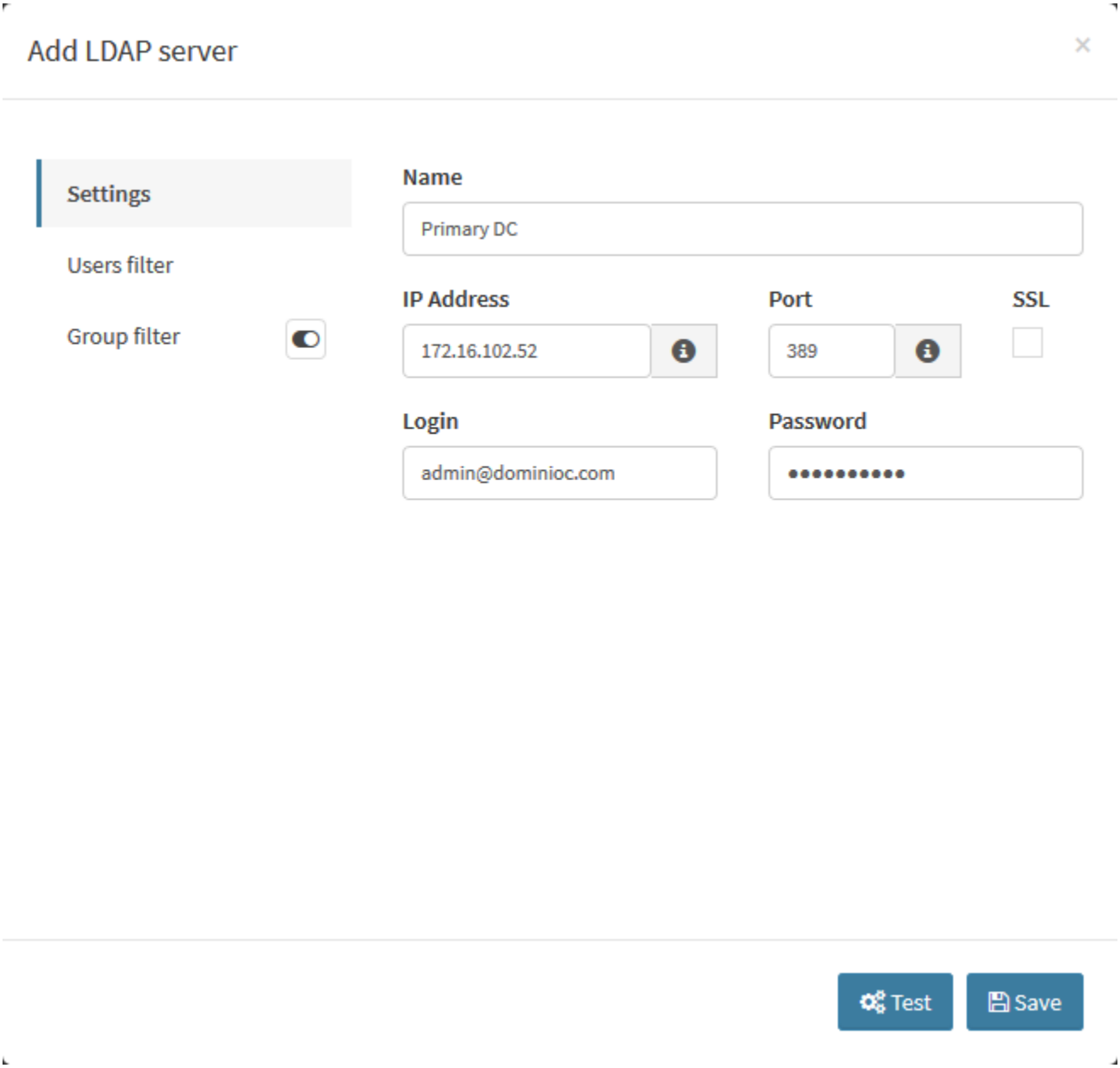


Authentication - Connection Fail

UTM - Windows Server - Edit Server

It is possible to edit the information located on the server selected in the selection box below “LDAP Server”, to do so, select the desired server in the selection box and clicking the edit button **[ ]**.

The following window will appear:

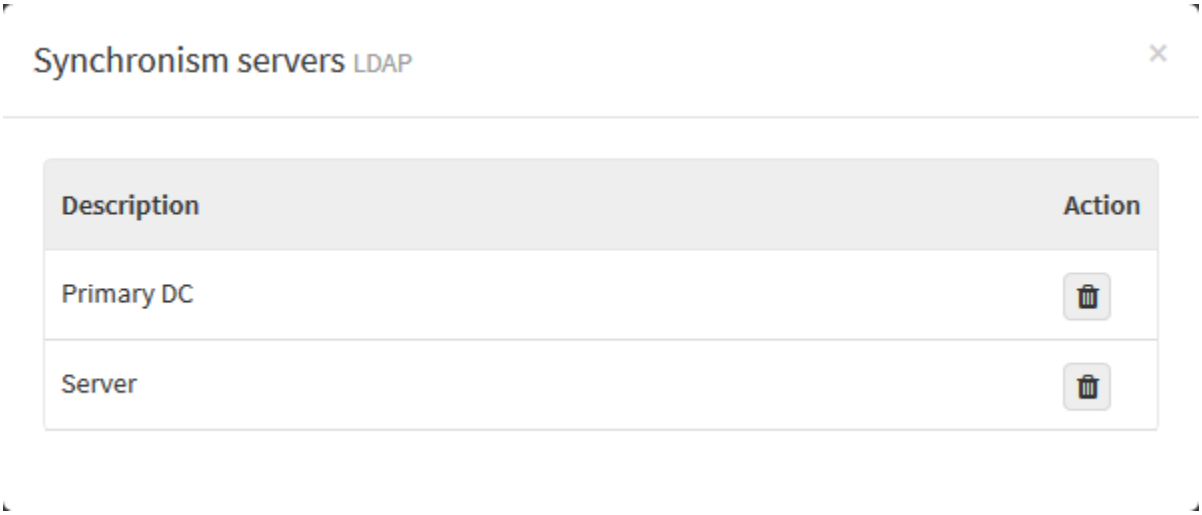


Authentication - Edit Domain

After completing the necessary changes click on the **[ ]** button to save the changes.

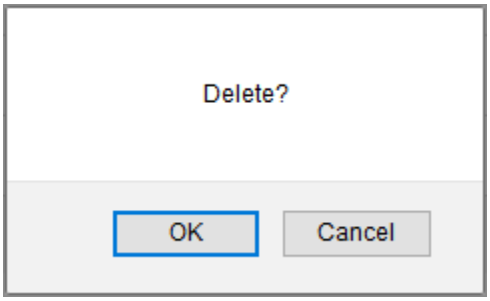
UTM - Windows Server – Remove Server

To remove any server, click on the delete icon **[ ]**, a panel with all created servers will be displayed, as shown in the image below:



Windows server – Removal Panel

Choose the server you want to be removed and click the delete **[ ]** icon to remove the desired server. A confirmation message will be displayed:

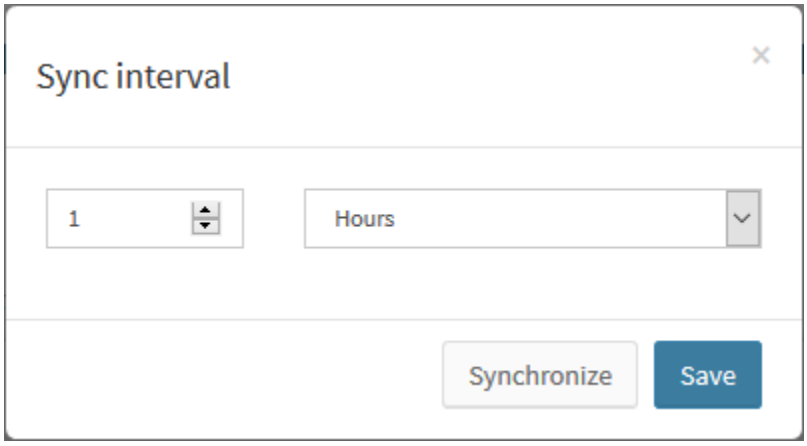


Windows server – Removal Message

Click **[OK]** to remove the selected server, or click **[Cancel]** to make no deletion.

UTM - Windows Server – Sync Interval

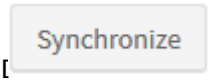
In the upper right corner, you can see the **[**  **]** button, where the synchronism interval is determined. As shown in the image below:

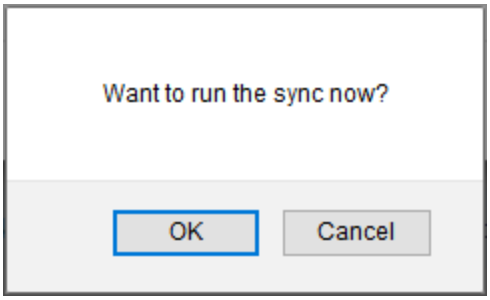


Authentication – Sync Interval

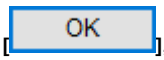
In the first selection box it is possible to determine a numerical value, with 1 being the minimum value.

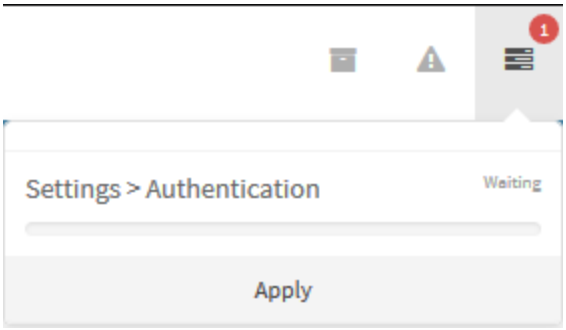
In the second checkbox it is possible to choose which time period to use, the two options are **hours** or **minutes**.

In addition, when clicking on the **[**  **]** button, it is possible to start the synchronism immediately, a verification message will appear asking for confirmation of this action, as illustrated by the image below:



Authentication - Want to run the sync now?

When clicking on **[**  **]**, the system will generate the apply in the queue **[**  **]**, it will be necessary to access the command queue [] and apply the synchronism. For more information on the command queue access the page: UTM - Command queue.



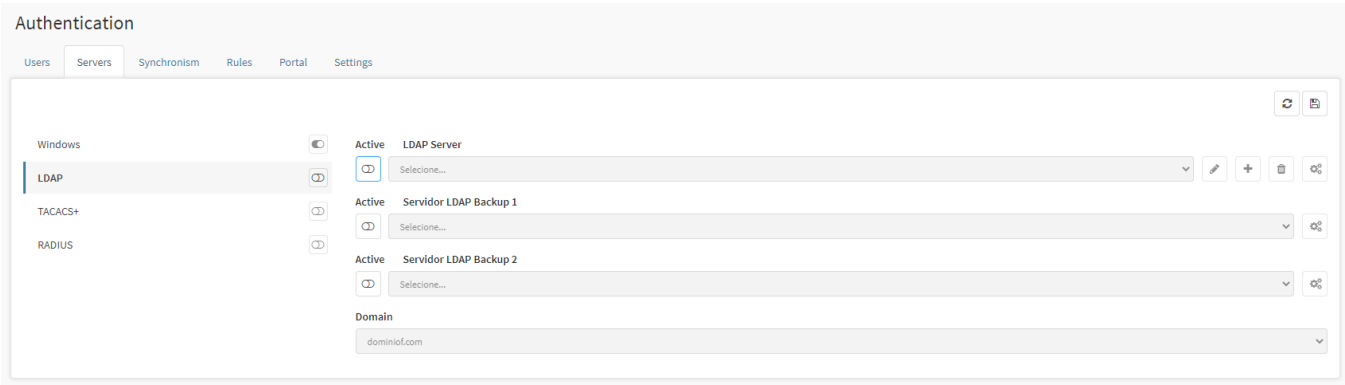
Authentication - Apply queue

Having the sync interval determined, click the **[Save]** button to save the settings made, or click outside the panel or the “x” at the top of that panel to discard the changes.

The principle of configuring the synchronism of an LDAP base is the same. However, it is important to consider that the filter and search base settings on an LDAP server are created by those who implement the directory service and it is necessary to have this information to be successful in the configuration.

UTM - Servers - LDAP Server

Through this screen it is possible to configure the LDAP authentication server.



Authentication - Faded LDAP Server field

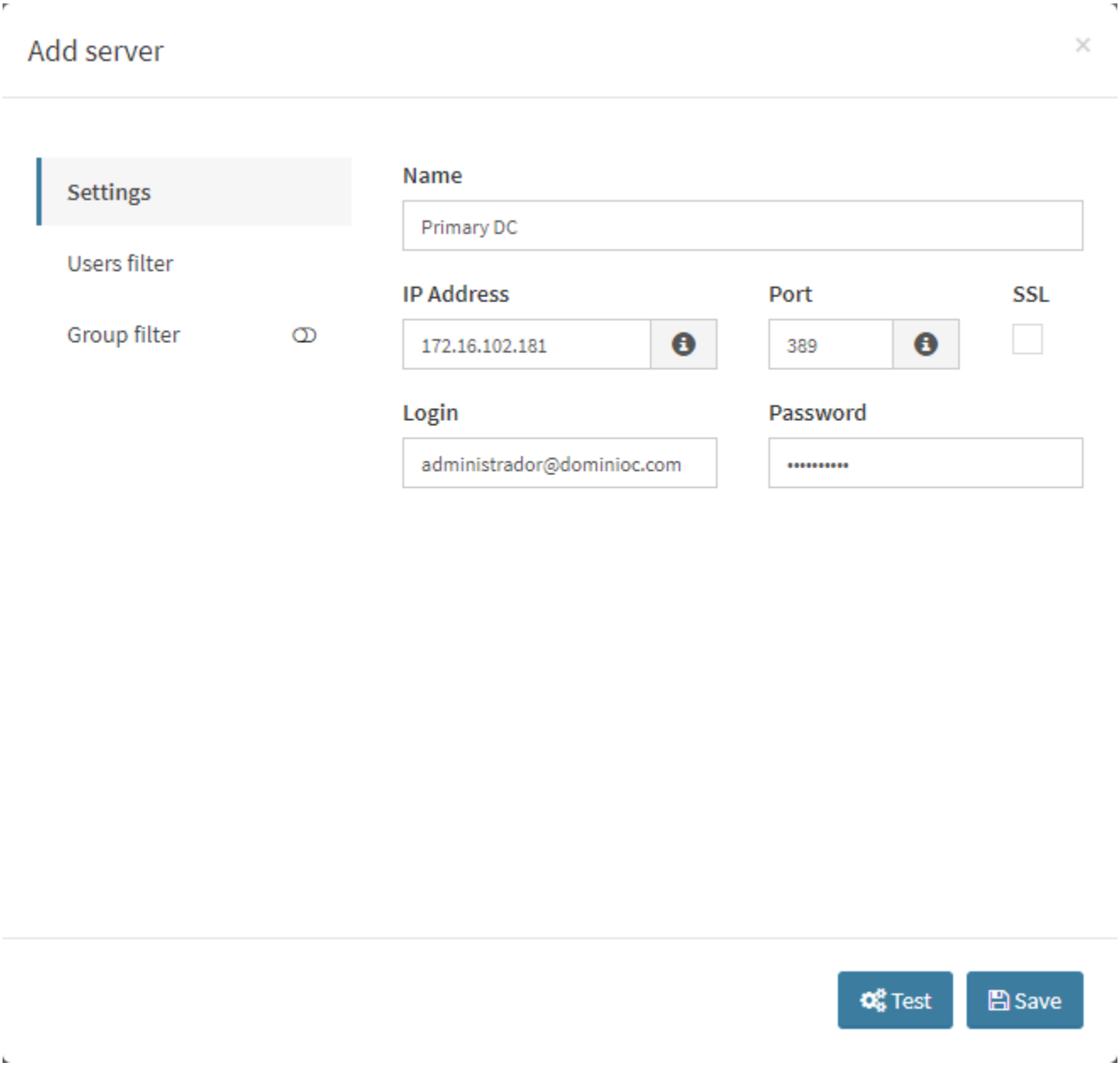
If all options are grayed out as in the image above, select the activate **[**  **]** icon, located on the right side of the “LDAP Server” option. Click on it in order to activate it, it should look like this: activate **[**  **]**. Once this is done, the options will be available for editing and the ***LDAP Server*** can be configured correctly.

It is also possible to register up to two extra servers for cases in which the primary server is off. The procedure is the same for all three, as we will see in the LDAP Server - Add Server, in the link bellow.

To add an LDAP Server, check this page LDAP Server - Add Server.

NGFW - LDAP Server - Add Server

To set up a new server click on the **[+]** button. And the screen below will be displayed:



Authentication - Add Windows Server

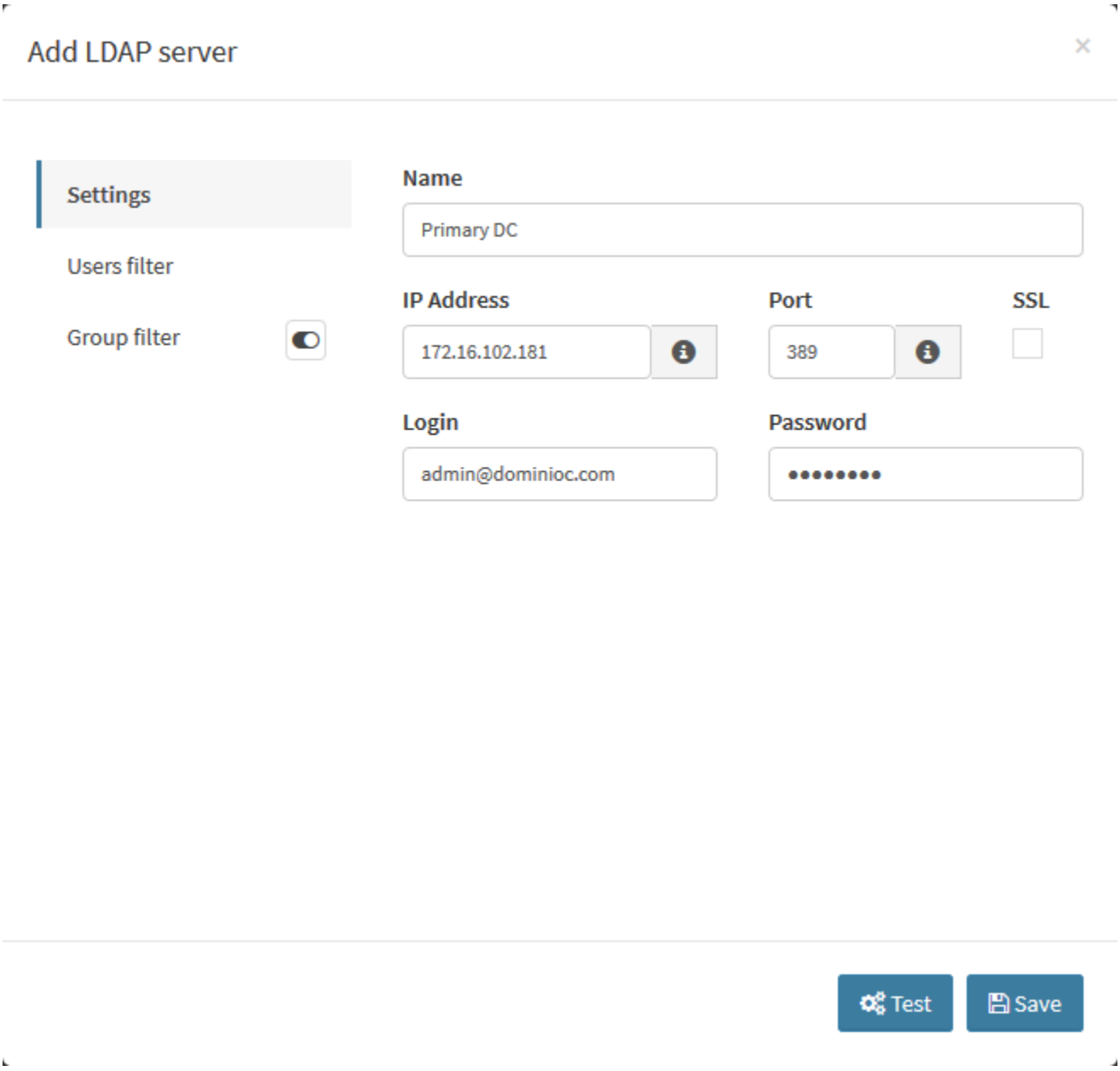
This window contains the following side tabs:

- *Settings;*
- *Users filter;*
- *Group filter.*

Next we will analyze each component of this window.

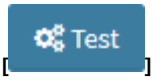
UTM - LDAP Server - Add Server – Settings tab

In this tab, the fields that refer to the LDAP server administration credentials can be configured.

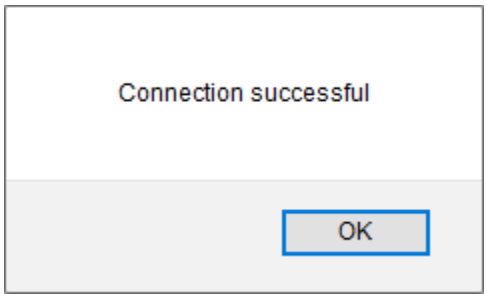


Authentication - Add Windows Server – Settings

- ***Name*:** Set a name for the sync connection. Ex.: *Primary DC*;
- ***IP Address*:** Set the IP address of the domain controller. Ex.: 172.16.102.191;
- ***Port*:** Set the port to connect to the domain controller, if the service is running on SSL select the option “SSL”. Ex.: 389;
- ***Login*:** Define a Windows server user with LDAP search rights, usually a member of the administrators group. Ex: “administrador@dominioc.com”
- ***Password*:** Set user password.

By clicking on the **[** 

] button, the system will validate the credentials of access to the Windows server.

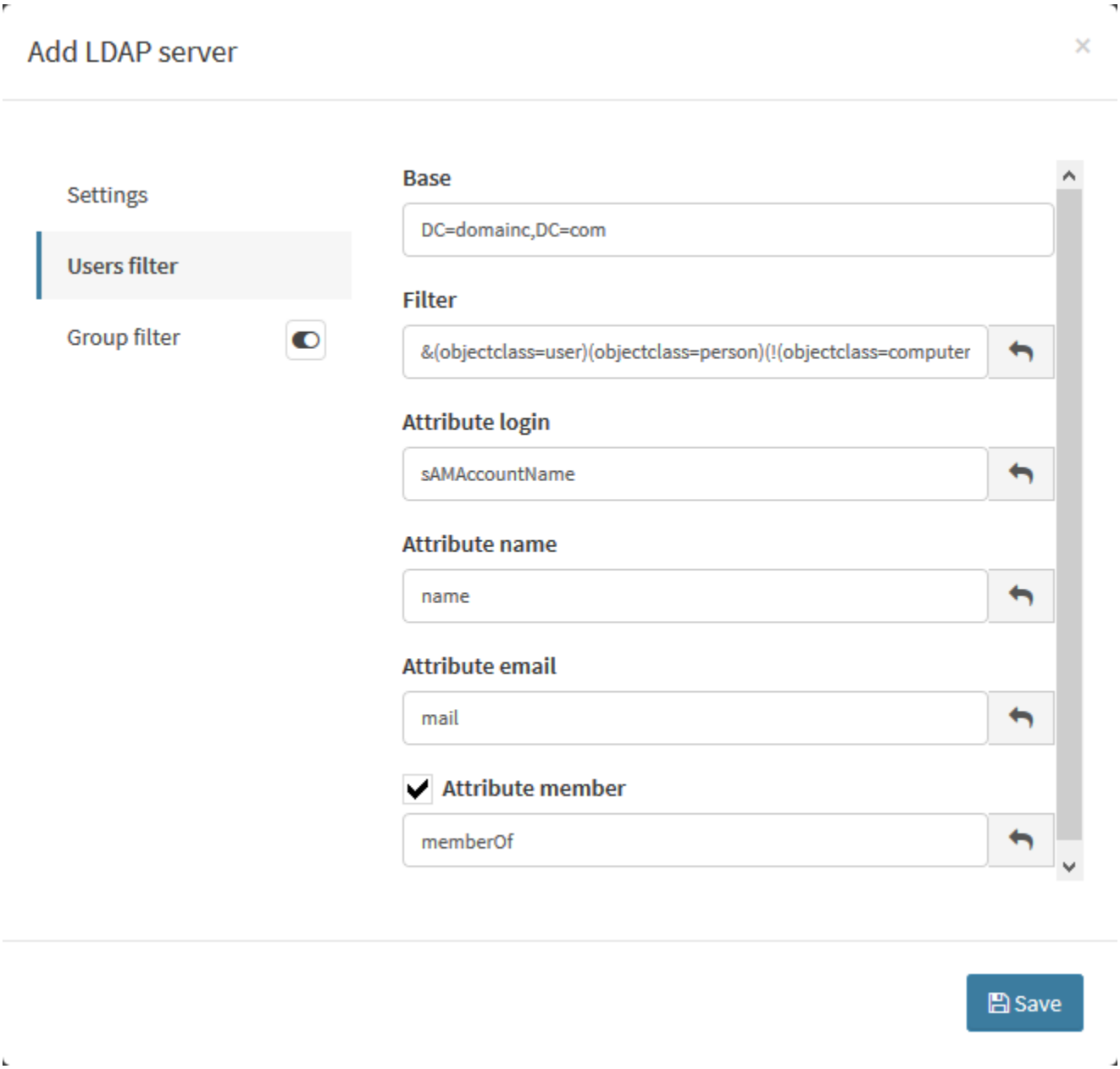


Authentication – Connection Successful

To continue configuring, access the next side tab: *Users filter*.

UTM - LDAP Server - Add Server – Users filter tab

In this tab, the fields referring to the user search base and their respective filters in the LDAP base of the Windows AD server are configured.



Authentication – Add Windows Server – User filter

Configure the “Base”, “Filter”, “Attribute login”, “Attribute name”, “Attribute email” and “Attribute member” fields according to the LDAP database of the respective Windows server.

These fields are filled in automatically when you click the **[ ]** button.

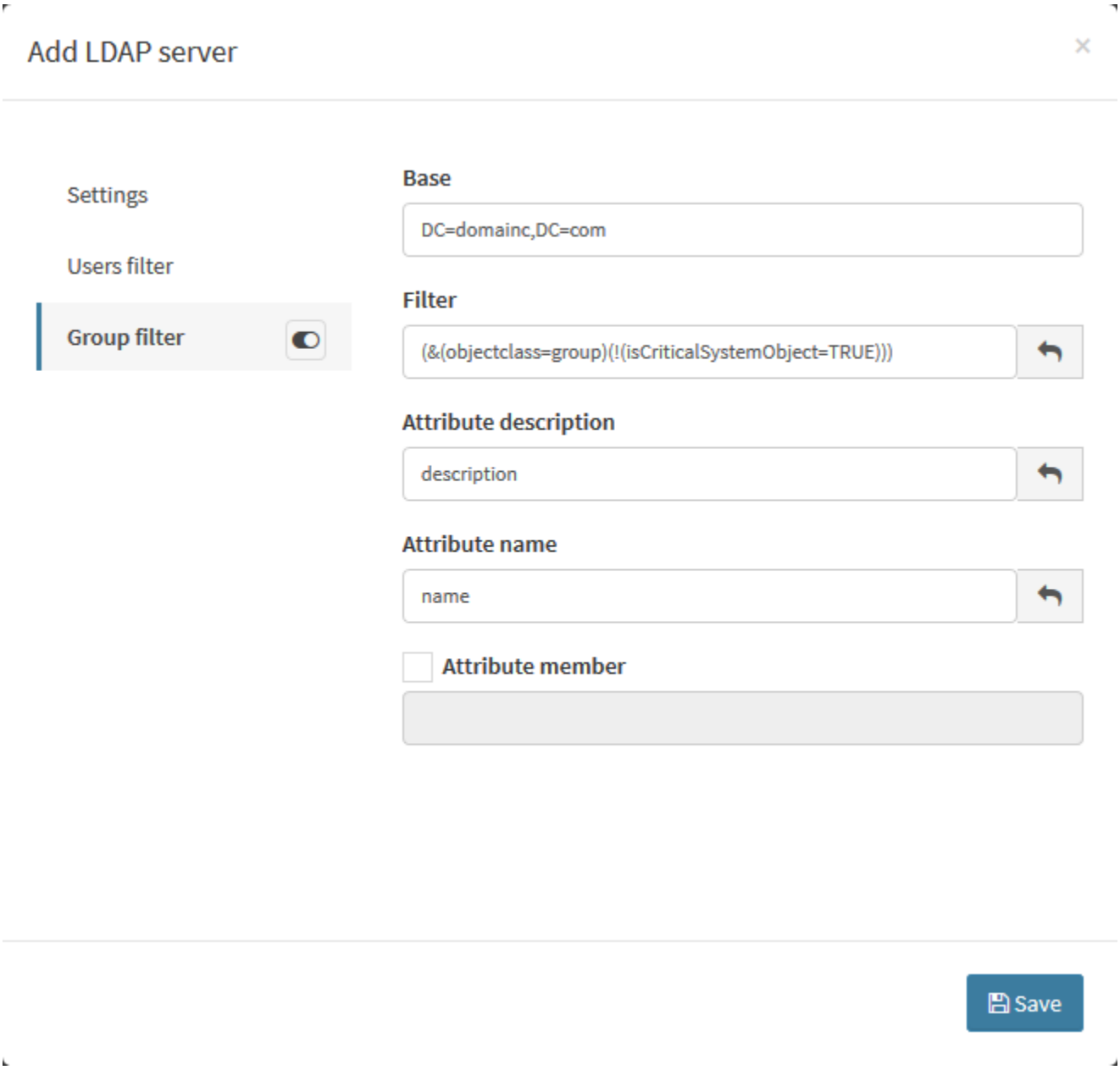
For the configuration of a Windows AD server with LDAP, it is necessary to manually change the fields to have the values below:

- ***Filter:*** *(&(objectclass=user)(objectclass=person)(!(objectclass=computer)))*
- ***Attribute login:*** *userPrincipalName*

To continue configuring, access the next side tab: *Group Filter*.

UTM - LDAP Server - Add Server – Group filter tab

In this tab it is possible to enable group synchronism by clicking on the [ ] button. Configure the “Base”, “Filter”, “Attribute description” and “Attribute member” fields according to the LDAP database of the respective server.



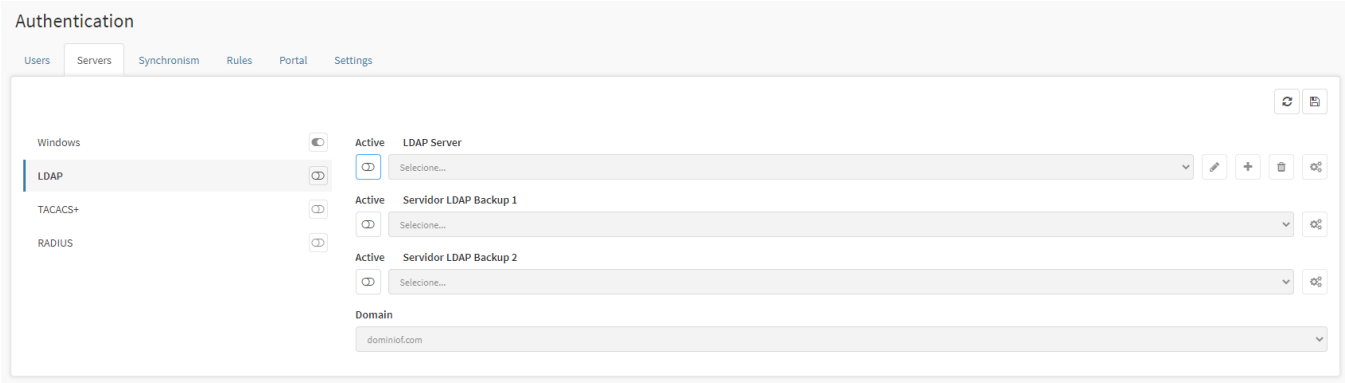
Authentication – Add Windows Server – Group filter

These fields are filled in automatically when you click the [ ] button.

Fill in the fields and click on [Save], the “servers” tab will be automatically displayed.

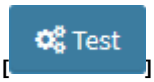
The principle of configuring the synchronism of an LDAP base is the same. However, it is important to consider that the filter and search base settings on an LDAP server are created by those who implement the directory service and therefore, it is necessary to have this information in order to be successful in the configuration.

After saving and concluding the set up, you will be redirected to the main page, and if you need to set up the additional servers, just follow the same steps you did for the first server.



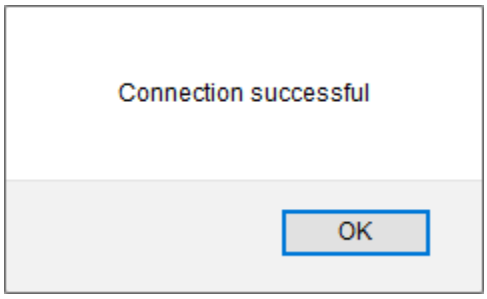
Authentication - Authentication LDAP Server

UTM - LDAP Server - Connection Test

After adding a connection, it is possible to perform a connection test by clicking on the connection test **[**  **]** icon, it is equivalent to the **[** 

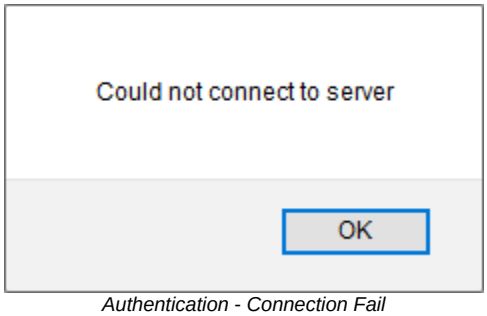
] button on the addition panel.

If the connection was successful, the following window will be displayed:



Authentication – Connection Successful

If the connection fails, the following window will be displayed:

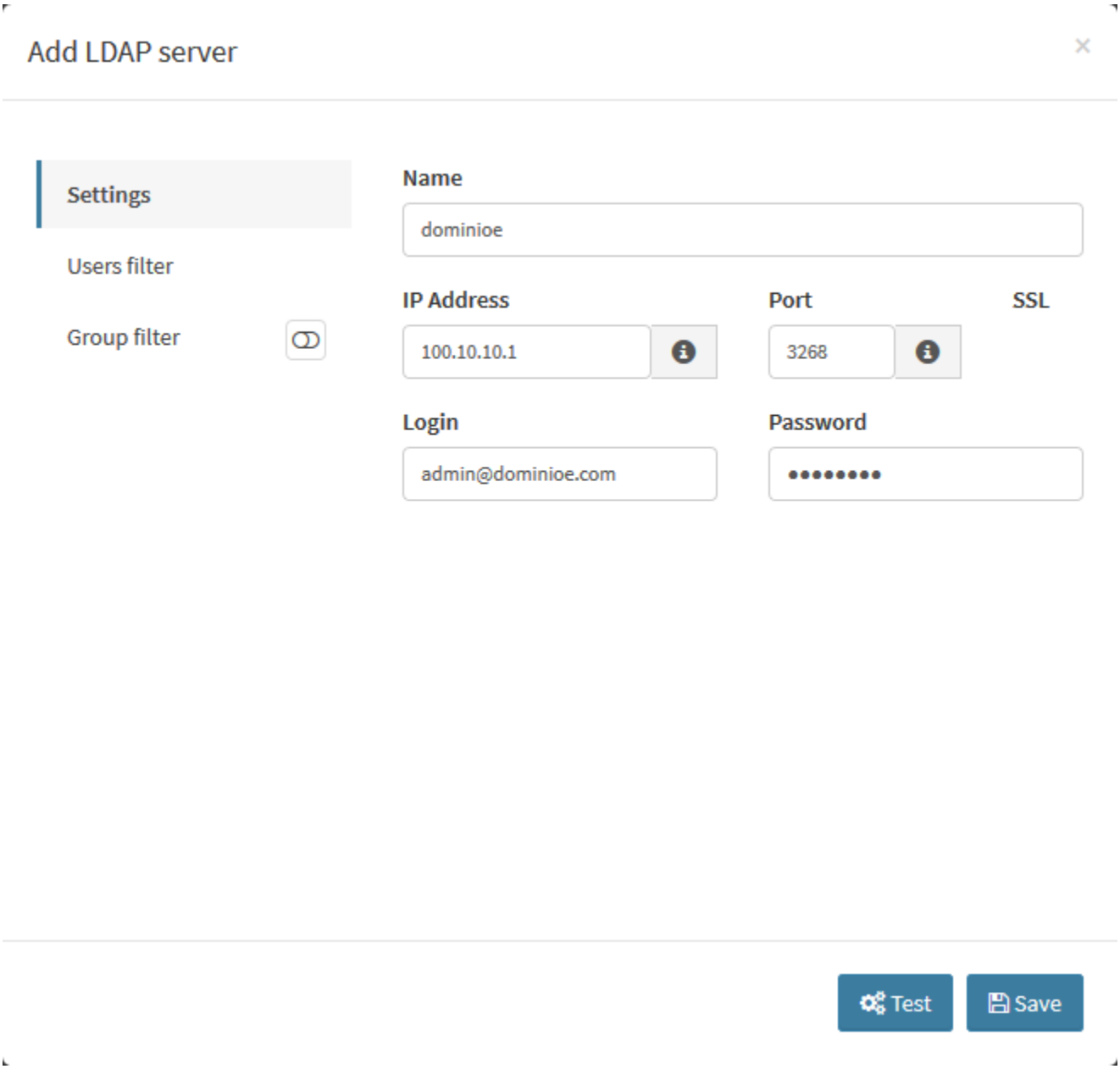


Authentication - Connection Fail

UTM - LDAP Server - Edit Server

It is possible to edit the information located on the server selected in the checkbox below “LDAP Server” and clicking on the edit button [ ].

The following window will appear:

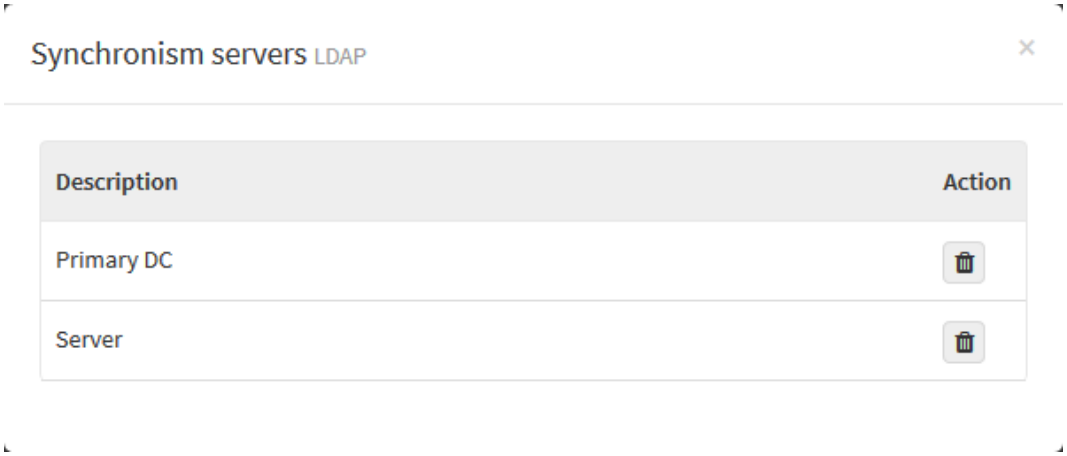


LDAP Server – Edit Domain.

After completing the necessary changes click on the [Save] button to save the changes.

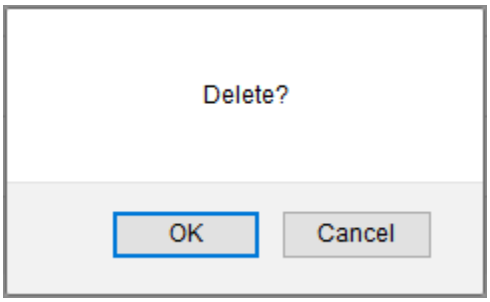
UTM - LDAP Server - Remove Server

To remove any server, click on the delete icon **[ ]**, a panel with all created servers will be displayed, as shown in the image below:



LDAP server – Removal Panel

Choose the server you want to be removed and click the delete **[ ]** icon to remove the desired server. A confirmation message will be displayed:

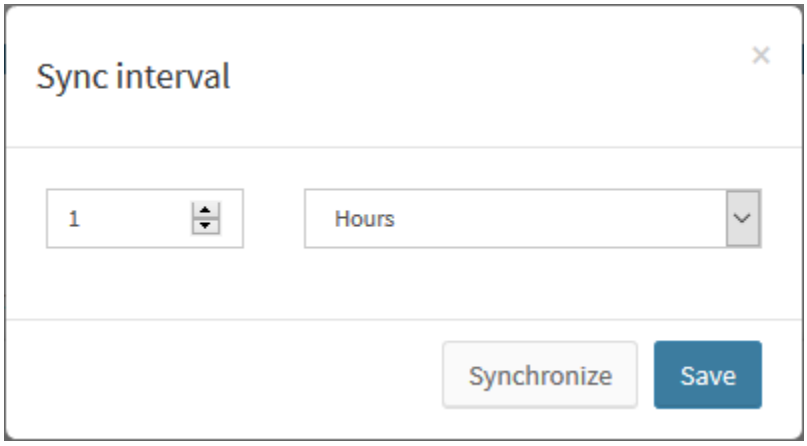


Windows server – Removal Message

Click **[OK]** to remove the selected server, or click **[Cancel]** to make no deletion.

UTM - LDAP Server - Sync Interval

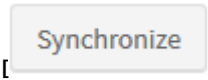
In the upper right corner, you can see the **[**  **]** button, where the synchronism interval is determined. As shown on the image below:

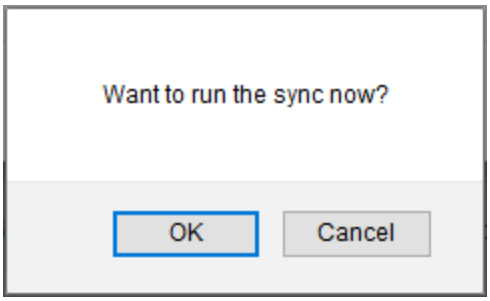


Authentication – Sync Interval

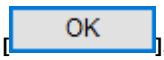
In the first selection box it is possible to determine a numerical value, with 1 being the minimum value.

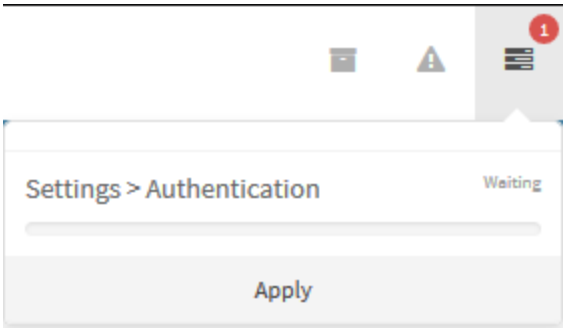
In the second checkbox it is possible to choose which time period to use, the two options are **hours** or **minutes**.

In addition, when clicking on the **[**  **]** button, it is possible to start the synchronism immediately, a verification message will appear asking for confirmation of this action, as illustrated by the image below:



Authentication - Want to run the sync now?

When clicking on **[**  **]**, the system will generate the apply in the queue, it will be necessary to access the command queue **[**  **]** and apply the synchronism. For more information on the command queue access the page: UTM - Command queue.



Authentication - Apply queue

Having the sync interval determined, click the **[Save]** button to save the settings made, or click outside the panel or the “x” at the top of that panel to discard the changes.

The principle of configuring the synchronism of an LDAP base is the same. However, it is important to consider that the filter and search base settings on an LDAP server are created by those who implement the directory service and it is necessary to have this information to be successful in the configuration.

UTM - Servers - TACACS+ Server

TACACS + is a set of interrelated protocols whose function is: To handle remote authentication and services related to moderating network access through a centralized server. TACACS + uses the TCP protocol on port 49, provides granular control and encrypts the content of each data packet during its transmission.

Among the various characteristics of TACACS + we can highlight:

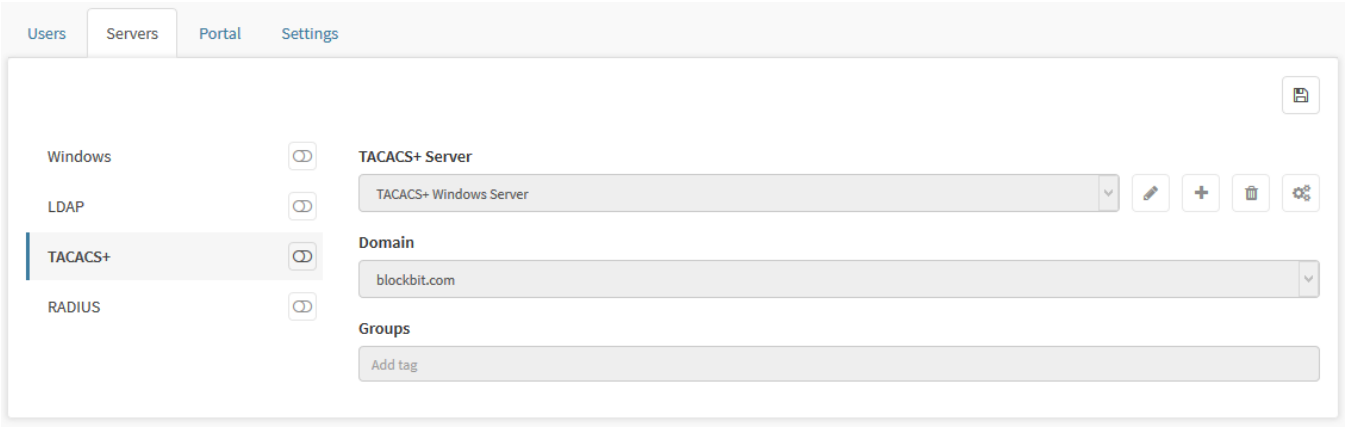
- Performance in TCP, eliminating transmission control mechanisms;
- Control of authentication, authorization and accounting services, allowing them to be made available in isolation;
- Decoupling authorization and authentication in a user's profile;

The main function of this protocol in BLOCKBIT NGFW is to perform the authentication of the access user against an account previously created on a TACACS + server.

Supported authentication types

- *PAP*;
- *CHAP*;
- *LOGIN*.

Through this screen it is possible to configure the TACAS + authentication server.



Authentication - TACACS + grayed out

If all options are grayed out as in the case of the image above, select the activate **[ ]** icon, located on the right side of the “TACACS +” option. Click on it in order to activate it, it should look like this: activate **[ ]**. Once this is done, the options will be available for editing and the **TACACS+** server can be configured correctly.

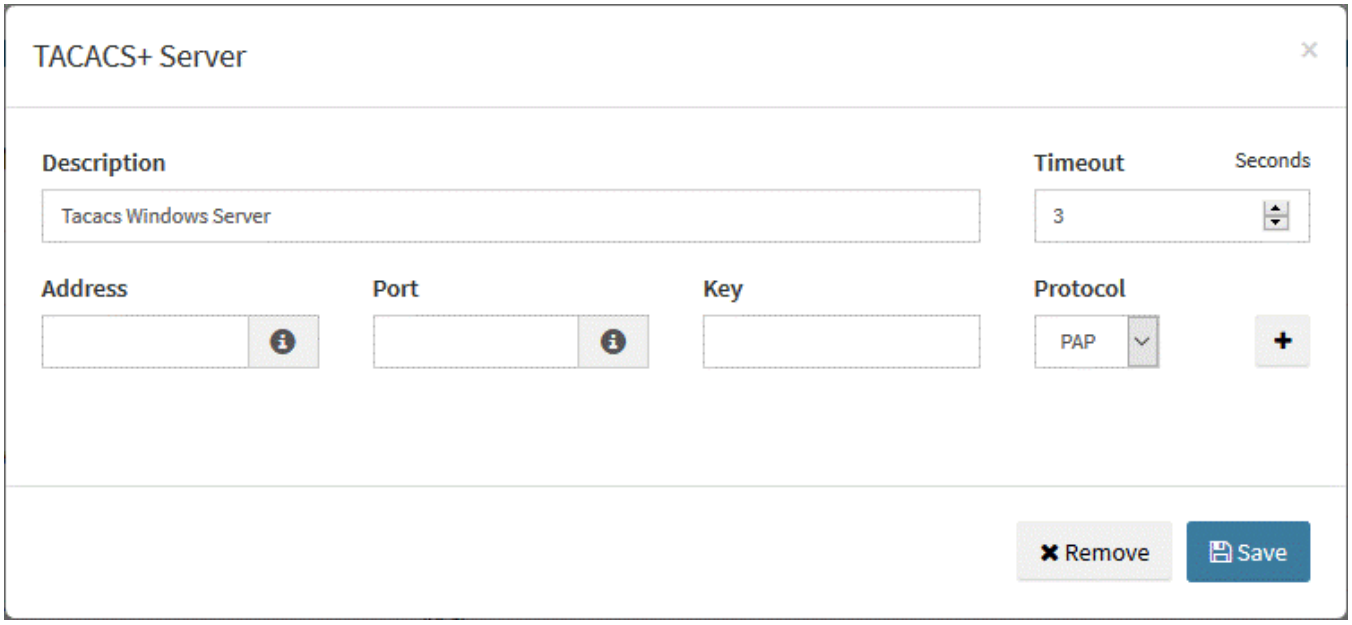
Below we will specify some fields:

- ***TACACS+ Server*:** Select the TACACS + profile that was created by clicking on the add **[ ]** button. Eg Primary DC;
- ***Domain*:** Defines the domain into which users will be imported. Ex.: *dominioc.com*.
- ***Groups*:** Determines the group to which the server belongs.

To add a TACACS + Server, check the *TACACS+ Server – Add Server* page.

UTM - TACACS+ Server – Edit Server

To edit the settings already made, select the desired server in the “TACACS + Server” drop-down menu and click on edit [ ], the screen below will be displayed:

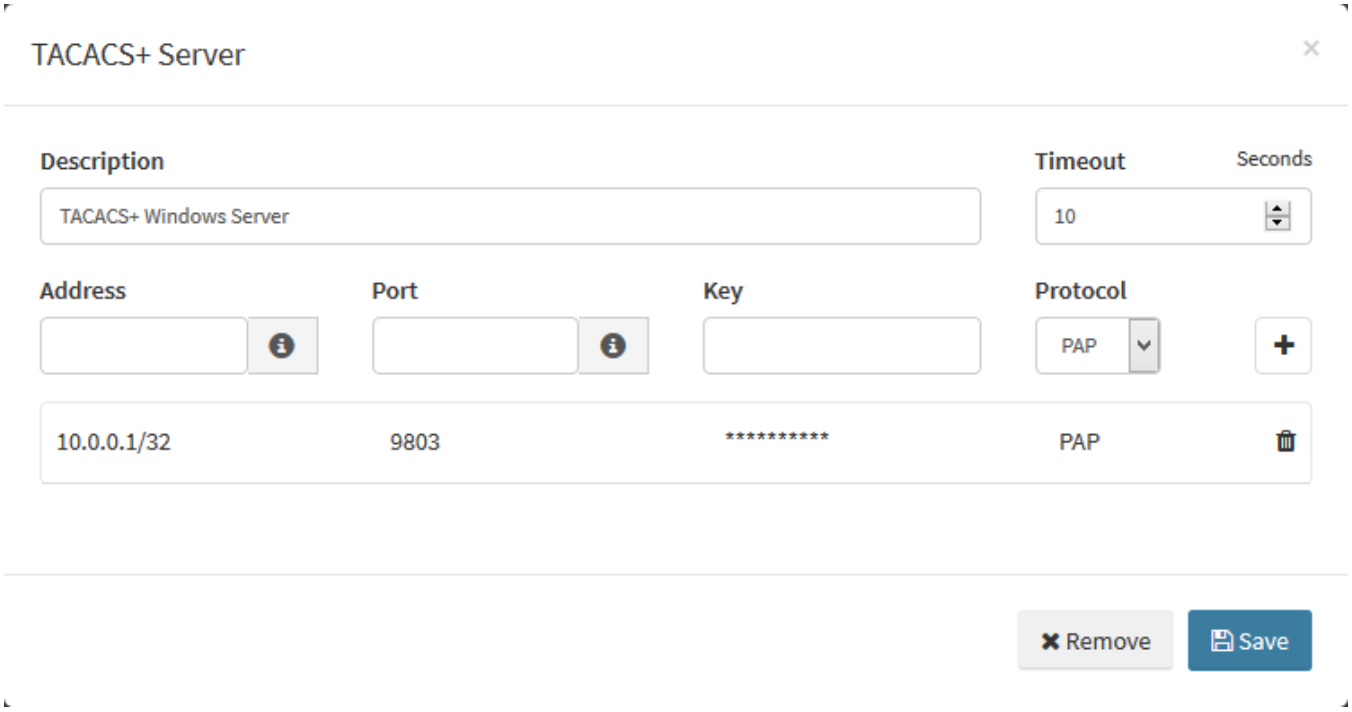


Authentication – TACACS+ server - Edit

In the same way as during the addition, it is possible to edit the desired settings and click save [Save], in order to record the necessary changes made.

UTM - TACACS+ Server – Add Server

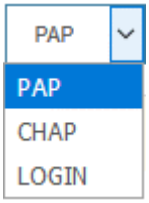
Click on add [+], located on the right side of the menu.



Authentication – TACACS+ server settings

Below we will specify some fields:

- ***Description*:** Enter the server description. Ex .: TACACS + Windows server;
- ***Timeout*:** Sets timeout in seconds for the server to wait for a response from the host. Ex.: 10;
- ***Address*:** IP address of the desired server. EX.:10.0.0.1/32;
- ***Port*:** Specifies a port number for the server. Ex.: 49;
- ***Key*:** Defines the authentication key used to perform the communication and encryption of the communication with the TACACS + authentication server. Ex .: blockbit.ngfw;
- ***Protocol*:** Determines the type of authentication protocol desired. EX .: PAP.



Authentication – TACACS+ Protocol.

After completing the Description, Timeout, Address, Port, Key and Protocol fields, click add [+] to add the server to the list of TACACS + servers;

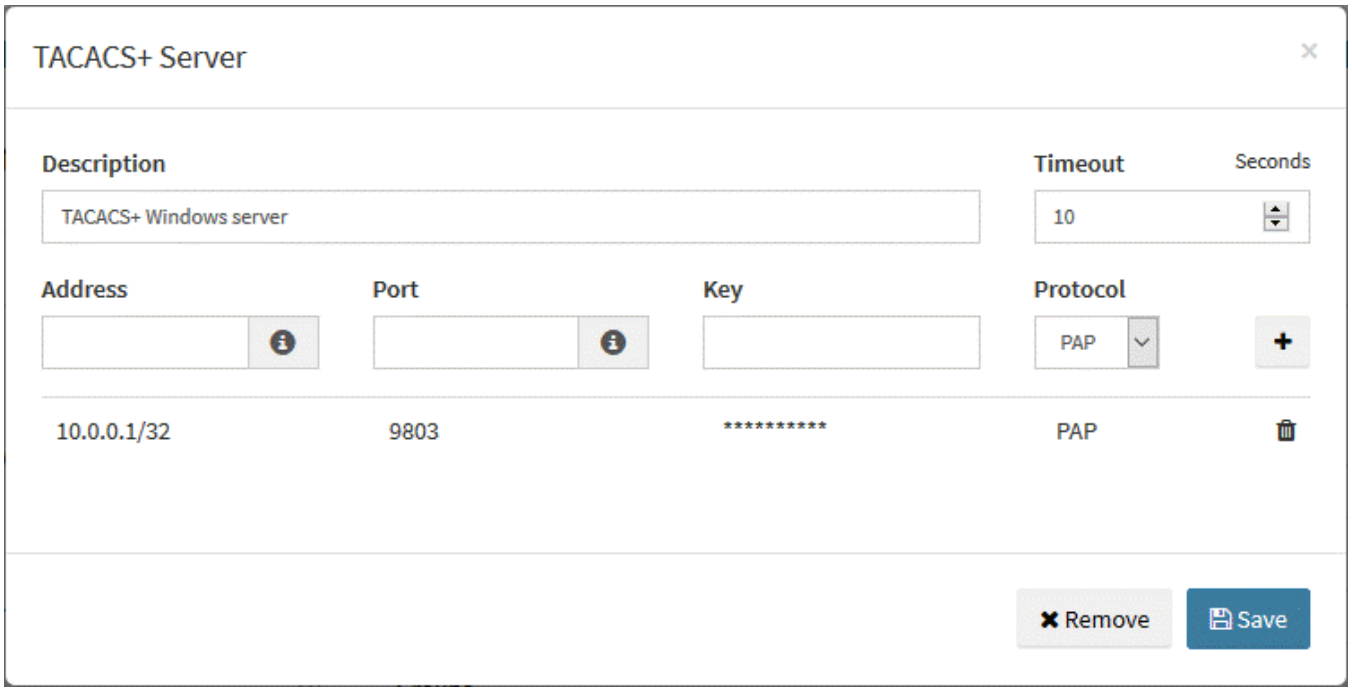
In authentication, it is possible to register several servers, the system will first test what is at the top of the list, if it is offline, the server below it will be tested, following this order successively.

The server list serves as a means of preventing possible communication failures with the TACACS + server, for example:

- Response time exceeded;
- Firewall or access list blocking traffic;
- TACACS + configured with the wrong authentication key;
- Among other possibilities ...

The system works by trying to connect with the servers registered in this list in order, trying to make the connection until one of these servers responds and authentication is performed. Precisely for this reason, it is essential that the server base be identical.

If you want to remove a server added to the list, click the remove icon **[ ]**.



Authentication – TACACS+ server list

After making the appropriate settings, click save **[Save]** to register them correctly, otherwise, click outside the screen to cancel the edits made;

Once added, the server will be displayed in the window, as shown in the image below:

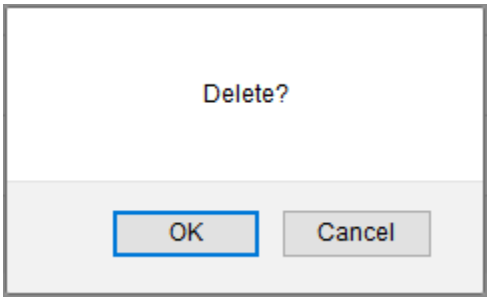
Authentication – TACACS+ server

UTM - TACACS+ Server – Delete Server

To remove any server, click on the delete icon **[ ]**, a panel with all created servers will be displayed, as shown in the image below:

Authentication – TACACS+ server – Removal Panel

Choose the server you want to be removed and click the delete **[ ]** icon to remove the desired server. A confirmation message will be displayed:

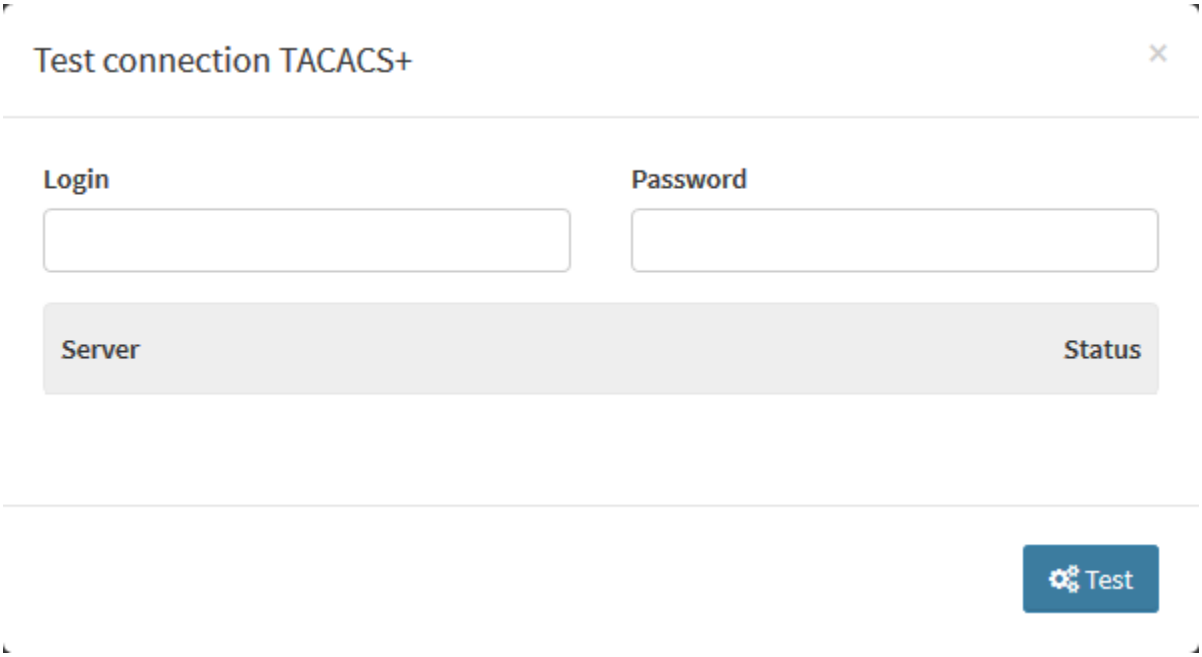


Authentication – TACACS+ server – Removal Message

Click **[** OK **]** to remove the selected server, or click **[** Cancel **]** to make no deletion.

UTM - TACACS+ Server – Connection Test

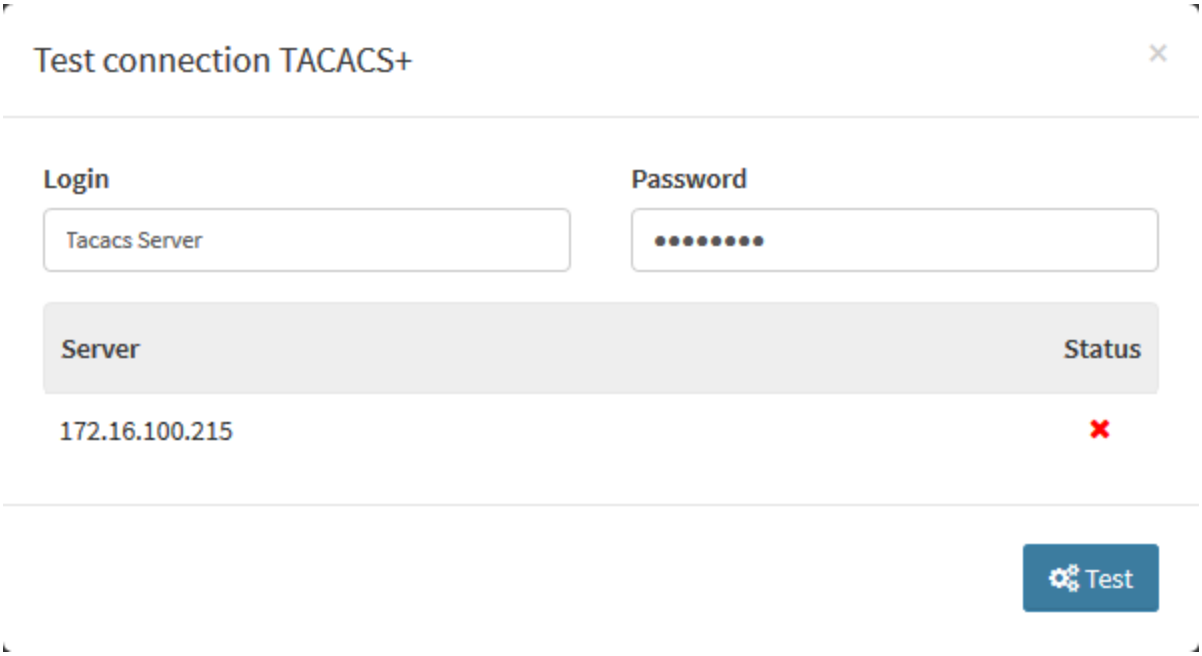
After adding a connection, it is possible to perform a connection test by clicking on the connection test icon **[ ]**, by clicking on this icon the screen below is displayed:



Authentication - TACACS + server - Connection Test

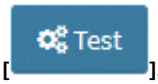
The function of this panel is to test the connection of a specific user to the TACACS + server, to do so, follow the steps below:

1. In “Login”, enter the login information that is used by the user to enter the TACACS + server. Use the same credentials that are registered with the TACACS + server user base;
2. In “Password”, type the password;
3. In the “Server” and “Status” list, we have a list of TACACS + servers and their current availability status, as shown in the image below;



Authentication - TACACS+ server – Connection Test Status

This interface allows you to register several authentication servers, the test is done starting with the on that is at the top, if the server is not working, the server listed below is tested, and so on.

4.When clicking on the test button **[**  **]**, a connection test is performed that updates the appropriate states in the list mentioned above;

UTM - Servers - RADIUS Server

RADIUS (Remote Authentication Dial In User Service), is a protocol widely used to manage access to the most diverse network services. This protocol defines a standard for exchanging information between a Network Access Server (NAS) and a Radius AAA server whose function is to perform authentication, authorization and account management operations.

RADIUS has a series of features that qualify it as an efficient authentication system adaptable to the most diverse network conditions.

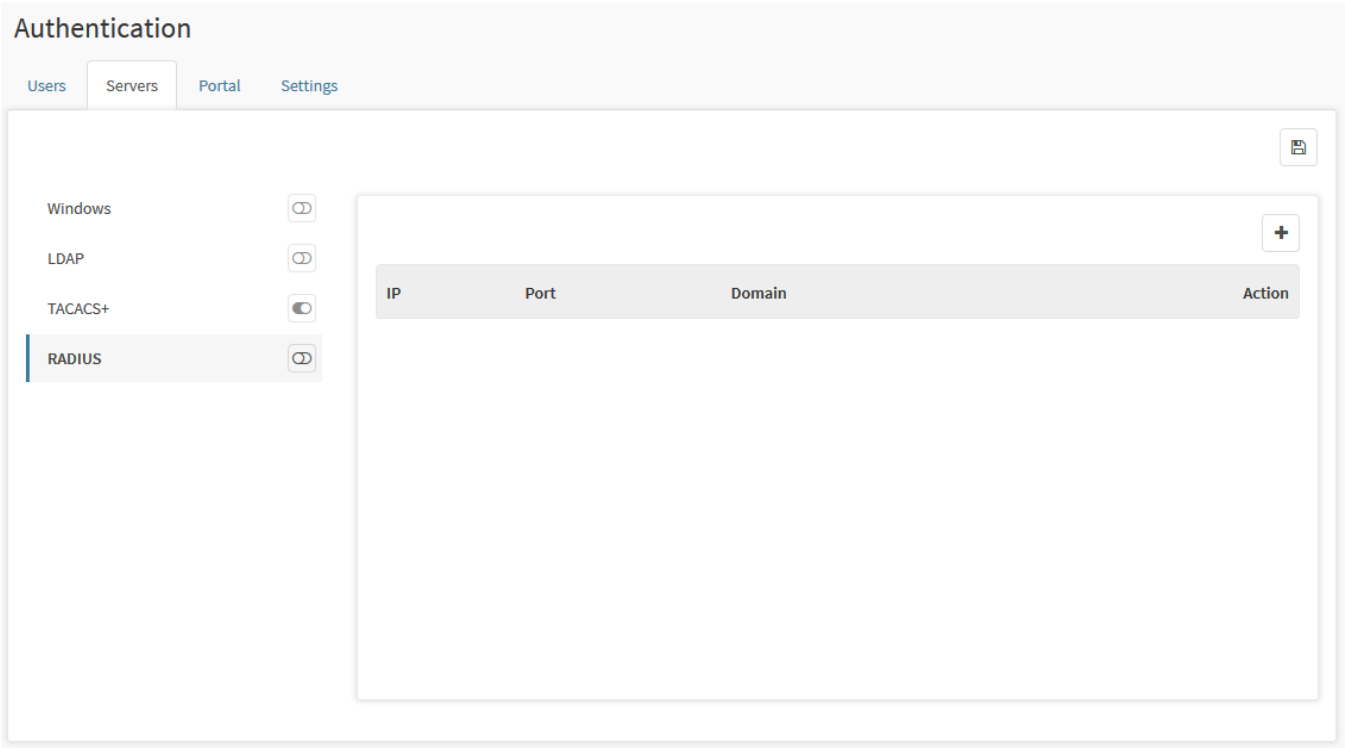
Radius operates in Client / Server mode and supports two authentication methods:

- *RSSO (Radius Single Sign ON)*;
- *Account Client Radius*.

To configure Radius authentication, it is necessary to certify the registration of domains and groups in order to integrate the user base of the Radius server.

Check the registered domains and make sure to register at least one “local group” for the respective domain of the Radius server. (In case of doubts, see the chapter "Users Tab").

Through this screen it is possible to configure the RADIUS authentication server.



RADIUS - *Radius Server Authentication*.

To use the RADIUS servers to allow administrator users' authentication for remote login on the GSM, check this page.

UTM - RADIUS SERVER – Radius Single Sign ON

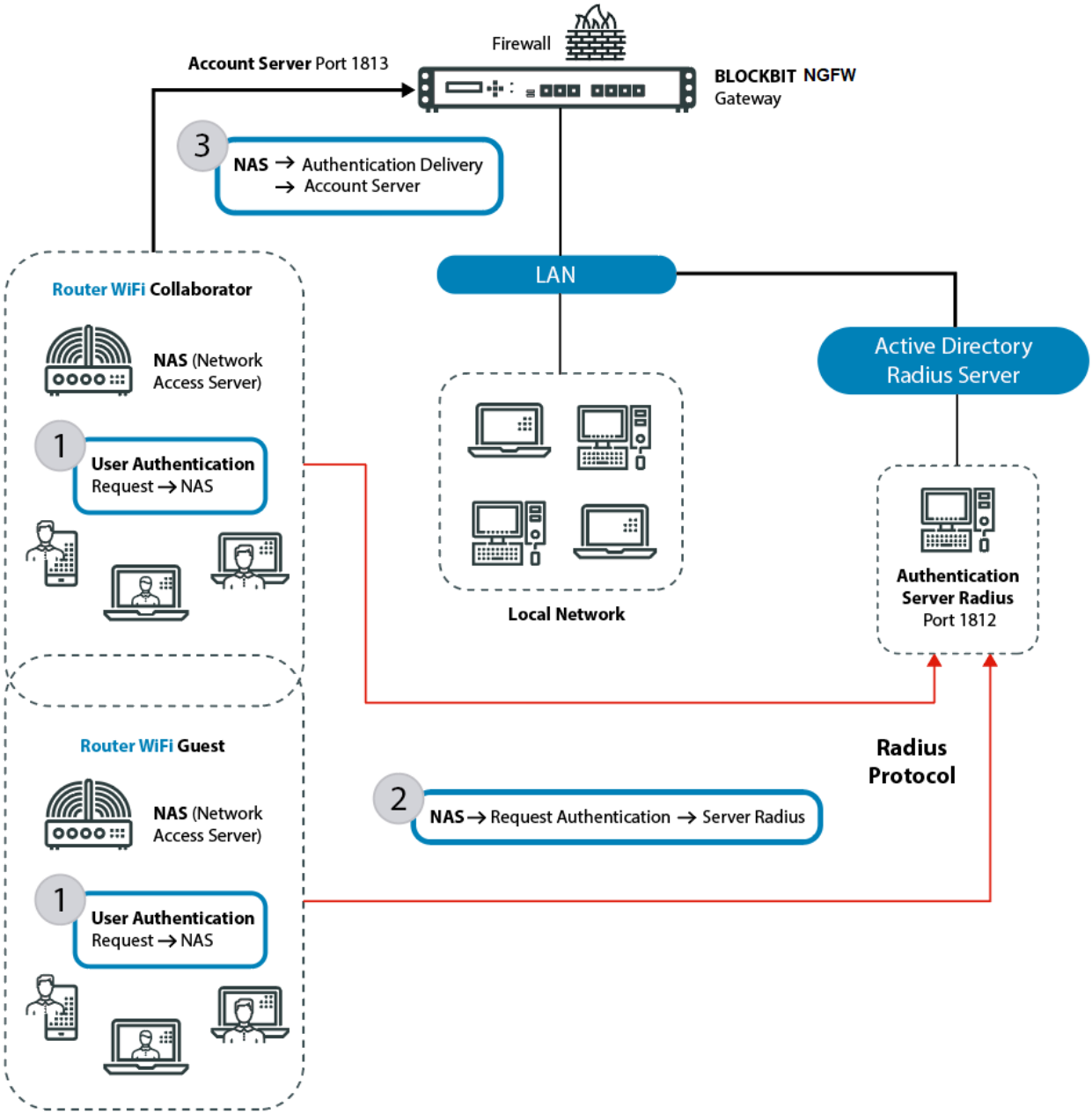
Support for NAS (Network Account Service) devices.

The NAS works as a client for the RADIUS server, which is responsible for sending the information of users who want to access the NAS service to the RADIUS server, which is responsible for verifying the user's authenticity and informing its validity for the NAS.

RSSO authentication has the role of integrating the authentication of NAS devices on Radius servers (for example: “Wireless Routers and / or Switches”) with BLOCKBIT NGFW transparently.

For this integration, Wireless Routers or Switches must support the **802.1x** protocol that provides authentication mechanisms and network access control.

RSSO diagram - Radius Single Sign ON



RADIUS - *RSSO – Radius Single Sign On*

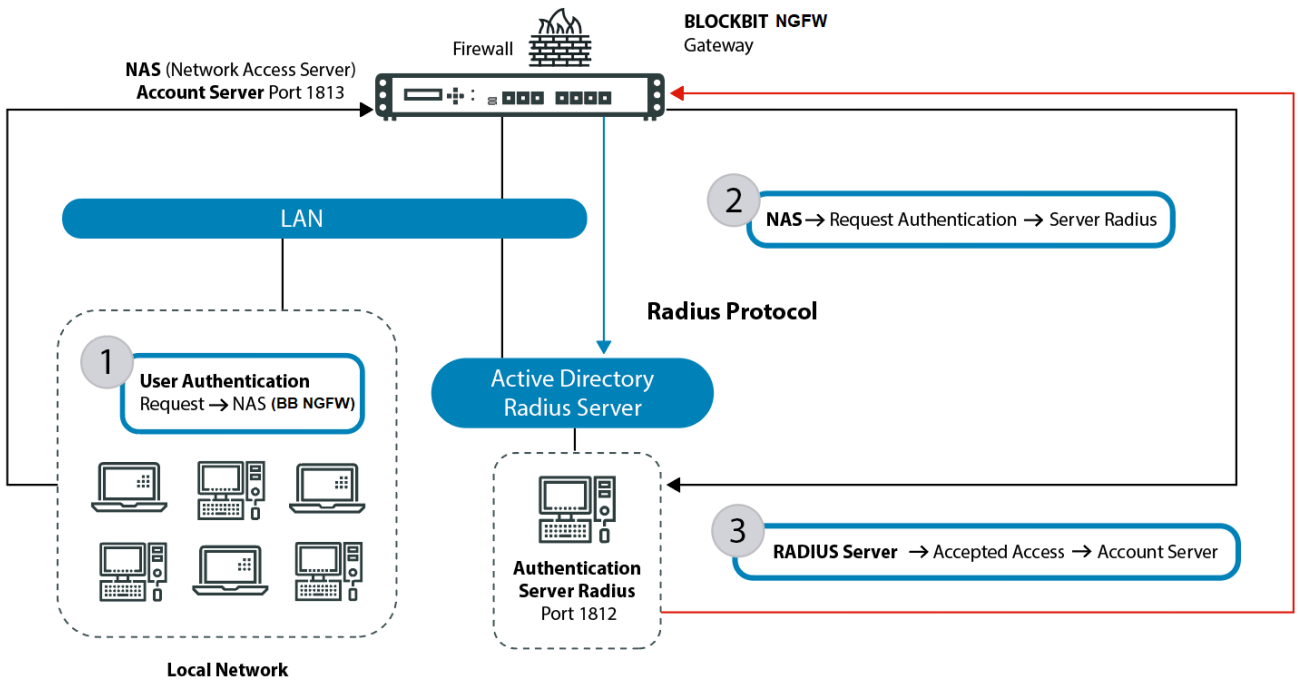
Account Client Radius

Standard Client Radius authentication enables your BLOCKBIT NGFW device with a NAS client that directly requests authenticity and login authorization to the Radius server for the user.

Supported authentication types

- MSCHAP;
- CHAP;
- PAP.

Radius Client Account Diagram

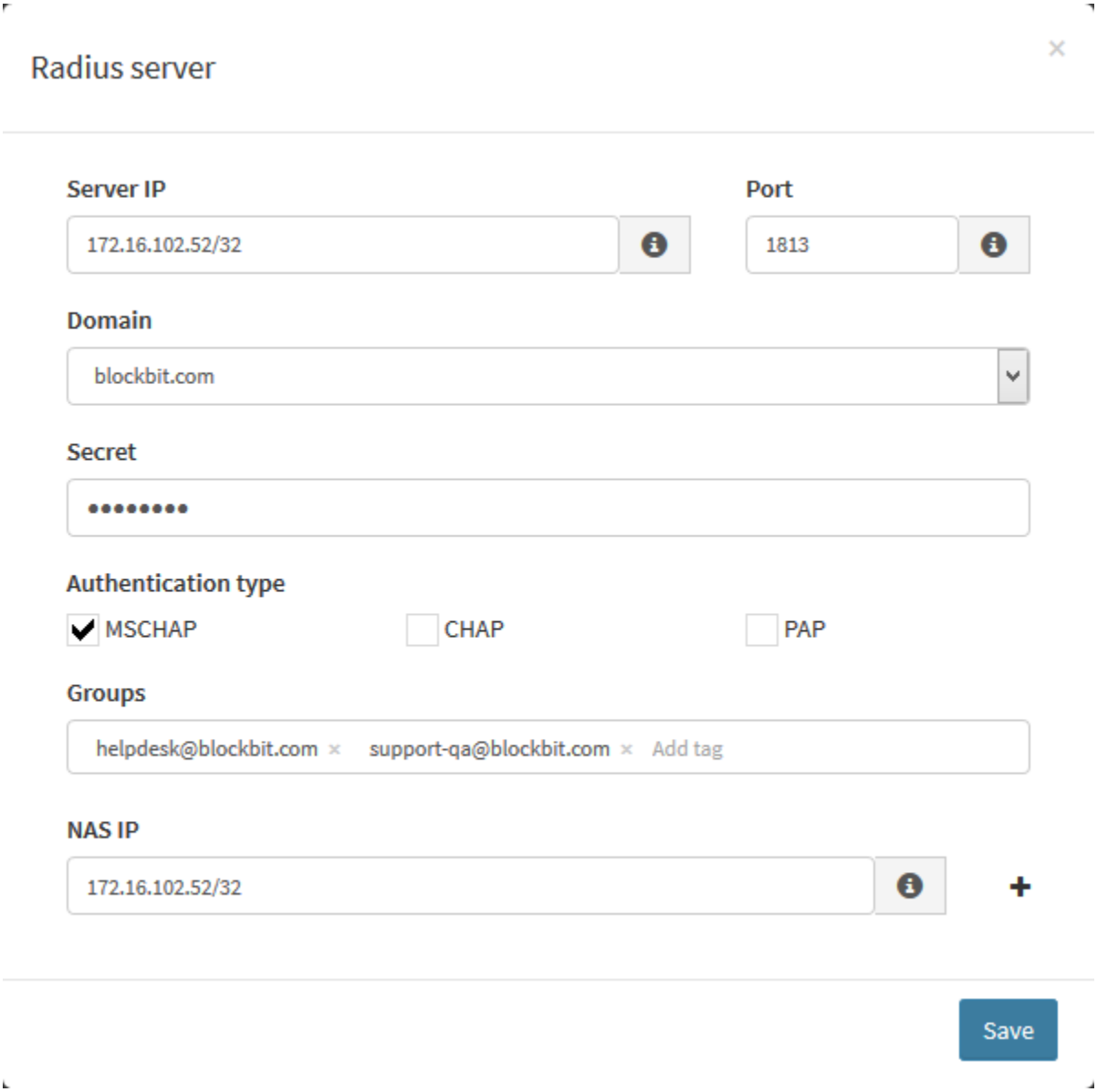


RADIUS - Account Client Radius diagram

UTM - RADIUS SERVER – Add Server

If all options are grayed out as in the case of the image above, select the activate **[ ]** icon, located on the right side of the RADIUS option ". Click on it in order to activate it, it should look like this: activate **[ ]**. Once this is done, the options will be available for editing and the **RADIUS Server** can be configured correctly.

Click on Add **[ ]** Radius server.



RADIUS - Radius server settings.

Below we will specify some fields:

- **Server IP:** IP address of the Radius authentication server. Radius server authentication ports. Standard port: 1812;
- **Domain:** Selection of the domain of the authentication server;
- ***Secret*:** Pre-shared key (Pre-Shared Key or PSK). Secret shared between the "Radius" authentication server and the "Blockbit NGFW" account server. Ex.: blockbit.ngfw.
- **Authentication type:** Selection of supported authentication types.

RADIUS – Radius – Authentication types.

- **Groups:** Selection of the “Group (s)” for self-registration to integrate the user base of the “Radius” server with the “Blockbit NGFW” account server.

In this process it is not possible to identify users removed from the remote server, in which case the network administrator will have the responsibility to manage the user base and manually update the BLOCKBIT NGFW when the removal of users from the remote Radius server base occurs.

- **NAS IP:** IP address of the “Wireless / e Routers or Switches or your NGFW Device” devices capable of receiving requests from authentication clients and forwarding the request to the network's Radius server.

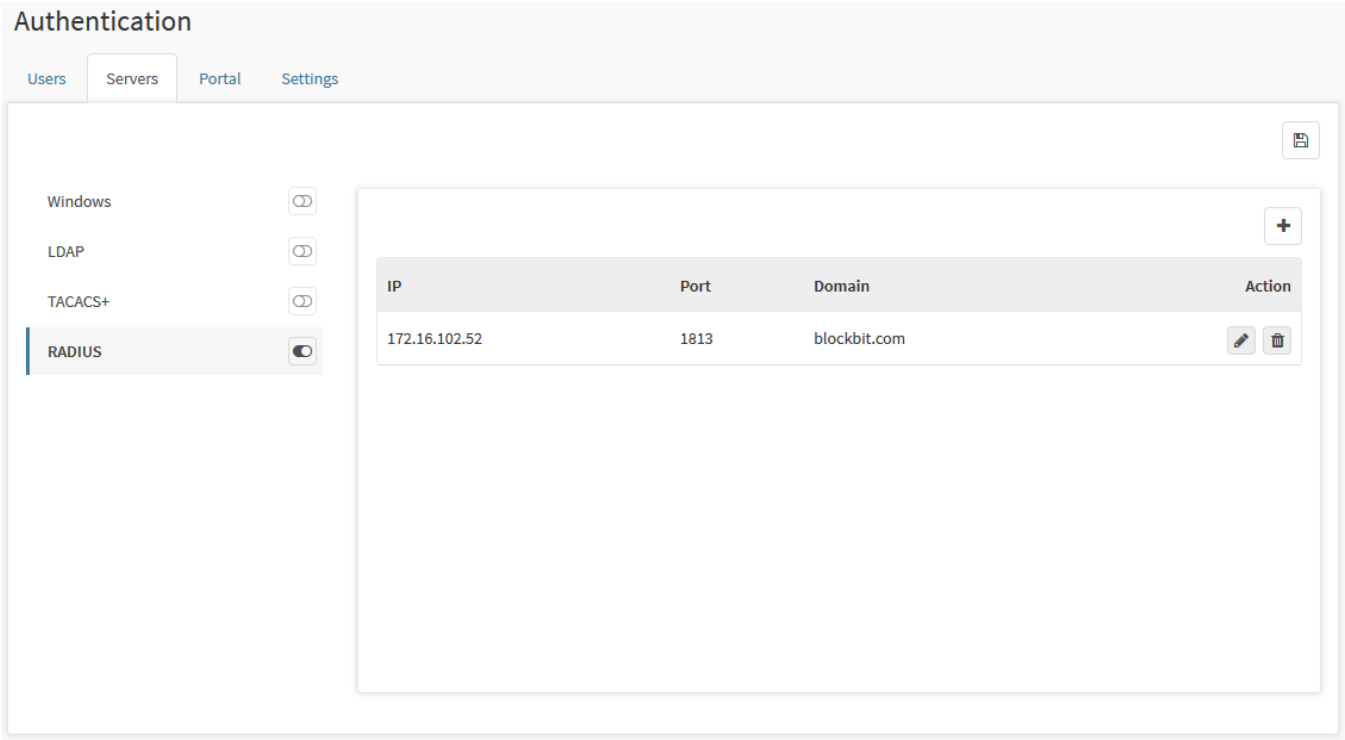
NAS devices must support the 802.1x protocol and allow configuration of the Radius Authentication Server identification for port 8012 and the Radius account server for port 8013.

In order to define security policies for the integrated users of the Radius database by group profiles, it is required that the administrator register “local” groups for the respective domain and associate the users integrated by the self-registration group for each group respectively..

After making the appropriate settings, click **[** 

] to register them correctly, otherwise, click outside the screen to cancel the edits made;

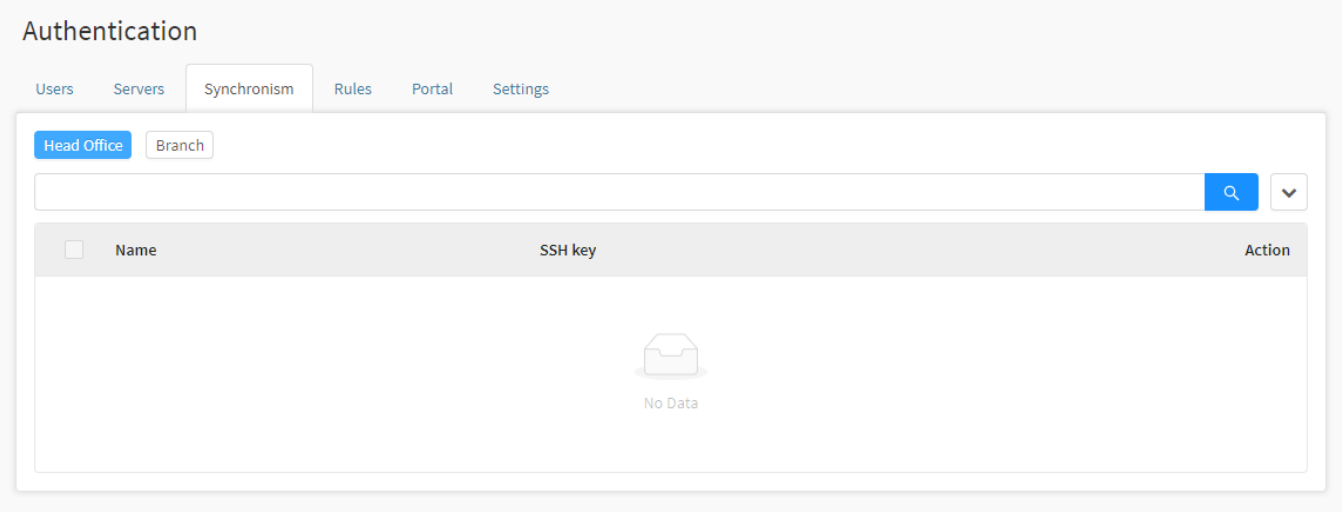
After finishing the settings, they are saved as shown below:



RADIUS - Columns

UTM - Authentication – Synchronism

It is possible to run the authentication of multiple NGFWs in the Synchronism tab, in Authentication, in the system's options.

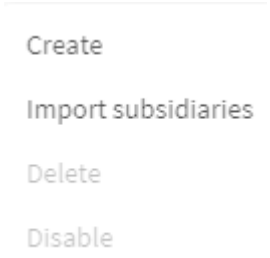


Authentication - Synchronism

In order to switch the synchronization mode, select between "Head Office" and "Branch".

Head Office

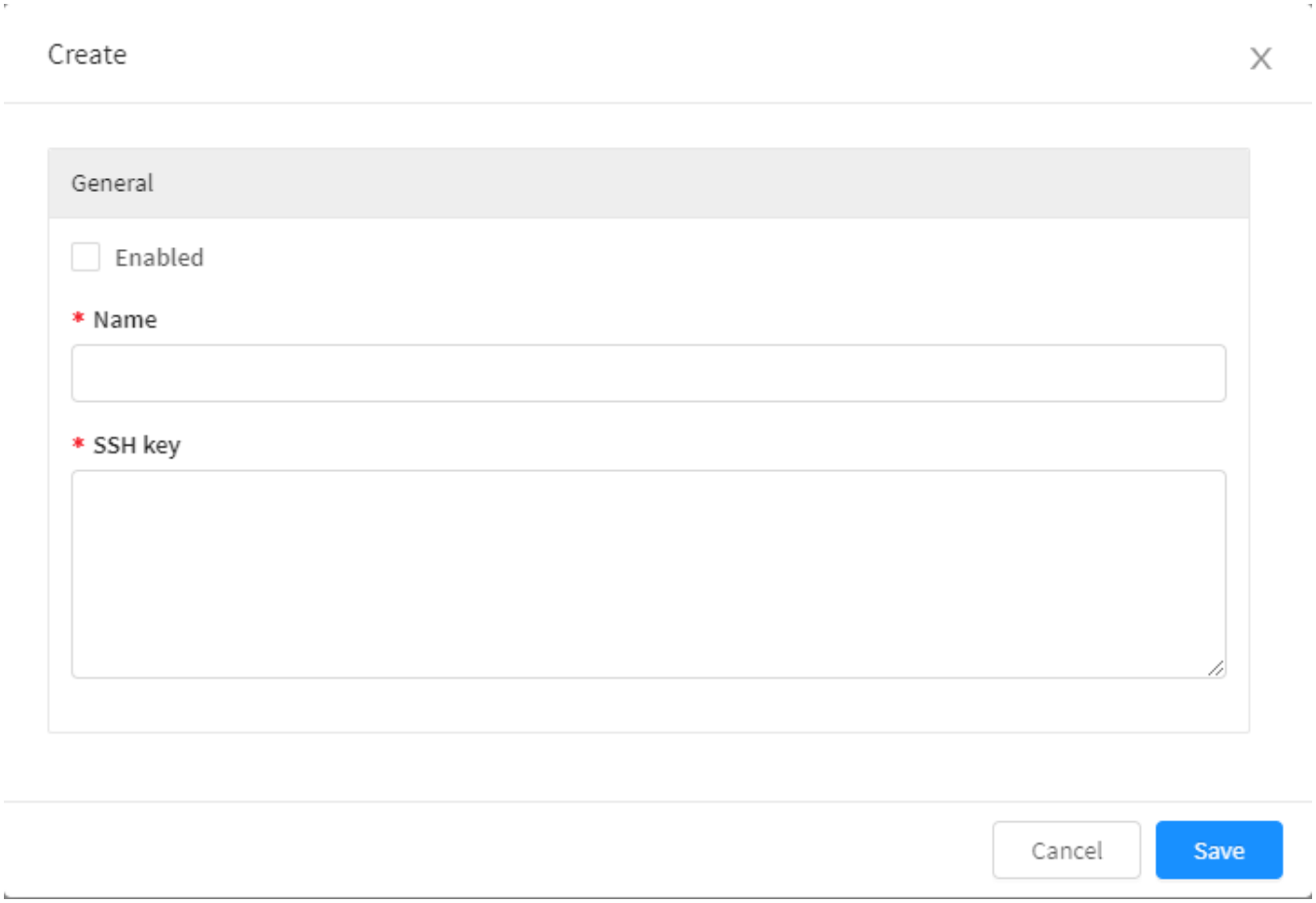
Next, to add new NGFWs to the synchronization base, click [ ] and the following options will be made available:



Synchronization - Add button

Create

After selecting "*Create*", it will be possible to add a new NGFW by its name and SSH key:

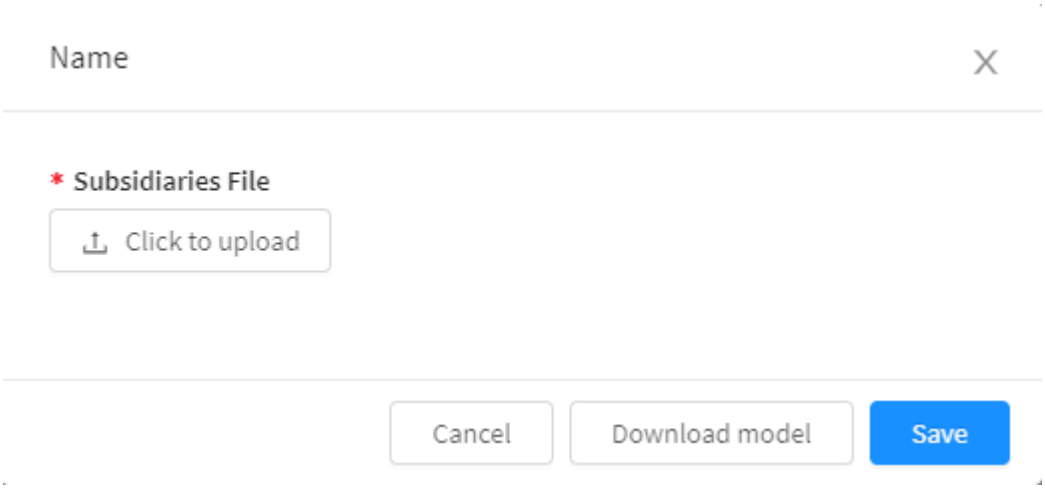


Create - Synchronism

Mark the "*enabled*" [Enabled] option so that the sync check can be done, and after including the necessary information, click [Save].

Import subsidiaries

In this part it is possible to upload subsidiary files, as to proceed with the synchrony.



 In download model, it is possible to download an example of the paramethers to be used in the synchronization.

After finishing the due changes, click the save **[** 

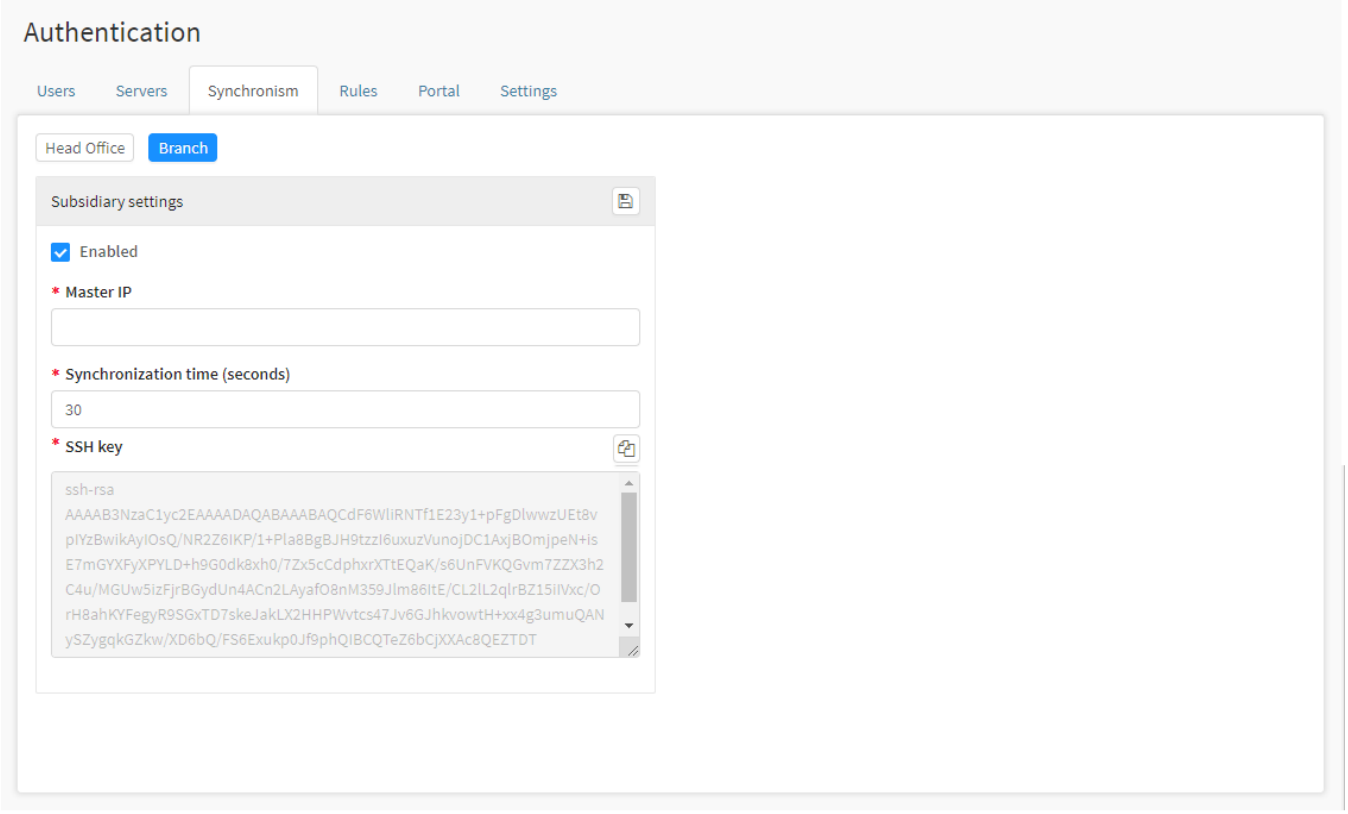
] button in order to keep them.

 This setup does not register and does not sync the users.

In order to effectively synchronize them, one must set up the servers.

UTM - Authentication – Synchronism - Branch

Next, we will analyze the components of the synchrony settings, in Branch mode.



Authentication - Branch mode

Enabled: Enables the Branch-Head Office synchronization. When enabling this option[Enabled], the "Master IP" and "Synchronization time" fields, will become mandatory to fill.

Master IP: Uses the main IP (Head Office) for the synchronization.

Synchronization time: Defines the communication interval between both, in seconds.

SSH Key: SSH key that will be used for the validation. It also has an option to copy said key [ ].

It's important to notice that when copying the users, only the user sessions from local networks with branch IPs are copied.

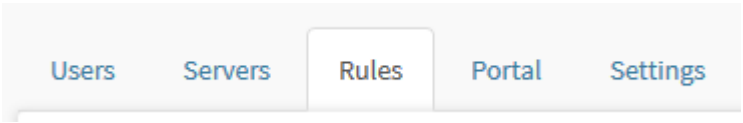
After having inserted the necessary information, click save[ ] and the setup will be concluded.

UTM - Authentication - Rules tab

This screen is where users can manage the authentication service through control Policies, which make it possible to allow or block access to the authentication service based on predetermined conditions or to define the parameters of the session of users who have authentication permission in a given service. These authentication Policies are applied to both the Captive Portal service and the Authentication Client.

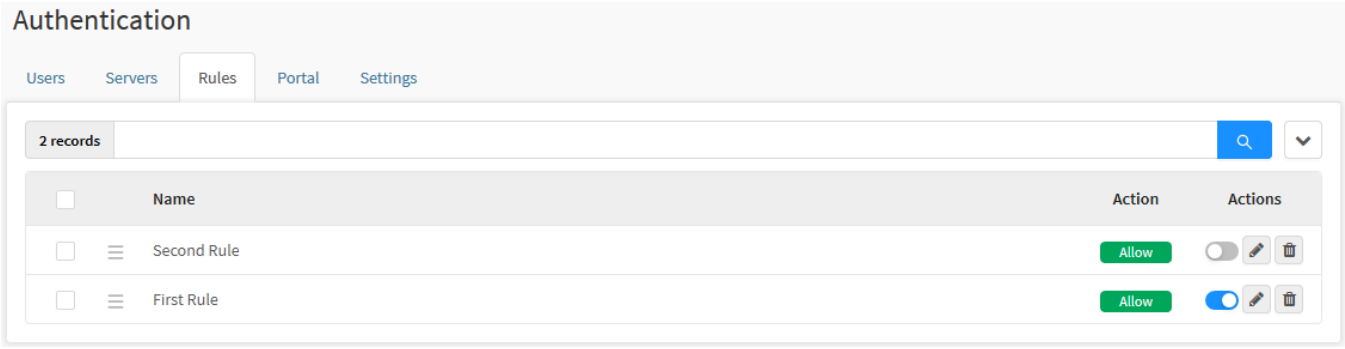
As in Policies, these are managed by “Priority”, and they are applied considering the “First Match Wins” method (The 1st positioned Policy among its peers has priority over the 2nd. The 2nd has priority over the 3rd, and so on, in a descending logic). Therefore, the Policies located above have priority while those below have lower priority and the action is applied to the first Policy that is found based on access conditions.

To configure these settings, click on the Rules tab:



Rules tab

The screen will appear, as shown by the image below:



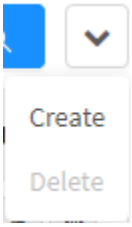
Authentication - Servers

In this session we will analyze:

- How to create, edit and delete these policies;
- The column components of this tab.

UTM - Actions menu

At the top right of the panel, we have the actions menu, which can be displayed by clicking the **[ ]** button, as illustrated by the image below:



Authentication – Action Menu

The menu consists of the following options:

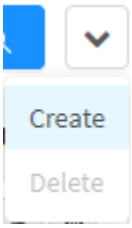
- *Create;*
- *Delete*.

Next, each action menu option will be detailed.

UTM - Actions Menu - Create

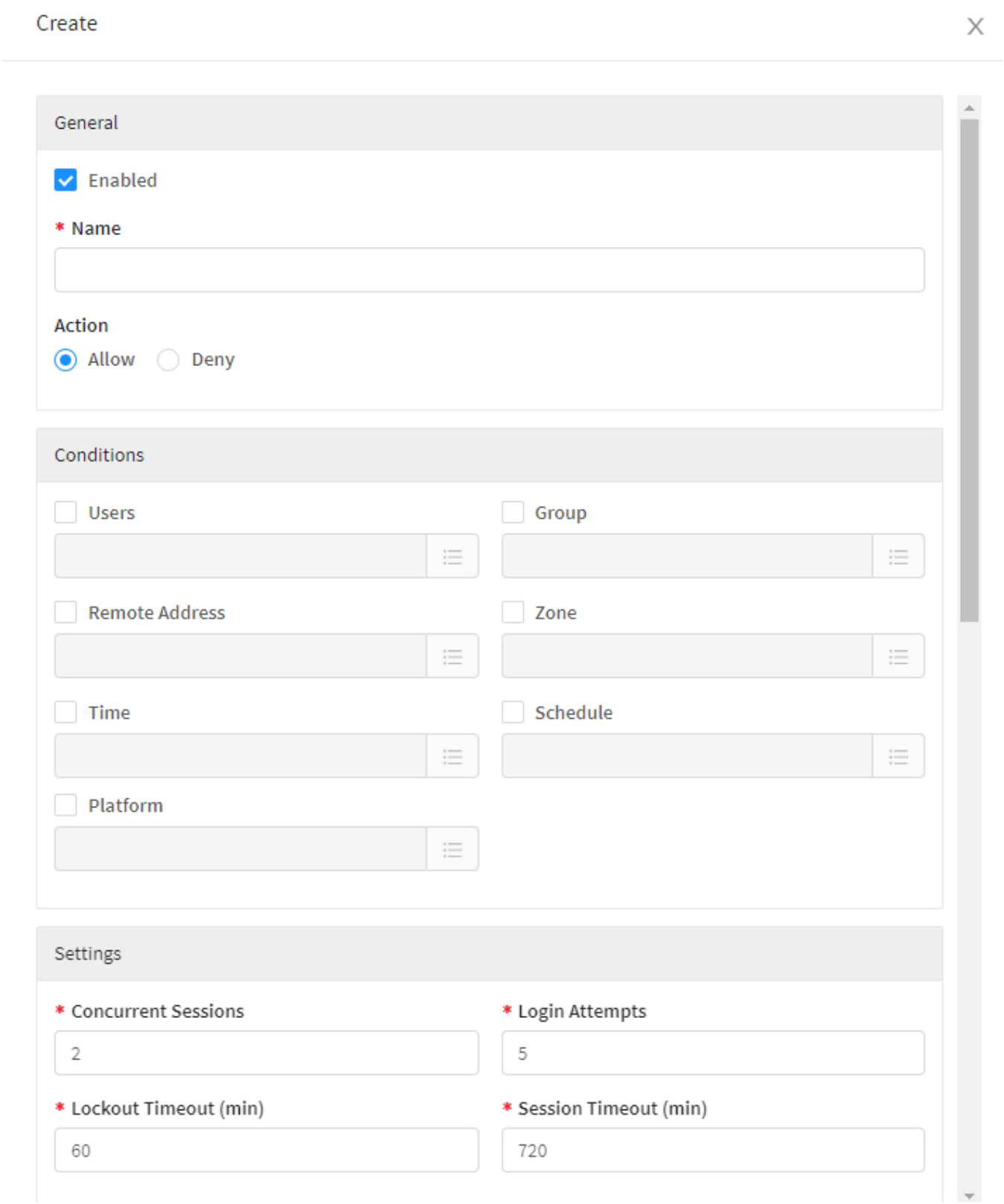
Through the Rules tab it is possible to configure and manage the control policies in the authentication service.

To add one of these Policies, click on the **actions menu [ ]** located at the top right and select "Create ":



Rules – Addition Button

By clicking this button the window below will be displayed:



Rules - Create Policy

- ***Enabled[ ]:*** *Defines whether the Policy will be enabled or disabled*;
- ***Name***: Determines the name of the Policy;

- **Action[ ]:** Determines the behavior of the Policy in question, having as possibilities:
  - ***Allow*:** This option grants access;
  - ***Deny*:** This one denies it.
- ***Conditions*:** Defines the conditions for applying the Policy, among the following options:
  - ***Users[ ]:*** By enabling this option, the Policy will be applied specifically to the selected users;
  - ***Group [ ]*:** When enabling this option, the Policy will be applied to the selected groups of users;
  - ***Remote Address [ ]*:** When enabling this option, the Policy will be applied specifically to remote access addresses, for more information about the object used in this field, see this page;

    > The control of remote access users will only be applied if traffic accessing the VPN service is authenticated via Firewall.

  - ***Zone [ ]*:** When enabling this option, the network zone in which the Policy will be applied is defined, the available options are LAN and WAN;
  - ***Time [ ]*:** When enabling this option, the Policy will be applied specifically to the selected "Time object", for more information about these objects, see the pages on *Time*;
  - ***Schedule[ ]*:** When enabling this option, the Policy will be applied specifically to the selected "Schedule object", for more information about these objects, see the pages on Schedules;
  - ***Platform [ ]*:** When enabling this option, it determines on which platform the Policy will be applied, this field allows the selection of objects of the "Dictionary type" to allow the use of regex by the user, for more information see the page *Dictionaries*.
- ***Concurrent Sessions*:** If the access control Policy is set to "Allow", this field is enabled for editing. It defines the maximum number of simultaneous user sessions. ***We recommend that 2 or more sessions are set as value***;
- ***Login Attempts*:** If the access control Policy is of the "Allow" type, this field is enabled for editing. It defines the maximum number of unsuccessful authentication attempts before the user is blocked;
- ***Lock Timeout*:** If the access control Policy is of the "Allow" type, this field is enabled for editing. It defines the amount of time "in minutes" for the user to be blocked after exceeding the defined number in the “Login attempts” field. *When a user is blocked by this option, he will be identified in the user management panel as "Blocked User", allowing the administrator to unlock him before the end of the Lock Timeout period.*
- ***Session Timeout*:** If the access control Policy is of the "Allow" type, this field is enabled for editing. It defines the maximum inactivity time of an authenticated user's session, so if the Firewall service does not detect traffic by the authenticated user in this Session Timeout interval, the user will be disconnected.

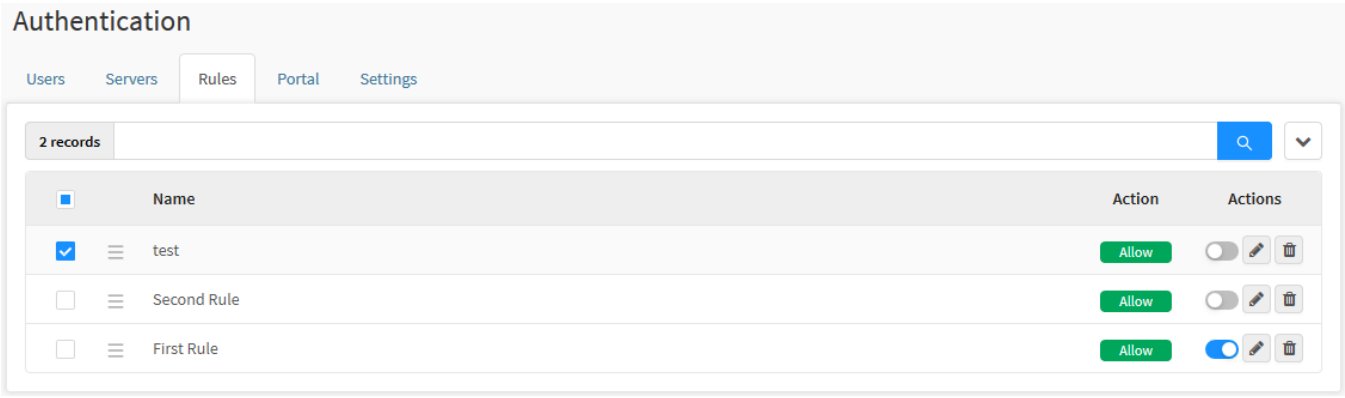
To save the changes click on [Save], otherwise, click on [Cancel] or in [ ] to cancel all settings and return to the previous screen.

After saving, you will need to access the **command queue [ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command Queue.

Next we will analyze the components of the column.

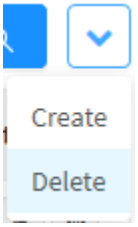
UTM - Actions Menu - Delete

To delete Policies, select the one you want to remove:



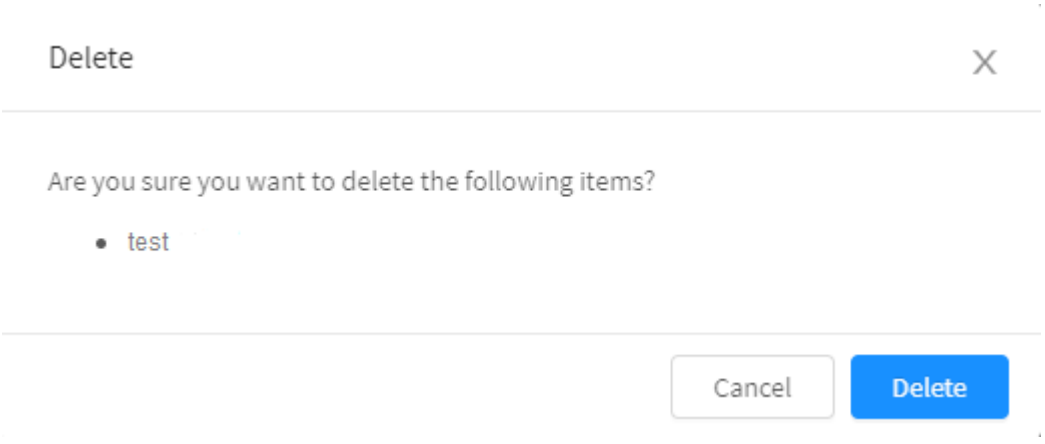
Rules - Selection

Click on the **actions menu [**  **]** located at the top right and select "delete":

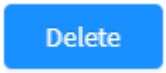
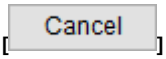


Rules – Addition Button

The following confirmation message will be displayed:



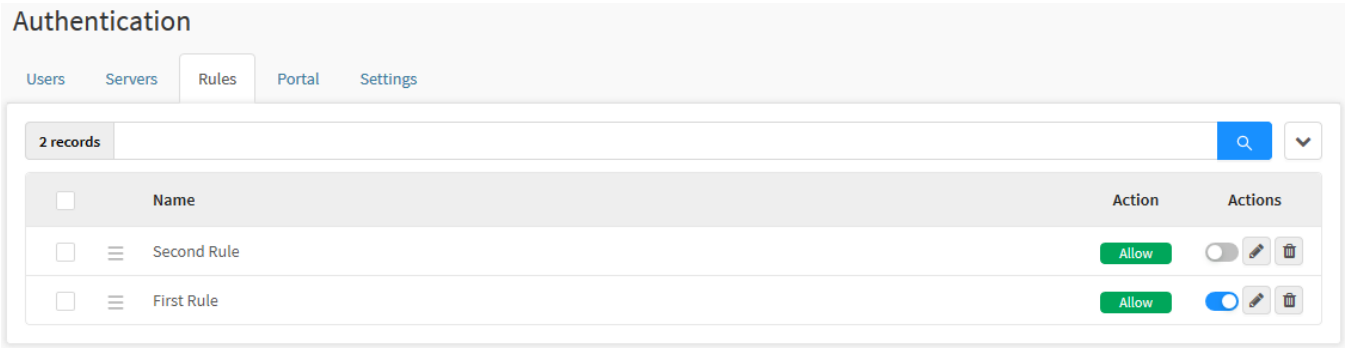
Rules – Deletion confirmation message

Click on **[**  **]** to delete the Policy or, **[**  **]** to keep it.

Next, we'll look at the column components.

UTM - Rules - Columns

The “Rules” tab consists on the following columns:



Objects – Rules tab

Below we will explain each column of the Rules tab:

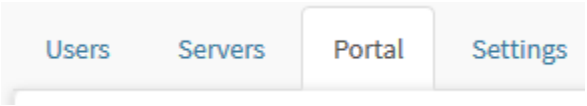
- **Select [ ]:** Select the desired Policies;
- **Move [ ]:** *Assigns the priority level to a Policy by allowing the user to move it upward or downward, upper positioned Policies have priority over the ones below , for more information check this* page;
- ***Name*:** Displays a Policy's name;
- ***Action*:** *Displays if a Policy is of the Allow or Deny type*;
- ***Actions*:** Contains a set of essential actions:
  - **Enable[ ]:** Through this option it is possible to enable or disable a Policy by switching it on or off;
  - ***Edit*[ ]:** Allows you to edit the settings of an added Policy, for more information, see this page;
  - **Delete[ ]:** Allows you to remove a Policy.

UTM - Authentication - Portal tab

Blockbit NGFW has the authentication portal, whose function is to proceed with the authorization and login of users on the Blockbit platform and also provide service for some other system resources.

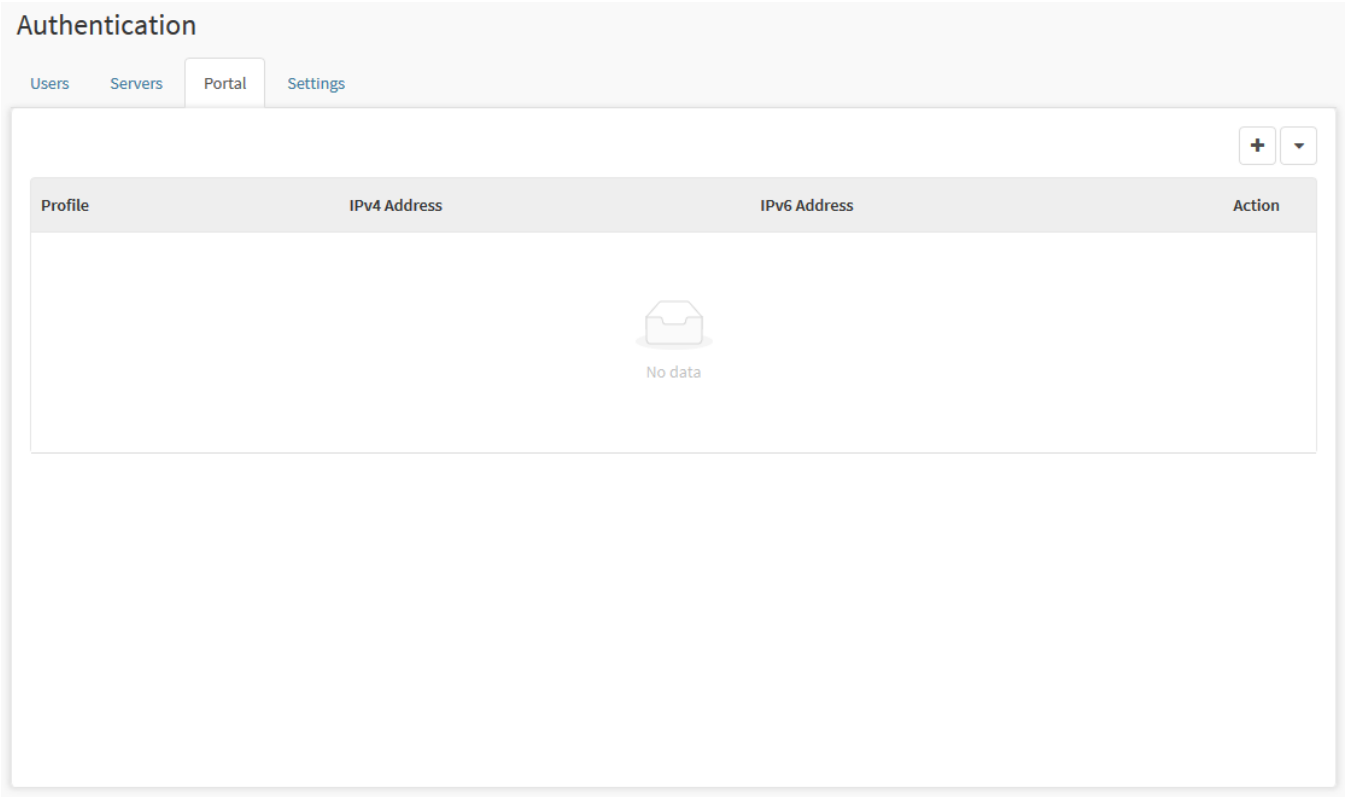
In this version, the authentication system requires enabling the service by profile to authorize the user's logon process.

To make these settings, click on the Portal tab:



Servers Tab

The screen will appear, as shown by the image below:



Authentication – Portal

In this session we will see:

- How to add, edit and remove portals;
- How the authentication portal works;
- How the Blockbit Client works;
- Example of social login setup.

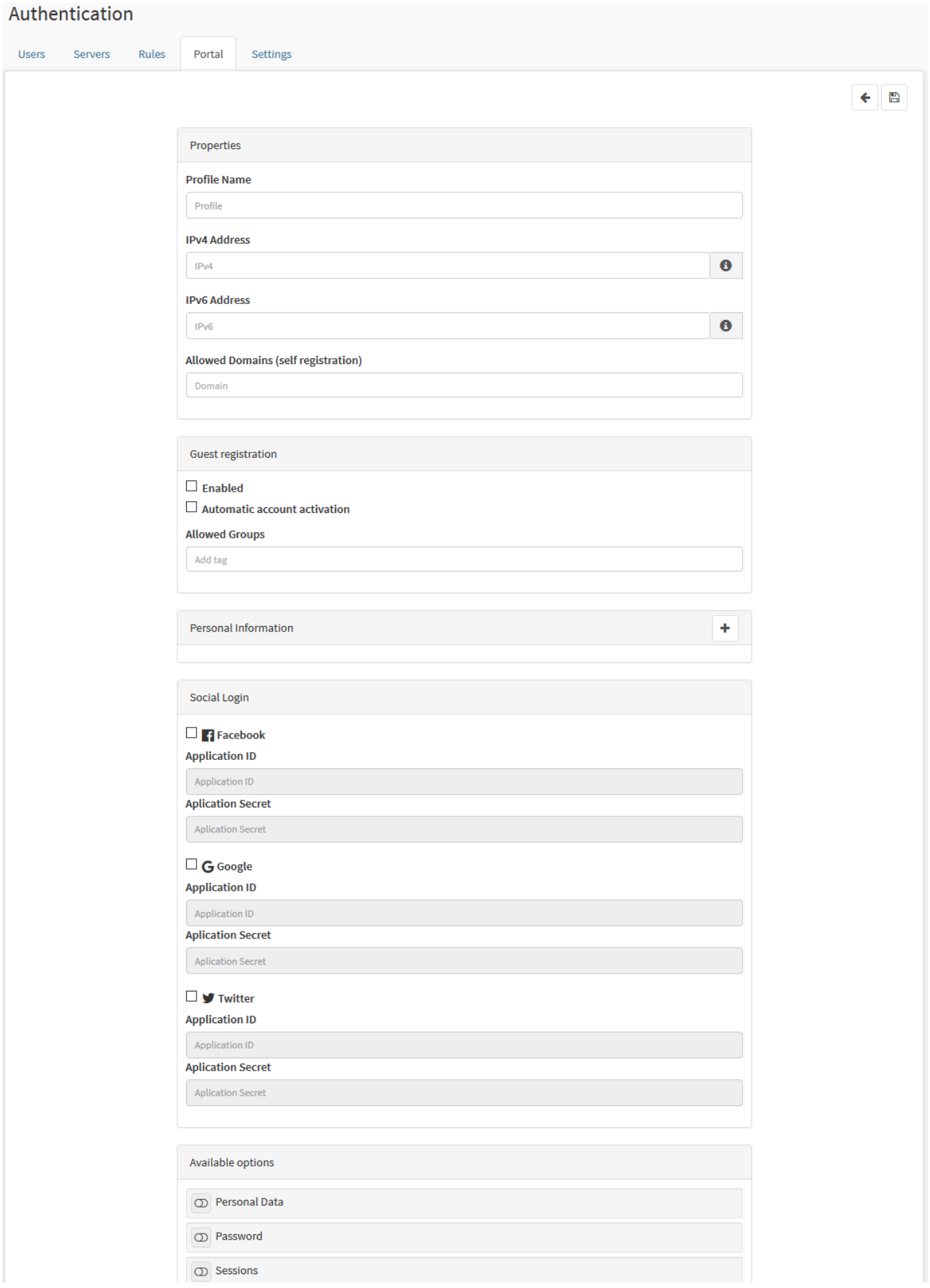
Next, we will analyze this screen in detail.

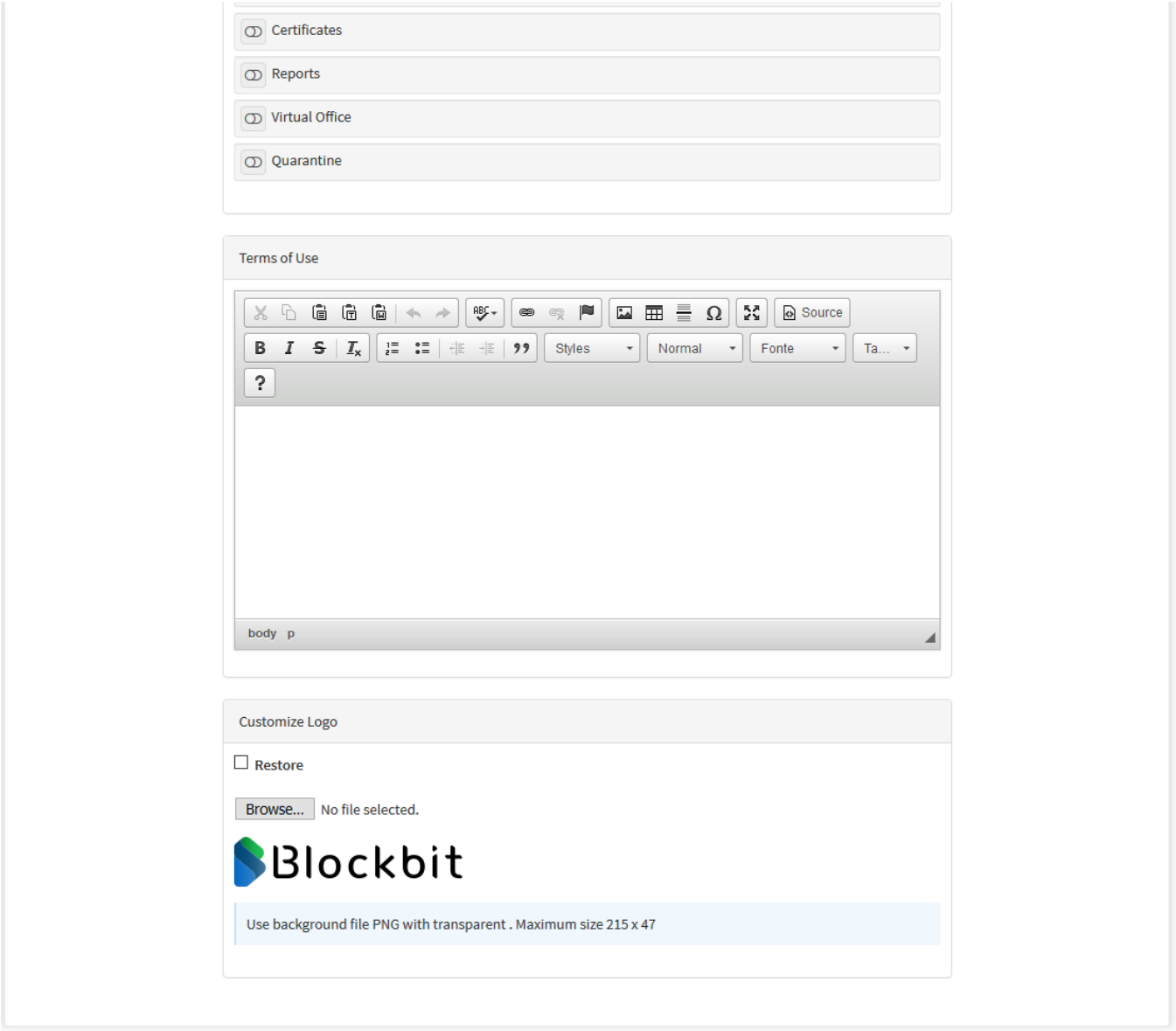
UTM - Portal – Add Profile

Through this button we can define the entire configuration of a portal profile, this feature allows multiple accesses to be created according to the type of user who will log in.

It is recommended to create a portal configuration specifically for guests, in order to distinguish and control "external" access. In addition to facilitating the implementation of rules and policies that apply specifically to users who are not employees of the company.

To create a profile, click the **[**  **]** button. The screen below will appear:


Authentication
Users
Servers
Rules
Portal
Settings
Properties
Profile Name
Profile
IPv4 Address
IPv4
IPv6 Address
IPv6
Allowed Domains (self registration)
Domain
Guest registration
Enabled
Automatic account activation
Allowed Groups
Add tag
Personal Information
Social Login
Facebook
Application ID
Application ID
Aplication Secret
Aplication Secret
Google
Application ID
Application ID
Aplication Secret
Aplication Secret
Twitter
Application ID
Application ID
Aplication Secret
Aplication Secret
Available options
Personal Data
Password
Sessions



Portal - Add profile

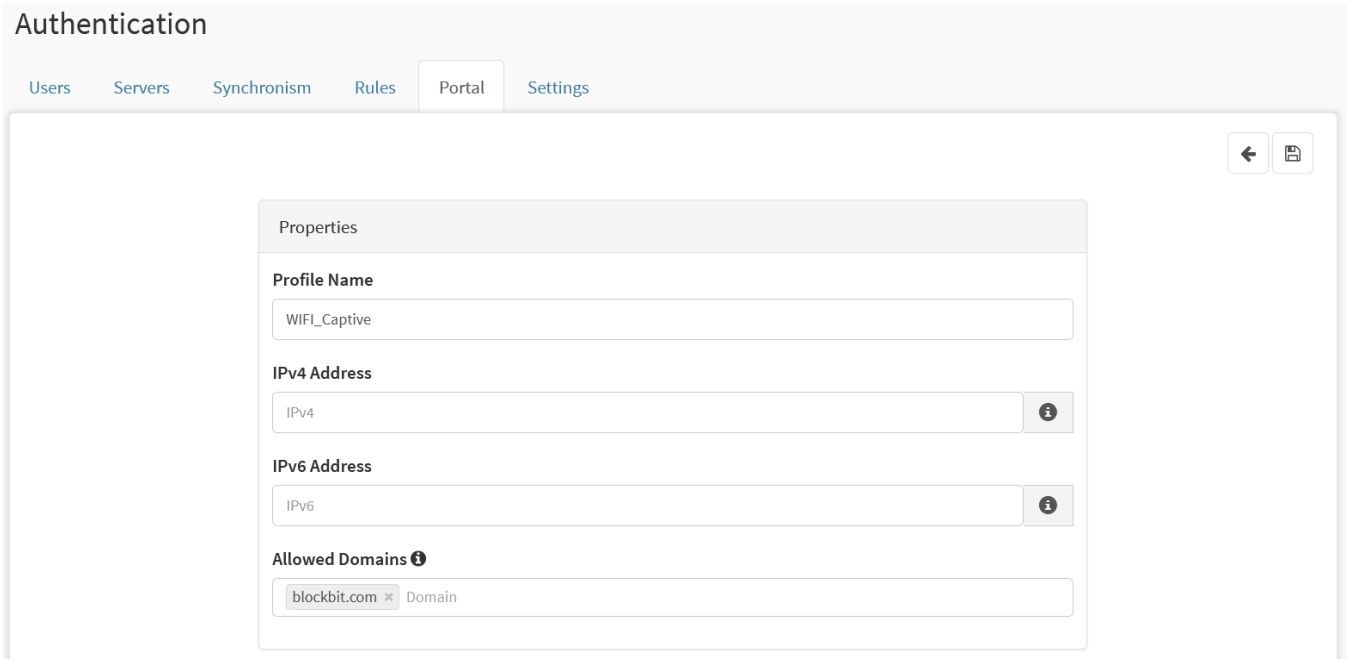
This screen consists of the following panels:

- *Properties*;
- *Guest Registration*;
- *Personal Information*;
- *Social Login*;
- *Available Options*;
- *Terms of Use*;
- *Customize Logo*.

Next, we will analyze each of these panels.

UTM - Add Profile - Properties

This it the panel where the properties of the portal authentication profile are set. This is the only panel whose fields are mandatory to be filled:



Authentication - Portal Settings

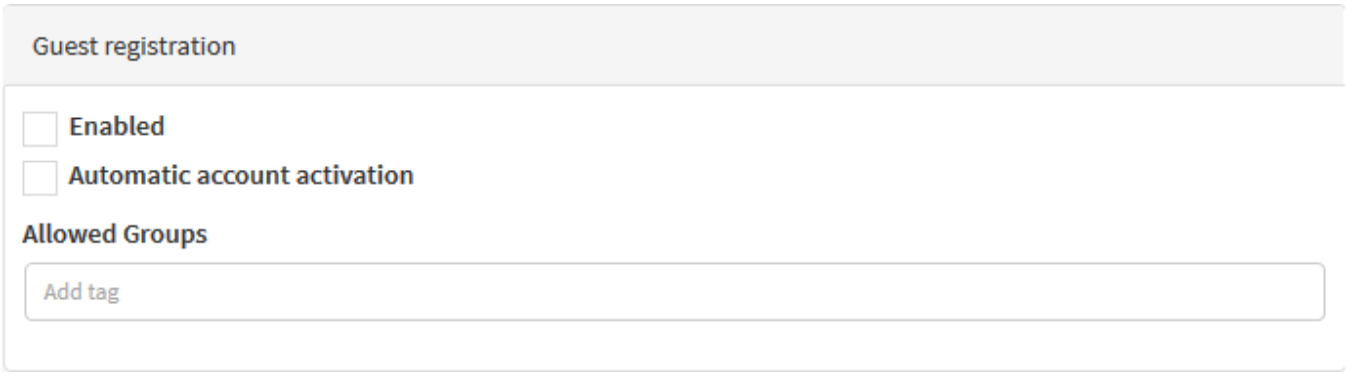
- ***Profile Name*****:** *Enter a name for the default profile. Ex .: "WIFI_Captive". Required field and cannot contain spaces or special characters (except the underscore: _);*
- ***IPv4 Address*****:** *Enter or select the IPv4 address of the local network from the list. Requirement NOT mandatory;*
- ***IPv6 Address*****:** *Enter or select the network's IPv6 address from the list. Requirement NOT mandatory. Ex.: "FE80 :: / 10";*
- ***Allowed Domains* (*self registration*):** Determines the domains allowed to authenticate and create new accounts. Domains added in this field are displayed in the "domain" field on the authentication portal, for more information, see this page. *Mandatory requirement.* Ex.*: "blockbit.com".*

If you just want to configure the properties, click on **[**  **]** to save the settings or on **[**  **]** to return to the *Portal* tab.

Next, we'll look at the *Guest Registration*.

UTM - Add Profile – Guest Registration

The **[*Guest Registration*]** panel has the function of configuring user self-registration, as shown in the image below:



Authentication - Portal Settings

In this panel we have the following fields:

- ***Enabled[ ]*:** If this check box is selected, user self-registration will be enabled in the system*;*
- ***Automatic account activation[ ]*:** If this check box is selected, when creating the account the user will be automatically enabled to use the system. Note that with this option enabled, no confirmation or release by the administrator will be required;
- ***Allowed Groups*:** This field determines which groups accept self-registration of users in the system.

It's advisable that a group be created for self-registration only, as in to distinguish the users registered by the administrator.

Attention: By checking the "Automatic Account activation" checkbox, no confirmation will be requested and access to registered users will be released immediately.

Next, we will analyze the *Personal Information* panel.

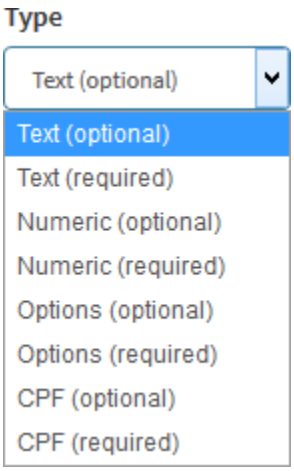
UTM - Add Profile – Personal Information

In the **[Personal Information]** panel, it is possible to add form fields to record information regarding the users who will register in the system, as shown in the image below:

Authentication - Portal Settings

By clicking on the **[ ]** button, you can add fields:

- ***Field*:** Determines what the field of the form will be, it is in this text box that the text to be typed to refer to the field of the form is determined. Ex.: Department*;*
- ***Type*:** If the type of data to be recorded by these fields is determined, it is possible to determine whether the type will be optional (“optional”) or mandatory (“required”). The possible options can be seen in the image below:



Authentication - *Type*

- ***Characters*:** Determines the amount of characters that the field will have. Ex.: 30*;*
- ***Rows*:** Determines the amount of lines that will be available in the form field. Ex.: 1.

Next, we will analyze the *Social Login* panel.

UTM - Add Profile – Social Login

Instead of forcing the user to create a new specific login account, the social login uses the information existing on a social network to log in Single Sign-on to Blockbit NGFW. By allowing the use of credentials already used in social media, access is facilitated since the user does not need to save multiple registration information for various sites. This feature is especially useful for casual users (guests).

This functionality uses the OAuth 2 feature that acts by delegating partial connection to some social media server functionalities to the third party application, thus allowing limited access but without sharing the credentials.

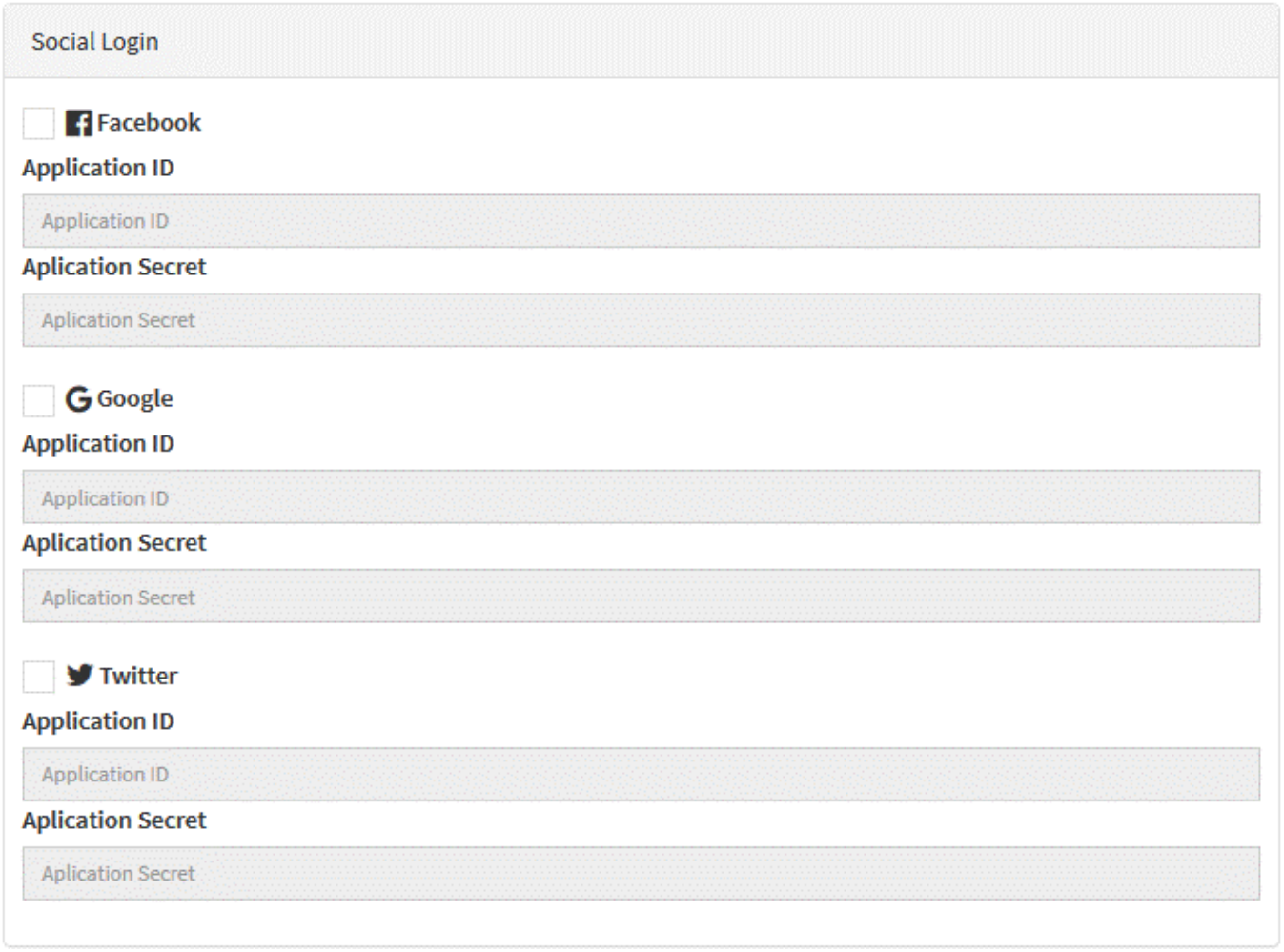
Blockbit NGFW allows Social Login on the following platforms:

- ***Facebook:*** Using *Facebook Developers*;
- ***Google:*** *Through Google APIs*;
- ***Twitter:*** Using *Twitter Apps*.

To use Social Login, it is necessary to configure the social media service correctly and receive authorization from their servers, however regardless of the particularities of the selected platform, it is necessary to obtain the ID and the Application Secret to inform in this panel of the NGFW.

For an easy understanding, see this page for an example of how to set up Social Login on Google APIs.

In this panel it is possible to enable login through social networks:



Authentication – *Social Login*

The fields available on the form are:

- ***Facebook [ ]*:** This checkbox allows you to enable login via “Facebook”*;*
  - ***Application ID*:** Determines the Facebook application ID;
  - ***Application Secret*:** Determines the secret key used to log into Facebook;
- ***Google [ ]*:** This checkbox allows you to enable login via “Google”, click on this *link* to see an example of how to set up Social Login on Google*;*
  - ***Application ID*:** Determines the Google Application ID;
  - ***Application Secret*:** Determines the secret key used to log in to Google;
- ***Twitter [ ]*:** This checkbox allows you to enable login via “Twitter”*;*
  - ***Application ID*:** Determines the Twitter application ID;
  - ***Application Secret*:** Determines the secret key used to log into Twitter;

Next, we'll look at the *Available Options* panel.

Social Login - Example: Setting up Social Login in Google APIs

In order to facilitate understanding, this session will present an example of how to configure Social Login to allow access through a Google account.

 The only differences in the configuration of Social Login are related to the registration process on the chosen platform (Google, Facebook or Twitter). However, regardless of the platform, it is necessary to obtain the Application ID and Secret to configure the *Social Login* panel.

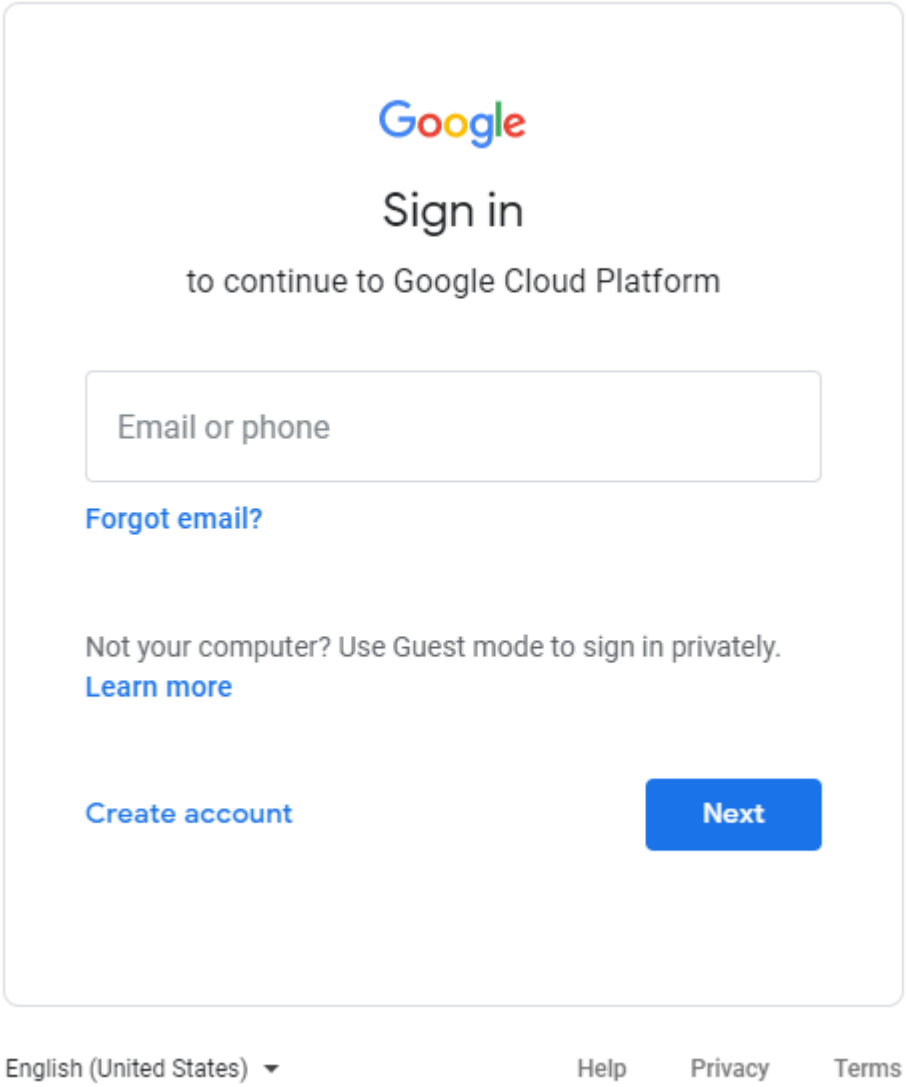
In this example we will perform the following steps:

- Google Developers Registration;
- Google APIs setup;
- Configuring Social Login in the NGFW;
- User registration by Social Login;
- Access to the portal through Social Login.

This example will not go into detail about each field in the portal creation panel, if you want more information about it, see this page.

Google Developers Registration

Initially go to the Google Developers URL: https://console.developers.google.com/projectselector/apis/credentials, the following screen will appear:

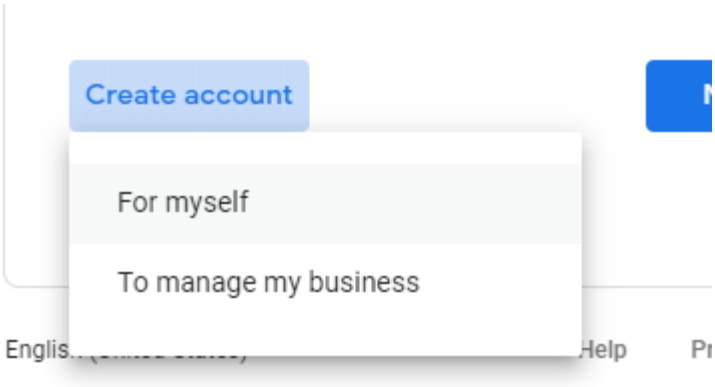


Google Sign in

Note that it is possible to use an existing account (or an email), if you already have an account that you want to use it is not necessary to create a new one.

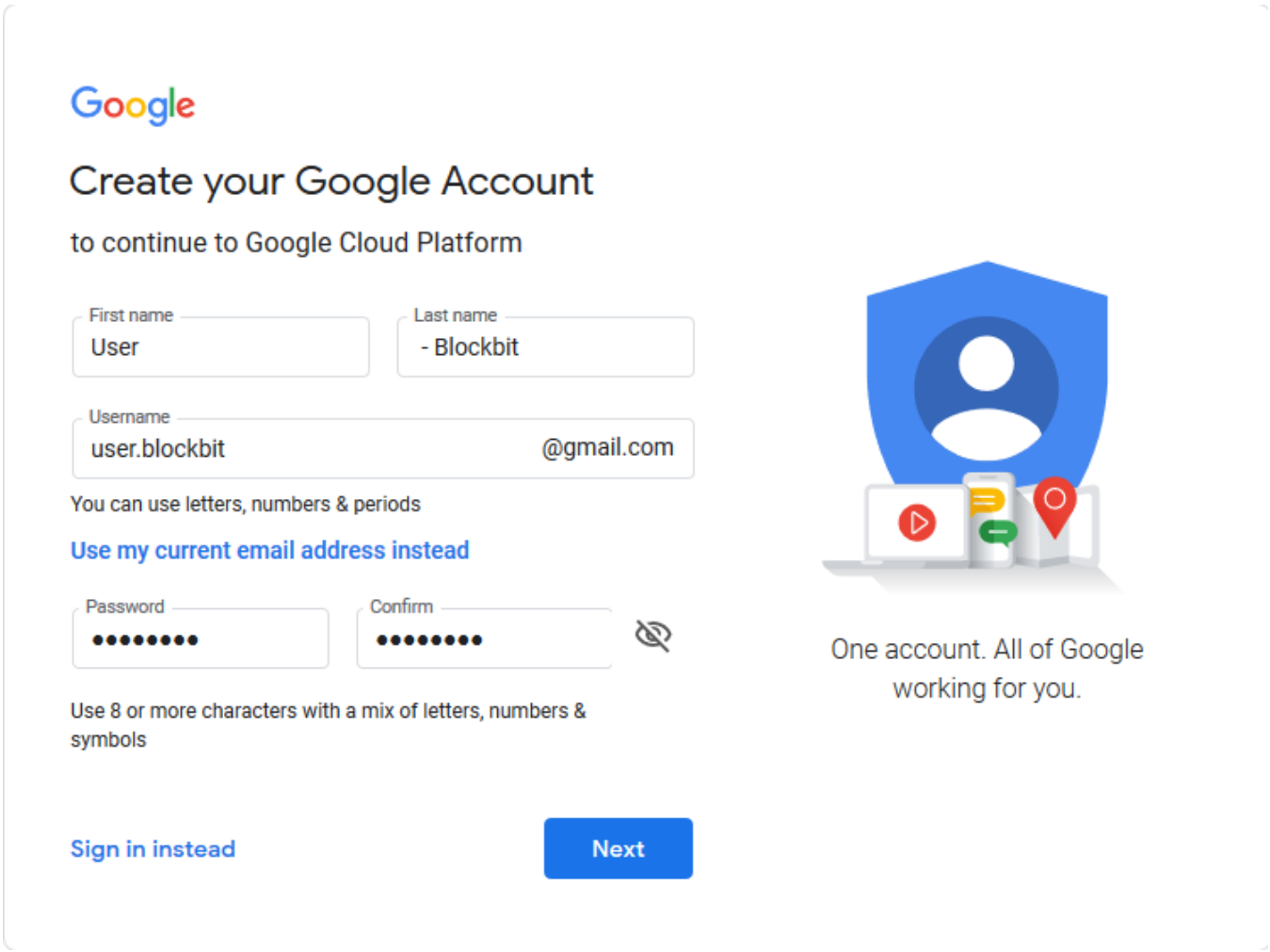
In this example we will create a new account to be used specifically for this procedure.

Click **Create Account** and select the option **To manage my business**:

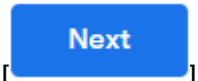


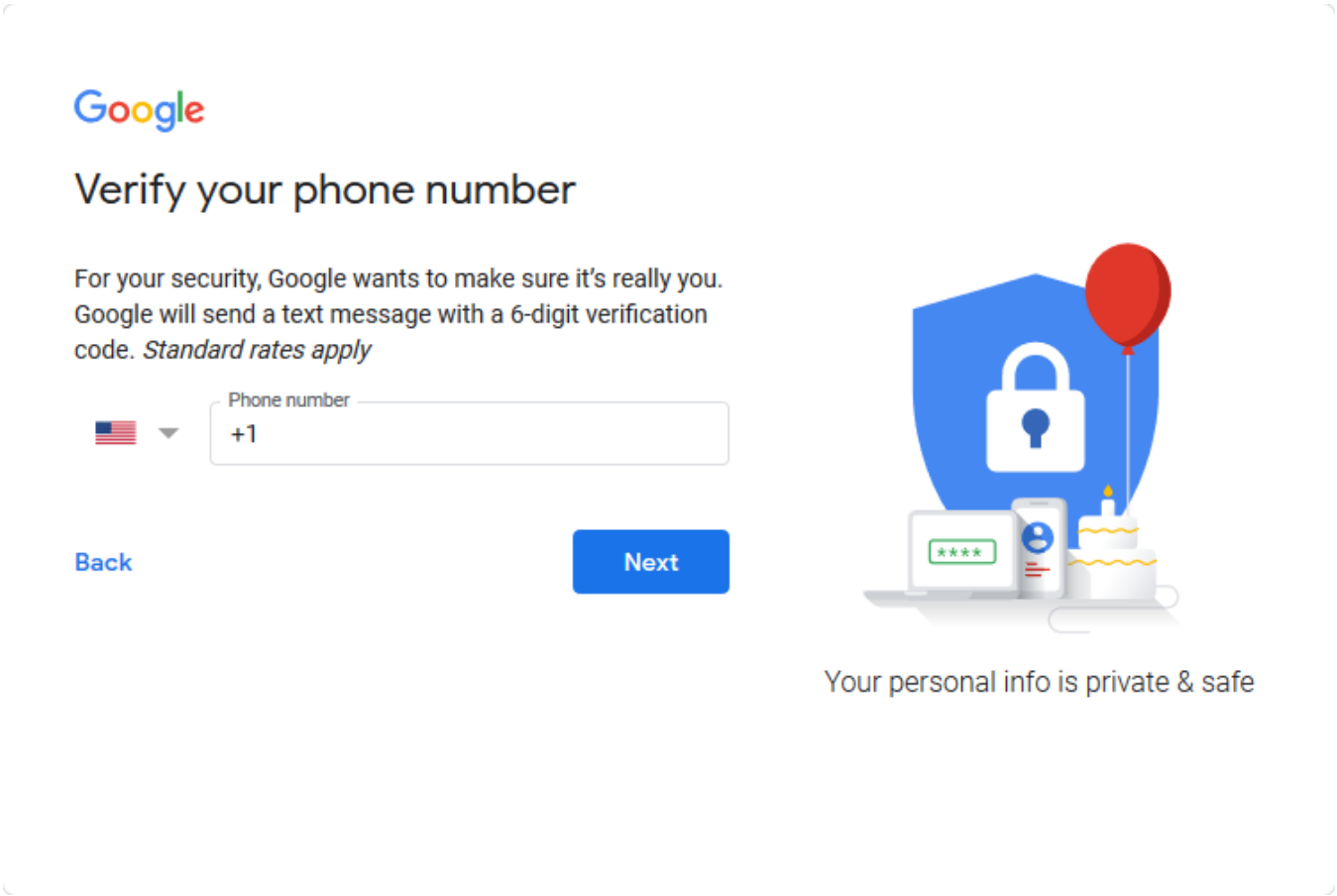
Google Sign In - Create Account

When the screen below is displayed, fill in the fields with the data of the new account to be created, in this example we will create an email exclusively for this procedure as well:



Google Sign In - Create your Google Account

After completing the relevant data, click **[**  **]** to proceed to the next step, the following screen will be displayed:

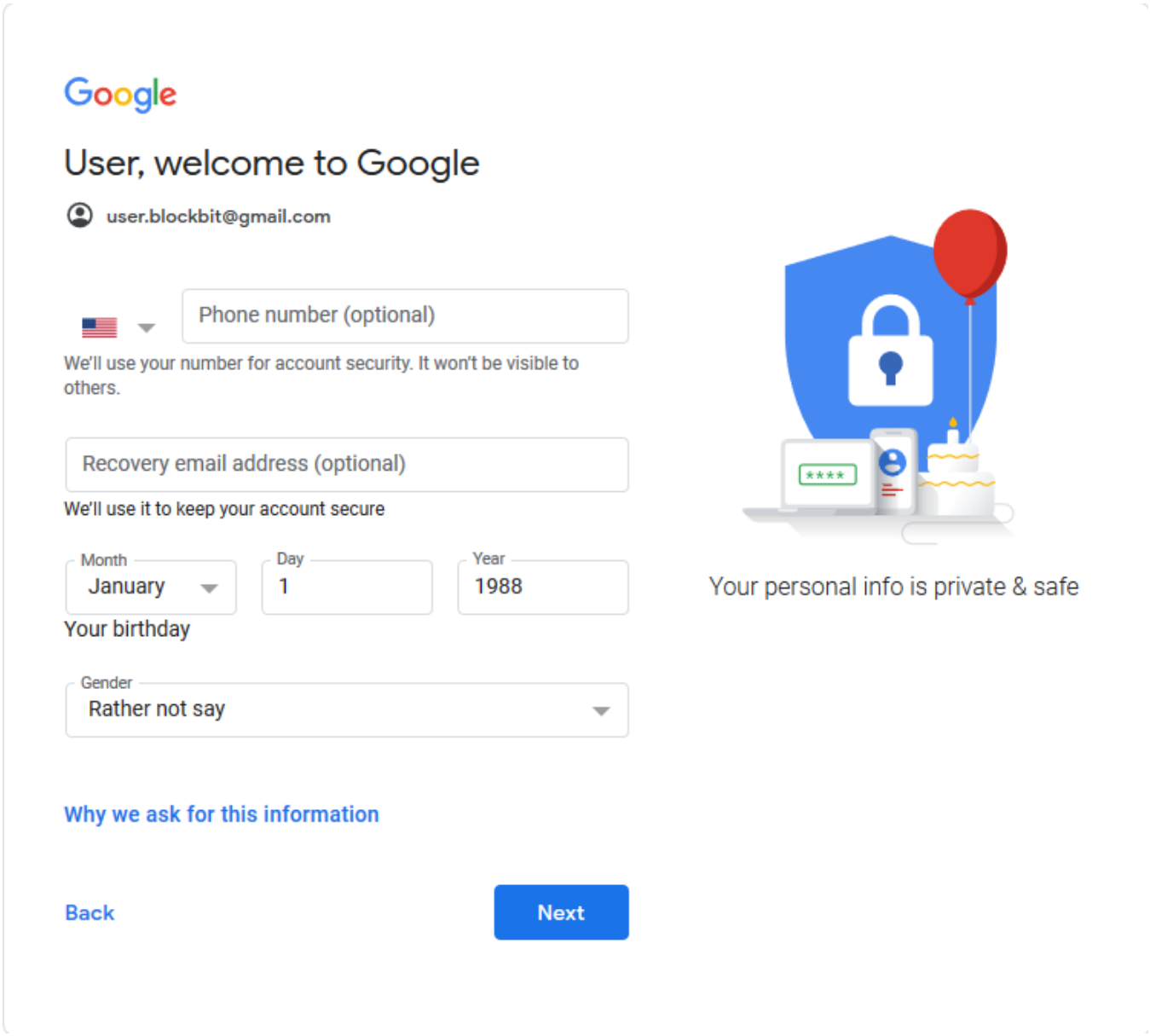


Google Sign In - Verify your phone number

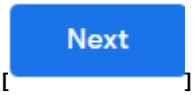
Add a phone number to verify the account and click **[** Next **]**.

> If you already have a Google account with the linked number, just use the same.

You will receive a confirmation code from Google, type it in the appropriate field and click **[** Verify **]** to confirm and go to the next step.



Google Sign In - Personal info



Complete with the user's personal information and click **[ ]** to continue. As you proceed, you'll be asked to accept Google's terms of engagement:

Google

Privacy and Terms

To create a Google Account, you'll need to agree to the Terms of Service below.
In addition, when you create an account, we process your information as described in our Privacy Policy, including these key points:

Data we process when you use Google

- When you set up a Google Account, we store information you give us like your name, email address, and telephone number.
- When you use Google services to do things like write a message in Gmail or comment on a YouTube video, we store the information you create.
- When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity – including information like the video you watched, device IDs, IP addresses, cookie data, and location.
- We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player.

Why we process it
We process this data for the purposes described in our policy, including to:

- Help our services deliver more useful, customized content such as more relevant search results;
- Improve the quality of our services and develop new ones;
- Deliver personalized ads, depending on your account settings, both on Google services and on sites and apps that partner with Google;
- Improve security by protecting against fraud and abuse; and
- Conduct analytics and measurement to understand how our services are used. We also have partners that measure how our services are used. Learn more about these specific advertising and measurement partners.

Combining data
We also combine this data among our services and across your devices for these purposes. For example, depending on your account settings, we show you ads based on

You're in control of the data we collect & how it's used

information about your interests, which we can derive from your use of Search and YouTube, and we use data from trillions of search queries to build spell-correction models that we use across all of our services.

You're in control
Depending on your account settings, some of this data may be associated with your Google Account and we treat this data as personal information. You can control how we collect and use this data now by clicking "More Options" below. You can always adjust your controls later or withdraw your consent for the future by visiting My Account (myaccount.google.com).

MORE OPTIONS

Cancel I agree

Google Sign In - Privacy and Terms

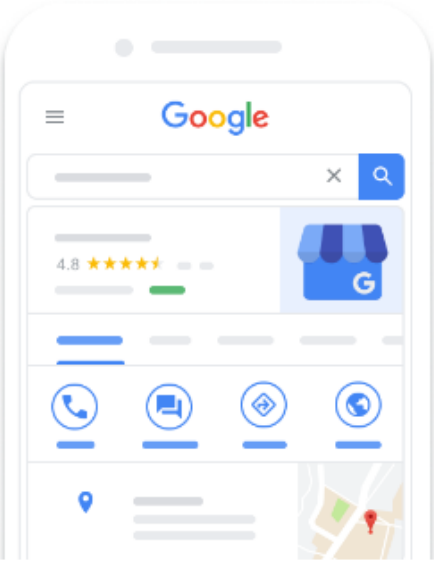
After reading the terms, click [I agree] to continue.

Google

Your Google Account is all set - now add your Business Profile

user.blockbit@gmail.com

Create your free Business Profile and let customers discover your business on Search and Maps



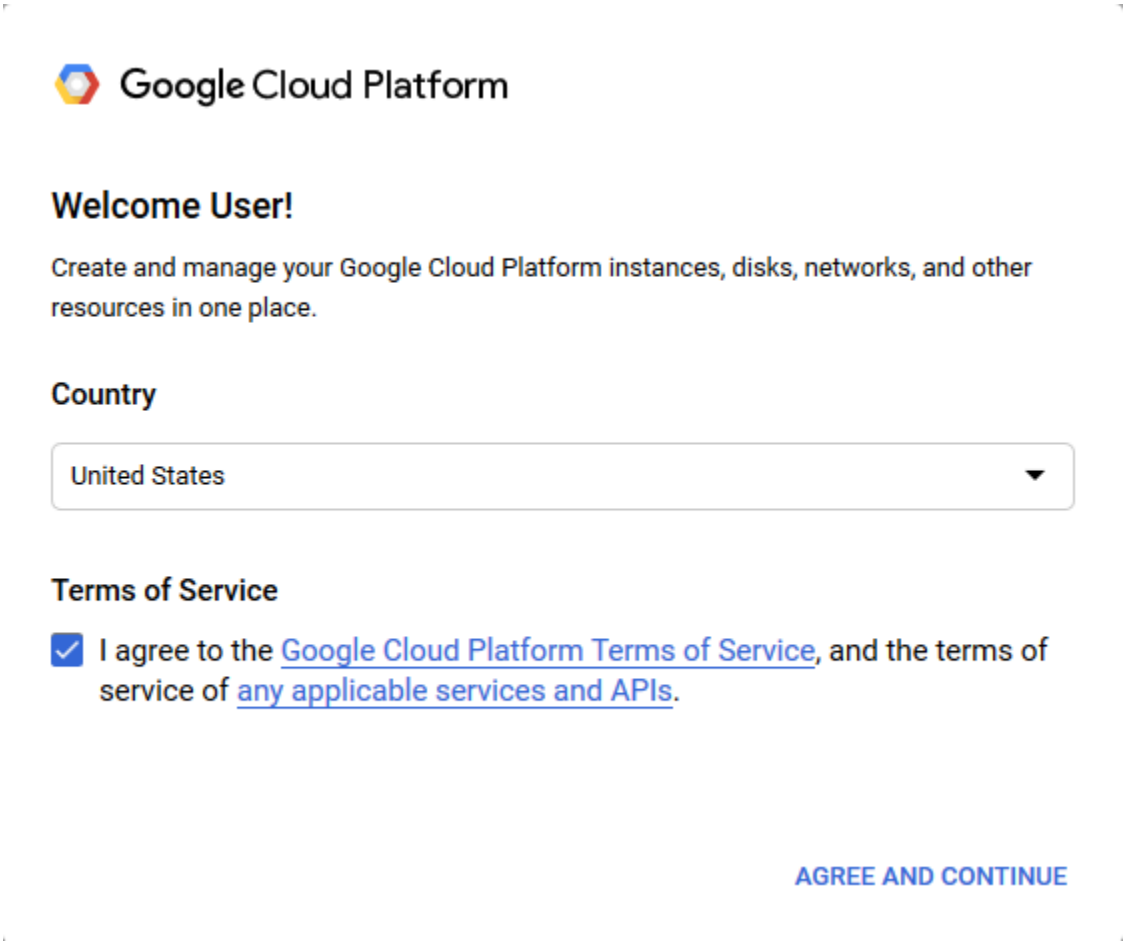
Not Now Continue

Google Sign In - Account is all set

Not Now

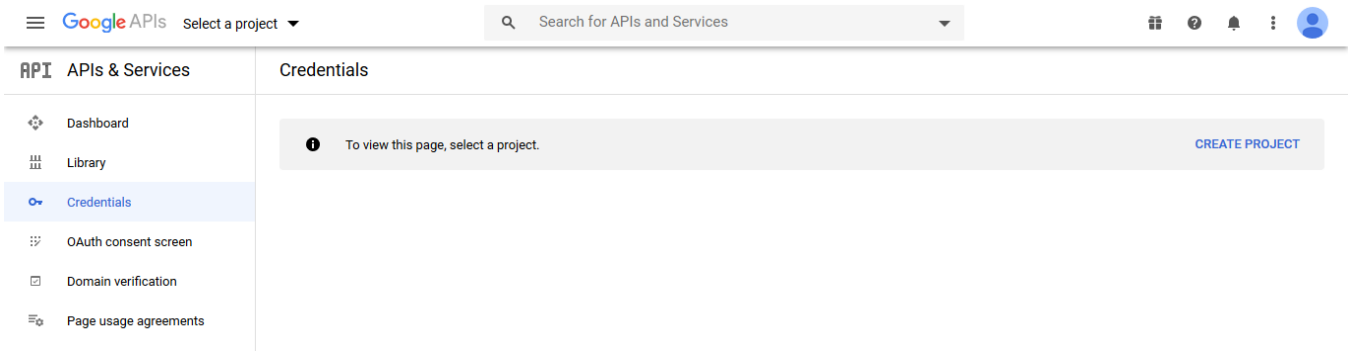
After reading the terms, click **[** **]** to be redirected directly to the ***Google APIs***.

The following pop-up will appear automatically:



Google Cloud Platform - Welcome Pop-up

Check the **[** **]** checkbox and click **[**AGREE AND CONTINUE**]** to access the Google APIs*:*

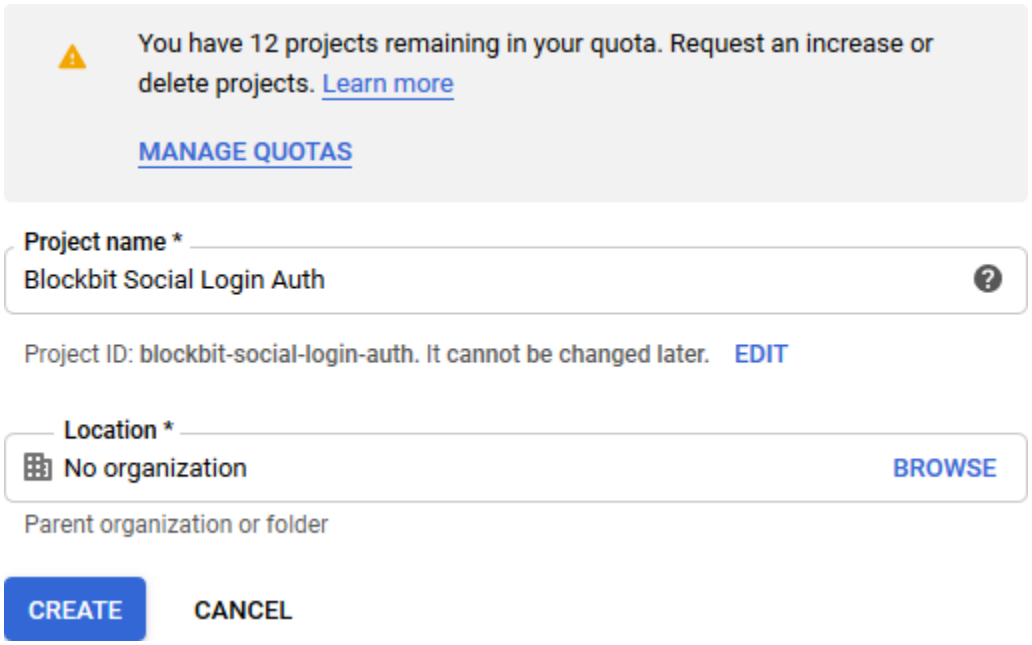


Google APIs - Credentials

Next, we will perform the Google APIs Configuration.

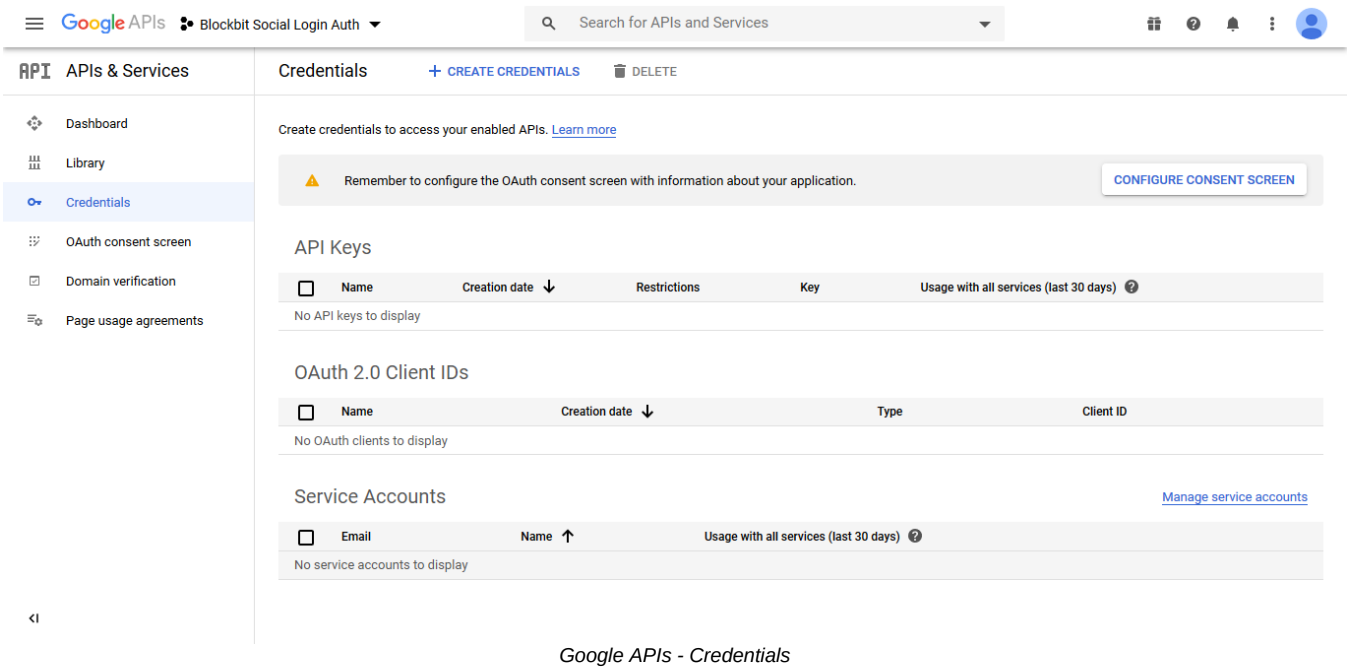
Google APIs setup

To configure social login on Blockbit NGFW, it is necessary to create a new credential. To do this, click [CREATE PROJECT].



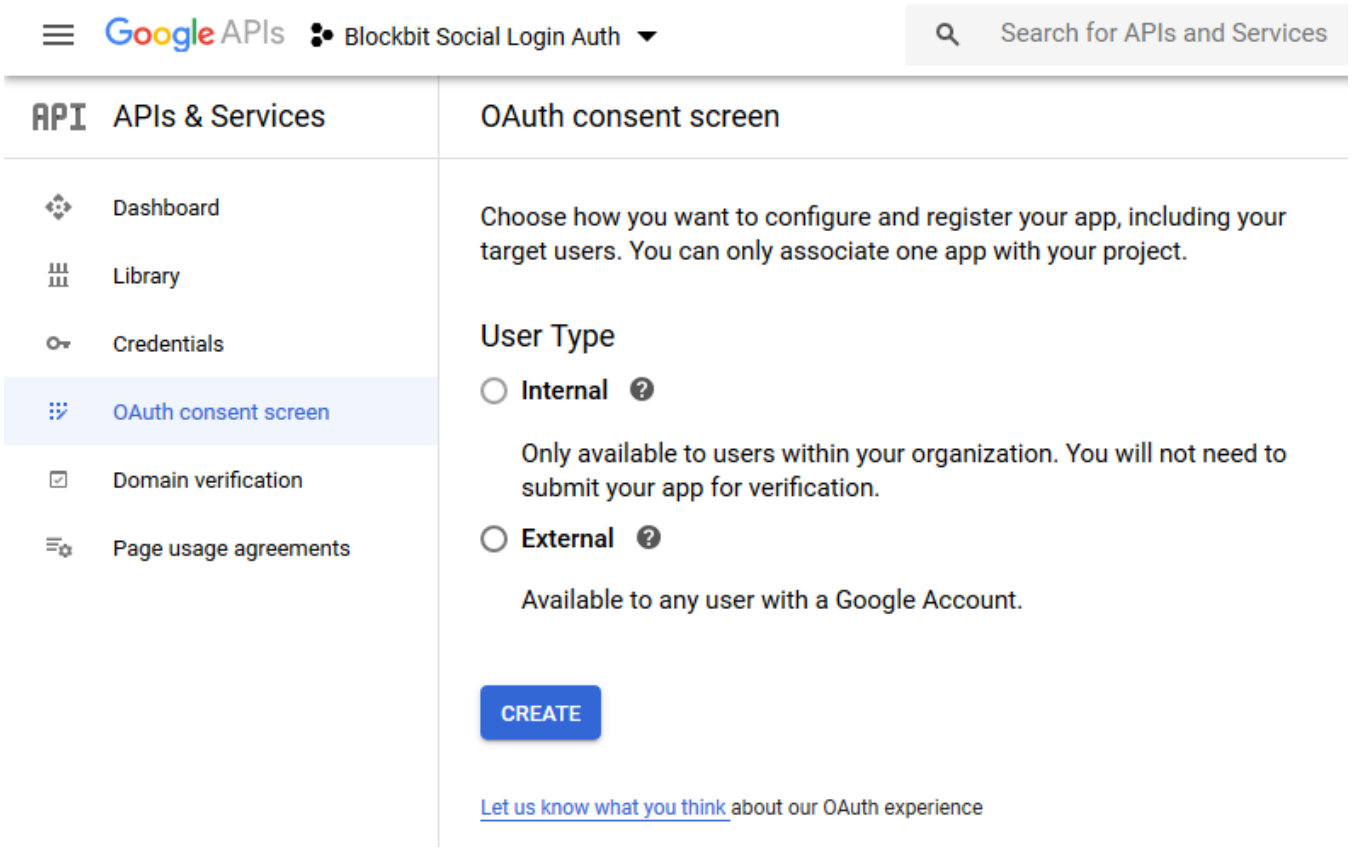
Google APIs - Create Project

Complete the **Project Name** field with the desired name and note that the project ID cannot be changed later, if you want to change it, click [EDIT] in this example the ID will not be changed. To proceed, click [CREATE], the following page will be displayed:



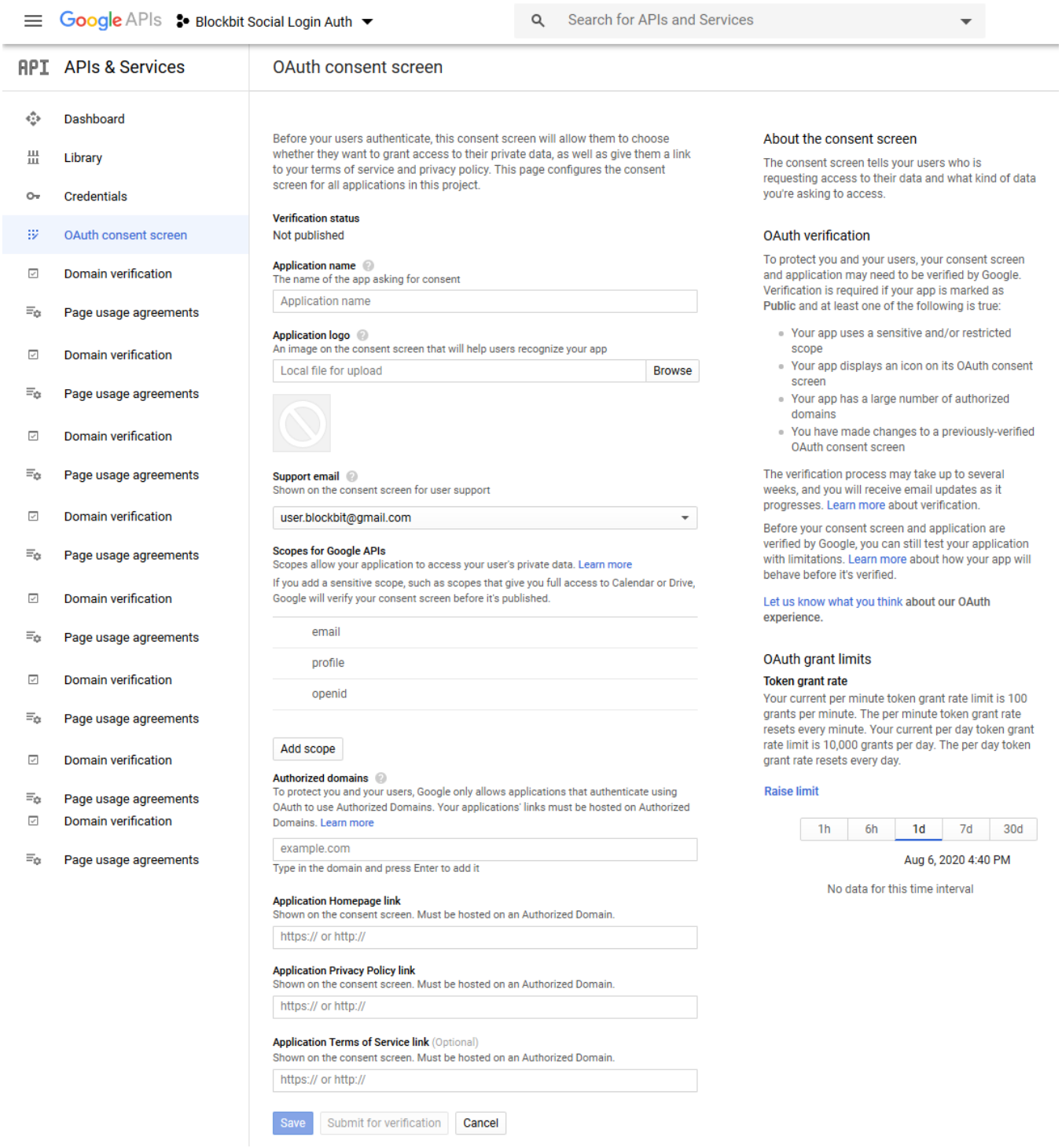
Google APIs - Credentials

After creating the project, as mentioned in the message at the top of the screen, you will need to configure OAuth consent, to do so, click [CONFIGURE CONSENT SCREEN].



Google APIs - OAuth consent screen - User Type

Select the **External** option to configure access for any user who has a Google account, once this is done, click [CREATE].



Google APIs - OAuth consent screen

Complete the form as indicated:

- ***Application Name:*** Enter the desired name. This field is required. Eg: "Portal BB";
- ***Authorized Domains:*** Type the domain that will be used and hit "Enter". Ex.: "blockbit.com";
- ***Application Homepage Link*****:** Enter the location of your NGFW homepage. Ex.: https://utm-example.blockbit.com
- ***Application Privacy Policy Link*****:** Enter the portal address. This field is required. Ex.: https://utm-example.blockbit.com:9803/apps/auth-login.php

When you finish completing the form on this screen, it will be as shown below:

OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status
Not published

Application name
The name of the app asking for consent

Portal BB

Application logo
An image on the consent screen that will help users recognize your app

Local file for upload | Browse

Support email
Shown on the consent screen for user support

user.blockbit@gmail.com

Scopes for Google APIs
Scopes allow your application to access your user's private data. Learn more

If you add a sensitive scope, such as scopes that give you full access to Calendar or Drive, Google will verify your consent screen before it's published.

- email
- profile
- openid

Add scope

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

blockbit.com

example.com

Type in the domain and press Enter to add it

Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.

https://utm-example.blockbit.com

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.

https://utm-example.blockbit.com:9803/apps/auth-login.php

Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

About the consent screen

The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification

To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. Learn more about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. Learn more about how your app will behave before it's verified.

Let us know what you think about our OAuth experience.

OAuth grant limits

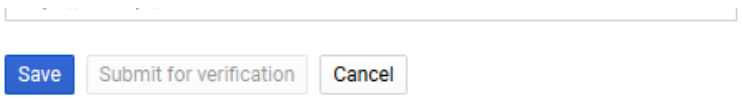
Token grant rate
Your current per minute token grant rate limit is 100 grants per minute. The per minute token grant rate resets every minute. Your current per day token grant rate limit is 10,000 grants per day. The per day token grant rate resets every day.

Raise limit

1h | 6h | **1d** | 7d | 30d

Aug 7, 2020 11:11 AM

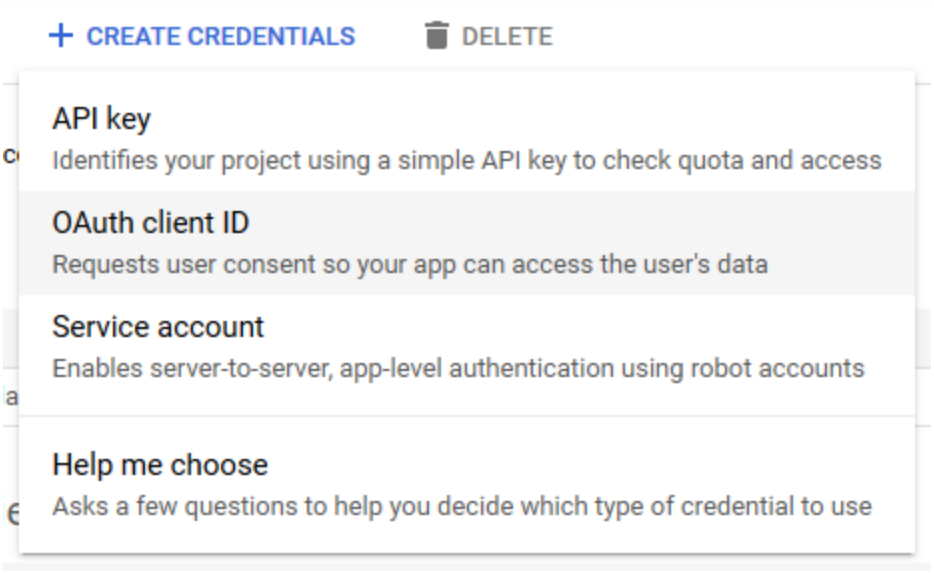
No data for this time interval



Google APIs - OAuth consent screen - Form

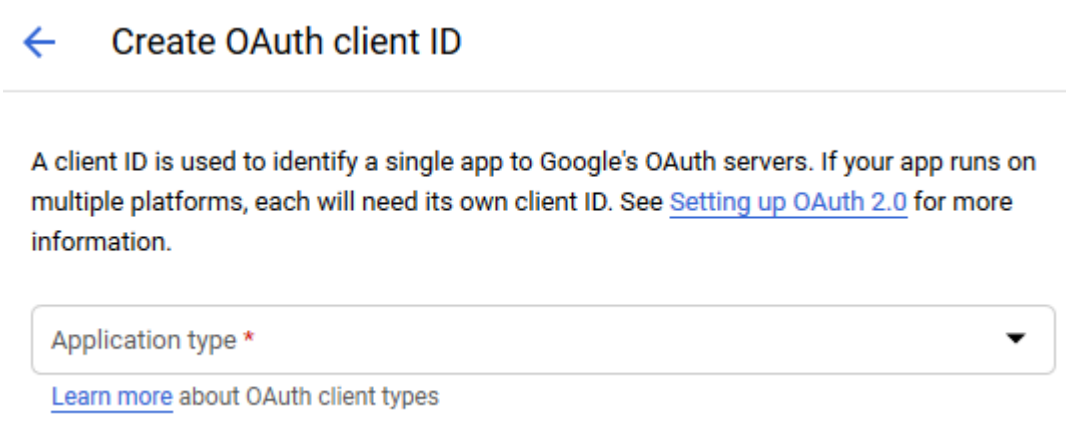
Finally, click [Save] to save the settings.

That done, in the left side menu, click [Credentials] to return to Google APIs - Credentials and click the [+ CREATE CREDENTIALS] option located at the top of the screen:



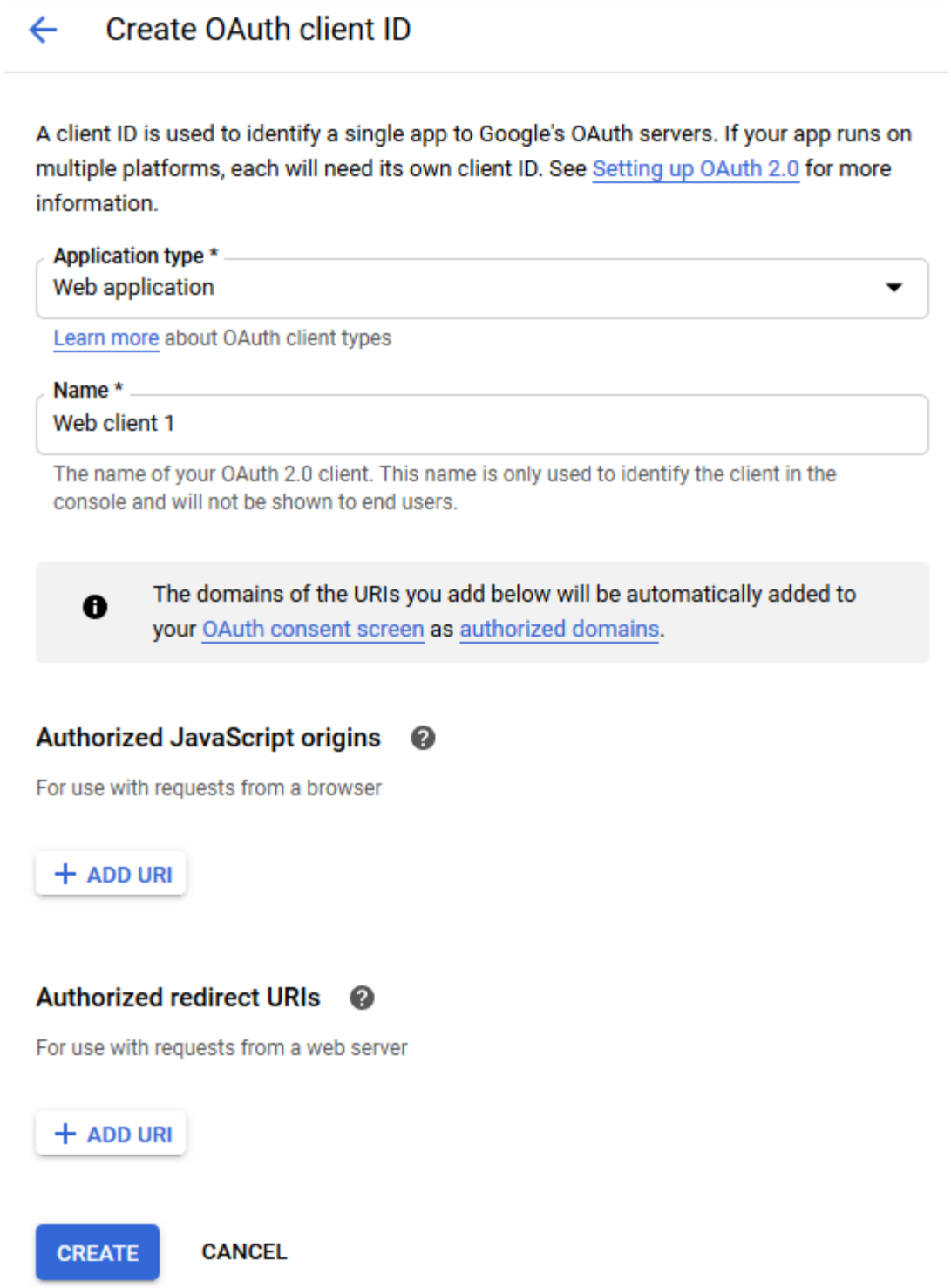
Google APIs - Credentials - Create Credentials

Select the option "Oauth client ID", this is the function used by Blockbit NGFW to perform the logins, the following screen will be displayed.



Google APIs - Credentials - Create OAuth client ID

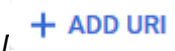
Click on the "Web Application" option, when making the selection, the form below will be displayed:



Google APIs - Credentials - Create OAuth client ID - Web Application

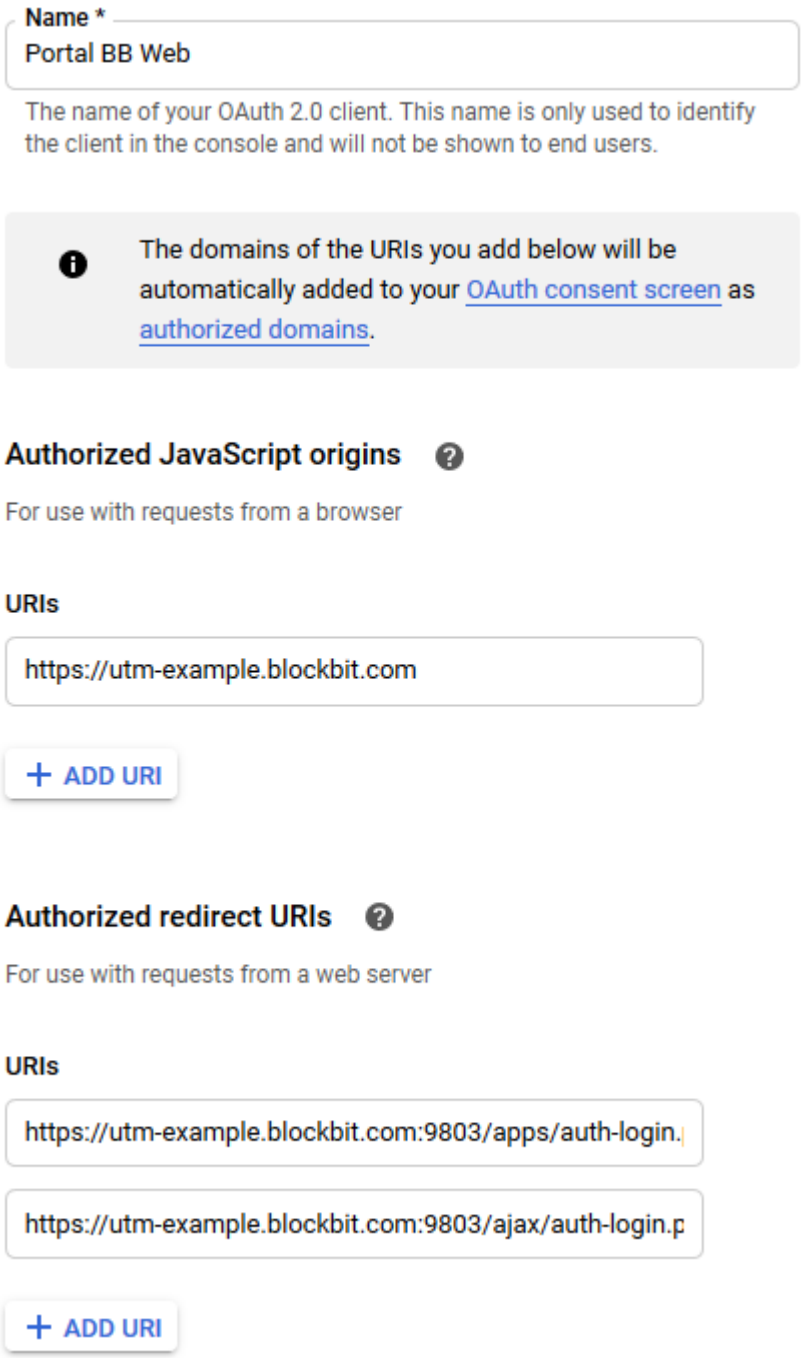
Complete the form as indicated:

In **Name**, type the name that will be used by the client 0Auth 2.0. Ex.: "Portal BB Web";

Right under ***Authorized JavaScript origins*** click on ***[***  ***]*** and add the URI that will be used by the Client. In this example we will use "https://utm-example.blockbit.com".

In ***Authorized redirect URIs*** click ***[*** + ADD URI ***]*** and add the URL for the full authentication portal. In the example we will add: https://utm-example.blockbit.com:9803/apps/auth-login.php and https://utm-example.blockbit.com:9803/ajax/auth-login.php?act=socialLogin&social=google.

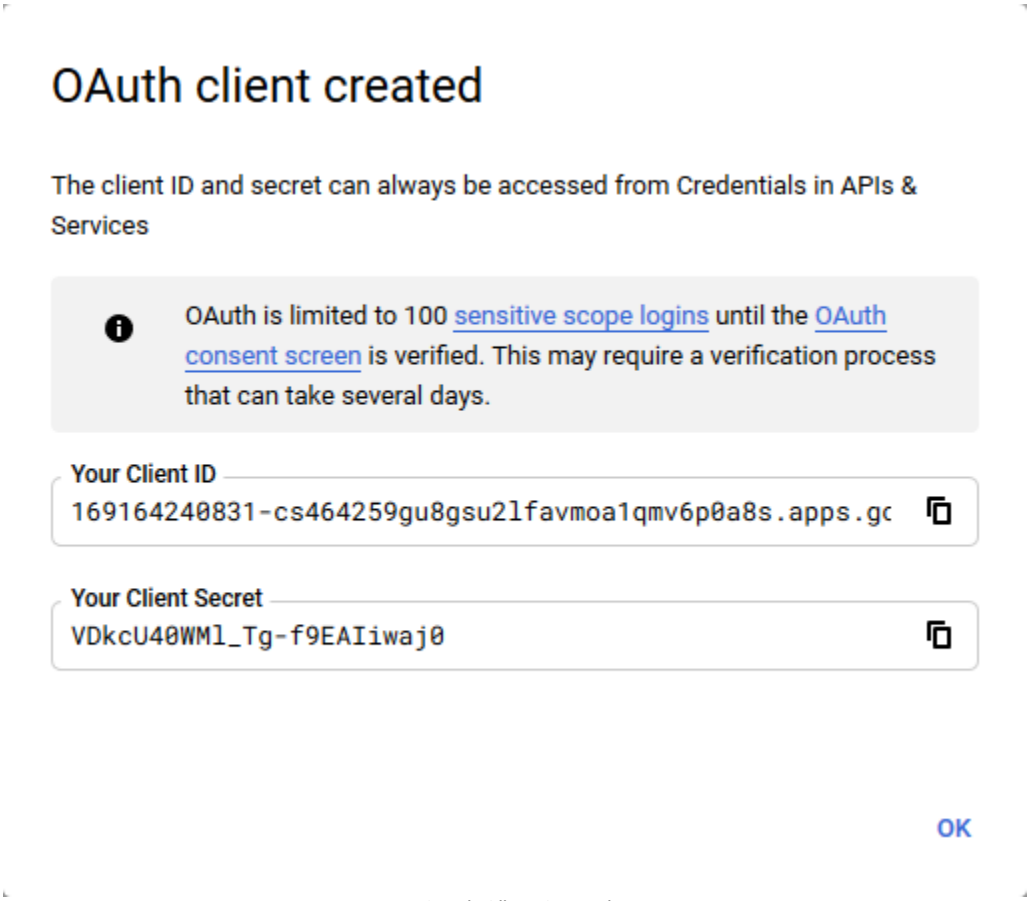
When you finish completing the form on this screen, it will be as shown below:



Google APIs - Credentials - Create OAuth client ID - Web Application - Form

Finally, click **[** CREATE **]** to save the settings.

The following window will be displayed confirming the creation of the 0Auth Client:

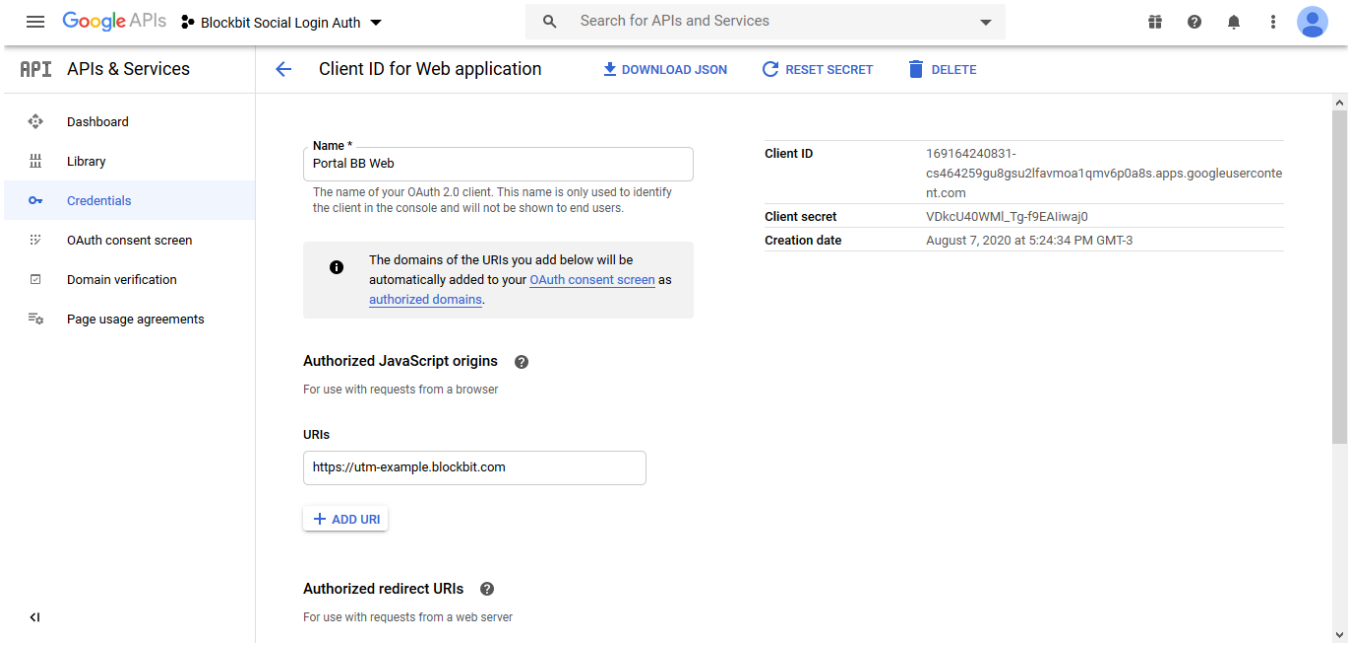


OAuth Client Created

On this screen, your **Client ID** and **Client Secret** will be available. This is exactly the two information needed to configure the NGFW Portal.

Click the **[** **]** icon to copy both information. Click **[** OK **]** when you are ready to close this window.

In case you end up losing these two information, just click on **[** Credentials **]** and on **OAuth 2.0 Client IDs** click on the **[** **]** icon, the screen with the information already registered will be displayed, however an extra panel will be available on the right informing the **Client ID** and **Client Secret**.

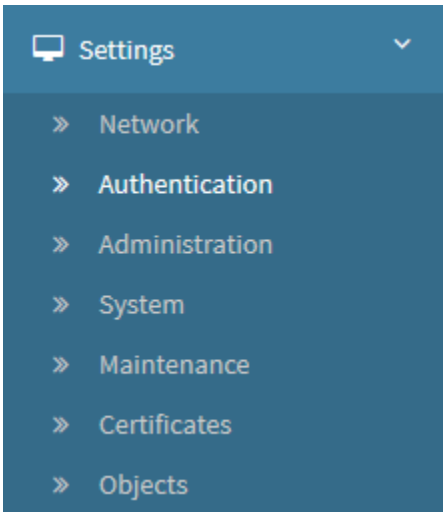


Client ID for Web application - Edit

This ends the configuration of Google APIs, having the **Client ID** and **Client Secret**, we can now make the settings for Social Login in the NGFW.

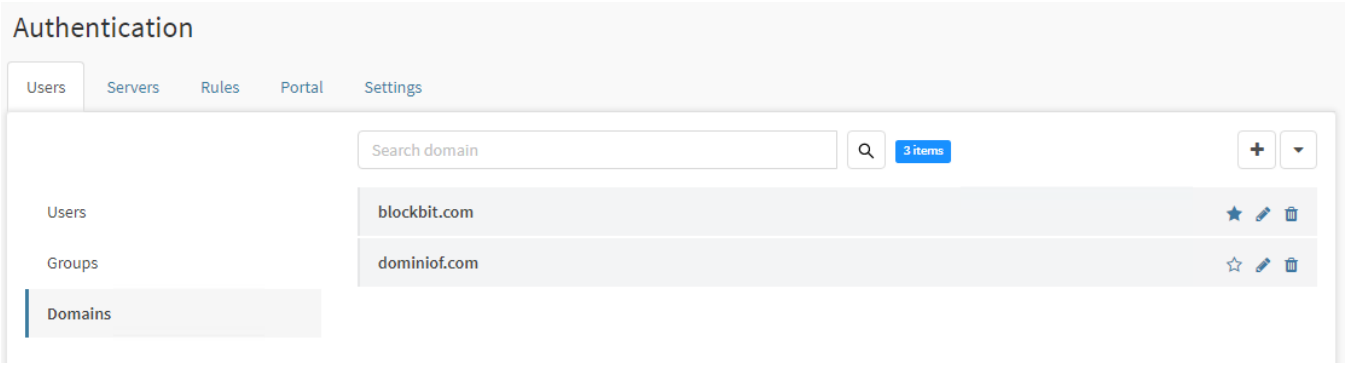
Configuring Social Login in the NGFW

Access the NGFW and in the side menu, click on Settings and select the option Authentication:



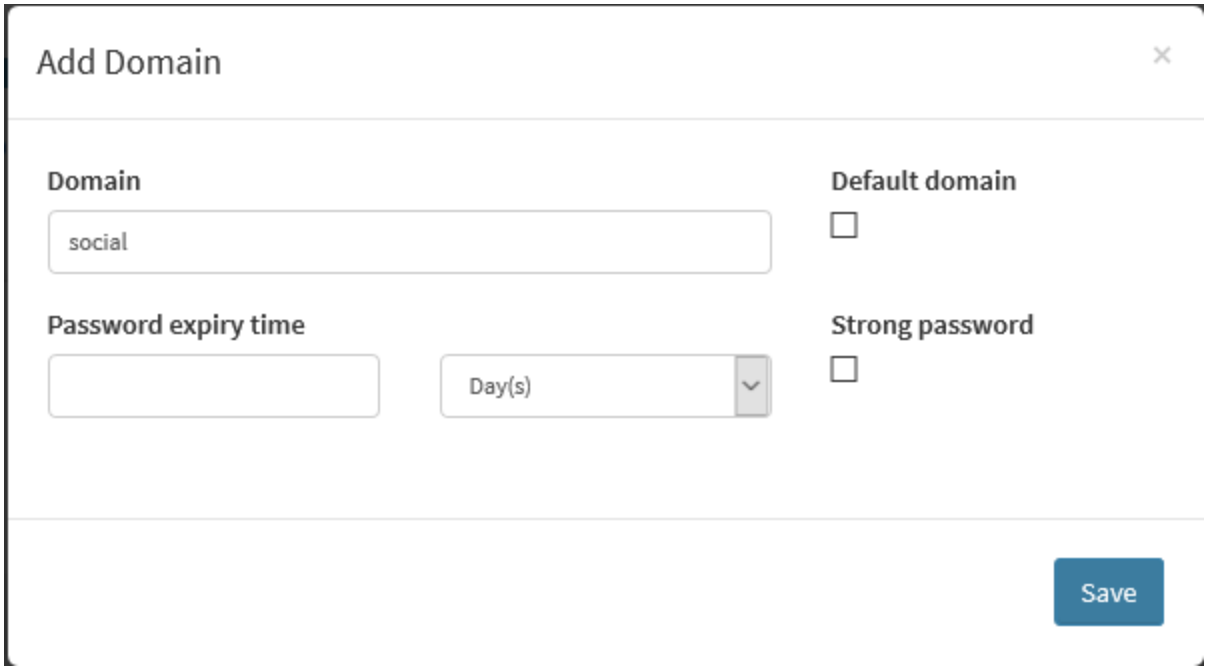
Settings - Authentication

Access the Users tab and select the Domains option on the side tab:



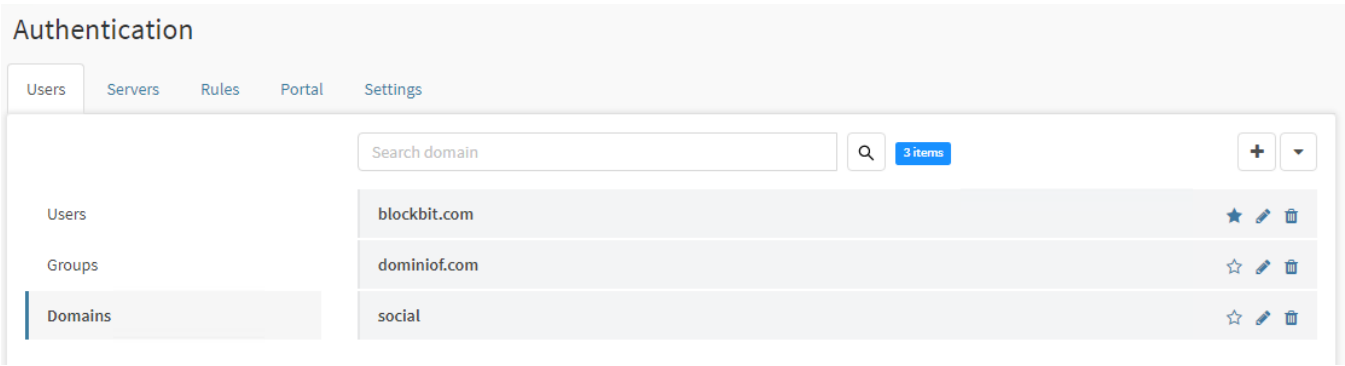
Settings - Authentication - Users Tab - *Domains*

Click on **[ ]** and complete the form to create a domain to be used specifically for authentication via Social Login, in this example the domain will be called "social".



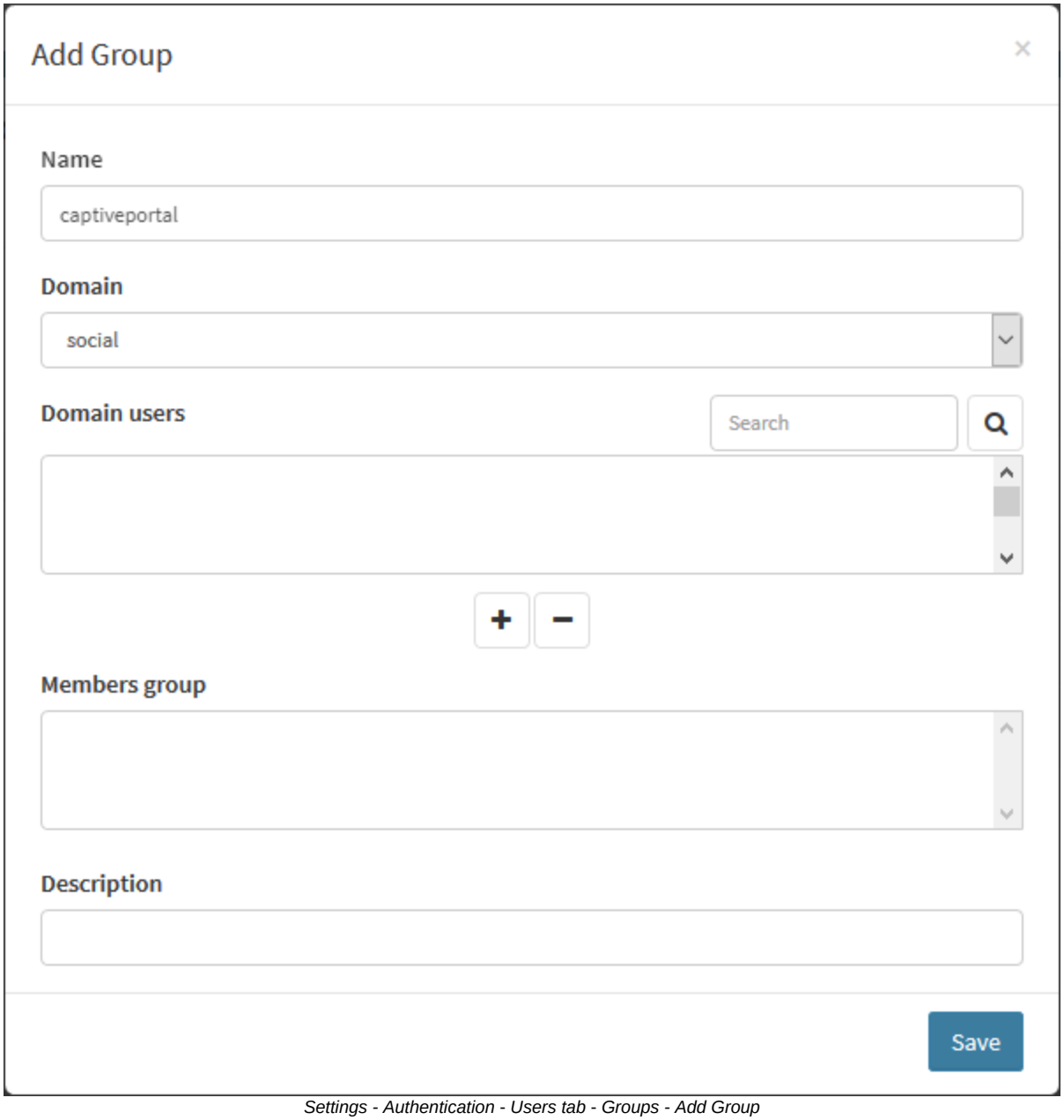
Settings - Authentication - Users tab - Domains - Add Domain

When finished, click [Save] to create the domain:



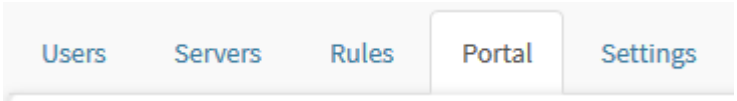
Settings - Authentication - Users tab - Domains

Now we are going to create a group for this domain, to do so, click on the Groups side tab and click [+] to complete the form and create a group. It will also be used specifically for authentication via Social Login, in this example the group will be called "captiveportal" and will use the domain we just created: "social".



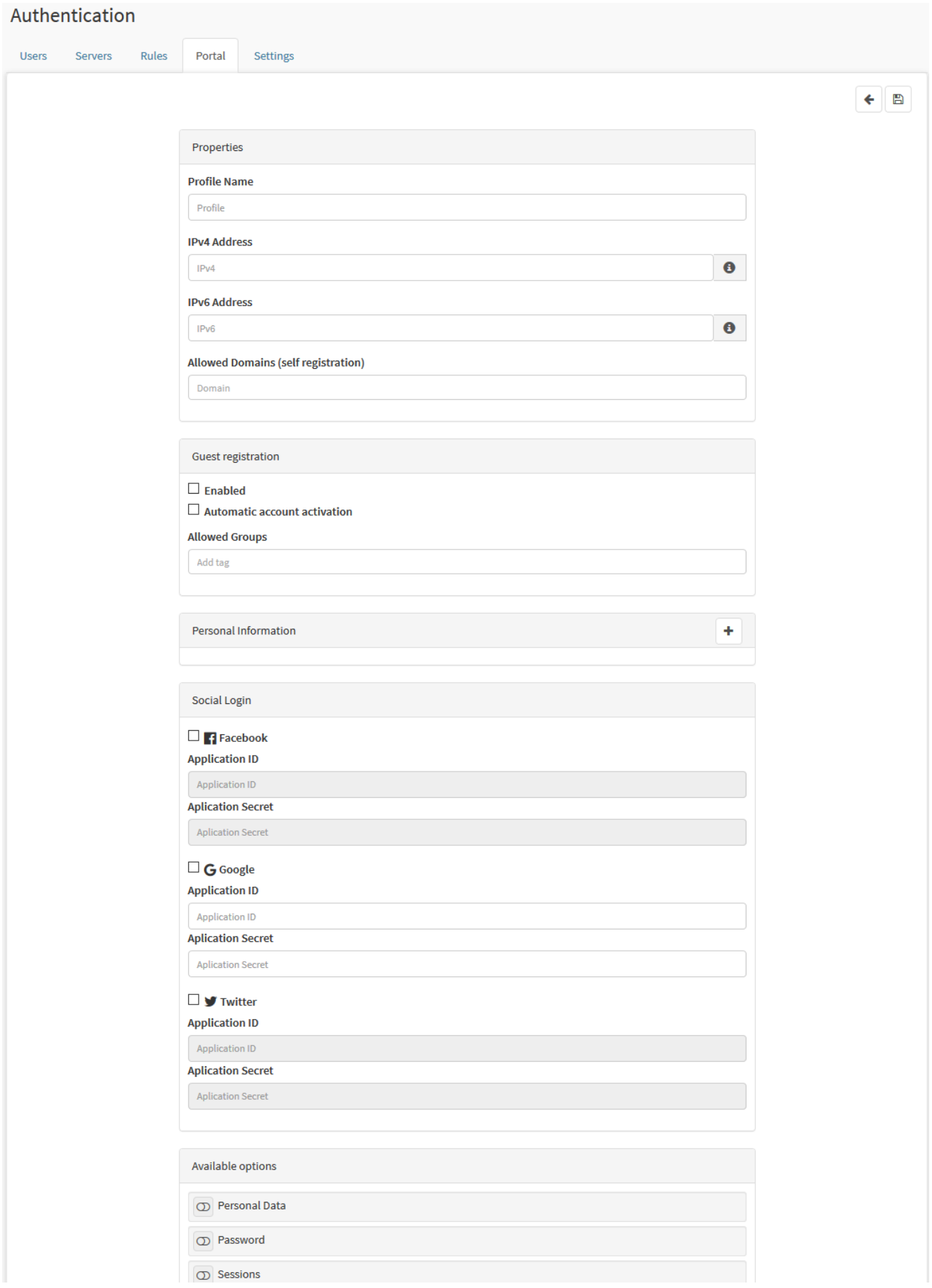
Settings - Authentication - Users tab - Groups - Add Group

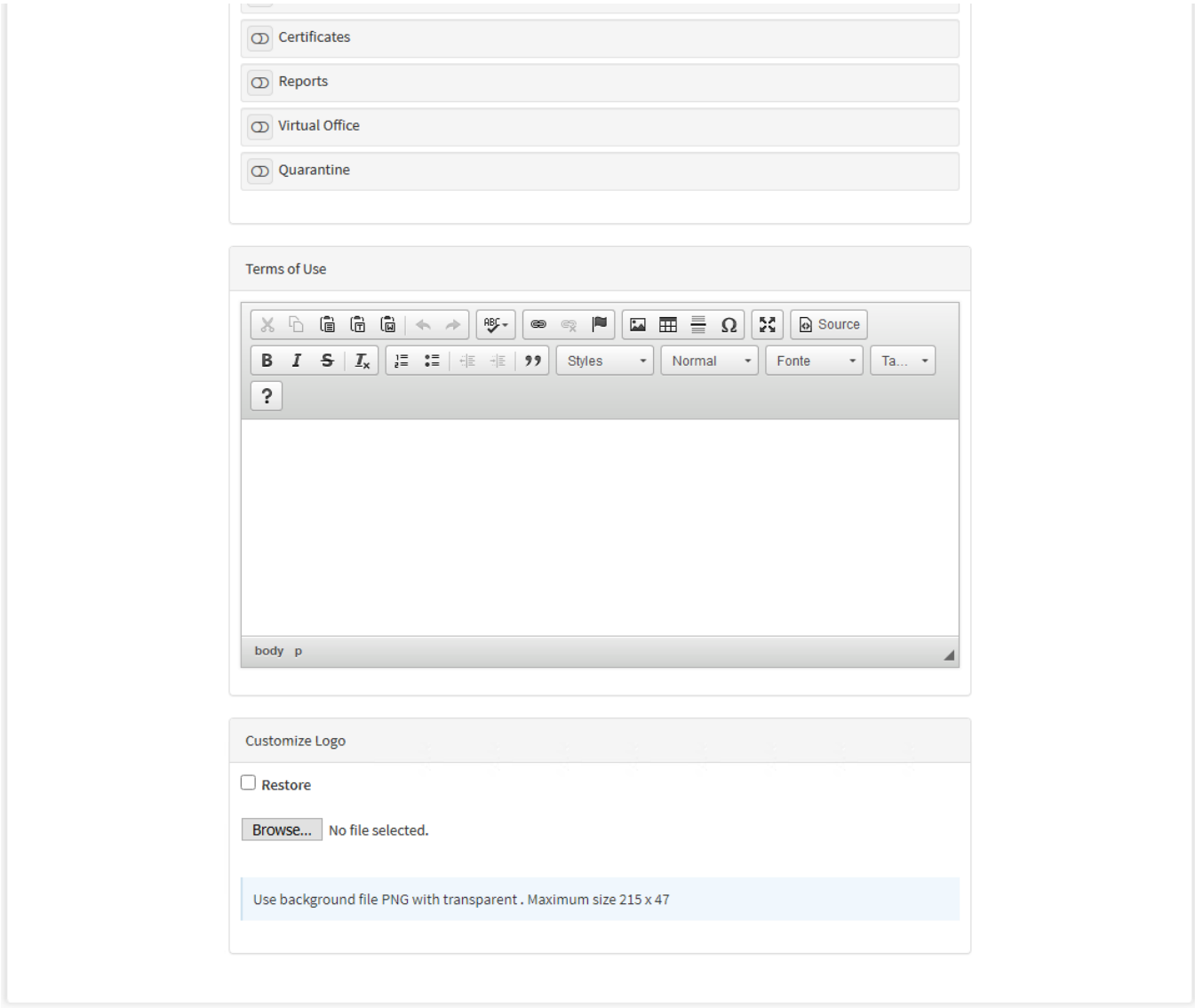
Finally, let's configure Social Login, access the Portal tab



Settings - Authentication - Portal tab

*Click **[ ]** to set up a new portal*.


Authentication
Users
Servers
Rules
Portal
Settings
Properties
Profile Name
Profile
IPv4 Address
IPv4
IPv6 Address
IPv6
Allowed Domains (self registration)
Domain
Guest registration
Enabled
Automatic account activation
Allowed Groups
Add tag
Personal Information
Social Login
Facebook
Application ID
Application ID
Aplication Secret
Aplication Secret
Google
Application ID
Application ID
Aplication Secret
Aplication Secret
Twitter
Application ID
Application ID
Aplication Secret
Aplication Secret
Available options
Personal Data
Password
Sessions



Settings - Authentication - Portal tab

Fill out the form as shown:

Painel Properties

- ***Profile Name*:** Name the profile Social Login;
- ***IPv4 Address*:** Add the portal IP;
- ***Allowed Domains*:** Add the domain we created in this example, in the case "social".

Guest Registration

- ***Enabled* [☑]:** Enable visitor registration;
- ***Automatic Account Activation* [☑]:** In this example we will allow visitor accounts to be activated automatically;
- ***Allowed Groups*:** Add the groups that will be used in the social login, in which case we will add the group created in the example: "captiveportal@social".

Social Login

- ***Google* [☑]:** Enable social login via Google;
- ***Application ID*:** In this field, add the code that appears in the Google Client ID, in the example it would be: 169164240831-cs464259gu8gsu2lfavmoa1qmv6p0a8s.apps.googleusercontent.com;
- ***Application Secret*:** In this field, add the code that appears in Google's Client Secret, in the example it would be: VDkcU40WMl_Tg-f9EAliwaj0;

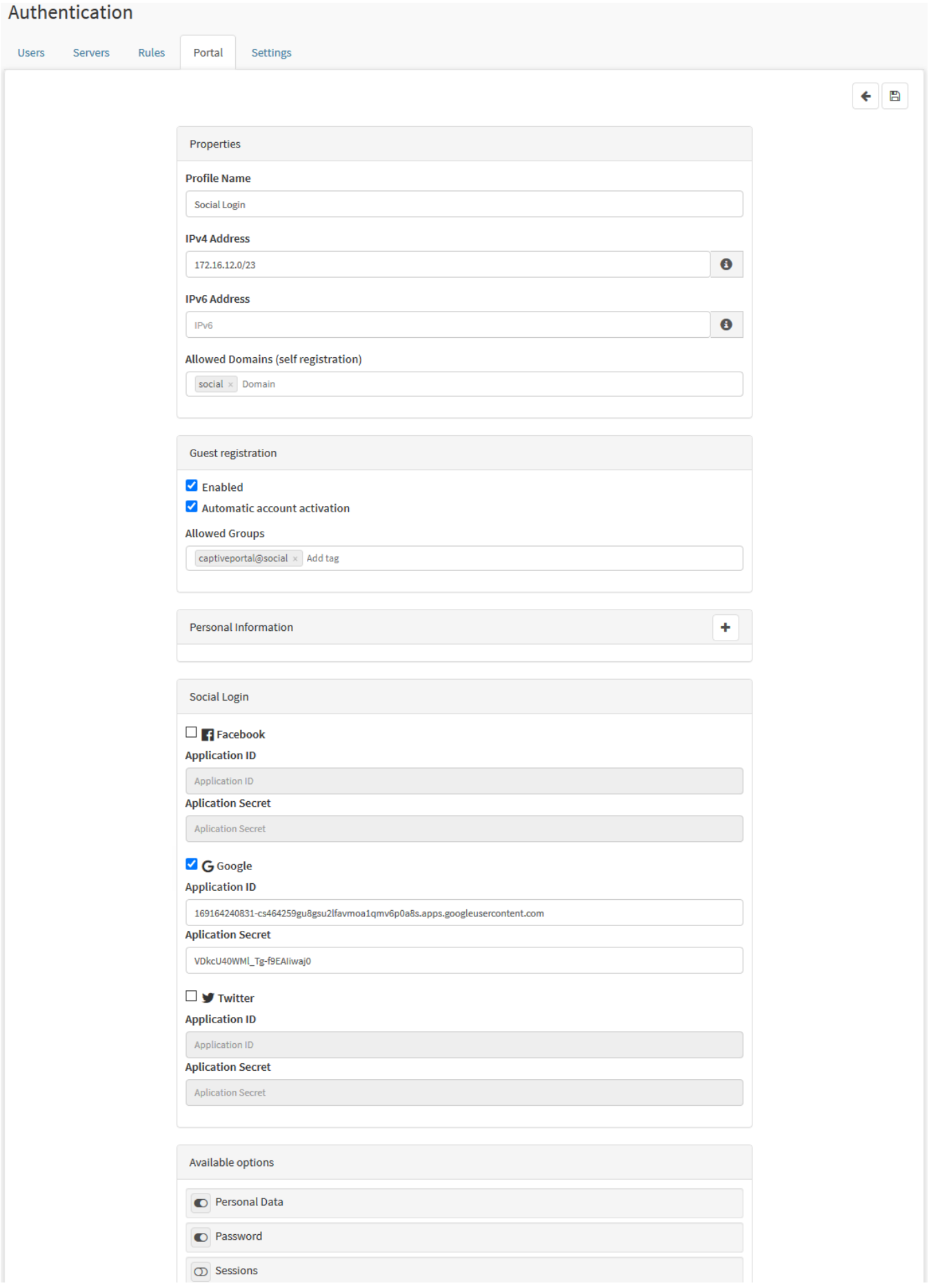
Available Options

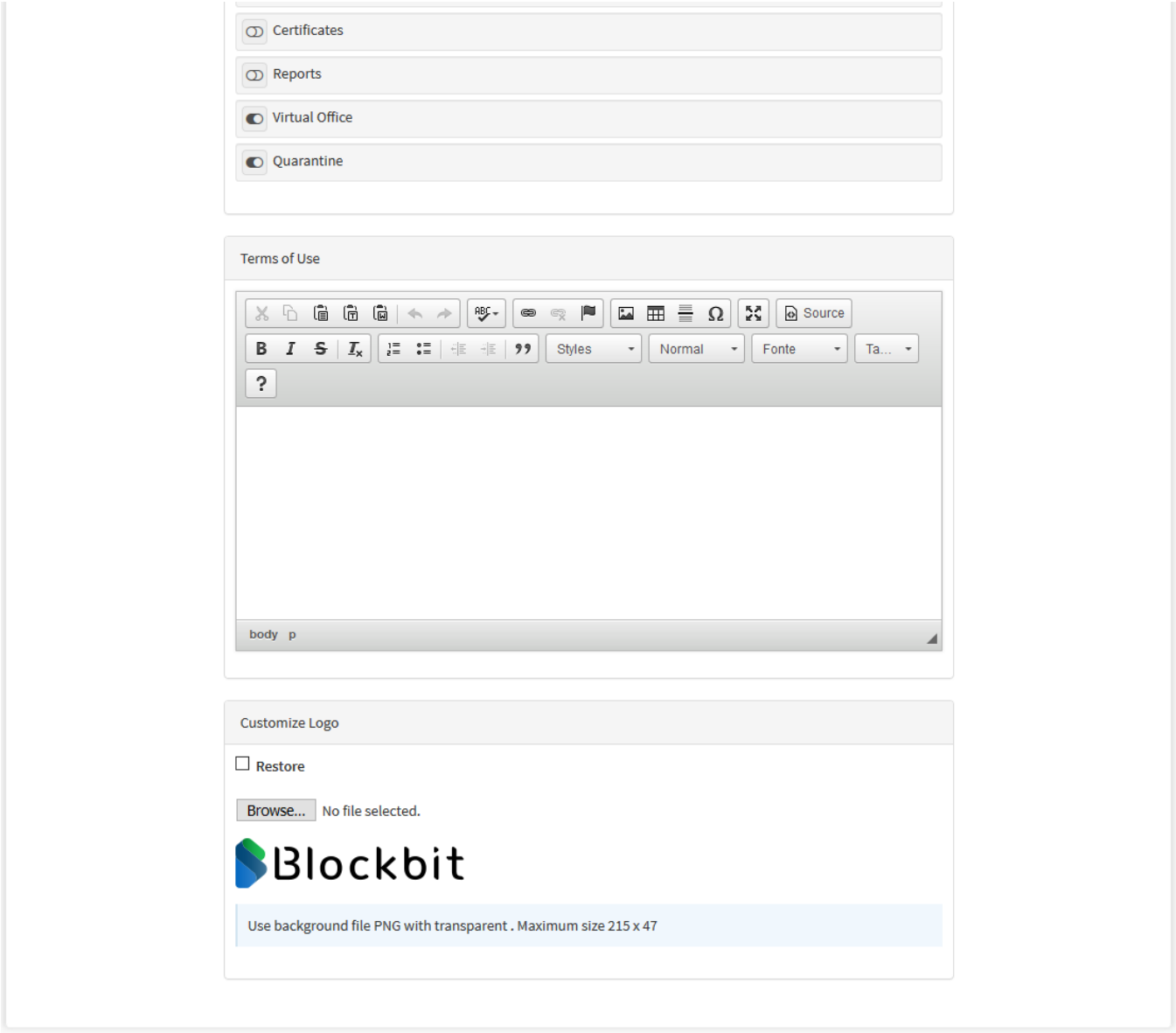
Enable through the checkbox **[**  **]** the features that will be available in Social Login.

Customize Logo

- ***Browse*:** If desired, add the logo that will be used on the lock screen.

When you finish completing the form on this screen, it will be as shown below:


Authentication
Users
Servers
Rules
Portal
Settings
Properties
Profile Name
Social Login
IPv4 Address
172.16.12.0/23
IPv6 Address
IPv6
Allowed Domains (self registration)
social
Domain
Guest registration
Enabled
Automatic account activation
Allowed Groups
captiveportal@social
Add tag
Personal Information
Social Login
Facebook
Application ID
Application ID
Aplication Secret
Aplication Secret
Google
Application ID
169164240831-cs464259gu8gsu2lfavmoa1qmv6p0a8s.apps.googleusercontent.com
Aplication Secret
VDkcU40WMl_Tg-f9EAliwaj0
Twitter
Application ID
Application ID
Aplication Secret
Aplication Secret
Available options
Personal Data
Password
Sessions



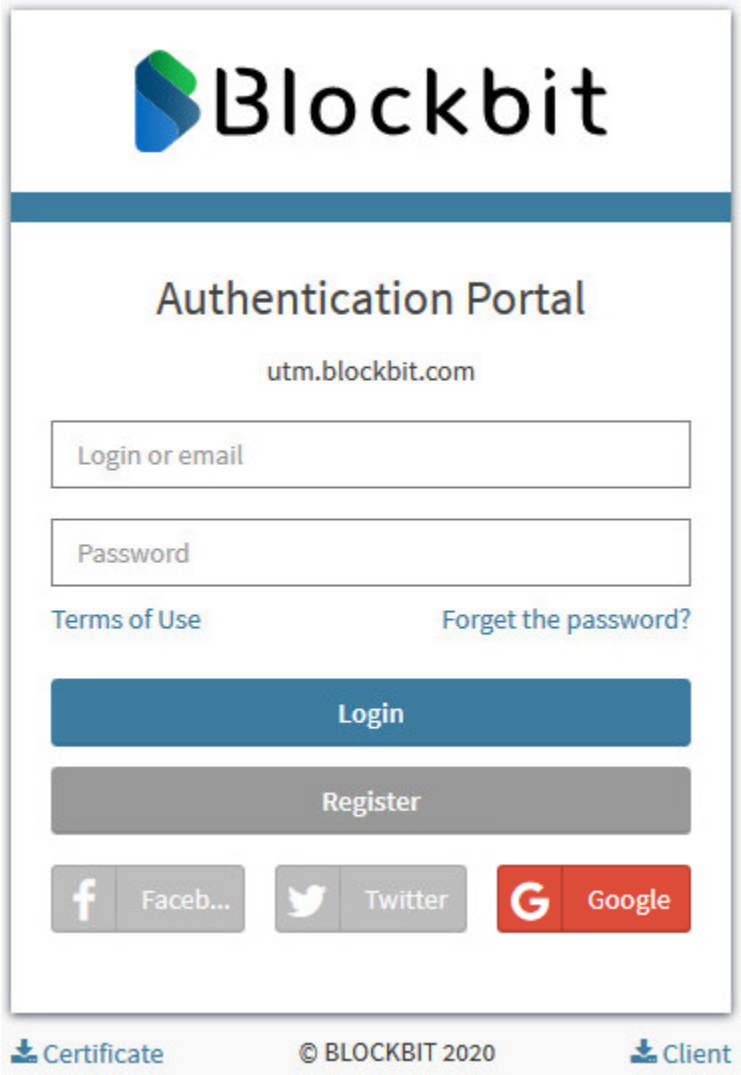
Settings - Authentication - Portal tab - Form

Click **[**  **]** to save the settings.

This concludes the configuration of Social Login at the NGFW, now we will register a new user through the social login and use it to enter the portal.

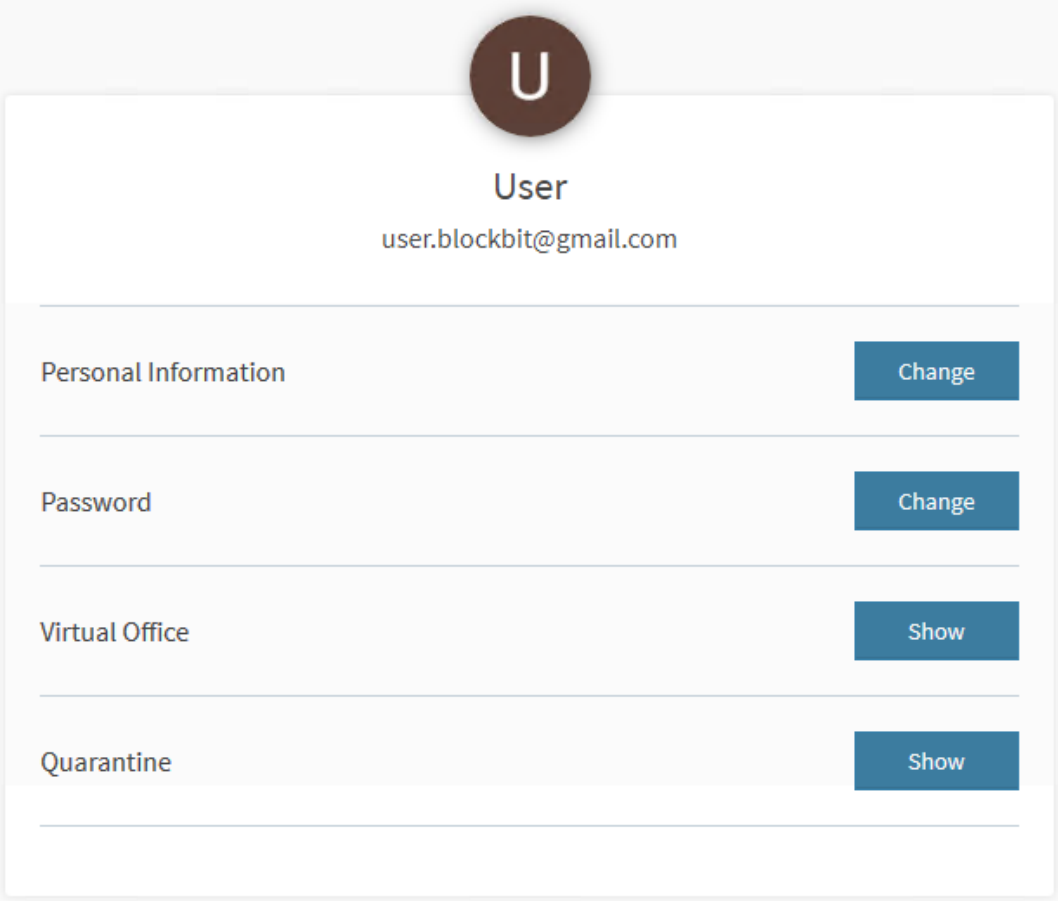
Access to the portal through Social Login

Returning to the authentication screen, the user can now select Google to log in by clicking the [Google] button again.



Authentication Portal

If the login was successful, the following screen will be displayed:



Login successfully

After performing these procedures, the social login will have been successfully enabled and configured.

For more information on configuring the portal, see this page.

UTM - Add Profile – Available Options

The **[Available Options]** area focuses on enabling the provision of some resources to the user who logs into the portal:

Authentication – Available Options

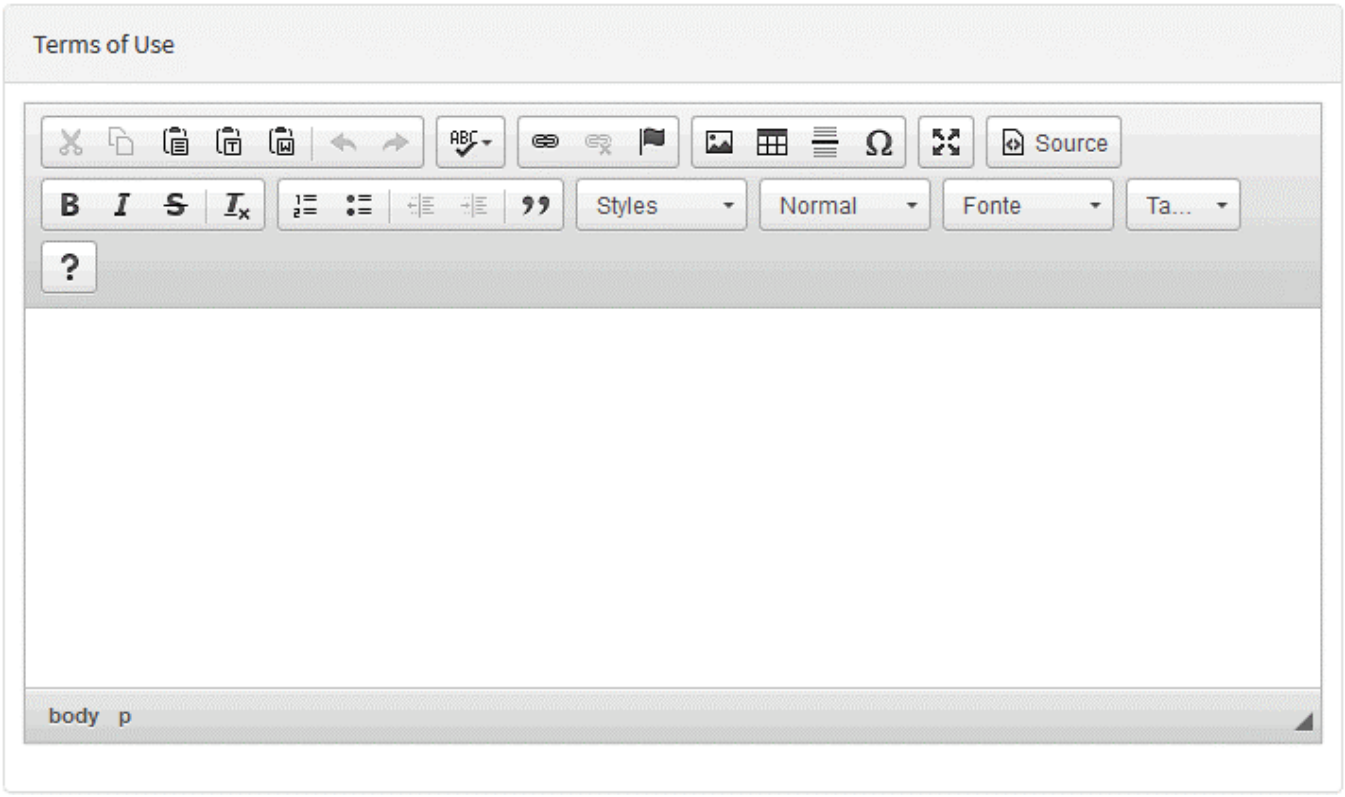
The available options are:

- ***Personal Data*:** It activates the request for the user's personal data;
- ***Password*:** It requires the user to use his password to access the portal;
- ***Sessions*:** It activates session limit on user access;
- ***Certificates*:** Activates the request for certificates when accessing the portal;
- ***Reports*:** Activates the logging of reports;
- ***Virtual Office*:** It makes Virtual Office available to users;
- ***Quarantine*:** Activates the quarantine on the portal.

Next, we'll look at the *Terms of Use* panel.

UTM - Add Profile – Terms of Use

The **[*Terms of Use*]** area aims to enable the creation of the terms of use that will be displayed on the portal, as shown by the following image:

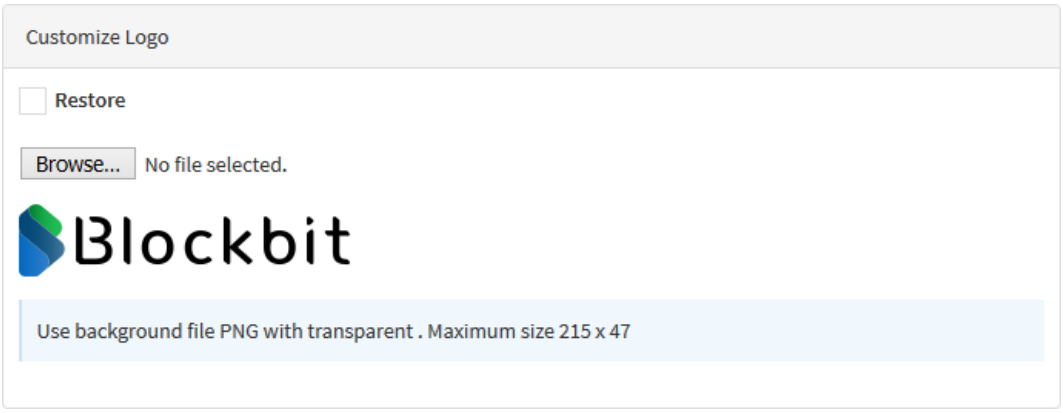


Authentication – Terms of use

Next, we'll look at the *Customize Logo* panel.

UTM - Add Profile – Customize Logo

Em **[*Customize Logo*]** é possível editar o logo que será exibido no portal, conforme demonstrado pela imagem abaixo:



Authentication – Customize Logo

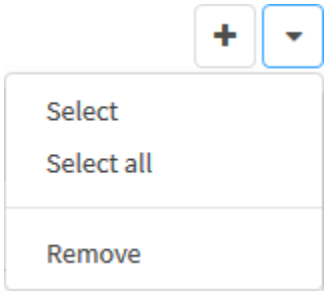
As opções disponíveis são:

- ***Restore*:** If checked, this checkbox has the function of restoring the default Blockbit logo;
- ***Browse*:** Allows you to import a PNG image with a maximum of 215 x 47.

After completing the settings in all fields, click **[**  **]** to save the profile, otherwise, click **[**  **]** to return to the Portal tab.

UTM - Portal - Actions Menu

At the top right of the “Portal” panel, next to the “Add” button, we have the actions menu, which can be displayed by clicking on the **[ ]** button, as illustrated by the image below:



Authentication – Action Menu

The menu consists of the following options:

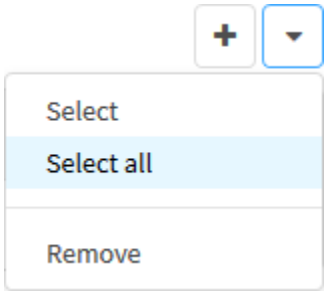
- *Select* and *Select All*;
- *Remove*.

Next, each action menu option will be detailed.

Portal - Actions Menu - Select and Select All

When clicking on the “Select” option, the removal icons will be replaced by checkboxes that can be used to perform a mass deletion through the actions menu.

The "Select All" option selects all items.

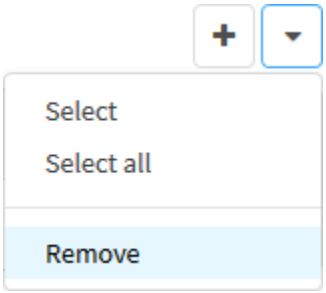


Portal – Select All

This allows changes that affect all items to be easily implemented.

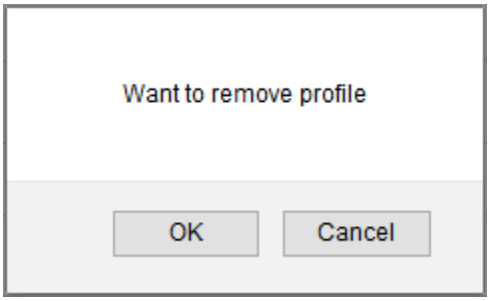
Portal - Actions Menu - Remove

To delete the desired profiles, click on the “Remove” option:



Portal - *Actions Menu - Remove*

The following confirmation message will be displayed:

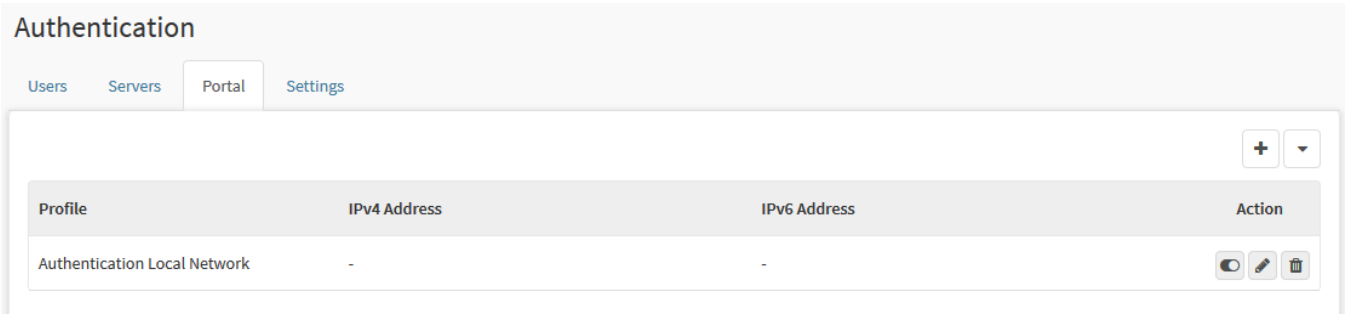


Authentication – Delete Profile

Click **[** OK **]** to delete, otherwise, click **[** Cancel **]** to not remove the domain.

Portal - Columns

Below we will explain each column of the Application Control tab:



Authentication – Portal

Below we will explain each column:

- **Checkbox[ ]:** Selects a profile when marked*;*
- ***Profiles*:** Displays the name of the registered portal;
- ***IPv4 Address*:** Displays the portal's IPv4;
- ***IPv6 Address*:** Displays the portal's IPv6;
- ***Actions*:** The “Actions” column consists of several buttons:
  - ***Enable*[ ]/*Disable*[ ]:** Allows you to enable or disable the portal added in the *Add Profile* button;
  - ***Edit* [ ]:** It allows to edit the settings of the portal added in the *Add Profile* option of the actions menu;
  - ***Delete* [ ]:** Deletes the profile, basically it is the equivalent of *Remove Profile* from the actions menu.

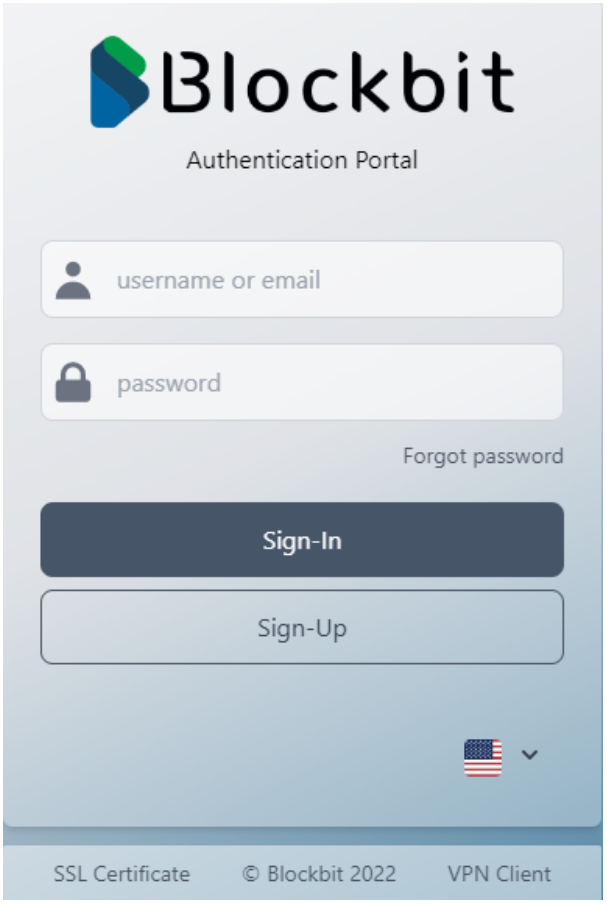
Authentication Portal

To access the authentication portal, in a browser, access the IP or URL using port 9803 as shown in the example below:

https://auth-fw.ead.labblockbit.com:9803

https://192.168.1.1:9803

The following login page will be displayed.



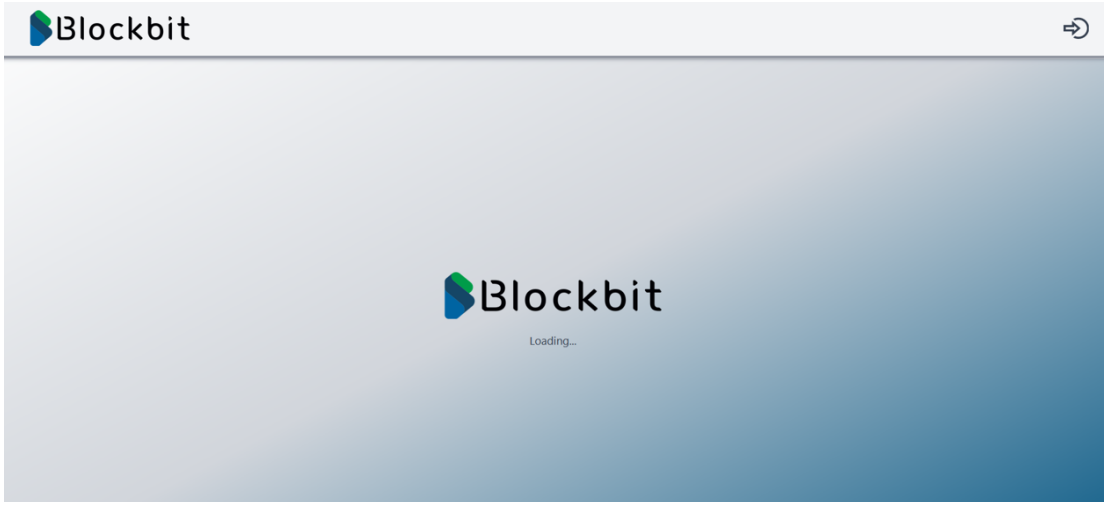
Captive Portal Login

Insert the username and password and click [Sign-In]. If you do not have a valid access, you may sign-up [Sign-Up] for yourself following the steps here explained.

Also the following functions are available in the login screen.

- **SSL Certificate:** Use this option to download the NGFW CA Certificate;
- **VPN Client:** Opens the VPN Blockbit Client download page;

Due to an update in the Captive Portal NGFW 2.4.0 security service, it is necessary to install the NGFW CA Certificate to use the Captive Portal in the Mozilla Firefox browser on the client machine; otherwise, Captive Portal will not load.



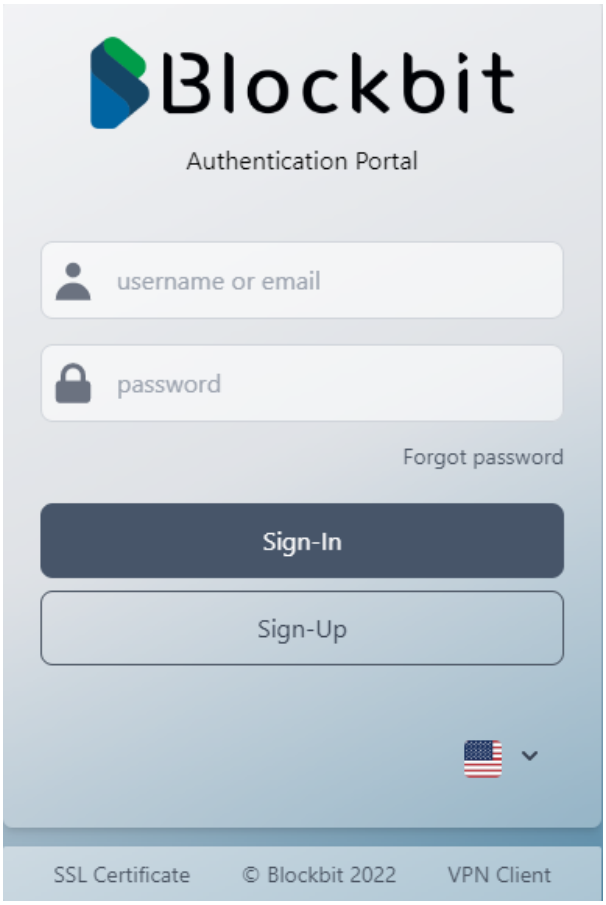
Loading - Mozilla Firefox without the CA Certificate

In this session we will analyze:

- Self-registration;
- How to apply a logon test;

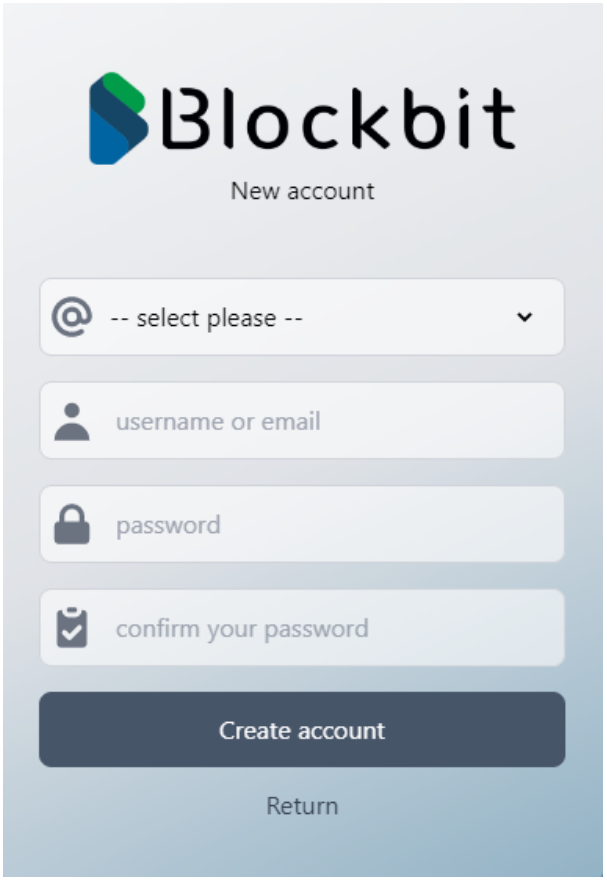
Self-registration

After configuring and enabling the self-registration in Authentication - Portal Tab it will be available in the authentication portal. As shown below:



Authentication – Register

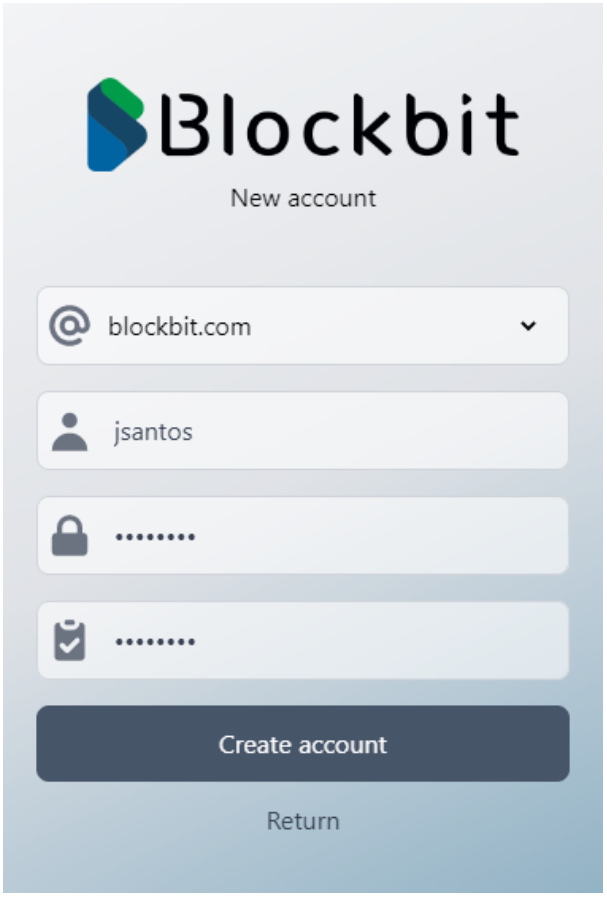
The [Sign-Up] button allows the user to create their own login. By clicking on it the following screen will be displayed:



Authentication – Create an *Account*

This form consists of the following fields:

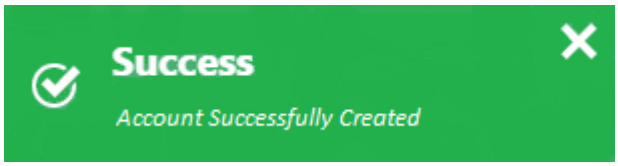
- ***Domain*:** Defines the domain to which the User will belong, the domains that appear in this checkbox are defined in the *properties* panel on the portal tab. Ex.: blockbit.com;
- ***User name or Email*:** Determines the user's name/E-mail. Ex.: user@blockbit.com;
- ***Password*:** Determines the user's password. Use letters, numbers and special characters. Ex.: q1Q!q1Q!;
- ***Confirmation*:** Repeat password to confirm;



Example

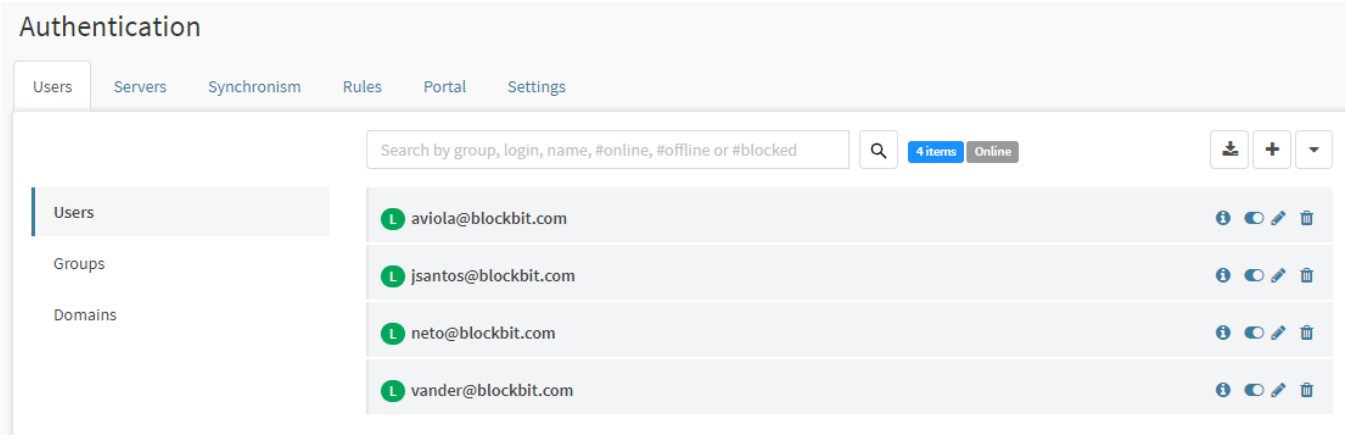
After performing the self-registration, click **[**  **]** to save all settings and create the user.

If the Automatic account activation option is activated in the *Guest Registration* panel in the portal tab, the activation will have already been done, the following message will be displayed:



User successfully created and activated

In addition to this message, if system notifications are enabled, the message "New guest user registered" will be displayed to the administrator, for more information about this user, just place the mouse over the **[**  **]** icon as shown in the image below:



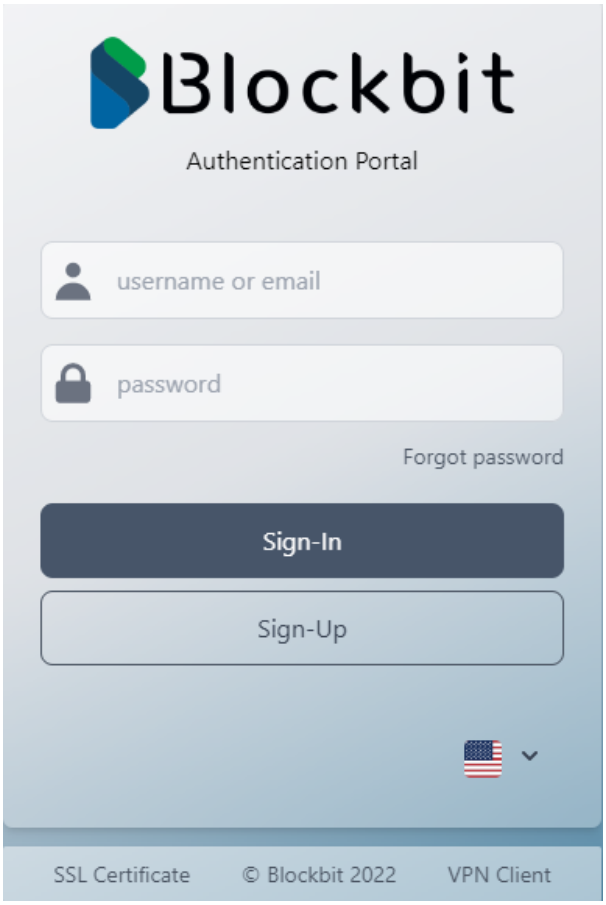
New guest user registered

In addition, if configured, the system will also notify the administrator via email and / or SNMP, for more information on how to perform this configuration, access this page.

After these steps, the user will be ready to be used normally.

Applying a logon test

To test if the captive portal login is working correctly, just login using a domain authentication user (for example “blockbit.com”) that has been registered or imported.



Authentication – Authentication Login

To do so, complete the fields:

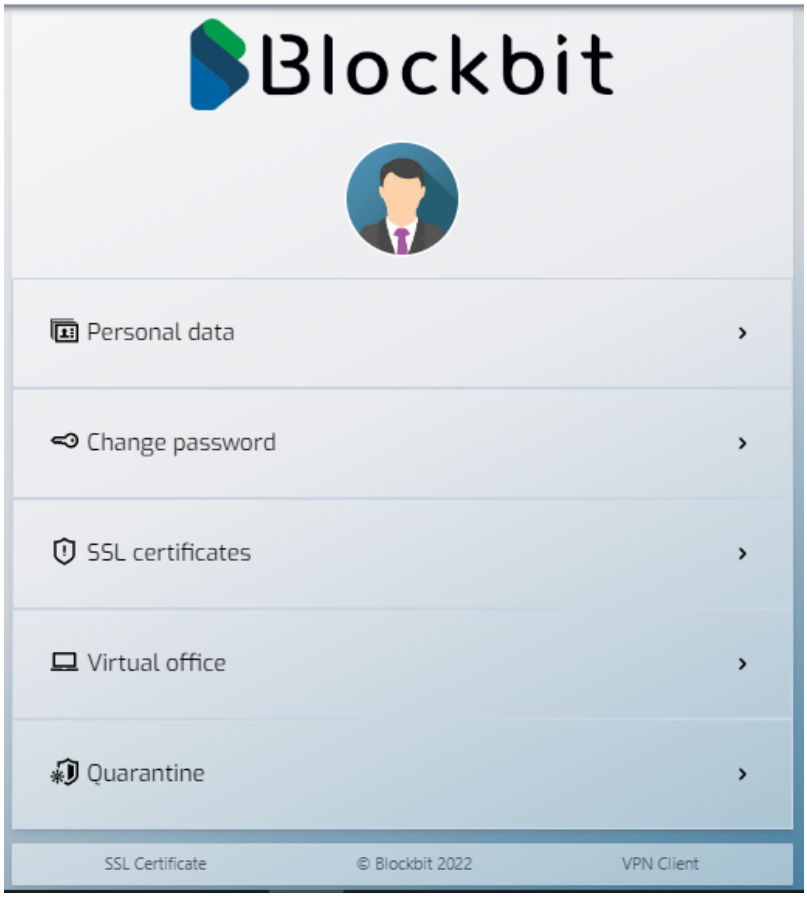
- ***Login or Email***: Enter user login. Ex.: *User*;
- ***Password*:** Enter user password. Ex.: q1Q!q1Q!.

Use the syntax*: ex.: "usuário@seu_dominio.com".*

During the login of users of the standard domain, it is not required to type the suffix "@domain".

Click on **[** 

] to access the authentication portal interface, the screen below will be displayed:



Authentication – User's portal

For more information on how to manage the authentication portal, see this page.

Management of the authentication portal

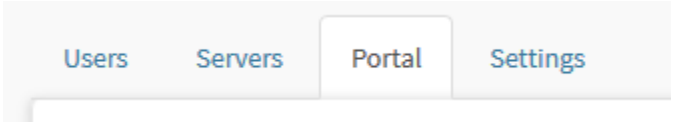
The portal management interface allows the administrator to parameterize the service in order to make the management of some resource items of the Blockbit NGFW platform available to the network user..

The authentication portal allows the user to manage some features of the platform.

- Personal data;
- Change password;
- Sessions;
- Download the Certification Authority (CA);
- Access the Terms of Use;
- Access custom reports;
- Others...

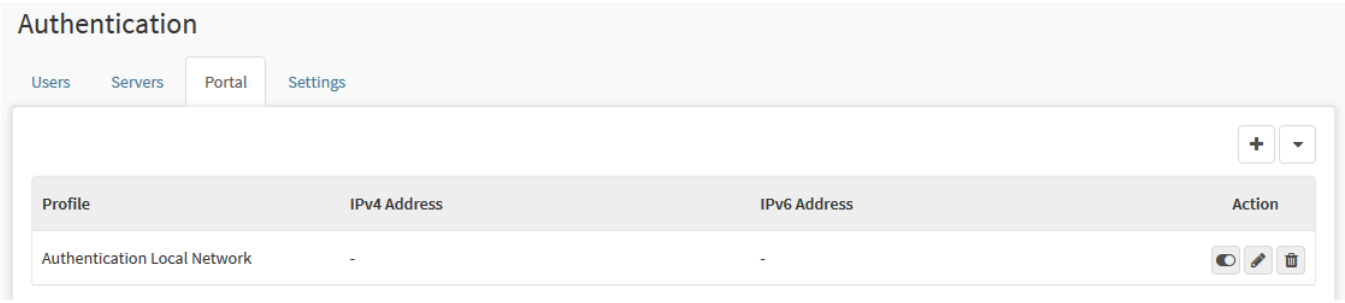
To have access to these resources, the administrator must change the authentication profile for this group of users.

To edit an authentication portal profile, access the Portal Tab.



Portal Tab

Click **Edit [ ]**.



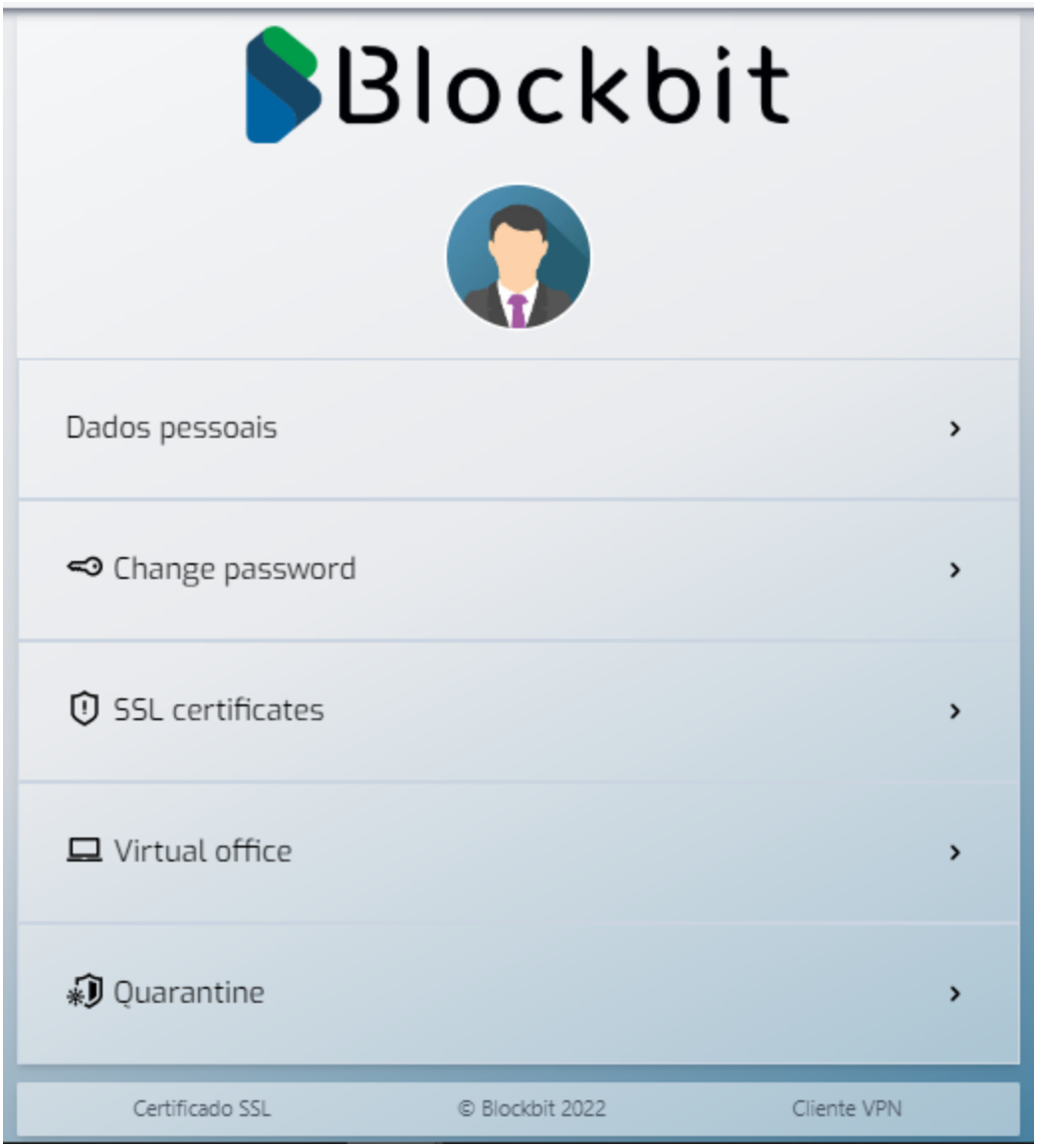
Authentication – Edit Authentication Portal

In the **[Available options]** box, enable the resource items you want to make available to your users from the authentication portal.

Authentication Portal – Available options

Then click ***Save*** **[**  **]**.

After enabling these items, the portal returns the right to the respective resources to the user, as the example below:

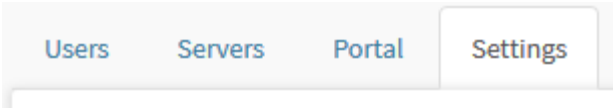


Authentication – User's Portal.

UTM - Authentication - Settings tab

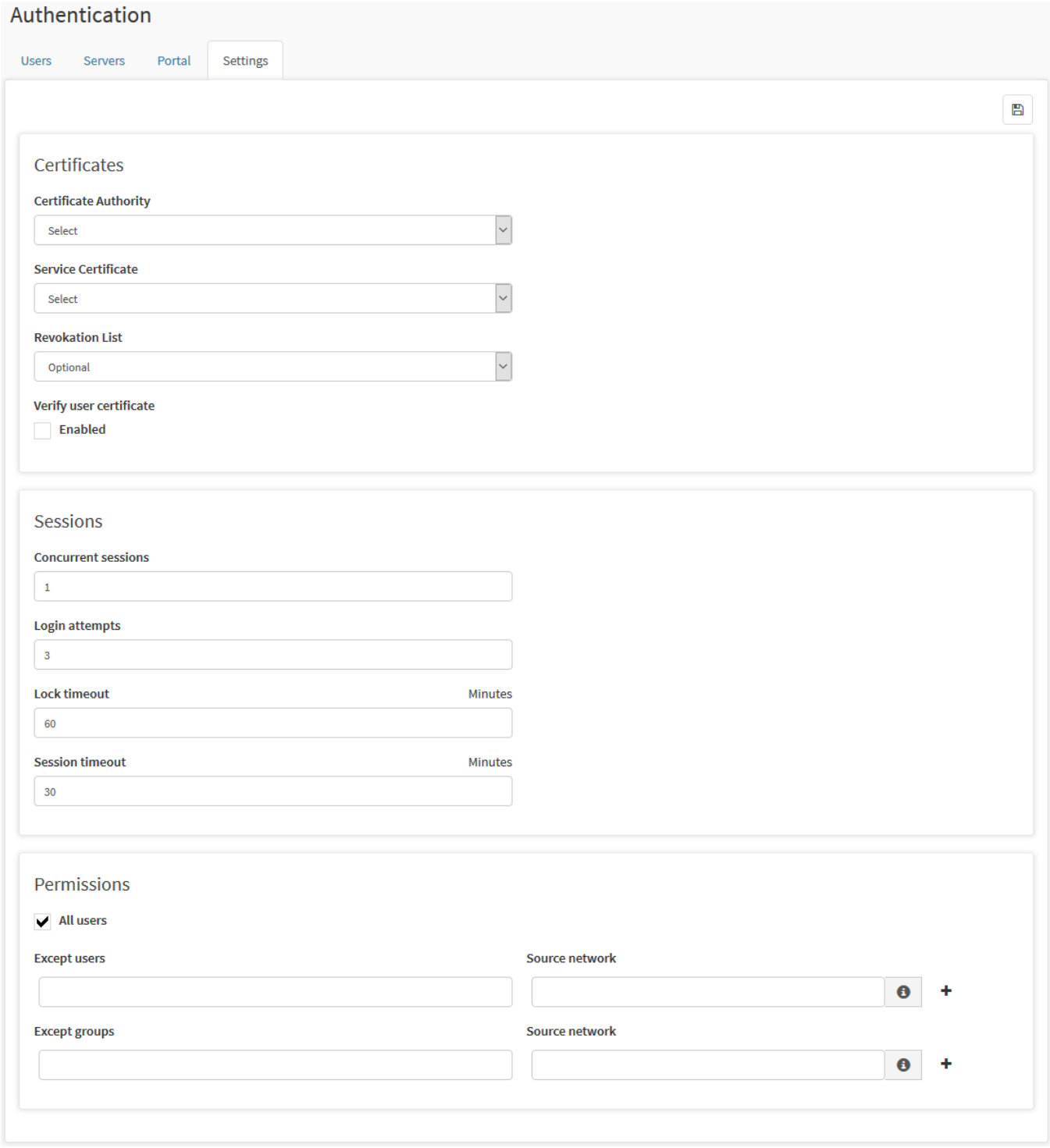
Blockbit UTM allows to define global parameters for authentication and also allows the determination of other system resources.

To configure and enable Proxy services, click on the tab, as shown below:



Settings tab

The screen below will appear:



Authentication – Settings

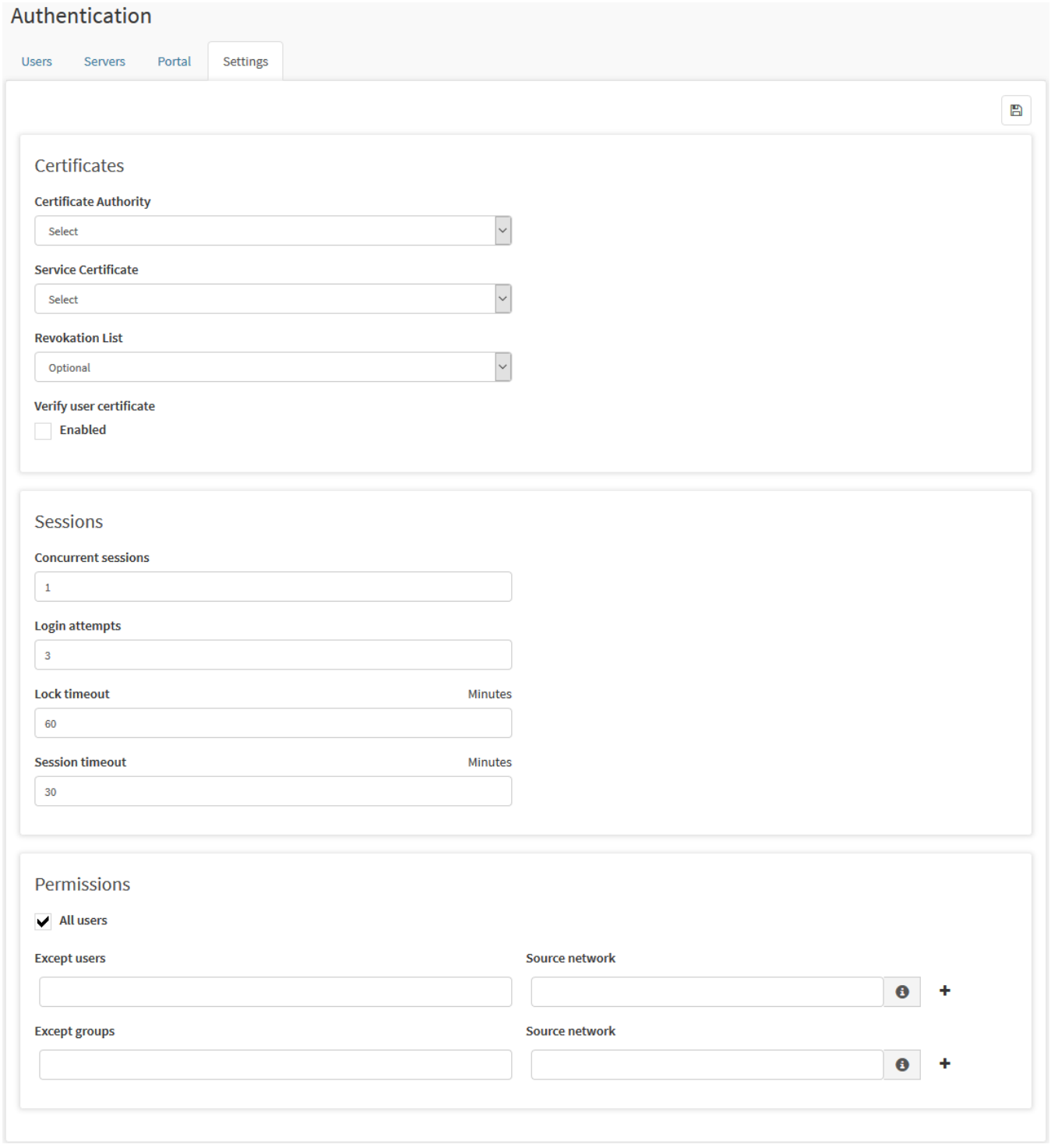
This screen is composed of the following panels:

- *Certificates*;
- *Sessions*;
- *Permissions*.

Next, we will analyze each panel on this screen.

Settings - Certificates

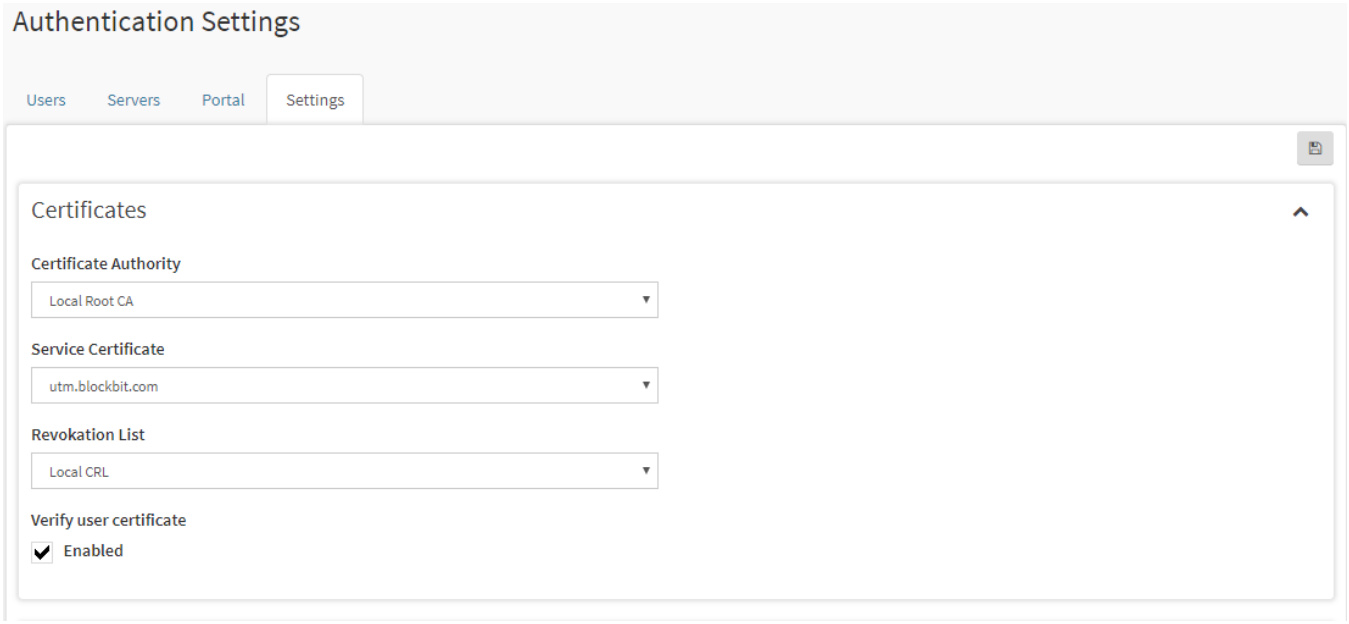
In this section we will enable authentication by validating a WEB address through a digital certificate.



Certificates

The administrator must associate the CA (Certificate Authority) and CS (Certificate Service) or digital certificate, including the list of revoked certificates, which ensures that if any user tries to use a revoked certificate, it will no longer be valid for the CA associated.

Select the corresponding ACs from the drop-down lists and click [ ].



Certificates selection screen

For more information on two-factor authentication, see this page.

Next, we will analyze the Sessions panel.

2FA (Two Factor Authentication)

Two-factor authentication (also known as 2FA) is a type (subset) of multi-factor authentication.

- **Multifactor**

Multifactor authentication (MFA) is a method for confirming a user's claimed identity, in which the user is only granted access after successfully presenting 2 (two) or more proofs (or factors) to an authentication mechanism:

    - **Knowledge** (Information owned exclusively by the user);
    - **Possession** (Of exclusive power of the user);
    - **Inherence** (Essential user characteristic).
- ***2FA***

Characterized by the identity verification method claimed by a user, using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are.

A good example of two-factor authentication is withdrawing money from an ATM; only the correct combination of a bank card (something the user has) and a PIN (personal identification number, something the user knows) or digital identification (unique identification of who he is) allows the transaction to be carried out.

Implemented in Blockbit UTM, it is an extra layer of security that requires not only a username and password, but also an identification that only this “user” has and that Blockbit UTM can use to identify him, that is, information that only the user in question should know or possess, the “Digital User Certificate”.

Because using a username and password, in combination with information that only the user knows, it is more difficult for potential intruders to have access to essential network resources and services or to commit theft of that person.

Next, we'll look at how Two Factor Authentication works.

How 2FA (Two Factor Authentication) authentication works

Service configuration, definition of an authentication profile and access to the portal are mandatory requirements for enabling and activating this authentication method.

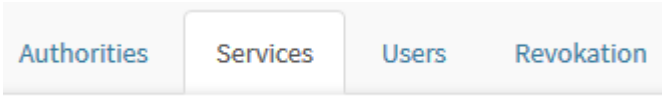
To configure 2 (two) factor authentication - 2FA it is necessary to certify the registration of digital certificates (services and users) and their reference to the authentication service.

In the example we are going to present, we already have a user base registered in a local domain “blockbit.com”, so it is enough to have the association of a corresponding user certificate registered and have the digital certificate installed.

- **SSL Certificates**

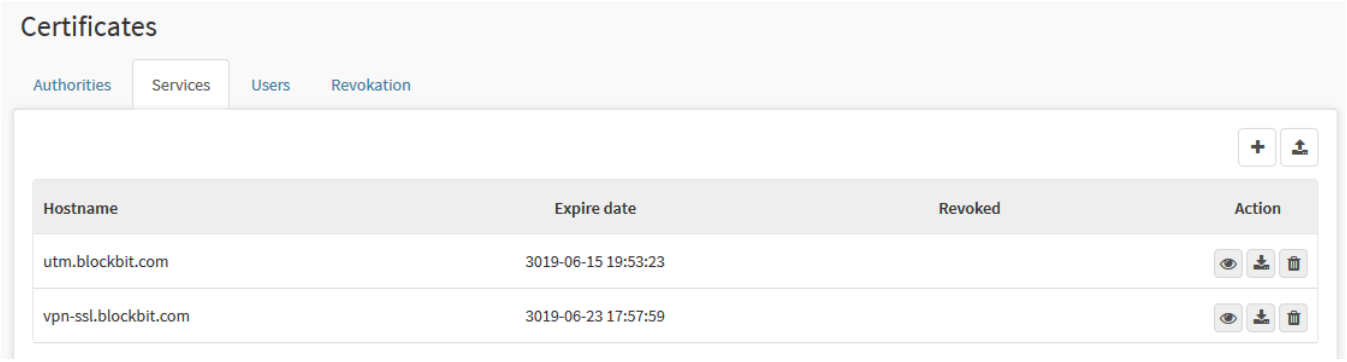
Check the creation of digital certificates for services and users.

Go to Settings, select the Certificates option and click on the Services tab.



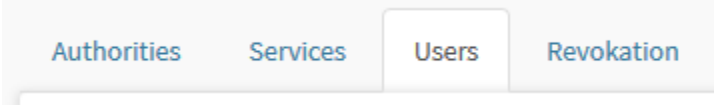
Services tab

The following screen will appear:



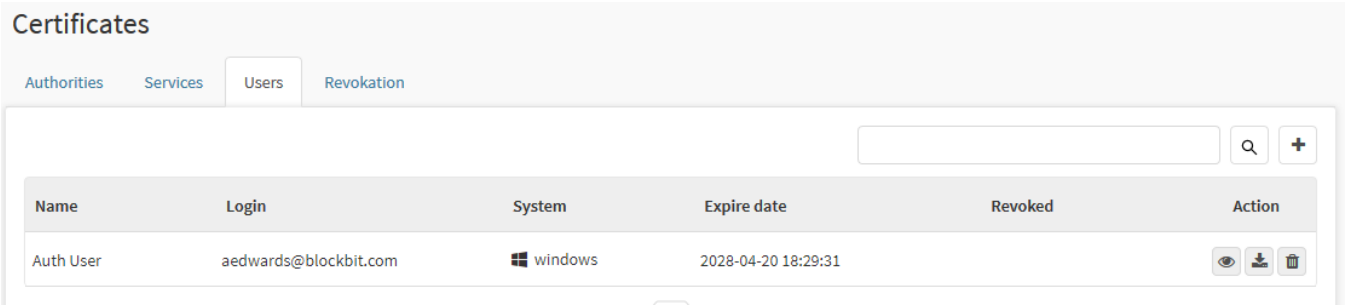
Certificate Management

Go to Settings, select the Certificates option and click on the Users tab.



Users tab

The following screen will appear:



Users certificate management

Next, we'll look at how to establish 2FA authentication access.

Establishing 2FA authentication access

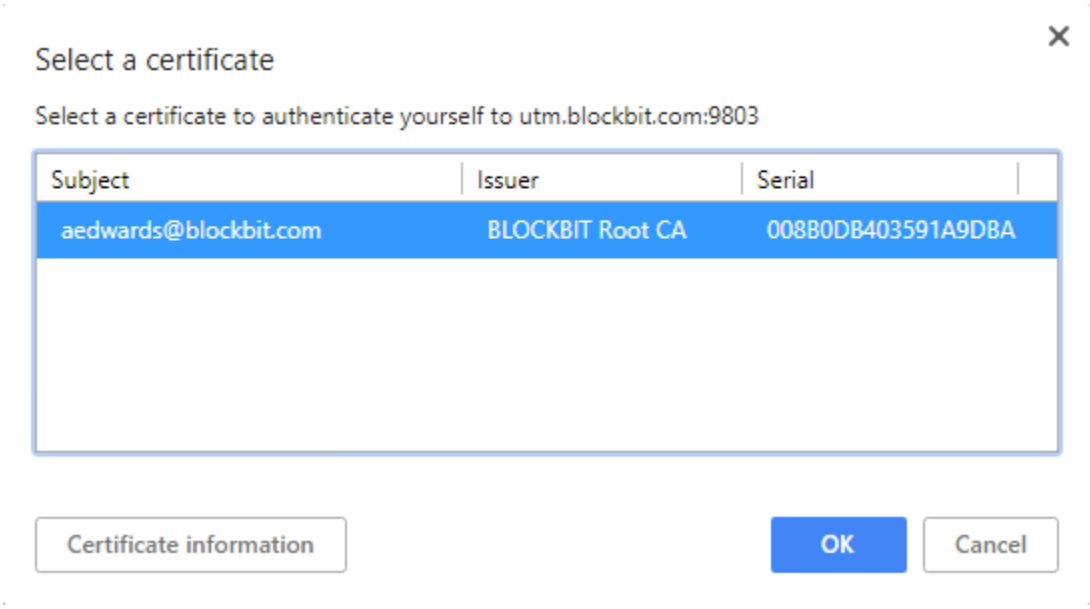
We will establish the authentication test using the web portal. Access a browser and type

https://utm.labblockbit.com:9803

We will make an access using an authentication user of the domain “blockbit.com” - registered / imported.

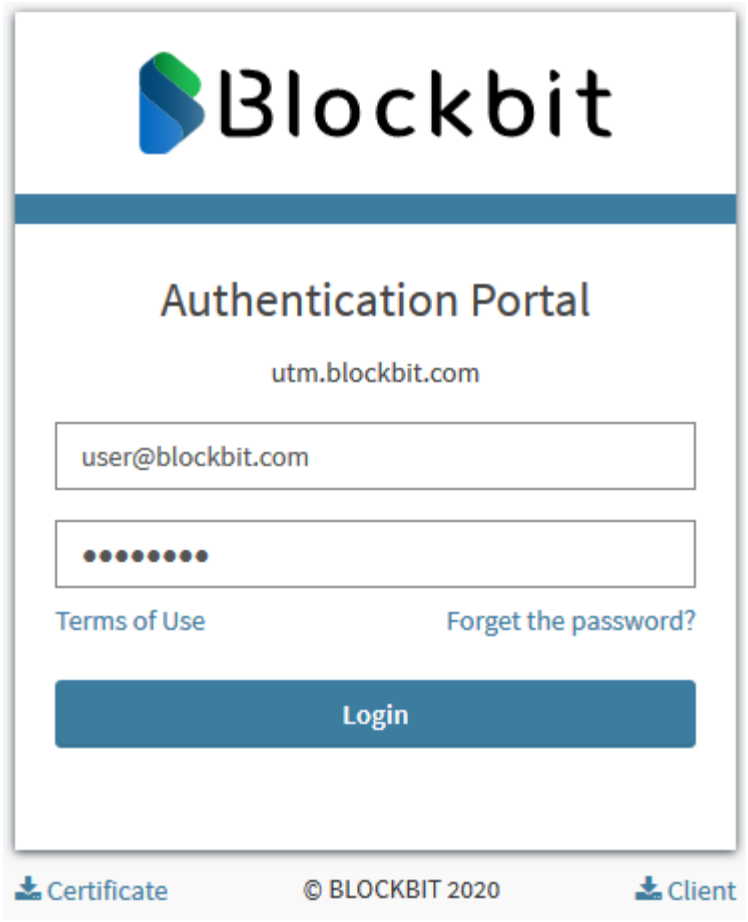
After configuring the authentication service with the user certificate validation option “enabled”, the authentication process starts to “require” the presentation of the “Digital Certificate” as an authentication item.

Select the corresponding user certificate to validate the authentication and click **[OK]**.



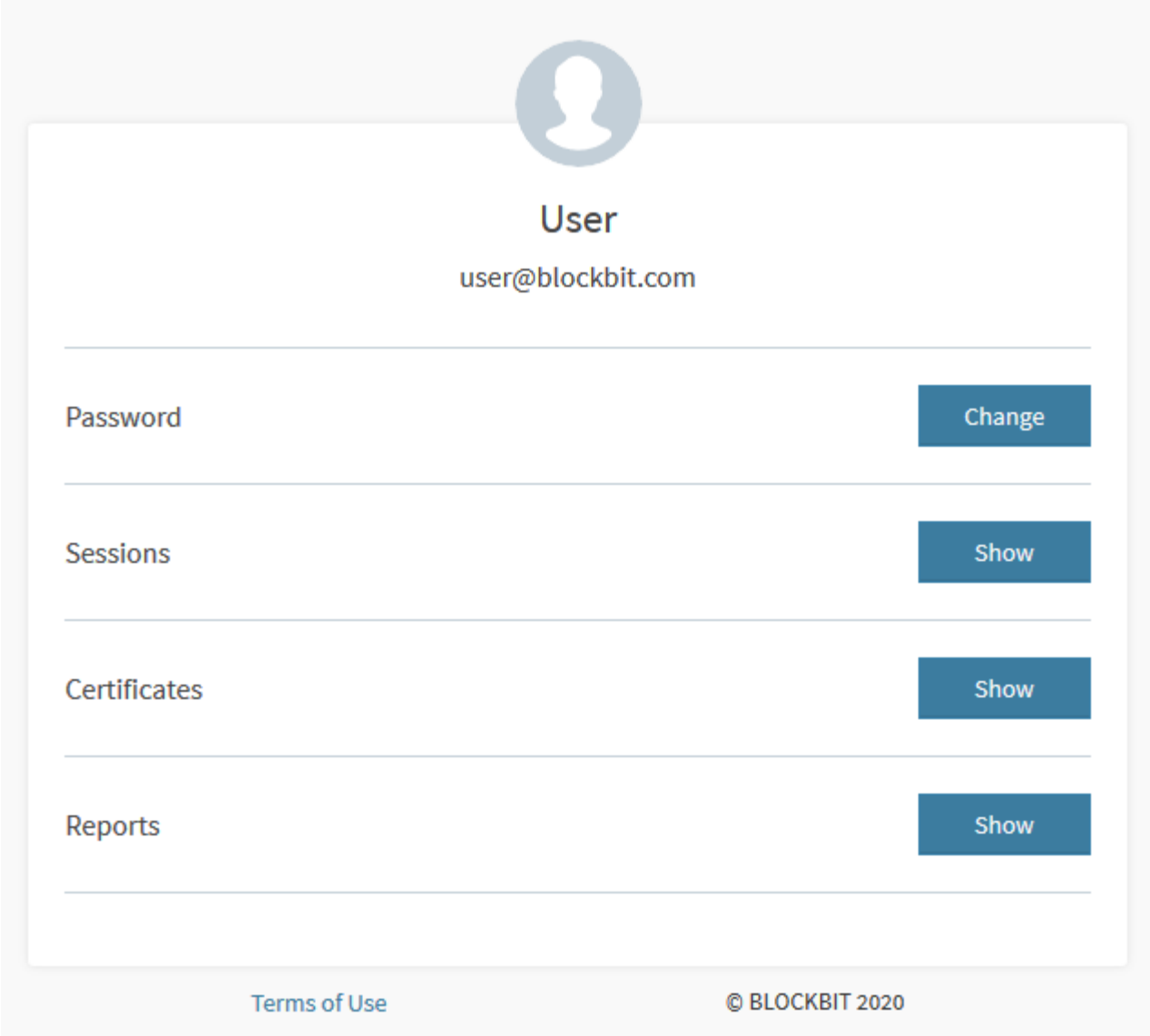
Select a Certificate

Then complete the process by identifying the user with the standard authorization data: “user@your_domain.com” and the respective password “xxxxxxx”.



User's Portal Authentication

Authentication Portal Interface



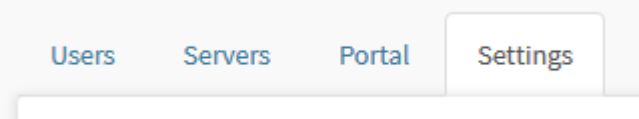
Authentication Portal Interface

Next, we will detail the 2FA configuration process.

2FA configuration

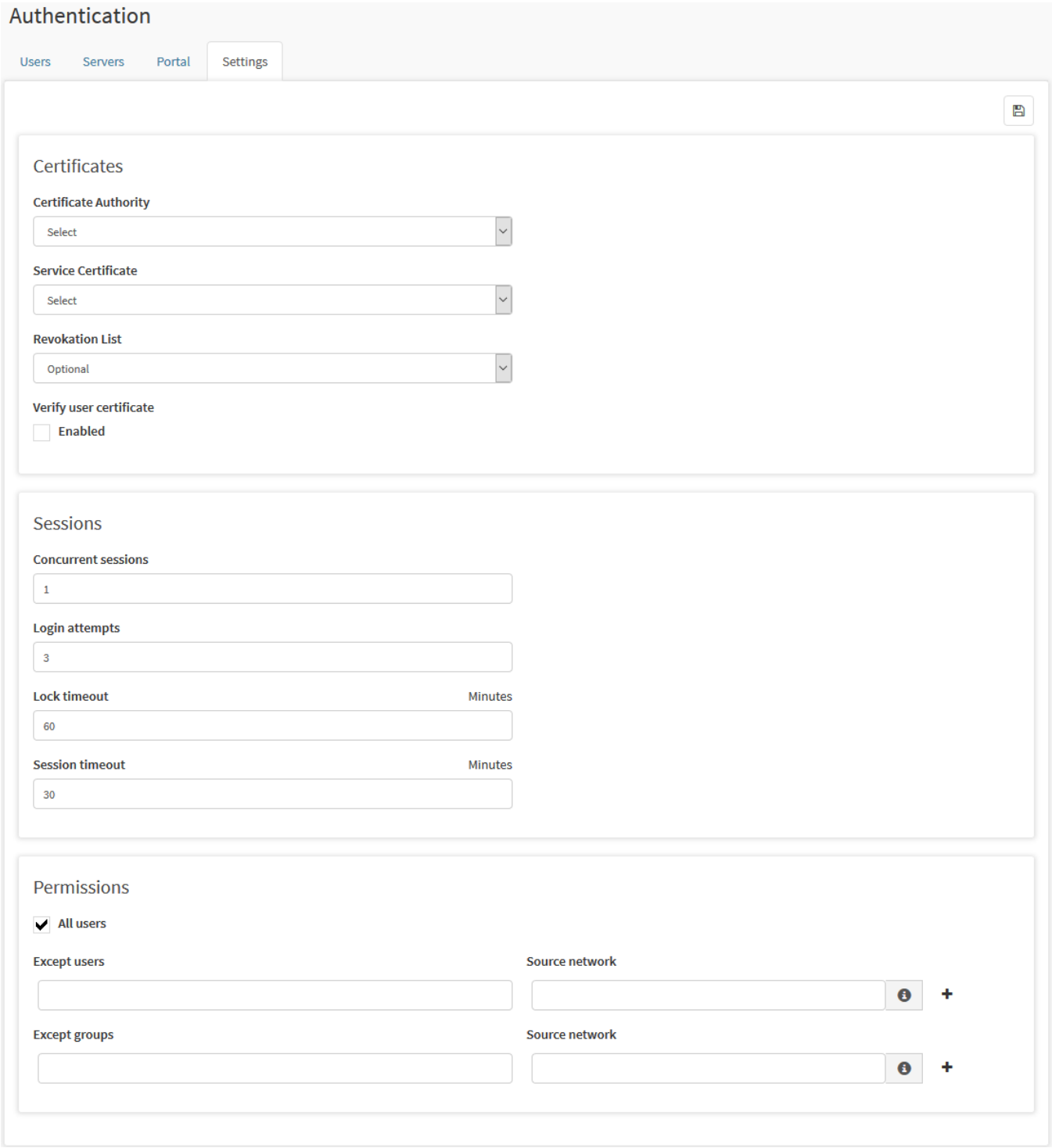
Authentication

Access the Settings tab.



Settings tab

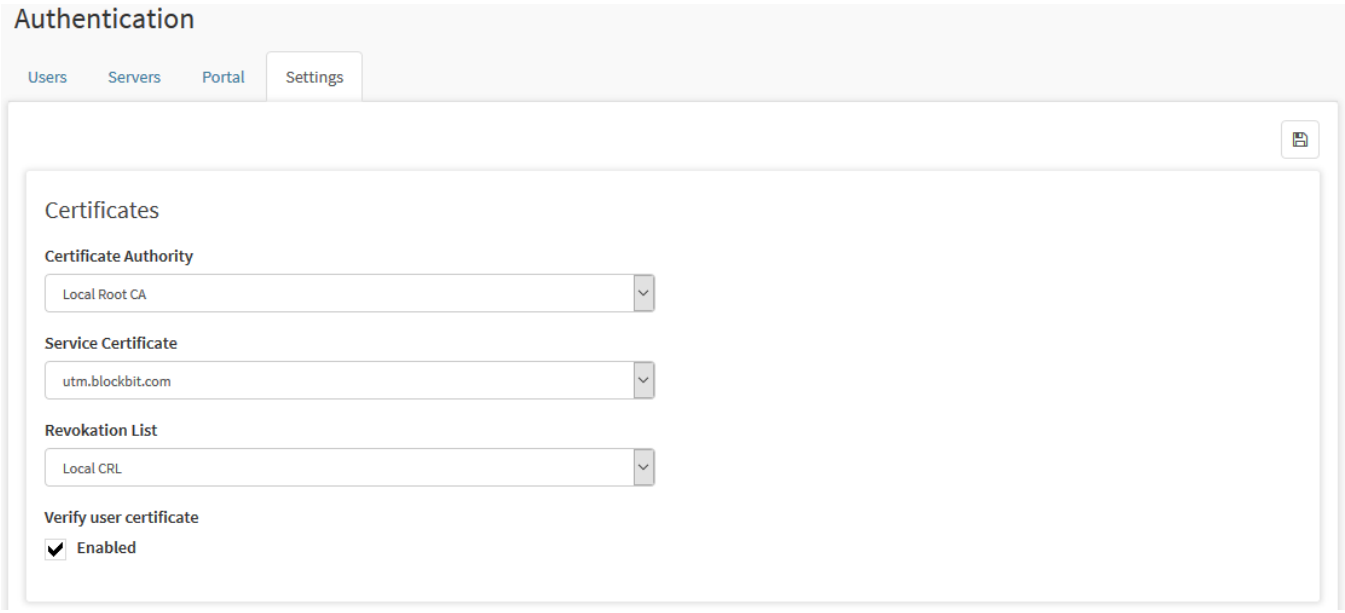
In this section we will enable authentication by validating a WEB address by digital certificate.



Authentication – Settings

The administrator must associate the CA (Certificate Authority) and SC (Service Certificate) or digital certificate, including the list of revoked certificates, which ensures that if any user tries to use a revoked certificate, it will no longer be valid for the CA associated.

Select the corresponding C.A.'s from the lists and click **[ ]**.



Authentication – Settings - Select certificate to 2FA

DONE! Authentication service enabled and configured for access using validation of the user's digital certificate as the 2nd authentication factor.

2FA Authentication supports the 5 (five) types of authentication:

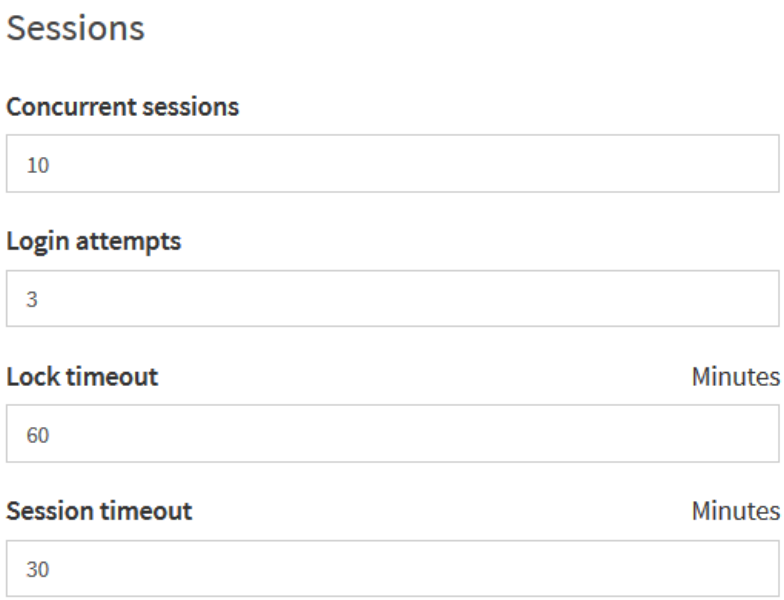
- *Local*;
- *Windows AD LDAP*;
- *LDAP (AD, Unix, Linux*);
- *TACACS+*;
- *Radius (Remote Authentication Dial in User Service).*

Settings - Sessions

It allows to define security parameters in the Blockbit UTM authentication module.

The parameters are:

- ***Concurrent sessions*:** Sets the maximum number of simultaneous user sessions;
- ***Login attempts*:** Defines the maximum number of unsuccessful authentication attempts, before the user is blocked;
- ***Lock timeout*:** Defines the time in minutes for the user to be blocked after exceeding the number defined in the “Login attempts” field;
- ***Session timeout*:** Sets the maximum downtime for an authenticated user's session.



Authetication – Sessions

Next, we'll look at the Permissions panel.

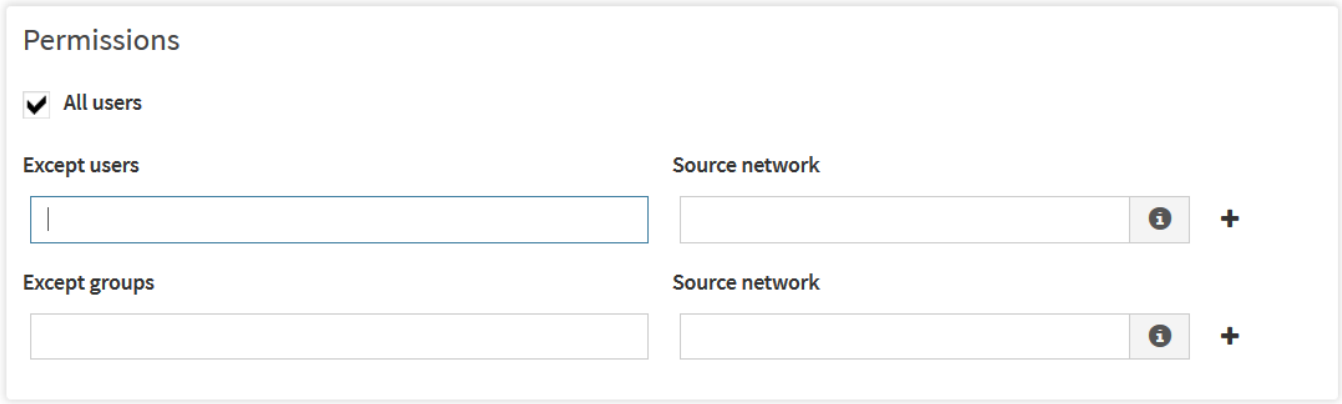
Settings - Permissions

It allows defining exceptions to users and groups in Blockbit UTM authentication.

It is possible to add more parameters by clicking on the **[+]** button;

The parameters are:

- ***All users[✓]*:** Allows all synchronized users to authenticate on the Blockbit UTM. This checkbox changes which fields are displayed below it:
  - If enabled, the **Except Users** and **Except Groups** fields will be displayed, defining that all users can authenticate, except those registered in the fields;
  - If it is disabled, the **Only Users** and **Only Groups** fields will be displayed, defining that only users registered in the fields can authenticate.
- ***Except users/Only Users*:** Defines that users can only authenticate when their IP address is defined in the **"Source network"** field;
- ***Except groups/Only Groups*:** Defines that users belonging to groups can authenticate, only when their IP address is defined in the **"Source network"** field;
- ***Source network*:** Defines the IP addresses or subnet that can authenticate.



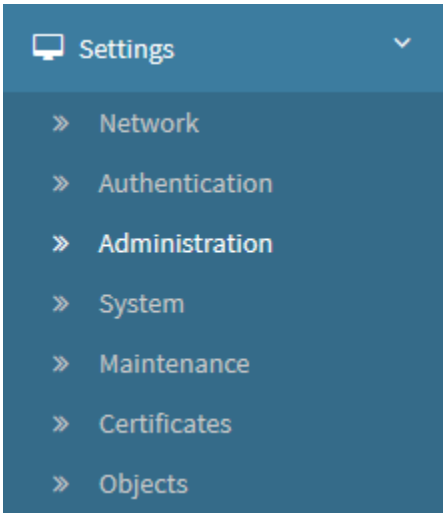
Authetication – Permissions

UTM - Settings - Administration

The administrator has the option of synchronizing the user base and groups in BLOCKBIT UTM with an existing base in the network on an “LDAP” server, thus centralizing the registration administration of all users and/or groups on the respective server.

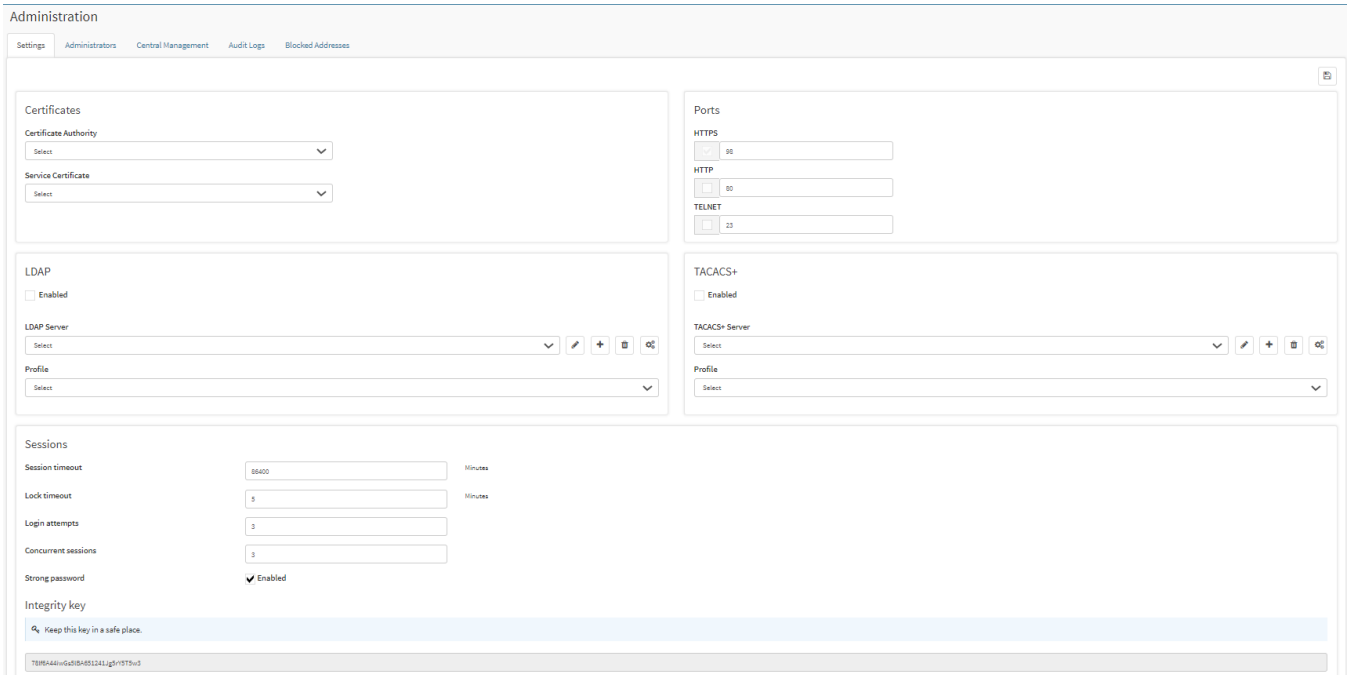
This item allows us to regulate access to the WEB administration interface, define and apply the general settings, manage the registration and permissions of the system administrators, audit the accesses and the applied settings, and also moderate the blockages due to unauthorized access attempts.

To access this screen, simply select the “Administration” option.



Settings - Administration

The screen below will appear:



Settings - Administration - Settings

The Administration screen has the following tabs:

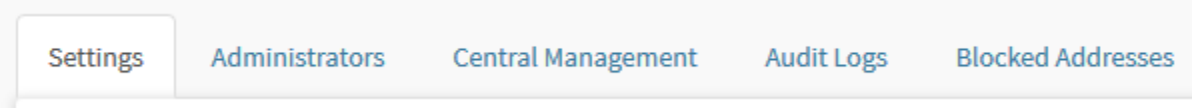
- *Settings*;
- *Administrators*;
- *Central Management*;
- *Audit Logs*;
- *Blocked Addresses*.

Next we will analyze the components of the settings tab.

Administration - Settings tab

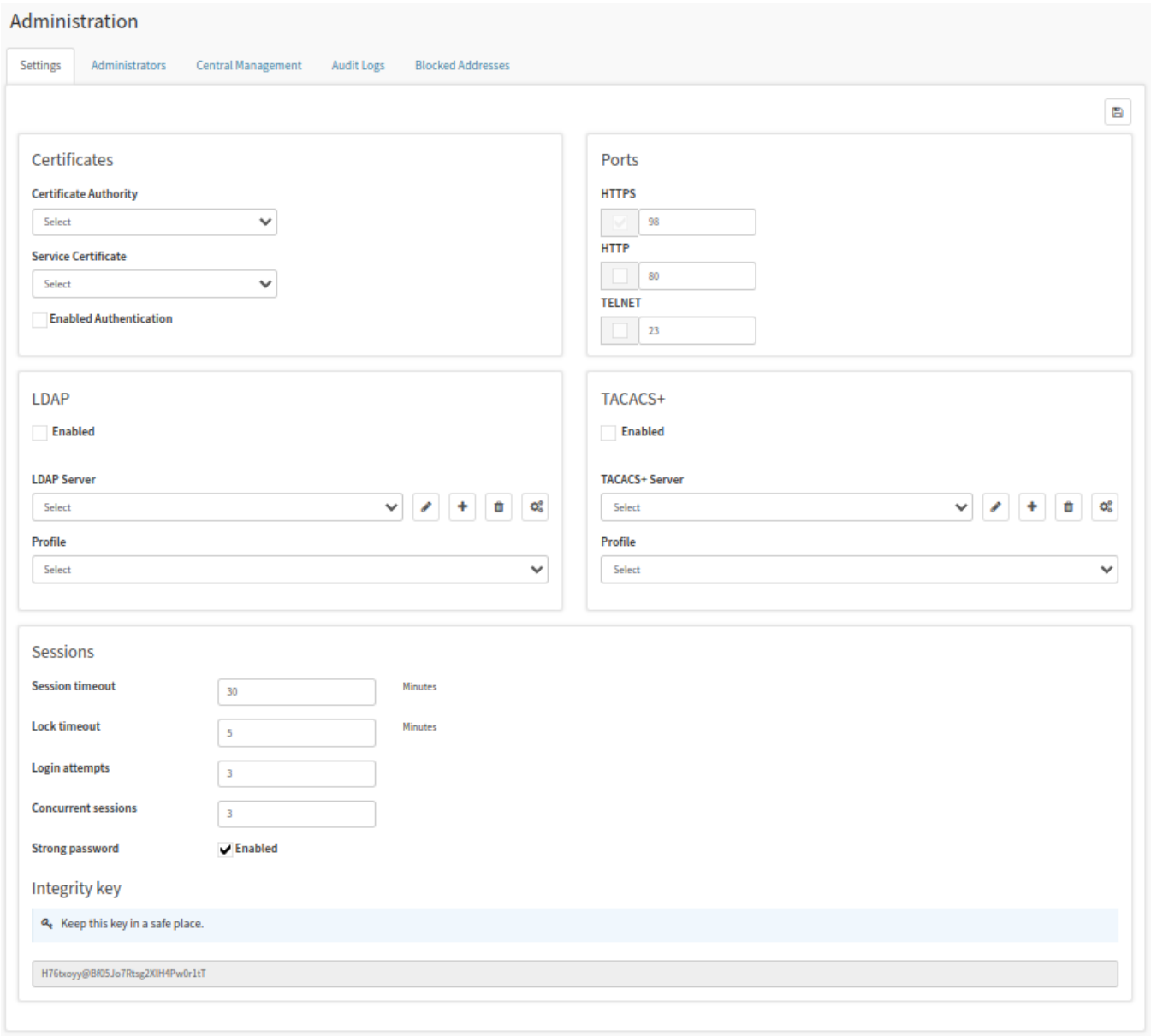
This item allows us to define security settings in relation to the system administration interface.

For access click on the "Settings" tab:



Settings tab

The screen shown by the image below will appear:



Administration - Settings

Alterar padrão das políticas Exchange Policies' standard

ID(1): HTTP Access

ID(2) : Telnet Access

For (Allow), Enable, and WAN/ALL Zones

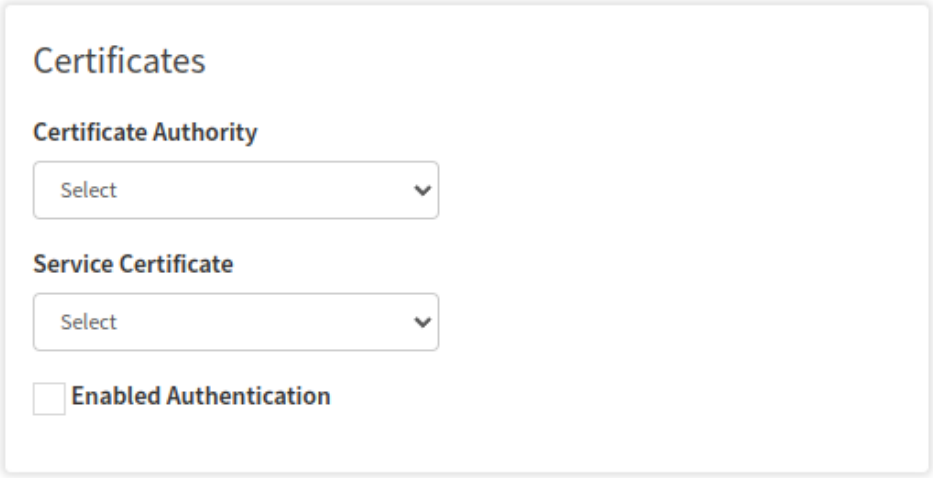
The tab is divided into the following panels:

- *Certificates;*
- *Ports;*
- *LDAP*;
- *TACACS+*;
- *Sessions*.

Next we will analyze each component of this screen.

Settings - Administration - Certificates

In the Certificates panel, it is possible to enable the use of certificates when accessing the administration interface, select the C.A. “Certificate Authority” and the C.S. “Certificate Service” or Digital Certificate for the “host” defined for accessing the WEB interface.

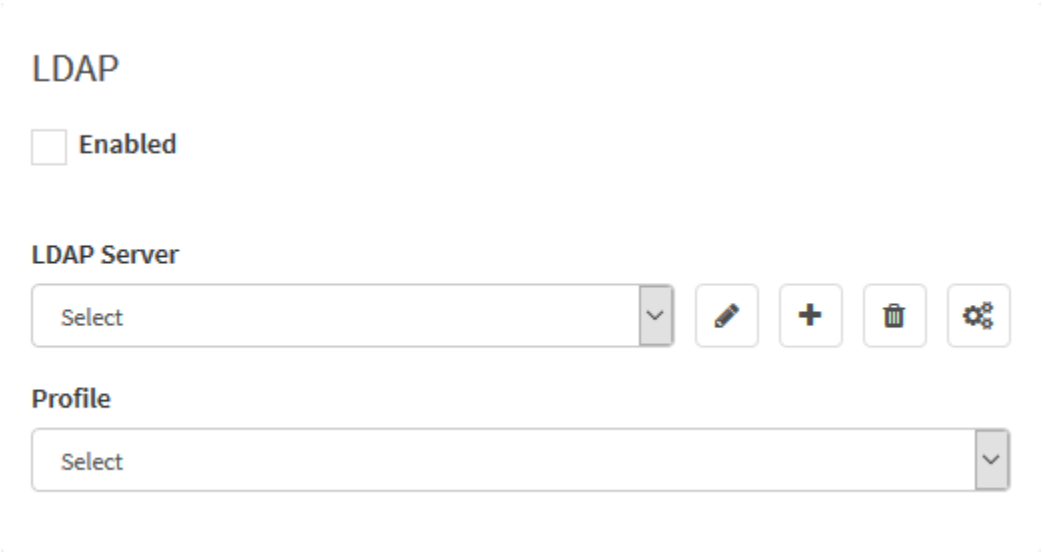


Settings - Administration - Certificates

- ***Enabled Authentication [☑]*:** Enables access by authentication though X.509 v3 certificate.

Settings - Administration - LDAP

In the LDAP panel you can choose to enable the integration of the Windows server user to be used as an administrator user in BLOCKBIT UTM.

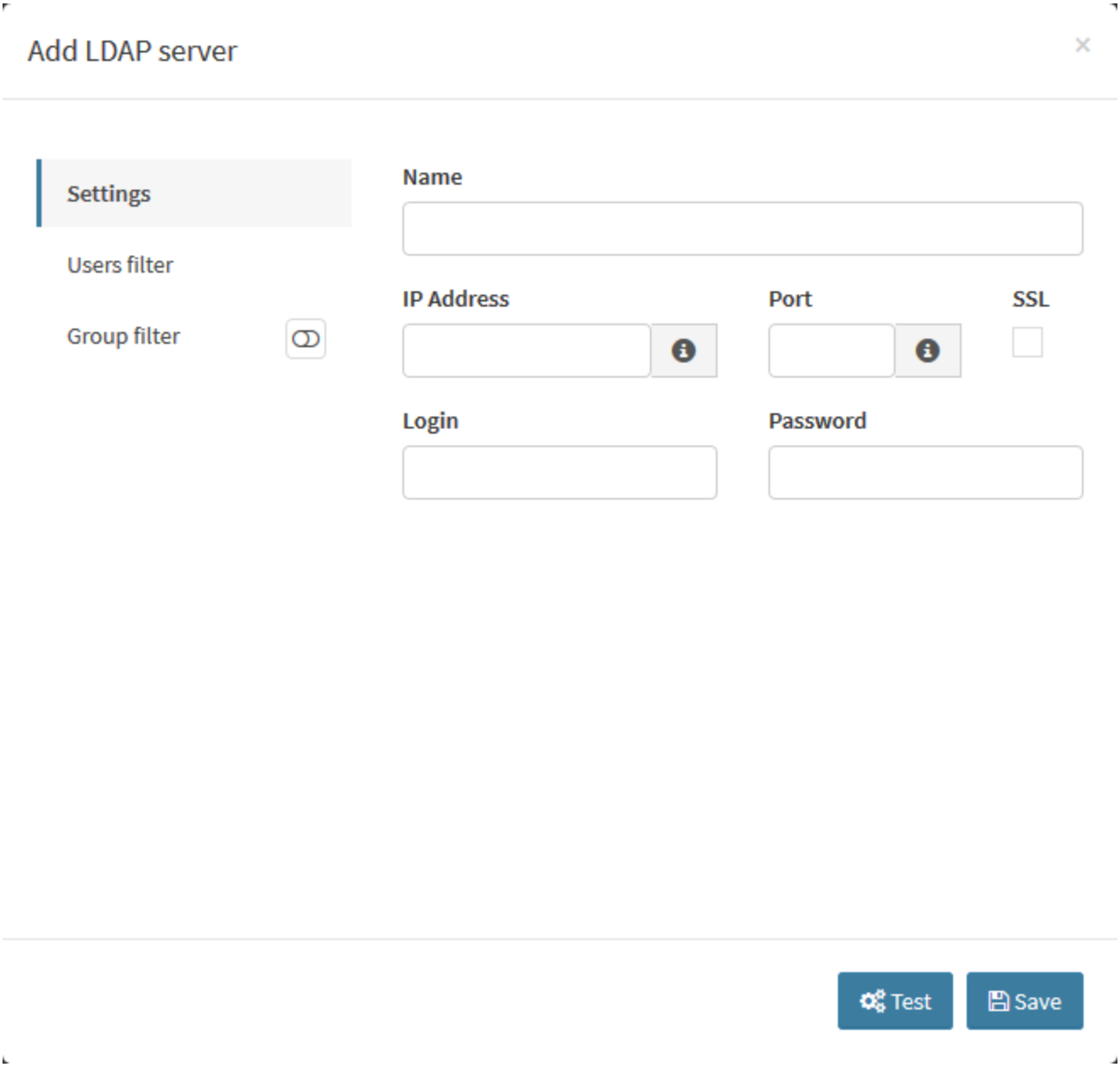


Settings - Administration - LDAP

- ***Enabled[ ]*:** If this checkbox is enabled, enables the use of the LDAP server;
- ***LDAP Server*:** Select the LDAP profile that was created in *Settings - Authentication*. Ex .: Primary DC;
- ***Domain*:** Define the domain in which users will be imported. Ex.: dominioc.com;
- ***Profile*:** Define the administrator user profile that will be used for integrated users through self-registration.

LDAP - Edit Server

To edit any server already added, click on the edit icon **[ ]**, a panel very similar to the addition will display the details of the server, as shown in the image below:

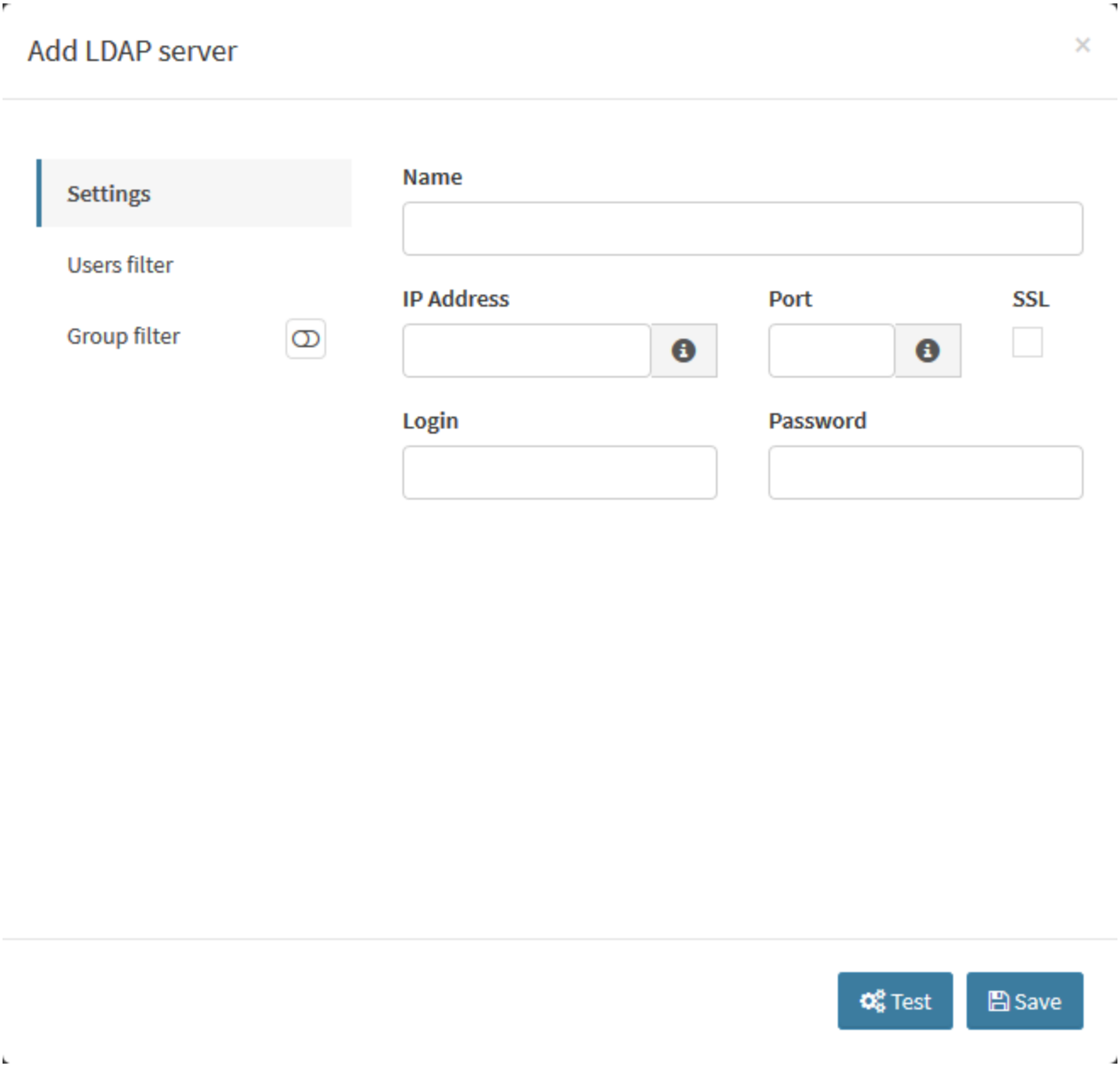


LDAP server – Edit Panel

Make the necessary edits and click [Save] to make the edit, or click outside the window to make no deletions.

LDAP - Add Server

To add a new server click on the [+] button. And the screen below will be displayed

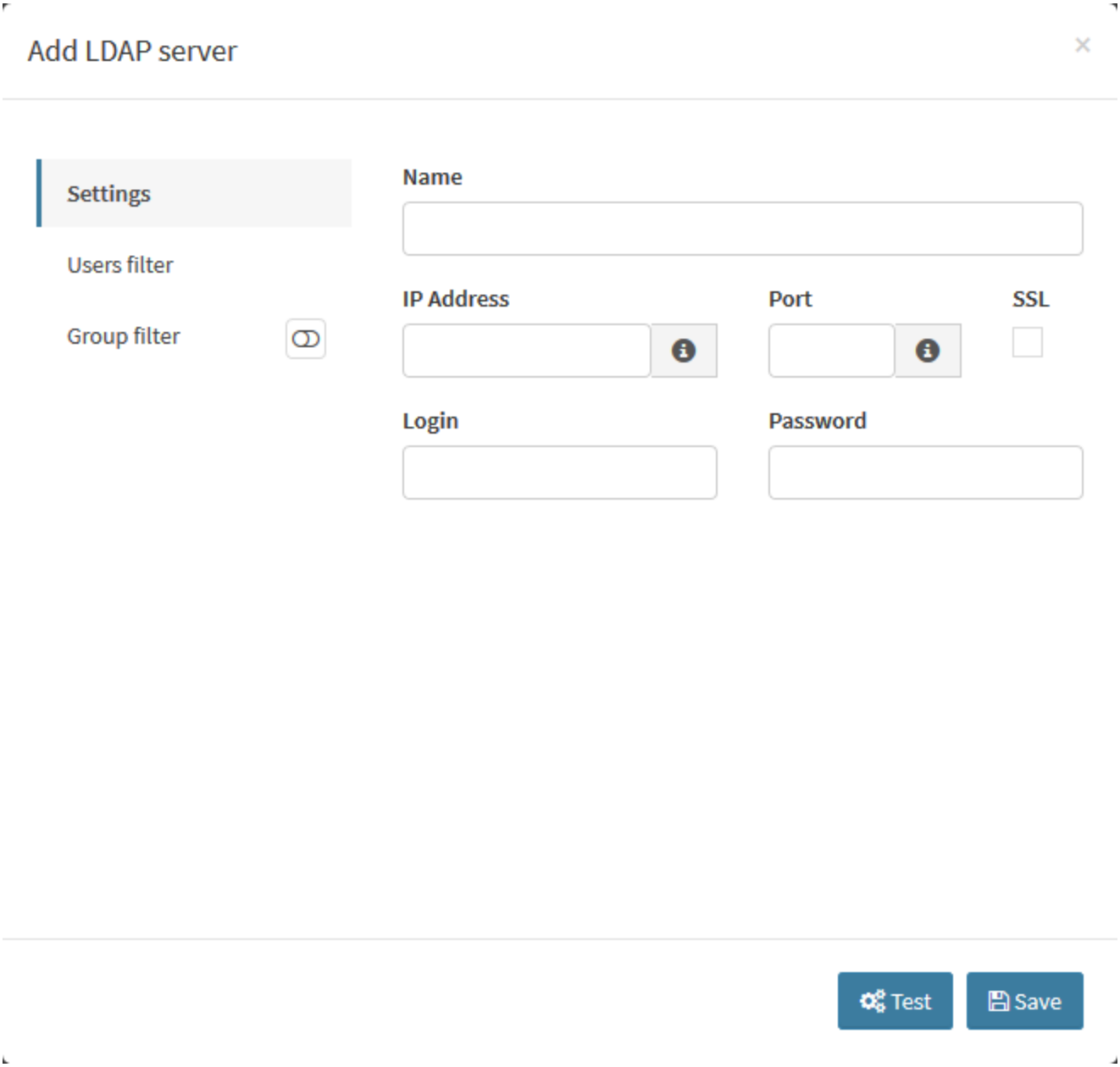


LDAP server - Addition Panel

Next we will analyze the "Settings" side tab.

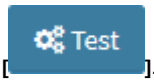
LDAP - Add Server - Settings

In this tab the fields that refer to the Windows AD server administration credentials can be configured.

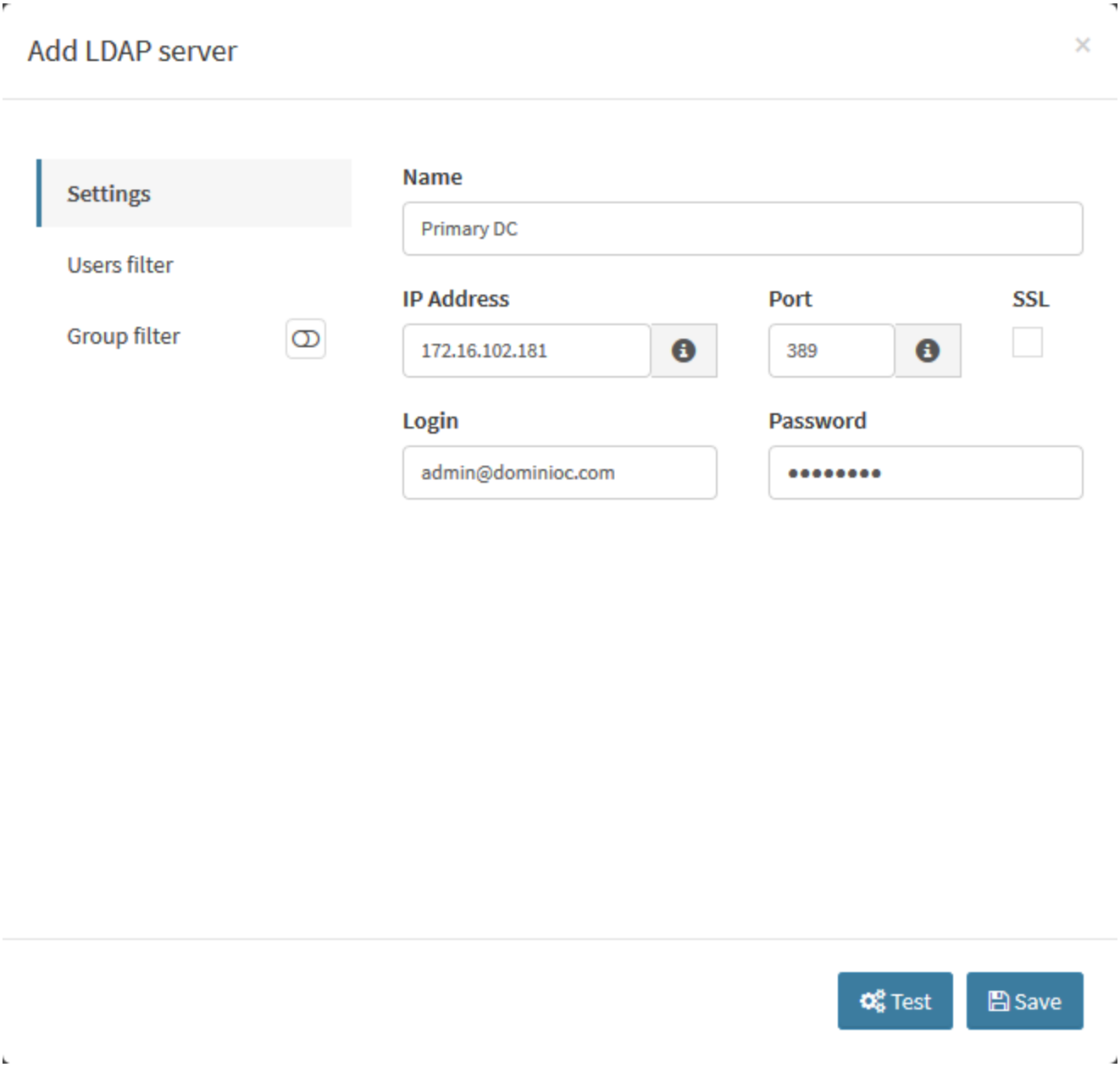


LDAP server - Addition Panel

- ***Name*:** Set a name for the sync connection. Ex.: *Primary DC*;
- ***IP Address*:** Set the IP address of the domain controller. Ex.: 172.16.102.191;
- ***Port*:** Set the port to connect to the domain controller, if the service is running on SSL select the option “SSL”. Ex .: 389;
- ***Login*:** Define a Windows server user with LDAP search rights, usually a member of the administrators group. Ex: *administrador@dominioc.com*;
- ***Password*:** Set user password.

To validate the access credentials click on [

].



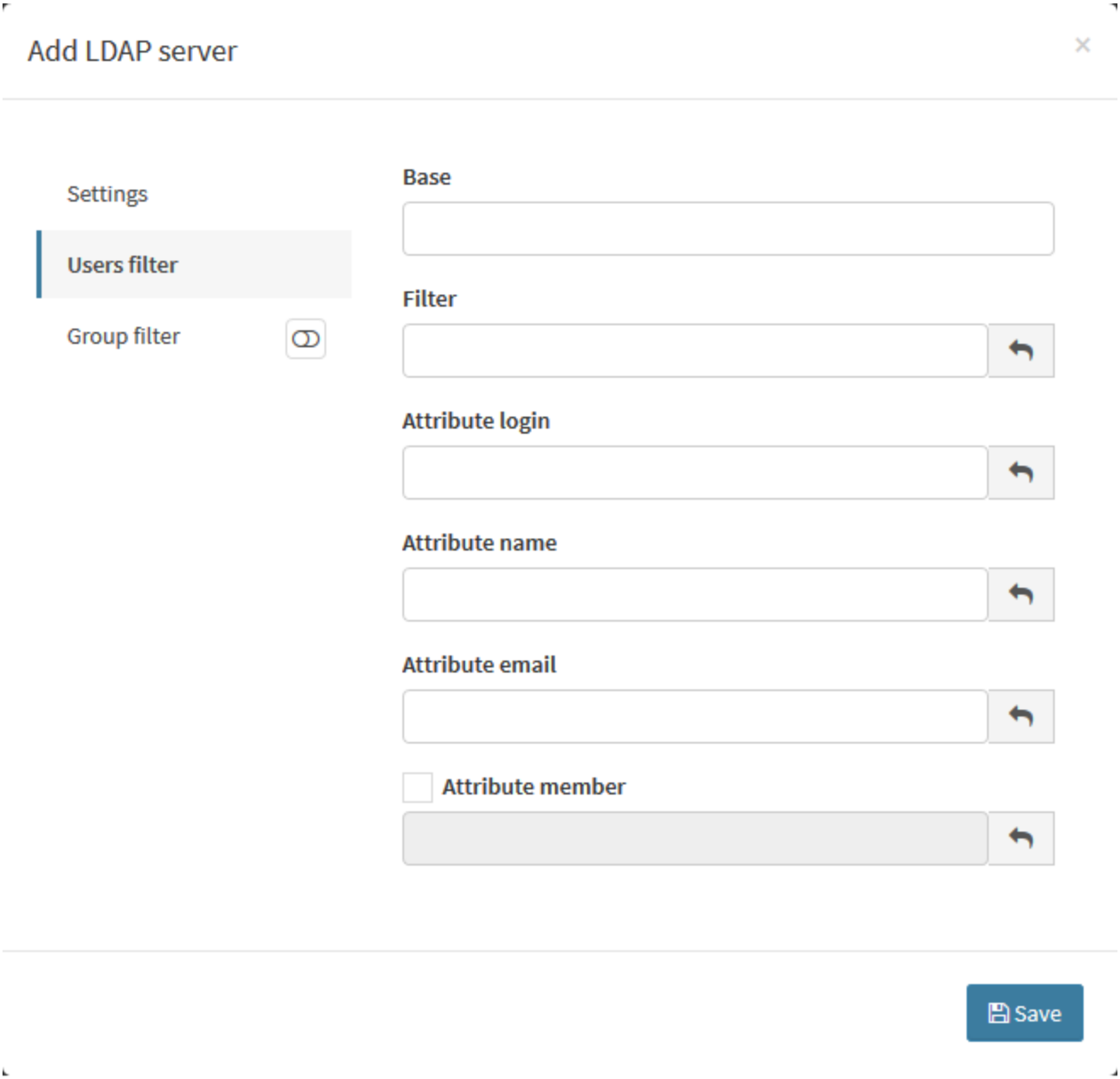
LDAP server - Addition panel - Settings

LDAP - Add Server – Users filter tab

In this tab, the fields referring to the user search base and their respective filters in the LDAP base of the Windows AD server are configured.

Configure the “Base”, “Filter”, “Attribute login”, “Attribute name”, “Attribute email” and “Attribute member” fields according to the LDAP database of the respective Windows server.

These fields are filled in automatically when you click the **[** **]** button.



LDAP server - Addition Panel - User Filter

For the configuration of a Windows AD server with LDAP, it is necessary to manually change the fields to have the values below:

- ***Filter:*** *(&(objectclass=user)(objectclass=person)(!(objectclass=computer)))*
- ***Attribute login:*** *userPrincipalName*

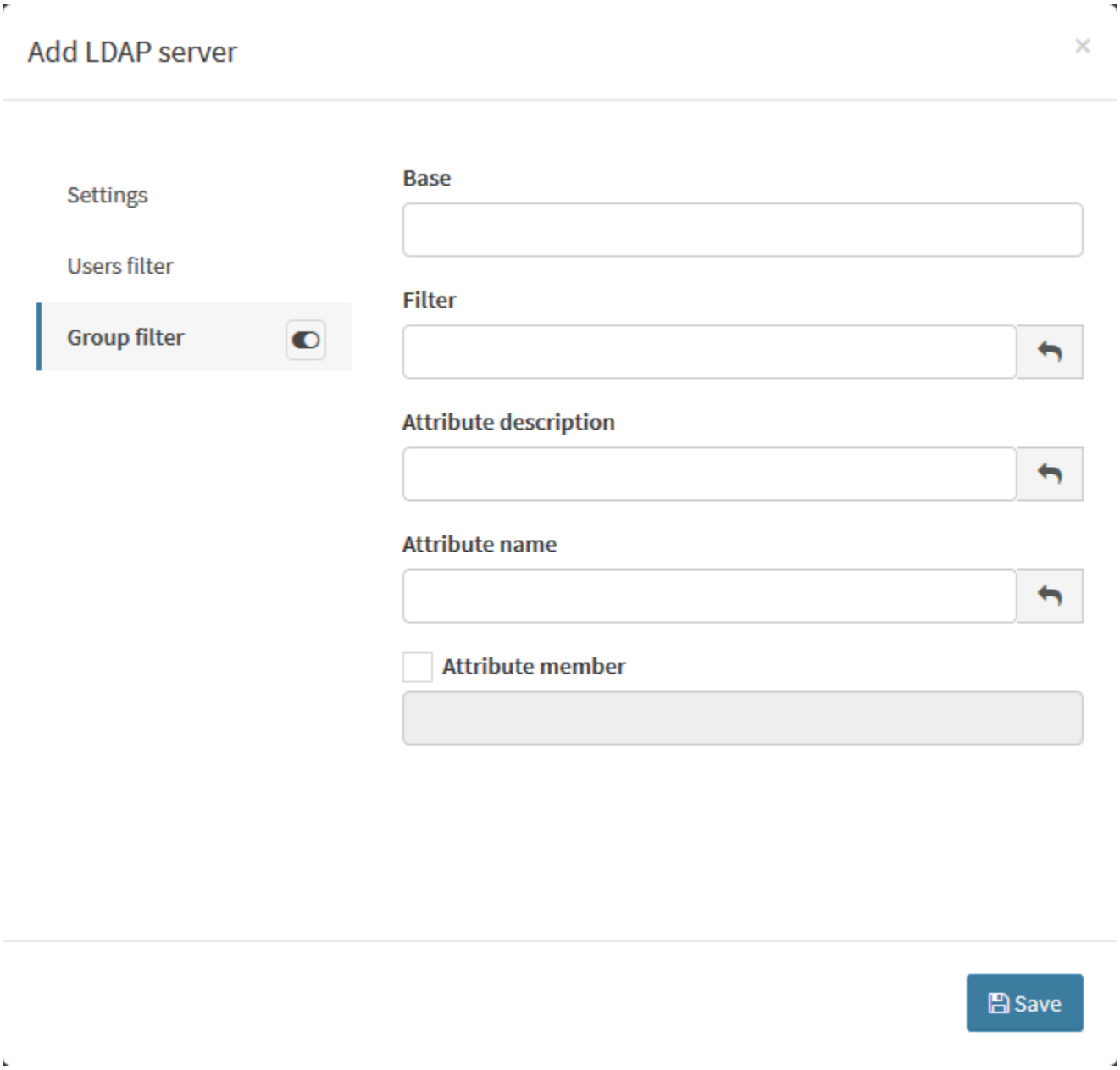
Fill in the fields and click [

].

LDAP - Add Server – Group filter tab

In this tab it is possible to enable group synchronism by clicking on the [ ] button. Configure the fields “Base”, “Filter”, “Description attribute” and “Member attribute” according to the LDAP database data of the respective Windows server.

These fields are filled in automatically when you click the [ ] button.



LDAP server - Addition panel - Group filter

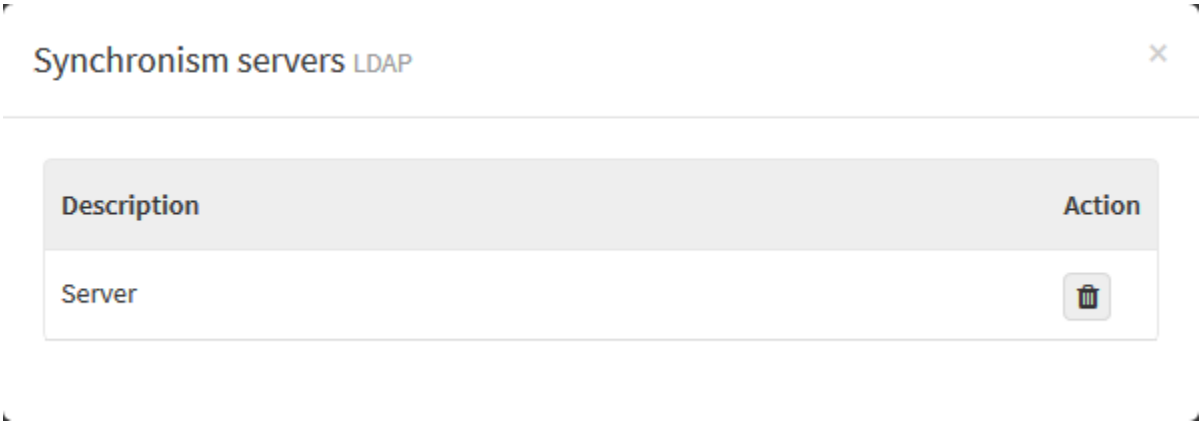
After filling in the fields, click [ ].

The principle of configuring the synchronism of an LDAP base is the same. *However, it is important to consider that the filter and search base settings on an LDAP server are created by those who implement the directory service and therefore, it is necessary to have this information in order to be successful in the configuration.*

After adding the LDAP server we will return to the previous screen.

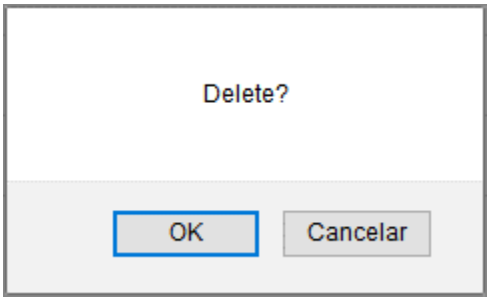
LDAP – Delete Server

To remove any server, click on the delete icon **[** **]**, a panel with all created servers will be displayed, as shown in the image below:



LDAP server – Removal Panel

Choose the server you want to be removed and click the delete **[** **]** icon to remove the desired server. A confirmation message will be displayed:



LDAP server – Deletion confirmation message

Click the **[** **]** button to remove the selected server, or click **[** **]** to make no deletion.

LDAP – Connection Test

After adding a connection, it is possible to perform a connection test by clicking on the connection test icon **[** **]**, by clicking on this icon a message will appear informing the current status of the server.

Settings - Administration - Ports

On the Ports panel, it is possible to enable the NGFW's administration by the HTTP and Telnet ports. It is important to remember that this resource is disabled by standard, and it must be enabled via WEB or CLI interface by using the following commands:

Command: *"admin-over-http"*
Usage: *admin-over-http <enable|disable|status|change-port>*

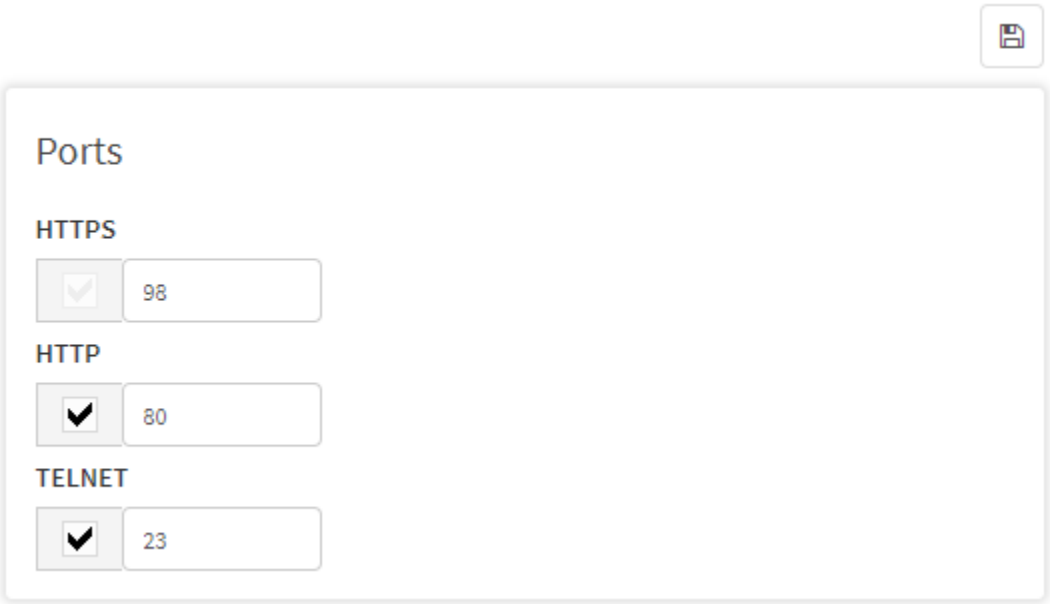
--enable: Enables the http access
--disable: Disables the http access
--status: Checks the http's status
--change-port <new-port>: Changes the http access port

It's also important to list the commands used to enable access via Telnet:

Command: "*admin-over-telnet*"
Usage: *admin-over-telnet <enable|disable|status>*

--enable: Enables the Service
--disable: Disables the Service
--change-port: Sets the Telnet Port
--status: Verifies the Service's status

By web interface, on Settings > Administration Ports, check the option to be enabled:



Settings - Administration - Ports

It's important to remember that some ports are not available for use Ex: 22, 9803 or 5432.
To change the Zone Protection Policies' standard, just access: Services Firewall Zone Protection:

ID(1): HTTP Access

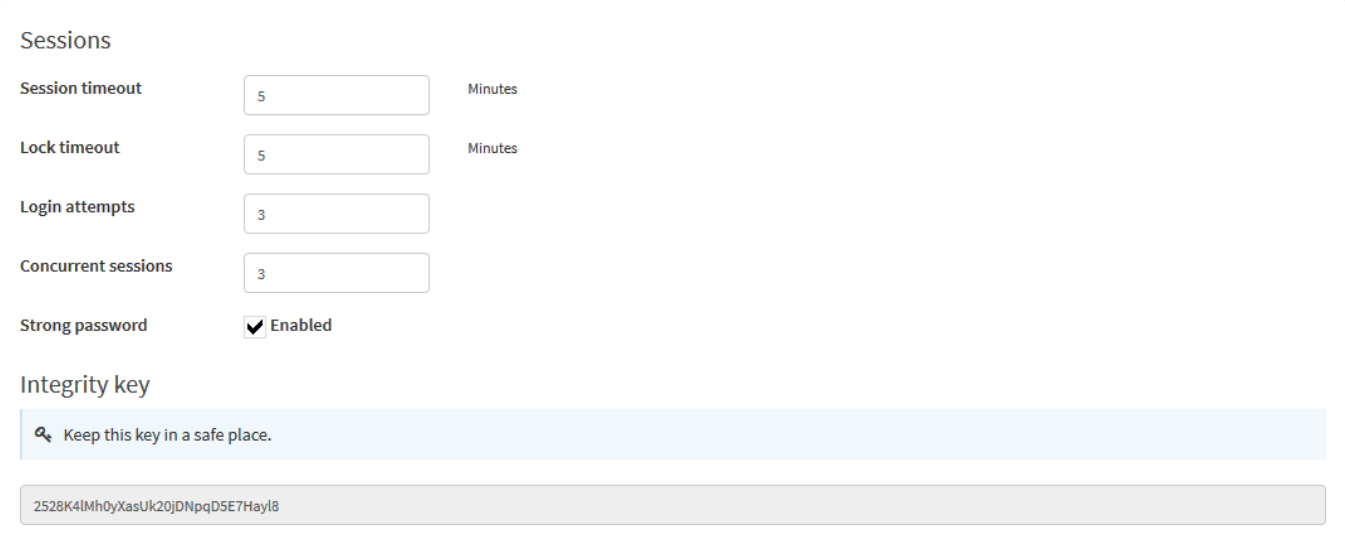
ID(2) : Telnet Access

(Allow), Enable, and WAN/ALL Zone

By having enabled and marked the box with the option of the port to be used, the resource will work normally.

Settings - Administration - Sessions

In the Sessions panel, you configure the "time out" times when accessing the WEB interface, according to the policy you intend to adopt. These parameters specify the security standards adopted when accessing the management of the BLOCKBIT UTM interface.



Administration - Sessions

- ***Session timeout*:** It is the time in minutes that the interface disconnects due to inactivity. Ex.: *5 minutes*;
- ***Lock timeout*:** It is the time in minutes that the interface unlocks an administrator user that was blocked by a password error. Ex.: *5 minutes*;
- ***Login attempts*:** Number of login attempts, upon reaching the configured value, login is blocked by connection attempts. Ex.: 3;
- ***Concurrent sessions*:** It is the number of simultaneous logins connected in the administration interface. Ex.: 3;
- ***Strong password[ ]*:** It is possible to enable only the use of strong passwords for the administrator login.

INTEGRITY KEY: System integrity key, used in the process of encrypting backup files, and the integrity stamp of reports.

Keep it in a safe place!

It is important to know that: In cases of reinstallation the user needs to configure this field with the same value (key) used in the previous installation. The process of restoring settings and validating the reporting key integrity key, depends on this key, in order to maintain the integrity of the reports and to successfully restore the settings from the previous database.

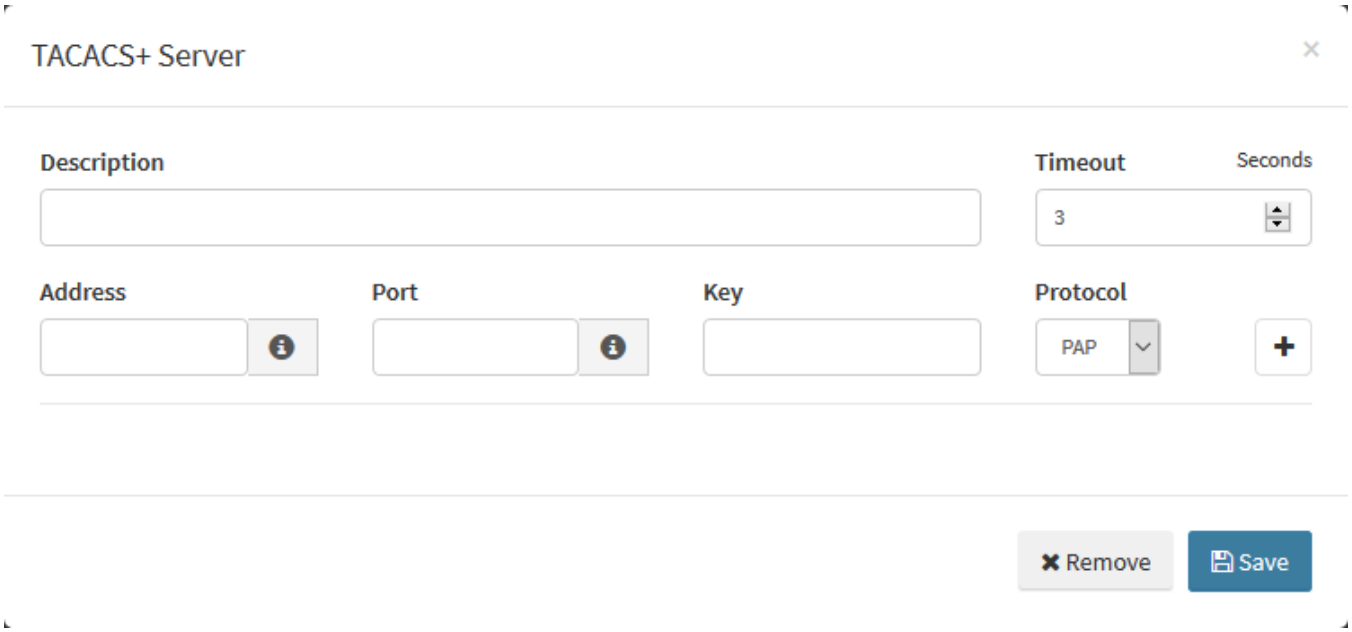
Settings - Administration - TACACS+

Back in the initial panel, in **[TACACS+]** you can choose to enable the integration of the TACACS+ server user to be used as an administrator user in BLOCKBIT UTM.

- ***Enabled*:** If this check box is enabled, enables the use of the **TACACS+ server**;
- ***TACACS+ Server*:** Select the TACACS + profile that was created in **System >> Authentication**. Ex.: *TACACS* Windows Server;
- ***Domain*:** Define the domain in which users will be imported. Ex .: dominioc.com;
- ***Profile*:** Define the administrator user profile that will be used for integrated users through self-registration.

TACACS+ Server - Edit Server

To edit the settings already made, select the desired server in the “TACACS + Server” drop-down menu and click on edit **[**  **]**, the screen below will be displayed:

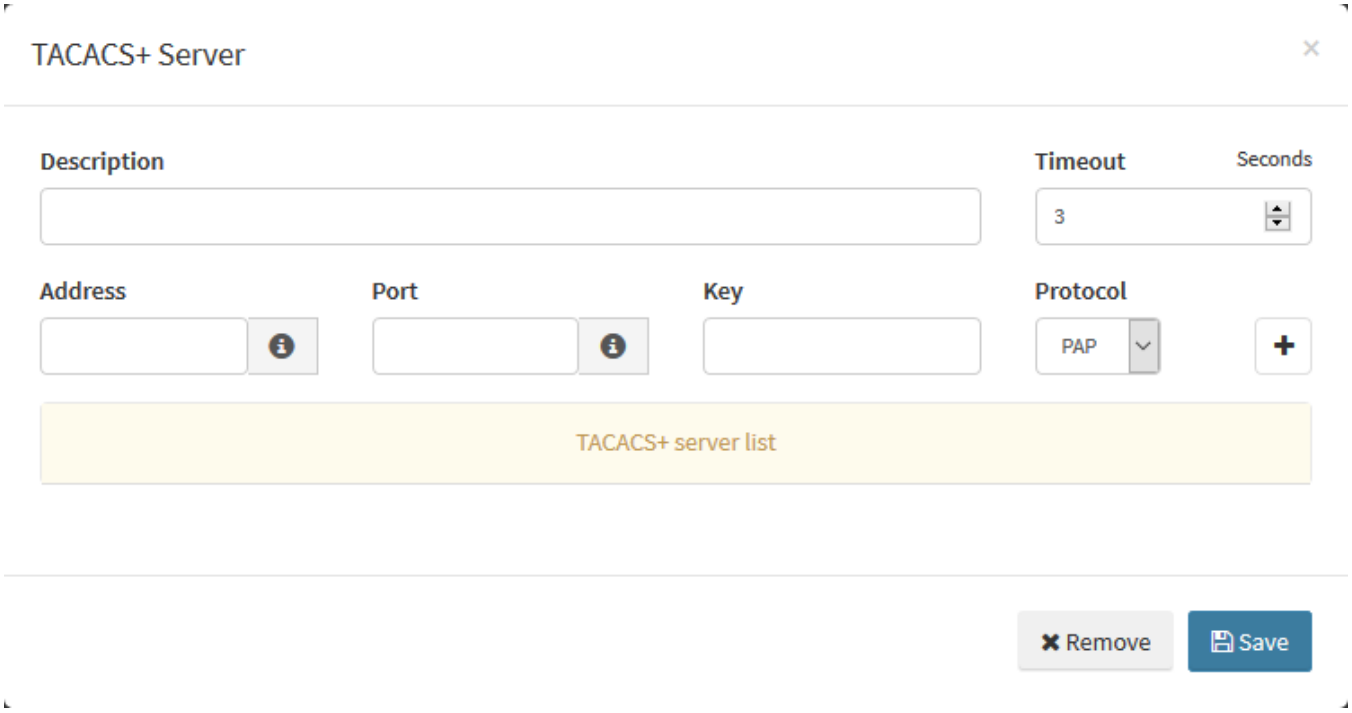


TACACS+ server - Edit

In the same way as during the addition, it is possible to edit the desired settings and click save **[**  **]**, in order to record the necessary changes made.

TACACS+ Server - Add Server

To add a new server click on the **[**  **]** button. And the screen below will be displayed:



TACACS+ - Server settings

Below we will specify some fields:

- ***Description:*** *Enter the server description. Ex.: TACACS + Windows server*;
- ***Timeout:*** *Sets timeout in seconds for the server to wait for a response from the host. Ex.: 10*;
- ***Address:*** *IP address of the desired server. EX.:10.0.0.1/32*
- ***Port:*** *Specifies a port number for the server. Ex.: 49;*
- ***Key:*** *Defines the authentication key used to perform the communication and encryption of the communication with the TACACS + authentication server. Ex .: blockbit.utm*;
- ***Protocol:*** *Determines the type of authentication protocol desired. Ex.: PAP;*

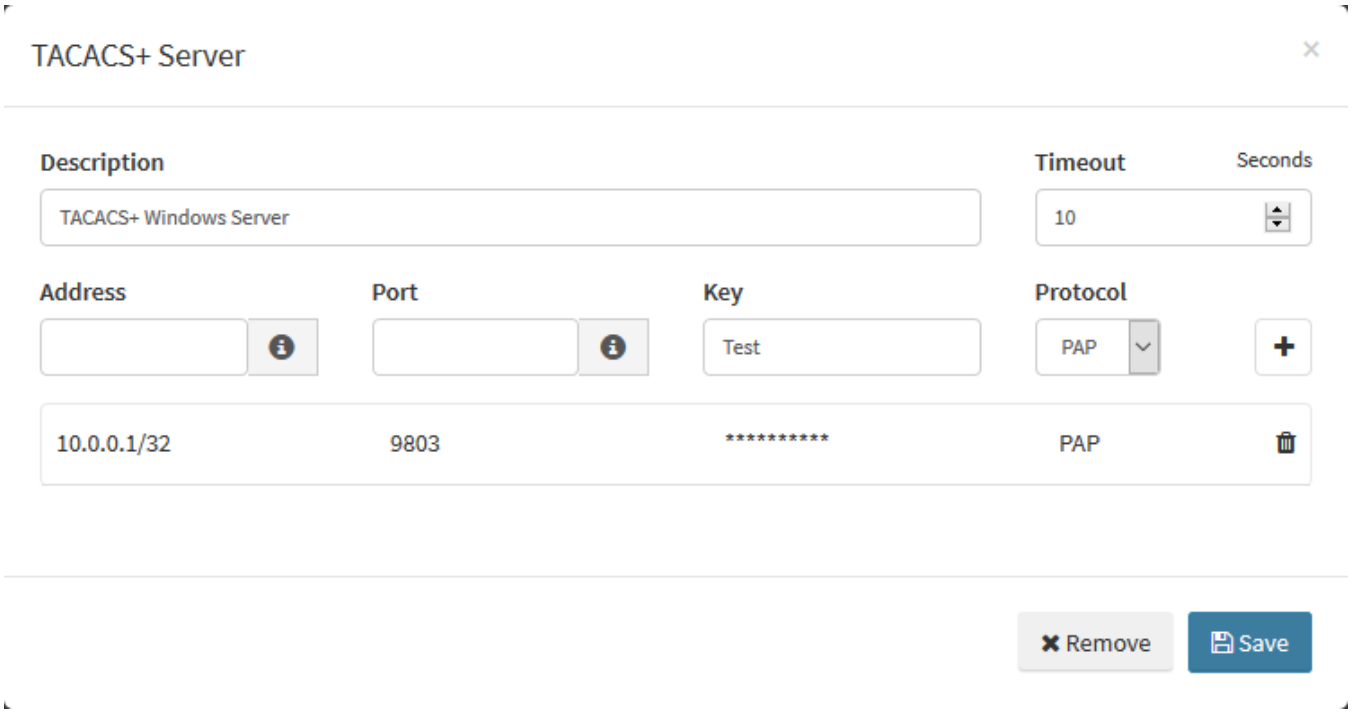
After completing the Description, Timeout, Address, Port, Key and Protocol fields, click the ***add*** **[ ]** icon to add the server to the list of TACACS + servers;

The server list serves as a means of preventing possible communication failures with the TACACS + server, for example:

- Response time exceeded;
- Firewall or access list blocking traffic;
- TACACS + configured with the wrong authentication key;
- Among other possibilities...

The system works by trying to connect with the servers registered in this list in order, trying to make the connection until one of these servers responds and authentication is performed. Precisely for this reason, it is essential that the server base be identical.

If you want to remove a server added to the list, click the remove icon **[ ]**.

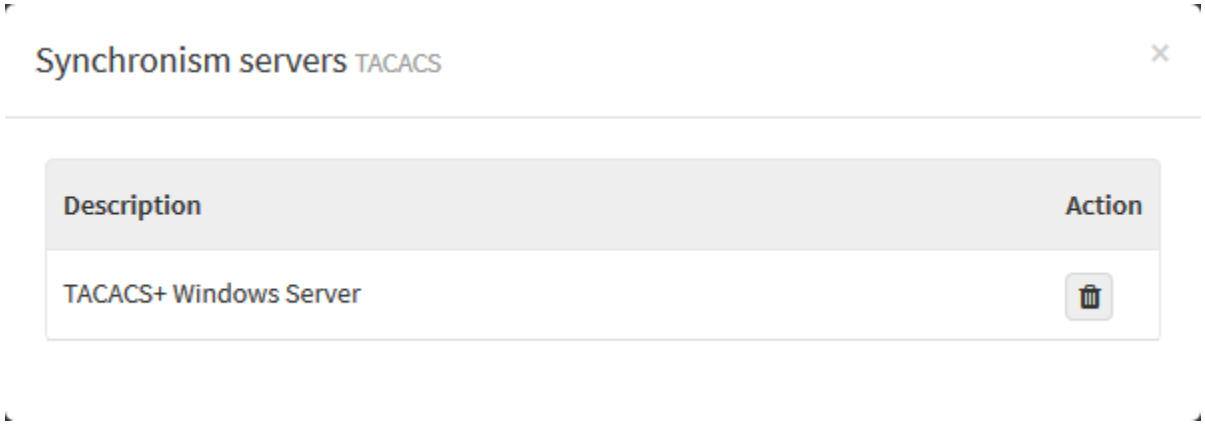


TACACS+ - Server list

After making the appropriate settings, click save **[**  **]** to register them correctly, otherwise, click outside the screen to cancel the edits made;

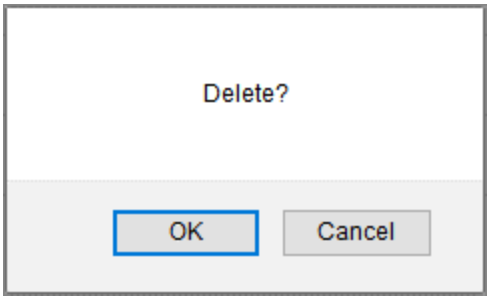
TACACS+ Server - Delete Server

To remove any server, click on the delete icon **[**  **]**, a panel with all created servers will be displayed, as shown in the image below:



TACACS+ server – Removal Panel

Choose the server you want to be removed and click the delete **[**  **]** icon to remove the desired server. A confirmation message will be displayed:

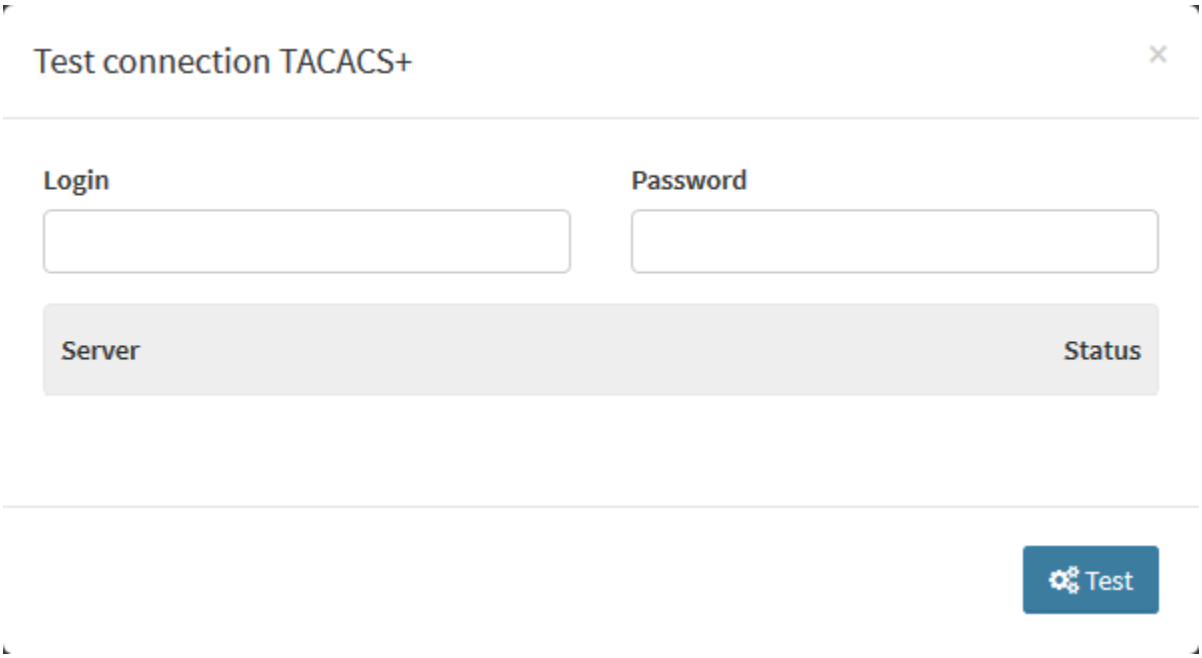


TACACS+ server – Deletion confirmation message

Click [OK] to remove the selected server, or click [Cancel] to make no deletion.

TACACS+ Server - Connection Test

After adding a connection, it is possible to perform a connection test by clicking on the connection test icon [ ], by clicking on this icon the screen below is displayed:



TACACS+ server – Test Connection

The function of this panel is to test the connection of a user to the database of the TACACS + server, for this purpose carry out the following steps:

1. In “Login”, enter the login information that was used to enter the TACACS + server;
2. In “Password”, type the password;
3. In the “Server” and “Status” list, we will have a list of TACACS + servers and their current availability status.

When clicking on the [Test] button, a connection test is performed that updates the appropriate states in the list mentioned above;

Administration - Administrators tab

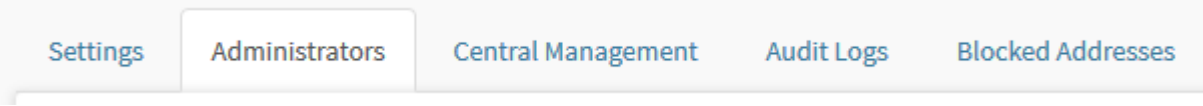
This item allows the management of registration and permissions among/for system administrators. By default the system already includes the administrator "admin", the password is defined in the "Configuration Wizard".

In the Administrators tab, it is possible to view all registered administrators with the options of "Search", "Edit", "Disable" or "Remove" a system administrator. There are two levels of system administrators:

Super administrador: Has full privilege over the interface including managing any administrator level. No need to set permissions.

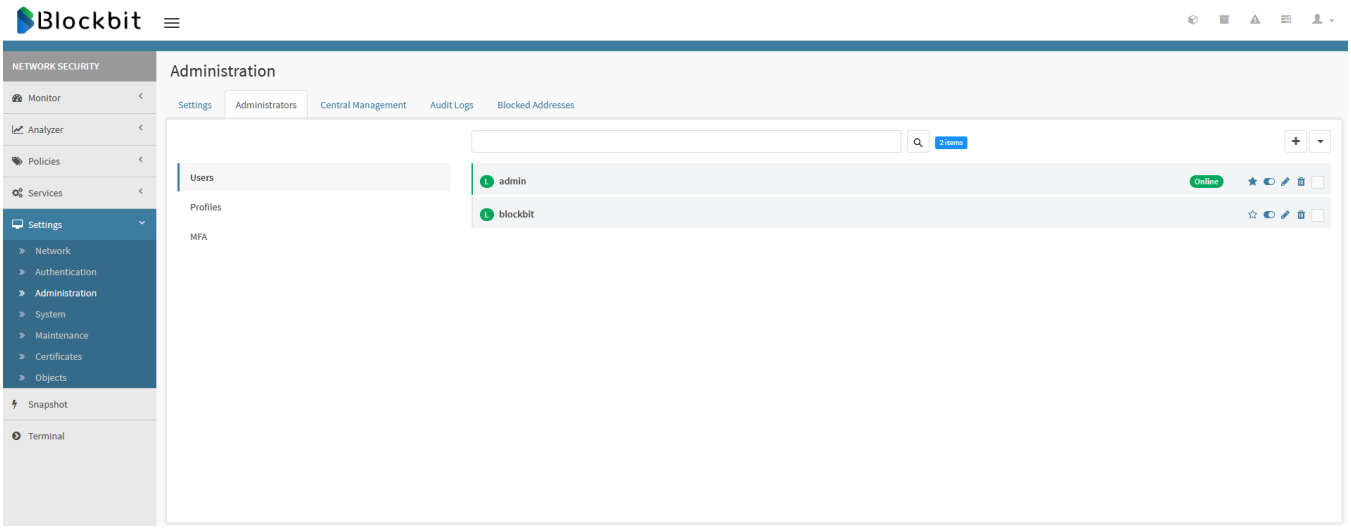
Common administrator: Restricted administration rights are required to set permissions on the functionalities through a profile in which it is defined where to view settings and management.

To access, click on the "Administrators" tab:



Administrators tab

The screen shown by the image below will appear:



Administration - Administrators

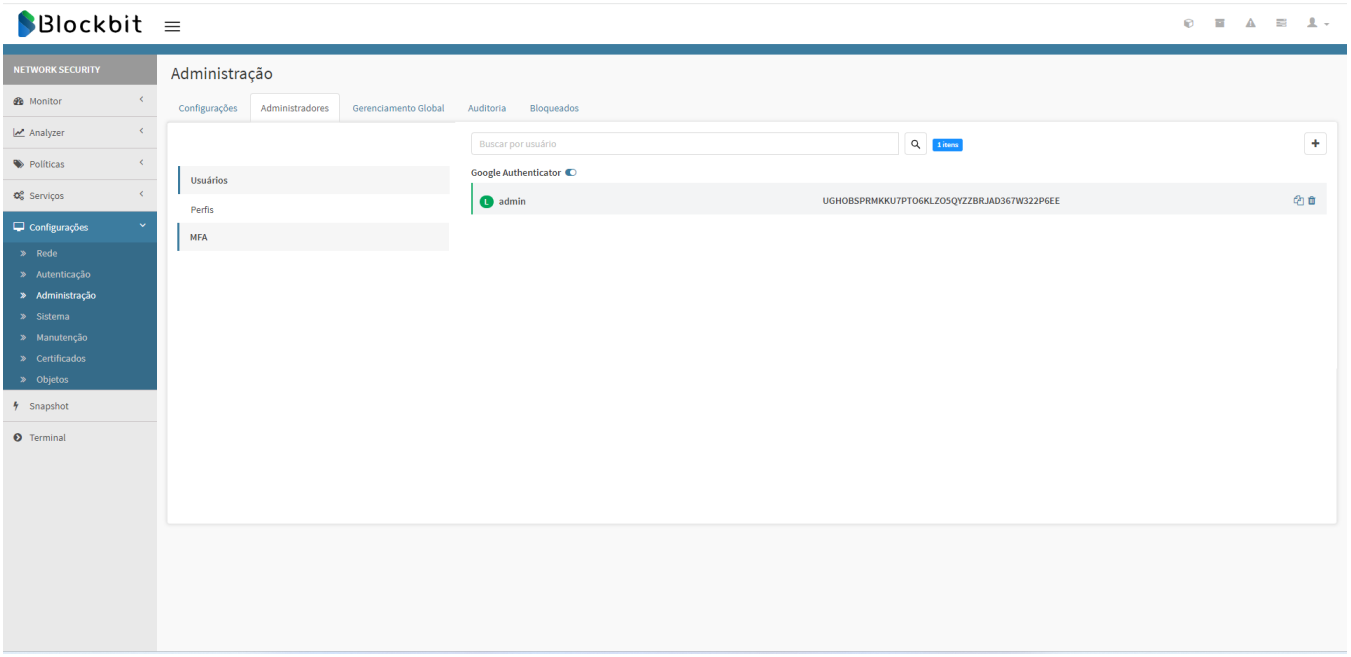
This screen is made up of two side tabs:

- *Users*;
- *Profiles*;
- *MFA*.

Next, we'll look at each tab in detail.

Administrators - Users

In Users, it is possible to create administrator users with access to the administration interfaces and MFA validation.



Administration - Administrators - Users

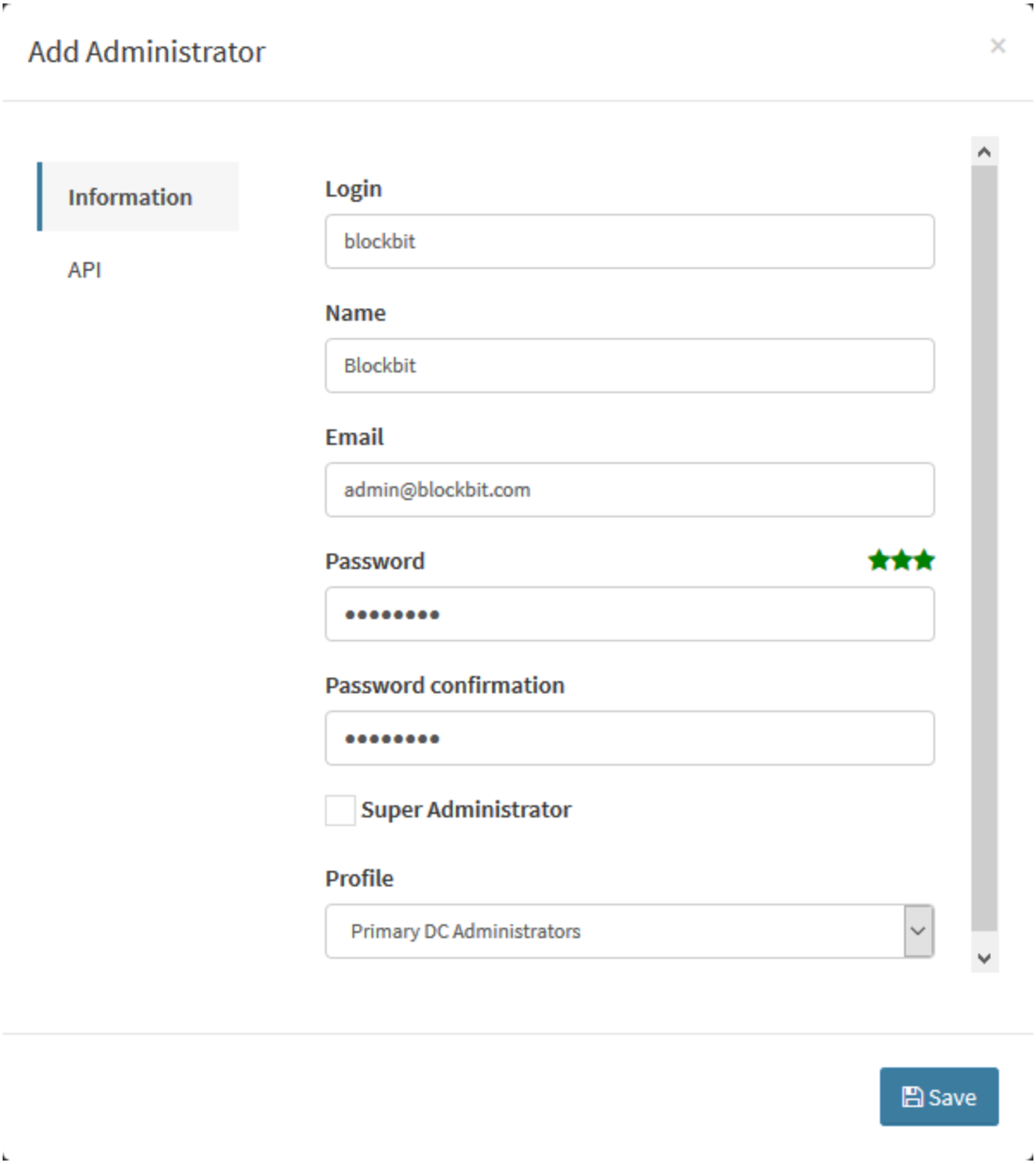
To add a system administrator, click **[**  **]**.

The registration interface is divided into 2 (two) side tabs:

- *Information*;
- *API*.

Information

To configure the “Information” tab, define the type of administrator, if you check the **Super Administrator [**  **]** checkbox, the “Profile” option is hidden, otherwise, select the profile with the permissions on the interfaces that the “Common Administrator” will have rights.



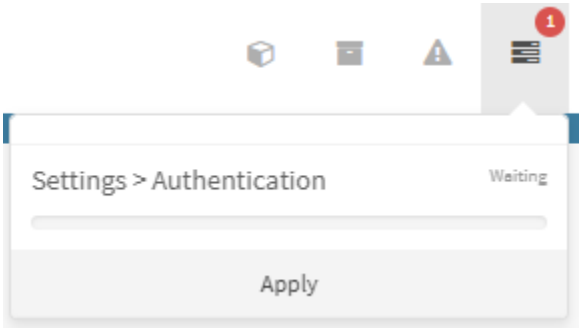
Administration – Add Administrator

- ***Login*****:** Inform the administrator login. Ex .: blockbit;
- ***Name*****:** Enter a name for the administrator. Ex.: Blockbit;
- ***Email*****:** Inform an email to the administrator. Ex.: admin@blockbit.com;
- ***Password*****:** Inform the password for the administrator user;
- ***Password confirmation*****:** Confirm the password for the administrator user;
- ***Super Administrator[ ]*****:** Inform if the administrator user will be super system administrator;
- ***Profile*****:** Enter the profile for the administrator user. Ex.: Primary DC Administrators;

Multi-factor Authentication

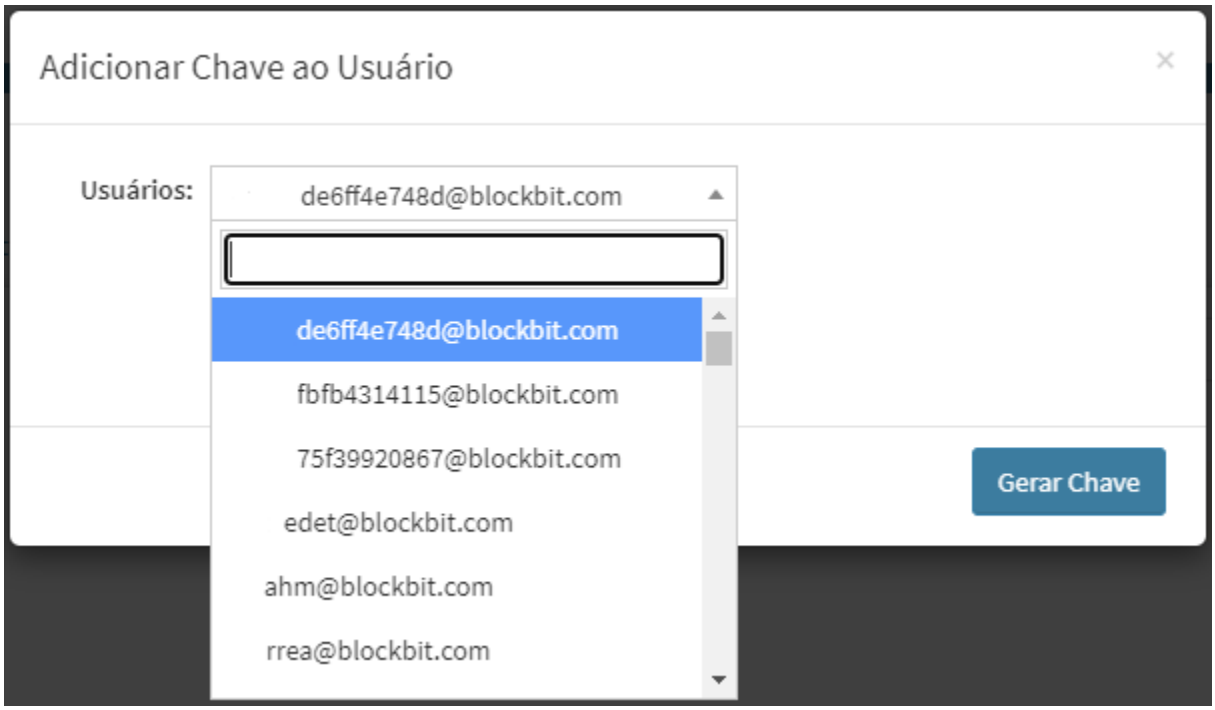
The MFA (Multi-factor Authentication) option allows the generation of a unique key to be used with the Google Authenticator for user validation by using an MFA token.

After having created a user in Administration Administrators Users, one must enable the MFA [Google Authenticator], and "apply the changes" since the functionality comes disabled by factory standards:

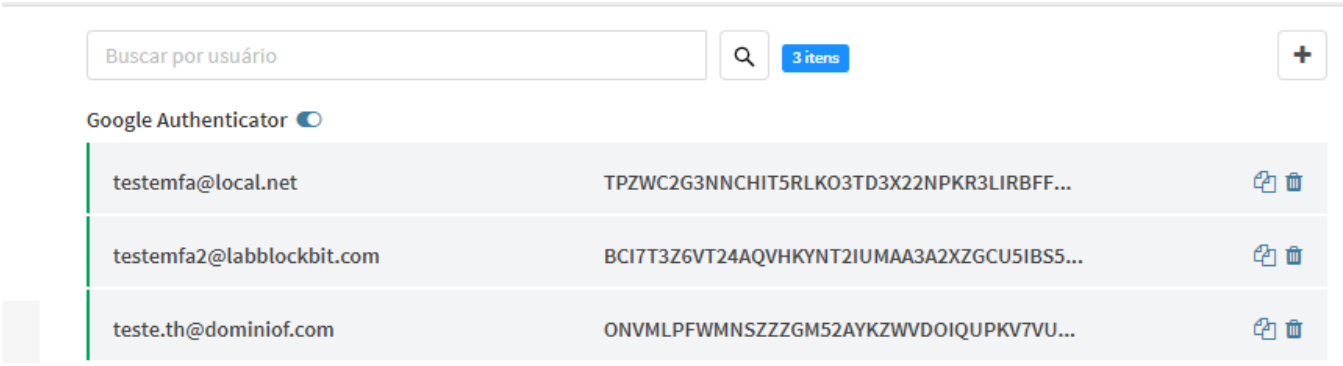


Settings Apply

After the activation of the service, a list with all the users will be displayed. By clicking on the " + " button, it will be possible to select a user and generate a key for this one:



Generate Validation Key

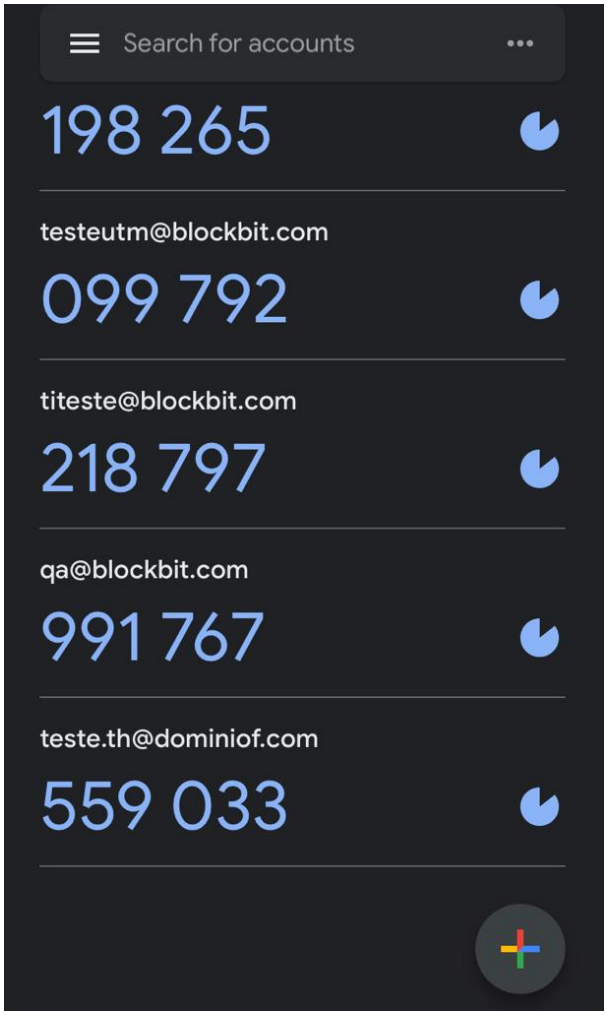


List of users with issued validation keys

The Copy [ ] and Delete [ ] buttons allow the copy or deletion of a key.

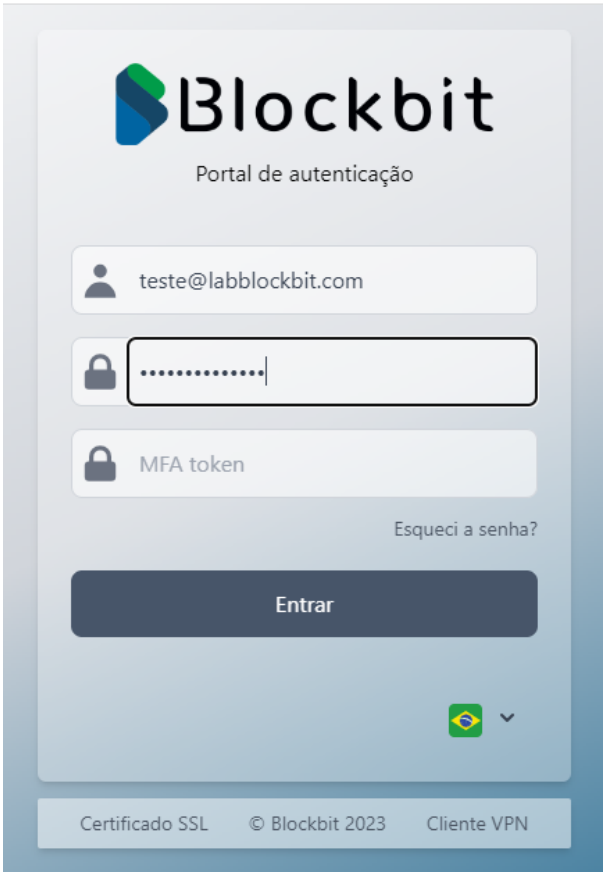
After having generated a validation key for a user it is necessary to have the Google Authenticator App in another device (a smartphone, or a laptop). On the App, click on the "+" option insert validation key and use the key obtained from the NGFW. Select the *"time-based"* key type.

By doing so, a six-digit validation token will be generated for the user.



Google Authenticator - Access Tokens

After obtaining the token, access the authentication portal, and log in:



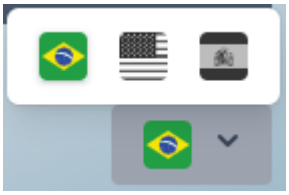
Login Screen

- : Insert the *Username*
- : In this field use the *Password* registered for this user.
- : In this field the *MFA Token* obtained from the *Google Authenticator* App must be inserted.

After filling these field, click "Login".

In case the password has been forgotten, click on "Forgot password".

To switch between languages, click on the flags displayed and select between one of the three available options:



Language selection

Select between Portuguese (), English () and Spanish ().

About the *Tokens*:

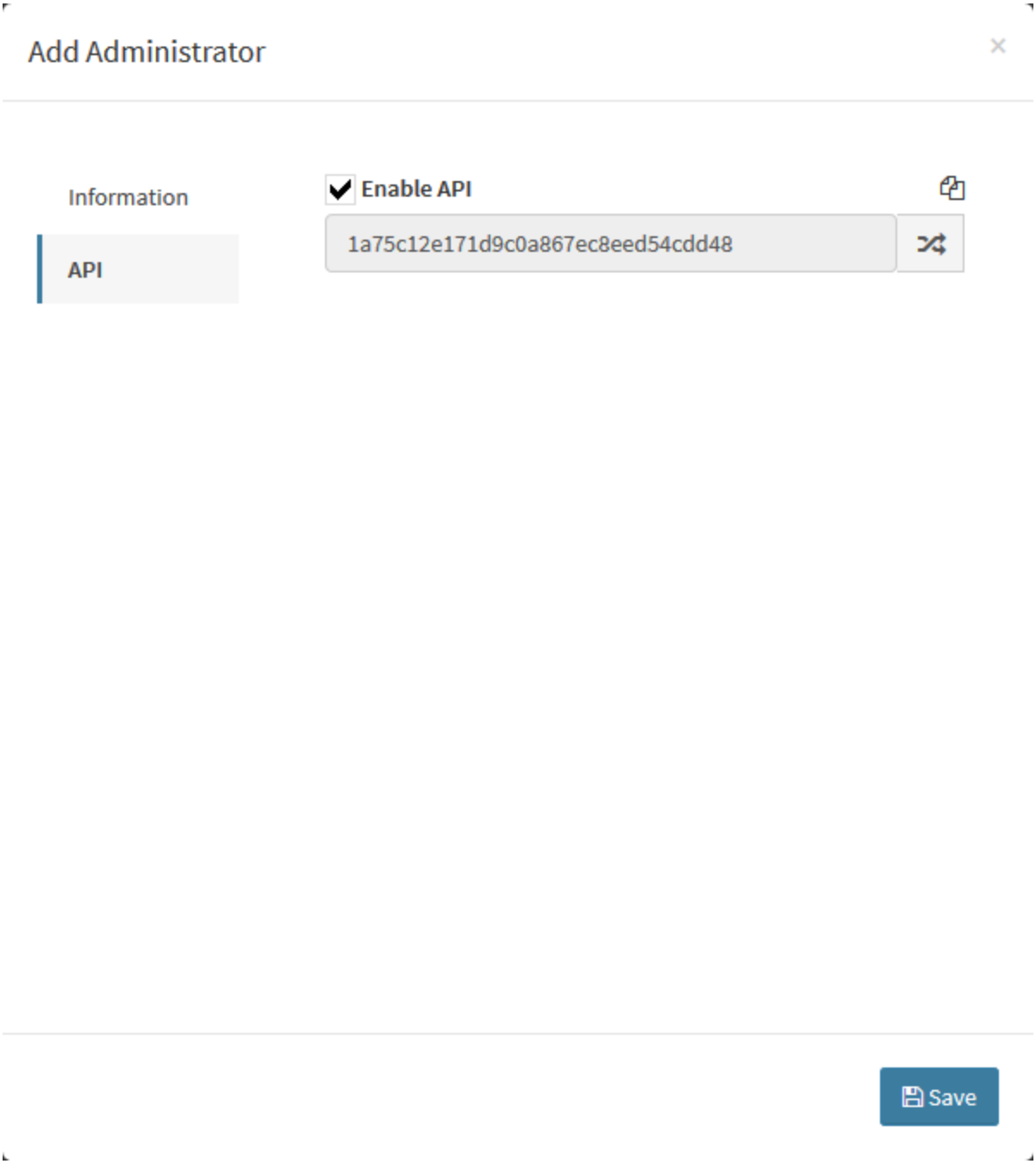
The tokens are meant to be used only once. The user can use up to 3 tokens, (the current, the previous and the next ones) uppon the attempt to use another token, the user becomes invalid. In case the token is typed in wrongly thrice, the user becomes invalid for 30 seconds.

It's important to remember that the token is changed often, so when logging in, one must consult the token on the Google Authenticator App.

By doing so, the authentication will have been successfully done.

API

In the API tab, it is configured whether the administrator user can have permission to access the GSM API.



Administration - Edit Administrator

- ***Enable API[ ]:*** This option enables the use of the API key and grants access to the GSM API. If this checkbox is enabled, the user can be added in the Administrator option on the Central Management tab and will be allowed to link UTM to GSM, and all actions performed by the GSM will be linked to this user in the reports. The value shown in the API Key field located on the Administrators tab will be identical to that shown on the Central Management tab.

After completing the changes, click **[Save]**.

Administrators - Profiles

In the Profiles tab, where the access permission profiles for the administration interfaces will be created.

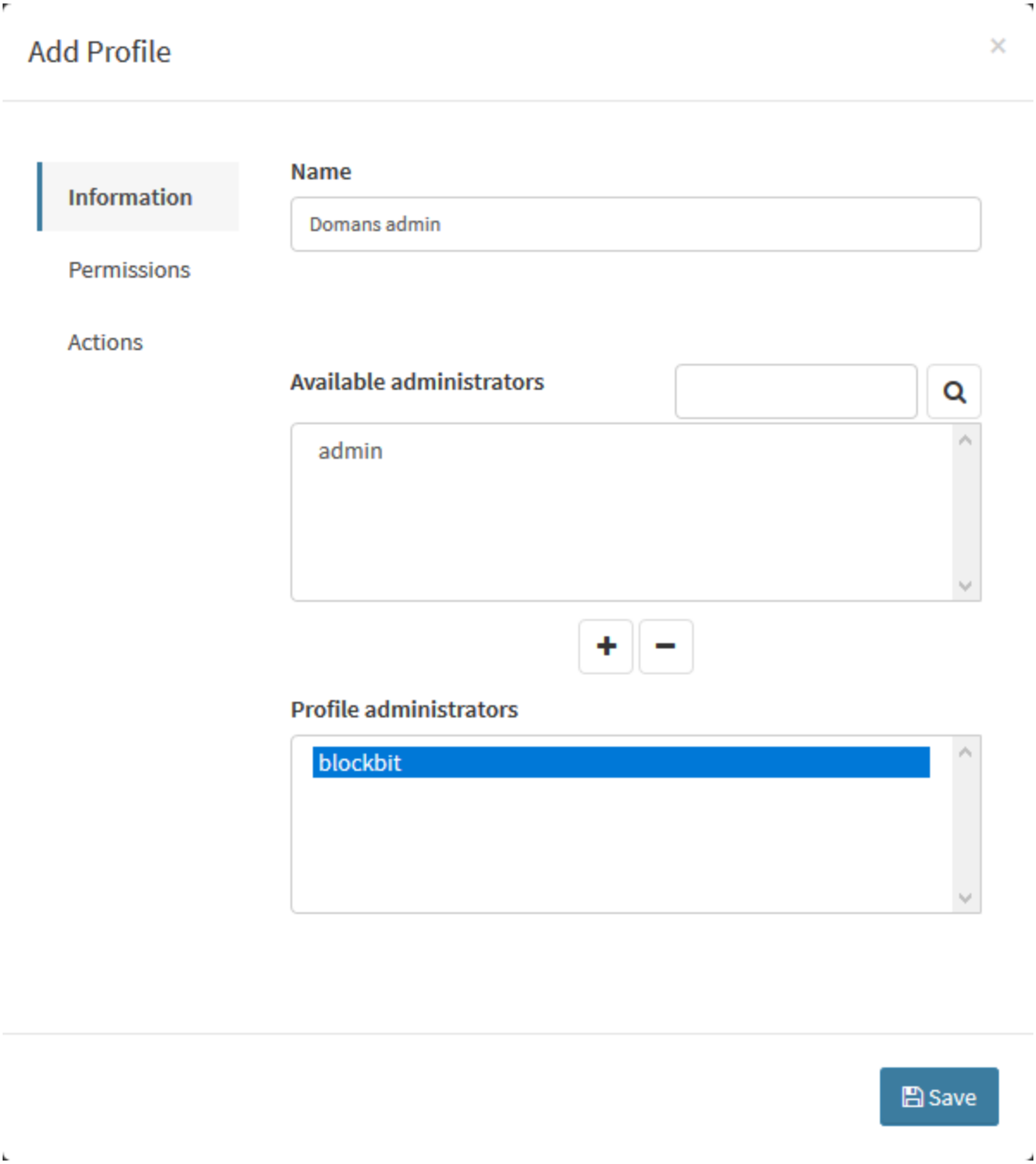
To add a profile, click **[**  **]**.

The registration interface is divided into 3 (three) tabs:

- *Information;*
- *Permissions;*
- *Actions*.

Information

Here's an overview of the Information tab:

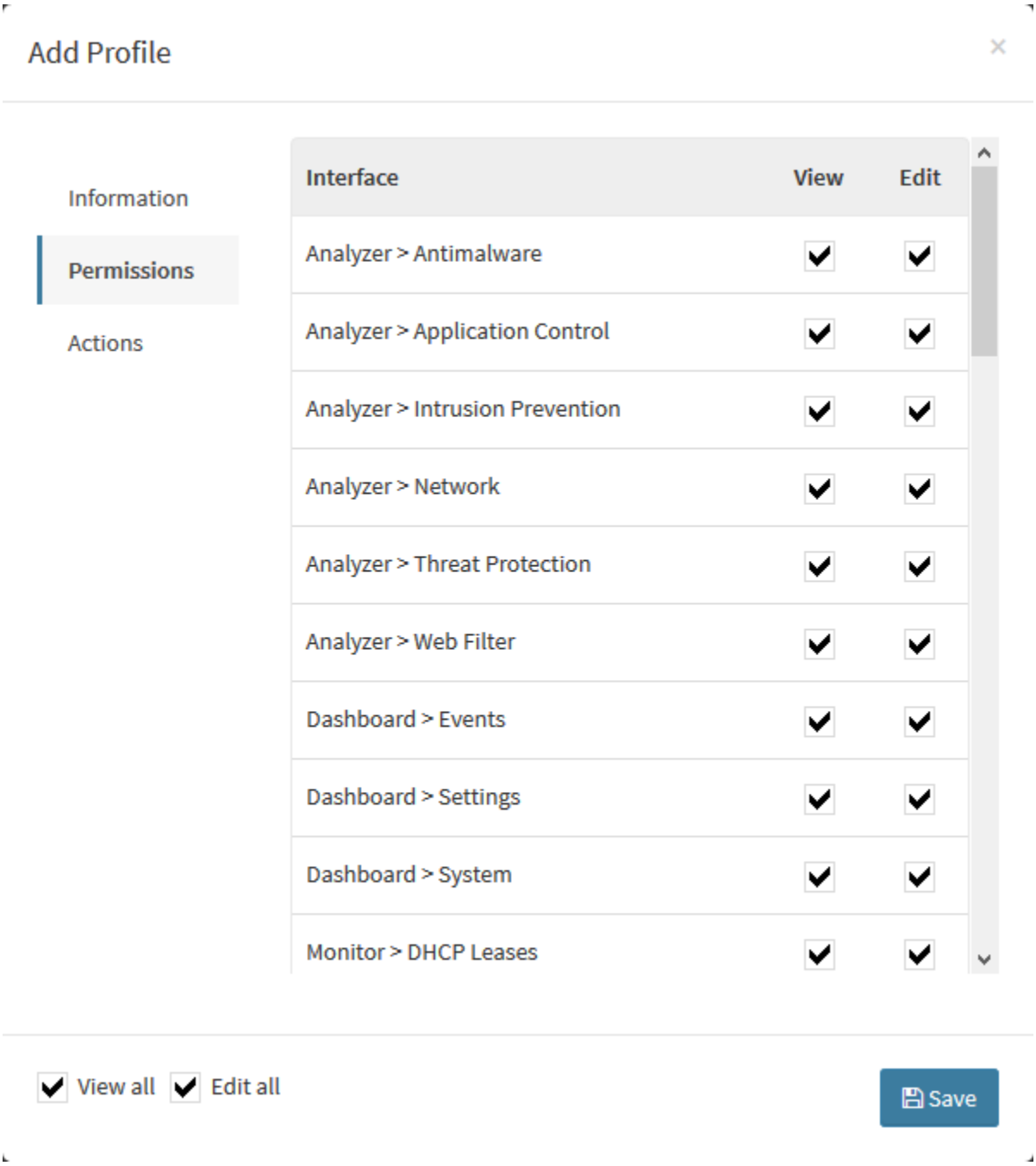


Administration - Add Profile

- ***Name*:** Inform a name for the profile to be registered. Ex.: *Domains Admins*;
- ***Available Administrators*:** List of uneven administrator users to be used in the profile. Click **[+]** to make an addition to Profile Administrators;
- ***Profile Administrators*:** Admin user belonging to the profile. Click **[−]** to remove the list from Profile Administrators. Ex.: blockbit.

Permissions

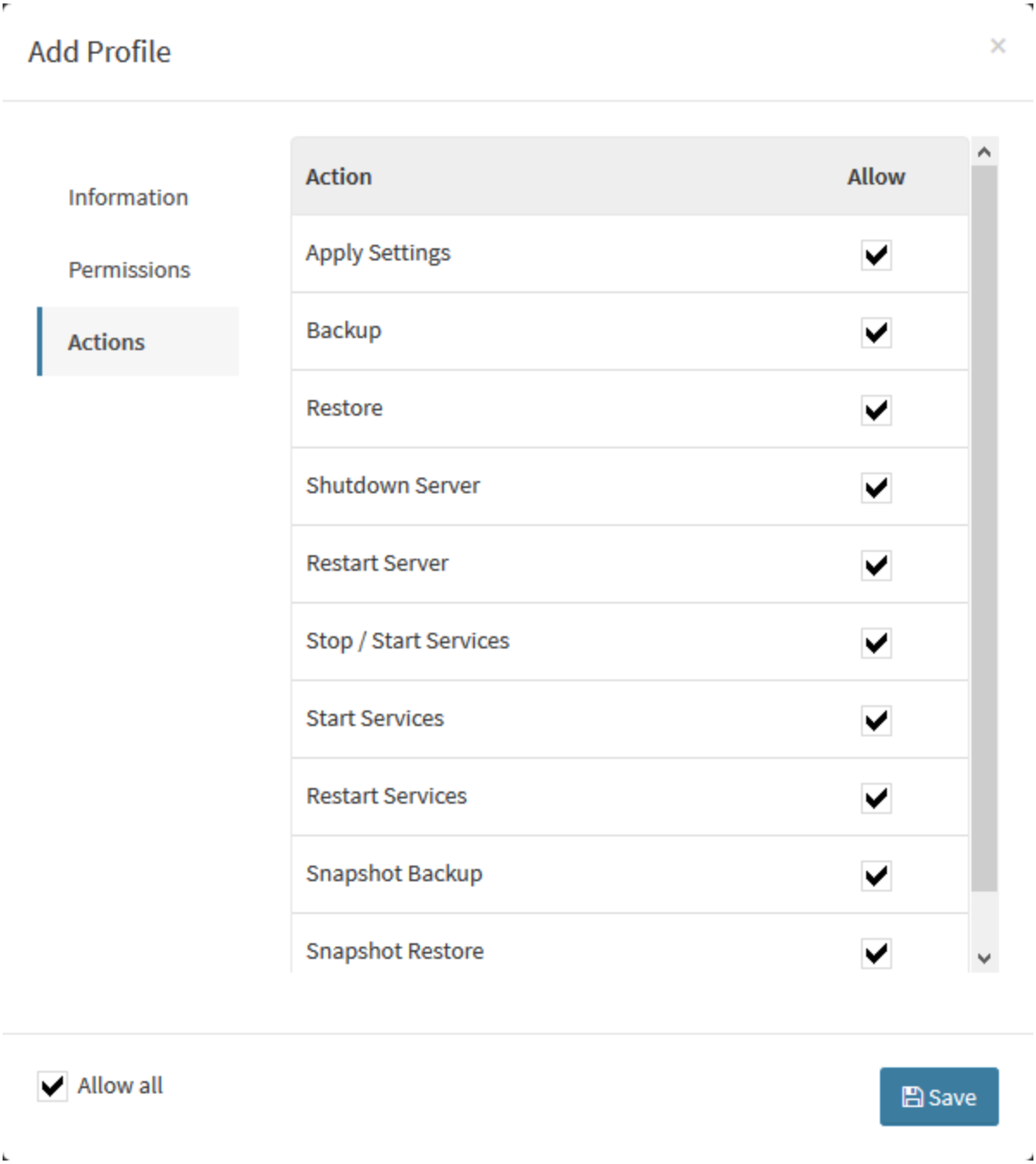
In the "Permissions" tab, the interfaces will be defined in which the profile can have access and the type of access, which can be of the type "View" and "Edit".



Administration - Add Profile - Permissions

Actions

In the "Actions" tab, it is possible to allow the administrator specific access to the system, as well as Apply Settings, Backup, Restore, Shutdown Server, Restart Server, Stop / Start Services, Start Services, Restart Services, Snapshot Backup and Snapshot Restore.

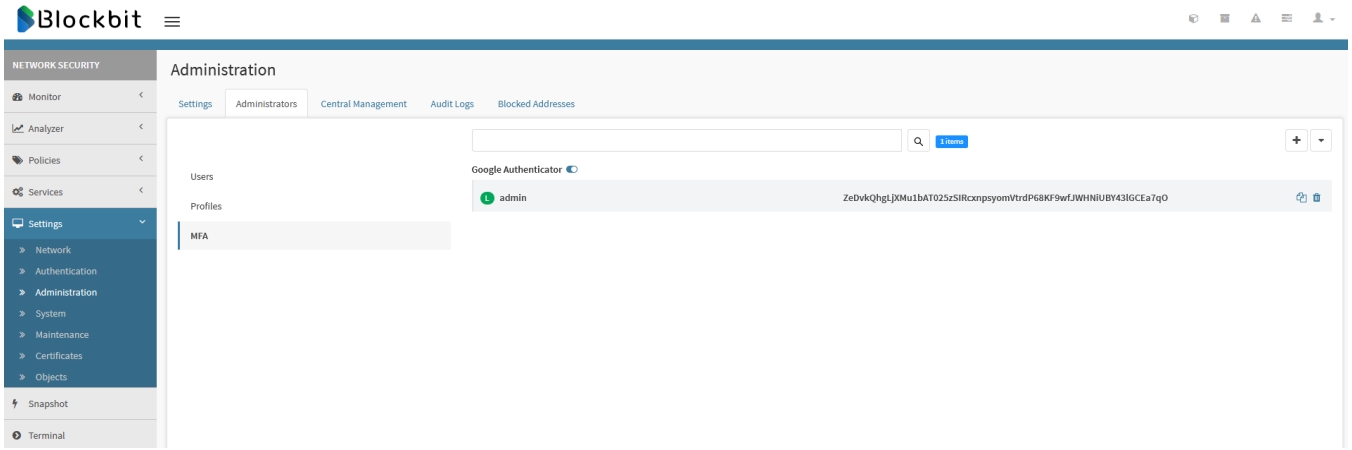


Administration - Add Profile - Actions

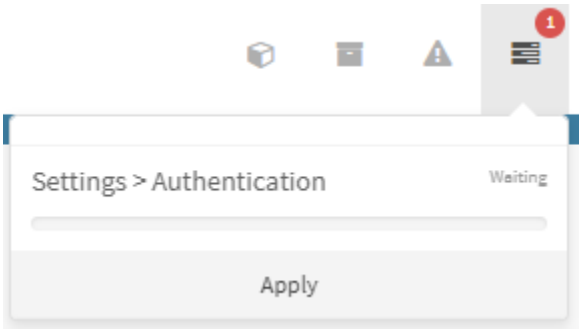
Then click [Save].

Administrators - MFA

The MFA (Multi-factor Authentication) option allows the generation of a unique key to be used with the Google Authenticator for administrator-type users validation by using an MFA token:



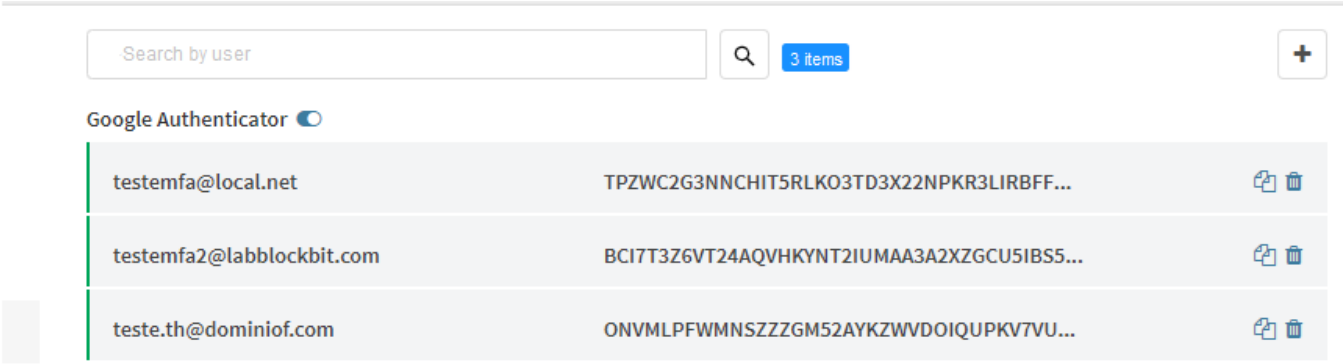
After having created a user in Administration Administrators Users, one must enable the MFA [Google Authenticator], and "apply the changes" since the functionality comes disabled by factory standards:



Settings Apply

After the activation of the service, a list with all the users will be displayed. By clicking on the "+" button, it will be possible to select a user and generate a key for this one:

Generate Validation Key

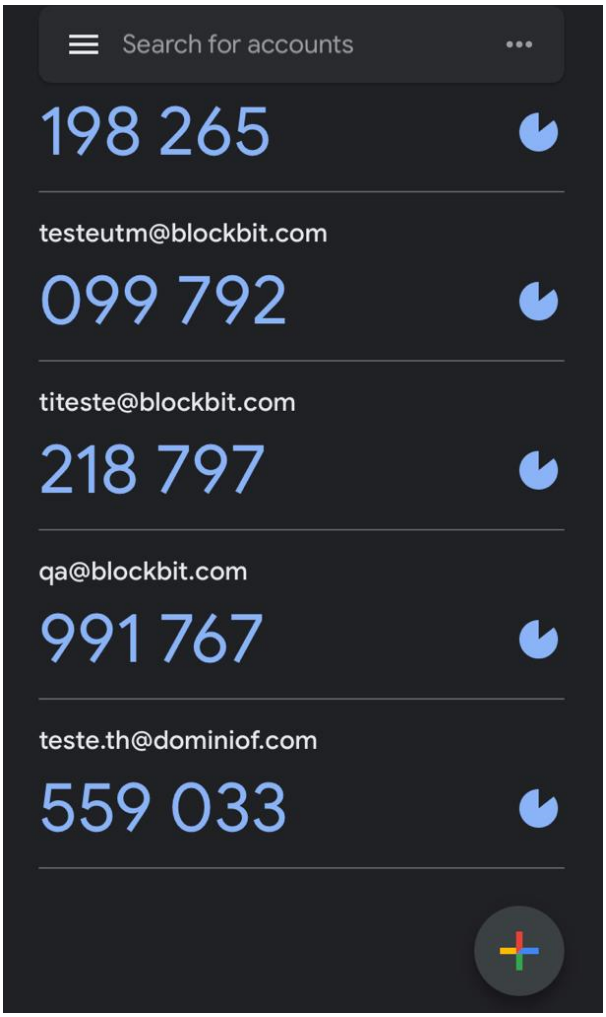


List of users with issued validation keys

The Copy [ ] and Delete [ ] buttons allow the copy or deletion of a key.

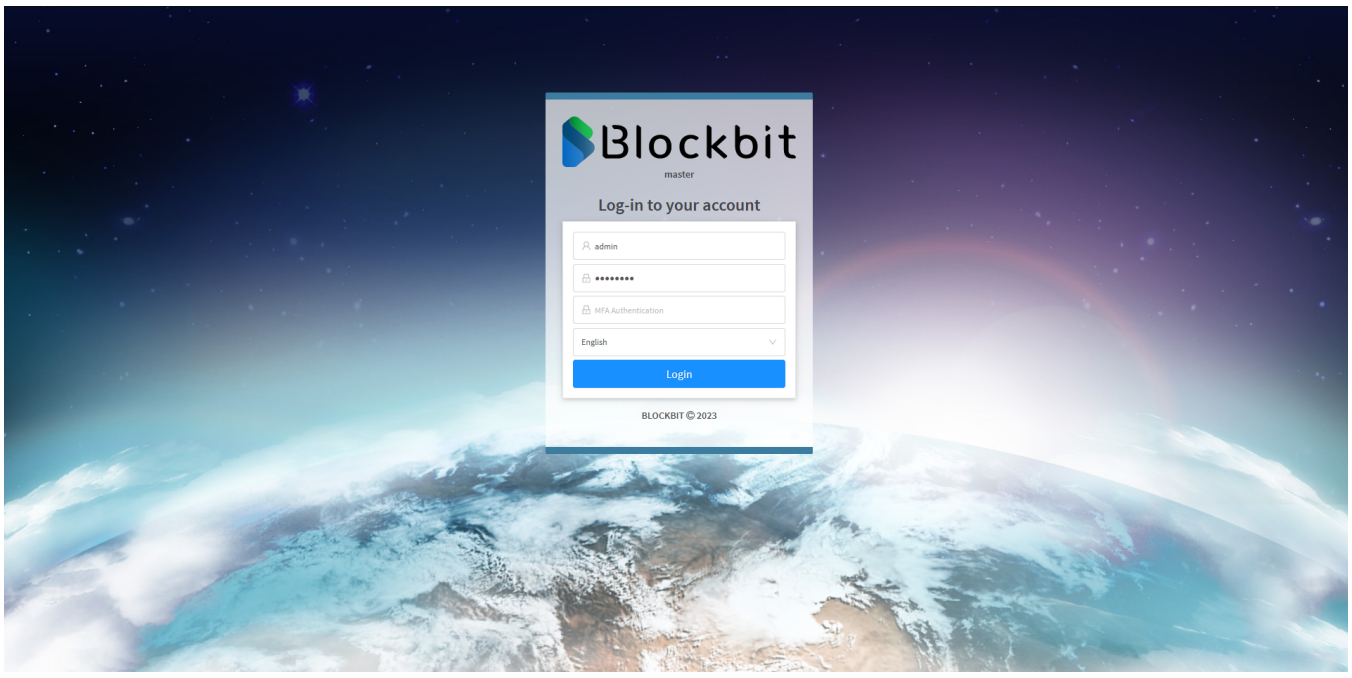
After having generated a validation key for a user it is necessary to have the Google Authenticator App in another device (a smartphone, or a laptop). On the App, click on the "+" option insert validation key and use the key obtained from the NGFW. Select the *"time-based"* key type.

By doing so, a six-digit validation token will be generated for the user.



Google Authenticator - Access Tokens

After obtaining the token, access the authentication portal, and log in:



Login Screen

- *User:* Insert the *Username*
- *Password:* In this field use the *Password* registered for this user.
- *MFA Token:* In this field the *MFA Token* obtained from the *Google Authenticator* App must be inserted.

After filling these field, click "Login".

About the *Tokens*:

The tokens are meant to be used only once. The user can use up to 3 tokens, (the current, the previous and the next ones) uppon the attempt to use another token, the user becomes invalid. In case the token is typed in wrongly thrice, the user becomes invalid for 30 seconds.

It's important to remember that the token is changed often, so when logging in, one must consult the token on the Google Authenticator App.

By doing so, the authentication will have been successfully done.

Administration - Central Management tab

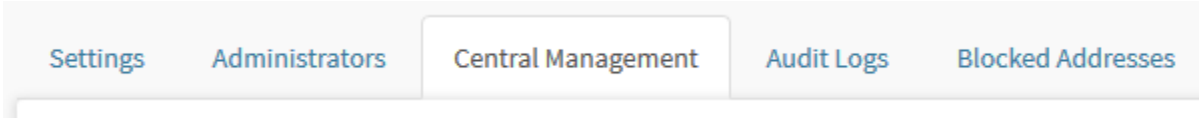
The global management feature is a platform integration tool, which aims to facilitate the process of managing multiple BLOCKBIT UTM Firewalls from a centralized management with BLOCKBIT GSM.

In this section you administrator has the option to enable integration with BLOCKBIT GSM that allows you to apply from system configurations to security policies, this is done through templates accessed remotely on your device, being securely integrated through the exchange of API deployment keys.

This integration also includes centralized management features of the dashboard, it also issues analytical reports (Logs) that provide complete visibility to the administrator regarding the monitoring of his network environment.

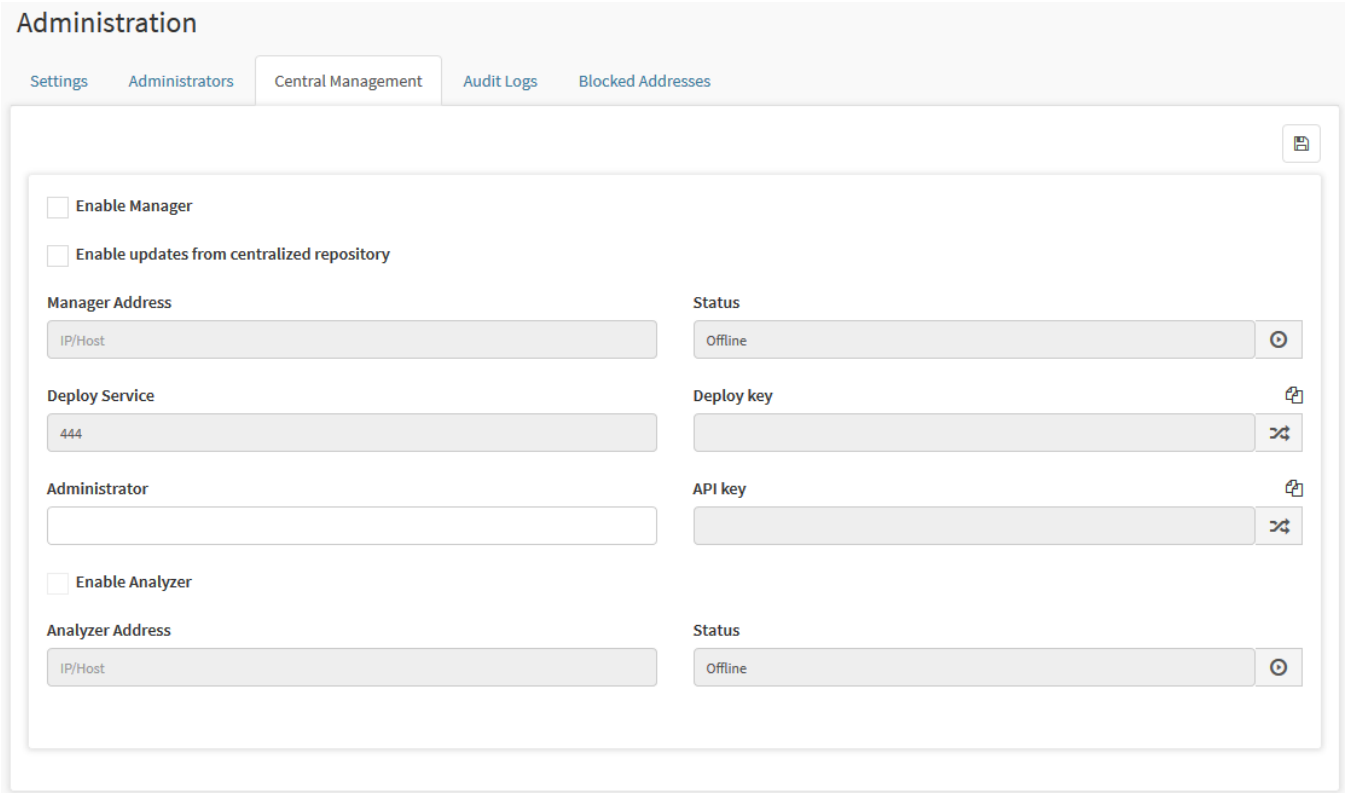
To enable this feature, it requires the prior installation of an Appliance for the BLOCKBIT GSM.

For access, click on the "Central Management" tab:



Central Management tab

The screen shown by the image below will appear:



Administration - Central Management

To facilitate the configuration process, here are the specifications of the configuration items of the integration with the BLOCKBIT GSM.

- ***Enable Manager [ ]:*** Check this checkbox for integration with the GSM for centralized configuration management services and security policy base;
- ***Enable updates from centralized repository [ ]:*** *Check this box to deploy the system update from the BLOCKBIT GSM integration for all BLOCKBIT UTM devices in the network branch managed by it*;

- **Manager Address:** Add the IP Address of the BB GSM that will be used as Manager Device. Ex.: 172.16.102.101;
- ***Status*:** The Default status is "offline". *To start the service, click the [ ] button and confirm the notification by clicking the [OK] button*;

Its default status "offline" is updated/changed to "online" after the configuration of the integration and the exchange of keys performed successfully. This procedure requires a copy of the deployment and API keys inserted and enabled in BB-GSM (see the GSM manual for the whole procedure).

- ***Deploy Service:*** *It refers to the communication port with the BLOCKBIT GSM Manager. Port [444/TCP]. Click generate [ ] key, then click copy [ ] key.*
- ***Deploy key:*** *This is the public key used as authentication for the deployment of "unpacking" template files from the configuration base and security policies distributed by the BB GSM to the BLOCKBIT UTM Firewall devices*. Click the generate **[ ]** key, then click copy **[ ]**.

This key must be copied and saved in the BLOCKBIT GSM settings (see the GSM manual for the procedure).

- ***Administrator:*** *Type and select from the list of administrators, the one with the right to deploy the BLOCKBIT GSM templates*.

This text box performs a search, so it is necessary to select the desired administrator from the list that will appear, it is NOT enough to just type the name of the administrator.

- ***API key:*** *This is the public key used as API authentication - "Application Programing Interface" - a set of routines and standards for accessing the BLOCKBIT GSM for receiving templates and accessing the "Loggers" base when enabled on the BLOCKBIT UTM device. Click generate [ ] key, then click copy [ ] key*;
- **Enable *Analyzer [ ]:*** *Check the checkbox for integration with the GSM Analyzer and consolidating all logs: "Traffic", "WEB Access", "Threats", "Attacks" and "Applications" on a single device with the advantage of a dedicated server for reporting management*;
- ***Analyzer Address:*** *Add the IP address of the Blockbit GSM device responsible for the Logger.* If its an "Integrated" Logger, it will be the same IP of *Manager Address field. Ex .: 172.16.102.101*;

  For more information, see the GSM manual chapter about Loggers.

- ***Status*:** "Default offline status". *To start the service, click the [ ] button to start the service and confirm the notification by clicking the [OK] button*;

Its default status "offline" is updated/changed to "online" after the configuration of the integration and the exchange of keys performed successfully.

This procedure requires a copy of the deployment and API keys inserted and enabled in the Blockbit GSM (see the GSM manual for the whole procedure).

To complete the configuration, click **[ ]**.

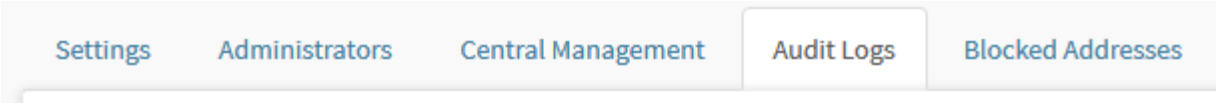
After applying the configuration, exchange keys for “Deploy” and “API”.

Administration - Audit Logs tab

This resource has the main purpose of "Auditing" all the operations carried out in the system, from "Visualization", "Configuration of a service". In addition, it is possible to access the "Settings" and or "Changes" of a compliance policy carried out by any of the system administrators, be it the "Super Administrator" or "Common Administrator".

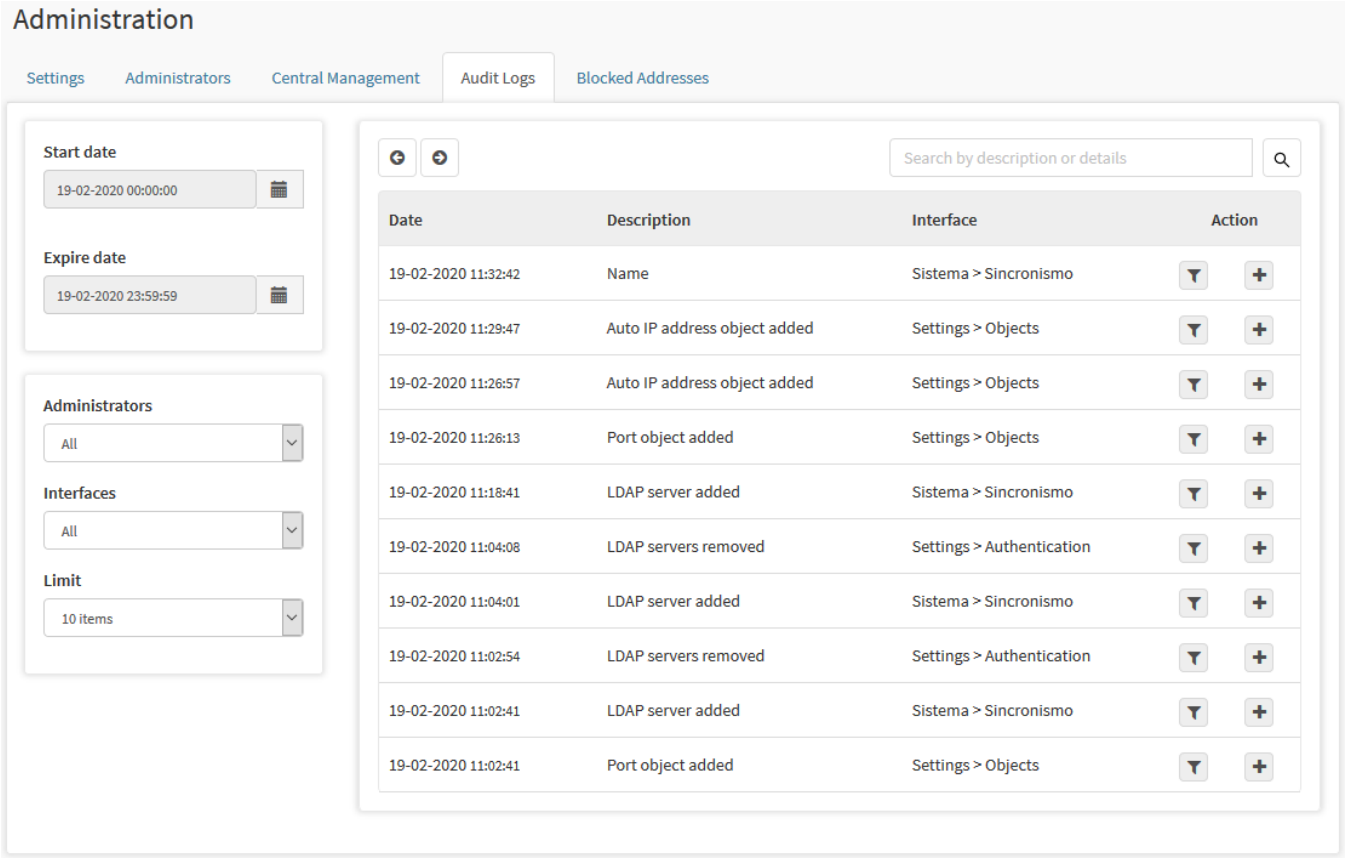
Through this panel it is possible to apply filters by: "Start / end date", "Administrators", "Interfaces" and also define the limit you want to display per page.

To access, click on the Audit Log Tab.



Audit Logs tab

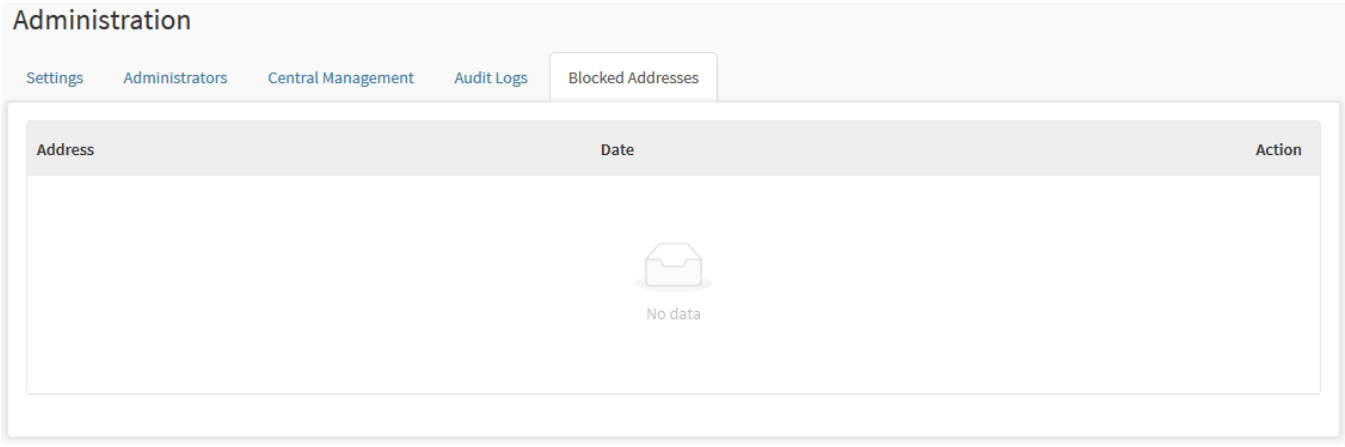
The screen shown by the image below will appear:



Administration - Audit Logs

Administration - Blocked Addresses tab

In the Blocked Addresses tab, you can view the list of IP/hosts blocked by attempted unauthorized access, and/or attempted persistent access, with the possibility of removing the blocking rule before the timeout established in the settings and policies for accessing the WEB management interface.

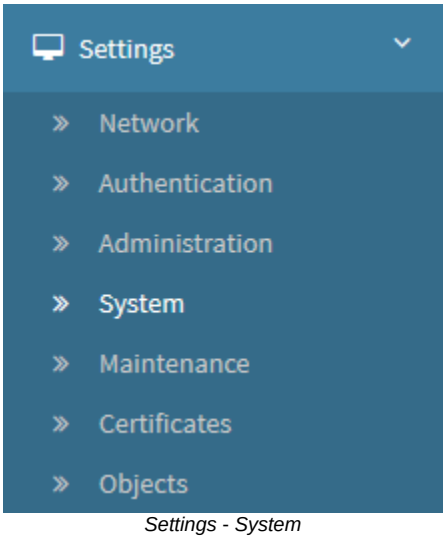


Administration - Blocked Addresses

UTM - Settings - System

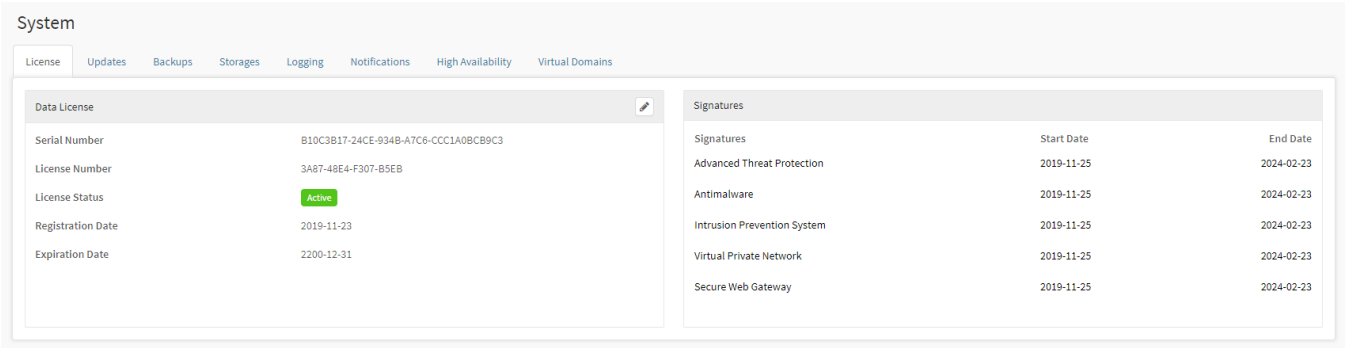
The “System” item allows us to: Manage access to the WEB administration interface, define and apply the general settings, manage the registration and permissions of the system administrators, audit the accesses and the applied settings, and also manage the blocking by attempts of unauthorized access.

To access this screen, simply select the “System” option.



Settings - System

The screen below will appear:



System - License

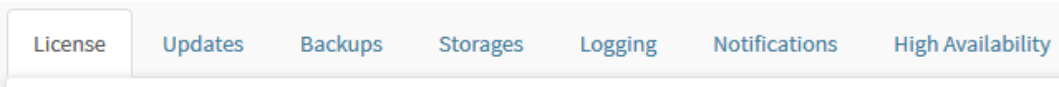
This screen consists of the following tabs:

- *License*;
- *Updates*;
- *Backups*;
- *Storages*;
- *Logging*;
- *Notifications*;
- *High Availability*;
- *Virtual Domains*.

System - License tab

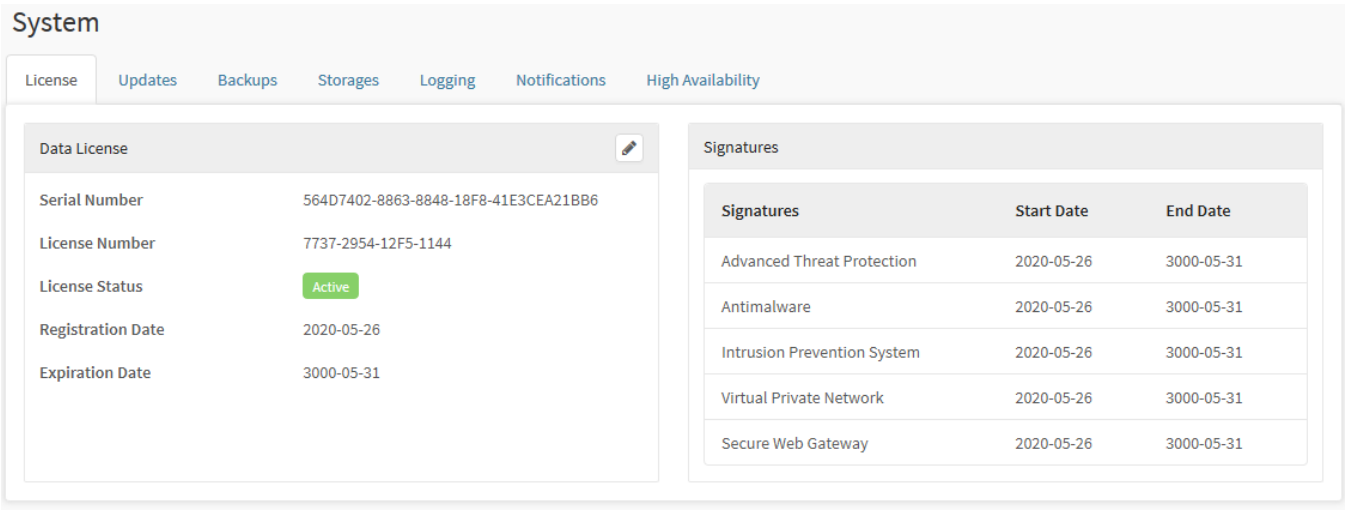
This interface is focused on displaying information about the license and subscription details.

If the tab is not selected, click on the "License" tab:



License tab

The screen will appear, as shown by the image below:



System - License

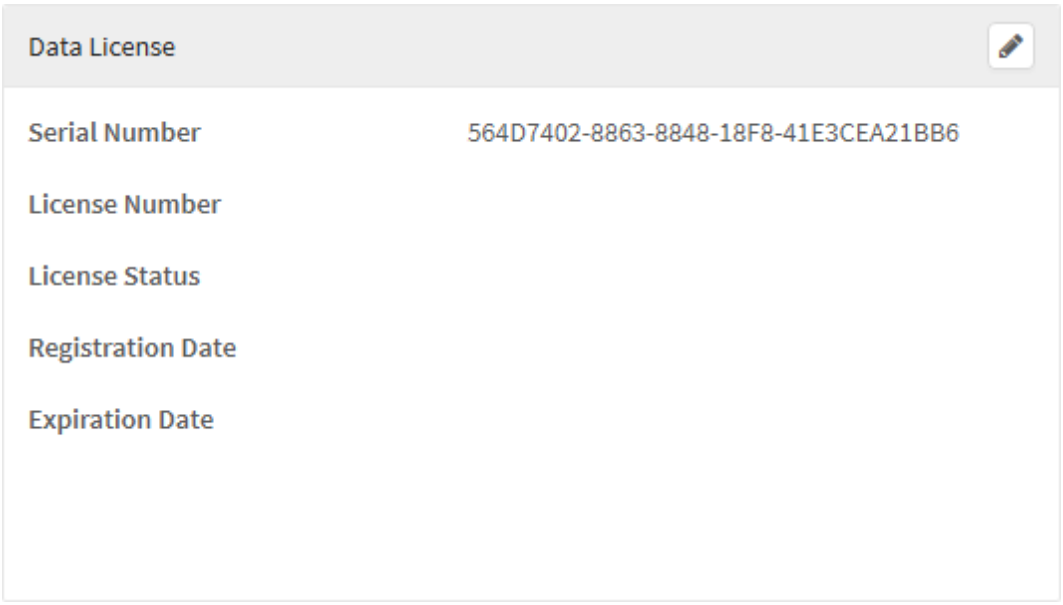
This panel consists of the panels:

- *Data License*;
- *Signatures*;

Next we will analyze each panel on this screen.

License - Data License

In the “Data License” widget, it is possible to view information regarding the license applied at the UTM, its serial number, license number, status, registration and expiration date. As shown on the screen below:



License - Data License

- ***Serial Number*:** Displays the serial number of the appliance. This data is used in the appliance's licensing process;
- ***License Number*:** *Displays the license number applied to the search appliance*;
- ***Registration date*:** Displays the date the license was registered in the system. Ex.: 2020-12-18;
- ***License expiration*:** Displays the system license expiration date: Ex.: 2021-01-31;
- ***Licensestatus*:** Displays the status of the license, active or inactive.

Below we will see how to make the UTM licensing.

How to activate license

In order to use BLOCKBIT UTM resources, it is necessary to license your installation, follow the steps below:

In order to license Blockbit Network Security, it is necessary to be connected to the internet with HTTPS access to the following addresses:

https://license.blockbit.com

https://update.blockbit.com

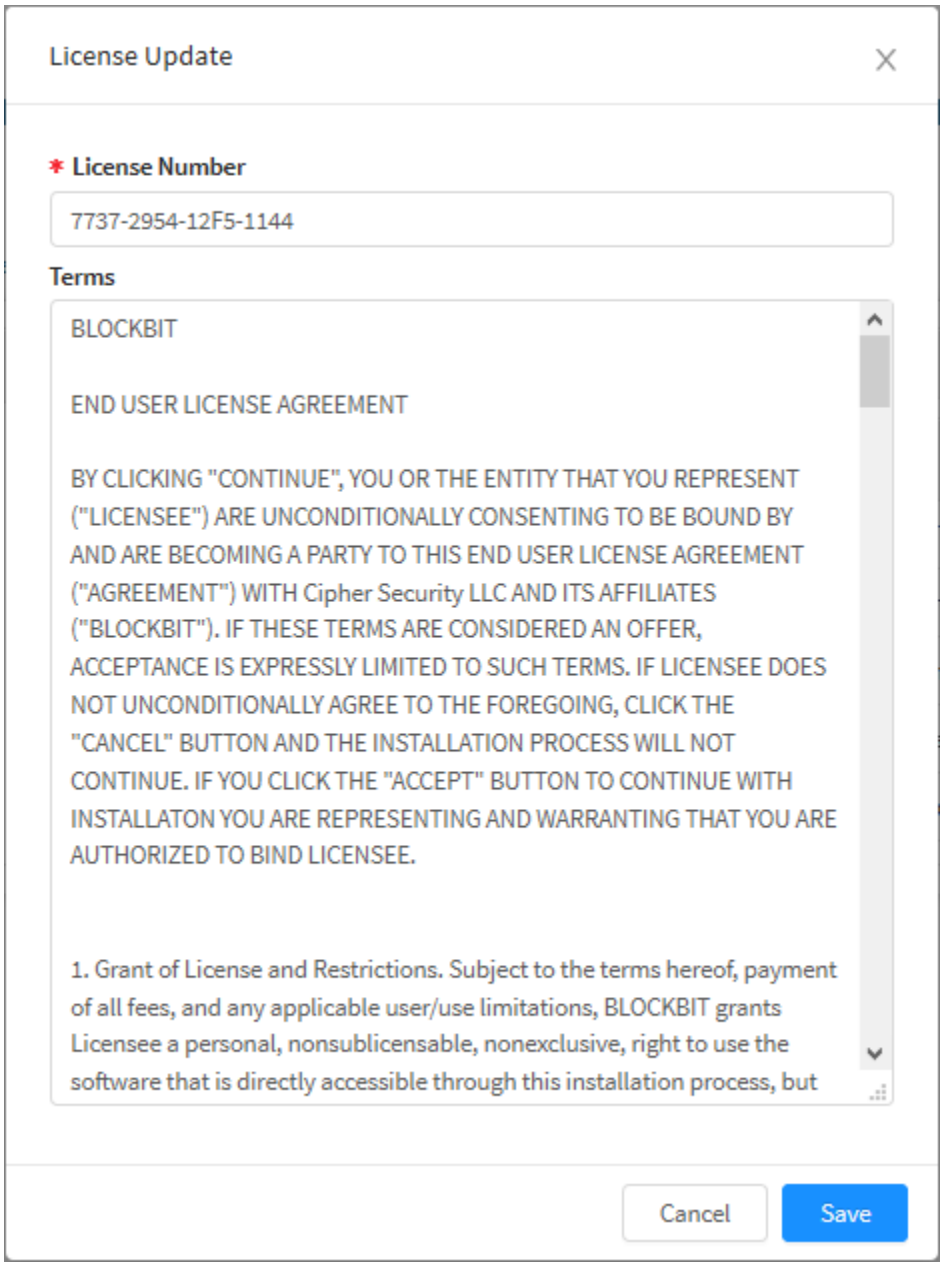
To apply or renew the activation license it is necessary to provide the **“Serial number”** also known as **UUID** (Universal Unique Indicator of your Blockbit UTM).

- The License widget will inform the Serial number, characterized by having five character blocks. Ex: B10C3B17-47ED-FD44-A5FE-6598E0D180A4. Copy and forward it to your service channel, which will provide you with the license number;
- You will receive the License number code, from your service channel, characterized by having four character blocks. Ex.: 6992-BA7B-2A1B-6749.

Enter the license key provided. Remember, the device being configured must be properly connected to the Internet for the system to validate the license.

Click **[**  **]**, enter the license data and click **[** 

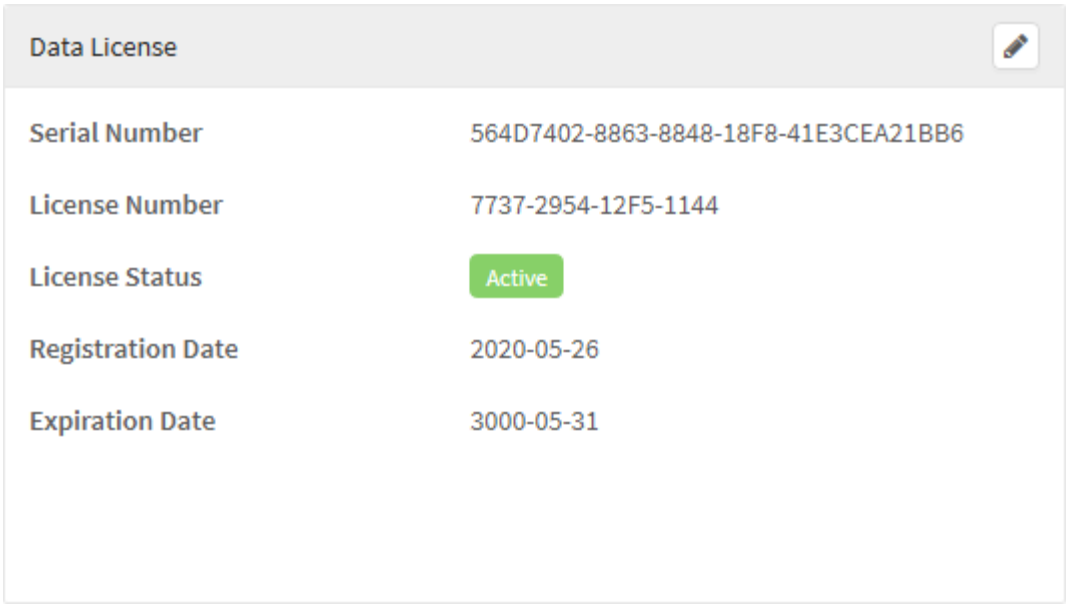
].



Update License

After saving the license, the request is sent to the **command queue [**  **]** where it can be executed to be applied in the system. For more information on the command queue access the page: UTM - COMMAND QUEUE.

After clicking "Apply" the system will update the security feeds, apply the patch patches and finally, make the settings regarding the product licensing. When finished, the following screen will be displayed:



License - License Information

This completes the licensing process for your product.

License - Signatures

In the “Signatures” widget, you can view the bases installed in the system and their respective start and end dates of the contract as shown on the screen below:

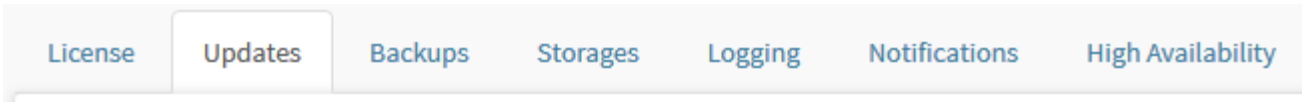
Signatures	Start date	Expire date
Advanced Threat Protection	2020-01-09	3000-01-14
Antimalware	2020-01-09	3000-01-14
Intrusion Prevention System	2020-01-09	3000-01-14
Secure Web Gateway	2020-01-09	3000-01-14
Virtual Private Network	2020-01-09	3000-01-14

License - Signatures

System - Updates tab

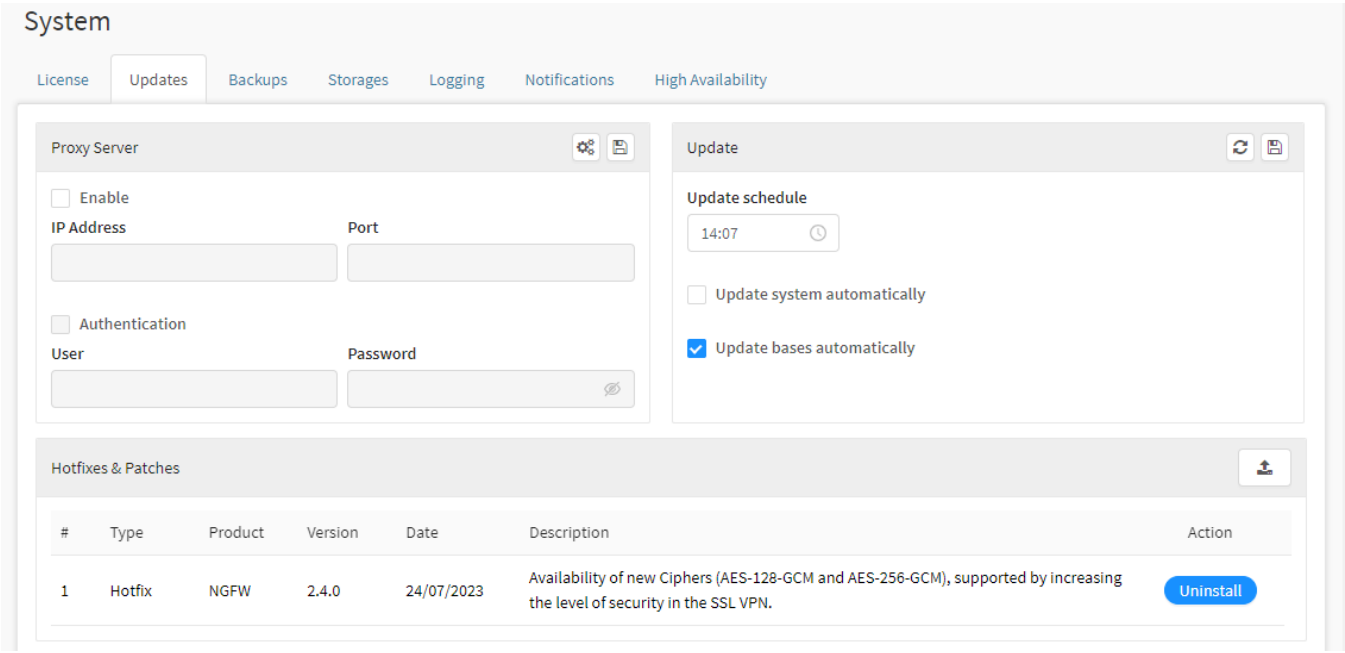
This interface allows the configuration of the proxy server and the scheduling of updates.

If the tab is not selected, click on the "Updates" tab:



Updates tab

The screen will appear, as shown on the image below:



System - Updates

The update of the signatures' base (IPS, WEB FILTER, APPLICATION CONTROL and ATP) are automaticaly done, without the necessity of rebooting the Blockbit Appliance or the management modules.

This screen consists of the panels:

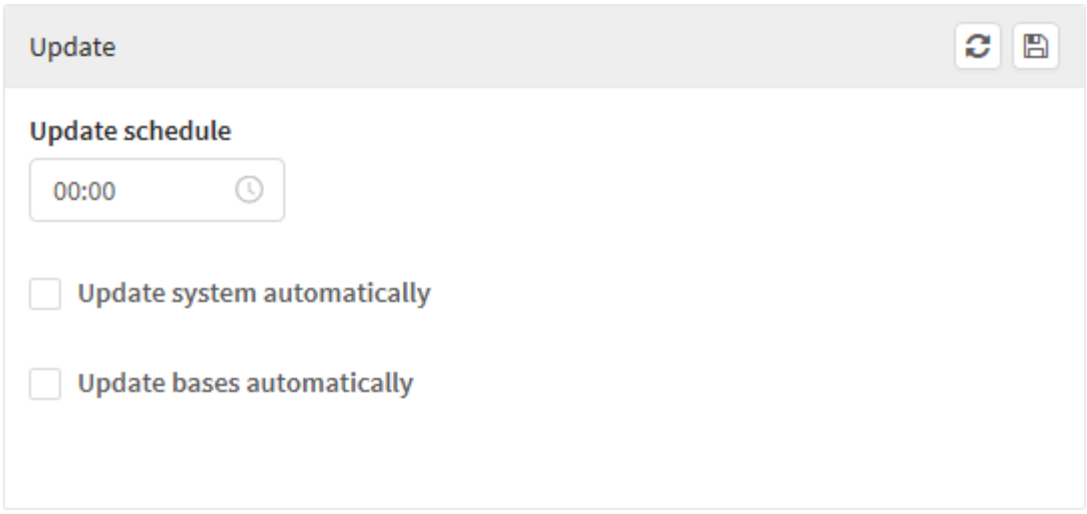
- *Proxy Server*;
- *Update*.

Next we will analyze each panel on this screen.

Updates - Update

In the Update Schedule widget it is possible to determine when the system will perform an automatic update.

Below we will analyze in detail the Update Schedule widget:



Updates – Update schedule

- **Update schedule:** In this checkbox it is possible to determine the time of the update. Ex.: 09:00;
- **Update system automatically[ ]:** If this checkbox is enabled, the system will perform a complete update (system update, bug fixes and new features) at the time specified in the option above. *It is the equivalent of running "update-system -s" on the CLI*. It is recommended to leave this option disabled. Ex.: Disabled;
- **Update bases automatically[ ]:** If this check box is enabled, the system will update the subscription base and security feeds at the specified time. It is recommended to leave this option enabled. It is the equivalent of running "update-system -b" on the CLI. Ex.: Enabled.

Following the regulations of ITIL, ISO 27.001 and ISO 27.002, it is recommended to keep automatic update disabled so that the user has control over the update operation of his system.

At the top right of the screen, we have two options:

- ***Update* [ ]:** By clicking on this option, the manual update will be performed immediately (it is also possible to perform the update through the CLI, for this purpose, access this link), the security feeds, system modules, patch patches and new features will be updated.;
- ***Save* [ ]**: This button has the function of saving the settings of this panel;

After saving, for the changes to take effect it will be necessary to access the **command queue [ ]**, when clicking on **[Apply]** the operation will be started.

It is recommended that no settings be changed on the system during the process of downloading and applying updates.

It's important to remind that the system will disable the automatic updates in case the High-Availability settings have been set up, due to the compatibility with the other nodes' settings (secondary device).

Updates - Hotfixes & Patches

The Hotfixes and Patches update mode, present on the NGFW's update module, allows the use of seasonally released packages by Blockbit for upgrading the system or correcting punctual problems in previously released functionalities. These packages replace the previous ones, allowing the improvement of a specific service without the necessity of releasing a new product version to solve minor problems.

Hotfix

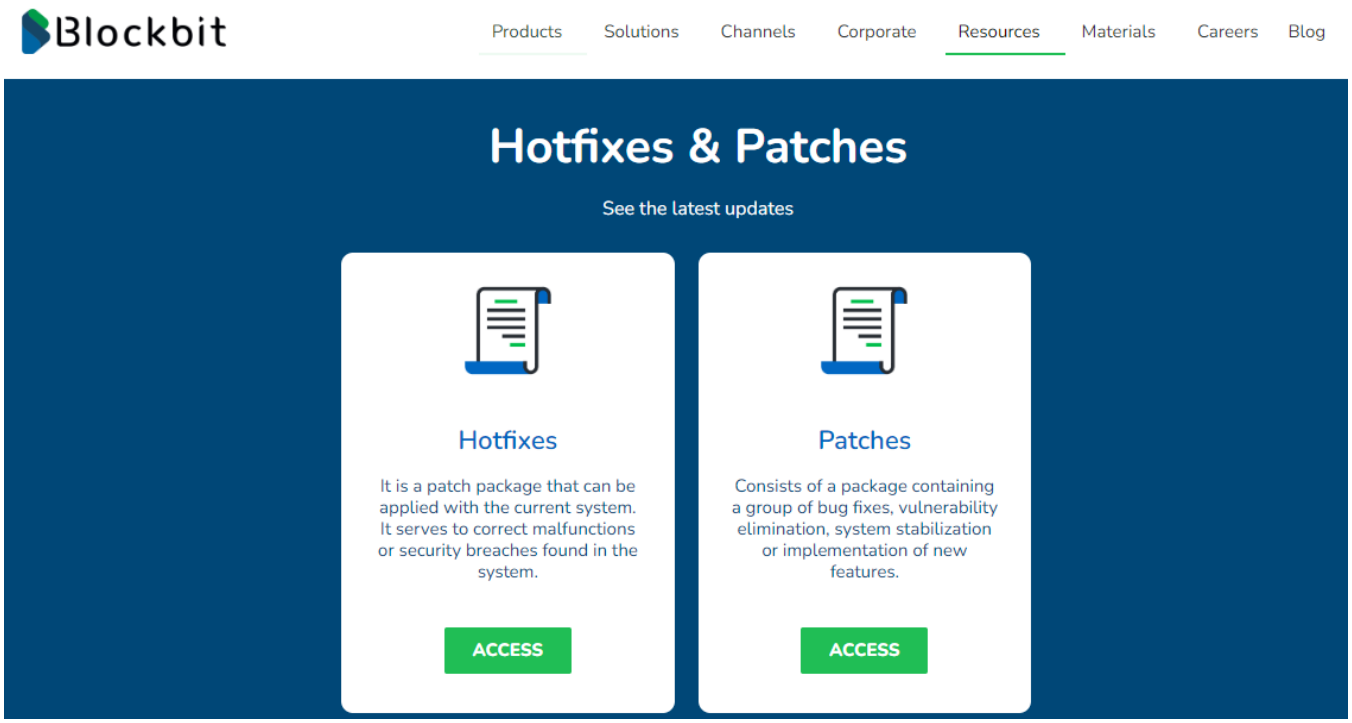
It is a correction/upgrade package that can be applied while the system is in course. It can correct flaws in course or security breaches found on the system that might require immediate action, or install implementations.

Patch

It is a larger package containing a group of Hotfixes. It can be used to correct a specific bug, eliminate vulnerabilities, stabilize the system or implement a new functionality.

How to install

To install a Hotfix or Patch, access https://www.blockbit.com/pt/resources/ and download the update package to be installed. Scroll down 'till the "Hotfixes & Patches" section appears on screen:



Hotfixes and Patches Download page - Blockbit website Resources

Páginas /... / Updates - Hotfixes & Patches

Hotfixes

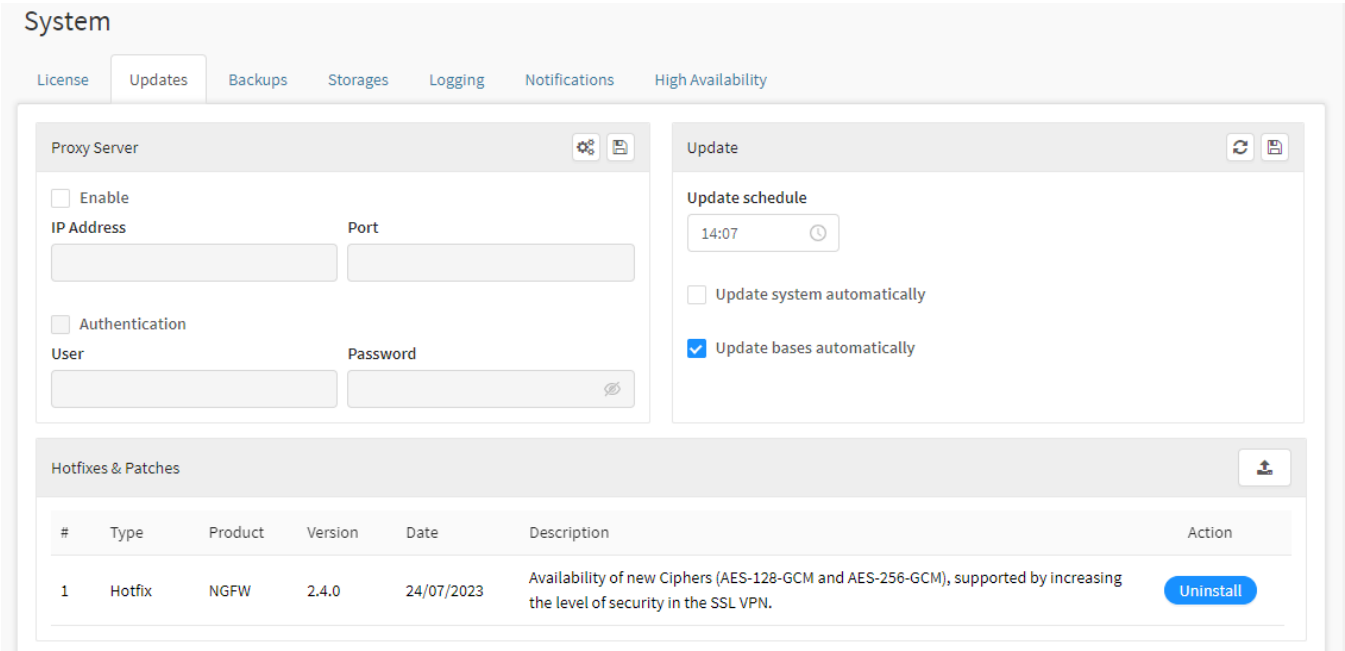
In this section are available the Hotfixes for the 2.4.0 version of the NGFW:

ID	Release Date	Description	CHECKSUM (MD5)	Download
#1	26/04/2023	New ciphers made available (AES-128-GCM e AES-256-GCM), increasing the security level of the SSL VPN.	cb3043d713831eb9016920ec620ea38a	2.4.0.1
#2	02/05/2023	The validation done on the DHCP return screen when deleting an interface has been exchanged.	aa46bf232f3ec55102bcd8c366420818	2.4.0.2
#3	11/08/2023	Correction done in the Logs generation service.	ebf136a38132e499d3b544fb5f420a29	2.4.0.3
#4	15/05/2023	Cluster update package.	baf61fdff084fdf81b355354f051b86b	2.4.0.4
#5	17/05/2023	Correction done in the Port Forwarding, it wasn't allowing the creation of a new forwarding rule.	6438320a1549649a0f4116f881c6eb70	2.4.0.5
#6	25/05/2023	Correction done in the arp sheet reading method. The cache sheet wasn't being updated correctly.	bb6d7f06e7f0efdcce487cbc7bb772f2	2.4.0.6
#7	06/06/2023	Correction done in the authentication of concurrent sessions by user.	bf3d71edbc9518305c3809d8a465cc55	2.4.0.7

Hotfixes

The process is the same to download and install a patches package, just click on Patch to be redirected to the page containing the updates, and by doing so download the update package required (soon there will be more details about the patches to be posted).

Then, access Settings System Updates:



NGFW Updates Page

The screen above shows a list of the installed *Hotfixes* and *Patches*. To upload the file that will be used, click on the upload button [ ] and apply the update (*Hotfix or Patch*) required:

Upload option

After selecting the file that will be installed, click install and it will be loaded. The system will automatically verify its signature and cryptography, then will apply its properties.

It's important to notice that the *NGFW* can receive upgrades throught the installation of Hotfixes and Patches even without being licenced.

The next pages contain the Hotfixes and Patches released so far .

Hotfixes 2.4.1

In this section are available all the NGFW's Hotfixes.

- Hotfixes for the 2.4.1 version:

ID	Release Date	Description	CHECKSUM (MD5)	Version
#3	20/10/2023	The use of single or double quotes has been blocked on the password validation fields.	3bceaa6d5956ceec607ef0b76f3dcac6	2.4.1.3
#5	20/10/2023	Adds a correction for critical Ishell vulnerability in the CLI.	201271f756e4abe7951341afa49849c0	2.4.1.5
#8	20/10/2023	Network mask saving in the ipset by the SDWAN service has been corrected.	5838d5e33c2e79ab10b33289b4915f7d	2.4.1.8
#9	20/10/2023	Correction done in the period selection field when searching for reports from the Analyzer Monitor.	39ff211761b1b5a065b73e8370df8d27	2.4.1.9
#10	17/01/2024	Correction done to listing PPP network interfaces for DNAT rules.	8f0537aa9d12f6e3dbfca2902a73ba39	2.4.1.10
#11	19/01/2024	Update that allows the use of Heartbeat LAG interface in Cluster. *Important: It's mandatory to disable the Cluster to install this Hotfix.*	9f01bf1571a9a1d942c058409f1b68e9	2.4.1.11
#12	14/02/2024	Control over repeated requests to reset PPPoE connection's IP has been implemented.	fdacf135145c53c3d8ba3409d1754b96	2.4.1.12
#13	09/02/2024	Correction done in the validation of network masks of route-based VPN TUN interfaces.	09b324ccfe5a91ec280845e878f07e70	2.4.1.13
#14	24/04/2024	Modification in the adsl-start for service aiming for improvements on the PPPoE tunnels establishment.	6a151ceb7c9eaf08d4d7644deaf39e4b	2.4.1.14
#15	24/01/2024	Improvement done in the display of information on the password field, in Settings System Notifications via E-mail.	d89a36b2d905153d7e3a8583f1965563	2.4.1.15
#17	11/12/2023	Improvement done in the security of access to the system's upgrade feature.	5208bae46d11387a4e4e63f538ec7ec9	2.4.1.17
#18	09/02/2024	Improvements and updates for the SNMP service's MIBs.	3ec3e05fd19740e9c85f8c3be1df30fa	2.4.1.18
#19	29/02/2024	Permission to register local and remote networks when opting for route-based tunneling in VPN IPSec service configuration.	a7535ad2188ea559a3c9bd4d30346b3f	2.4.1.19
#20	13/12/2023	Correction done in the editing and saving of MAC objects.	aa98135f6c9823582bc5968a3d80b37f	2.4.1.20
#21	16/02/2024	Correction done in the events' filtering by "sessid", in Security Events.	99b06025af5a6840b5b9d0a98673603b	2.4.1.21
#22	04/12/2023	Correction done in the creation of IPv4 and IPv6 Policies' forms.	c718e328669963de1e5c520843dec0ff	2.4.1.22
#23	04/03/2024	Improvement done in the sync of dynamic routes between cluster nodes. *Notice: It is mandatory to disable the Cluster in order to install this Hotfix.*	2a02bd7e4629bfa1e263cca257c43142	2.4.1.23
#24	01/12/2023	Improvement done in the Portal's logo settings.	e4def25a305c9b6756b7c7facf0cf21d	2.4.1.24
#25	15/01/2024	Improvement done in the backup data storage in the database, in Cluster mode. *Notice: It is mandatory to disable the Cluster in order to install this Hotfix.*	2e5610c42ea3ccdd5512c4235ff4b015	2.4.1.25
#26	14/12/2023	Correction done in the DNAT rules, now working properly with the use of scheduling.	13bfd5376cff9621aaf9fa62ea28754c	2.4.1.26
#27	27/12/2023	Correction done in the VPN IPSec service notifications.	a13e9d758c576ac351f4da3b25318adb	2.4.1.27
#28	25/04/2024	Security upgrade for some of the graphical Interface's components.	5a05ff287c3b4eb5076ee780bf5c075c	2.4.1.28
#29	01/12/2023	Correction done in the download analysis and block processes by the Threat Protection.	ae34cc7731c7ca45855b85f85143e6a9	2.4.1.29
#31	06/03/2024	Implementation of enhancements to the System Status screen user interface and the CLI, aimed at improving visibility and monitoring of the status of the High Availability Cluster service.	073af01cb620b6ca807132dfea1020f6	2.4.1.31
#30	28/12/2023	Correction done in the DNAT rule with two or more source interfaces.	c1180904146deb081f21fc60a2c47408	2.4.1.30
#32	18/01/2024	Network driver for the boards with the i225 chipset from Intel (IGC).	4dc2eaa32e23025c729158cebba1315f	2.4.1.32

		Important: If the new driver is required for your hardware, after installing or uninstalling your NGFW will reboot.		
#33	09/02/2024	Improvement done to blocking the super admin user removal.	97009ce84c66488860df25f64b83c75f	2.4.1.33
#34	23/01/2024	Improvement done in the functioning of the system Backup - Now, and Scheduled.	eb21bd94b17daa31a423d36ca399cbfe	2.4.1.34
#35	28/12/2023	Correction done in the super administrator status display.	5472ce4540b3f212060f3f81288f152b	2.4.1.35
#36	05/01/2024	Security correction done in the Threat Protection service. *Notice: It is mandatory have internet access to install or uninstall this Hotfix.*	f02407124454a71f0ff3d417d78f7a79	2.4.1.36
#37	08/05/2024	Correction and reintegration of network interfaces previously deleted from SD-WAN configuration profiles.	5ea4596fe46696cf91614568c87cf8f4	2.4.1.37
#39	21/12/2023	Improvement done in the functioning of the IPv4 interfaces on the DHCP relay service.	20a0a7a6b378b6b517423d095156cca3	2.4.1.39
#40	07/02/2024	Correction done on the display of the DHCP's settings.	878dcd746adf372800750548a41df80f	2.4.1.40
#41	05/02/2024	Improvement done in the route creation and DNAT (Port Forwarding) rule using the SD-WAN service.	732ee0faa81aefd3ff81aa44ce7f8707	2.4.1.41
#42	07/05/2024	NGFW 2.4.1 Patch 1 - Packages with new resources and corrections: 3, 5, 8, 9, 12-15, 17-22, 24, 26-29, 33 e 39.	83b51d0b0a3681e07e56e4ca37638def	2.4.1.42
#44	02/05/2024	Corrections of virtual office configurations.	8d89e5c013d071ce2238b28a7efbf452	2.4.1.44
#45	13/03/2024	Correction done in the size of snapshot file during save and download.	710a84f0211f9ec077cb2959a7600200	2.4.1.45
#46	TBA	Corrections of faults in hotfix application on GSM	TBA	2.4.1.46 TBA!
#47	TBA	Corrections of SNMP V3 configurations.	TBA	2.4.1.47 TBA!
#48	TBA	TBA	TBA	2.4.1.48 TBA!
#49	TBA	Correction of error where DHCP services doesn´t upload on backup.	TBA	2.4.1.49 TBA!
#50	TBA	Correction of proxy error on explicit mode.	TBA	2.4.1.50 TBA!
#51	13/03/2024	Correction done in the use of LAG interface as a VIP in High Availability configurations. *Notice: It is mandatory have internet access to install or uninstall this Hotfix.*	65cfde7f2f0bfe1d55bb78dee0bfd580	2.4.1.51
#52	22/03/2024	Correction in the CSV Report Filters - Log Session.	77e1c64df11cd583c392dae5bcf614a1	2.4.1.52
#54	22/03/2024	Registers the 'crypto-optimization' command to enable/disable cryptography modules.	8cb2e26a8bf86be25f4eb893262dd497	2.4.1.54
#55	22/03/2024	Adjustment to the maximum number of IGMP multicast groups.	27a0ac8920eba0d9247cbbd36f7f10d2	2.4.1.55
#58	27/03/2024	Improvements in the management of static/dynamic IRQ services.	3c7534eff917c7a752d6d85c73b25ac7	2.4.1.58
#60	22/03/2024	Correction in the configuration field of IPSec VPN for Remote Access. *Notice: The VPN-IPSEC service will restart after applying this hotfix.*	243d5bcda95d160aef3604fd3ddc002d	2.4.1.60
#61	22/03/2024	Correction implemented in the 'DPD Close Action' field on the IPSEC Site-to-Site VPN screen.	ab85b424942830912fcb5591b27b7662	2.4.1.61
#62	03/04/2024	Optimization of authenticated session synchronization between the Headquarters and its branches.	3a36555aedb9525fd2df763b01858ba1	2.4.1.62
#63	22/04/2024	Optimization of Subscriptions viewing in the license management interface.	1d13f4b68f3510905992e1e3ff6ca39e	2.4.1.63
#64	09/04/2024	Optimization in the validation of RSA keys for IPSEC Site-to-Site VPN.	158883a07a6c9668341037426e1a44f1	2.4.1.64
#65	06/05/2024	Patch package related to DNAT/Port Forwarding functionality including, in addition to new fixes, the content of Hotfixes with IDs 43, 56, and 57: • Addition of functionality and correction of Port Forwarding between local network domains (HF 43), • Correction in the construction of Port Forwarding rules with IPS (HF 56) • Correction in source IP address and authentication conditions for Port Forwarding rules (HF 57) • Correction in the removal and deactivation operations of Port Forwarding rules	791aa0a19a4ce03a02a9a8e41d08744c	2.4.1.65

		• Correction in the persistence of authenticated sessions after executing the fwreload command • Correction in the assembly flow of Port Forwarding rules.		
#66	22/04/2024	Improvement in system notification management with Windows Authentication Servers.	e55874b72a46942bc29db19f8ffd059c	2.4.1.66
#67	22/04/2024	Improvement in DHCP utilization in IPSec VPN configuration for remote access.	bb439cd18262e1b4aa10e69d4b2a41f3	2.4.1.67
#68	TBA	Correction of user synchronization issues.	TBA	2.4.1.68 TBA!
#69	22/04/2024	Optimization of the functionality of Site-to-Site IPSec VPN menus when accessed via GSM.	b3b2652f46a68ca91327428268e0cf56	2.4.1.69
#70	TBA	TBA	TBA	2.4.1.70 TBA!
#71	28/05/2024	Correction of SDWAN issue.	0e192310049519274a98ad5c0662d28b	2.4.1.71
#72	23/05/2024	Correction of issue where non cathegorized URLs weren't being sent to the Lab.	6be04afe39aaa90e7158e87482a07eeb	
#73	08/05/2024	Adjust the DSL Interface configuration linked to the Physical Interface configured as a DHCP Server.	786e05434ba103bb96d39faccda4ce27	2.4.1.73
#74	TBA	TBA	TBA	2.4.1.74 TBA!
#75	TBA	Correction of High Avaliability Cluster issue.	TBA	2.4.1.75 TBA!
#76	23/05/2024	Correction of errors where PPPOE TCPMSS rules were being scripted for wrong devices and other DSL update rules.	b7314dcc468ab2d6b4d41d9a1e04e2f3	2.4.1.76
#77	08/05/2024	Improved policy maintenance after creating/editing network interfaces.	e8d9306784cc8fe99eddd990b1ba344e	2.4.1.77
#78	TBA	Correction of error that allowed objects with the character ".".	TBA	2.4.1.78 TBA!
#79	08/05/2024	Correction in the DSL interface form, allowing the password field to be changed.	f8195f56732e7476d0a0673abc423406	2.4.1.79
#80	TBA	Correction of file removal issue.	TBA	2.4.1.80 TBA!
#91	17/06/2024	Corrects error where TACACS configurations weren't being applied.		2.4.1.91
#92	14/10/2024	Allow update to Blockbit Platform 2.4.2	cf24e13adb660121dfbdab511973a260	2.4.1.92

ID	Release Date	Description	CHECKSUM (MD5)	Download
#1	26/04/2023	New ciphers made available (AES-128-GCM e AES-256-GCM), increasing the security level of the SSL VPN.	cb3043d713831eb9016920ec620ea38a	2.4.0.1
#2	02/05/2023	The validation done on the DHCP return screen when deleting an interface has been exchanged.	aa46bf232f3ec55102bcd8c366420818	2.4.0.2
#3	11/08/2023	Correction done in the Logs generation service.	ebf136a38132e499d3b544fb5f420a29	2.4.0.3
#4	15/05/2023	Cluster update package.	baf61fdff084fdf81b355354f051b86b	2.4.0.4
#5	17/05/2023	Correction done in the Port Forwarding, it wasn't allowing the creation of a new forwarding rule.	6438320a1549649a0f4116f881c6eb70	2.4.0.5
#6	25/05/2023	Correction done in the arp sheet reading method. The cache sheet wasn't being updated correctly.	bb6d7f06e7f0efdcce487cbc7bb772f2	2.4.0.6
#7	06/06/2023	Correction done in the authentication of concurrent sessions by user.	bf3d71edbc9518305c3809d8a465cc55	2.4.0.7
#8	12/06/2023	Solves a few exception treatments in the Proxy service's connections.	9fcf75fa90444ad2e517519d8541be21	2.4.0.8
#9	16/06/2023	Proxy-SSH's installation.	19a3f569a13e998cf5cff8e17ae22c7d	2.4.0.9
#10	22/06/2023	Improvement in the custom categories matching performance of profiles in Web Filter.	ebe288313f58756e1ff9e446eb5b39cb	2.4.0.10

#11	15/08/2023	Correction of the Port Forwarding rules when a non-valid IP is being used.	1364f7edcc53dd577a23dba10fff4c5f	2.4.0.11
#12	15/08/2023	DHCP relay update package.	e4b9d9b2d195f8e84f33b2100b9ffcd8	2.4.0.12
#13	21/07/2023	Removal of the tap interface in the network settings, due to the NG VPN.	e6a176e0cc759338df781fa792f464e0	2.4.0.13
#14	21/07/2023	Adjustment of the receiving and updates in the deploy of policies of the GSM.	337e9f0d04e4ad2fdaecde0dd7f843ad7	2.4.0.14
#15	14/08/2023	Admin commands to enable/disable some of the kernel's modules. Enable: TFTP, FTP, PPTP, H323; Disable: TFTP, FTP, PPTP, H323.	1407d578d41900d01bb76760010290dd	2.4.0.15
#16	26/07/2023	Creation of a command to restore the Mac Address of the network Interfaces, after restoring the snapshot of a different machine.	b3e3e2d4ec40d6b9ed00d96e19a93a5f	2.4.0.16
#17	23/08/2023	Correction done in the period that can be selected when searching for reports on Analyzer Monitor.	754e2a7b8b10e54f8b613e05a9583b83	2.4.0.17
#19	08/05/2024	The "DPD Close Action" option has been included on the advanced options of the IPSEC VPN tunnels's options.	8f4177b1d583e09a143b4bb4ac039fef	2.4.0.19
#20	28/08/2023	Correction on the remote certificate importation.	7f5419f930a473ff9c9cd2f0a1ef0c2f	2.4.0.20
#22	13/09/2023	Correction done in the DHCP relay in multiple interfaces/VLANs.	584293367e4b340ade07012bf9455c4d	2.4.0.22
#24	20/09/2023	Adds a critical vulnerability correction for the ishell.	2287919d16f7f08c5104ba9a25a0124f	2.4.0.24
#28	24/10/2023	Modification in the adsl-start for service aiming for improvements on the PPPoE tunnels establishment.	eb0fcea8e13d696ead539273dedae9d8	2.4.0.28
#29	14/02/2024	Control over repeated requests to reset PPPoE connection's IP has been implemented.	7611d3b08c4f5a860819b9abd9f07102	2.4.0.29
#30	30/11/2023	Improvement done in the applicantion of default route via VLAN interface after system boot.	e4e94e96cce59d5d54f20a0fa65d3cf4	2.4.0.30
#31	09/02/2024	Improvements and updates for the SNMP service's MIBs.	2b59b4f3ba5bfe9626c9d687856ef3a9	2.4.0.31
#32	17/11/2023	Network driver for the boards with the i225 chipset from Intel (IGC). ***Important: If the new driver is required for your hardware after installing or uninstalling, your NGFW will reboot.***	f6ddca764b21f88310c02cd51594b543	2.4.0.32
#33	11/12/2023	Improvement done in the security of access to the system's upgrades feature.	e88f3d85fc4f8a4074a924f7454f4141	2.4.0.33
#34	27/02/2024	Correction done in the filtering of events by "sessid", in Security Events.	34b339ad20d45976dcff34fa131a3f07	2.4.0.34
#36	04/12/2023	Correction done in the creation of IPv4 and IPv6 Policies' forms.	a7f8bbc3f4251a41393b23e8d41ee10d	2.4.0.36
#37	06/12/2023	Improvement done in the Portal's logo settings.	a62584a34ec459657785d99a47f9ad99	2.4.0.37
#38	14/12/2023	Correction done in the DNAT rules, now working properly with the use of scheduling.	9a9d924eafad87bdd9503d3c549ca1ad	2.4.0.38
#39	08/12/2023	Security upgrade for some of the graphical Interface's components.	ef7088270b0e8a7858c579bdba81b305	2.4.0.39
#40	27/12/2023	Correction done in the VPN IPSec service notifications.	31e77bd975c0d88f8d88870b2563df22	2.4.0.40
#42	01/12/2023	Correction done in the download analysis and block processes by the Threat Protection.	036ecc62c03b475b9703d66c9ef9f70c	2.4.0.42
#43	27/02/2024	Correction done in the DNAT rule with two or more source interfaces.	297efb9db5359c0b213265d575cd8d51	2.4.0.43
#44	28/12/2023	Improvement done to blocking the super admin user removal.	b8b120db8473268288d6bffcb61d1be3	2.4.0.44
#47	22/04/2024	Optimization in the validation of RSA keys for IPSEC Site-to-Site VPN.	d8d3288b12aedaf5d7ead7dfab90c57e	2.4.0.47 New!

Next, we will analyze the *Patches*

Hotfixes and Plugins

In this section are available all the NGFW's Hotfixes.

- Hotfixes for the 2.4.2 version:

ID	Release Date	Type	Description	CHECKSUM (MD5)	Version
#1	09/12/2024	Hotfix	Adjustments to Global Management with High Availability Cluster. *Note: It is necessary to disable the Cluster to perform the installation.*	6701070f64d361f3599cb61d72e91aaa	2.4.2.1
#2	16/12/2024	Plugin	Blockbit AI installation plugin with three modules: **Consult** for quick queries, **Assist** for task automation, and **Analyze** for data analysis. *Note: This installation will take approximately 5 minutes and it needs to reload the administration page.*	1d06f0dd50eec20537990de579222698	2.4.2.2 Beta!

For more information about updating to version 2.4.2, visit the page.

Next, we will analyze the *Patches*

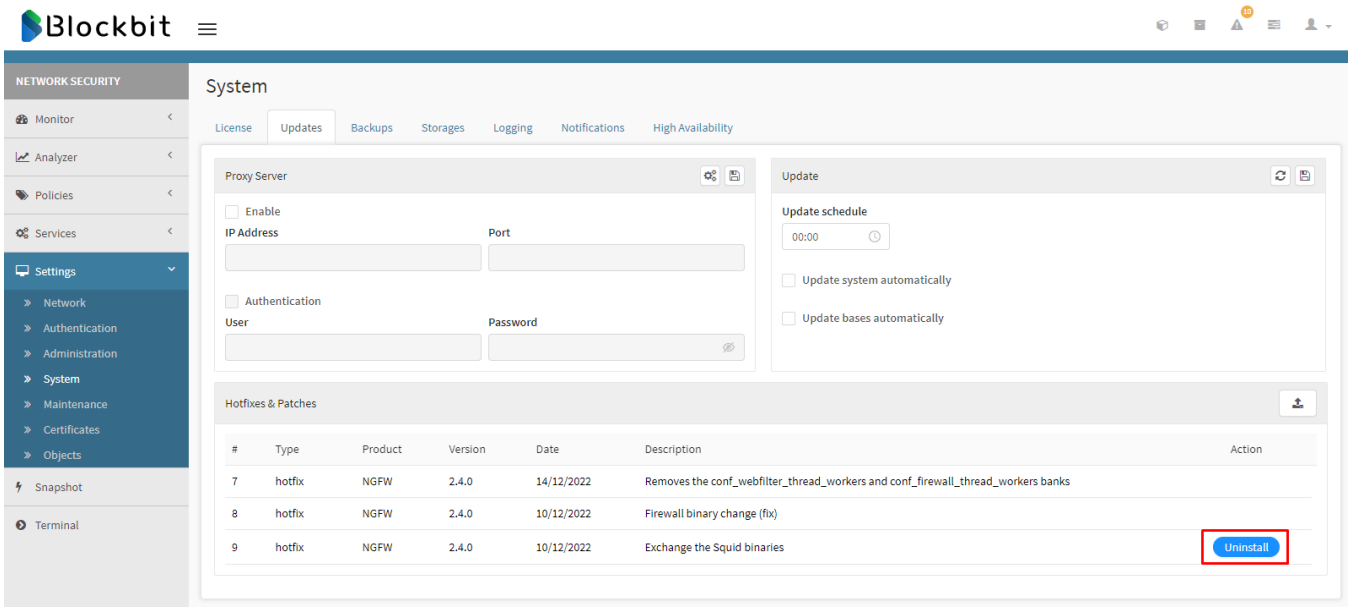
Rollback

This option allows a hotfix or patch to be uninstalled, restoring the pre-update package.

To uninstal a hotfix or patch, follow the next steps:

- Access the updates menu (settings system updates) and click the *"Uninstall"* button to perform the Rollback.
- A list containing the currently installed updates will be displayed and the system will calculate the requirements for the Rollback, as for example, the necessity of an even previous one to be deleted.

On the case bellow, we have Hotfixes 7, 8 and 9 applied to the system, and Hotfix 8 will be deleted, however this process may require the deletion of hotfix 9. In this case, the system will inform if such action is mandatory or not. Note:



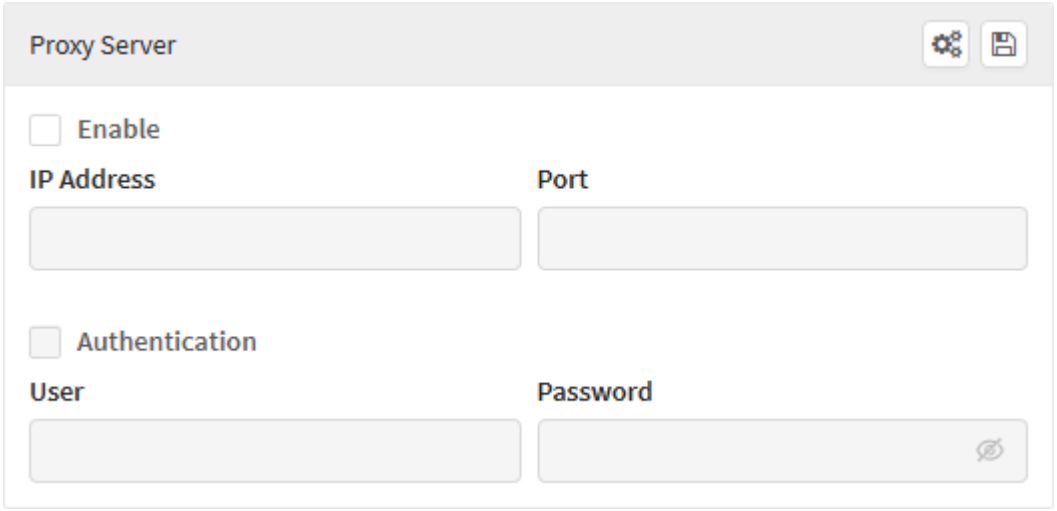
Updates - Rollback

To run the Rollback, select the package to be deleted and after the system is done calculating this action's requirements, click on the *"Uninstall"* button. The steps informed by the system will be followed and the reverting process for the previous state, completed.

Updates - Proxy Server

In Proxy Server it is possible to program a proxy to perform Updates without having to have internet in the UTM.

Below we will analyze in detail this panel:



Updates – Proxy Server

- ***Enable*** **[ ]:** If this checkbox is enabled, it activates updates via proxy, and you need to complete the text boxes below:
  - ***IP Address*****:** Enter the IP of the proxy. Ex: 10.0.0.1;
  - ***Port*****:** The proxy port. Ex.: 75;
- ***Authentication*****[ ]:** If it is necessary to have a user to access the proxy, check this checkbox and enter the username and password in the text boxes below:
  - ***User*****:** The user required to access the proxy;
  - ***Password*****:** The password required to access the proxy user.

To test connectivity with the proxy, click the **[ ]** button at the top right of the screen, to save your settings, click the **[ ]** button;

After saving, for the changes to take effect it will be necessary to access the command queue **[ ]** and apply the changes made. For more information on the command queue access the page: UTM - Command Queue.

After performing these procedures, the proxy server will have been successfully configured.

System - Backups tab

The System Backup option generates a complete "image" of the system, which includes from the "Operating System", the "configuration database" and the "dashboard statistics data", ensuring a complete copy of the system, way it is also guaranteed its restoration in a much faster and more efficient way.

The Snapshot option is a faster and more compact way to save the settings.

Follows the particularities of Backup and Snapshot:

Snapshot Features

Snapshot dumps the UTM database and services configuration files:

- *Operating system service configuration files:*
  - Network;
  - Services;
  - Database;
  - Proxy;
  - And others.
- *UTM services configuration files;*
- *Database configuration files;*
- *Antimalware quarantine.*

The snapshot does not include specific files that would cause problems to restore on a new installation or on another machine.

Backup Features

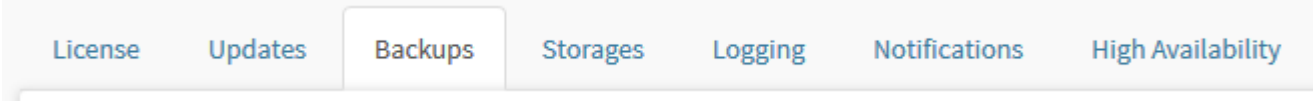
Backup includes just about everything in a system image:

- *All UTM settings;*
- *The license;*
- *Network configuration (including Mac Address).*

The backup only does not include temporary files or some directories and files that cannot be restored to another installation because of disk protection.

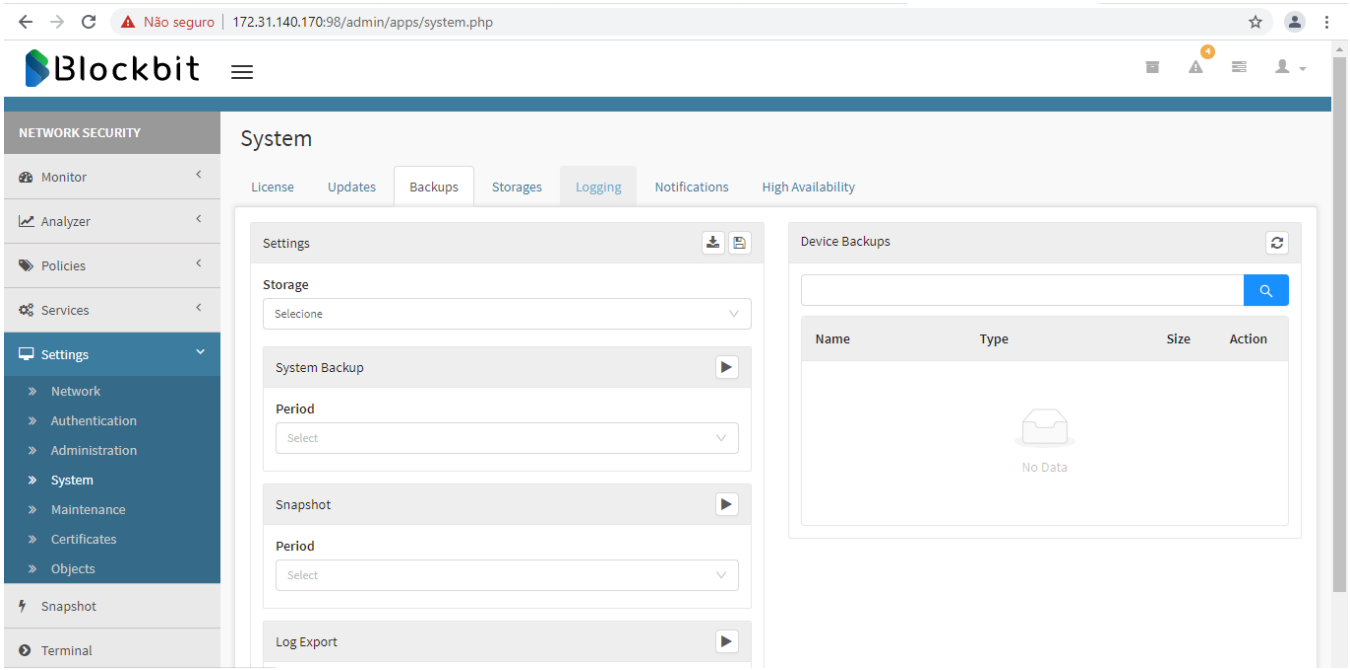
Before configuring the backup service, you need to configure the *Storage service.*

To access the backup management interface, click on the "Backups" tab.



Backups Tab

The screen will appear, as shown by the image below:



System - Backups

This screen consists of the panels:

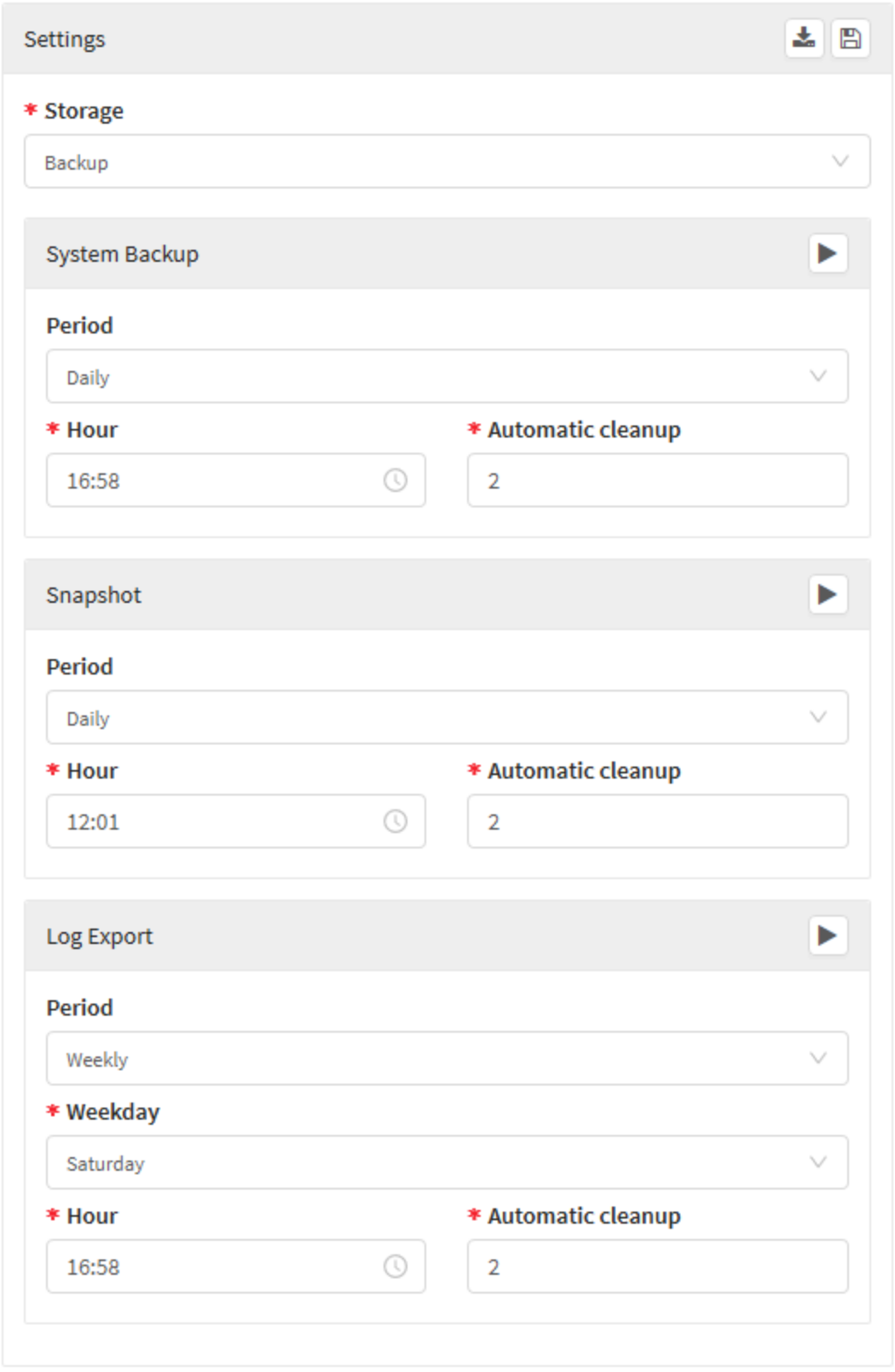
- *Settings*;
- *Device Backups*.

Next, we'll look at each panel in detail.

Backups - Settings

In this panel you configure the backup service and define the storage location among the storage options "NFS", "SSH" or "Disk", previously registered in *Storages*.

The system makes it possible to perform the following actions: system backup, snapshot and log export.



Backups - Settings

SETTINGS

- ***Storage*:** Defines the location where the backups will be stored. Ex.: *Backup*;

SYSTEM BACKUP

- ***Period*:** Defines the period that the system backup will be performed:

    - ***Daily:*** Performed daily;
    - ***Weekly:*** Performed weekly.
- ***Hour*****:** *Defines the time to be backed up*. Ex.: 12:01;
- ***Automatic cleanup*****:** *Defines the number of backups to be stored on storage*. Ex.: 2.

SNAPSHOT

- ***Period*****:** Defines the period that the system backup will be performed:
    - ***Daily:*** Performed daily;
    - ***Weekly:*** Performed weekly.
- ***Hour*****:** *Defines the time to be backed up*. Ex.: 12:01;
- ***Automatic cleanup*****:** *Defines the number of snapshot backups to be stored on storage*. Ex.: 2.

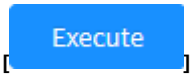
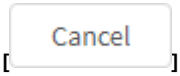
LOG EXPORT

- ***Period*****:** Defines the period that the log export will be performed:
    - ***Daily:*** Performed daily;
    - ***Weekly:*** Performed weekly.
- ***Hour*****:** *Defines the time to be backed up*. Ex.: 12:01;
- ***Automatic cleanup*****:** *Defines the number of log backups to be stored on storage*. Ex.: 2

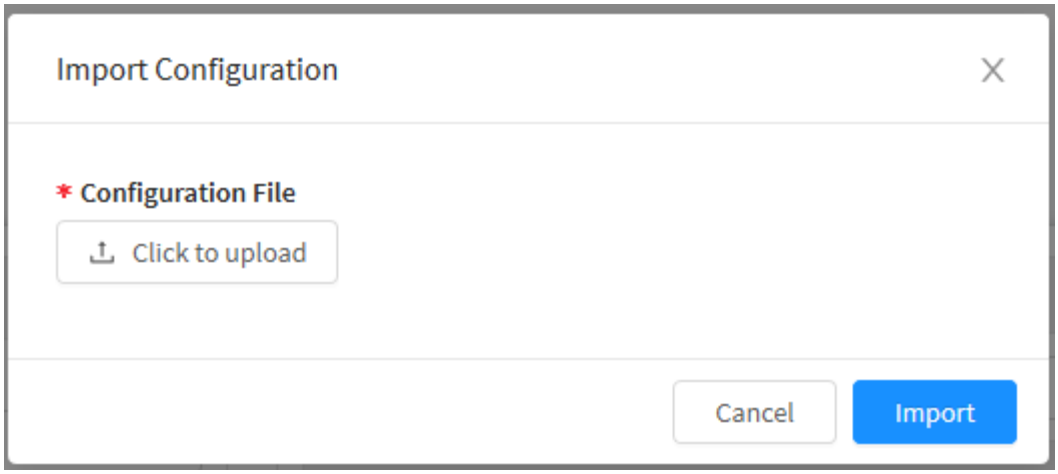
You can still perform a backup immediately by clicking the buttons **[**  **]**.

The following message will be displayed:

Backup execution confirmation message

Click on **[**  **]** to perform the backup or on **[**  **]** to close that window.

In addition, it is also possible to migrate settings from legacy versions by clicking the **[**  **]** button, the following window will be displayed:



Import Configuration

Click the [Click to upload] button to add the desired file.

For more information on how to use this feature, see How to: Import and Export UTM 1.5 to UTM 2.0.

Click on [Import] to import the configuration or on [Cancel] to close that window.

Finally, for the settings to be made, it will be necessary to access the **command queue [ ]** and apply the settings. For more information on the command queue access the page: UTM - Command queue.

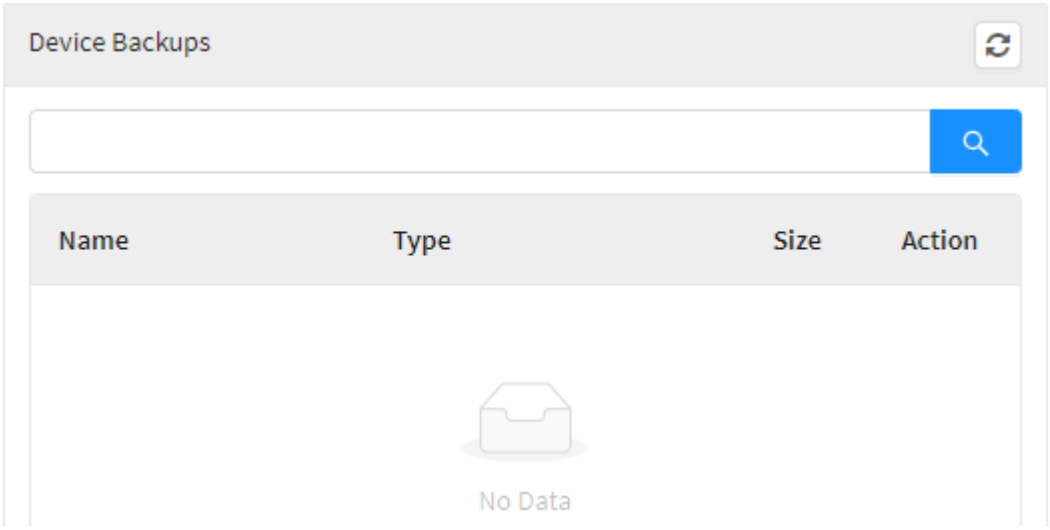
The Backup is generated in encrypted mode, so to be restored in the event of a possible reinstallation of the system, it is necessary to use the same integrity key as the previous installation located in *Settings - Administration - Sessions* in Integrity.

After performing these procedures, the policy will have been successfully configured.

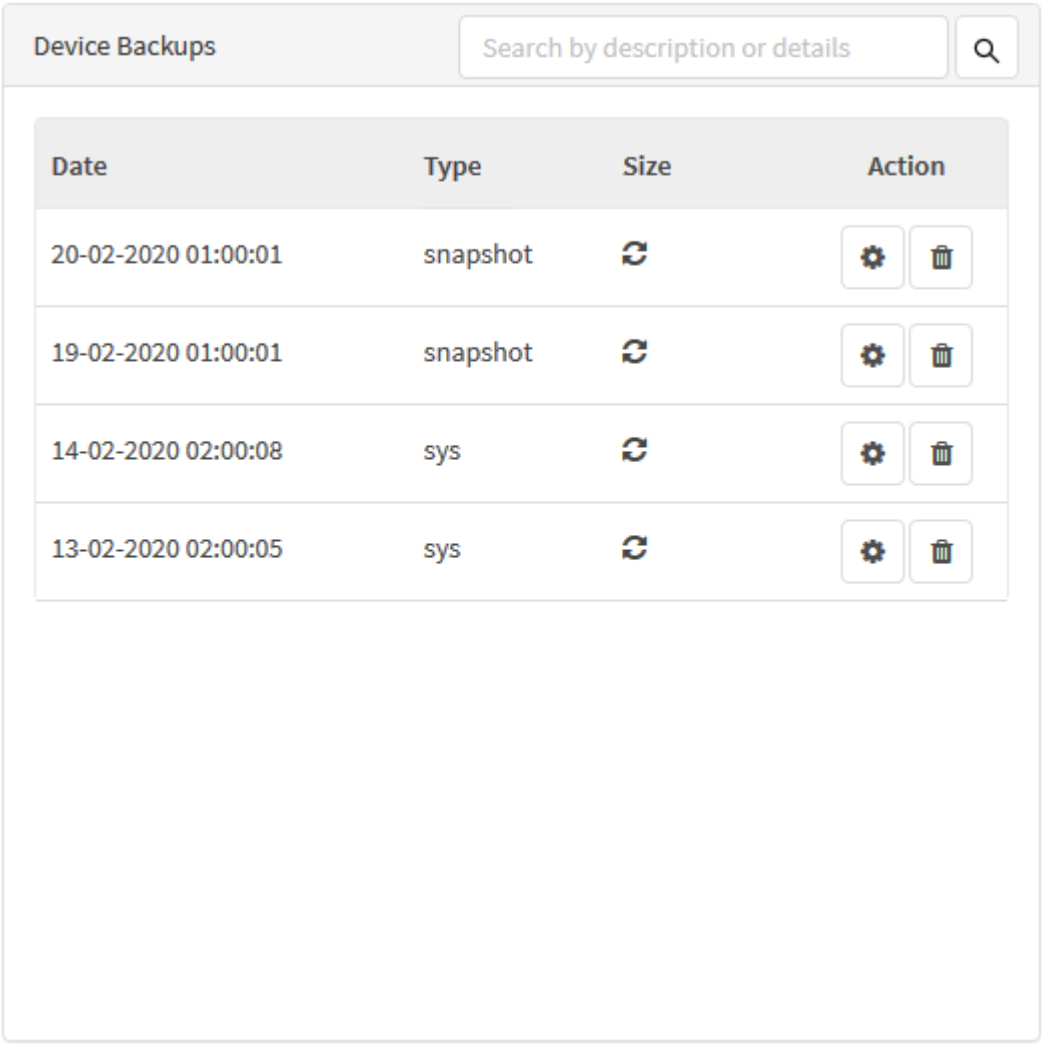
After that, click on the [ ] button to save the settings.

Backups - Device Backups

In this area the system returns the list of backup files available in the selected storage and configured in the settings panel.



Device Backups



- ***Date*:** In this column, the file is generated with the system's date and time when it's scheduled;
- ***Type*:** In the "Type" column, the type of backup is informed;
- ***Size*:** The size is displayed after clicking the **[**  **]** button;
- ***Action*:** It has two action buttons with the following features:
  - ***Restore* [**  **]:** It is responsible for restoring the backup;
  - ***Delete* [**  **]:** Used to delete a backup from storage.

If you are doing a reinstallation, remember that the backup was saved in “encrypted” mode and, therefore, the algorithm used in encryption uses the integrity key generated by the “Configuration Wizard” of the original installation of the encryption and decryption system of the backup/restore.

To successfully restore the backup from the current installation, the same license key used when activating the product during the previous installation is required.

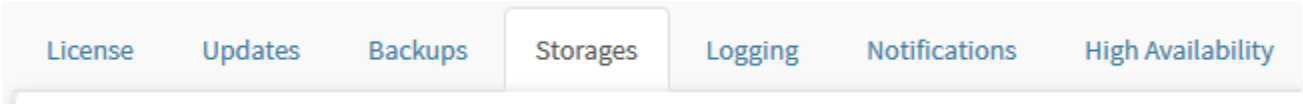
To restore a backup, just access the **[**  **]** icon and confirm that the desired file is restored.

System - Storages Tab

Storage refers to a device or system meant to store data digitaly in a permanent form. It's essential in computer systems and networks, used to store files, documents, databases and other types of information.

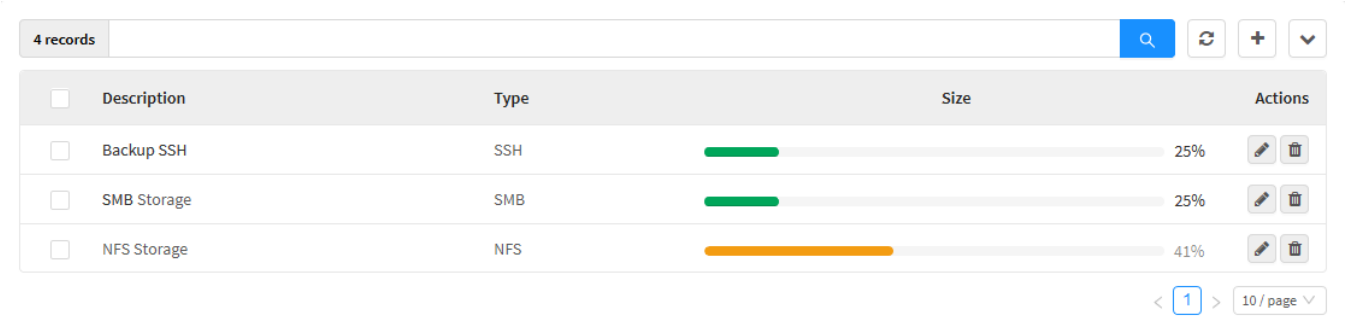
Storages can take different forms, such as Hard disk drives (HDDs), Solid state drives (SSDs) and Network-attached storages (NAS). They offer additional storage capacity in a remote way allowing the users to store and access great quantities of data in an efficient and trustable way. They ensure data availability, integrity and security, summing up to the efficient work in IT operations and trustable data storage.

In the Blockbit security solution, those are used for storing backups. To access this section, just click on the "Storages" tab:



Storages tab

The screen will appear, as shown on the image below:



System - Backup Storages

In this section we will expose the types of storage supported by the system and its applications:

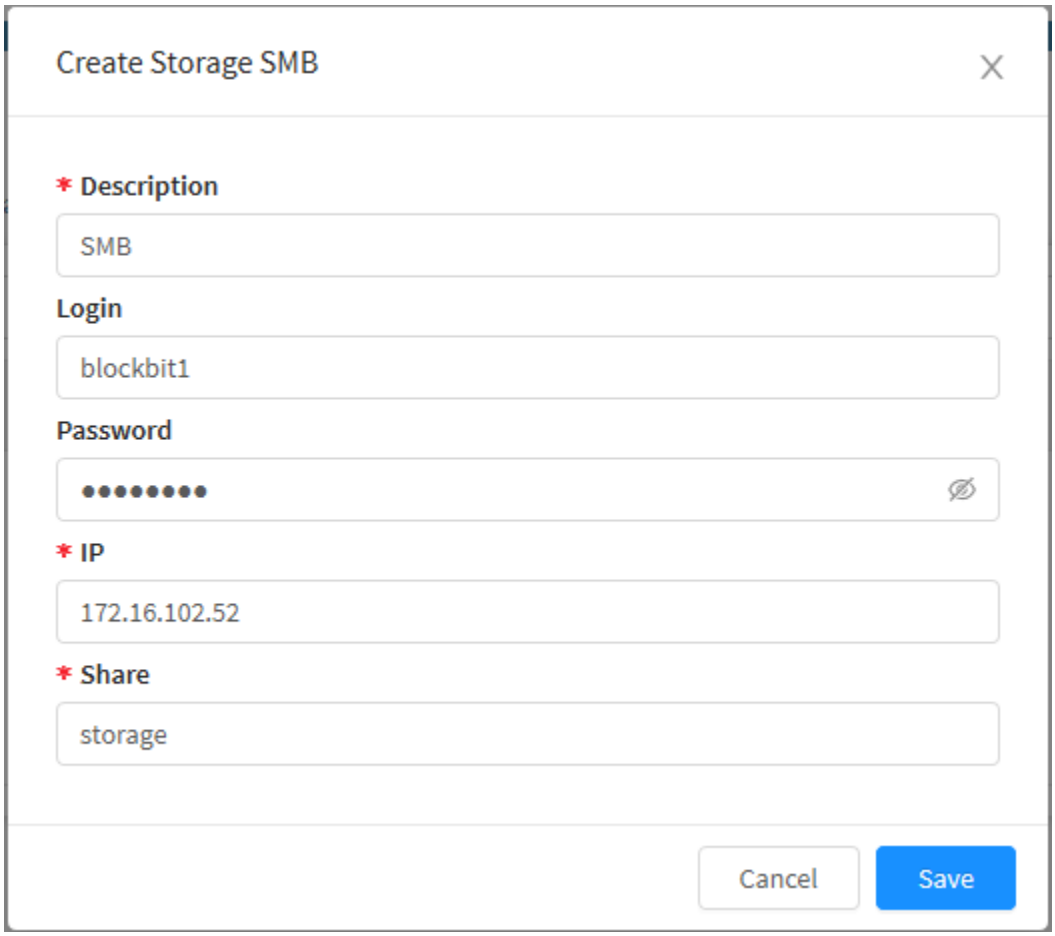
- *SMB*;
- *NFS*;
- *SSH*;
- *Disc*.

In the following we will analyze each type of storage in detail.

Storage - SMB

“Server Message Block” commonly used in folder sharing by Windows. This storage model is made available by the system for access through the SSL VPN portal;

To add an SMB store, click **[+]** and configure the form according to the specifications for connection to the respective SMB server**.**



Storage - Add SMB storage

- ***Description*:** Connection name. Ex.: SMB;
- ***Login*:** File server user. Ex.: blockbit1;
- ***Password*:** File server user password;
- ***IP*:** Select the IP address of the file server. This field will show the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage to be used. Ex .: 172.16.102.52;
- ***Share*:** Name of the folder that was shared on the file server. Ex.: storage.

It's important to mention that to use the SMB share + Threat Protection with an SSL VPN profile it's necessary to register all users that will have access, individualy, when creating a sharing profile, in Services VPN SSL Portal + SMB.

For more information on how to create a single IP object, see the following page.

After filling in all fields click on **[** Save **]** to finish or click on **[** Cancel **]** to close the window without making any changes;

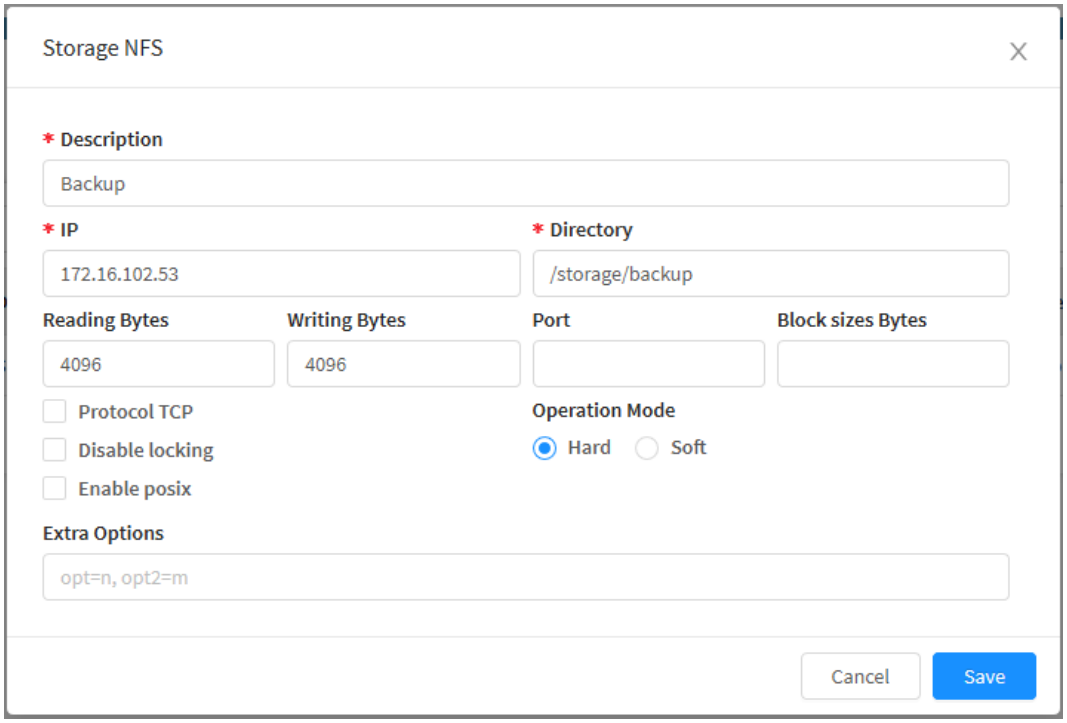
After saving, for the settings to take effect, it will be necessary to access the **command queue [**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

Click on the **[**  **]** button to update the data on this panel.

Storage - NFS

The “Network File System” is commonly used for sharing folders on UNIX servers. This storage model is made available by the system for “Backup /Restore” applications

To add an NFS storage, click on [+] and configure the form specifying the fields "Description", "IP" and "Directory" of the NFS server for the storage of the backup/restore feature.



Storage - Add NFS storage

- ***Description*:** Name of the NFS store. Ex.: Backup;
- ***IP*:** Select the IP address of the NFS server. This field will show the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage to be used. Ex .: 172.16.102.53;
- ***Directory*:** Storage directory on the NFS server. Ex.: / storage / backup;
- ***Reading Bytes*:** Sets the reading speed of the server bytes;
- ***Writing Bytes*:** Sets the writing speed of the server bytes;
- ***Port*:** Defines the port used by the server;
- ***Block sizes Bytes*:** Determines the size of the NFS storage blocks;
- ***Protocol TCP* [ ]:** If this check box is enabled, the TCP protocol will be used by the NFS server;
- ***Disable locking* [ ]:** If this check box is enabled, stored files cannot be blocked;
- ***Enable posix* [ ]:** When activating this check box, this storage will be enabled to be accessed by systems that use POSIX requirements (Portable Operating System Interface);
- ***Extra Options*:** The configuration of this item can be configured based on the configurations and specifications of the NFS server.

For more information on how to create a single IP object, see the following page.

The administrator, not knowing the details of the NFS server configuration, can maintain the default values of the interface configuration.

After filling in all the necessary fields click on **[** Save **]** to finish or click on **[** Cancel **]** to close the window without making any changes;

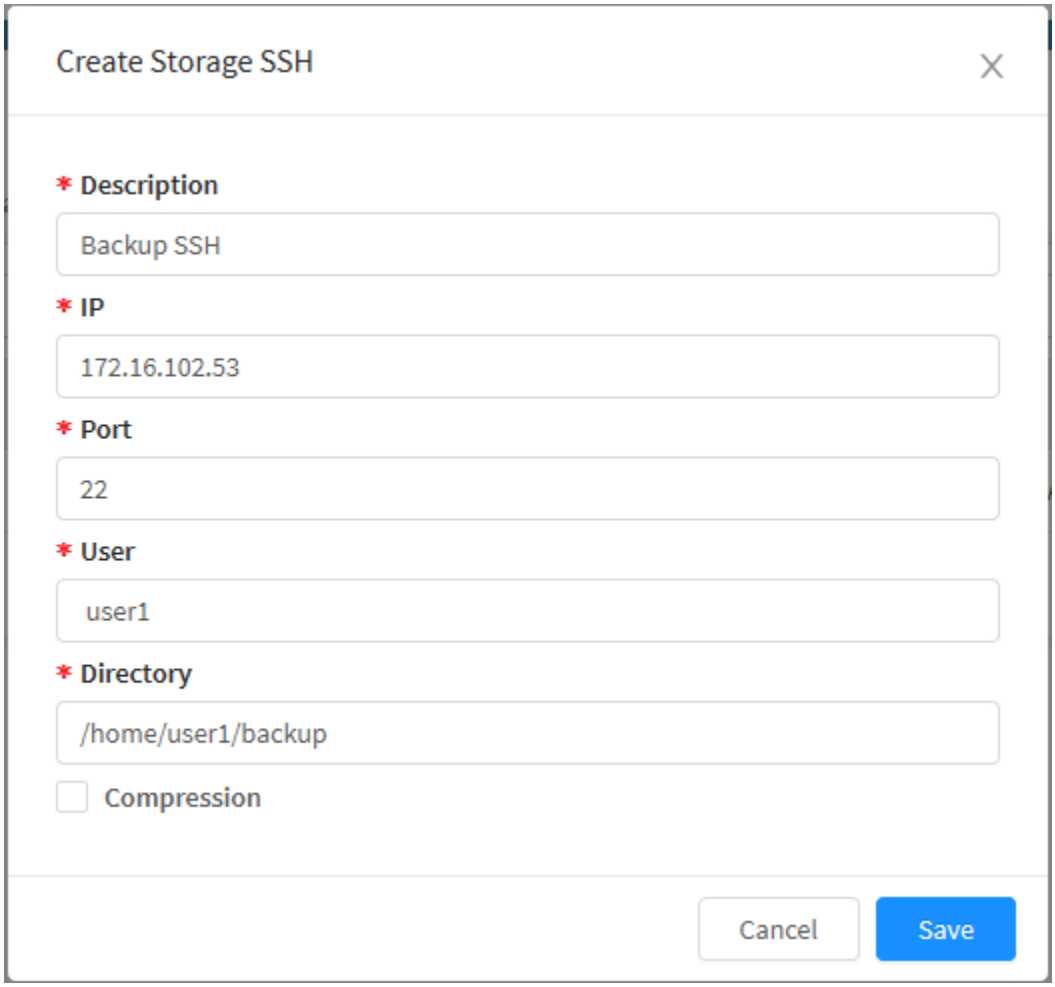
After saving, for the settings to take effect, it will be necessary to access the **command queue [**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

Click on the **[**  **]** button to update the data in this panel.

Storage - SSH

The "Secure Shell" is a cryptographic network protocol commonly used to securely connect network services. This storage model is made available by the system for “Backup/Restore” applications;

To add SSH storage, click **[+]** and configure the form specifying the fields "Description", "IP" and "Directory" of the NFS server for the storage of the backup/restore feature.



Storage - Add SSH storage

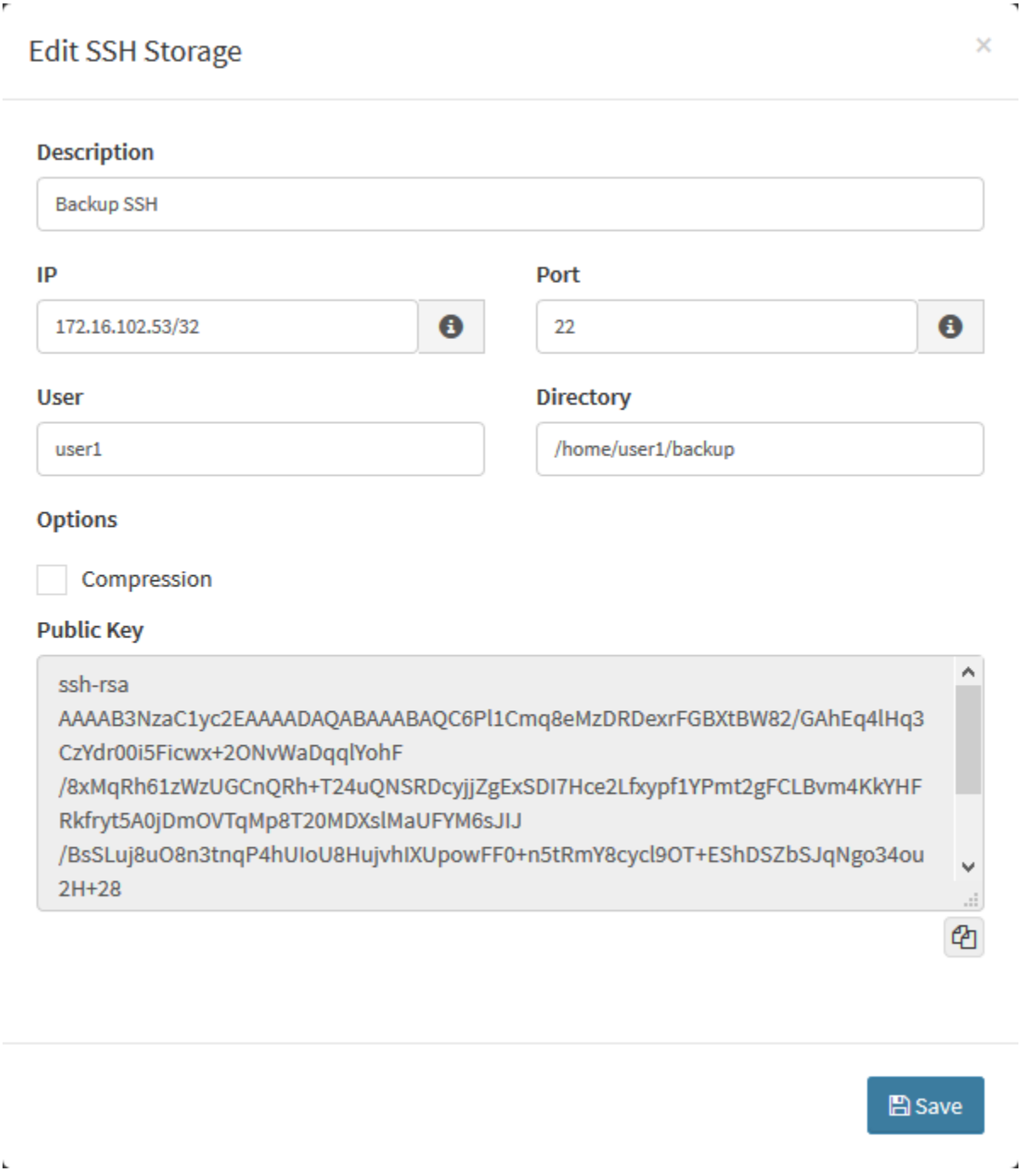
- ***Description*:** SSH storage name. Ex.: SSH Backup;
- ***IP*:** SSH server IP address. This field will show the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage to be used. Ex .: 172.16.102.53;
- ***Port*:** SSH service port. Ex.: 22;
- ***User*:** User responsible for the ssh connection. Ex.: user1;
- ***Directory*:** *Storage directory on the SSH server. Ex.: / home / user1 / backup;*
- ***Compression*[ ]:** When you activate this check box, the data from this storage will be compressed.

For more information on how to create a single IP object, see the following page.

After filling in all fields click on [Save] to finish or click on [Cancel] to close the window without making any changes;

After saving, for the settings to take effect, it will be necessary to access the **command queue [1]** and apply the changes made. For more information about the command queue visit the page: UTM - Command queue.

After that, we will edit the storage “SSH” by clicking on the [✎] button that is in the Action column, the screen below will be displayed.

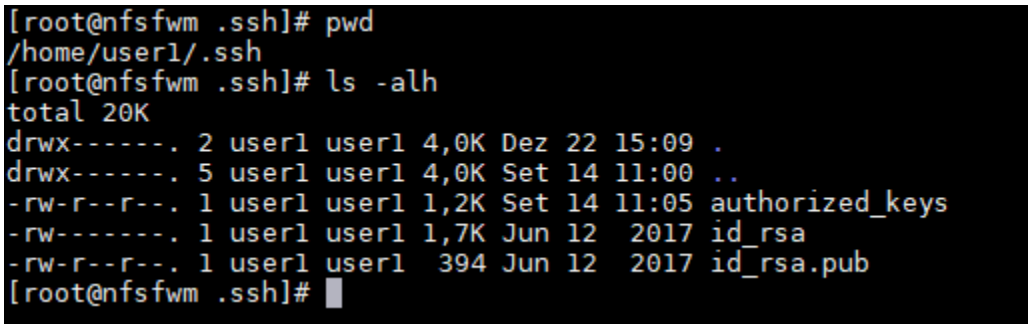


SSH - *Edit storage SSH*.

To create a backup file in a Cluster, you will need the Public Key of all devices.

The system will generate a public key to be exported to the SSH server, by clicking on the **[** **]** icon, after copying the key we will go to the remote server where the SSH.

In the user's .ssh directory where the backup will be stored, for example: “/home/user1/.ssh”, the key that was copied in the authorized_keys directory will be saved, as shown in the image below.



SSH - SSH authorized_keys

When editing the file we will paste the key and save the changes.

SSH - Edit SSH authorized_keys

After that, click on the **[** **]** button so that the data is displayed on the main screen.

Storage - Disc

It is a physical data storage device. Type devices (USB-HDD; USB-SSD) are supported. This “Storage” model is made available by the system for “Backup / Restore” applications.

To identify a “Disc” type device, click on **[ ]**, in this way, the device type will be recognized, assembly and access unit configuration according to your identification.

The system requires that “Disk” devices be formatted according to the EXT4 log file system.

To perform the formatting of the disk, just access the Blockbit UTM console, access the *Terminal*.

To log in to the terminal, use the admin user and the personalized password.

The default password is:

Login: admin

Password: admin

It is highly recommended to change the default password for the "admin" console user. To change the default password, it is necessary to create a secure password. This password must contain at least 8 characters with upper and lower case letters, numbers and special characters. To change the password, use the CLI command "passwd", check this page for more information.

*Access to the terminal is restricted, to list the available commands, type: **?**.*

```
admin  >?
arp               disable-pim   ifconfig    reboot               sync-users
arping            disable-rip   ifstat      reset                sysctl
configure-bgp     disable-snmp  iostat      reset-admin-blocks   tcpdump
configure-ospf    enable-bgp    iotest      reset-admin-password tcptop
configure-ospf6   enable-ospf   ip          reset-admin-sessions tcptrack
configure-pim     enable-pim    ipcalc      reset-logs           telnet
configure-rip     enable-rip    iplist      reset-stats          tracepath
configure-rip6    enable-root   iptraf      rewizard             traceroute
conntrack         enable-snmp   ldapsearch  route                update-license
date              ethtool       less        sar                  update-system
debug-auth        exit          lscpu       service-disable      uptime
debug-dhcp        fdisk         lsusb       service-enable       vmstat
debug-events      free          mkfs        service-start        vtysh
debug-firewall    fsck          more        service-status       watch-cpu
debug-ha          fwrecovery    mtr         service-stop         watch-io
debug-threats     fwreload      netads      show-sessions        watch-mem
debug-vpn         grep          netstat     show-uuid            watch-srv
debug-web         help          nslookup    show-vpn-conn        wc
dig               history       ntpdate     show-vpn-info        whois
disable-bgp       host          passwd      shutdown
disable-ospf      hostname      ping        speedtest
admin  >
```

Terminal

1. To list the new disk, type: **fdisk –l**

```
admin > fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes, 625142448 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
```

```
Disk identifier: 0x000b93f6

Dispositivo Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     1026047      512000   83  Linux
/dev/sda2         1026048   625141759   312057856   8e  Linux LVM

Disk /dev/mapper/root: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/swap: 4177 MB, 4177526784 bytes, 8159232 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/data: 293.9 GB, 293890686976 bytes, 574005248 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 8000 MB, 8000110592 bytes, 15625216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin  >
```

Before formatting the disk, it may be necessary to proceed with partitioning the disk.

Partitioning the disk, execute the command: ex.: **fdisk -l / dev / sdb**

```
admin  >fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

Type **"m"** to list the parameter / command base of the "fdisk" utility for disk partitioning.

```
Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   g   create a new empty GPT partition table
   G   create an IRIX (SGI) partition table
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
```

```
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help):
```

Delete the current partition. “**d - delete a partition**”

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted

Command (m for help):
```

Add a new partition. “**n - add new partition**”

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-31299583, default 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-31299583, default 31299583):
Using default value 31299583
Partition 1 of type Linux and of size 14.9 GiB is set

Command (m for help):
```

Save the new partition table to disk. “**w - write table to disk and exit**”

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

To format the identified disk already partitioned, type: **mkfs -t ext4 / dev / sdb1**

```
admin  >mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3912192 blocks
195609 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
```

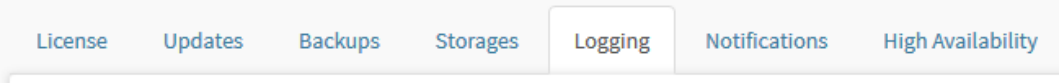
```
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Once connected to the server and formatted to the EXT4 standard, the device is ready to list. Click on **[**  **]**, the system will apply the “AUTO_MOUNT” feature and the device will automatically be available for selection.

After saving, for the policy to take effect it will be necessary to access the command queue **[**  **]** and apply the changes made. For more information on the command queue access the page: UTM - Command queue.

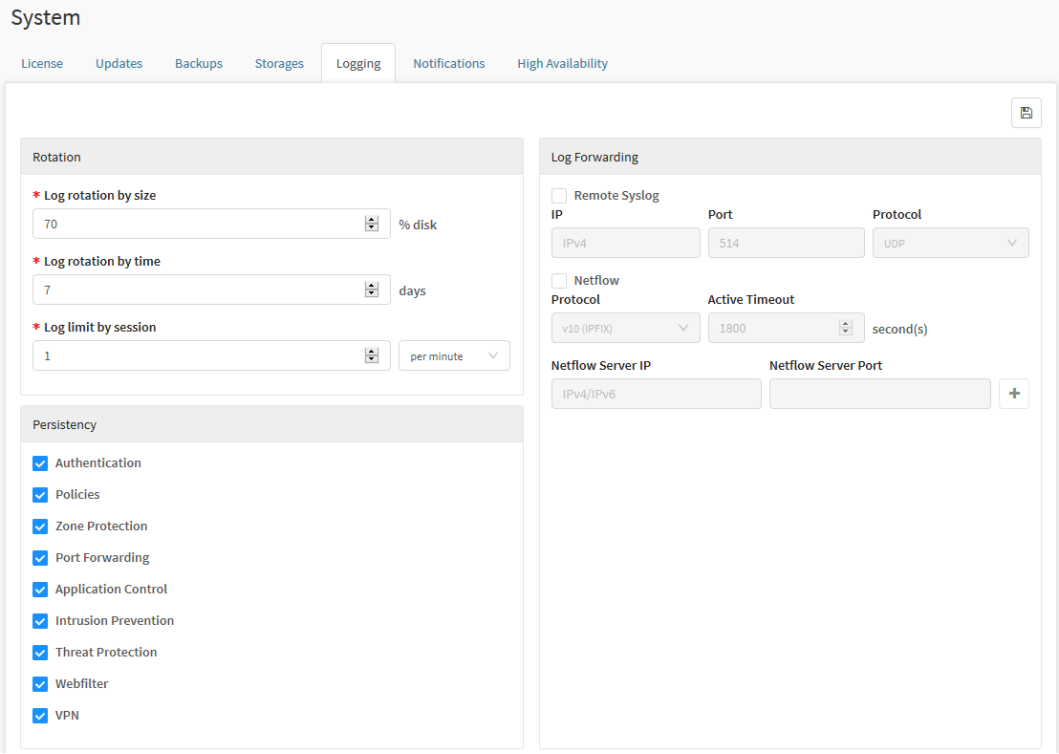
System - Logging tab

If the tab is not selected, click on "Logging".



Logging tab

The screen shown below will appear:



System - Logging

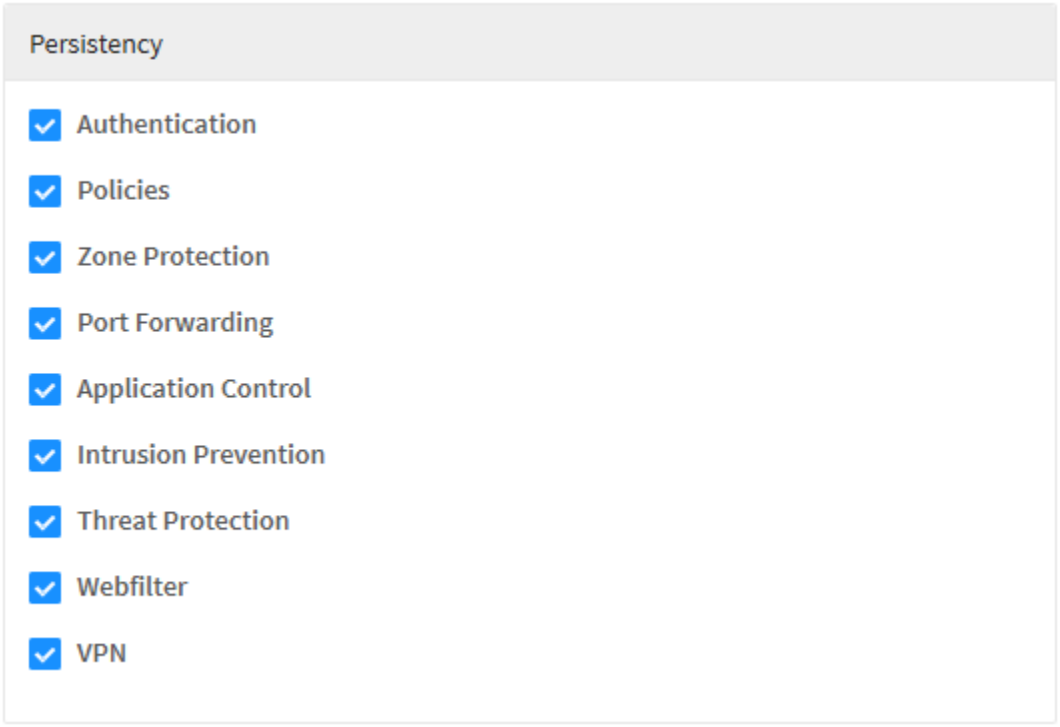
This screen is divided by the following panels:

- *Rotation*;
- *Persistence;*
- *Log Forwarding*.

Next we will analyze each component of this screen.

Logging - Persistence

In this panel you make the Logs persistence settings.



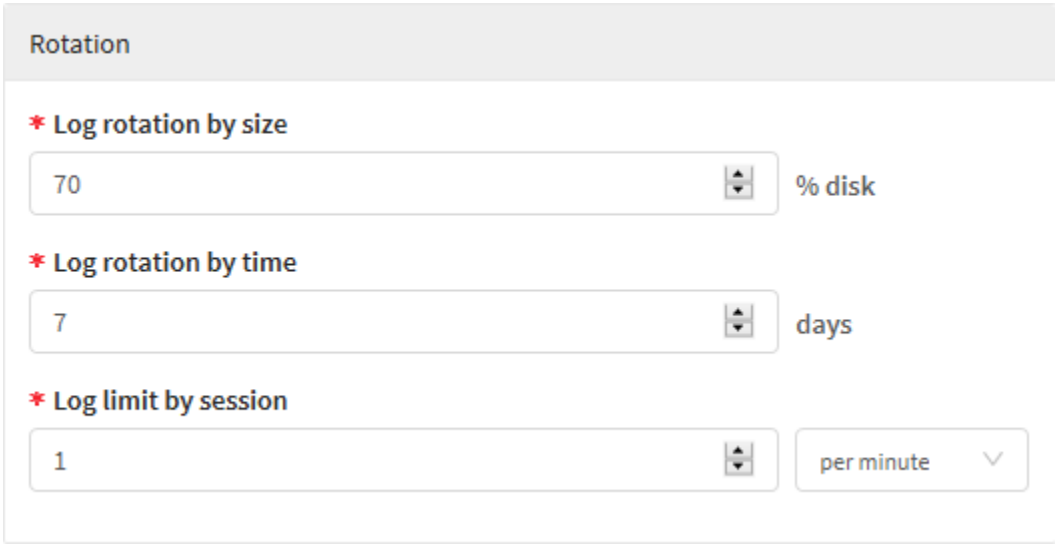
Logging - Persistence

- ***Authentication[ ]*:** When you enable this check box, persistence in the Authentication Log is activated;
- ***Policies[ ]*:** When you enable this check box, persistence in the Security Policies Log is activated;
- ***Zone Protection[ ]*:** When you enable this check box, persistence in the Zone Protection Log is activated;
- ***Port Forwarding[ ]*:** When you enable this check box, persistence in the Port Forwarding Log is activated;
- ***Application Control[ ]*:** When you enable this check box, persistence in the Application Control Log is activated;
- ***Intrusion Prevention[ ]*:** When you enable this check box, persistence in the Intrusion Prevention Log is activated;
- ***Webfilter[ ]*:** When you enable this check box, persistence in the Webfilter Log is activated;
- ***VPN[ ]*:** When you enable this check box, persistence in the VPN Log is enabled.

Click on **[ ]** to restart the firewall services and activate the settings made.

Logging - Rotation

In this panel you configure the operation of the System Logs and define the rotation and limit of the records.



Logging - Settings

- ***Log rotation by size*:** Sets the rotation of the log by percentage of disk size. Ex.: *70%*;
- ***Log rotation by time*:** Defines the rotation of the log by time of existence. It is defined in days. Ex.: 7 days;
- ***Log limit by session*:** Limit logs per session. It is defined in seconds, minutes or hour. Ex.: 1 minute.

Click on **[**  **]** to restart the firewall services and activate the settings made.

Logging - Log Forwarding

In this panel, all details regarding the routing of logs and application of Netflow are configured.

What is Netflow?

Netflow is a high performance network protocol focused on collecting and monitoring information about packet flow at interfaces. Through the analysis of the data captured by NetFlow it is possible to obtain information about the analyzed networks. The use of Netflow makes it possible to concretely visualize the traffic patterns of the network, which contributes qualitatively so that the Administrator understands the profile of his network, facilitating the audit process and improving the accuracy in applying measures to improve availability and quality of services (QoS).

Netflow works by performing the following steps:

- Checks and monitors incoming and outgoing traffic from a device;
- It aggregates the data captured by the monitor and exports it to a management system;
- After collecting data from the management system, it is responsible for analyzing and pre-processing the information.

During the process of packet traffic on an interface, datagrams are captured by the flowcache according to the criteria used by the router, after countless entries this process eventually expires causing the flow exporters to gather the records and forward them for analysis and processing of the Netflow, using the data for future reference. Finally, through an analysis application it is possible to use the data to visualize the flow and intensity of the traffic, allowing an analysis with a high level of specificity, for example, the origin and destination of the network traffic and the volume generated, which makes it possible to accurately determine the direct cause of possible network congestion.

Blockbit acts at the level of traffic checking and monitoring and collecting data for export to a management system.

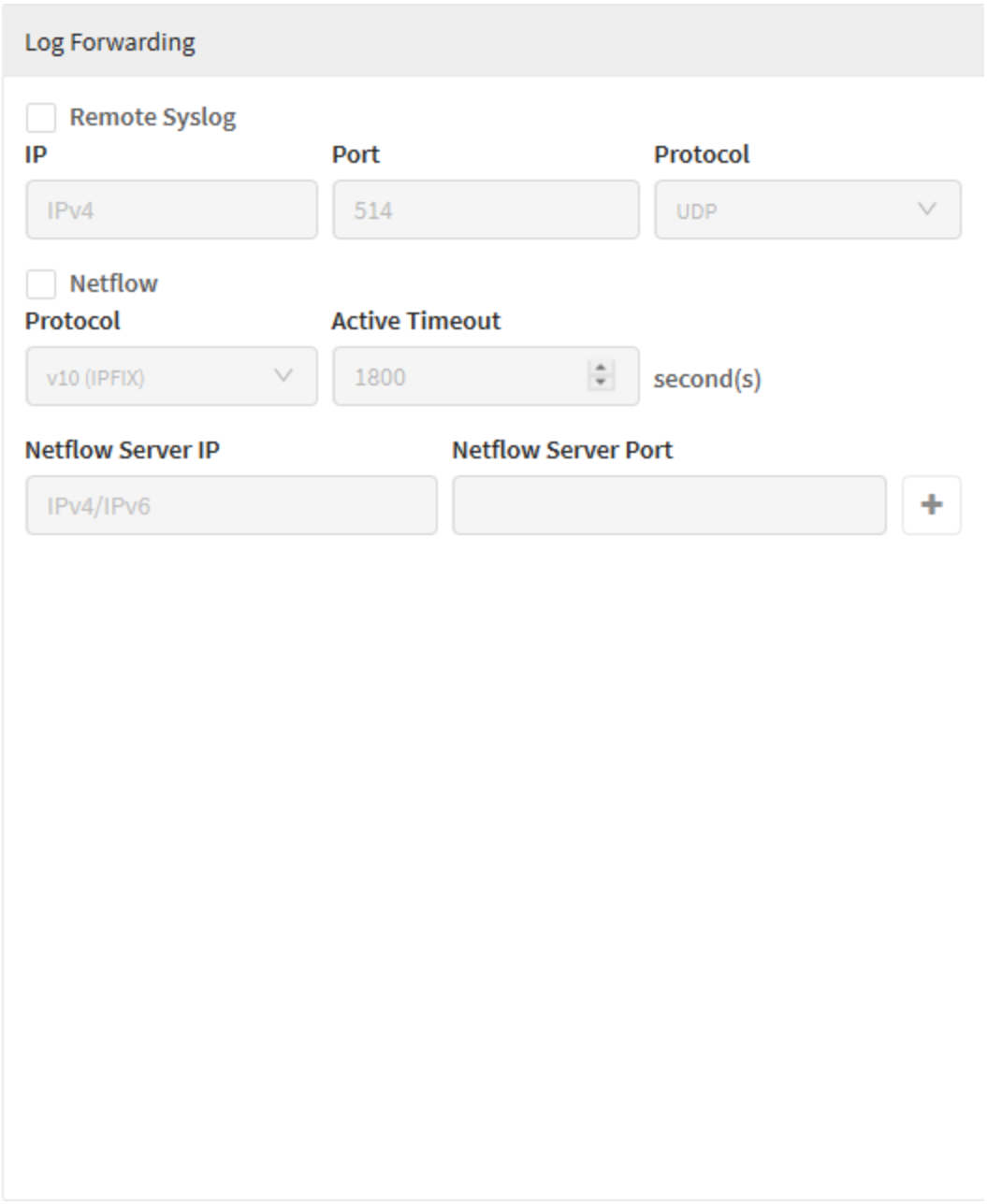
Netflow comes integrated with Blockbit UTM and has the following features:

- Full support for Netflow v5, v9 and IPFIX versions;
- Full support for IPv4 and IPv6 networks;
- Capture translation events (NAT);
- Capture of incoming and outgoing packets;
- Packet capture on physical, virtual, VLAN, DSL and MPLS network interfaces.

 For correct operation, this service must be optionally enabled by the administrator in the system's Traffic Logging settings.

To apply Netflow to IPv4 or IPv6 policies, enable the Traffic Logging checkbox in the Properties panel when creating policies.

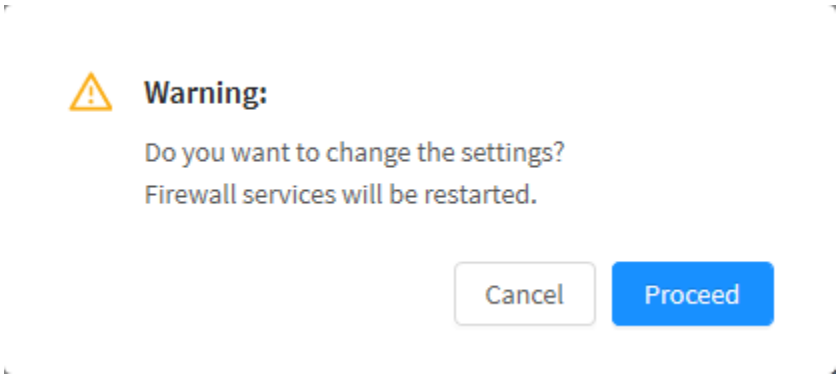
Next we will analyze how to configure the requirements of the Log Forwarding panel:



- ***Remote Syslog[ ]*:** When you enable this check box, Remote Syslog is activated:
  - ***IP:*** After enabling the field above, add the remote Syslog IP;
  - ***Port:*** Set the remote Syslog port;
  - ***Protocol:*** *Defines the protocol used by the remote Syslog, which can be TCP or UDP*.
- ***Netflow[ ]***: When you enable this check box, Netflow is activated:
  - ***Protocol*:** Defines the protocol to be used by Netflow, which can be v10 (IPFIX), v9 or v5;
  - ***Active Timeout*:** *Determines the time needed to export flows to the collector*;
  - ***Netflow Server IP*:** Sets the IP of the Netflow server;
  - ***Netflow Server Port*:** *Sets the Netflow server port*.

Click on **[ ]** to add a Netflow server, if you want to remove one of them, click on **[ ]**.

Click on **[ ]** to save and activate the settings made, note that this will restart the firewall services. The following message will be displayed:



Warning: Do you want to change de settings? Firewall services will be restarted.

ATTENTION: *Keep in mind that when clicking on the "Proceed" button, the firewall services will IMMEDIATELY restart, with a momentary stop in the services*

Click on **[** Proceed **]** to apply the settings and restart the firewall, or on **[** Cancel **]** to close this window.

After saving the settings, click on **[** **]** and apply the settings made.

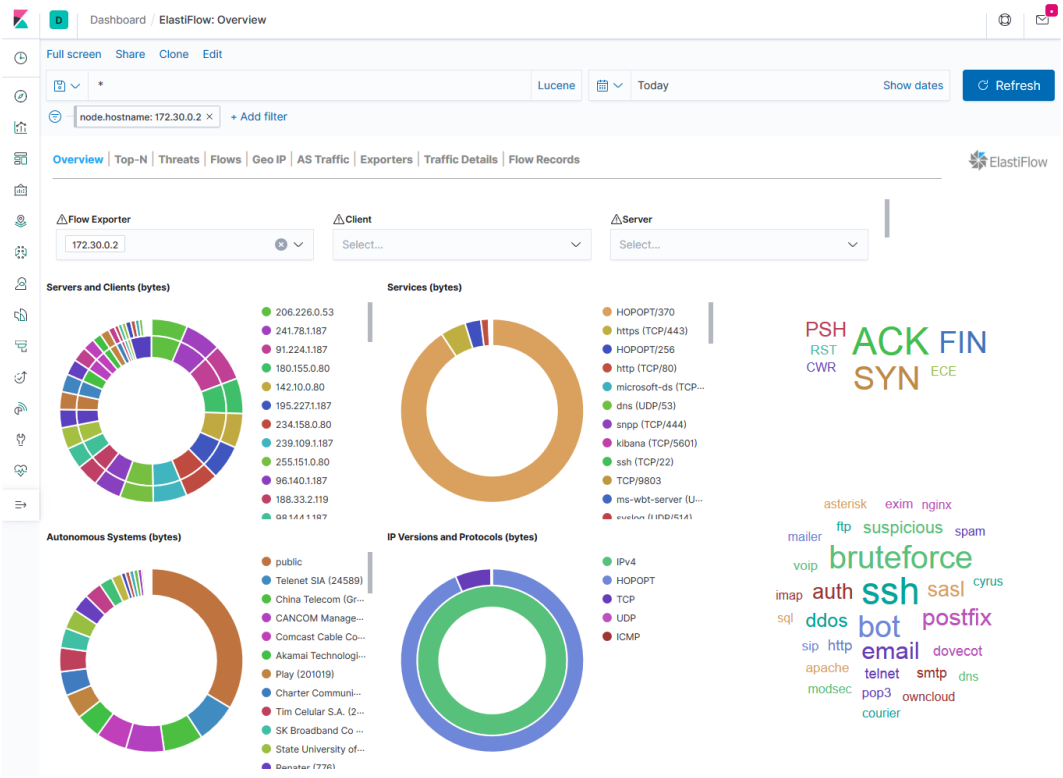
Integration with Elastiflow

Blockbit UTM allows the integration of information captured by Netflow with the resources available in Elastiflow, it is an Opensource solution whose function is to collect Netflow data and provide the visualization and monitoring of this network information using the Elastic Stack, which allows analysis in a more transparent and user-friendly way.

Here are some examples of diagrams created by Elastiflow:

Overview

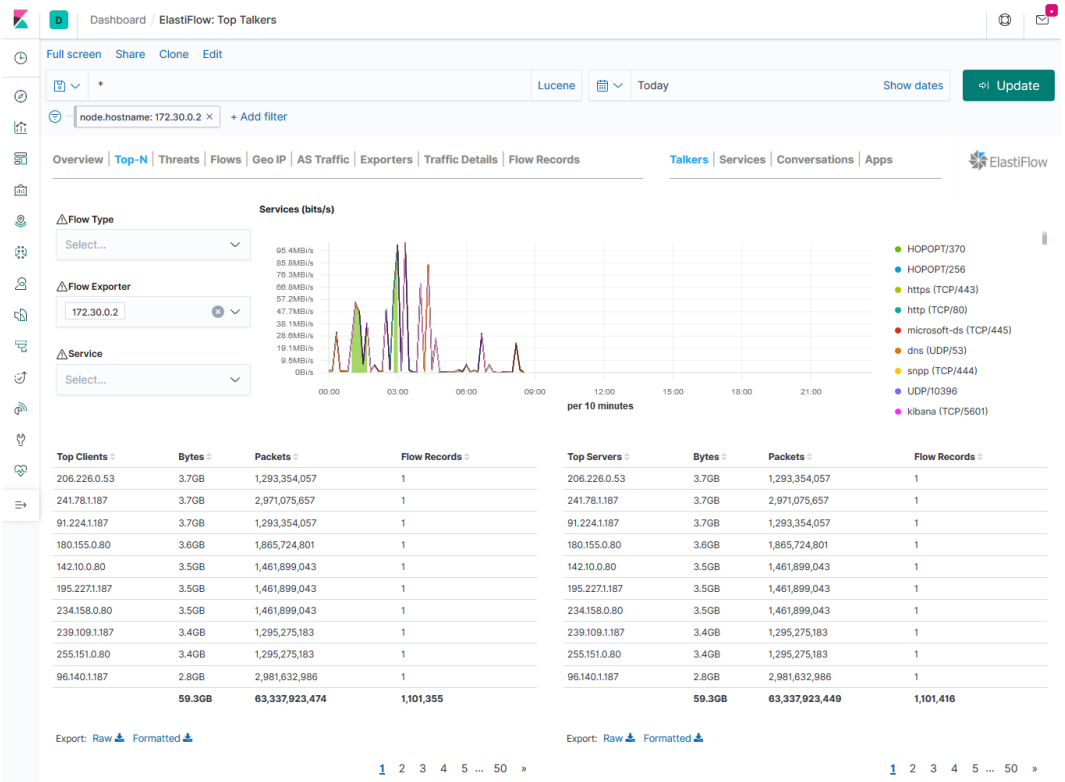
It serves to display an overview of the servers, clients, services and protocols of the network:



Elastiflow - Overview

Top-N

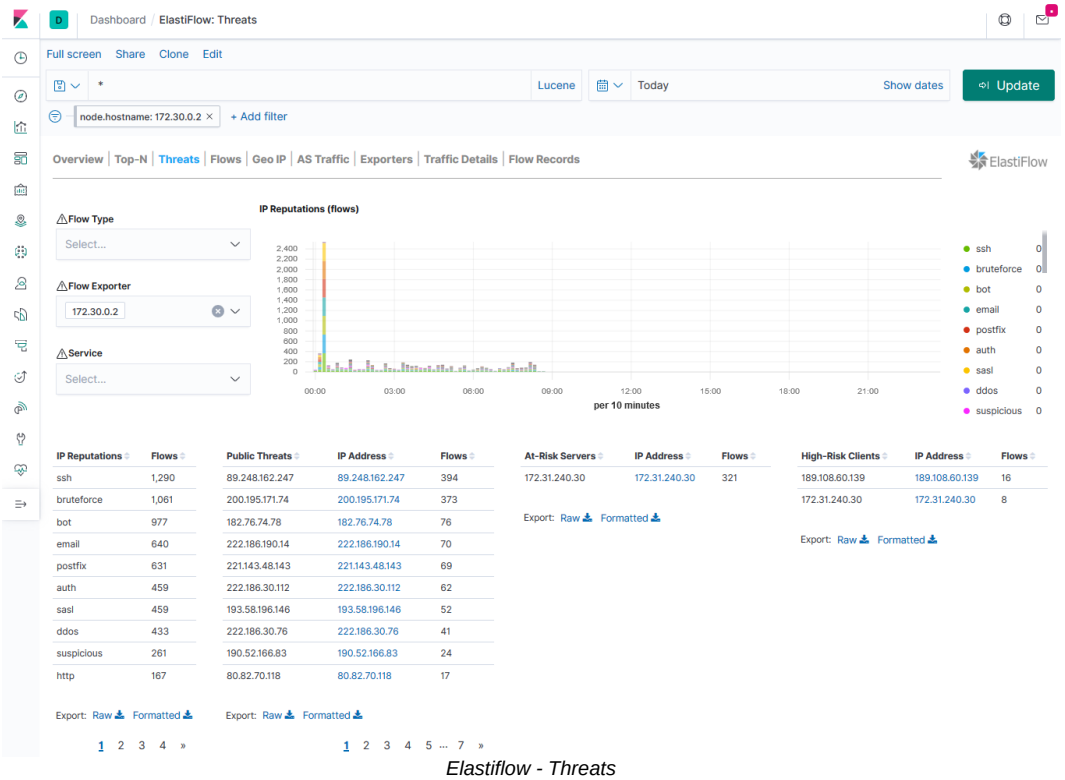
Whose function is to show the most active services, applications and accesses on the network:



Elastiflow - Top-N

Threats

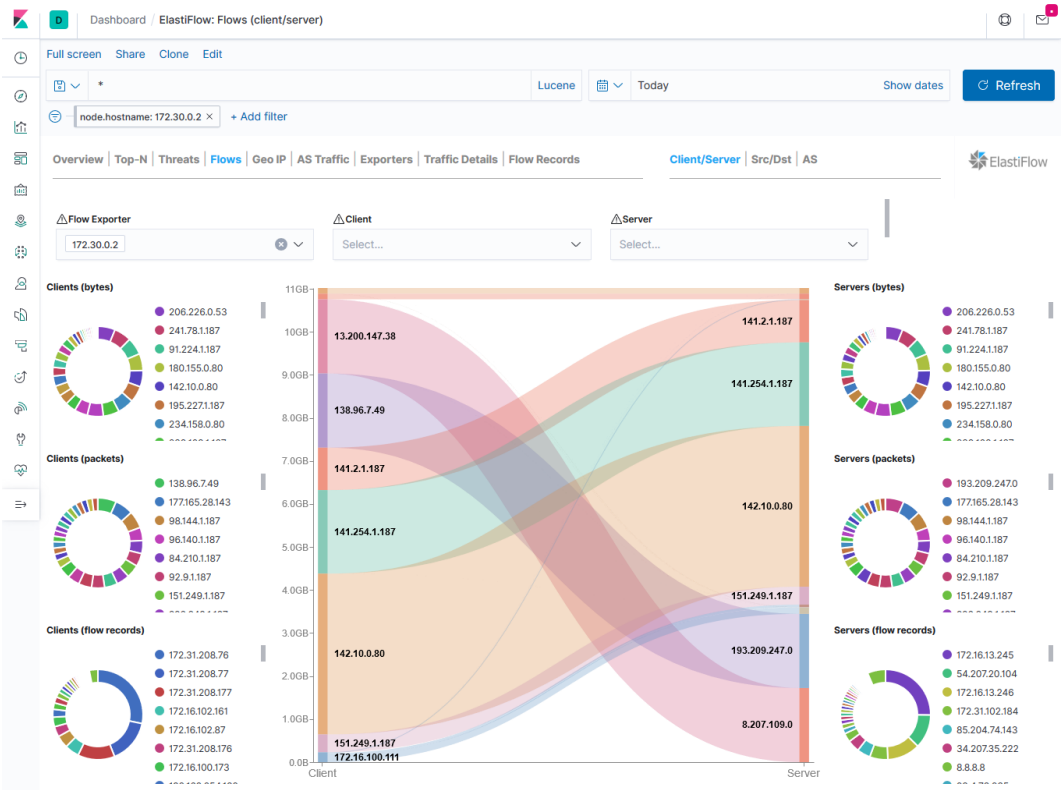
Displays all threats detected by netflow based on a list of public IPs made available by Elastiflow itself divided by type of risk:



Elastiflow - Threats

Flows

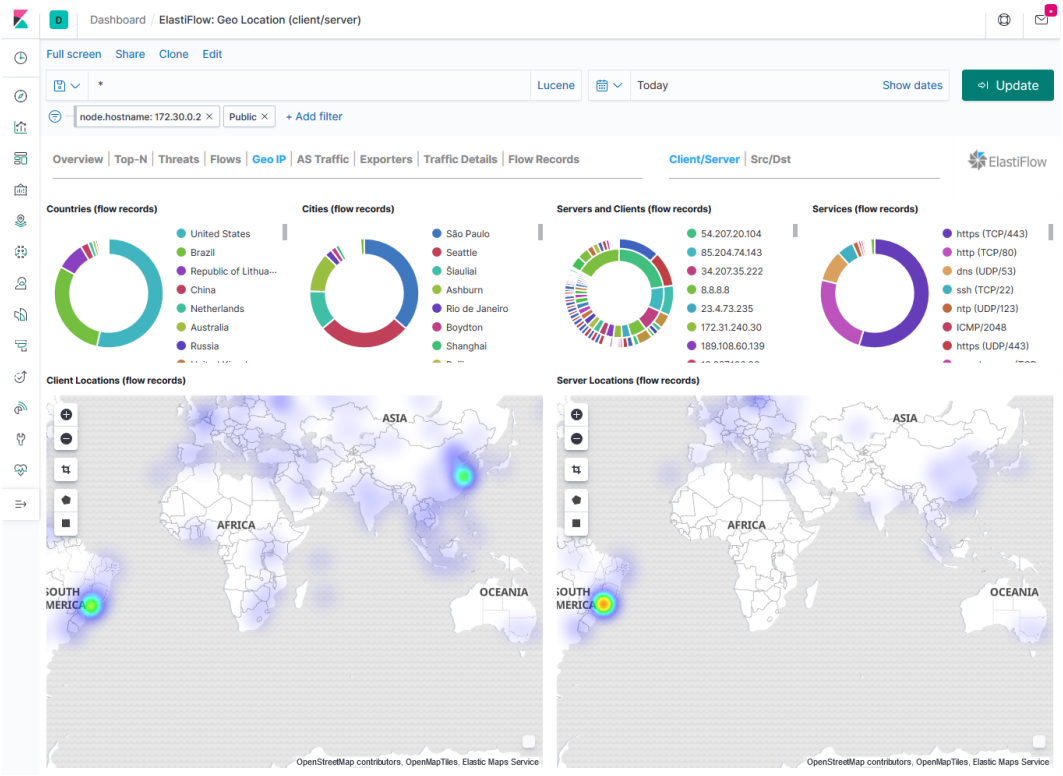
Displays information relevant to the network flow:



Elastiflow - Flows

Geo IP

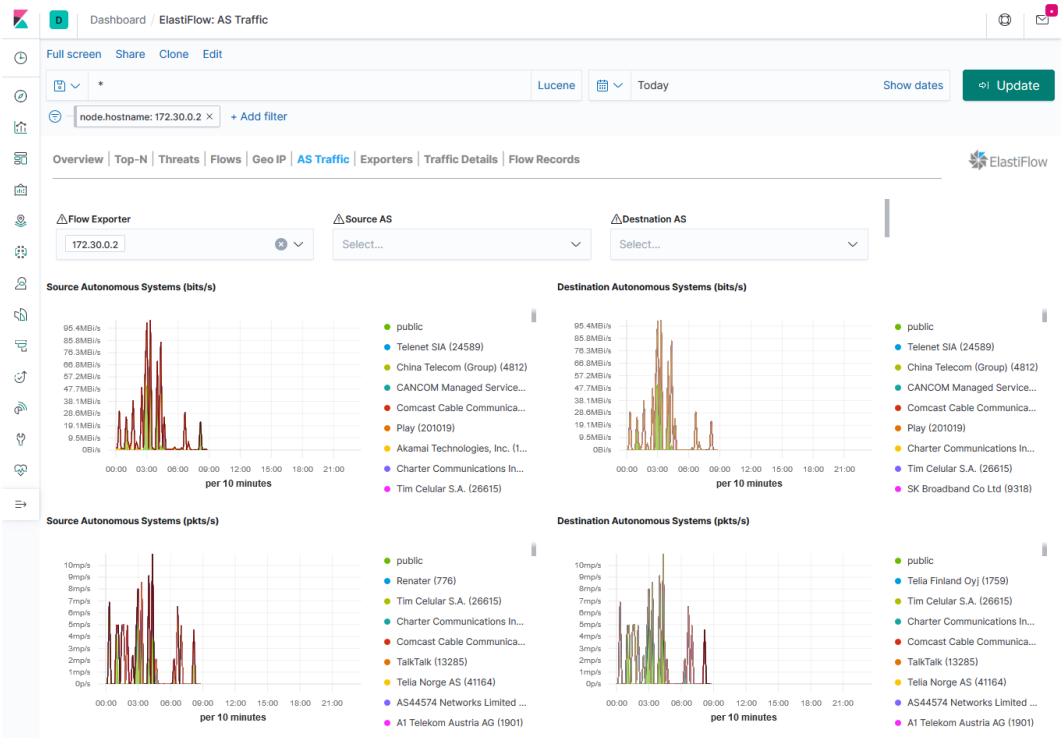
Displays data on the geolocation of the accesses detected by Netflow:



Netflow - Geo Ip

AS Traffic

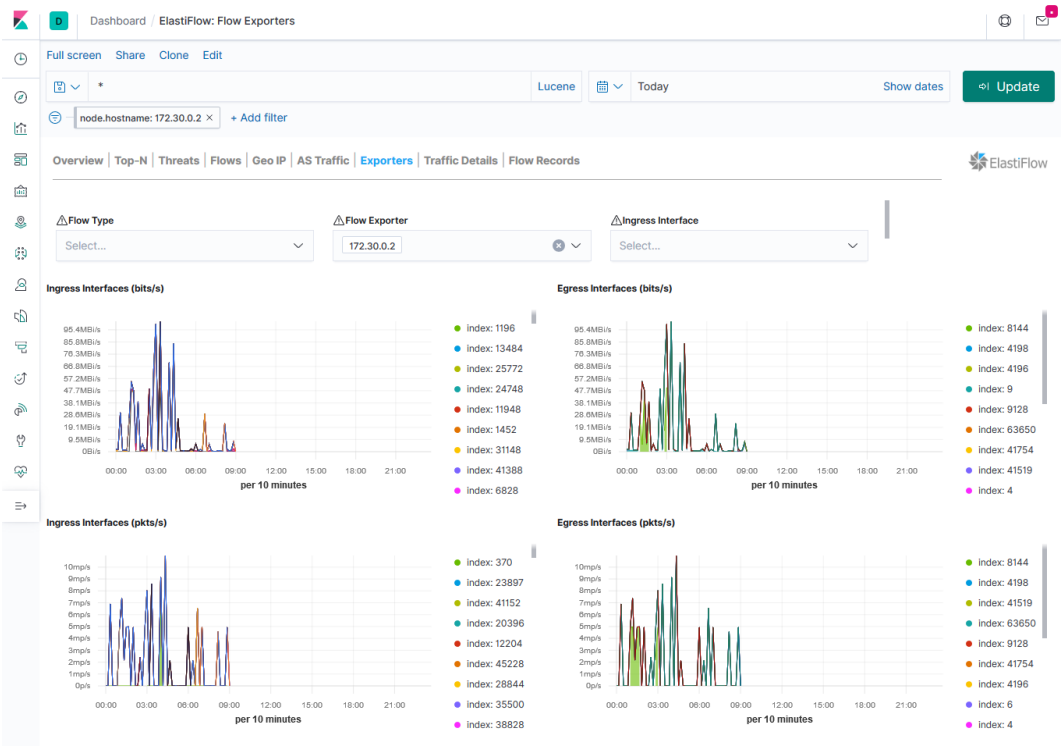
Its function is to display information about the traffic entering and leaving autonomous systems:



Netflow - AS Traffic

Flow exporters

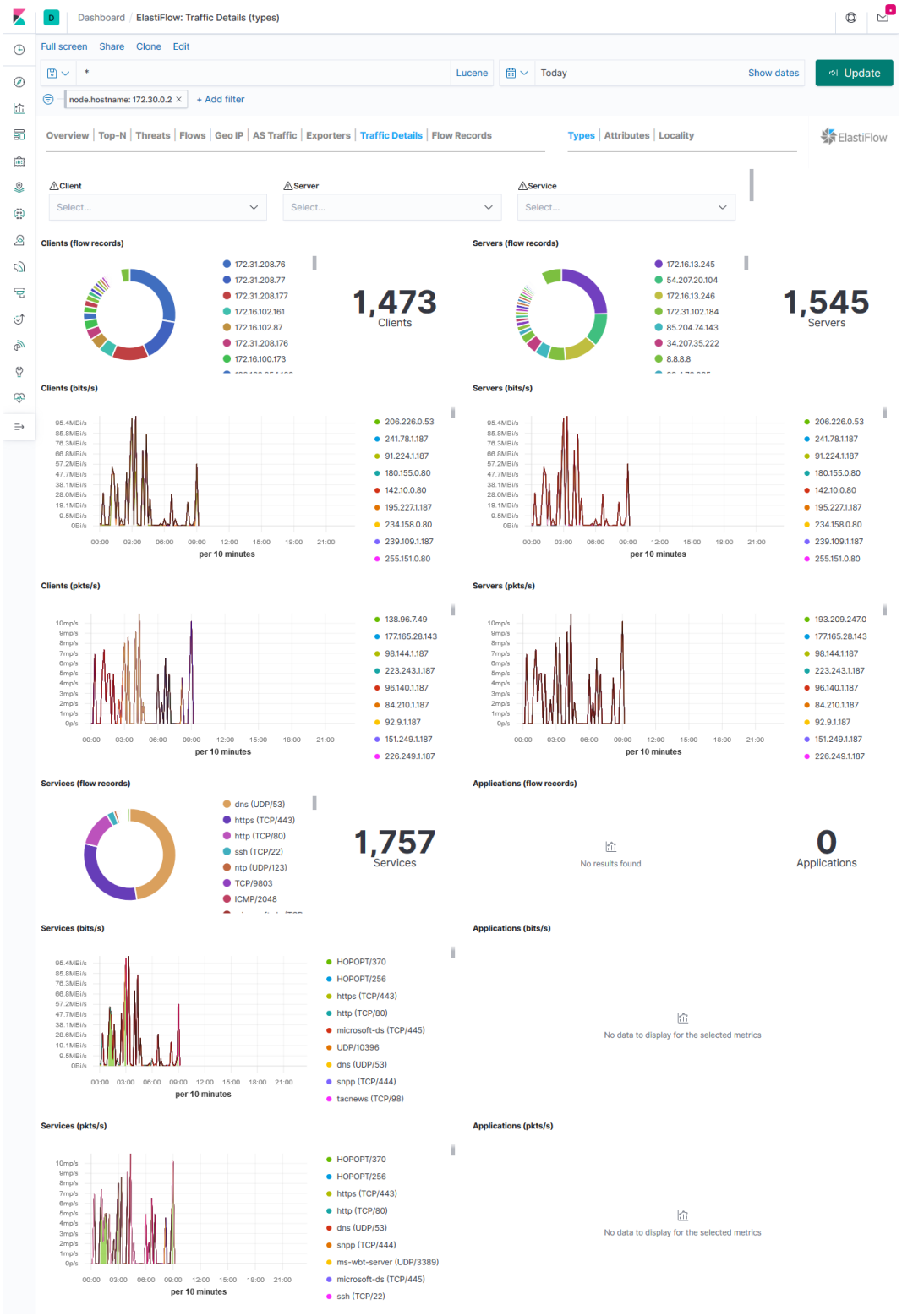
Shows the input and output of bits and packets on the interfaces:



Netflow - Flow Exporters

Traffic details

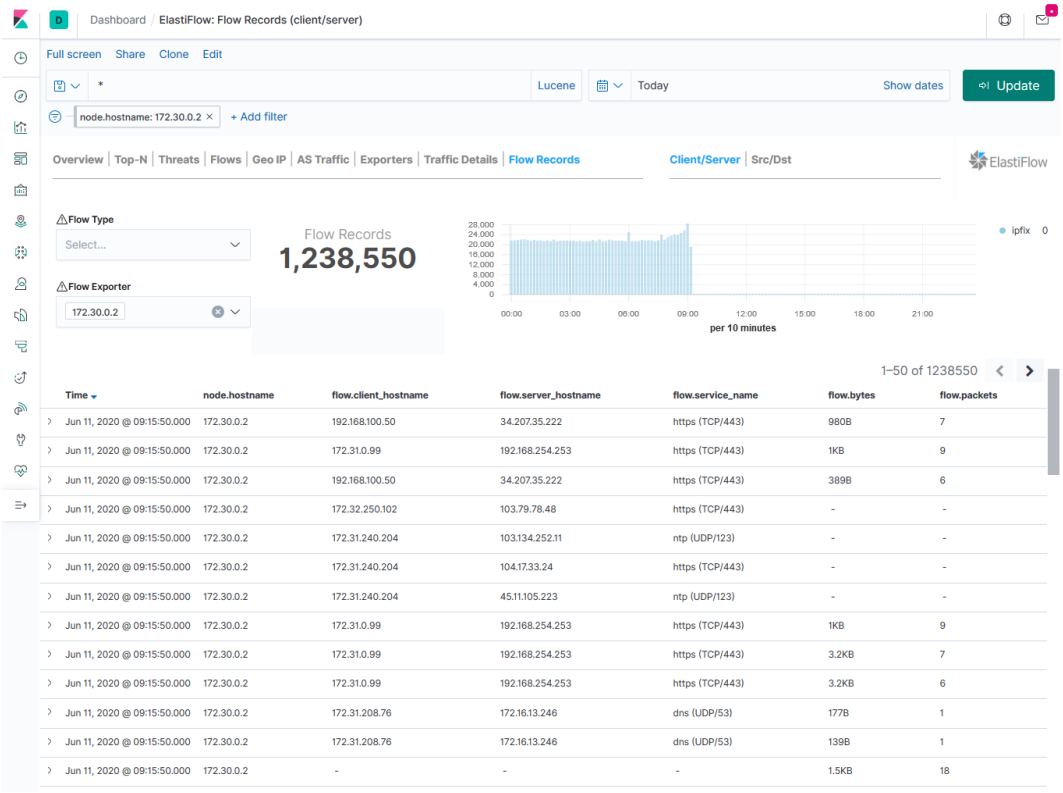
Shows more specific information about network traffic:



Netflow - Traffic Details

Flow records

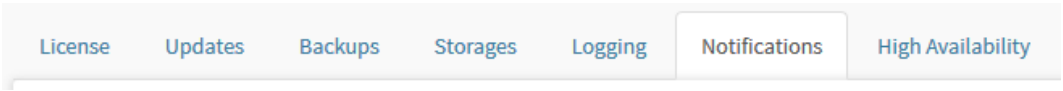
Shows a history of the entire network flow:



Netflow - Flow Records

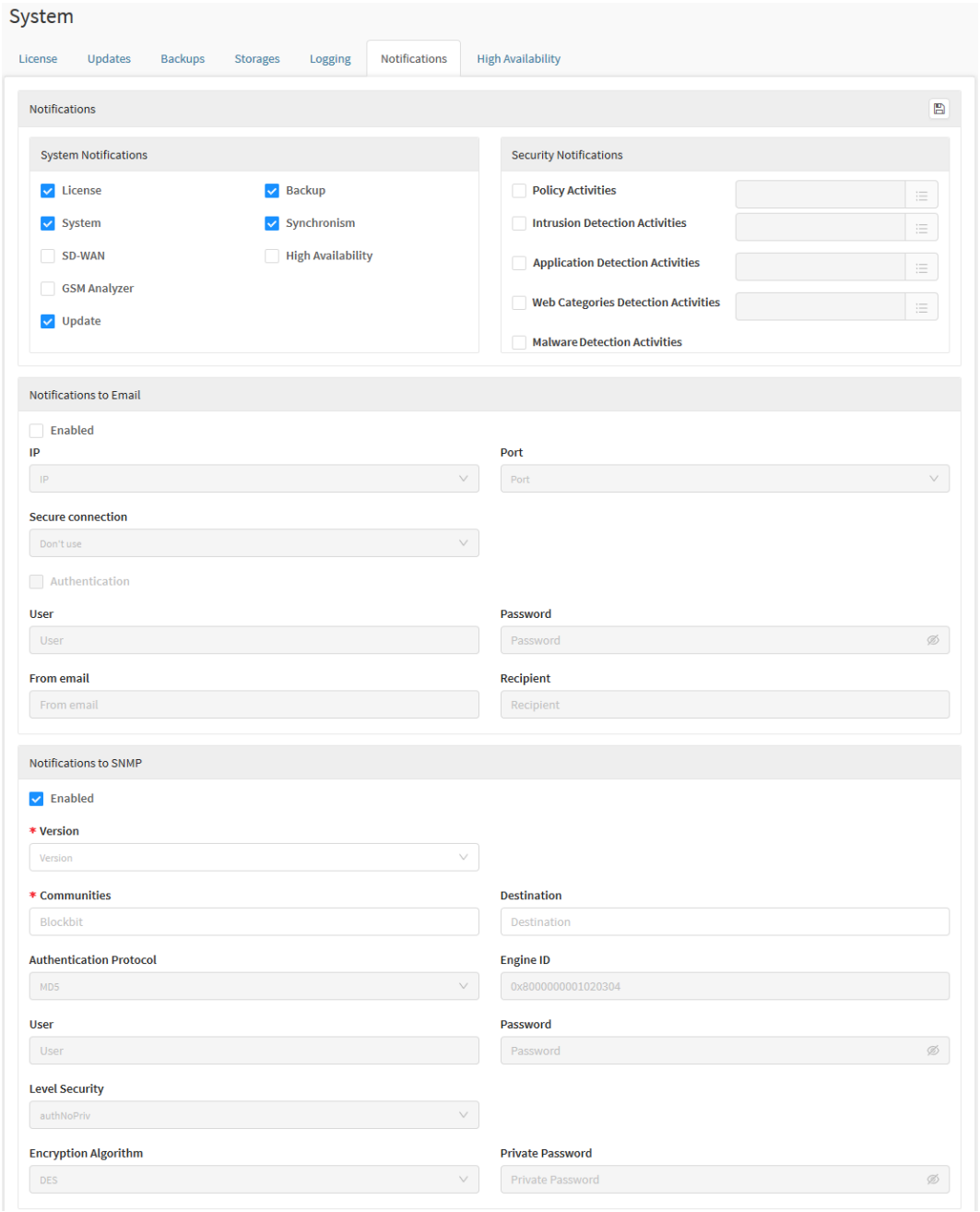
System - Notifications tab

If the tab is not selected, click on "Notifications".



Notifications tab

The System “Notifications” screen will appear, as shown by the image below:



Intrusion Prevention - Profiles

This screen is divided by the following panels:

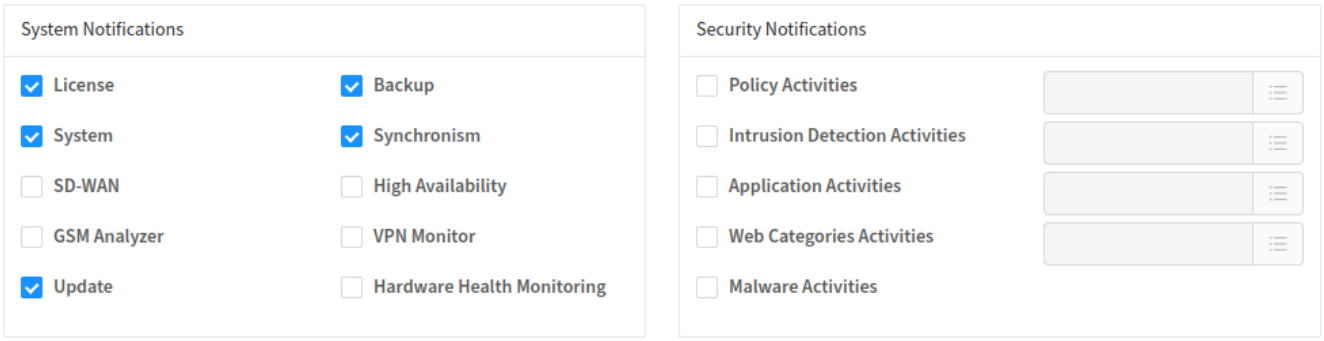
- *Notifications*;
- *Notifications via Email*;
- *Notifications via SNMP*.

Next, we will analyze each component of this screen.

Notifications

In the Notifications panel you can configure the service to send two classes of notifications.

- *System Notifications*;
- *Security Notifications*.



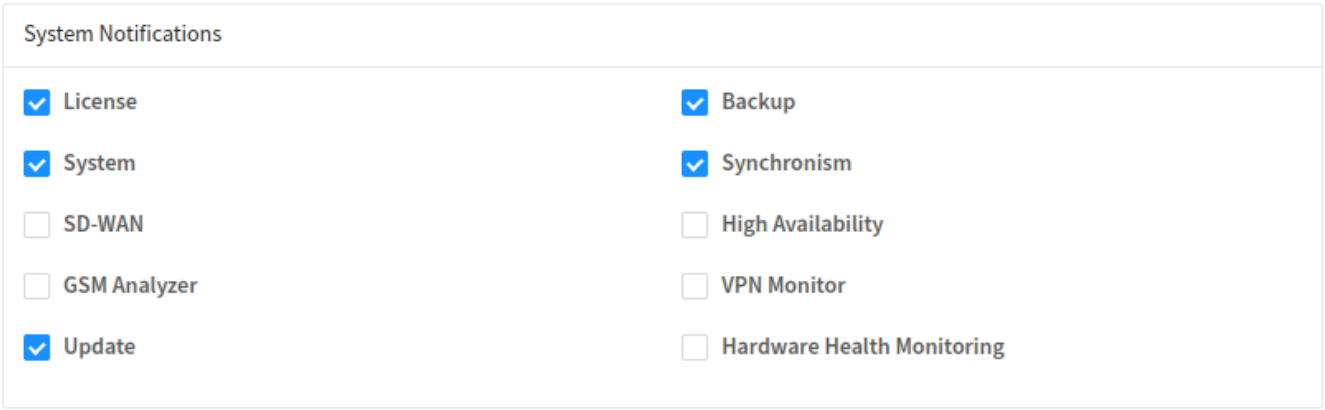
Administration - Notifications

System Notifications

In this section, you, the administrator, can enable which system notifications to be sent: "License", "Update", "Backup", "Performance", "Synchronism", "SD-WAN", "High availability" and "GSM Analyzer". The "enabled" notifications will be triggered for "viewing" on the WEB interface, in the action frame on the upper right through the **[** **]** icon in "real time", and forwarded "E-mail" or "SNMP Trap", when enabled. Examples:

- *Licence close to expiration alert;*
- *System and base update alert;*
- *Backup generator conclusion alert;*
- *High CPU usage alert;*
- *Synch with Domain Controller alert;*
- *Link crash alert;*
- *Cluster HA service changes alert;*
- *Miscommunication with the GSM/Analyzer alert:*
- *High hardware temperature alert;*
- *Cooling system fail alert;*
- *Others.*

To see the enabled notifications in the WEB interface in real time, click on ***[*** ***]*** *on the upper right corner. When enabled, notifications can be sent by E-mail and SNMP Trap.*



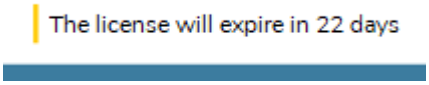
Administration - System Notifications

License Notifications

After having enabled the license notifications, the number of remainig days until your license expires will become available in the alerts icon [ ], located in the reight superior side of the screen, in the form of a notification.

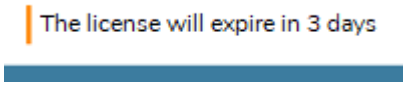
The total remaining days will also be displayed in the central superior part of the screen, when there is a specific amount of days until your license expiration day, as shown bellow:

When there are between 30 and 11 days left, the message will be displayed with a yellow stripe:



Yellow striped license expiration message - Notifications

When there are between 10 and 2 days left until expiration, the alert message will be displayed with an orange stripe:

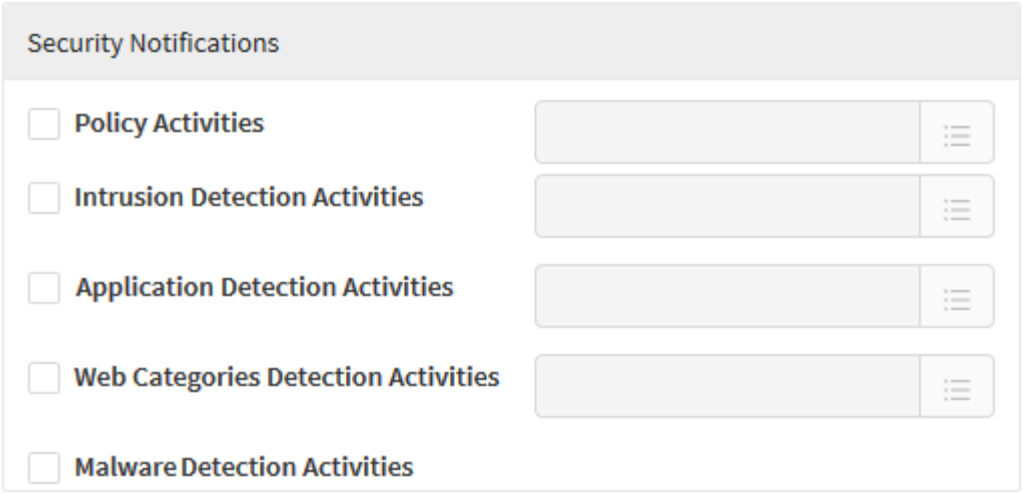


Orange striped license expiration message - Notifications

Security Notifications

In this section you, the administrator, can enable which security notifications should be sent: *"Policy Activities"*, *"Intrusion Detection Activities"*, *"Threat Detection Activities"*, *"Application Activities"*, *"Web Categories Activities"* and *"Malware Activites"*. The **enabled notifications [ ]** will be triggered for "visualization" in the WEB interface, in the same action frame on the upper right side through the icon **[ ]** in "real time", and sent by "E-mail" or by "SNMP Trap", when enabled.

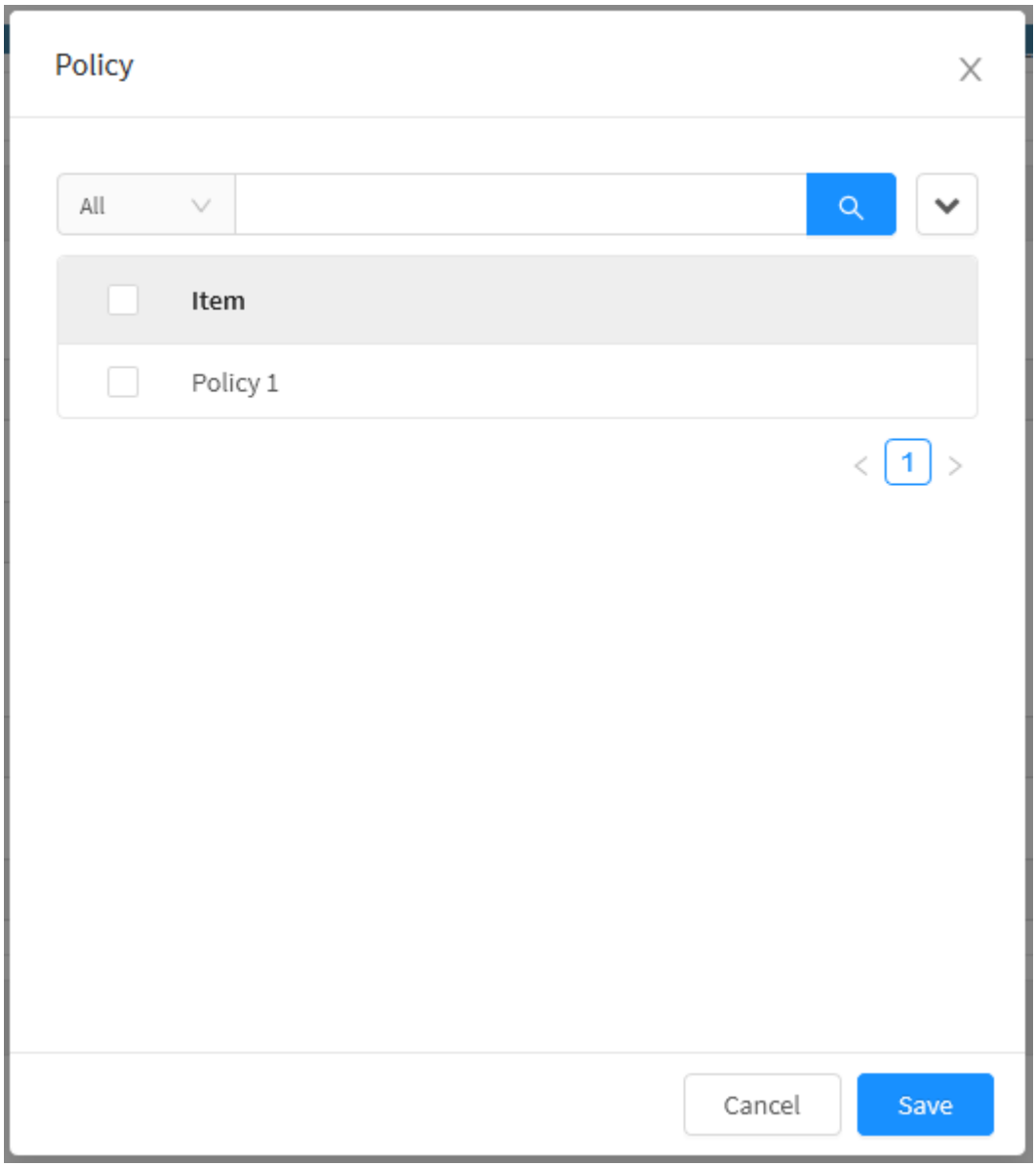
Policy security notifications will only be generated if logging is enabled on the same.



Administration - Security Notifications

In the case of security notifications, the administrator selects among the specific activities for each case: *“Policy Activities”*, *“Intrusion Detection Activities”*, *“Threat Detection Activities”*, *“Application Activities”*, *“Web Categories Activities”* and *“Malware Activites”*. Below is an example of how to make this selection:

By clicking on the **[** **]** icon in Policy Activities the screen below will be displayed:



Administration - Policy Activities

When selecting a specific policy, when there is any activity related to it, the system will trigger a **notification [** **]**.

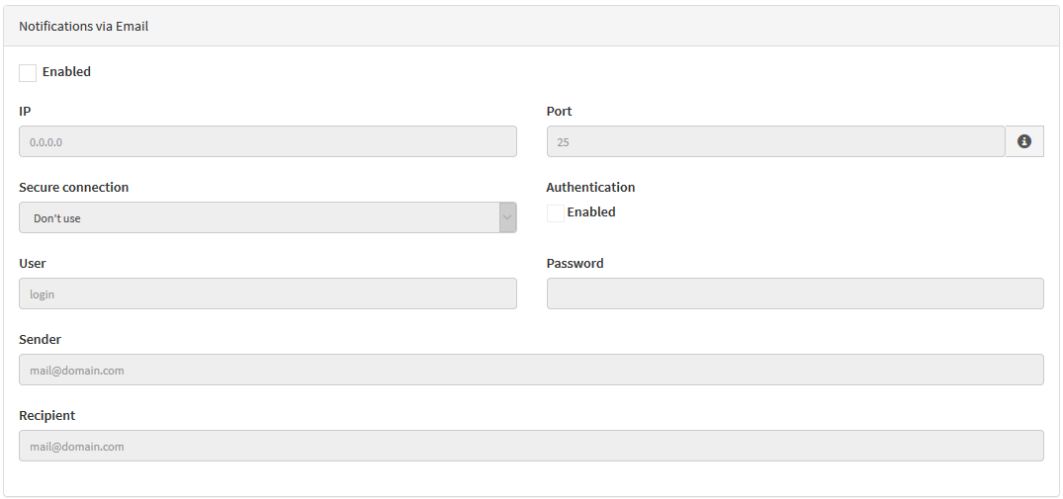
To complete the configuration, click on **[** Save **]** if you want to close this window without making any changes, click on **[** Cancel **]**.

The system includes two resources for sending **“Notifications”**:

- *Notifications via Email*;
- *Notifications via SNMP*.

Notifications via Email

In the Notifications via Email box, you can configure the system for sending email notifications to an exclusive administrator, determined by the recipient's address. These notifications are the same as those returned in real time, alerted via the top right menu by the **[ ]** icon.



Administration - Notifications via Email

- ***Enabled [ ]*:** To enable the service;
- ***IP*:** Inform the email server IP;
- ***Port*:** Inform the port on which you will connect to the SMTP server. Ex.: 587;
- ***Secureconnection*:** Inform the type of encryption of the connection. Eg SSL / TLS;
- ***Authentication [ ]*:** Inform whether the connection will be authenticated or not;
- ***User*:** If the authentication option is enabled, inform a user to authenticate with the email server. Ex.: admin@blockbit.com;
- ***Password*:** If the authentication option is enabled, enter a password to authenticate to the email server;
- ***Sender*:** Inform a valid sender to which the notifications will be forwarded, this address must exist in the remote server's mailing list. Ex.: notifications@blockbit.com;
- ***Recipient*:** Inform the recipient to receive notifications. Ex.: administrator@blockbit.com.

You can configure the system to use a “local” or “remote” email server, if you want to receive email notifications, configure the service and click **[ ]**.

If your email account has MFA activated, you will need to disable it or configure for not use by applications only. Check with your email provider.

For more information about notifications, click on this page.

If you want to know about SNMP notifications, click on this page.

Notifications via SNMP

In the Notifications via SNMP frame it is possible to configure the system for sending notifications by SNMP trap. Unlike an SNMP data collection service, a “Trap” is a notification service initiated by the monitored server, this initiates the communication and delivery of alerts to the remote SNMP server. The service supports communication with SNMP v1, SNMP v2 and SNMP v3 protocols.

Next, we will provide some details about the differences between the SNMP protocol versions.

- ***SNMP v1***

The first version of SNMP has an extremely fragile authentication scheme, its only security mechanism being "community names". These represent a management group with specific permissions, that is, the assignment of the rights to use SET and GET instructions on a given parameter to members of this community. The storage of these names is local, that is, each agent that implements SNMP must register the permissions given to each management community that can make use of its parameters.

It is important to note that permissions are given to a particular community, not specific management stations, in fact, there is no listing of members of a community.

The "authentication" of an NMS “Network Management Station” is done through the declaration, sent in text format, of the name of the community to which it belongs. The NMS, therefore, must maintain a list of the relevant community names for each agent in the network. To simplify the management task, there is a tendency to maintain a certain uniformity in the management groups registered in the various entities of the network, but this is not mandatory.

The main flaw of this security model lies in the fact that anyone who knows the community name with the appropriate privileges can send an SNMP command over the network. To make matters worse, as there is no privacy in SNMP v1, information about community names is sent in text form and without encryption in UDP messages that travel over the network, it is extremely simple for an attacker to intercept these names and relate them to stations which are destined.

Given this total insecurity generated by the combination of the lack of privacy with the simple and decentralized authentication model, almost all implementations of this version of SNMP in production systems disable the SET instruction, and restrict the parameters accessible by the GET instructions to non-confidential information. This attitude greatly limits the functionality of the protocol, but at the same time guarantees security in environments where it is essential.

- ***SNMP v2***

Originally, a reform of the SNMP security model was part of the goals in creating the second version of the protocol. SNMPv2 (RFC 1901, 1996) emerged to address some of the shortcomings of SNMPv1.

Added at least two new functions:

- Get-bulk-request: Access to large blocks of information in the MIB;
- Inform-request: Allows a manager to send relevant information directly to other managers;
- Among the novelties of SNMPv2, the highlights are:
    - Management of decentralized networks, allowing the existence of more than one management station and, consequently, the exchange of information between them;
    - Possibility of transferring large blocks of information;
    - Introduction of 64-bit counters, enabling better monitoring of variables that reach their limits quickly with 32-bit counters;
    - Improvement in error handling of variables, defining the success or error status of the operation for each PDU variable and no longer for the PDU. Thus, if one variable contains an error, the others will not be sacrificed, being the variable field in that the problem occurred filled with an error code.

The final version of the protocol that was standardized was version 2c, which despite introducing new features such as the “GetBulkRequest” instruction, did not make any changes to the protocol's security model and the model based on community names remained.

- ***SNMP v3***

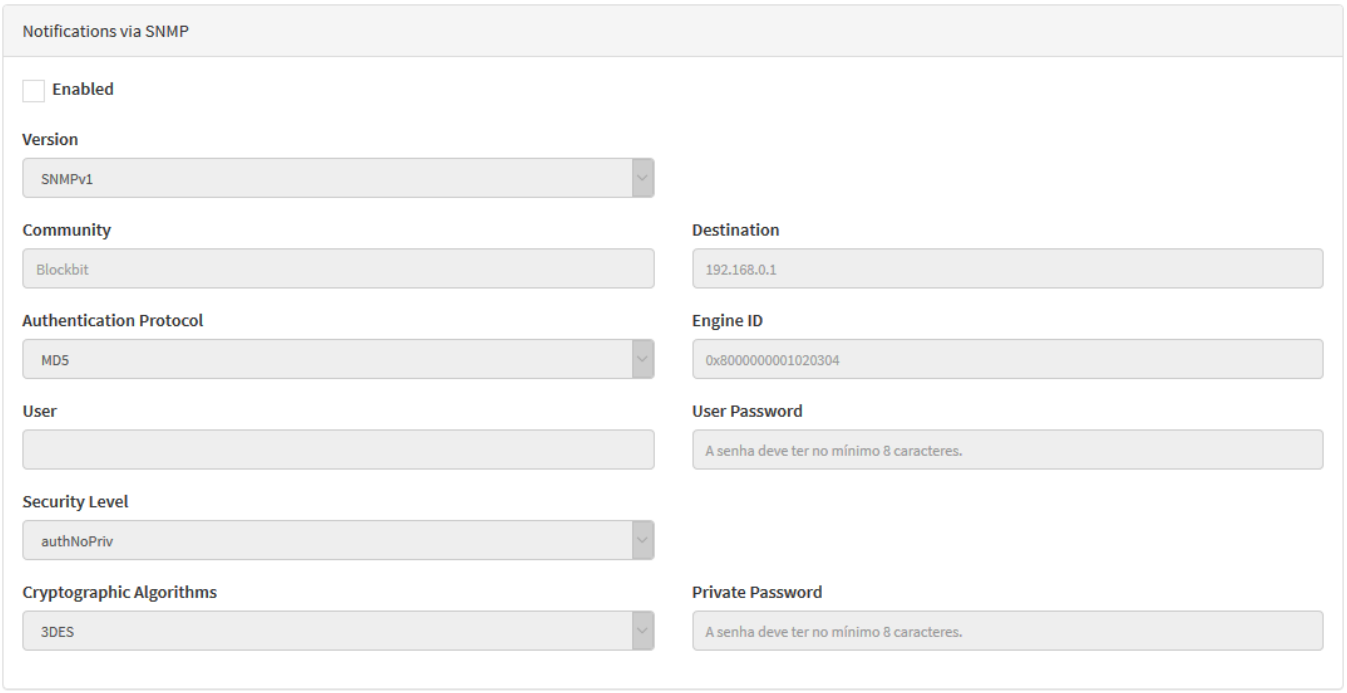
This version of the protocol was mainly focused on improving the security offered by previous versions of the SNMP protocol. Mechanisms have been developed to address each of the security flaws discussed so far. In this way, it became possible to use the full potential of the protocol, including SET instructions, without compromising network security. The new security model guarantees confidentiality, integrity, authentication and access control.

Generally speaking, the effective PDU that carries the SNMP instruction (either SNMPv1 or SNMPv2) is encapsulated in an SNMPv3 PDU. This operation provides security-related functions at the message processing level. For this communication to be effective, both the management station and the agents must be using the same SNMP engine.

The two main modules of the SNMP v3 security model are the User-based Security Model (USM) and the View-based Access Control Model (VACM). The USM is in charge of authenticating, encrypting and decrypting SNMP packets, while the VACM is in charge of managing access to data in the MIB.

To send notifications via SNMP Trap, access the panel shown below and configure according to the interface fields and configuration parameters of the remote SNMP server and the version of the protocol in use.

To configure notifications, access the System menu, select the Administration option and on the Settings tab configure the Notifications panel via SNMP TRAP.



Administration - Notifications via SNMP

Initially, enable notifications via SNMP by checking the Enabled **[** **]** checkbox;

- ***Version*****:** Inform the version used by your SNMP server. The available options are SNMP v1, SNMP v2 and SNMP v3. Ex.: *SNMP v2*;
- ***Community*****:** Inform the community that has been configured on the SNMP server. This field will only be available in SNMP v1 and SNMP v2 versions. Ex.: Blockbit;
- ***Destination*****:** Inform the SNMP server IP. Ex.: 172.16.102.52;
- ***Authentication Protocol*****:** Inform which encryption method will be used, this feature is only possible for SNMP v3. Ex.: *MD5*;
- ***EngineID*****:** Inform which SNMP mechanism will be configured based on what was configured on the SNMP server, this feature is only possible for SNMP v3. The Engine ID is a mechanism that serves as a unique identifier for the agent. The Engine ID is used with a hash function to generate keys for authentication and encryption of SNMP v3 messages;
- ***User*****:** Inform a user to perform authentication on the remote service;
- ***User Password*****:** Enter a password for user authentication on the remote service;
- ***Security Level*****:** Inform the security level in the remote service, which can be authenticated privately or not (non-private authentication);
- ***Cryptographic Algorithms*****:** Inform the encryption algorithm that has been configured on the remote server for authentication;
- ***Private Password*****:** If the Security Level is configured as AuthPriv, it is necessary to configure the private password for the connection.

The Authetication Protocol, Engine ID, User, Password, Security Level, Cryptographic Algorithms, Private Password fields will only be enabled for completion, if the version chosen in the Version for SNMP v3 field.
In turn, if the selected version is SNMPv3, the Community field will be disabled.

Then click **[** **]** to save.

After making the settings, the notifications that occurred will be displayed by clicking on the notifications button **[** **]** located at the top of the screen.

For more information about notifications via Email, click on this page.

If you want to know about Blockbit MIBs, click on this page.

Finnaly, click here to get more information about Zabbix.

Blockbit MIBs

The SNMP (Simple Network Management Protocol) is a series of parameters used for the administration, capture, ordering and editing of the information of the devices managed in the network, the SNMP protocol is capable of monitoring the network and after capturing the management data, orders them in a MIB (Management Information Base), explaining the current conditions in which the system is.

The MIB is a database that groups the management information of an object within a network, being hierarchically ordered in order to define the properties of the data sets belonging to the administered device, the MIB hierarchy is composed of OID (Identifiers of Object) that, briefly, represent the characteristics of the device administered.

To use MIBs it is necessary to have an SNMP manager and add Blockbit MIBs to the databases.

The following table shows the Blockbit MIBs and a brief description of their function:

Blockbit MIBs

MIB name	*SNMP OID*	Description
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."AUTHSESSIONS"	1.3.6.1.4.1.8072.1.3.2.4.1.2.12.65.85.84.72.83.69.83.83.73.79.78.83.1	Displays the amount of simultaneous authentications.
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."CONNSESSIONS"	1.3.6.1.4.1.8072.1.3.2.4.1.2.12.67.79.78.78.83.69.83.83.73.79.78.83.1	Displays the amount of simultaneous connections.
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."SERVICES"	1.3.6.1.4.1.8072.1.3.2.4.1.2.8.83.69.82.86.73.67.69.83	Displays the current status of UTM services.
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."DHCPLEASES".1	1.3.6.1.4.1.8072.1.3.2.4.1.2.10.68.72.67.80.76.69.65.83.69.83.1	Collect the quantity of IPv4 DHCP leases.
MIB::nsExtendOutLine."DHCPLEASES".2	1.3.6.1.4.1.8072.1.3.2.4.1.2.10.68.72.67.80.76.69.65.83.69.83.2	Collect the quantity of DHCP IPv6 leases.
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."TRAFFICSUM".1	127.0.0.1.1.3.6.1.4.1.8072.1.3.2.4.1.2.10.84.82.65.70.70.73.67.83.85.77.1	This query returns the total RX throughput of all network interfaces.
NET-SNMP-EXTEND-MIB:: nsExtendOutLine."TRAFFICSUM".2	127.0.0.1.1.3.6.1.4.1.8072.1.3.2.4.1.2.10.84.82.65.70.70.73.67.83.85.77.2	This query returns the total TX throughput of all network interfaces.

For more information on SNMP Notifications, visit this page.

Finally, click here for more information about Zabbix.

Zabbix

Zabbix is an open source, real time resource monitoring system. It collects data from monitored devices at regular intervals and tests avaliability and performance using triggers that can be configured. These data are compared to those in a data bank and then, graphics and reports are generated.

Templates' Download

Name	Link
Blockbit NGFW Template for SNMP	6.4 to 7.0
Blockbit Services Monitor	4.3 to 6.0

To configure SNMP monitoring, run the command:

```
enable-snmp
```

For more information, check [enable-snmp].

After configuring, you can access the Dashboard.

For more information about Zabbix, visit Dashboard (zabbix.com).

To create the Dashboard with the Blockbit NGFW template, Zabbix collects the following data:

- **CPU:** percentage of processing power being used.
- **Memory:** percentage of memory being used.
- **Disk:** percentage of disk being used.
- **Serviess:** services' statuses.
- **Bandwidth use:** traffic at the moment .
- **Link avaliability:** Link status.

Blockbit NGFW also send SNMP notifications:

To get SNMP notifications, first enable the SNMP Trapper at Zabbix.

- **Licence:** Licence expiration.
- **Backup:** last backup status.
- **System:** Databases and system status.
- **Synchronism:** synchronism with Domain Control.
- **SD-WAN:** Link avaliability.
- **High Availability:** Changes in High Avaliability cluster services.
- **GSM Analyzer:** GSM Analyzer communication status.
- **VPN monitor:** VPN status.
- **Update:** Update status.

System - High Availability Tab

The Blockbit NGFW natively supports the *High Availability* feature (H.A) maintaining an “Appliance” in “backup” mode that goes into operation quickly in the event of failure with the “PRIMARY DEVICE”, which minimizes downtime.

This feature aims to meet the condition of a "Fault Tolerance" and "availability" system that refers to capacity in a network environment of the system in H. A mode, in order to accept connections and function normally in a transparent manner to the end user, even when one or more of the “PRIMARY” device components are not operational.

The Blockbit NGFW High Availability feature requires two (2) devices, preferably identical, configured to provide a reliable and seamless connection between networks. The H.A system implies redundancy, synchronism and includes a failover mechanism, among other characteristics.

When using different devices, it is important to keep in mind the physical and performance differences.

- ***H.A. Active/Active***

As all network traffic must pass through the firewall, it is extremely necessary that the traffic flow remains uninterrupted.

Even in the event of an interruption on the primary device's functioning, whether due to a hardware, software, or network failure, the active secondary device automatically becomes the primary device preventing the loss of connection of directly connected services.

In an Active/Active system the handling of packet flow traffic is considered indispensable, in order to guarantee the persistence of the users' authentication session and the control of the sessions of the states of the TCP and UDP connections.

The H.A Active / Active synchronization process is responsible for synchronizing the system settings, authentication sessions and the connection states of the device, which ensures a reliable and continuous connection between networks.

In cases of unavailability of the “Primary Active H.A.” device, the “Secondary Active H.A.” takes over ownership of the network sessions and requests in a transparent manner without "overburden" or loss of services.

In the process of reestablishing the Primary HA, the device interacts through the Heartbeat interfaces with the Secondary HA device, applies a reverse synchronization of the system settings, updates the authentication session tables and connection controls and resumes ownership of the sessions, thus providing a session's ownership. Resilient, scalable and easy to manage solution.

- **Hardware redundancy (*Failover*)**

When a resource on the primary device fails, the secondary must take over operational functions, transparently to users. For greater performance and reliability, we use the CARP protocol.

The Multiple CARP IP addresses service refers to an implementation of the Common Address Redundancy Protocol (CARP) that allows the use of multiple virtual network interfaces with CARP IP addresses. CARP is a networking protocol used to achieve high availability and failover in computer networks. It allows multiple hosts to share a virtual IP address, with one host acting as the active node and the others acting as backup nodes.

Some of the biggest advantages are:

  - Fast and efficient failure detection;
  - Monitoring of all network interfaces;
  - Balance avoiding overload of a single node;
  - Sharing the same virtual IP;
  - Flexibility and scalability in the configuration of each node.

- ***Heartbeat Interface***

The monitoring and synchronization processes of the system data are applied through a dedicated network interface called “*Heartbeat*”.

Due to the monitoring and synchronization processes being applied through a “heartbeat interface” (dedicated), it is important to consider the possibility of failures in the communication network and not in the device, therefore, the system allows configuring a “redundant heartbeat” interface, that is, in case of communication problems on the primary interface, the system performs the tests and synchronism through the secondary heartbeat interface.

- **Fault detection**

Responsible for monitoring devices, ensuring availability between the two devices (gateways), and detecting possible failures, whether due to equipment damage or imperfections in communication through the “Heartbeat” monitoring interfaces.

- **Settings sync**

Synchronization process of the configuration files, it ensures that the secondary device is configured and updated when the primary device fails.

- **User session persistence**

Synchronization process of user authentication sessions. Ensures continuity of connections in the failover process between H.A devices.

- **Connection session persistence**

Synchronization process of network traffic connection status sessions. Responsible for ensuring the continuity of connections in the failover process between H.A devices.

- **Log shipping and notifications**

Service of notifications and alerts of the H.A. service's occurrences.

- **Service Level Agreement**

The cluster availability SLA is of 99.98%.

- **Primary server reintegration (*Failback*)**

The reintegration of the primary device is simple and automatic.

When restarting the primary (inactive) device connected to the network through the switch, the monitoring service must verify the existence of any configuration to be synchronized with the secondary (active) device. After synchronization, the same failover process is performed, in which the secondary device interfaces must be disabled, that is, it changes its status back to “stand-by” and rehabilitates the network interfaces on the primary device, making it “Active” again.

 The VRRP protocol (Virtual Router Redundancy Protocol) *RFC 3768 e RFC 2787 is supported in all of the Blockbit models.

For more information regarding the H.A. setting, check the *H.A. Configuration - Primary Device* page.

Important considerations in H.A. mode

In this chapter we will cover some relevant information regarding the implementation of the H.A. mode in Blockbit UTM.

Secondary server activation time

The total “FailOver” time, that is, activation of the secondary device in the event of failure of the primary device depends on several factors:

- Failover interval time (x) No. Failure detection;
- Routing convergence time.

The total time depends on the network topology implemented in the H.A environment, the number of network interfaces, the types of network protocols implemented, the number of static and dynamic routes. It is not possible to determine an exact time for activation of the secondary H.A. device.

H.A. devices connected to layer 2 switches

If HA devices are connected to layer 2 switches, you must enable the STP - Spanning Tree Protocol (802.1D) protocol on all layer 2 switches connected to HA devices (PRIMARY and SECONDARY) in order to avoid “Possible loops” in network traffic.

However, when the STP - Spanning Tree Protocol is enabled on a switch port, it does not immediately allow network traffic through that port, rather the protocol switches between some statuses until determining the network topology and this causes a delay in routing traffic.

In tests, it has been identified that the STP delay can reach up to 50 seconds. In the case of activation of the secondary device, the activation time may be longer than 1m: 30s. (1 minute and 30 seconds).

There are some switch models that already implement a more updated version of the STP protocol, the RSTP - Rapid Spanning Tree (802.1w) which significantly reduces the time to identify the network topology, which includes the detection of loop more quickly.

It is recommended to consult the switch manufacturer's documentation on how to configure the STP or RSTP protocol.

Enabling and configuring the RSTP protocol on the switch ports connected to the H.A devices avoids looping and reduces the “FailOver” activation time of the secondary H.A. device.

H.A. devices connected to layer 3 switches

If H.A. devices are connected to layer 3 switches, after a “FailOver”, that is, activation of the secondary device, layer 3 switches may not be able to successfully route traffic.

Layer 3 switches can maintain the ARP table for a relatively long time after “FailOver”, which can cause the list of IPS addresses and corresponding MAC addresses to not be updated for each switch port connected to HA devices, this is because the table is not updated by special ARP packages. As a consequence, traffic “freezes” and the H.A. does not work.

To solve this problem, it may be necessary to decrease the update time of the ARP table of layer 3 switches.

Network topology - H.A. mode

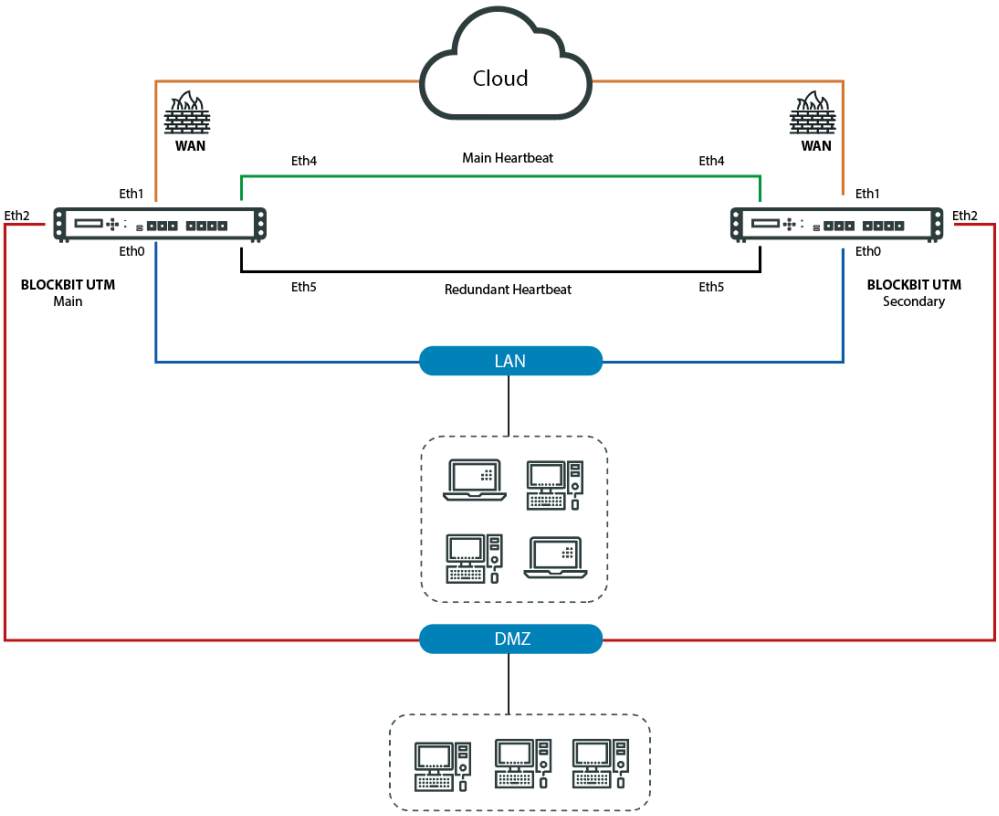
Initially, it is important to define what the physical topology of the network will look like before implementation, in order to properly adapt the installation and configuration of the network interfaces of Blockbit UTM devices in H.A. mode.

We must consider the previous notes, remembering that: To make the H.A. service available, the system requires at least a "heartbeat" interface dedicated to the "FailOver" tests.

It is important that this structure is documented with physical and logical notes according to the topology defined in the structural documentation of the network.

To implement the H.A. mode, it is imperative that the Appliances have the same hardware model and are properly licensed.

Implementation model:



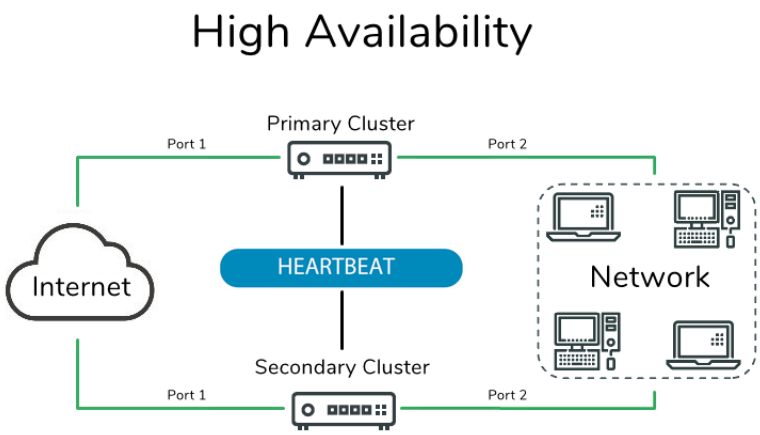
Network topology - H.A. mode

Example - H.A. Configuration

This section will walk you through setting up a primary and secondary server using Active-Passive H.A.

For more information about H.A. see this page.

This demonstration will take into account the following structure:



High Availability - Structure

The following IPs will be used in this example:

High Availability - IP Addressing

Name	IP adress	Heartbeat
Primary Cluster	172.31.170.20	100.100.100.1
Secondary Cluster	172.31.170.21	100.100.100.2

The steps we will take in this demonstration will be:

1. Primary Cluster Configuration;
2. Secondary Cluster Configuration and Synchronization;
3. Validation of H.A. Settings.

We will start the demonstration by configuring the Primary Cluster interfaces.

H.A. Configuration - Primary Device

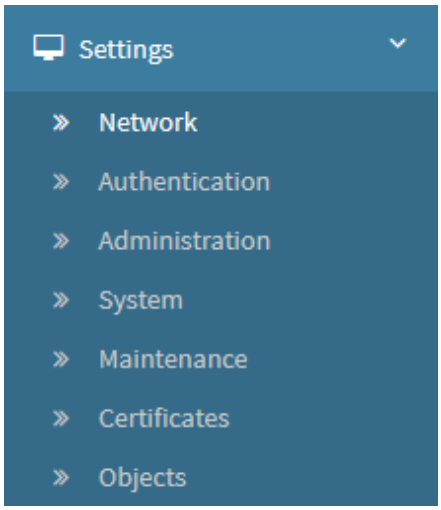
First of all, the Primary Device must be properly licensed with the Secondary Device registered as Appliance H.A on the license server and that an interface of each NGFW is connected, in order to isolate the heartbeat (which will be used in the synchronism of the H.A) between the two devices.

In this example we will make the following settings:

- Configuração da interface física e interface virtual para gerenciamento do nó do cluster; Configuration of the physical and virtual interfaces for the cluster node's management;
- Configuration of the heartbeat interfaces as the communication with the secondary cluster's IP needs to be functional for the heartbeat to be effective;
- Primary device configuration.

Interface Configuration

Initially, access the Settings menu and click on Network:



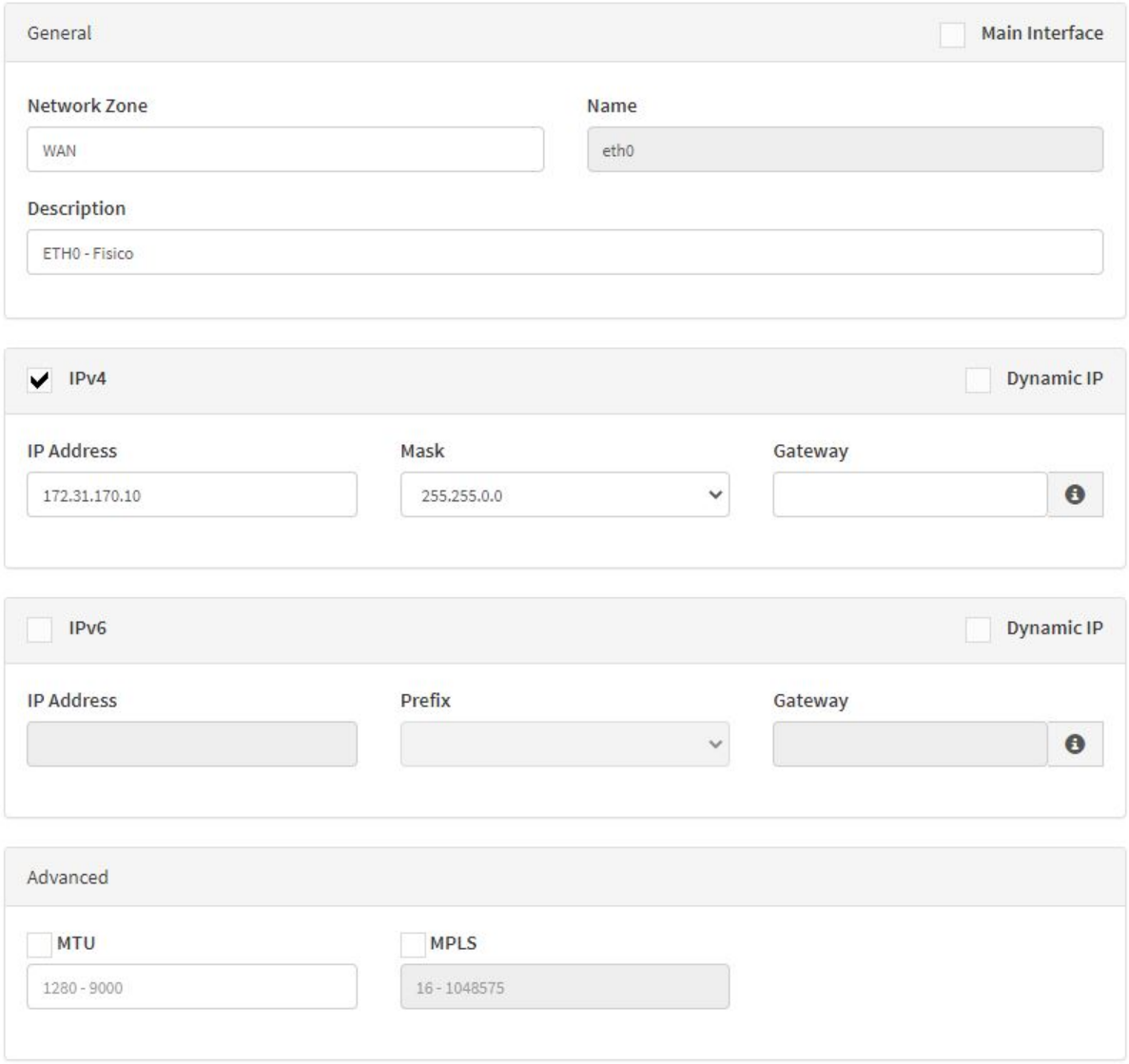
Settings - Network

Click on the Interfaces tab:

Interfaces tab

Some details of the interfaces tab will not be considered in this example, if you want more information, see this page.

Configure your network as needed, in this example eth0 was configured as follows:

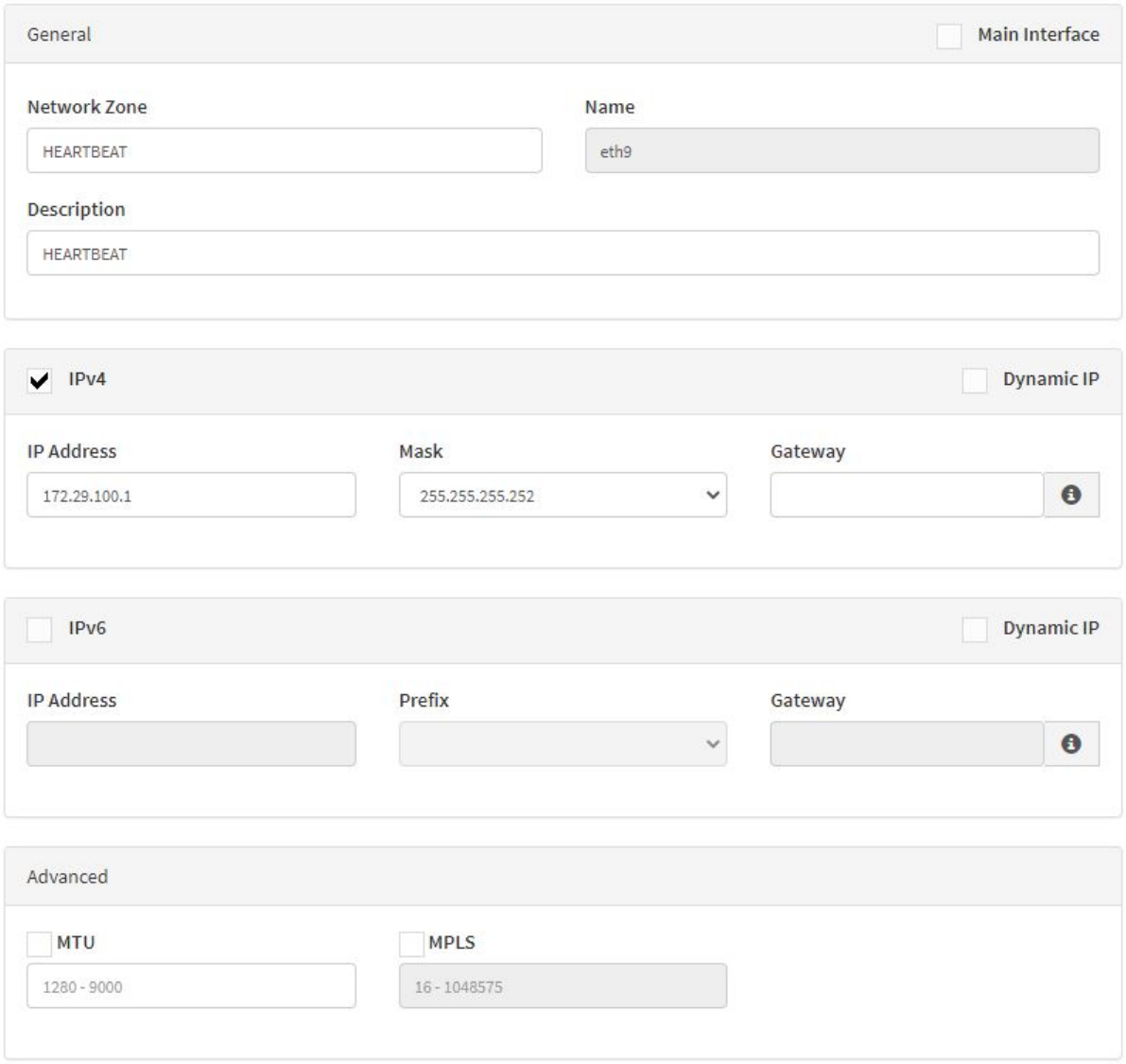


Eth0 settings

- **Main Interface [✔]:** When this box is checked, it defines the interface as "main";
- **Network Zone:** We will define the zone as WAN;
- **Description:** We will add a standard description. Ex.: Local Network;
- **IPv4[✔]:** Check this checkbox to enable the fields below;
- **IP Address:** The IP address used by the interface. Following the topology, the IP will be 172.31.170.10;
- **Mask Address:** The mask used by that IP address will be *255.255.0.0.*

Click **[ ]** to save the settings:

Configure a virtual network or Alias, which will be used on the settings of the nodes listing, in this example the eth1:0 has been configured as follows:

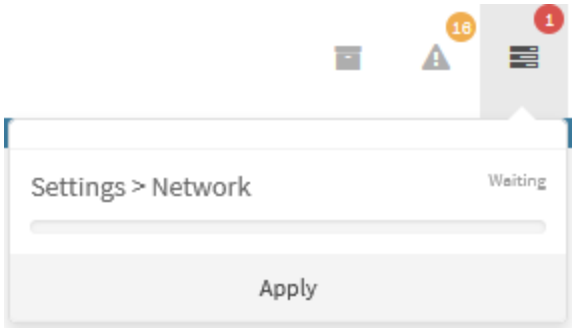


eth1:0 settings

- **Main Interface [✔]:** When this box is checked, it defines the interface as "main";
- **Network Zone:** We will define the zone as CLUSTER;
- **Description:** We'll add the description. Ex.: Cluster Interface;
- **IPv4[✔]:** Check this checkbox to enable the fields below;
- **IP Address:** The IP address used by the interface. The IP address used by the interface 172.29.100.1;
- **Mask Address:** The mask used by that IP address will be *255.255.255.252*.

Click **[** 💾 **]** to finish the settings:

When finished, activate both interfaces by clicking **[** 🔘 **]** and applying to make the settings:



Apply Queue - Apply

The screen below shows the Primary Cluster interfaces already configured and correctly enabled:

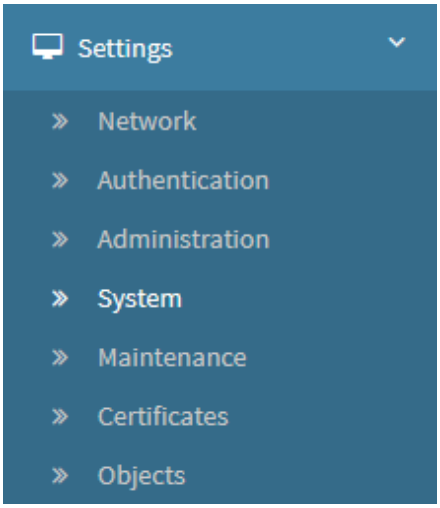
Interface	Address	Gateway	Type	Zone	Action
eth0	172.31.170.10/16	-	Physical	WAN	
eth1	10.10.10.1/24	-	Physical	LAN	
eth1:0	10.10.10.3/24	-	Alias	-	
eth2	10.189.253.1/24	-	Physical	WAN	
eth2v0	10.189.253.3/24	-	Virtual	LAN	
eth3	10.189.253.234/29	-	Physical	LAN	
eth4	-	-	Physical	-	
eth5	-	-	Physical	-	
eth6	-	-	Physical	-	
eth7	-	-	Physical	-	
eth8	-	-	Physical	-	
eth9 Main Interface	172.29.100.1/30	-	Physical	HEARTBEAT	

Network Settings - Interfaces

Next, we'll cover the cluster's H.A. settings:

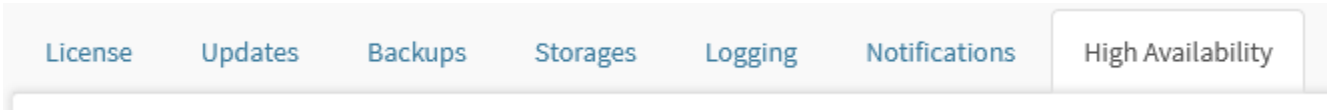
H.A. Settings

Access the Settings menu and click on the *System* option:



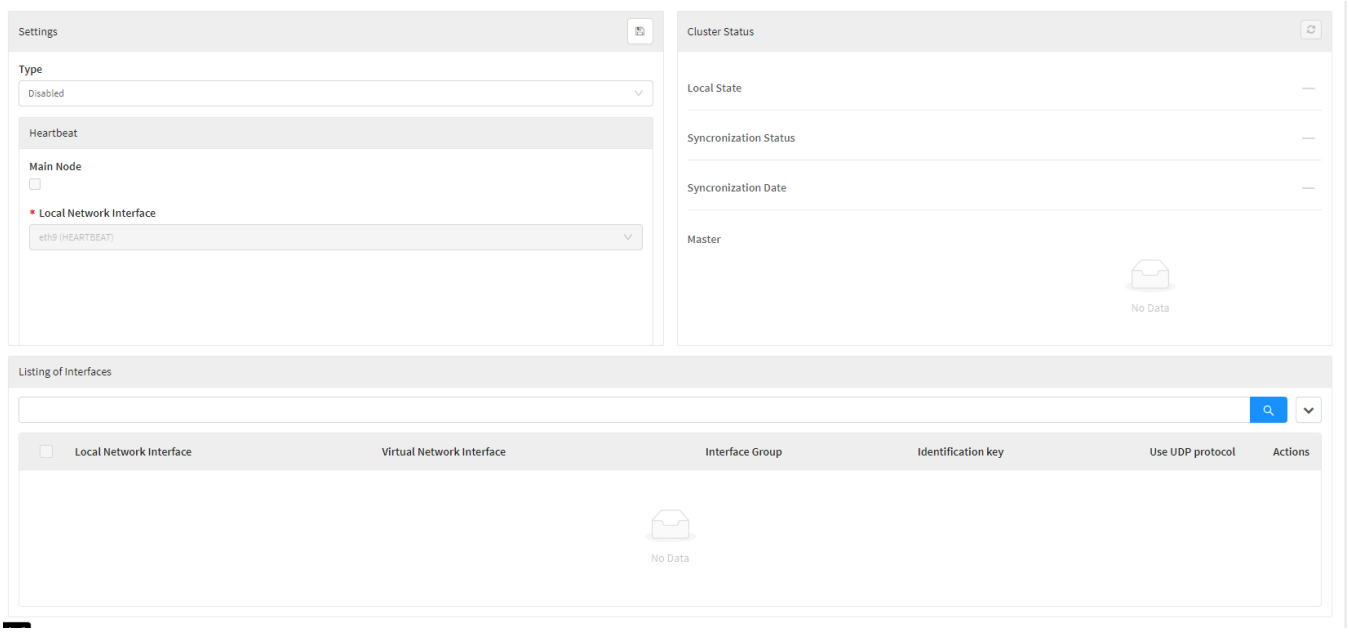
Settings - System

Click on the High Availability tab:



High Availability Tab

The following screen will be displayed:

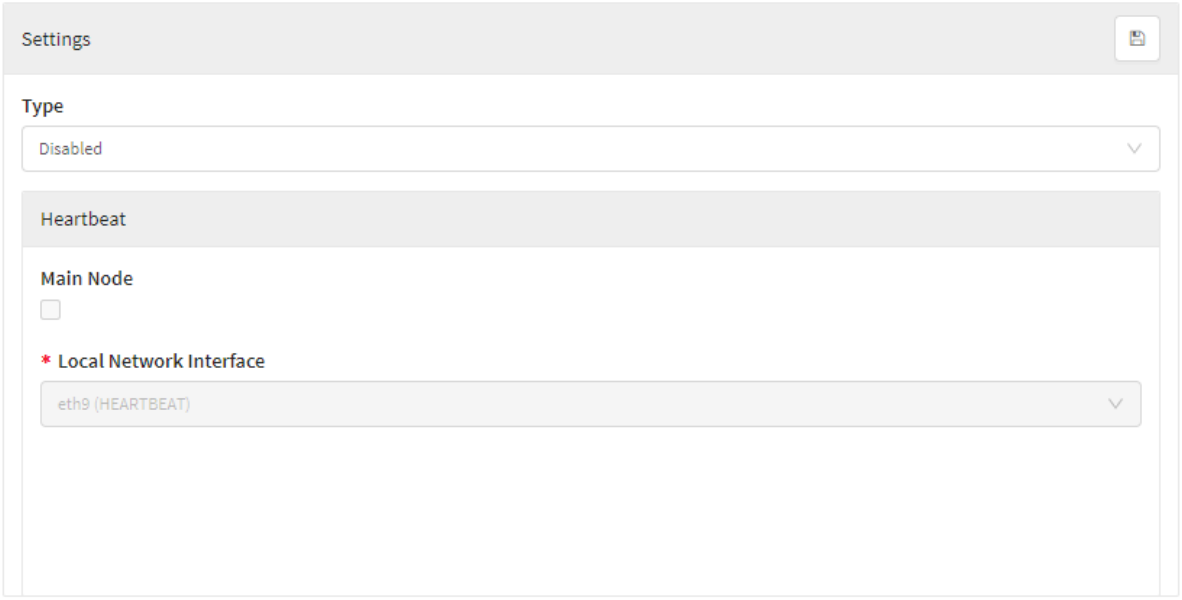


System - High Availability

Next we will detail the panels that we will need to configure.

Settings

Complete the form as shown below:



High Availability - Settings

- **Type**
  - **Disabled:** Service not set up for use.
  - **High Availability:** When selecting this option we enable the other fields to start the configuration.

Next, one configures the *Heartbeat*.

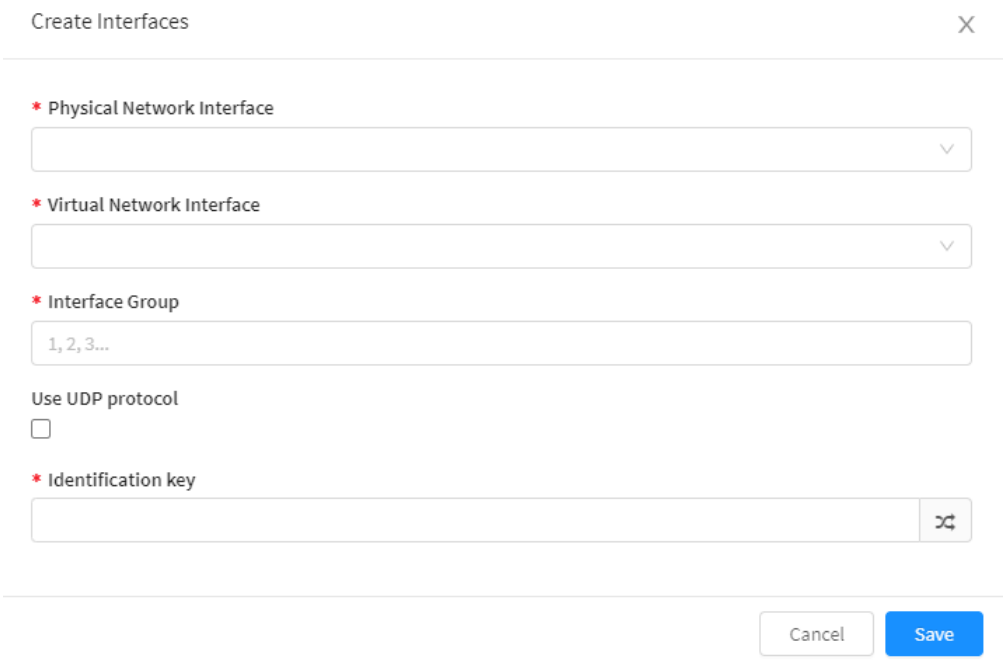
Heartbeat

- **Main Node**: Select this option only in the Primary Device [ ]
- **Local Network Interface**: Select the eth# network configured in *Interfaces as* the *Heartbeat* that will be used in the monitoring and sync process between the devices.

When finished, click on **[ ]** to save the settings, then click *Apply* in the command queue to conclude.

Interfaces' Listing

Click on [ ] ans select *Create Interface,* the following screen will appear.

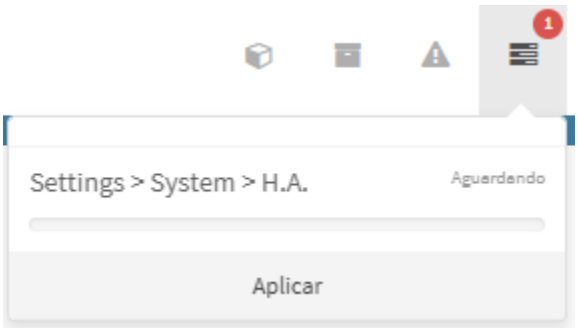


High Availability - Create Interfaces

- **Physical network interface**: Select a physical network..
- **Virtual network interface**: Select a virtual network or alias.
- **Interface group**: Select a group to segment the network.
- **Use UDP protocol**: Select [☐] this option.
- **Identification key**: Click on [⇄] to automatically generate an identification key or create a personalized key respecting the 46 characters limit.

Click on *save* [Save] to conclude the settings.

Open the *ApplyQueue* [1] and select *Apply* to conclude the settings.



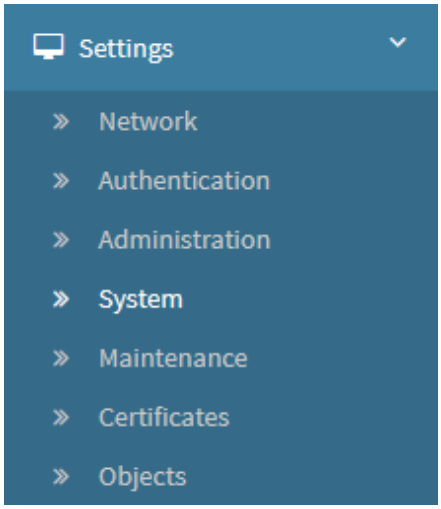
Apply Queue - Apply

These steps conclude the settings of the Primary Cluster, next, we'll analyze the settings of the Secundary Device.

H.A. Configuration - Secondary Device and Synchronization

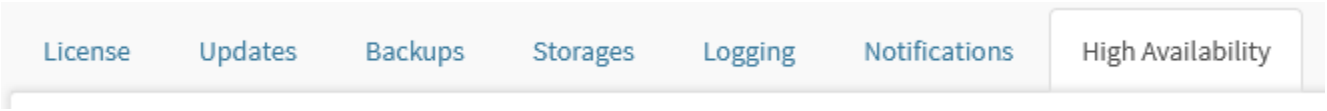
The configuration on the Secundary Device is done in the same way as the Primary Device .

Access the Settings menu and click on the *System* option:



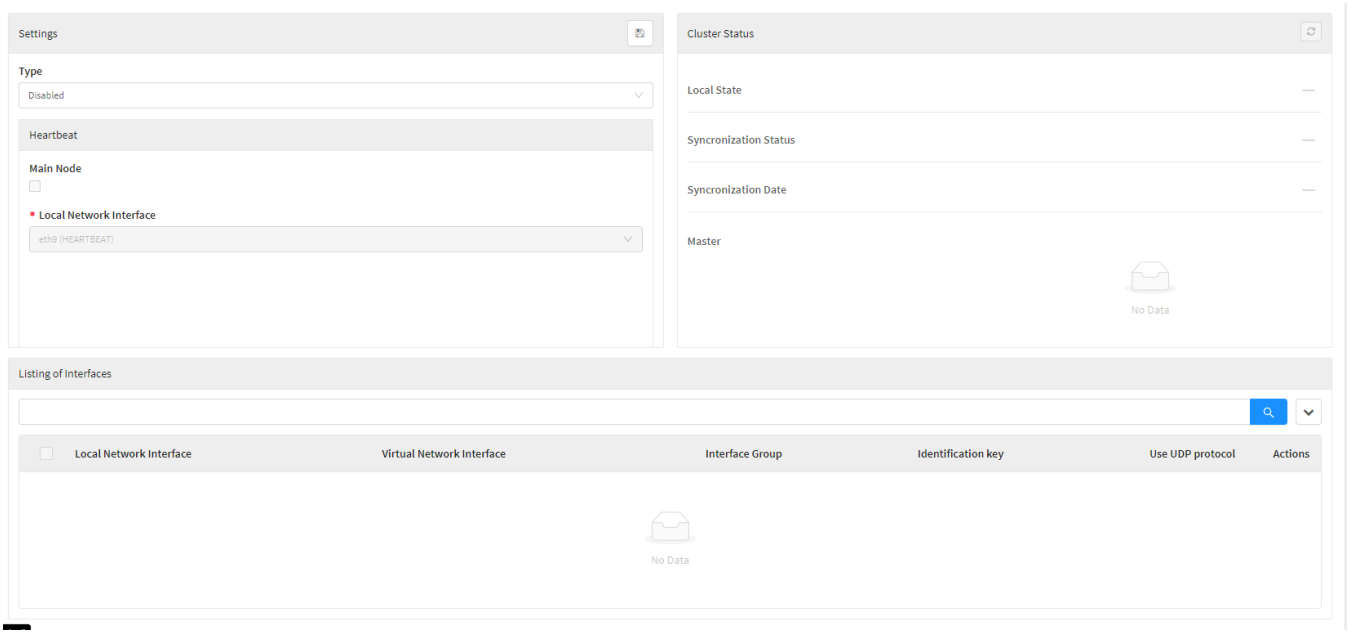
Settings - System

Click on the *High Availability* tab:



High Availability Tab

The following screen will be displayed:

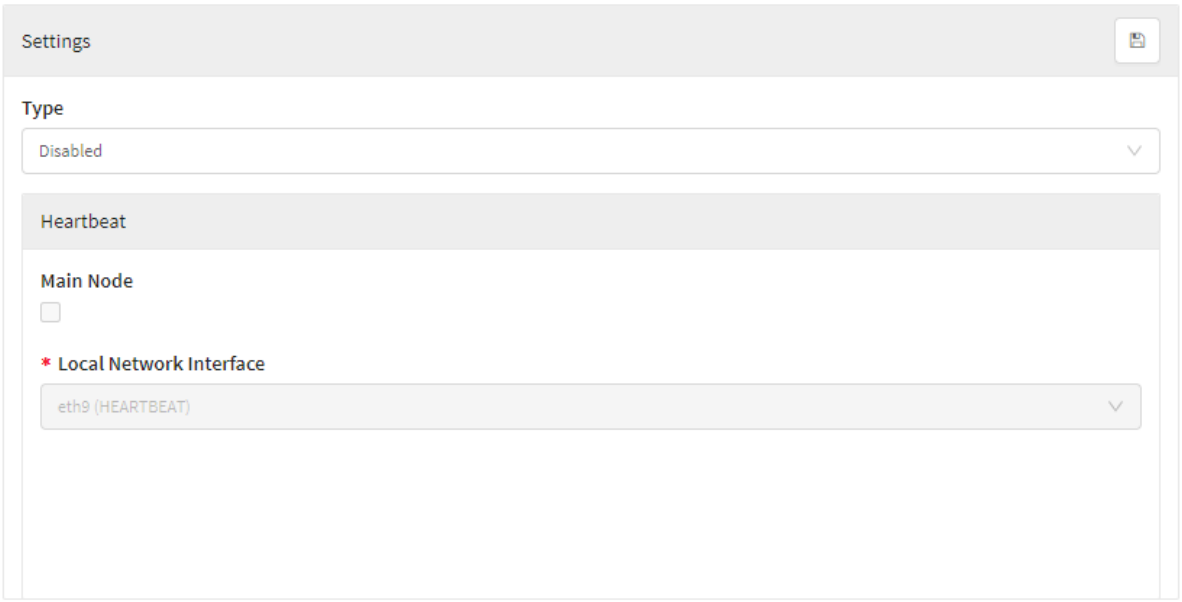


System - High Availability

Next we will detail the panels that we will need to configure.

Settings

Complete the form as shown below:



High Availability - Settings

- **Type**
  - **Disabled:** Service not set up for use.
  - **High Availability:** When selecting this option we enable the other fields for configuration.

Next, one configures the *Heartbeat*.

Heartbeat

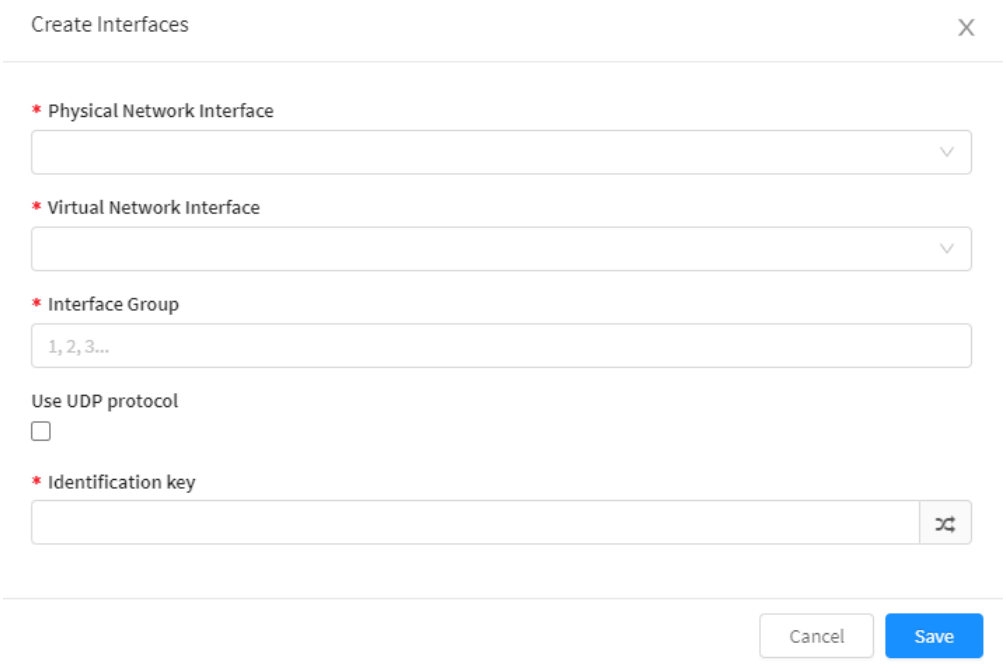
- **Main Node**: Do not check this box. [ ]
- **Local Network Interface**: Select the eth# network configured in *Interfaces as* the *Heartbeat* that will be used in the monitoring and sync process between the devices.

On the secundary cluster, the "Main Node" option **must not** be selected, only on the primary device .

When finished, click on **[ ]** to save the settings.

Listing of Interfaces

Click on [ ] ans select *Create Interface,* the following screen will appear.

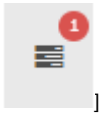


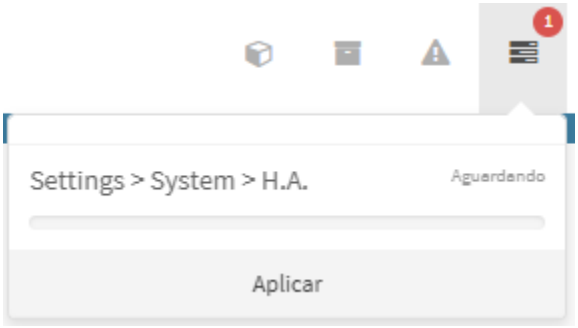
High Availability - Create Interfaces

- **Physical network interface**: Select a physical network.
- **Virtual network interface**: Select a virtual network or alias.
- **Interface group**: Select a group to segment the network.
- **Use UDP protocol**: Select [ ] this option.
- **Identification key**: Click on [ ] to automatically generate an identification key or create a personalized key respecting the 46 characters limit.

The information inserted must be exactly the same as the information configured on the primary cluster, except for the main node checkbox and the IPs addresses of the Heartbeat and VIP interfaces.

Click on *save* [Save] to finish the settings.

Open the *ApplyQueue* [] and select *Apply* to conclude the settings.



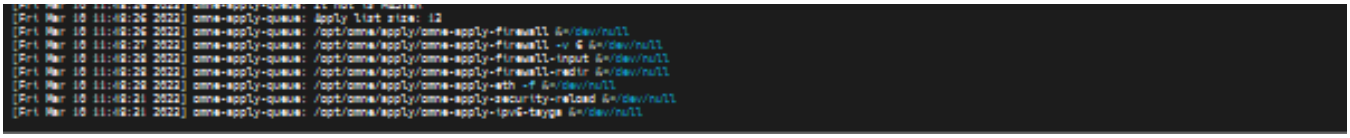
Apply Queue - Apply

Sync

After the Apply is completed, the devices will start syncing.

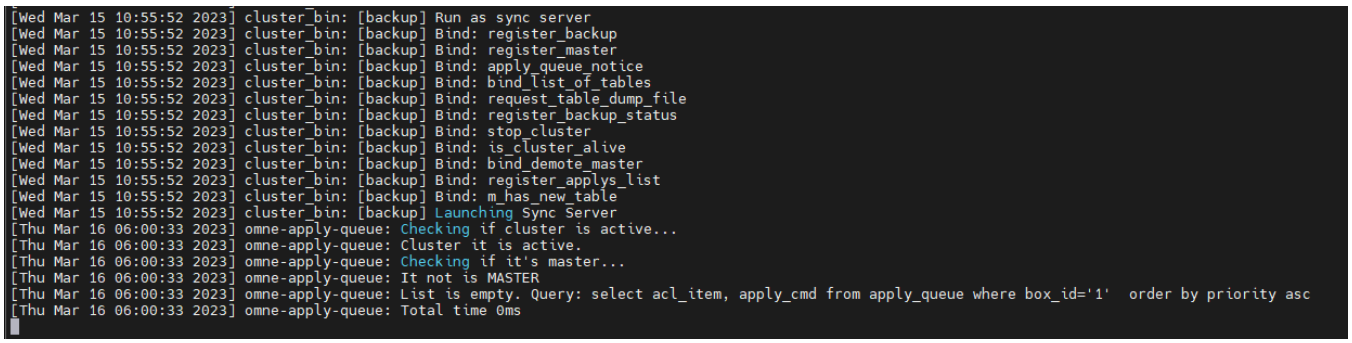
Access CLI in the secundary device and insert the command *debug-cluster -t*.


admin +debug-cluster -t
[Fri Mar 18 11:47:21 2022] cluster_bin: Start of cluster_bin - date/time at compile time: Mar 18 2022 12:17:42
[Fri Mar 18 11:47:21 2022] omne-apply-queue: /opt/omne/apply/omne-apply-cluster &>/dev/null
[Fri Mar 18 11:47:21 2022] omne-apply-queue: Total time 1161ms
[Fri Mar 18 11:47:21 2022] cluster_bin: Database is Okay!
[Fri Mar 18 11:47:21 2022] cluster_bin: heartbeat ip/mask: ["172.25.188.2/28"]
[Fri Mar 18 11:47:21 2022] cluster_bin: heartbeat interface name: eth3
[Fri Mar 18 11:47:21 2022] cluster_bin: Heartbeat ip: 172.25.188.2
[Fri Mar 18 11:47:21 2022] cluster_bin: Heartbeat mask: 28
[Fri Mar 18 11:47:21 2022] cluster_bin: Main Node: f
[Fri Mar 18 11:47:21 2022] cluster_bin: Saving Main Node status to: disable
[Fri Mar 18 11:47:21 2022] cluster_bin: Main Node saved as disable
[Fri Mar 18 11:47:21 2022] cluster_bin: Startup Ucarp
[Fri Mar 18 11:47:21 2022] cluster_bin: [ucarp] Looking for minor node interface
[Fri Mar 18 11:47:21 2022] cluster_bin: Minor Ucarp Interface is: eth1
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd begin
[Fri Mar 18 11:47:21 2022] cluster_bin: /usr/sbin/ucarp -i eth1:0 -s 10.10.10.2 -a 10.10.10.2 -v 100 -M -z -x 24_t -u /opt/omne/init/vip-up.sh -d /opt/omne/init/vip-dn.sh -p &vBSDHJ -0
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd end
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd begin
[Fri Mar 18 11:47:21 2022] cluster_bin: /usr/sbin/ucarp -i eth2v0 -s 10.185.252.2 -a 10.185.252.2 -v 200 -M -z -x 24_f -u /opt/omne/init/vip-up.sh -d /opt/omne/init/vip-dn.sh -p HaHiPKd -0
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd end
[Fri Mar 18 11:47:21 2022] cluster_bin: Start monitoring the status
[Fri Mar 18 11:47:21 2022] ucarp: [INFO] Local advertised ethernet address is [00:0c:29:f8:22:d1]
[Fri Mar 18 11:47:21 2022] ucarp: [INFO] Local advertised ethernet address is [9a:fa:2f:6a:6d:f1]
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Switching to state: BACKUP
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Spawning [/opt/omne/init/vip-dn.sh eth2v0 10.185.252.2 24_f]
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Switching to state: BACKUP
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Spawning [/opt/omne/init/vip-dn.sh eth1:0 10.10.10.2 24_t]
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] Ip [10.10.10.2] deleted : ip addr del 10.10.10.2/24 dev eth1:0
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] annunciato-20 has released 10.10.10.2/24
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth2v0] Ip [10.185.252.2] deleted : ip addr del 10.185.252.2/24 dev eth2v0
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] === BACKUP: annunciato-20 ===
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth2v0] Secondary interface. Status ignored!
[Fri Mar 18 11:47:21 2022] cluster_bin: [signal] Remote signal received
[Fri Mar 18 11:47:21 2022] cluster_bin: [signal] Node has been demoted
[Fri Mar 18 11:47:21 2022] cluster_bin: Keep Cluster Running
[Fri Mar 18 11:47:21 2022] cluster_bin: [backup] Start loop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: Clear table apply_queue_cluster
[Fri Mar 18 11:47:21 2022] cluster_bin: Clean table: apply_queue_cluster
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:22 2022] cluster_bin: Waiting for neighbors nodes to respond
[Fri Mar 18 11:47:22 2022] cluster_bin: try connect: /usr/bin/ping -I eth3 -w 1 -c 1 172.25.188.1 > /dev/null
[Fri Mar 18 11:47:22 2022] cluster_bin: Could not create file descriptor. client_fd: -1
[Fri Mar 18 11:47:26 2022] cluster_bin: 172.25.188.1 is alive
[Fri Mar 18 11:47:26 2022] cluster_bin: Finding Master
[Fri Mar 18 11:47:26 2022] cluster_bin: [bauckup] Register Master
[Fri Mar 18 11:47:26 2022] cluster_bin: Master registered as being ip 172.25.188.1
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Master Registered with Success
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Run as async server
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: register_backup
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: register_master
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: apply_queue_notice
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: bind_list_of_tables
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: request_table_dump_file
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: register_backup_status
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: stop_cluster
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: is_cluster_alive
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: bind_demote_master
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: register_applys_list
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Bind: m_has_new_table
[Fri Mar 18 11:47:26 2022] cluster_bin: [backup] Launching Async Server
[Fri Mar 18 11:47:26 2022] cluster_bin: Async Server launched with 1 threads
[Fri Mar 18 11:47:26 2022] cluster_bin: BackupDB begin
[Fri Mar 18 11:47:26 2022] cluster_bin: Backup Deleted
[Fri Mar 18 11:47:26 2022] cluster_bin: BackupDB: /usr/bin/pg_dump -U postgres brcconfig -b -c -t obj_addr -t box_net_device -t box_cluster_nodes -f /opt/omne/conf/cluster_restore_tables.sql
[Fri Mar 18 11:47:26 2022] cluster_bin: Database Restore File Found! File size = 1758#
[Fri Mar 18 11:47:26 2022] cluster_restorer: Launching cluster database restore service...
[Fri Mar 18 11:47:26 2022] cluster_bin: BackupDB ends
[Fri Mar 18 11:47:26 2022] cluster_bin: To Create Dictionaries Tables
[Fri Mar 18 11:47:26 2022] cluster_restorer: Waiting for restore signal...
[Fri Mar 18 11:47:26 2022] cluster_bin: Load Std Enabled Service List
[Fri Mar 18 11:47:26 2022] cluster_bin: __LoadEnabledServiceList__
[Fri Mar 18 11:47:26 2022] cluster_bin: service_list_size:1
[Fri Mar 18 11:47:26 2022] cluster_bin: Init Enabled Services List
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_firewall
[Fri Mar 18 11:47:26 2022] cluster_bin: End Enabled Services List
[Fri Mar 18 11:47:26 2022] cluster_bin: Calculating table lists
[Fri Mar 18 11:47:26 2022] cluster_bin: Calculating table lists end
[Fri Mar 18 11:47:26 2022] cluster_bin: Sending Status To Master...
[Fri Mar 18 11:47:26 2022] cluster_bin: Status was sent to master
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Sync start
[Fri Mar 18 11:47:26 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:26 2022] cluster_bin: trunc_tab_size: 226
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: Created Subscription settings_sync_1_brcconfig
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Waiting to sync 226 table(s)
[Fri Mar 18 11:47:26 2022] cluster_bin: Sync progress: 226/226/226
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Sync done! lines: 674
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Sync start done
[Fri Mar 18 11:47:26 2022] cluster_bin: Backup Deleted
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync start
[Fri Mar 18 11:47:26 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:26 2022] cluster_bin: trunc_tab_size: 2
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: Created Subscription settings_sync_1_brcvar
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Waiting to sync 2 table(s)
[Fri Mar 18 11:47:26 2022] cluster_bin: Sync progress: 2/2/2
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync done! lines: 12
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync start done
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Sync start
[Fri Mar 18 11:47:26 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:26 2022] cluster_bin: trunc_tab_size: 3
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: Created Subscription settings_sync_1_radius
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Waiting to sync 3 table(s)
[Fri Mar 18 11:47:26 2022] cluster_bin: Sync progress: 3/3/3
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Sync done! lines: 55
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Sync start done
[Fri Mar 18 11:47:26 2022] cluster_bin: Load NEW Enabled Service List
[Fri Mar 18 11:47:26 2022] cluster_bin: __LoadEnabledServiceList__
[Fri Mar 18 11:47:26 2022] cluster_bin: service_list_size:5
[Fri Mar 18 11:47:26 2022] cluster_bin: Init Enabled Services List
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_firewall
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_proxy
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_webcache
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_webfilter
[Fri Mar 18 11:47:26 2022] cluster_bin: Service found: service_snmp
[Fri Mar 18 11:47:26 2022] cluster_bin: End Enabled Services List
[Fri Mar 18 11:47:26 2022] cluster_bin: Loading service_firewall apply list
[Fri Mar 18 11:47:26 2022] cluster_bin: Running service_firewall apply list
[Fri Mar 18 11:47:26 2022] omne-apply-queue: Checking if cluster is active...
[Fri Mar 18 11:47:26 2022] omne-apply-queue: Cluster it is active
[Fri Mar 18 11:47:26 2022] omne-apply-queue: Checking if it's master...



CLI - degug-cluster -t

After the command is completed, an indication that the server is active and that it is not the primary server will be displayed.

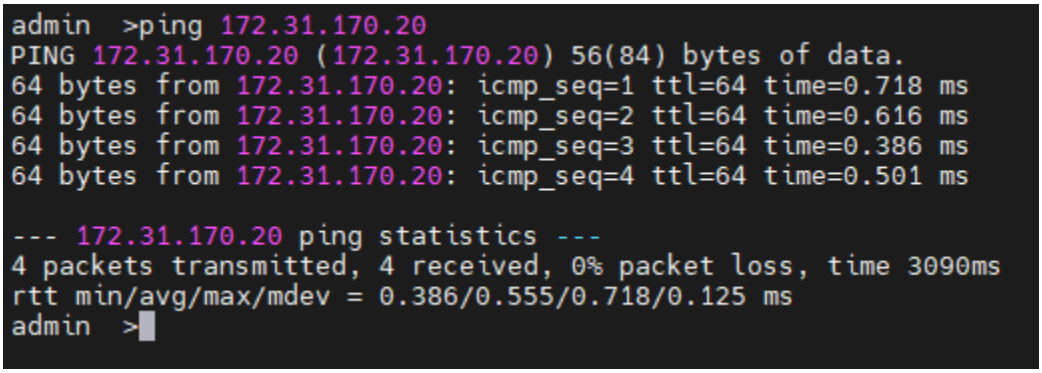


For extra information, check the Validation of Settings page.

H.A. Configuration - Validation of Settings

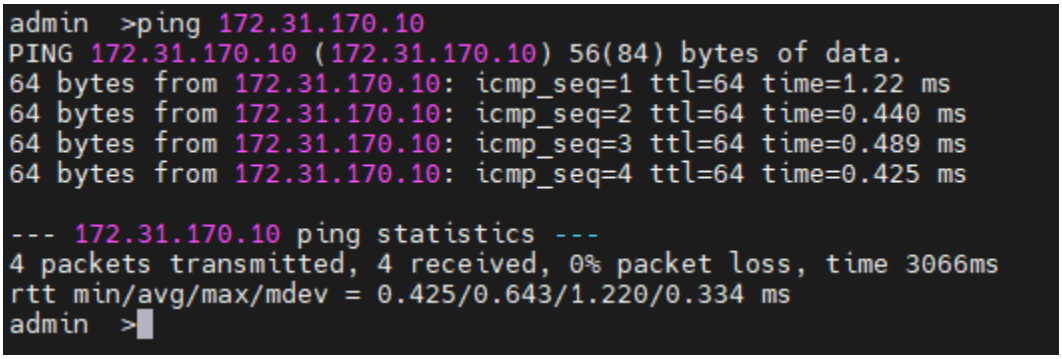
To carry out the validation, we will access the CLI interface of the Primary Device and run some commands, if you need more information about it, see this page.

One of the simplest tests to validate the communication between the H.A. clusters is to *ping* from the Primary Device (172.31.170.10) to the Secondary Device (172.31.170.20) and check for an answer, as shown on the image below:



CLI - Validation of communication from the Primary to the Secondary Device

It is also possible to perform these same steps at the other end, following a demonstration using the *ping* command to check the communication from the Secondary Device (172.31.170.20) to the Primary (172.31.170.10):



CLI - Validation of communication from the Secondary to the Primary Device through the Ping command

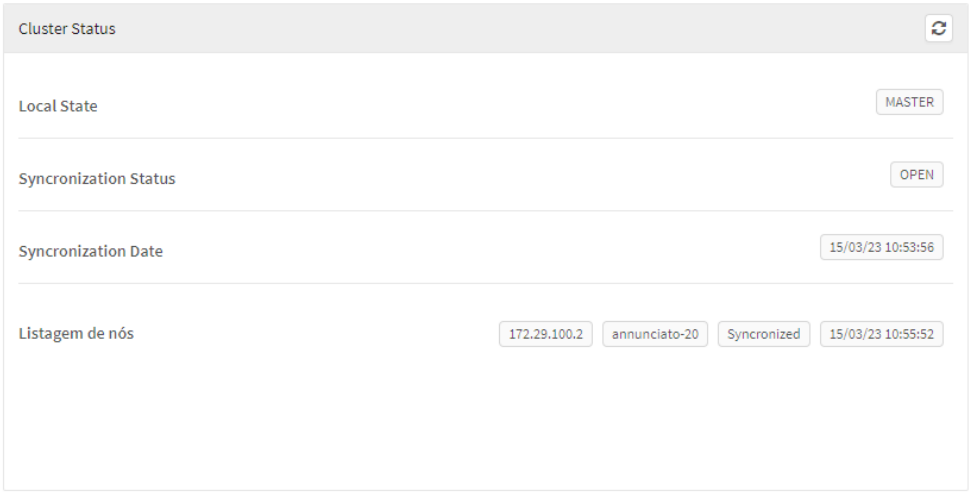
Still in the CLI interface it is possible to debug the status of the H.A. using the command [debug-cluster], an example of the information displayed on the Primary Device follows:

CLI - H.A. debugging on the Primary Device

The following is an example of the information that is displayed when applying the [debug-cluster] command on the Secondary Device:


admin -debug-cluster -t
[Fri Mar 18 11:47:21 2022] cluster_bin: Start of cluster_bin - date/time at compile time: Mar 18 2022 12:17:02
[Fri Mar 18 11:47:21 2022] omne-apply-queue: /opt/omne/apply/omne-apply-cluster &>/dev/null
[Fri Mar 18 11:47:21 2022] omne-apply-queue: Total time 1161ms
[Fri Mar 18 11:47:21 2022] cluster_bin: Database is Okay!
[Fri Mar 18 11:47:21 2022] cluster_bin: heartbeat ip/mask: ["172.25.100.2/28"]
[Fri Mar 18 11:47:21 2022] cluster_bin: heartbeat interface name: eth5
[Fri Mar 18 11:47:21 2022] cluster_bin: Heartbeat ip: 172.25.100.2
[Fri Mar 18 11:47:21 2022] cluster_bin: Heartbeat mask: 28
[Fri Mar 18 11:47:21 2022] cluster_bin: Main Node: f
[Fri Mar 18 11:47:21 2022] cluster_bin: Saving Main Node status to: disable
[Fri Mar 18 11:47:21 2022] cluster_bin: Main Node saved as disable
[Fri Mar 18 11:47:21 2022] cluster_bin: Startup Ucarp
[Fri Mar 18 11:47:21 2022] cluster_bin: [ucarp] Looking for minor node interface
[Fri Mar 18 11:47:21 2022] cluster_bin: Minor Ucarp Interface is: eth1
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd begin
[Fri Mar 18 11:47:21 2022] cluster_bin: /usr/sbin/ucarp -i eth1:0 -s 10.10.10.2 -a 10.10.10.2 -v 100 -M -z -x 2&_t -u /opt/omne/init/vip-up.sh -d /opt/omne/init/vip-dn.sh -p 8v8SH3 -B
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd end
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd begin
[Fri Mar 18 11:47:21 2022] cluster_bin: /usr/sbin/ucarp -i eth2v0 -s 10.105.252.2 -a 10.105.252.2 -v 200 -M -z -x 2&_f -u /opt/omne/init/vip-up.sh -d /opt/omne/init/vip-dn.sh -p HeHlfKi -B
[Fri Mar 18 11:47:21 2022] cluster_bin: ucarp_create_cmd end
[Fri Mar 18 11:47:21 2022] cluster_bin: Start monitoring the status
[Fri Mar 18 11:47:21 2022] ucarp: [INFO] Local advertised ethernet address is [00:0c:29:f8:52:d1]
[Fri Mar 18 11:47:21 2022] ucarp: [INFO] Local advertised ethernet address is [5a:fa:6f:6a:6d:f1]
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Switching to state: BACKUP
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Spawning [/opt/omne/init/vip-dn.sh eth2v0 10.105.252.2 2&_f]
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Switching to state: BACKUP
[Fri Mar 18 11:47:21 2022] ucarp: [WARNING] Spawning [/opt/omne/init/vip-dn.sh eth1:0 10.10.10.2 2&_t]
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] Ip [10.10.10.2] deleted : ip addr del 10.10.10.2/24 dev eth1:0
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] annunciato-28 has released 10.10.10.2/24
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth2v0] Ip [10.105.252.2] deleted : ip addr del 10.105.252.2/24 dev eth2v0
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth1:0] === BACKUP: annunciato-28 ===
[Fri Mar 18 11:47:21 2022] cluster-vip-dn: [eth2v0] Secondary interface. Status ignored!
[Fri Mar 18 11:47:21 2022] cluster_bin: [signal] Remote signal received
[Fri Mar 18 11:47:21 2022] cluster_bin: [signal] Node has been demoted
[Fri Mar 18 11:47:21 2022] cluster_bin: Keep Cluster Running
[Fri Mar 18 11:47:21 2022] cluster_bin: [backup] Start loop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcconfig] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: Clear table apply_queue_cluster
[Fri Mar 18 11:47:21 2022] cluster_bin: Clean table, apply_queue_cluster
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [brcvar] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Publications settings_sync_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Publications settings_sync_* dropped
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Subscriptions c_subscription_* to drop
[Fri Mar 18 11:47:21 2022] cluster_bin: [radius] Subscriptions c_subscription_* dropped
[Fri Mar 18 11:47:22 2022] cluster_bin: Waiting for neighbors nodes to respond
[Fri Mar 18 11:47:22 2022] cluster_bin: try connect: /usr/bin/ping -I eth3 -w 1 -c 1 172.25.100.1 > /dev/null
[Fri Mar 18 11:47:22 2022] cluster_bin: Could not create file descriptor. client_fd: -1
[Fri Mar 18 11:47:24 2022] cluster_bin: 172.25.100.1 is alive
[Fri Mar 18 11:47:24 2022] cluster_bin: Finding Master
[Fri Mar 18 11:47:24 2022] cluster_bin: [bauckup] Register Master
[Fri Mar 18 11:47:24 2022] cluster_bin: Master registered as being ip 172.25.100.1
[Fri Mar 18 11:47:24 2022] cluster_bin: [Backup] Master Registered with Success
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] Run as async server
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: register_backup
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: register_master
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: apply_queue_notice
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: bind_list_of_tables
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: request_table_dump_file
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: register_backup_status
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: stop_cluster
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: is_cluster_alive
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: bind_remote_master
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: register_apply_list
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] 21nd: m_has_new_table
[Fri Mar 18 11:47:24 2022] cluster_bin: [backup] Launching Sync Server
[Fri Mar 18 11:47:24 2022] cluster_bin: Sync Server launched with 1 threads
[Fri Mar 18 11:47:24 2022] cluster_bin: BackupDB Begin
[Fri Mar 18 11:47:24 2022] cluster_bin: Backup Deleted
[Fri Mar 18 11:47:24 2022] cluster_bin: BackupDB: /usr/bin/pg_dump -U postgres brcconfig -b -c -t obj_addr -t box_net_device -t box_cluster_nodes -f /opt/omne/conf/cluster_restore_tables.sql
[Fri Mar 18 11:47:24 2022] cluster_bin: Database Restore File Found! File size = 17054
[Fri Mar 18 11:47:24 2022] cluster_restorer: Launching cluster database restore service...
[Fri Mar 18 11:47:24 2022] cluster_bin: BackupDB ends
[Fri Mar 18 11:47:24 2022] cluster_bin: To Create Dictionaries Tables
[Fri Mar 18 11:47:24 2022] cluster_restorer: Waiting for restore signal...
[Fri Mar 18 11:47:24 2022] cluster_bin: Load Old Enabled Service List
[Fri Mar 18 11:47:24 2022] cluster_bin: __LoadEnabledServiceList__
[Fri Mar 18 11:47:24 2022] cluster_bin: service_list_size:1
[Fri Mar 18 11:47:24 2022] cluster_bin: Init Enabled Services List
[Fri Mar 18 11:47:24 2022] cluster_bin: Service found: service_firewall
[Fri Mar 18 11:47:24 2022] cluster_bin: End Enabled Services List
[Fri Mar 18 11:47:24 2022] cluster_bin: Calculating table lists
[Fri Mar 18 11:47:24 2022] cluster_bin: Calculating table lists end
[Fri Mar 18 11:47:24 2022] cluster_bin: Sending Status To Master...
[Fri Mar 18 11:47:24 2022] cluster_bin: Status was sent to master
[Fri Mar 18 11:47:24 2022] cluster_bin: [brcconfig] Sync start
[Fri Mar 18 11:47:24 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:24 2022] cluster_bin: trunc_tab_size: 226
[Fri Mar 18 11:47:25 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:25 2022] cluster_bin: Created Subscription settings_sync_1_brcconfig
[Fri Mar 18 11:47:25 2022] cluster_bin: [brcconfig] Waiting to sync 226 table(s)
[Fri Mar 18 11:47:26 2022] cluster_bin: Sync progress: 226/226/226
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Sync done! lines: 674
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcconfig] Sync start done
[Fri Mar 18 11:47:26 2022] cluster_bin: Backup Deleted
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync start
[Fri Mar 18 11:47:26 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:26 2022] cluster_bin: trunc_tab_size: 5
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: Created Subscription settings_sync_1_brcvar
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Waiting to sync 5 table(s)
[Fri Mar 18 11:47:26 2022] cluster_bin: Sync progress: 5/5/5
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync done! lines: 12
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: [brcvar] Sync start done
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Sync start
[Fri Mar 18 11:47:26 2022] cluster_bin: execute_truncate_tab
[Fri Mar 18 11:47:26 2022] cluster_bin: trunc_tab_size: 5
[Fri Mar 18 11:47:26 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:47:26 2022] cluster_bin: Created Subscription settings_sync_1_radius
[Fri Mar 18 11:47:26 2022] cluster_bin: [radius] Waiting to sync 5 table(s)
[Fri Mar 18 11:48:25 2022] cluster_bin: Sync progress: 5/5/5
[Fri Mar 18 11:48:25 2022] cluster_bin: [radius] Sync done! lines: 55
[Fri Mar 18 11:48:25 2022] cluster_bin: log_min_messages altered
[Fri Mar 18 11:48:25 2022] cluster_bin: [radius] Sync start done
[Fri Mar 18 11:48:25 2022] cluster_bin: Load NEW Enabled Service List
[Fri Mar 18 11:48:25 2022] cluster_bin: __LoadEnabledServiceList__
[Fri Mar 18 11:48:25 2022] cluster_bin: service_list_size:6
[Fri Mar 18 11:48:25 2022] cluster_bin: Init Enabled Services List
[Fri Mar 18 11:48:25 2022] cluster_bin: Service found: service_firewall
[Fri Mar 18 11:48:25 2022] cluster_bin: Service found: service_proxy
[Fri Mar 18 11:48:25 2022] cluster_bin: Service found: service_webcache
[Fri Mar 18 11:48:25 2022] cluster_bin: Service found: service_webfilter
[Fri Mar 18 11:48:25 2022] cluster_bin: Service found: service_snmp
[Fri Mar 18 11:48:25 2022] cluster_bin: End Enabled Services List
[Fri Mar 18 11:48:25 2022] cluster_bin: Loading service_firewall apply list
[Fri Mar 18 11:48:25 2022] cluster_bin: Running service_firewall apply list
[Fri Mar 18 11:48:26 2022] omne-apply-queue: Checking if cluster is active...
[Fri Mar 18 11:48:26 2022] omne-apply-queue: Cluster it is active.
[Fri Mar 18 11:48:26 2022] omne-apply-queue: Checking if it's master...
[Fri Mar 18 11:48:26 2022] omne-apply-queue: It not is MASTER
[Fri Mar 18 11:48:26 2022] omne-apply-queue: Apply list size: 12
[Fri Mar 18 11:48:26 2022] omne-apply-queue: /opt/omne/apply/omne-apply-firewall &>/dev/null
[Fri Mar 18 11:48:27 2022] omne-apply-queue: /opt/omne/apply/omne-apply-firewall -v 6 &>/dev/null
[Fri Mar 18 11:48:28 2022] omne-apply-queue: /opt/omne/apply/omne-apply-firewall-input &>/dev/null
[Fri Mar 18 11:48:28 2022] omne-apply-queue: /opt/omne/apply/omne-apply-firewall-redir &>/dev/null
[Fri Mar 18 11:48:28 2022] omne-apply-queue: /opt/omne/apply/omne-apply-eth -f &>/dev/null
[Fri Mar 18 11:48:31 2022] omne-apply-queue: /opt/omne/apply/omne-apply-security-reload &>/dev/null
[Fri Mar 18 11:48:31 2022] omne-apply-queue: /opt/omne/apply/omne-apply-tpvs-tayga &>/dev/null

In addition, after making the configuration, the interface itself displays the current status of both *Devices*. In Primary, Information displays the current status of the machine and details of the synchronization process:

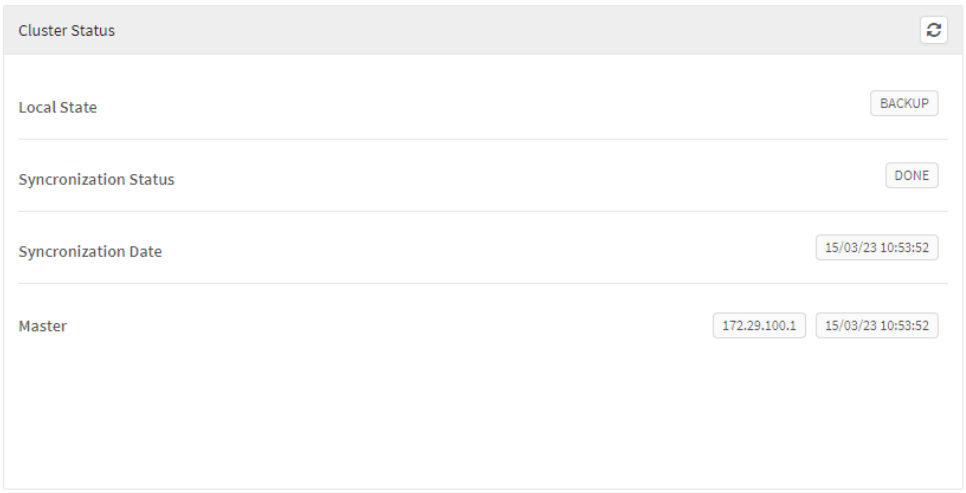


Primary Device - Status

Cluster Status

- **Local state**: Indicates if it is the primary or secundary device.
- **Synchronization status**: Indicates if the synchronization is happening.
- **Synchronization date**: Indicates the last synchronization done.
- **Listing of nodes**: Presents the following information;
    - Secundary device Heartbeat IP.
    - Secundary device Hostname.
    - Synchronization Status. Status information;
        - *"Fail to Register"*
        - *"Sync in Progress"*
        - *"Registered"*
        - *"Fail to Sync"*
        - *"Synchronized"*
        - *"Init Sync"*
        - *"Stopped"*
        - *"Not Responding"*
    - Last synchronization date.

Here it is possible to verify the Cluster Status on the secundary device.

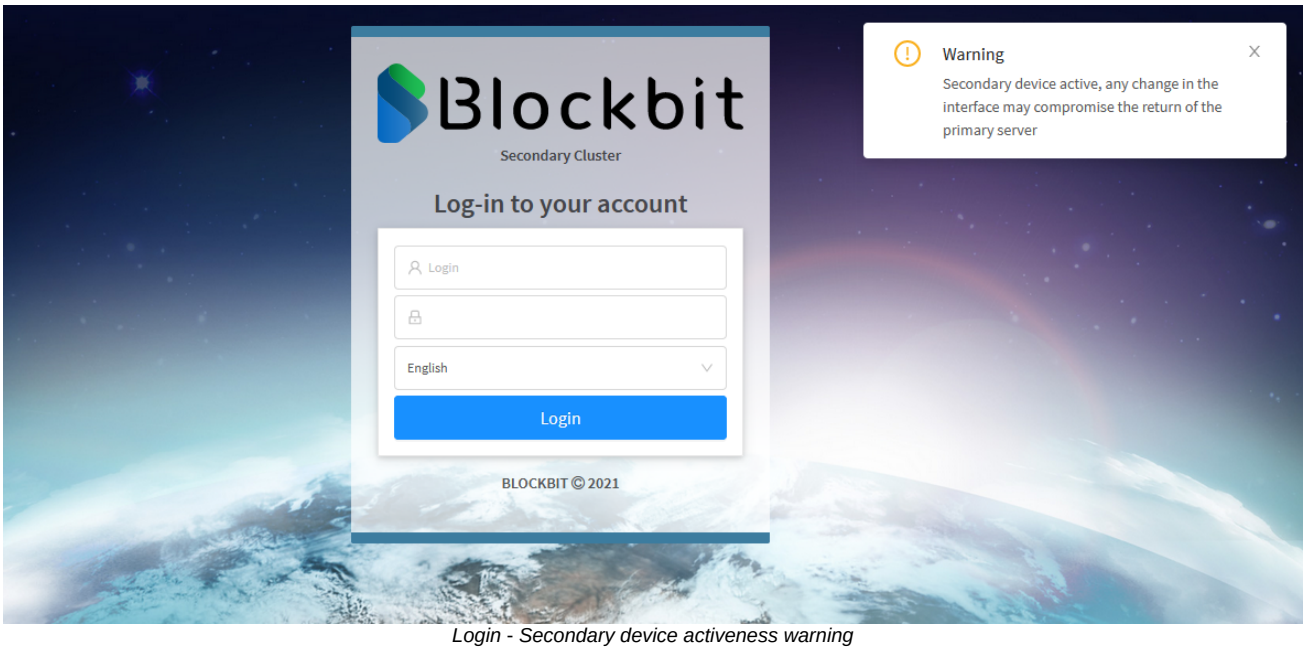


Secundary Device - Status

Cluster Status

- **Local state**: Indicates if it is the primary or secundary device.
- **Synchronization status**: Indicates if the synchronization is happening.
- **Synchronization date**: Indicates the last synchronization done.
- **Master**: Presents the following information:
  - Primary device Heartbeat IP.
  - Last synchronization date.

Finally, to ensure that the H.A. is working correctly, we can turn off the Primary Cluster, for that we will use the [shutdown] command on the CLI interface. Due to the fact that the primary cluster is no longer available, the secondary will take priority and will go up to IP 172.31.170.20 as previously configured on the wizard. The login panel will display a notification on the upper right corner of the screen, as shown on the screenshot below:

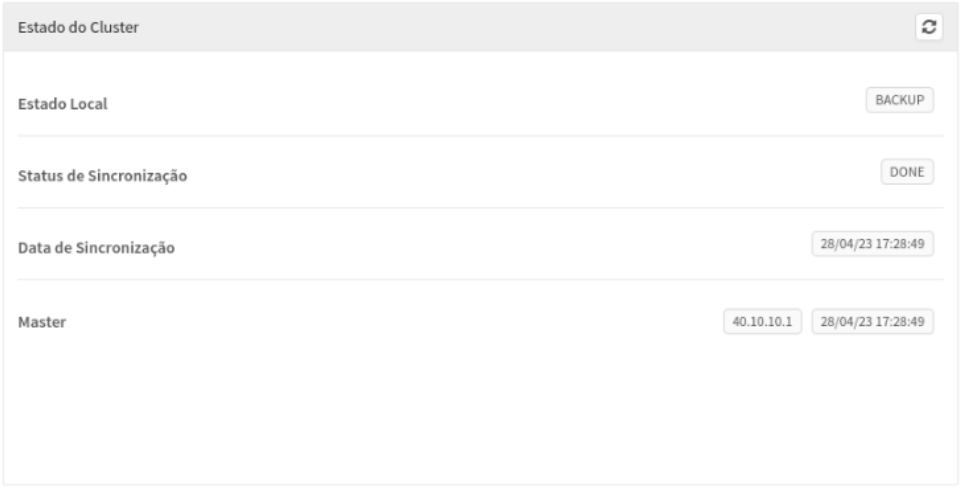


Login - Secondary device activeness warning

In addition, on the High Availability tab, in System, this message will be displayed:

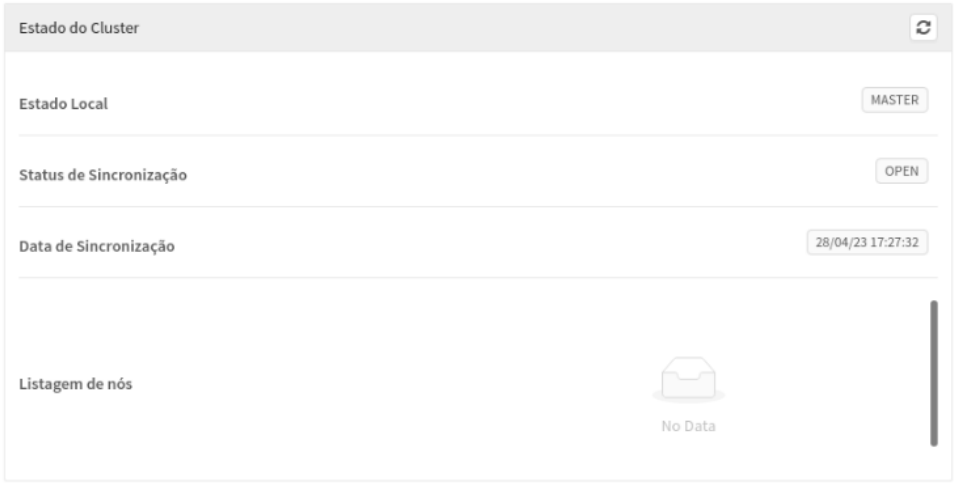
High Availability - Secondary device active

And the information panel will reflect these changes showing that the Primary Device has been deactivated, as shown below:



Secondary Device

Note that the 'Node Listing' field does not display any information when the primary device isn't in sync with a backup device.



Secondary Device - Cluster Status after the Primary has been shut down

This concludes the demo, for more information regarding High Availability, see this page.

System - Virtual Domains

The Virtual Domains (VDOM) tab enables the user to create one or more virtual Firewalls. The Virtual Domains are a method of dividing a Blockbit Firewall into other Firewalls that work as several independent Firewalls. They provide completely separate Firewall policies and settings for VPN services routing for each network or connected organization.

The virtual Domains allow the division of your physical appliance into many virtual Firewalls.

As global resources are applied to shared resources thoroughout the whole Blockbit physical appliance, those destined to a Virtual Domain are meant for a single specific Virtual Domain.

By standard, all the resource settings by Virtual Domains are defined as limitless. This means that any single VDOM is able to utilize all of the resources of the Blockbit physical appliance, if necessary. In this case, all of the other Virtual Domains would be left resourceless up to the point of being left unable to operate properly. Because of this, it is advisable to define some maximum resources usage parameters, thinking about your customers' needs.

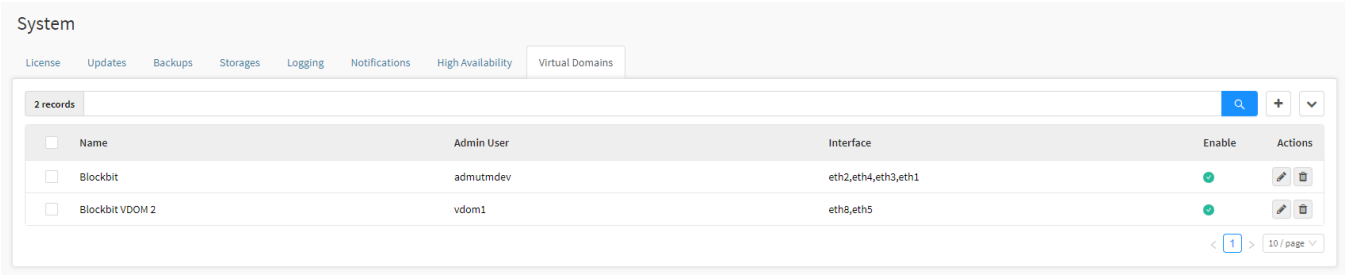
Each Virtual Domain has its own resouce settings. These settings include maximum and minimum level. The maximum level is the largest amount of these resources that a said Virtual Domain can utilize, if available in the Blockbit physical appliance. The minimum levels are a guaranteed level of resource in order to keep it working, regardless of how much resource the others may be using.

Blockbit appliances supporting Virtual Domains:

- BB 2
- BB 5
- BB 10
- BB 30
- BB 50
- BB 100
- BB 500
- BB 1000
- BB 2000
- BB 10000
- BB 15000
- BB 20000
- BB 30000

Creating a Virtual Domain

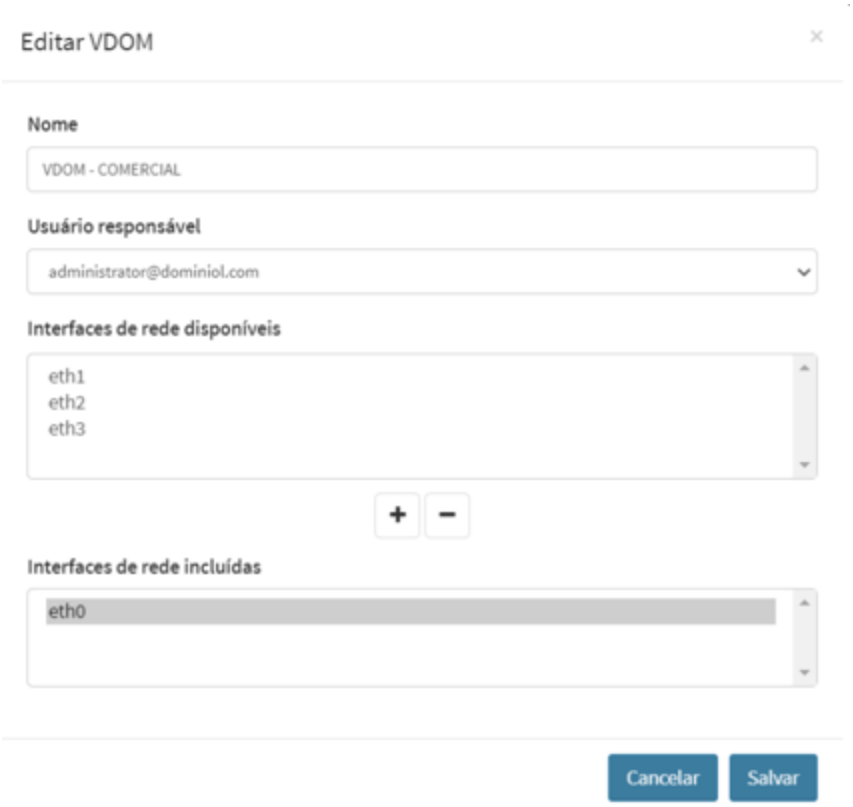
In order to create a Virtual Domain, in Settings System Virtual Domain tab click the [ ] button:



Creation of a VDOM

Please, note that the *Virtual Domains* option is only available for the *system administrator*.

On the next screen, it is possible to rename the VDOM, create independent administrators for each one of the virtual systems, enabling the creation of virtual contexts that can be managed differently, and set up the network interfaces that will be available:



Configuring a VDOM

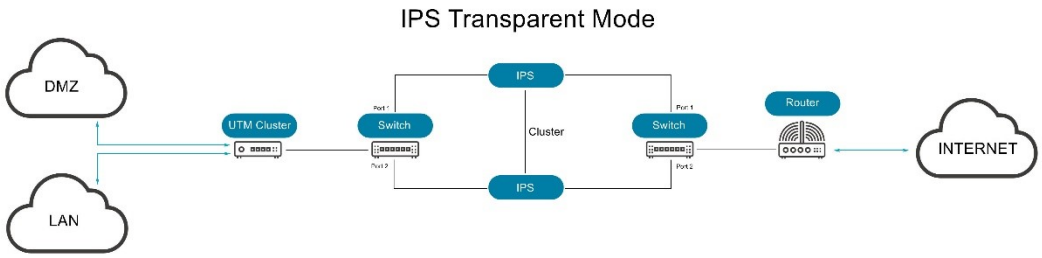
The control of certificates is also dealt with individually in each virtual system, isolating the operations of adding, removing and using the certificates directly.

Keep in mind that the user must be of the ***local*** type and not ***super administrator type***.

After selecting the network interfaces that will be included, click the [Save] button.

IPS in transparent mode

The IPS cluster in transparent mode keeps the bridges activated, however, taking into account the particularities of this mode, there is performance degradation thanks to the creation of switch loops. The resolution to this problem is the implementation of the STP (Spanning Tree Protocol) on the switches, this protocol has as main objective the control of redundant links ensuring the creation of a loop-free topology when switches or bridges are interconnected by several paths.



IPS in transparent mode

The STP acts at the layer 2 level of the OSI model, making constant communication with the network switches and through this monitoring, performs a list of the performance of the inspected links, once this is done, the protocol determines which link has the best performance and creates a switches present on the network logically disabling all redundant links and thus creating a single link between two LAN bridges, this main link will be maintained until the moment there is a failure, if this is the case, the STP will again determine the best link in order to always keep bridges active.

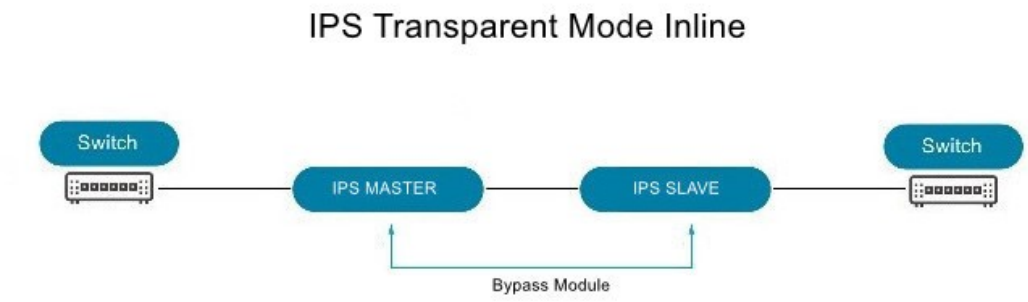
The main benefits of the Spanning Tree protocol are:

- Network loop prevention;
- Shortest recovery in response to changes (caused by changes or network failures);
- Simplification of bridging logic (thanks to the use of a root bridge that guarantees efficient data forwarding);
- Prevention of connection problems (STP provides several paths that can be activated if the main path has a failure or instability).

For the Spanning Tree Protocol to work correctly with Blockbit devices, it will be necessary to configure the STP so that it always prioritizes the ports or paths that are interconnected to the Blockbit H.A. Master.

IPS in transparent Inline mode

In this topology, if the Master falls, the Slave will automatically disable the Bypass and assume priority, the benefits of this topology are: There is no need to use the STP, it does not depend on the configuration of the Switch (since automatically the doors and paths that interconnect with the Blockbit Master) and it is possible to save two doors.



IPS in transparent Inline mode

In this mode, IPS can be configured in 3 ways:

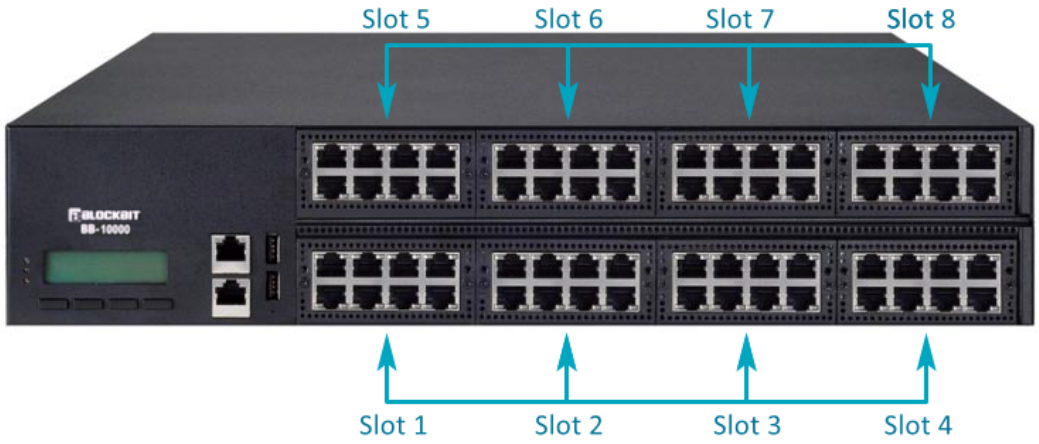
- *Off*;
- *Boot*;
- Manual.

IPS bypass

The Bypass key is a hardware device that acts as a fail-safe access point, its purpose is to ensure the continuity of traffic, it provides an access route for active security devices, such as intrusion prevention systems and appliances protection against malware.

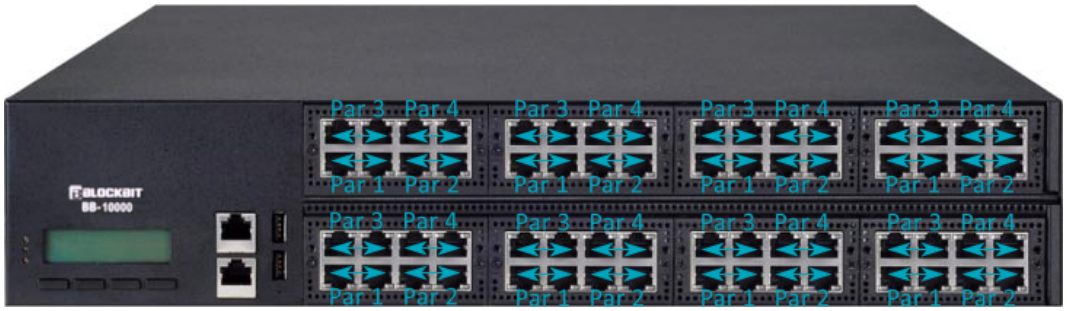
When the Bypass key is activated, it acts to ensure that the Link will continue to be available by redirecting traffic to a pre-defined alternative path, effectively creating a diversion in traffic in order to ensure that the link remains operational, giving enough time for a redundant link is activated. In this way, inactive devices will not cause network downtime in the event of a system failure (power outage, or any reason that makes the appliance unavailable) or if they are disconnected for configuration or maintenance updates.

The appliance is structured in slots and bypass pairs, being ordered from bottom to top, from left to right, therefore, the first slot will always be located in the bottom left corner of the appliance, going right until the end of the line, the next of the sequence will be the top slot on the left and will follow the same logic until the end of the line, as shown in the image below:



Order of Slots

The same occurs with pairs: The first pair is on the bottom left, the next position is on the bottom right, the next position will be on the top left, followed by the top right, as illustrated by the image below:



Pair Order

For more information about the CLI bypass configuration, access the CLI chapter.

Bypass configurations in an H.A. structure

In an H.A. structure it is recommended that the master has the following configurations:

- *system_off*;
- *just_on*.

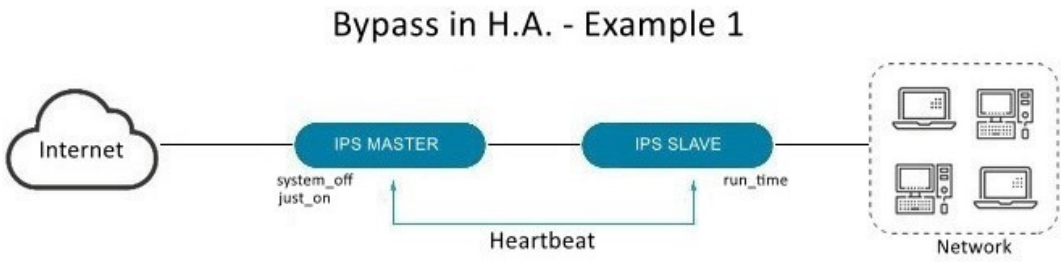
And the slave is configured as:

- *run_time*.

The operation of the Bypass in an H.A. structure can be better analyzed in 3 scenarios:

Normal Operation

The traffic acts normally with the IPS active, meanwhile the bypass monitors the device through the heartbeat to ensure its activation if necessary.



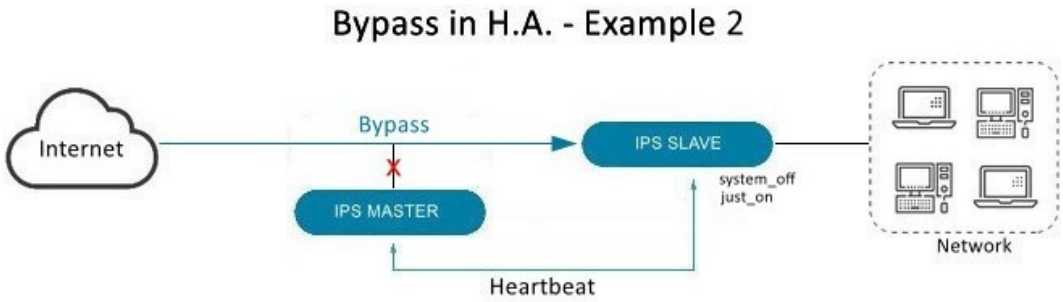
Example 1 - Normal Operation

Master failure

The Bypass kicks in by redirecting traffic to the slave in order to prevent the link from being lost, the IPS remains active normally.

Therefore, in an event where the master has a fault, the slave will assume all the functions of the master and consequently will be configured with:

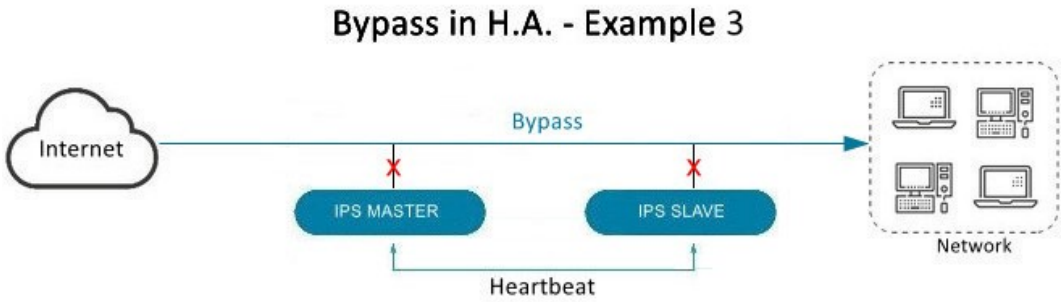
- *system_off*;
- *just_on*.



Example 2 - Master failure

Master and Slave failure

If by chance the slave also fails, the traffic is still not interrupted, but in this scenario it is not possible to inspect the packets as the IPS will be inoperative.



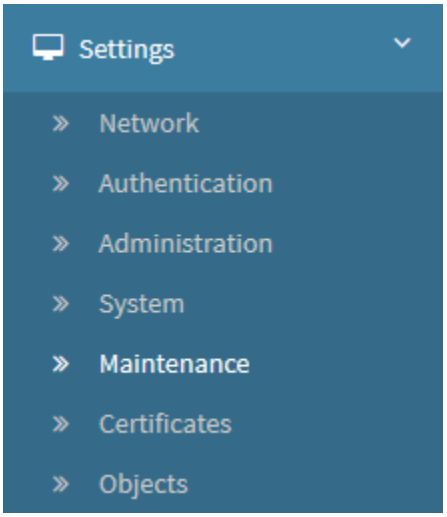
Example 3 - Master and Slave failure

For more information about the CLI bypass configuration, access this *link*.

UTM - Settings - Maintenance

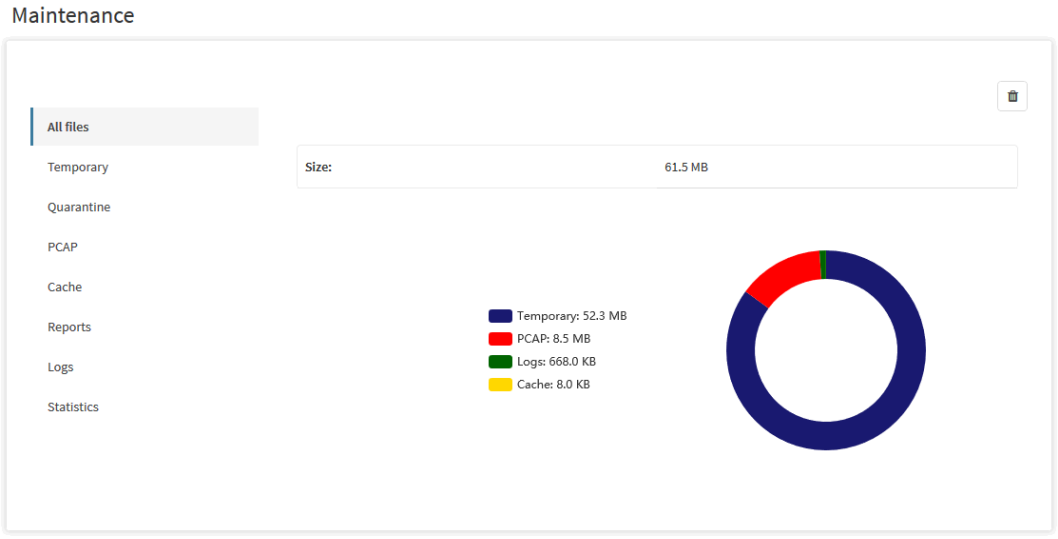
The maintenance service of Blockbit UTM is responsible for cleaning the data allocated on the local disk of the appliance or the virtual machine.

To access this screen, just select the “Maintenance” option.



Settings - Maintenance

The screen below will appear:



Settings - Maintenance - All Files

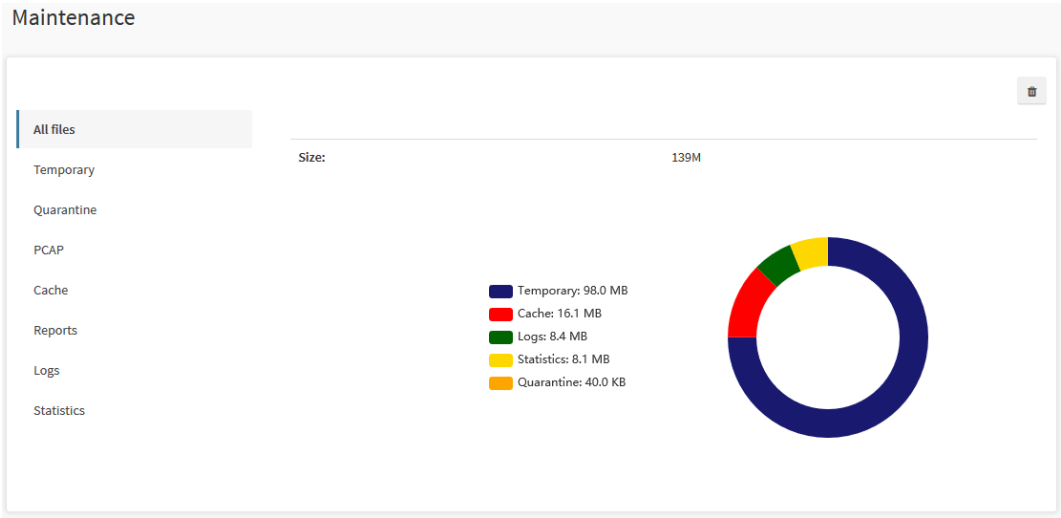
Below are the directories and reports that can be managed by the maintenance tool.

- ***All Files*:** All files listed below;
- ***Temporary*:** Temporary service and system files;
- ***Quarantine*:** Antimalware service quarantine files;
- ***PCAP*:** Network dump files generated;
- ***Cache*:** Web Cache service files and folders;
- ***Reports*:** Generated reports;
- ***Logs*:** Service and system log files;
- ***Statistics*:** Automatically generated statistics such as Dashboards and Analyzer.

Next we will analyze the components of this screen.

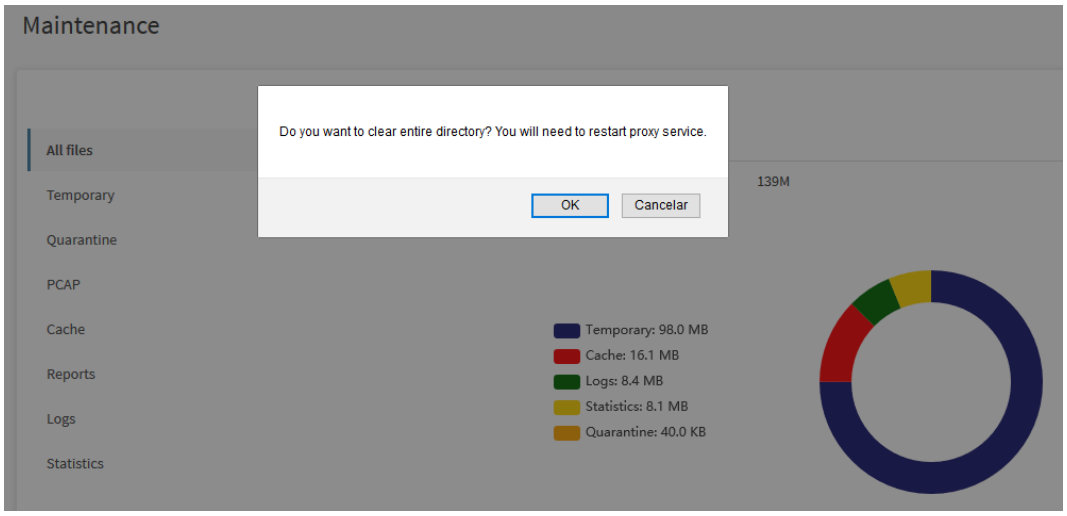
UTM - Maintenance - All Files

In the All Files tab it is possible to view the graph informing the size of all directories for maintenance in the system.



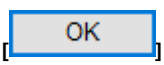
Maintenance – All files

Through the **[**  **]** button, it is possible to delete data from all directories.



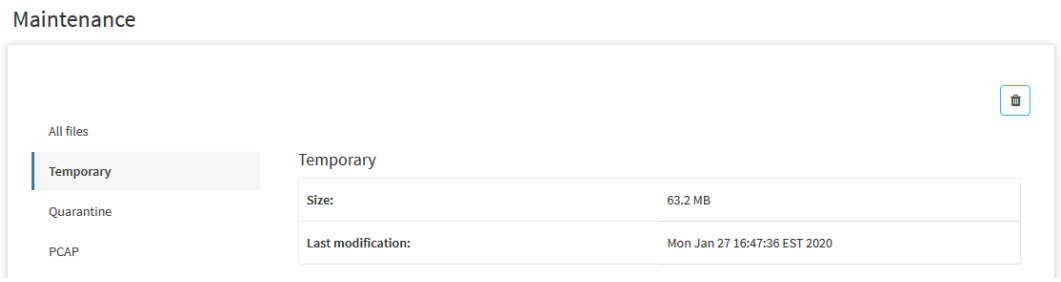
Maintenance - Clear All files

When selecting the option to erase all data, the system will display an alert saying that the proxy service will be restarted.

After clicking the **[**  **]** button, data from all directories will be removed.

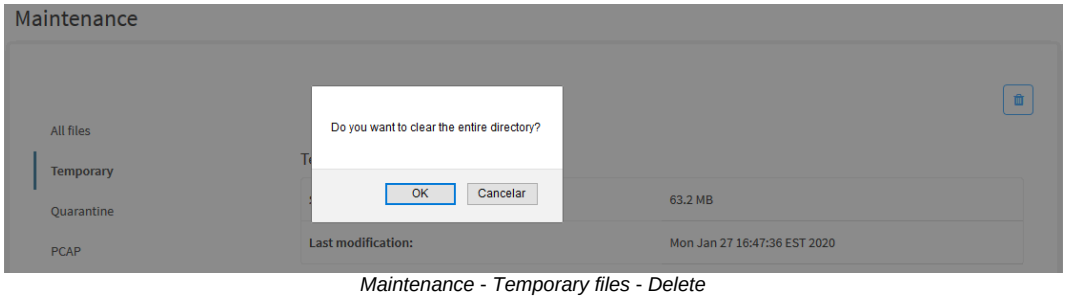
UTM - Maintenance - Temporary

In the temporary tab it is possible to view the size of the temporary directory and its last change.

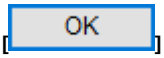


Maintenance - Temporary files

By clicking on the **[**  **]** button, it is possible to delete the directory data as shown in the screen below.

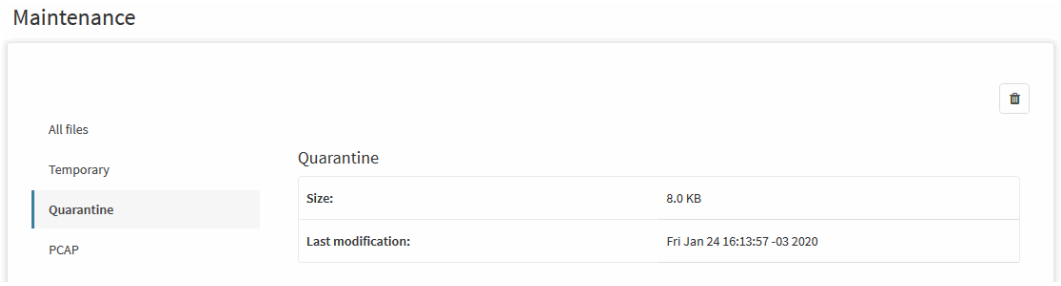


Maintenance - Temporary files - Delete

With the **[**  **]** button, all data in the temporary directory will be deleted.

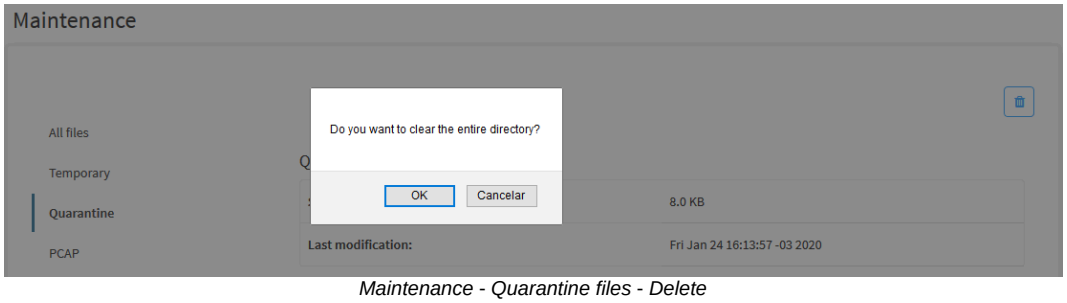
UTM - Maintenance - Quarantine

In the Quarantine tab it is possible to view the size of the temporary directory and its last change.

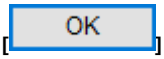


Maintenance - Quarantine files

By clicking on the **[**  **]** button, it is possible to delete the directory data as shown in the screen below.



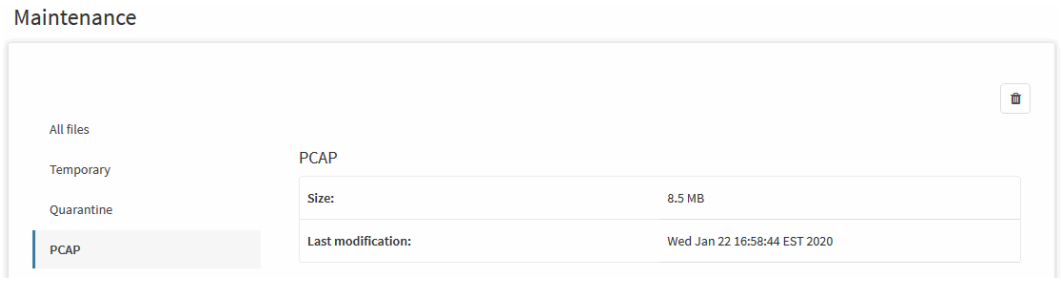
Maintenance - Quarantine files - Delete

After clicking the **[** 

] button, the data in the quarantine directory will be removed.

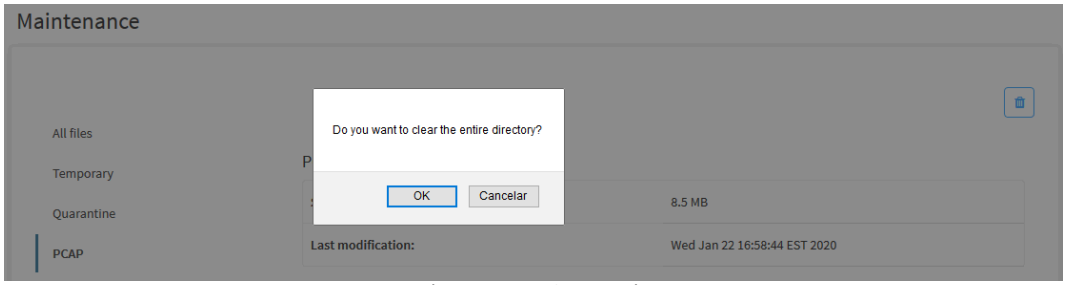
UTM - Maintenance - PCAP

In the PCAP tab it is possible to view the size of the directory and the date of the last change.

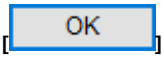


Maintenance - *PCAP*

By clicking on the **[**  **]** button, it is possible to delete the directory data as shown in the screen below.

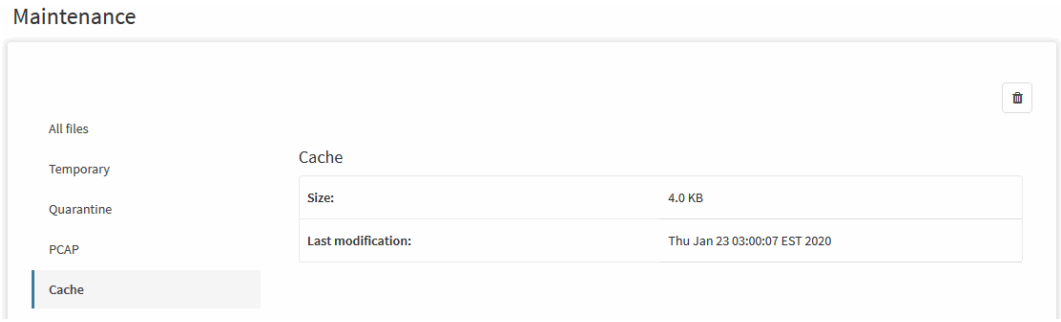


Maintenance - PCAP - Delete

After clicking the **[**  **]** button, data from the PCAP directory will be removed.

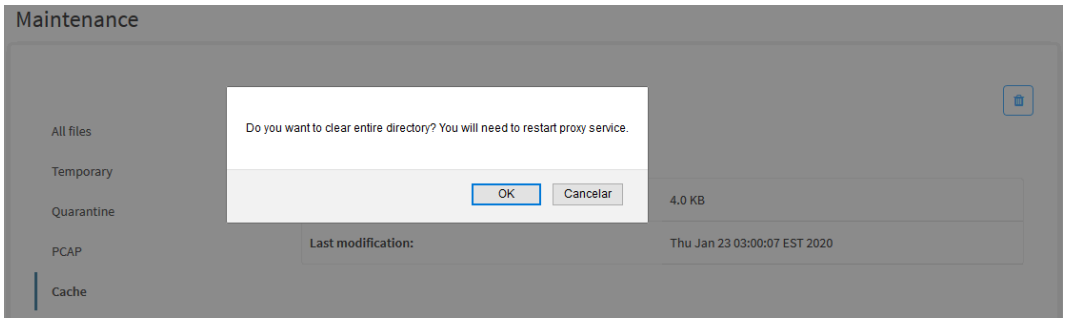
UTM - Maintenance - Cache

In the cache tab it is possible to view the size of the directory and the date of the last change.



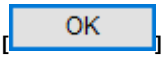
Maintenance - Cache

By clicking on the **[**  **]** button, it is possible to delete the directory data as shown in the screen below.



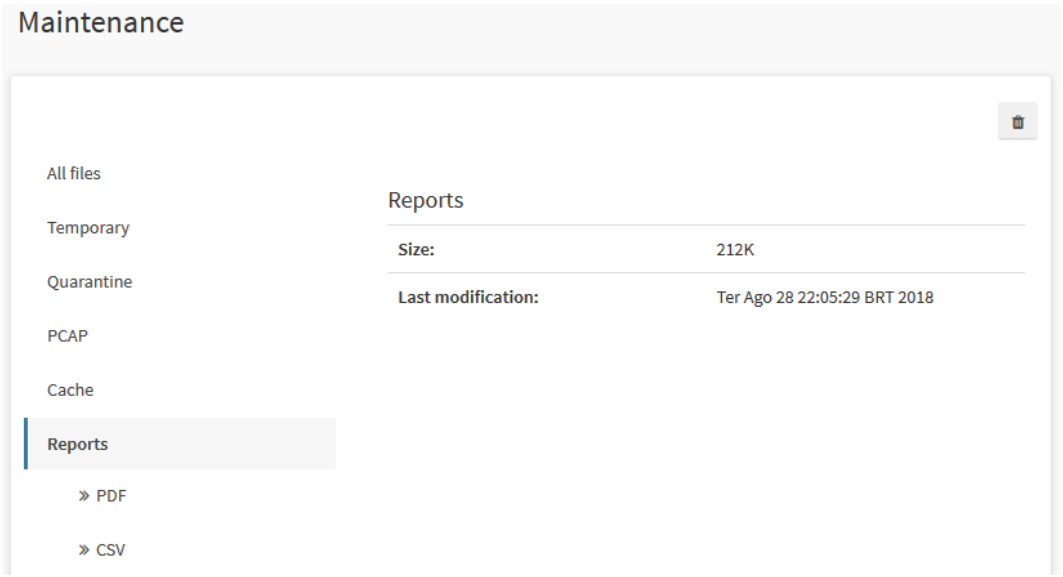
Maintenance - Cache - Delete

When selecting the option to clear the Cache, the system will display an alert saying that the proxy service will be restarted.

After clicking the **[**  **]** button, the data in the cache directory will be removed.

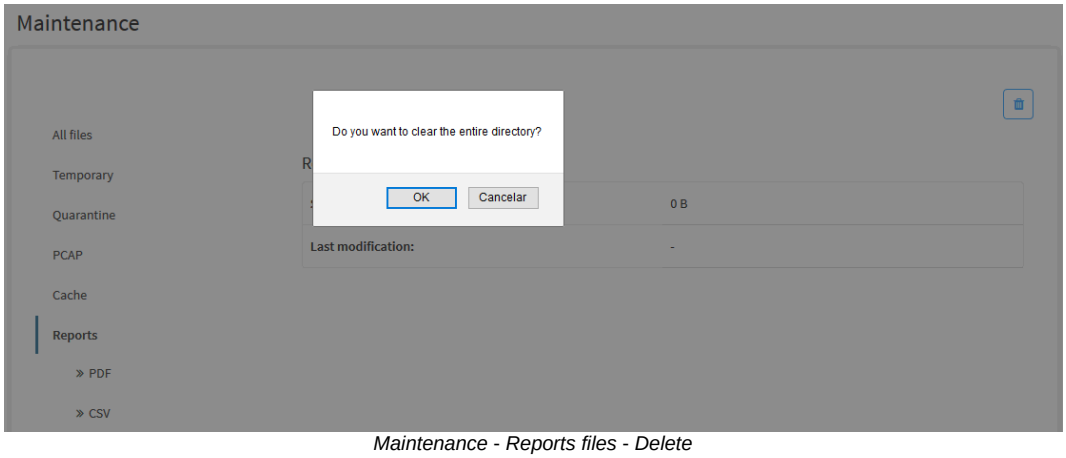
UTM - Maintenance - Reports

In the reports tab it is possible to view the size of the directory and the date of the last change, it is dividing into 2 PDF and CSV subdirectories, so it is possible to delete the entire contents of the directory or just a specific subdirectory.

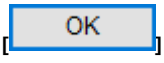


Maintenance - Reports

To delete, just click the **[**  **]** button, as shown in the screen below.



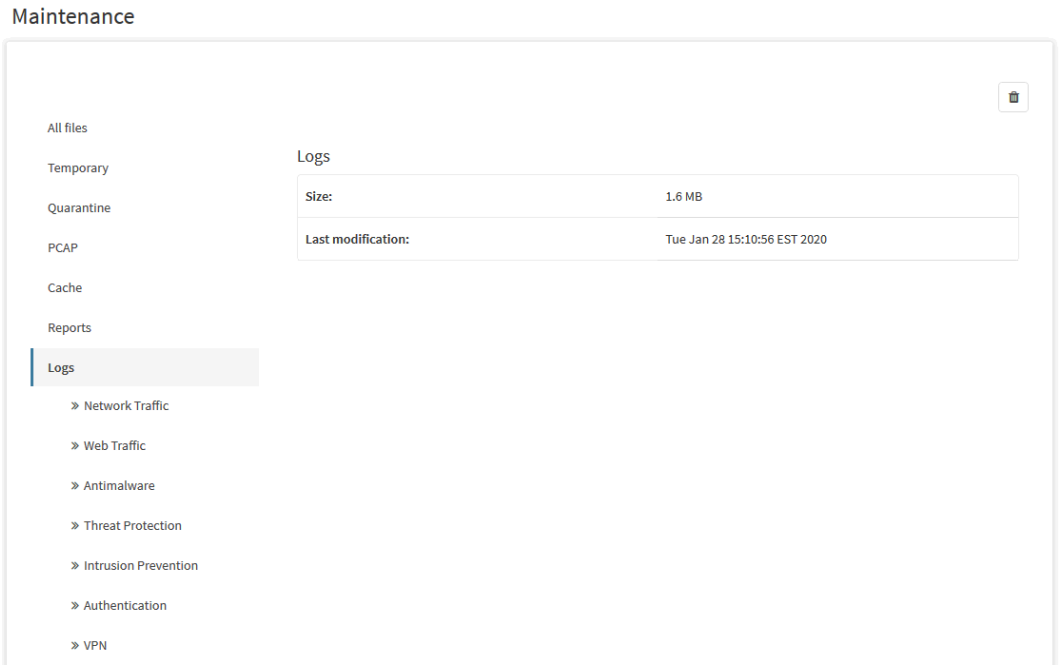
Maintenance - Reports files - Delete

After clicking the **[** 

] button, the data in the reports directory will be removed.

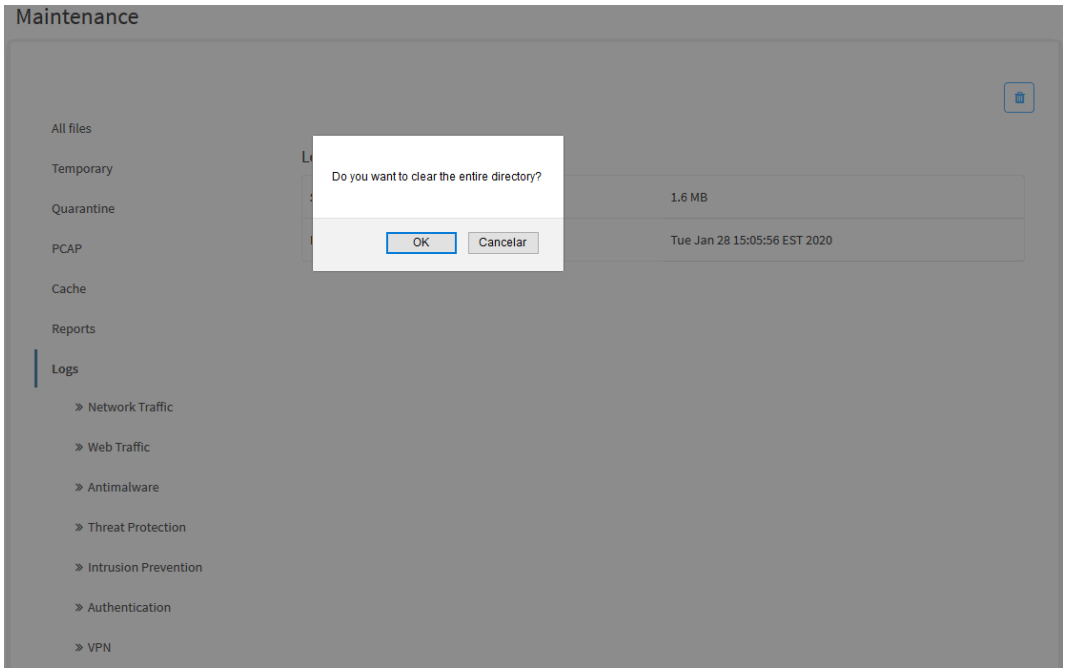
UTM - Maintenance - Logs

In the logs tab it is possible to view the size of the directory and the date of the last change, the logs directory is divided into some subdirectories, they are: "Network Traffic", "Web Traffic", "Antimalware", "Threat Protection", "Intrusion Prevention "," Authentication "and" VPN "this way it is possible to delete the entire contents of the directory or just a specific subdirectory.

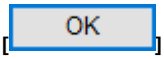


Maintenance - Logs

To delete, just click on the **[**  **]** button, as shown in the screen below.



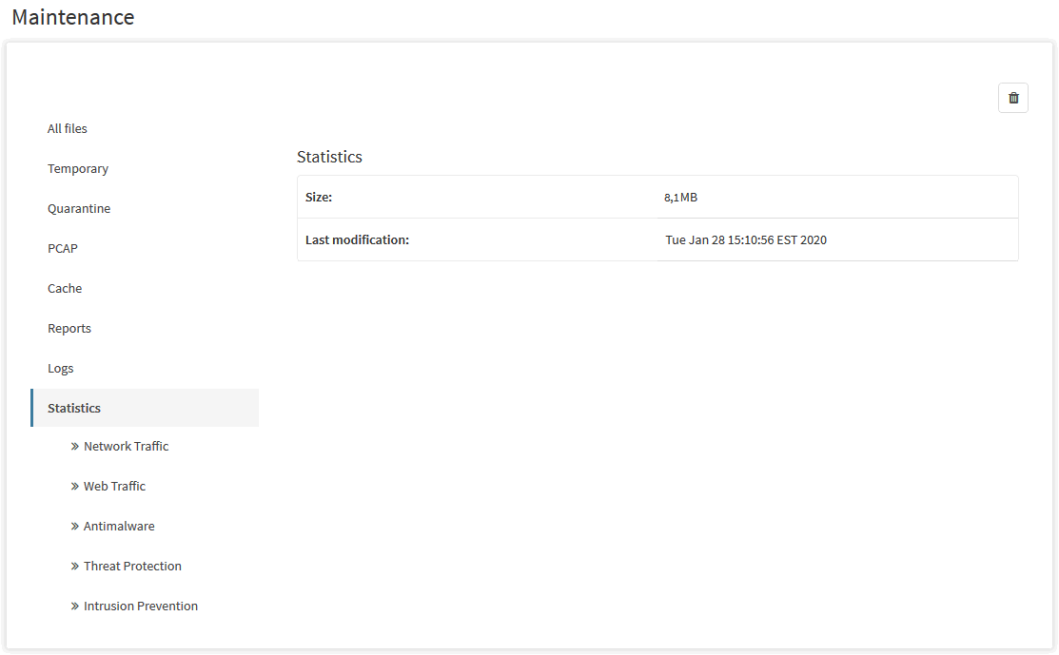
Maintenance - Logs

After clicking the [

] button, data from the log directory will be removed.

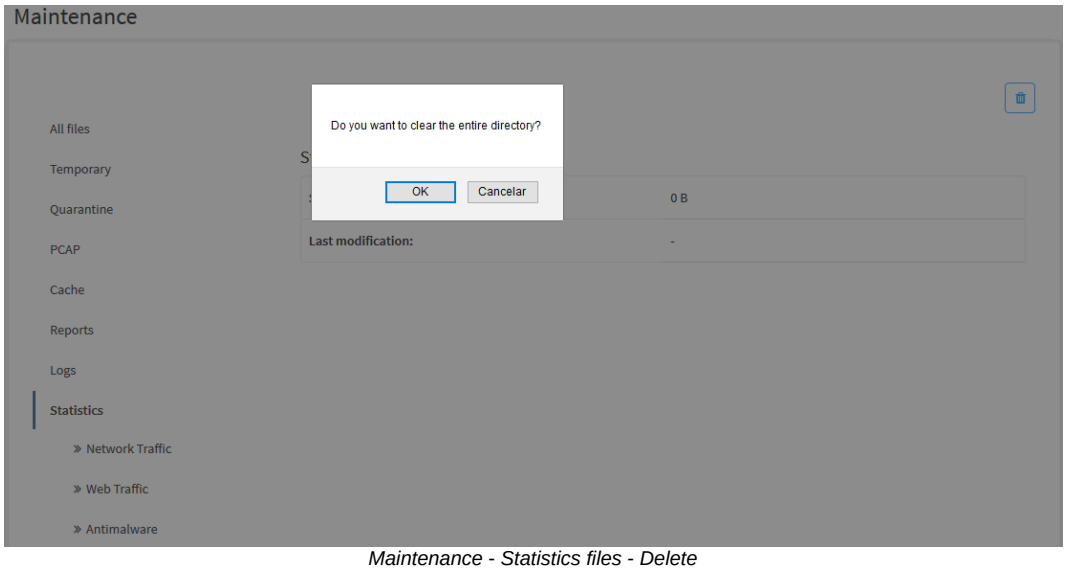
UTM - Maintenance - Statistics

In the statistics tab it is possible to view the size of the directory and the date of the last change, the logs directory is divided into 5 subdirectories, they are: "Network Traffic", "Web Traffic", "Antimalware", "Threat Protection" and "Intrusion Prevention "in this way it will be possible to delete the entire contents of the directory or just a specific subdirectory.



Maintenance - Statistics files

To delete, just click on the [ ] button, as shown below.



Maintenance - Statistics files - Delete

After clicking the [OK] button, data from the statistics directory will be removed.

UTM - Settings - Certificates

The SSL Certificate, technically called Secure Socket Layer (SSL) is a global standard in security technology, it is able to create an encrypted channel between a web server and a browser (browser) in order to ensure that all data transmitted is protected and safe.

SSL technology has been incorporated into all popular browsers and works automatically when a user connects to a protocol-enabled server.

SSL (Secure Sockets Layer) has an encryption system that uses two keys to encrypt data: A public key known to everyone and a private key that only the recipient has.

What is the private key?

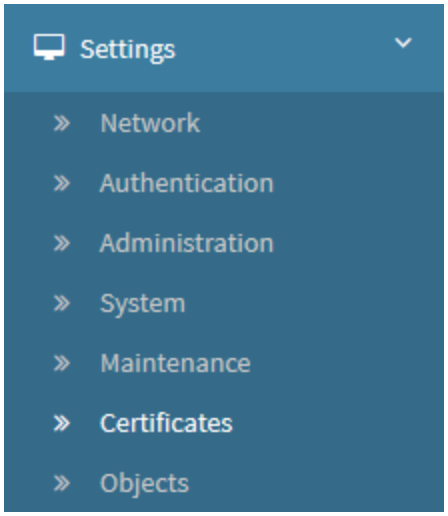
The private key is generated simultaneously with the public key and are related to each other in an asymmetric encryption system. The private key must be kept confidential and in the possession of its holder only. It is possible to digitally sign documents and files unequivocally by their owner.

What is the public key?

The public key is generated simultaneously with the private key and are related to each other using an asymmetric encryption system. The public key is associated with the data of its owner and is used to verify the digital signature that was created with the corresponding private key. It is also used to encrypt messages or files that can be decrypted with the corresponding private key.

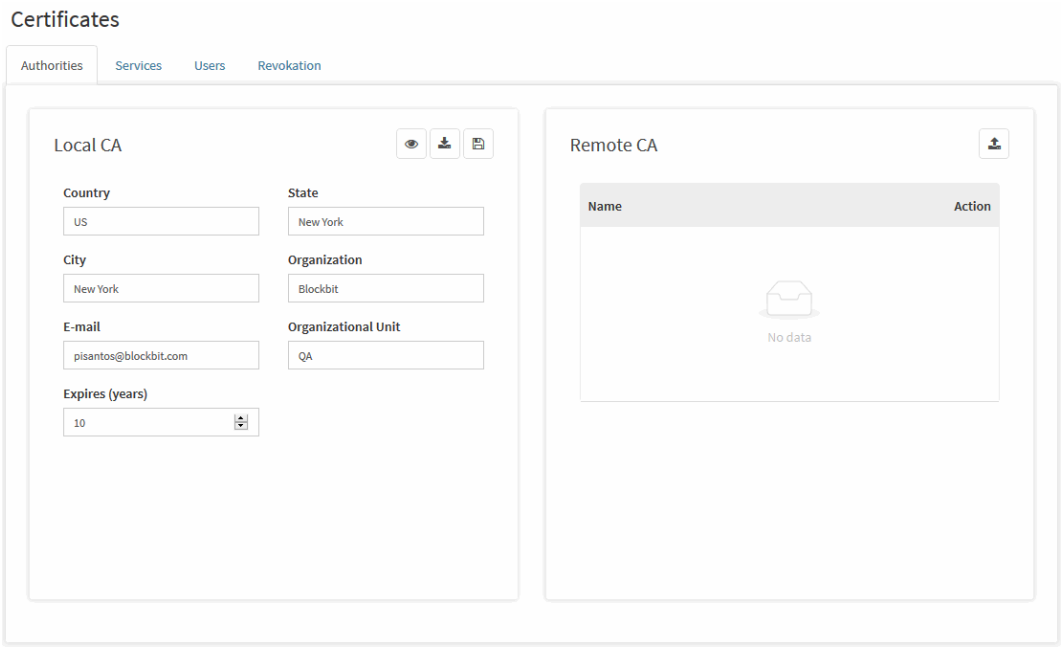
For more information on how the SSL certificate works, check this page.

To access this screen, just select the option “Certificates”.



Settings - Certificates

The screen below will appear:



Settings - Certificates - Authorities

The Authorities screen has the following tabs:

- *Authorities*;
- *Services*;
- *Users*;
- *Revokation*.

Next we will analyze the components of this screen.

Certificates - Understanding SSL operation

When your browser connects to an SSL server, it will automatically ask the server for a digital certificate from the Certification Authority (CA), it will authenticate the server's identity in order to securely secure data traffic to the real destination, and not a spoofed address.

However, in the event of a failure with the Certification Authority, your browser will open a window to inform you of the problem you encountered, allowing you to log out or continue at your own risk.

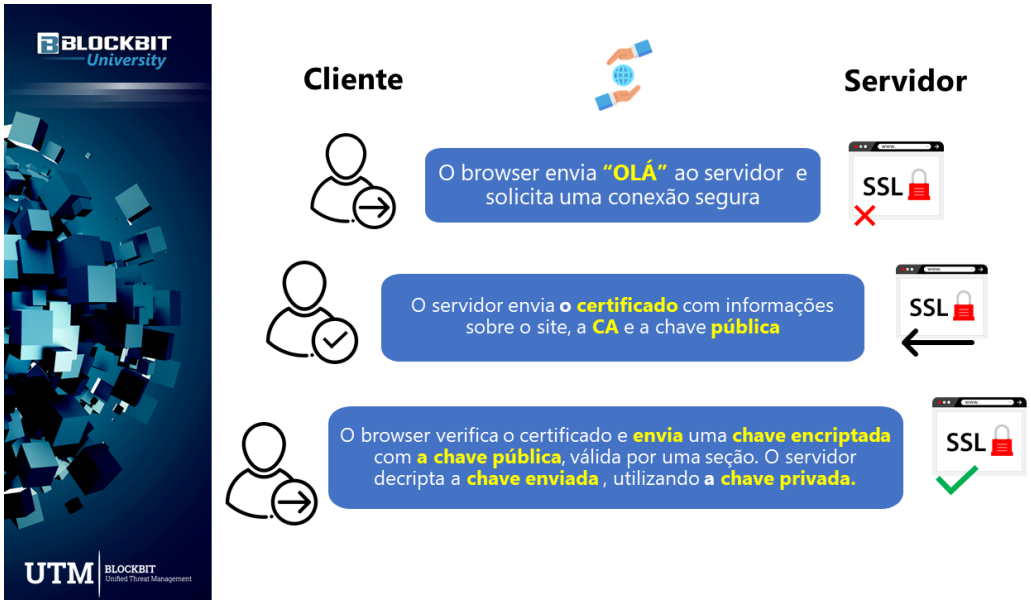
If everything goes as expected, your browser will automatically encrypt all information before sending.

When the information reaches a secure server, it is decrypted using a secret key. The moment the server returns data or information to the source of the connection, this information is also encrypted by the server before being sent, your browser will automatically decipher it upon receipt.

In traffic to WEB applications on secure servers, it is also possible to authenticate clients that connect in order to ensure, for example, that the user is not trying to impersonate another person who has restricted access. Another feature of SSL technology is the ability to authenticate data so that an intercessor cannot replace it with false information without being detected.

For example:

Think of the message as being a safe lock on a bank as it has two keys: one to lock (encrypt) and one to unlock (decrypt) the door.



Certificates - Working from an SSL connection

SSL connections are an effective means of securing data traffic in web applications.

Simplifying the SSL Certificate ensures your customer (user) that the data sent to your web application is always assured.

When your browser connects to an SSL server, it will automatically ask the server for a digital certificate from the Certification Authority (CA), it will authenticate the server's identity in order to securely secure data traffic to the real destination, and not a spoofed address.

However, in the event of a failure with the Certification Authority, your browser will open a window to inform you of the problem you encountered, allowing you to log out or continue at your own risk.

If everything goes as expected, your browser will automatically encrypt all information before sending.

When the information reaches a secure server, it is decrypted using a secret key. The moment the server returns data or information to the source of the connection, this information is also encrypted by the server before being sent, your browser will automatically decipher it upon receipt.

In traffic to WEB applications on secure servers, it is also possible to authenticate clients that connect in order to ensure, for example, that the user is not trying to impersonate another person who has restricted access. Another feature of SSL technology is the ability to authenticate data so that an intercessor cannot replace it with false information without being detected.

For example:

Think of the message as being a safe lock on a bank as it has two keys: one to lock (encrypt) and one to unlock (decrypt) the door.

Certificates - Working from an SSL connection

SSL connections are an effective means of securing data traffic in web applications.

Simplifying the SSL Certificate ensures your customer (user) that the data sent to your web application is always assured.

Certificates - Authorities tab

The purpose of a certification authority is to confirm the ownership of the certificates, confirming that the certificate received when accessing a particular website or address actually belongs to the entity providing it. This is what ensures that you are even securely accessing SSL / HTTPS websites and addresses.

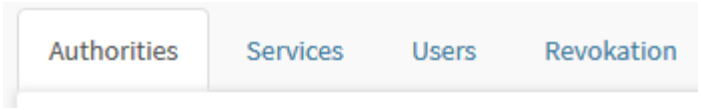
BLOCKBIT UTM allows the administrator to create his own certification authority, which is a simple and practical way to obtain the certificate that will be used to ensure reliability in accessing the solution's resources:

- BLOCKBIT UTM WEB interface;
- Web authentication or Captive portal;
- SSL interception on proxy accesses;
- IPSEC RAS VPN;
- SSL VPN Site-to-site;
- SSL VPN RAS.

BLOCKBIT UTM generates a Certification Authority in the execution of the “Configuration Wizard”, which is carried out in the system installation process.

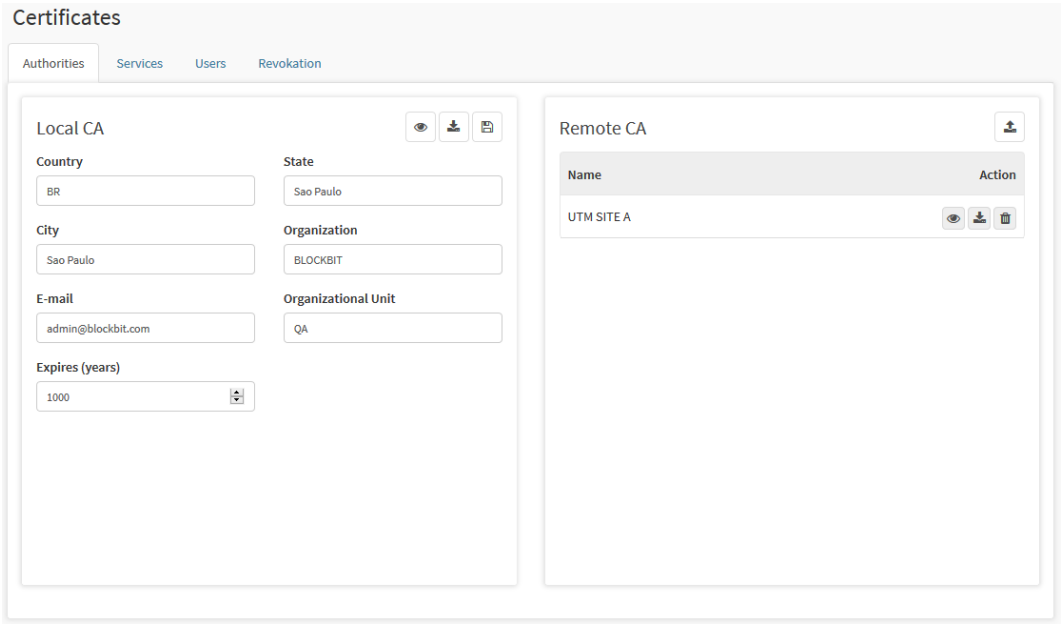
This same certifying entity is responsible for issuing digital certificates for services and users supported by BLOCKBIT UTM.

To access the certificate management interface, access the Authorities tab.



Authorities Tab

The screen will appear, as shown by the image below:



Authorities - Certificate Management

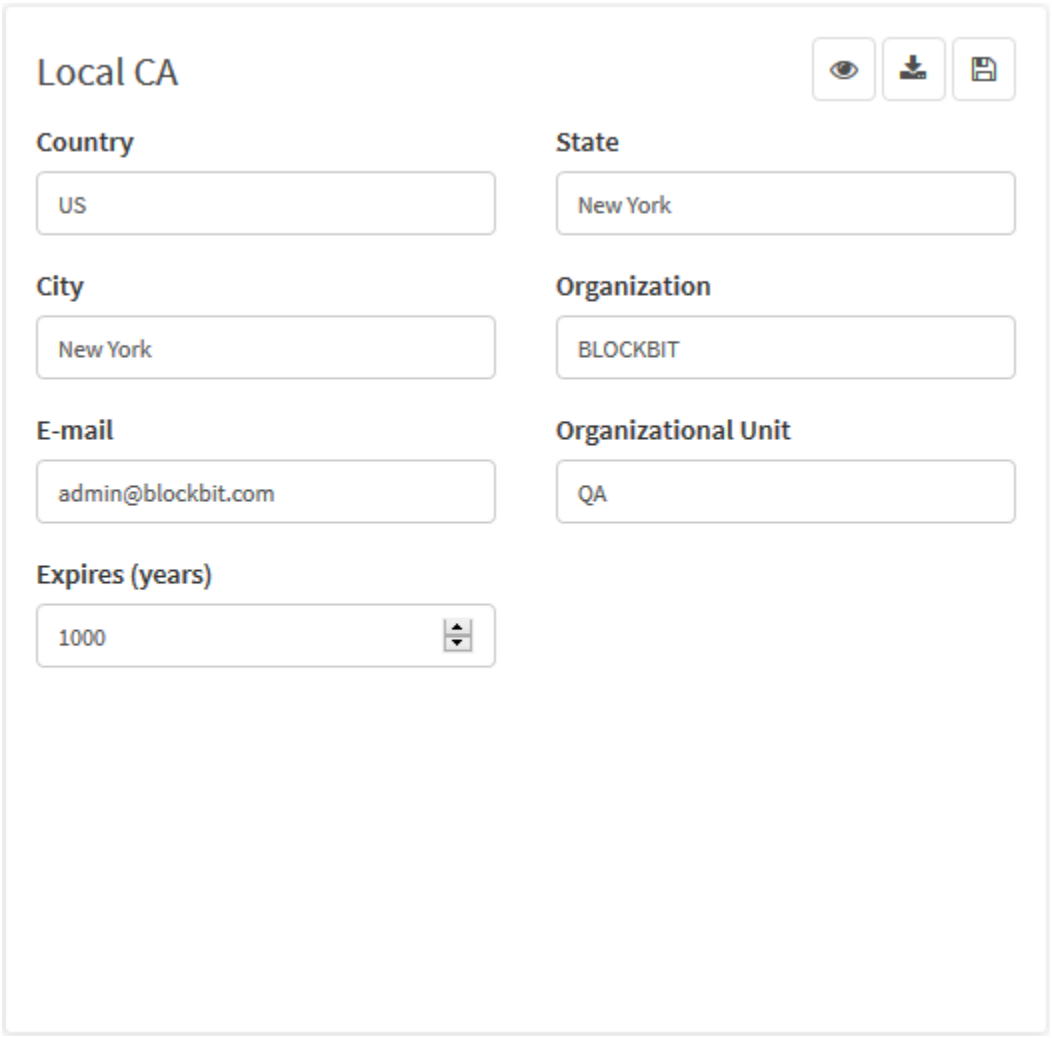
The Authorities interface is divided into:

- *Local CA*;
- *Remote CA*.

Next, we'll look at each panel.

Authorities - Local CA

In the Local CA box you can download to import the Local CA on the network devices, or generate a new one (CA - Certificate Authority).



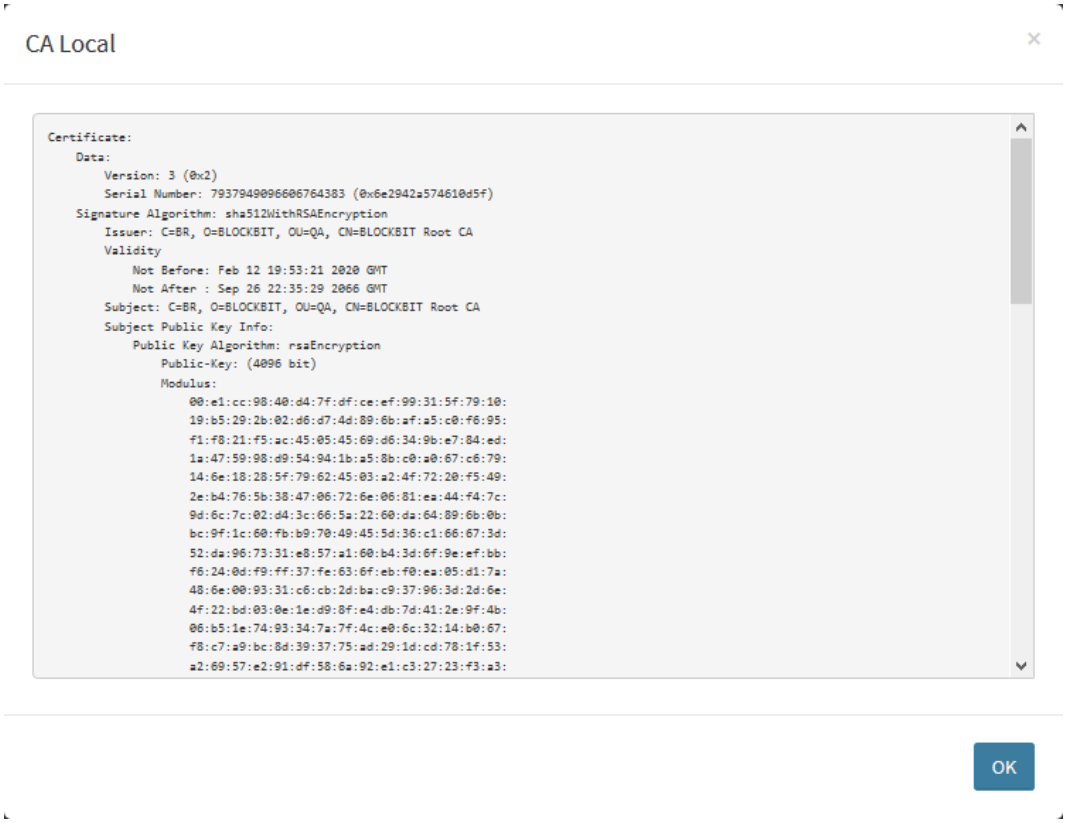
Authorities - Local CA

The information on this screen was configured during the installation process, for more information check this page.

- ***Country*:** Set the country. Ex.: *US*;
- ***State*:** Set the state. Ex.: *New York*;
- ***City*:** Define the city. Ex.: *New York*;
- ***Organization*:** Set your company name. Ex.:Blockbit;
- ***E-mail*:** Set the administrator email. Ex.: admin@blockbit.com;
- ***Organizational Unit*:** Define the department. Ex.: QA;
- ***Expires (years):*** Set the certificate validity time. Ex.: 10 years;

At the top of this panel we have the following options:

- ***View*[ ]:** By clicking on this button it is possible to view the certificate, as shown below;



Authorities - CA Local

- ***Download*[ ]:** Serves to download the certificate;

After the CA Download. Install the CA on all devices on the network.

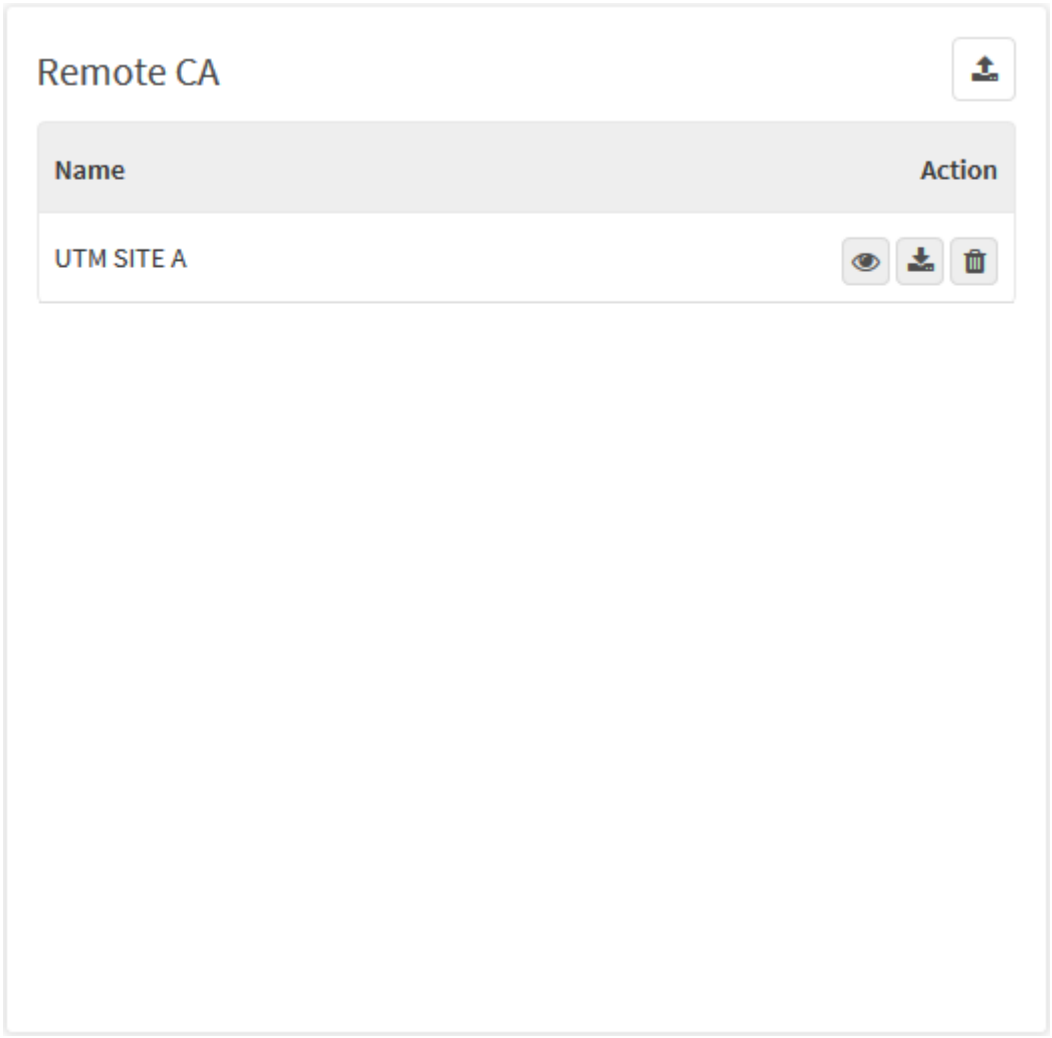
- ***Save*[ ]:** Only in case of special needs can the administrator generate a new one (CA - Certificate Authority).

Saving a CA requires the server to generate a new certification body. This action requires reinstallation of the new CA on all devices on the network.

If you want to recreate the CA, you must also re-create the Server Certificate, this procedure requires the installation of the new CA on all devices on the network. Download the CA and reinstall on all workstations. Remembering that for validation of the new CA. you must RESTART the server.

Authorities - Remote CA

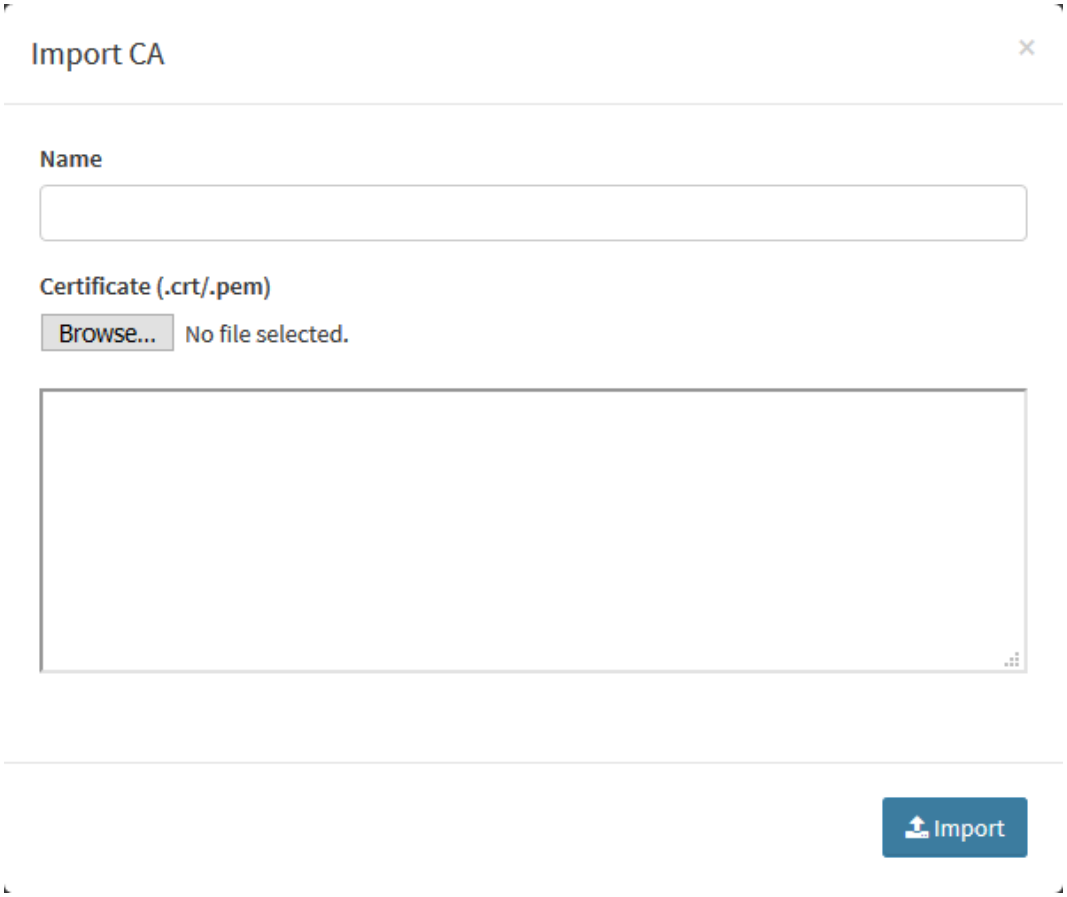
In the Remote CA framework you have the option to import a certificate signed by a valid certifying entity.



Authorities - Remote CA

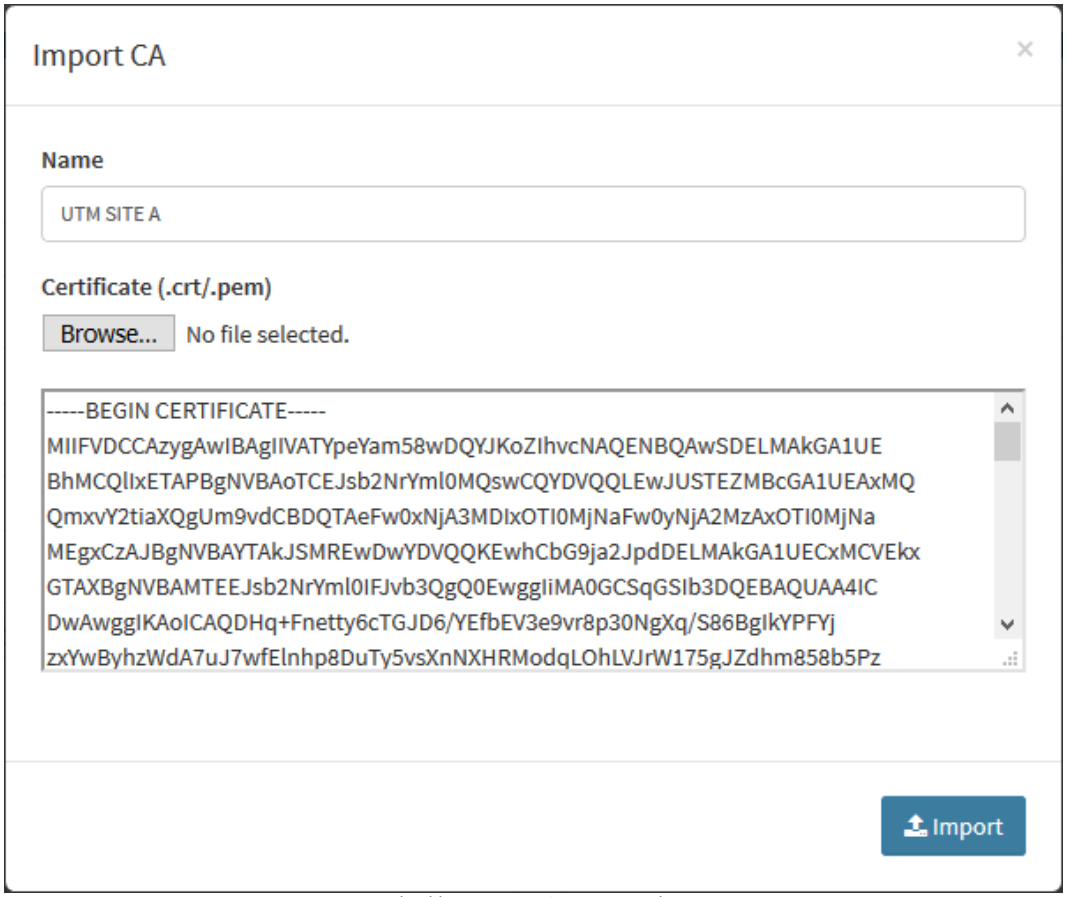
The certificate must be in the ".crt" or ".pem" format. The file containing the certificate, includes the identity information, public key, expiration date and signature.

To import the certificate, click **[ ]**.



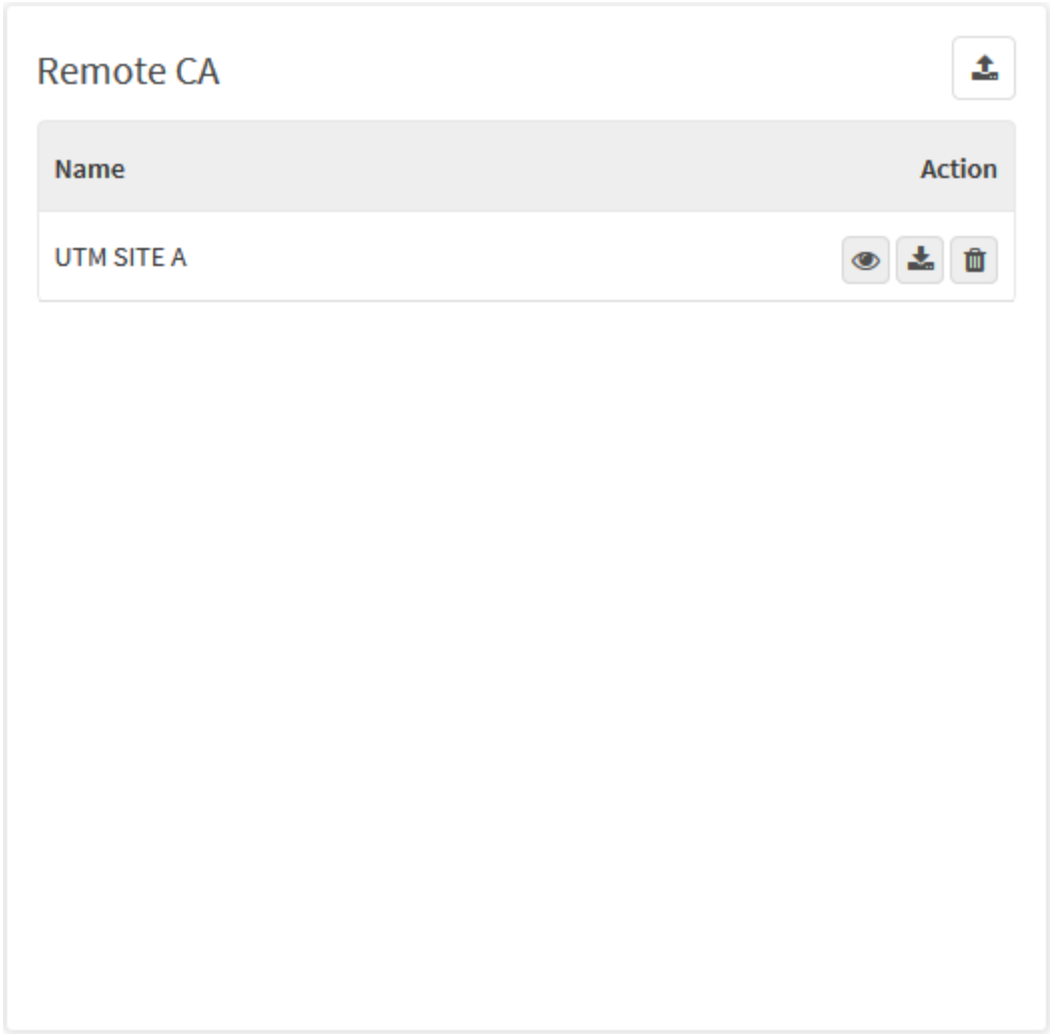
Authorities - Import CA

Select the corresponding files for the import, click **[** Browse... **]** and name it according to what you want.



Authorities - Import CA - Import done

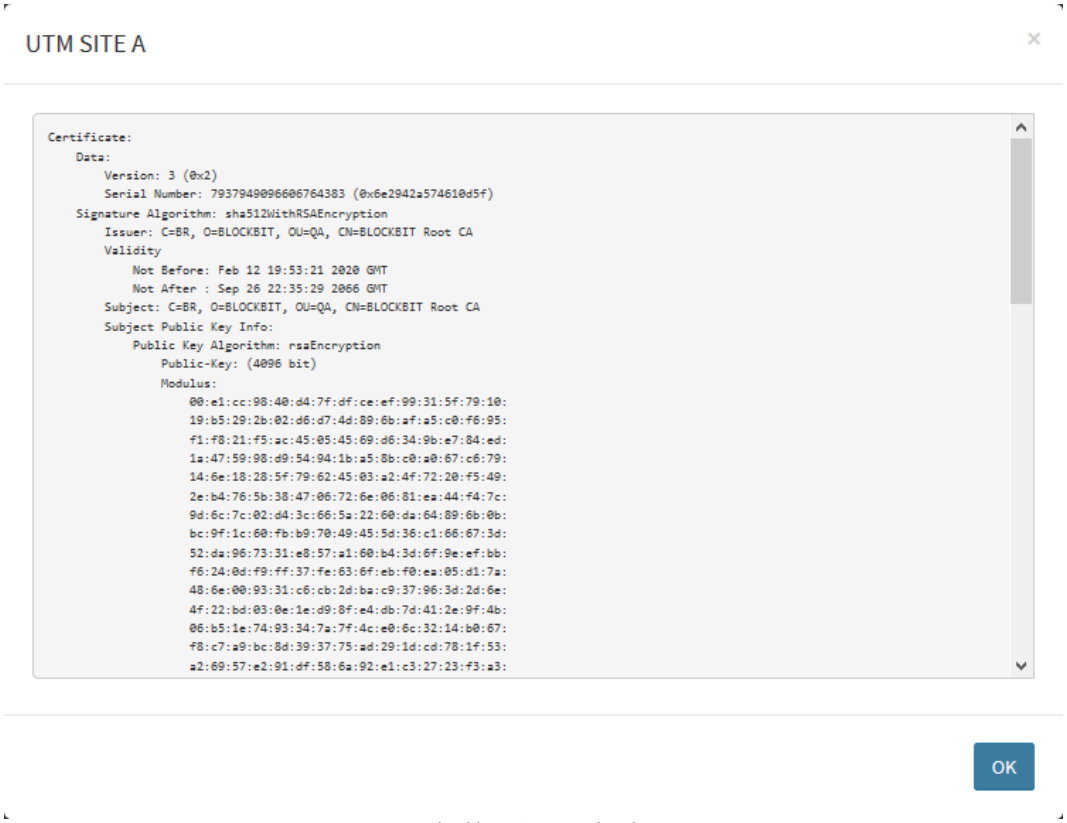
Click **[**  **]** to add it to the Remote CA list, as shown below:



Remote CA - Listed certificates

At the top of this panel we have options similar to those displayed in the *Local CA* panel;

- ***View*[ ]:** By clicking on this button it is possible to view the certificate, as shown below;



Authorities - CA Local - View

- ***Download*[ ]:** As with Local CA, it serves to download the certificate;
- ***Delete*[ ]:** Only in case of special needs can the administrator generate a new one (CA - Certificate Authority).

Certificates - Services tab

We have already seen that Certification Authorities are companies responsible for validating the identity of a web application.

This validation is performed using digital certificates or services.

It is very important to understand the distinction between the digital certificate and the service certificate and also who can have or use these certificates.

The digital certificate is an electronic document that guarantees and protects online transactions and the virtual exchange of documents, messages and data that have legal validity. With this technology, the system can validate and reinforce online security mechanisms, through this technique it is possible to guarantee privacy and confirm the authenticity of user information and access to applications related to the certificate.

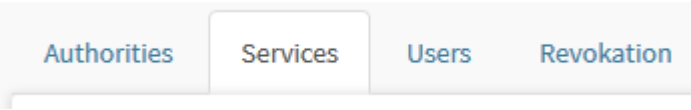
The certificate may be held by an Individual, Legal Entity, Equipment or Application. Examples of ownership: In the case of Equipment / Application, we can exemplify a server certificate (service) issued to a common name (domain host) of your network.

In this item, the administrator can register, import, view and manage Certificates of Services “**CS - Certificate Services**” each for a purpose.

BLOCKBIT UTM WEB interface.

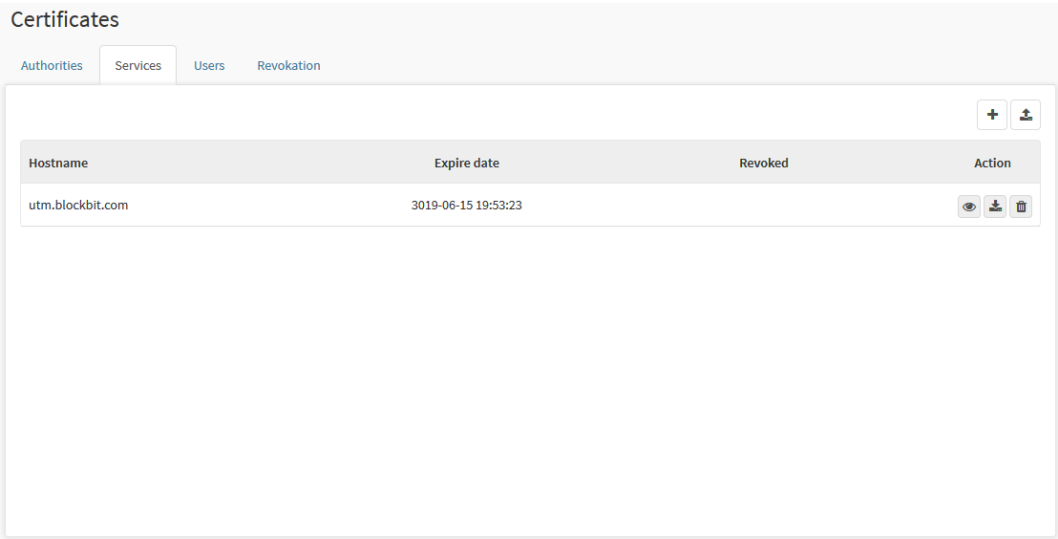
- Web authentication or Captive portal;
- SSL interception on proxy accesses;
- IPSEC RAS VPN;
- SSL VPN Site-to-site;
- SSL VPN RAS.

To access the interface click on the Services tab.



Services tab

The screen will appear, as shown by the image below:



Certificate – Services

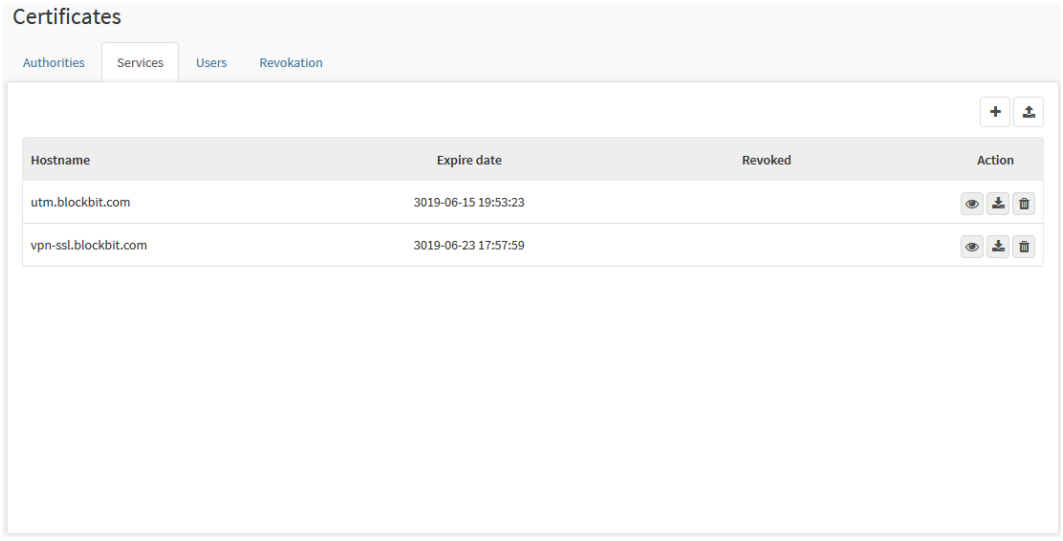
Service Certificates are used to resolve server host names corresponding to services published on the network, so it is important to remember that names (hosts) that are added or configured as “**Service Certificates**”, must be registered and configured in the service DNS, in this way, it can resolve the names corresponding to the services published through its BLOCKBIT UTM.

Services - Add button

To register a service certificate, click on **[ ]** and fill in the Hostname field with the name corresponding to the service that will use the certificate as a validator.

Services - New service certificate

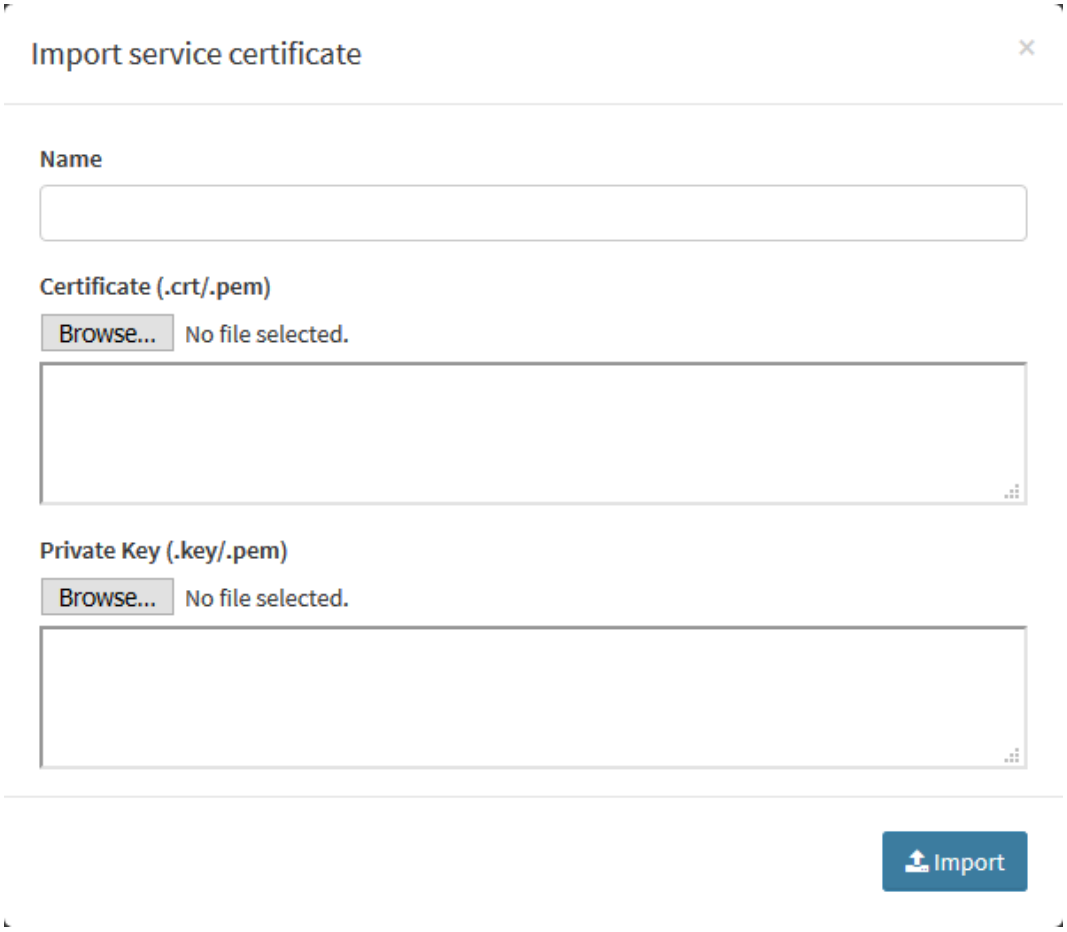
When the addition is complete, the certificate will be displayed:



Services - New service certificate installed

Services - Import button

To import a signed Certificate, click on [ ], and fill in the Name field with the name corresponding to the service that will use the certificate as a validator, once this is done, specify the locations from which the certificates will be imported.



Services - Import service certificate

- ***Name*:** Defines the name of the certificate to be used;
- ***Certificate* [*.crt*/*.pem*]:** The ".crt / .pem" certificate contains the certificate, including identity information, public key, expiration date and signature;
- ***Private Key* [*.key*/*.pem*]:** The ".key / .pem" certificate contains private identity information.

Click [Browse...] and select each corresponding certificate, after this step, click [Import].

Normally imported CS - "Certificate Services" or "Service certificates" correspond to a valid "C.A - Certificate Authority" or a "Remote CA".

Extensions related to digital certificates:

Digital certificate related extensions

Extension	Description

.kdb	*Key Database File*
.p12	*PKCS-(Public Key Cryptography Standards) #12 Data File*
.csr	*Certificate Signing Request*
.pem	*PEM Encoded Certificate File*
.crl	*Certificate Revocation List*
.p7m	*PKCS#7- (Public Key Cryptography Standards) - Encrypted Message*
.sst	*Microsoft Serialized Certificate Store*
.pkcs	*PKCS - (Public Key Cryptography Standards) – File*
.dsa	*PKCS7 - (Public Key Cryptography Standards) - Signature*

Certificates - Users tab

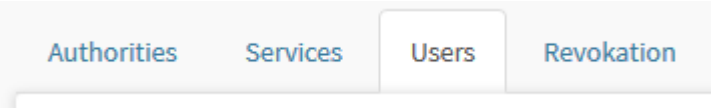
Certificates are usually issued to a specific web application server, services or even users, for specific purposes, validity times and recipients.

We have already seen the certification authorities and service certificates, in this item we will see user certificates, which are used as a security factor in processes and services that require authentication or presentation of credentials.

Two-factor authentication, also known as 2FA, is additional information that is used to allow access to a particular service. In this case, when this feature is enabled on services that require user authentication, it must have a user certificate to validate its credential and thus, have its authorized access on the respective service.

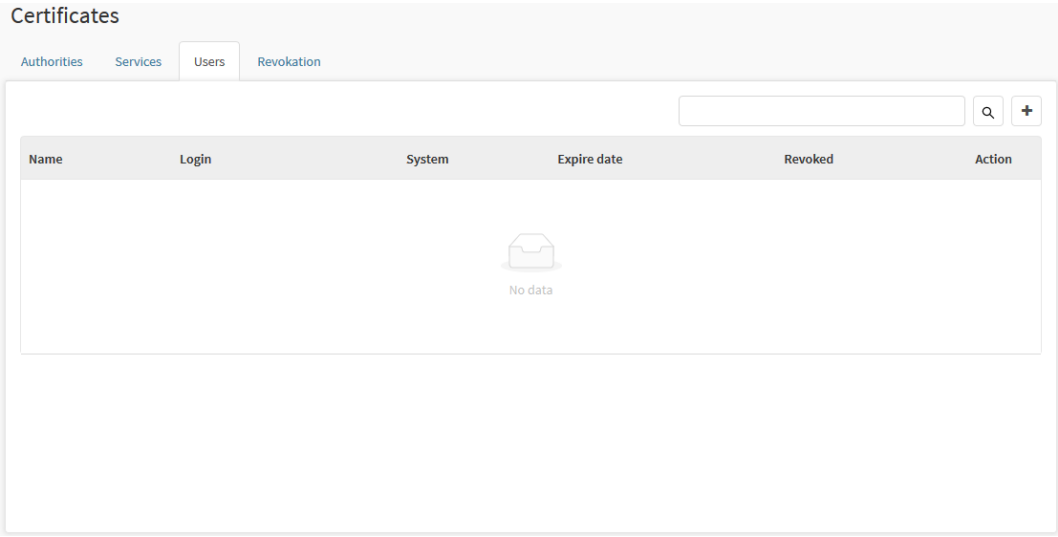
In this item, the administrator can manage, register and view user certificates for multiple operating systems.

To access the interface click on the Users tab.



Users tab

The screen below will appear:

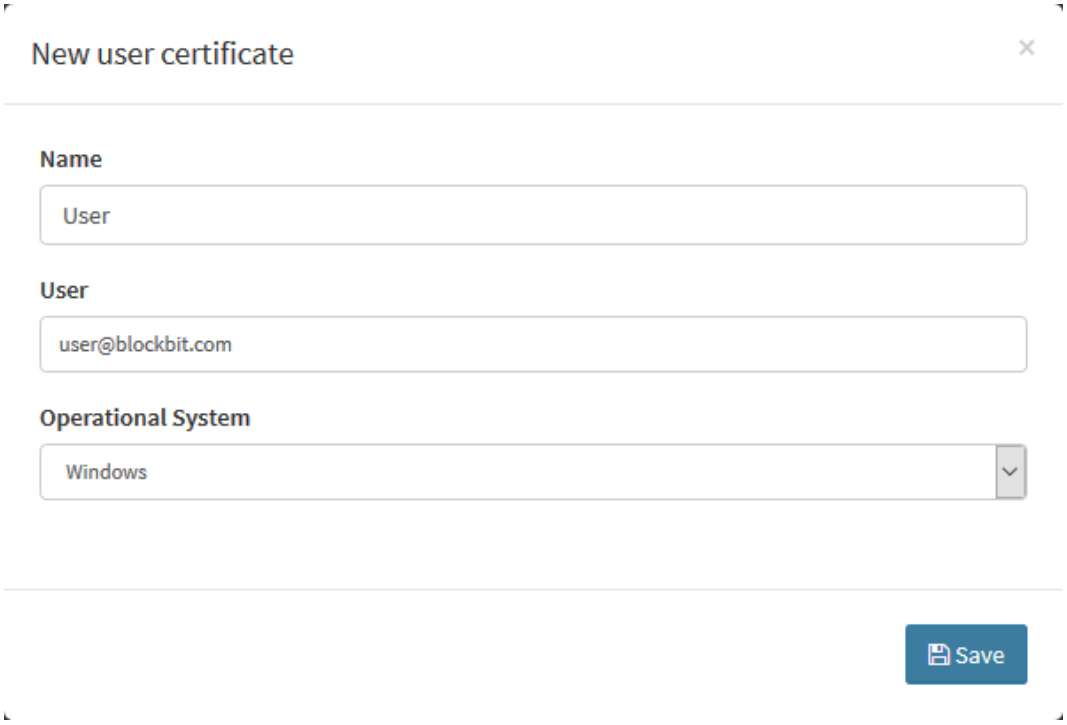


Certificate Management – Users

Next, we'll look at how to add a user on this screen.

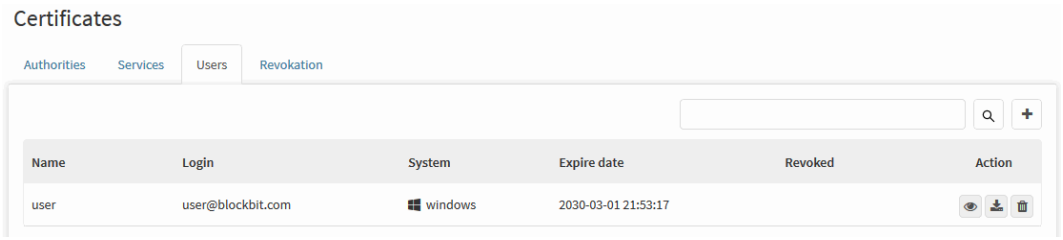
Users - Add button

To register a user certificate, click on [+] and fill in the Name field, and select the corresponding User from the list and associate it with the Operating System of your origin connection according to the supported list.



Users - *New user certificate*

Click the [Save] button to complete the addition.



Users - New user certificate installed

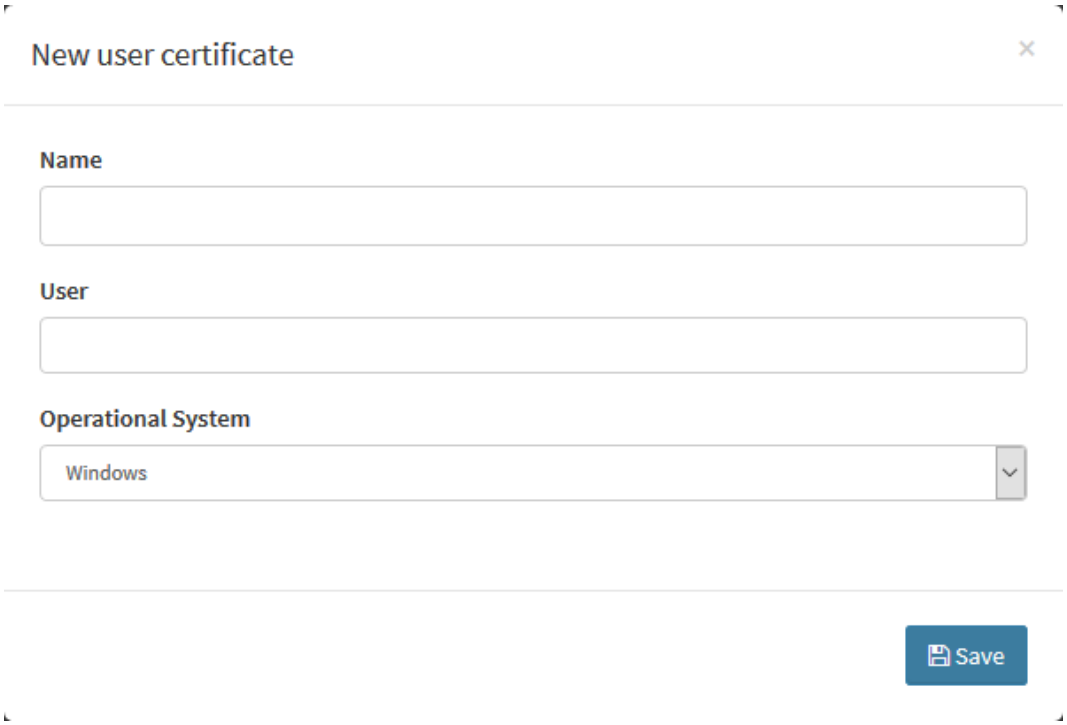
Certificate management supports “Multiple” user certificates for multiple Operating Systems.

Users - Installing a user certificate

In the example that we will present, we already have a base of users registered in a local domain "blockbit.com".

After ensuring that user certificates have already been created, access the SSL certificate management area to download C.U. (Certificate User).

Click the **[+]** button, the following window will be displayed:



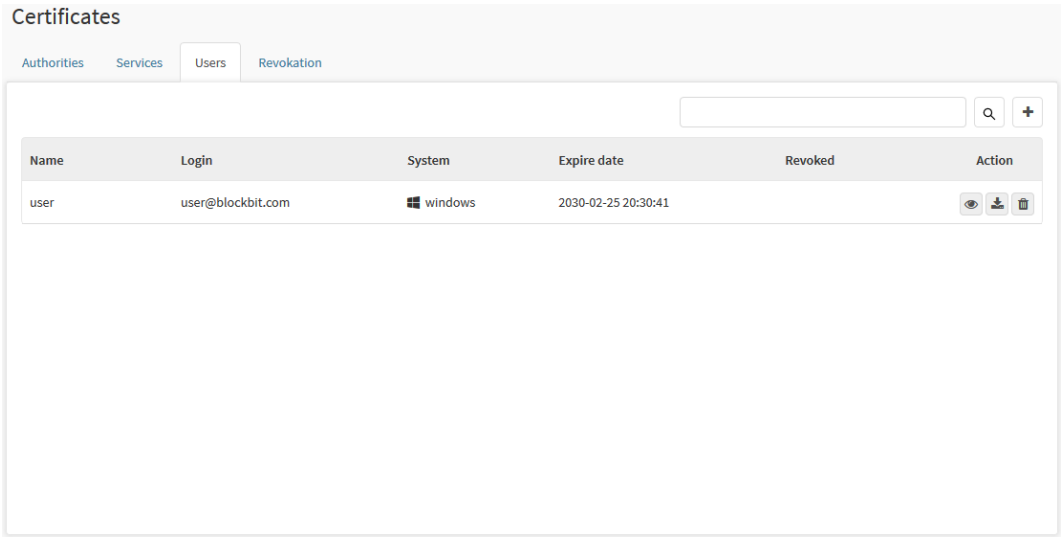
Certificates - New user certificate

- ***Name*:** Add username.
- ***User*:** Select the user used in the certification.

Users added in this window are registered in authentication, for more information check this page.

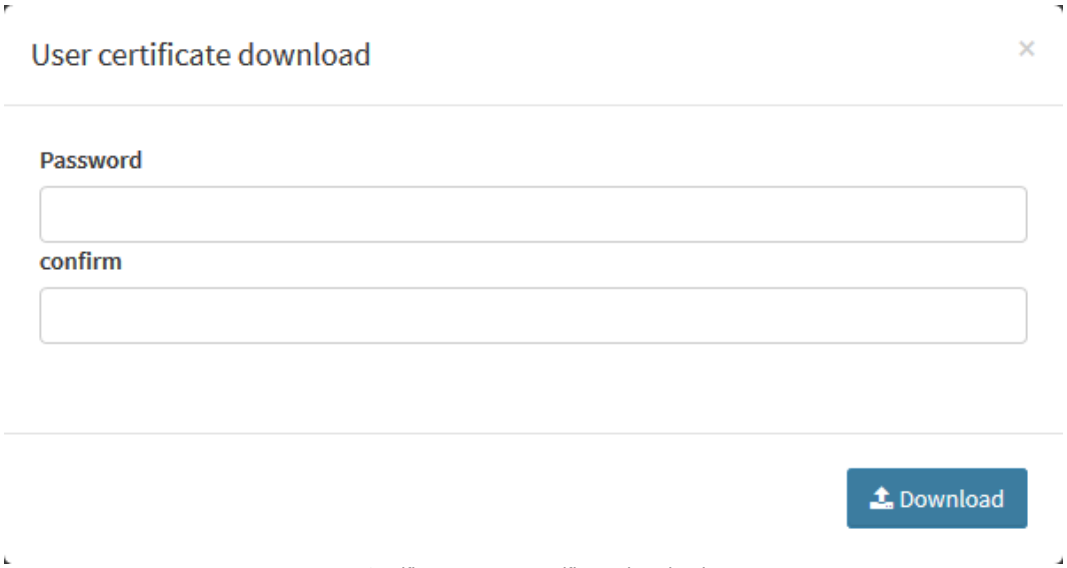
- ***Operational System*:** Select the operating system to be used, the available options are:
  - *Windows*;
  - *Linux*;
  - *macOS*;
  - *Android*;
  - *Iphone*;
  - *Windows Phone*.

Click **[Save]** to save the settings.



Certificates - Install user´s certificate

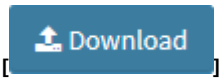
Select the desired user from the list and click **[**  **]** to download the certificate. The following window will be displayed:



Certificates - User certificate download

At the time of “Download” it is necessary to define a password (Master key), which will be requested when installing the certificate.

⚠ Only the user “owner” of the certificate must have the value of this password “Master key”. That guarantees that only "he" has the right or permission to install the corresponding certificate.

Click the **[**  **]** button to download the certificate.

There are two ways to install the certificate:

- *MMC*;
- *Auto Install*.

Next, we will analyze each of these modes:

MMC

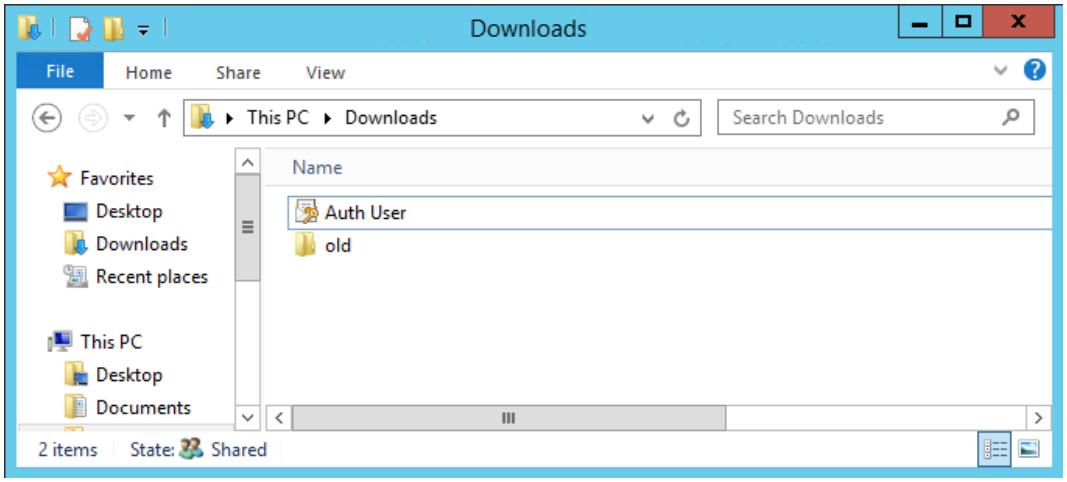
MMC is a Microsoft management console for installing and configuring Apps (applications) on the local station.

Auto Install

Auto execution of the certificate, which makes a call to the “Windows installer” that runs a “Wizard” (an installation wizard).

Exemplifying the installation of user certificates on the respective workstations by the Auto Install method.

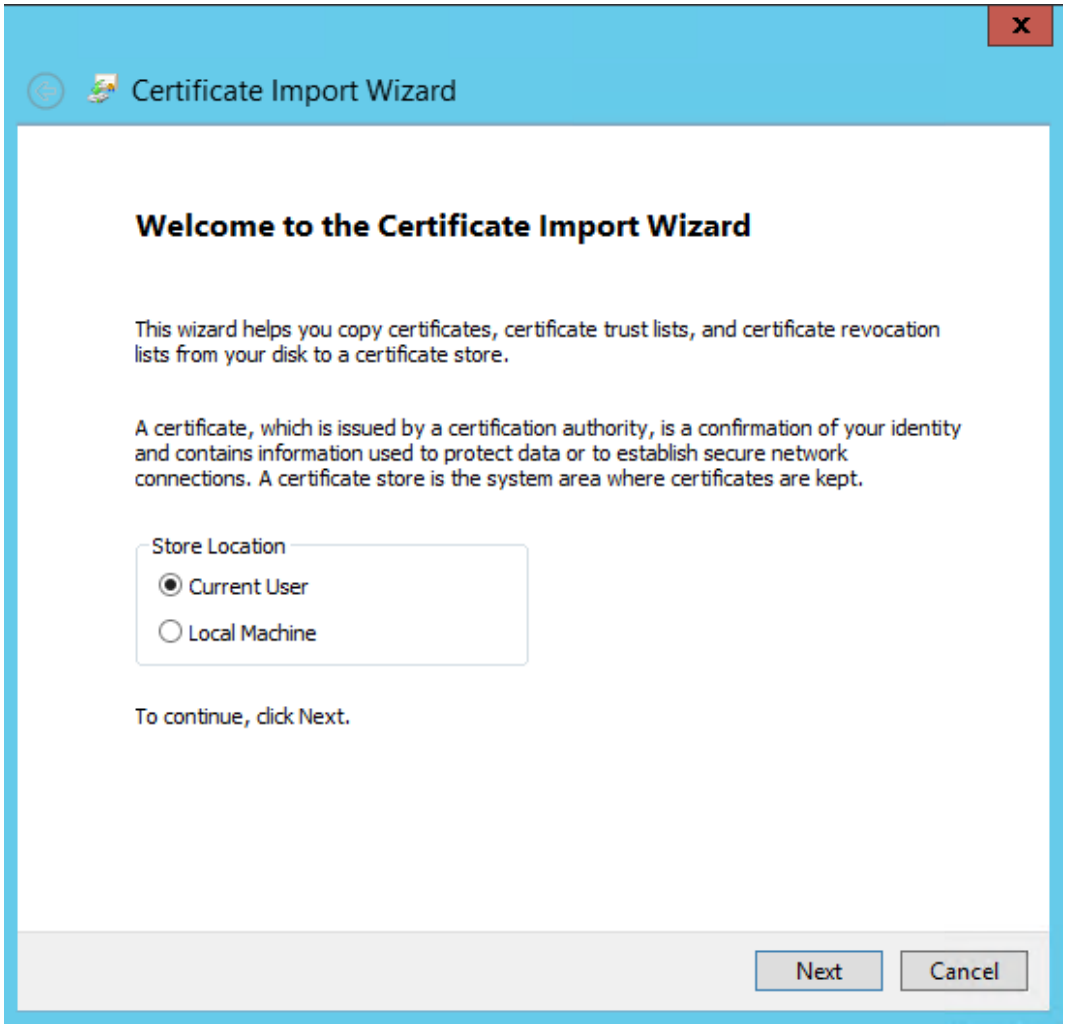
Locate the file saved on the respective workstation and perform the Auto Install of the user certificate.



Install user certificate

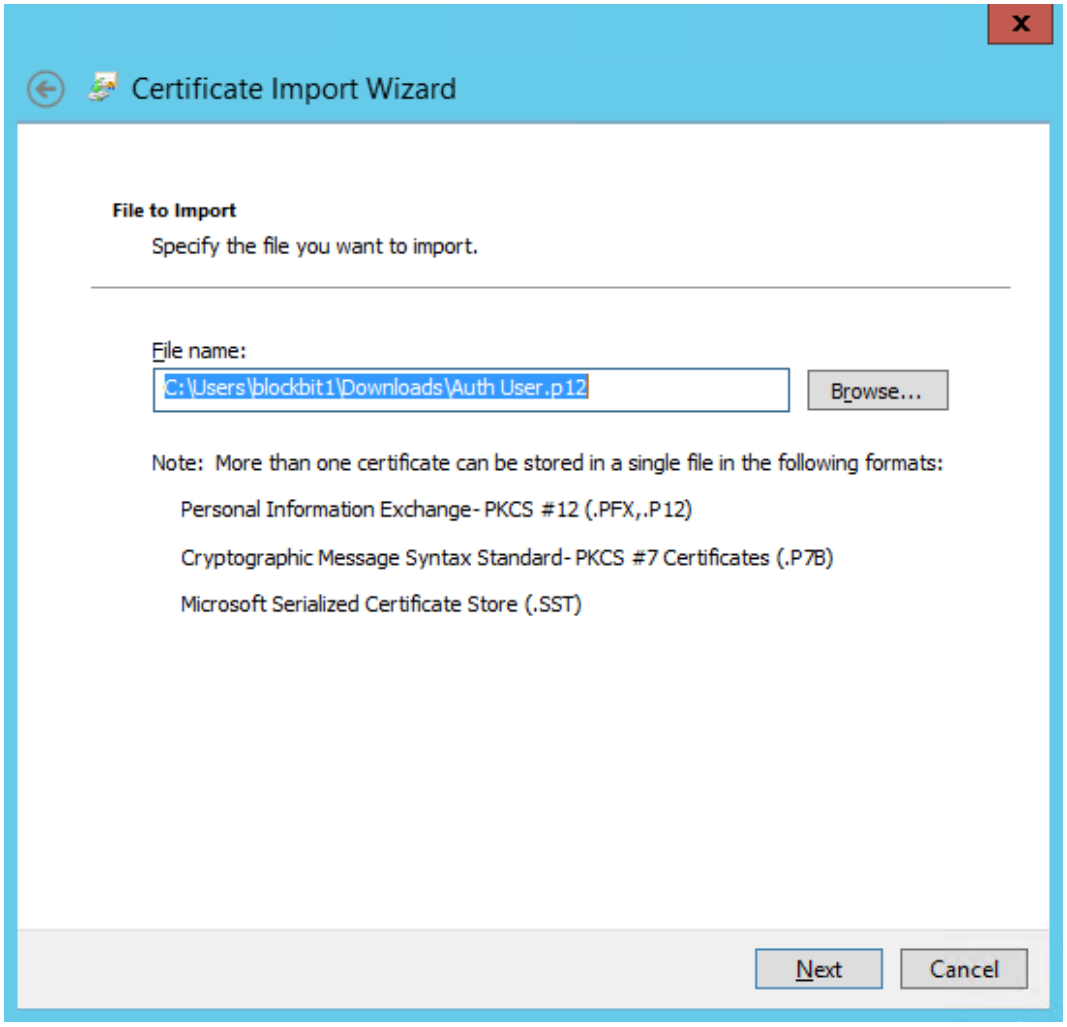
Click on the **[.p12]** file by following the steps in the **[Certificate Import Wizard]**.

Select the repository location **[ ]** Current User and click **[Next].**



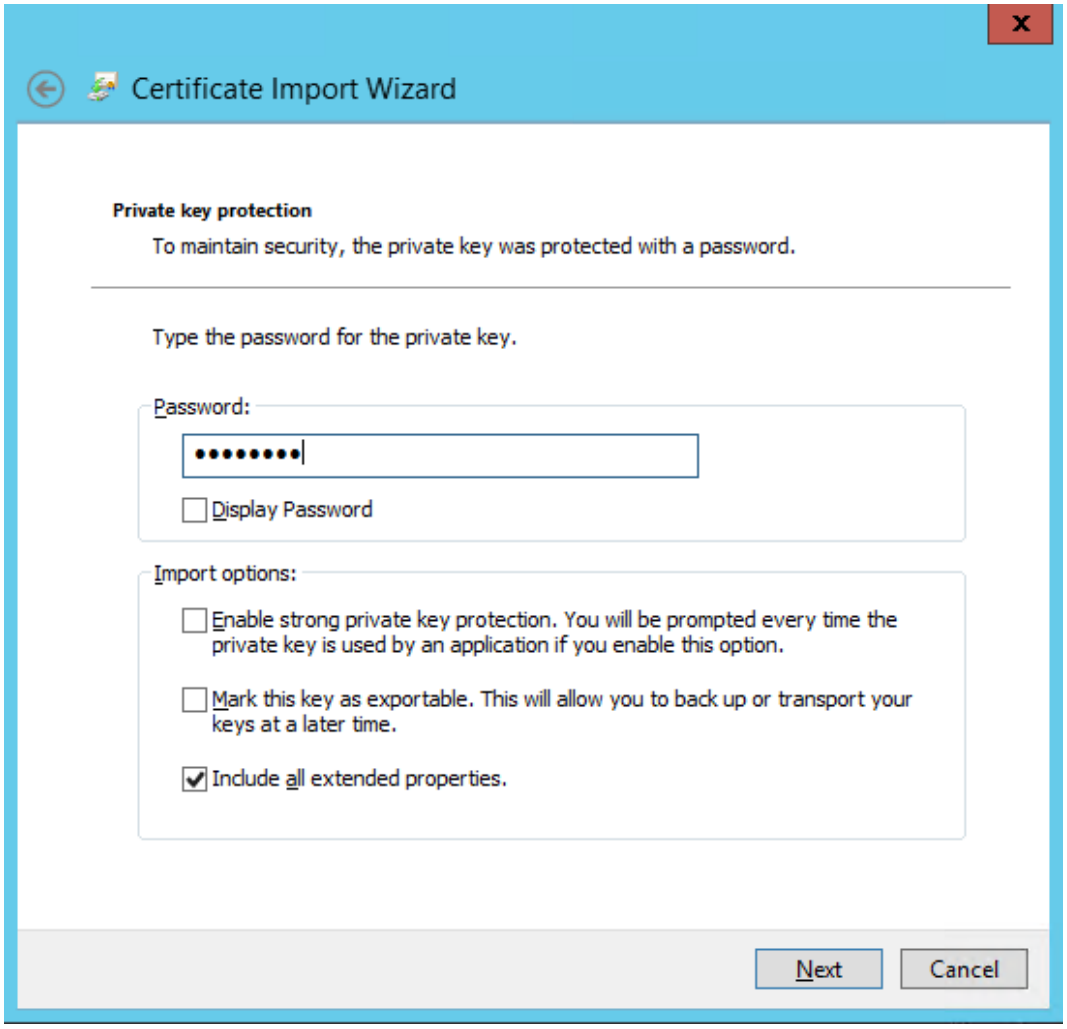
Certificate Import Wizard

Locate and specify the file to import, Ex.: *"C:\Users\$User\DownloadsAuth_User.p12"*. Click **[*Browse*]**, then click **[Next].**



File import

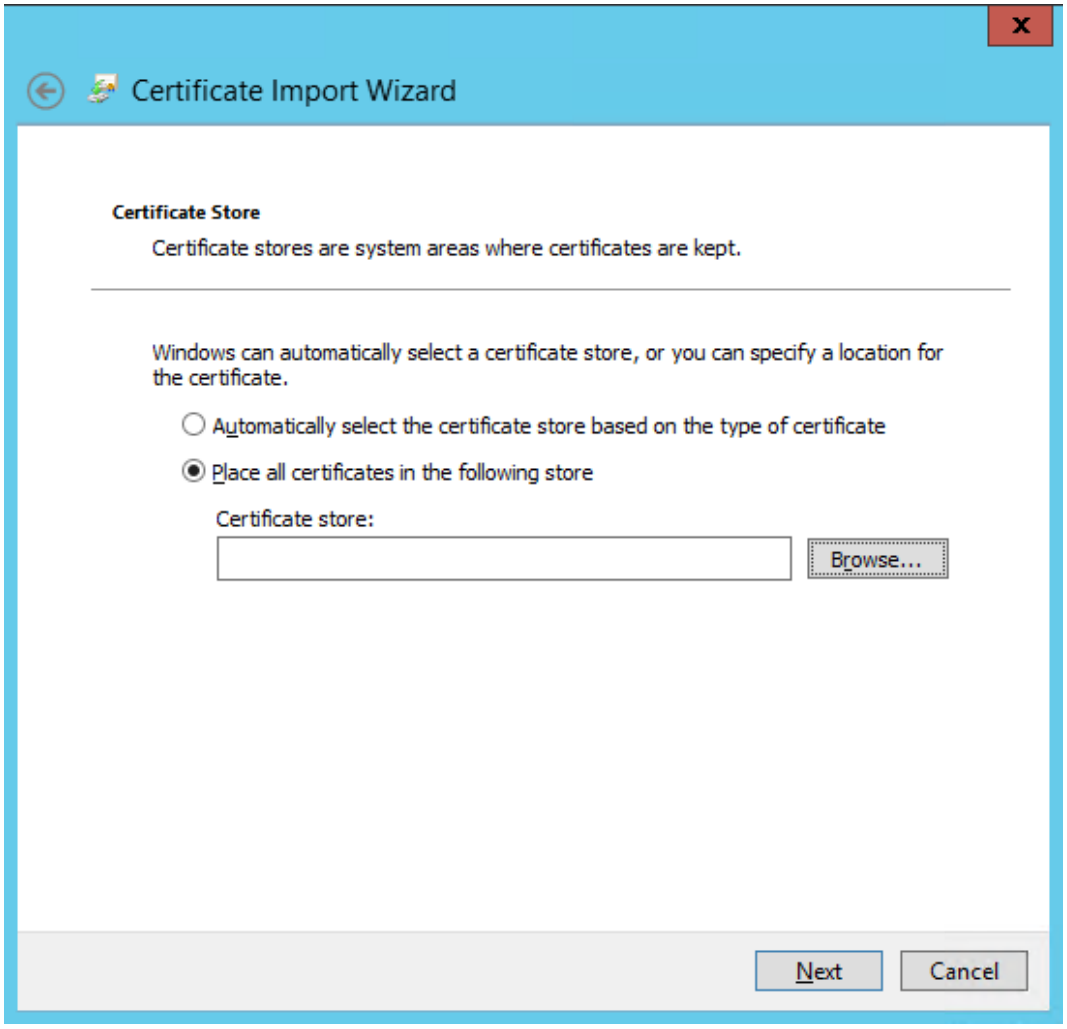
Enter the protection password to access the private key. The Password refers to the password “Saved” when downloading the user certificate. Click on **[Next].**



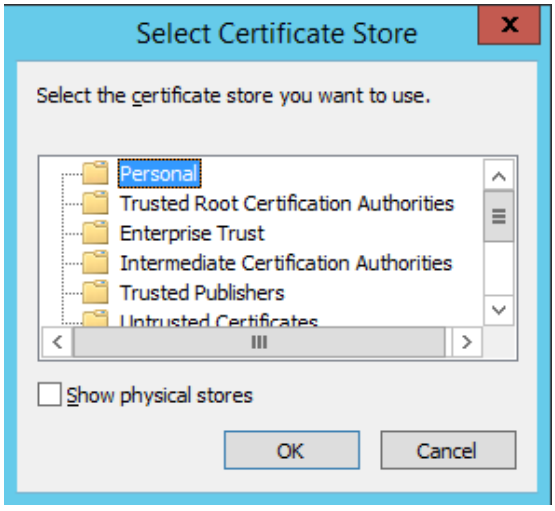
Private key protection

Change the selection to the repository where the user certificate will be installed.

[ ] ***Place all certificates in the following store...*** Click on **[Browse]**

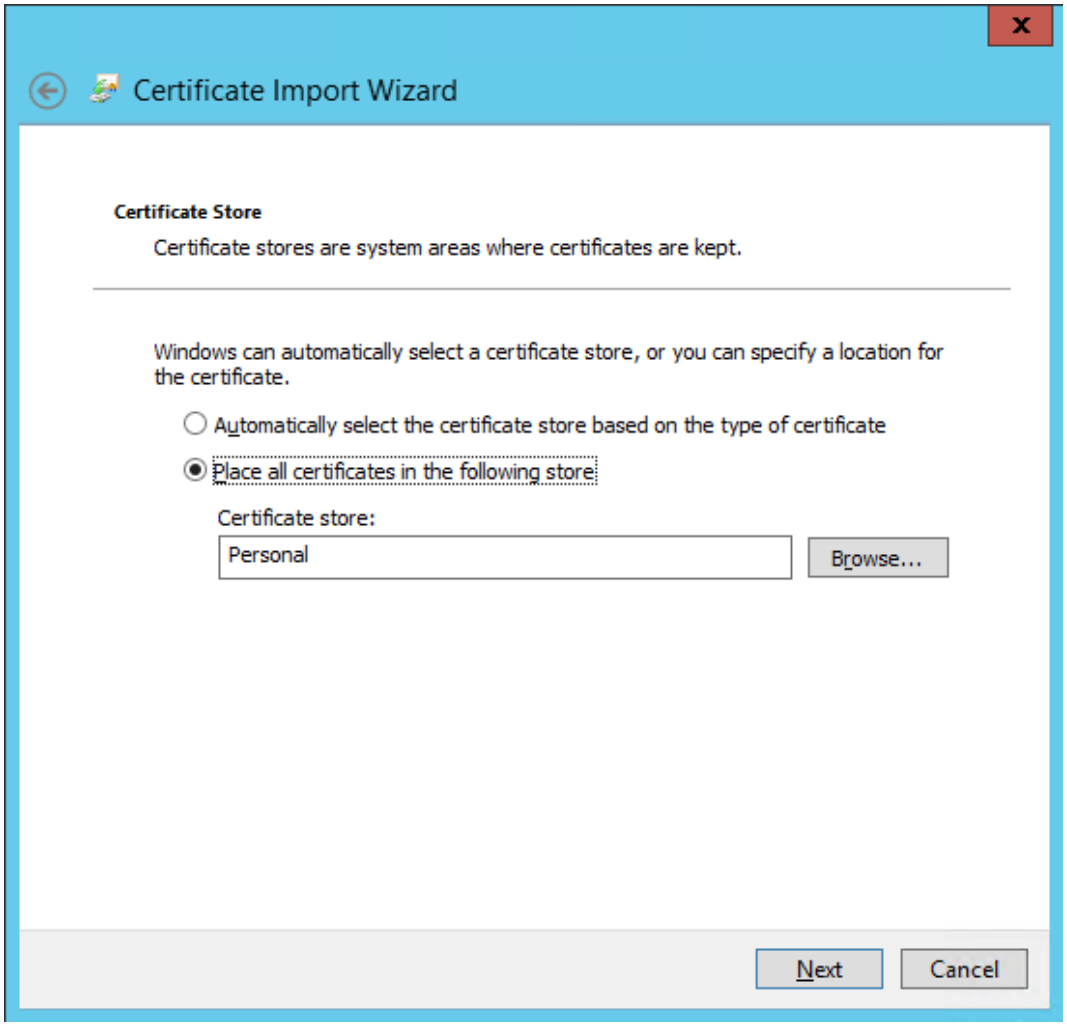


Select certificate Store



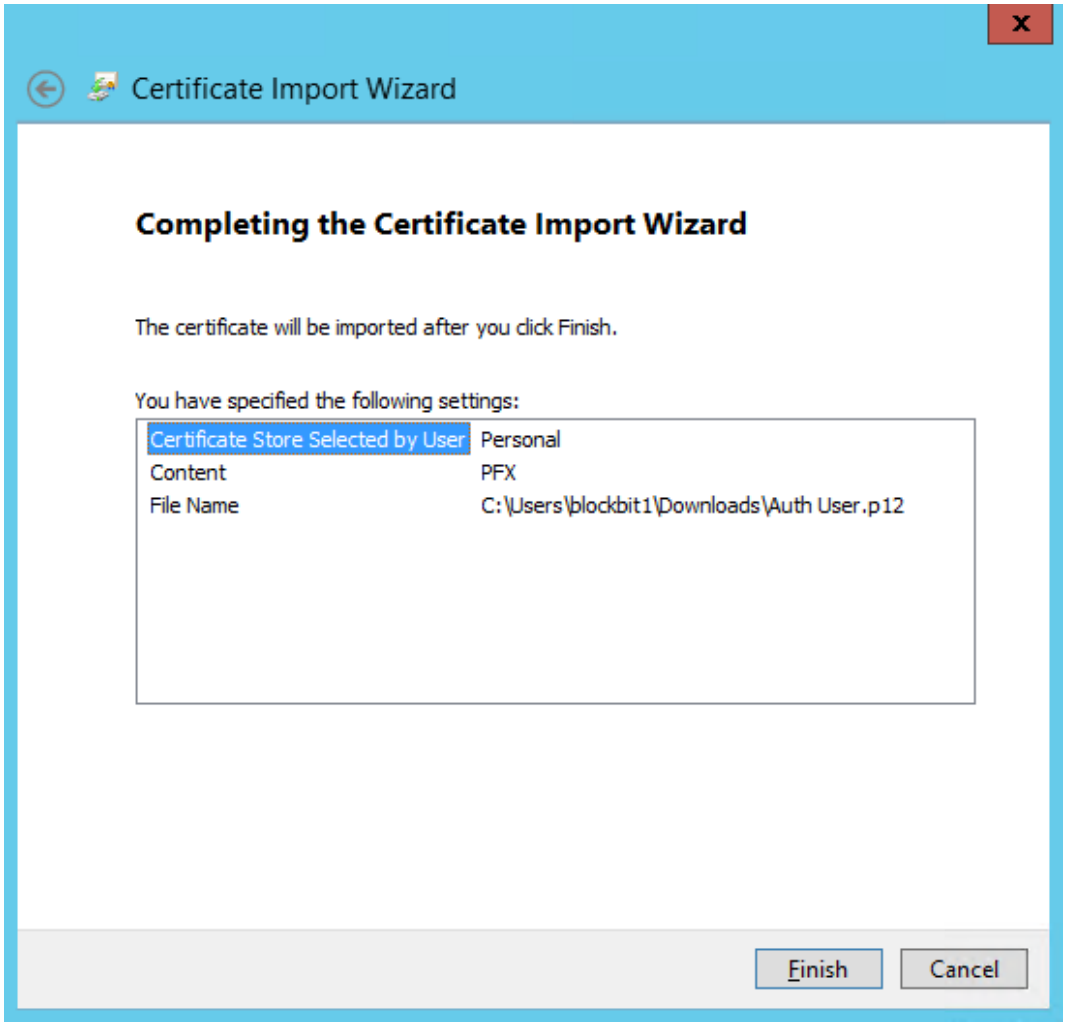
Definition certificate store

Select the **[Personal]** folder and click **[OK]** and then **[Next]**.



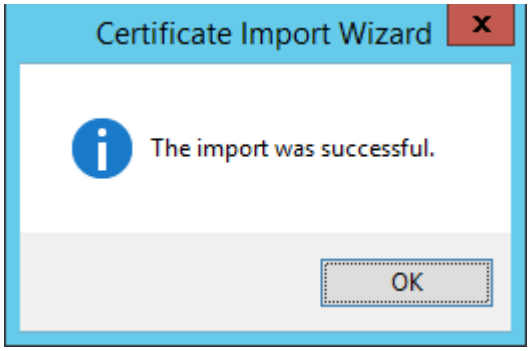
Finish certificate import Wizard

Completing the user certificate installation wizard, check that the repository selected for installation and the file corresponds to the respective user and click **[Finish]**;



Finish certificate import Wizard

Finally, the wizard returns a notification that the Import was successful. Click **[OK]**.



The import was successful

Certificates - Revokation tab

Digital certificates are electronic documents with a determined validity period and may vary according to the type of certificate purchased, and the revocation of a digital certificate is the process of canceling it, when during the period of its validity.

Revocation can be requested at any time by the certificate holder, or his responsible. Whenever it is understood that there is a need to cancel it, whether due to the compromise of the security of your private key or changes to the certificate information, among other possible reasons, such as:

- When found improper or defective emission of the same;
- Loss or theft of the certificate (including the PC in the case of digital certificate A1);
- Improper access;
- Compromise or suspicion of insecurity of the private key corresponding to the public key contained in the certificate;
- Compromise or damage to the storage media, including the computer in the case of digital certificate A1;
- Finding incorrect information on the certificate;
- Need to change any information on the certificate;
- Change in the name or corporate name of the holder (equipment, applications and legal entities);
- Extinction, dissolution or transformation of the certificate holder (equipment, applications and legal entities);
- Extinction, dissolution or transformation of the AC related to the certificate.

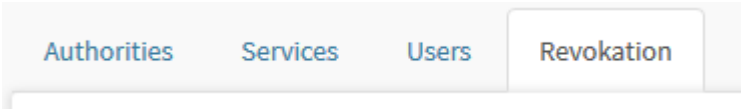
To revoke a certificate means to end its validity before the foreseen term, that is, making it impossible, from the revocation, its use.

It is important to maintain a “List of Revoked Certificates (LCRs)”, which are usually files with the extension “.crl”.

The idea is to show the certificates that are not active, revoked or canceled, specifically for that “CA - Certificate Authority” (or Certifying Authority), thus preventing an invalid certificate from being used.

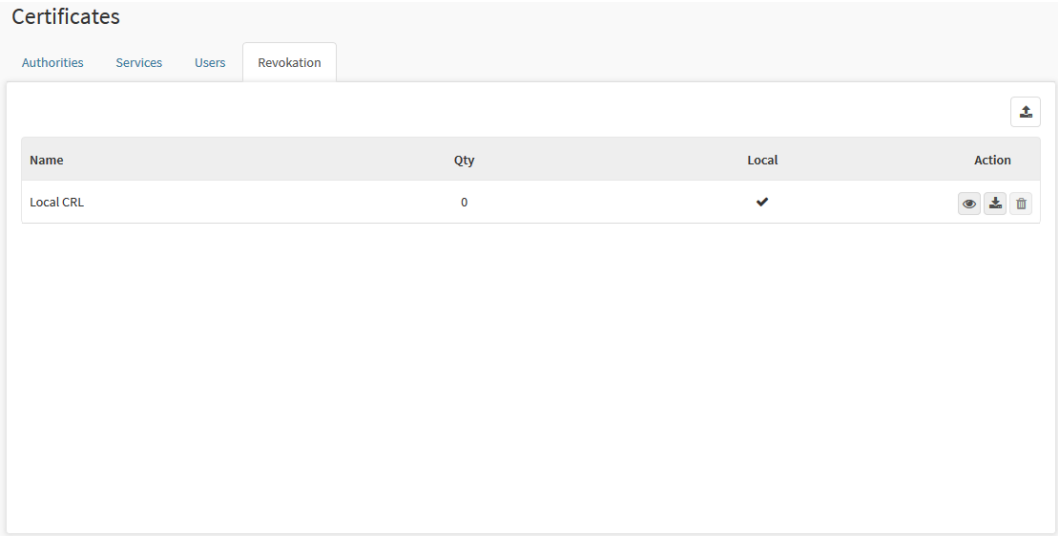
In this item, the administrator can manage the list of revoked certificates for a certifying entity (**“CA - Certificate Authority”**), view the CA data and status, if **“Valid”** or **“Revoked”**, as well as the option to **“Download”** of the ".crl" file referring to the list of revocation occurrences.

To access and manage the list click on the Revokation tab.



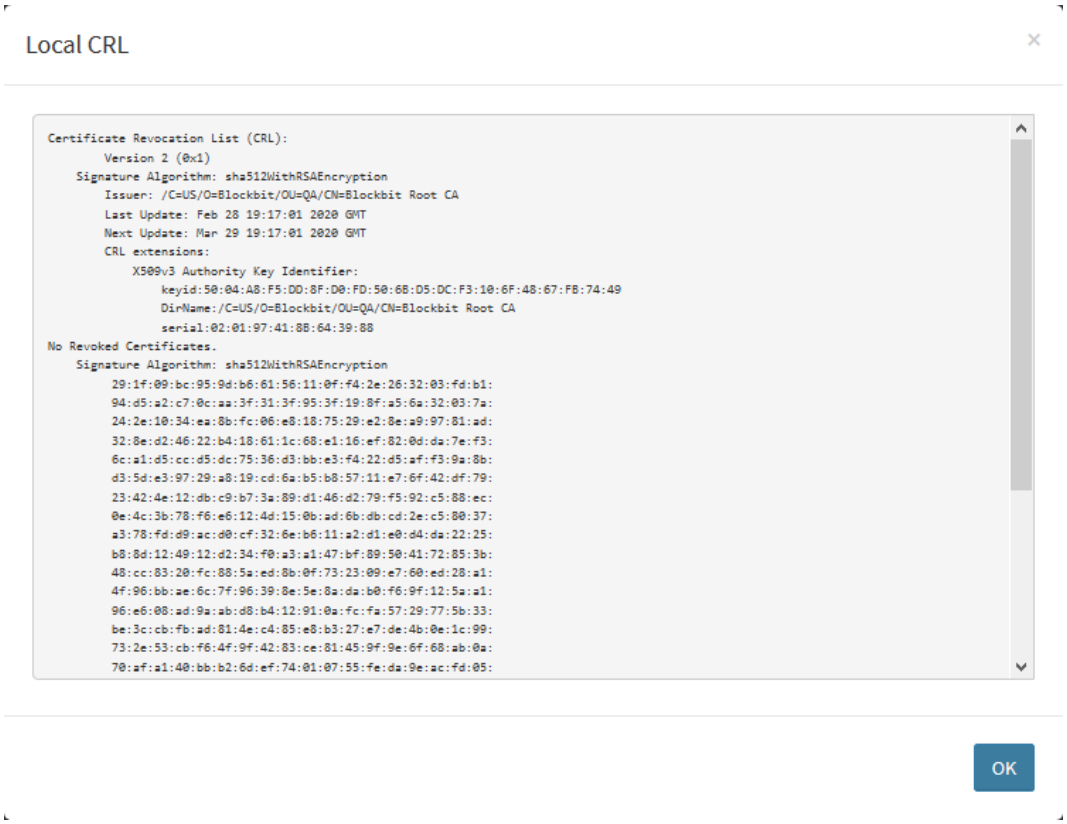
Revokation tab

The window below will appear:



Certificates - Revokation

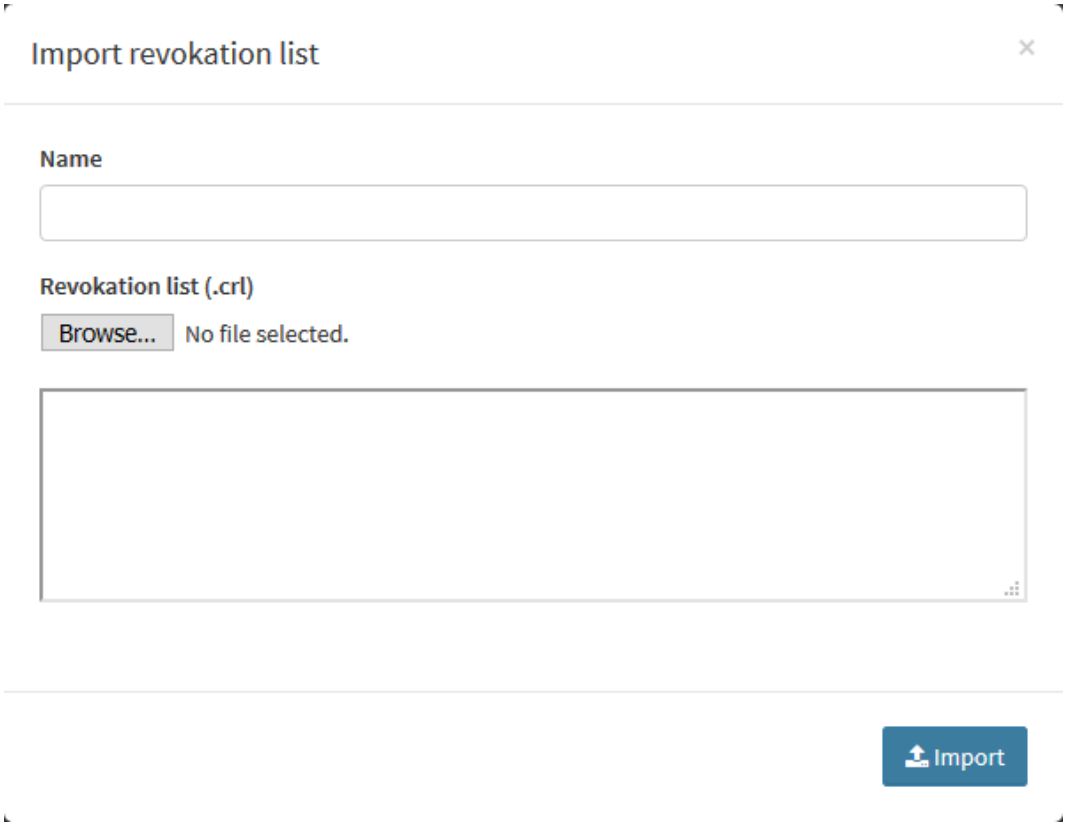
To view the CA data and its status click on [ ].



Certificate - Local CRL

Aba Revokation - Import Revocation List

To import a revocation list of Signed Digital Certificates, click [ ], the following window will be displayed:



Revokation - Import revokation list

Fill in the Name field with the corresponding name to identify the Remote CA.

Click [Browse...] and select the desired certificate, then click [Import].

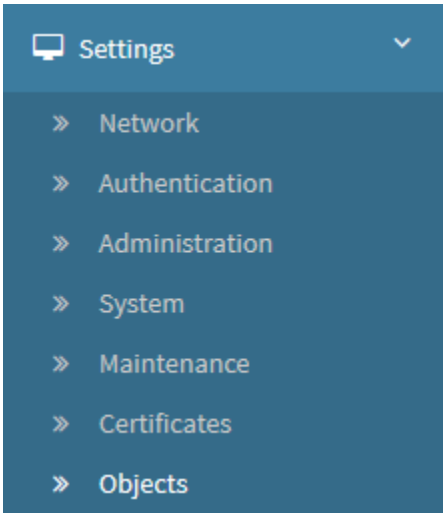
The ".crl" file contains the identity information, the list of revoked certificates and the revocation date.

UTM - Settings - Objects

The system was developed object-oriented to facilitate the process of configuration, maintenance and reading of rules. Objects are a resource whose purpose is to interact in a friendly manner with the user in order to simplify the process of setting up, enabling services and general system resources. Objects can be shared between system services.

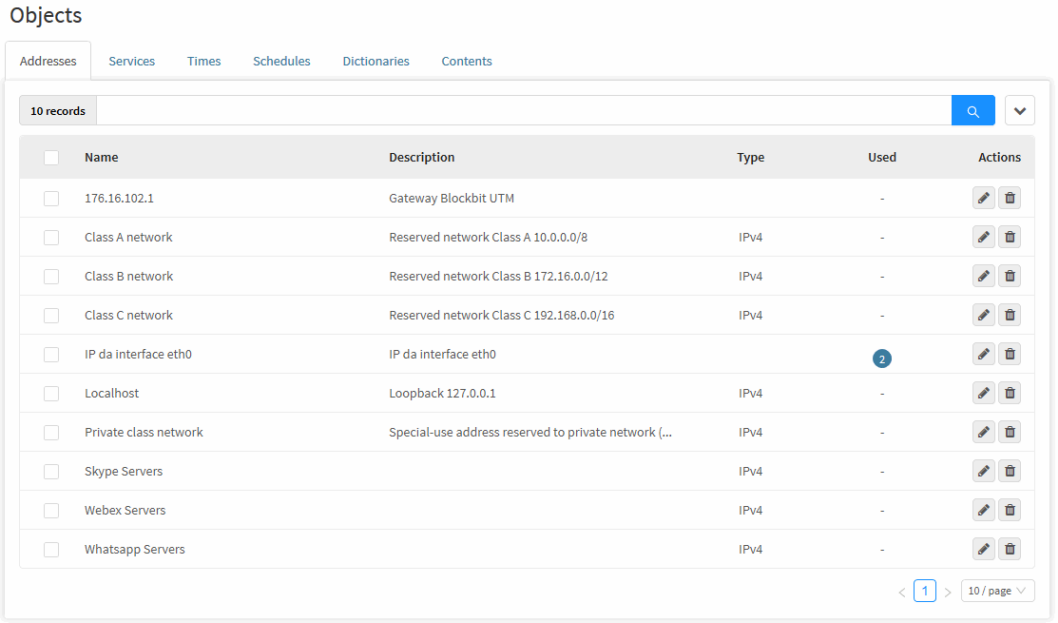
Any changes made to an object are automatically replicated and applied to all services used by the respective object.

To access the screen, just select the “Objects” option.



Settings - Objects

The following screen will be displayed, from there, we can “Add”, “Edit”, “Remove”, “Group” and even “Import” lists of some types of objects.



Settings - Objects - Addresses

The objects screen has the following tabs:

- *Addresses*;
- *Services*;
- *Times*;
- *Schedules*;
- *Dictionaries*;
- *Contents*.

Next, the components of the *Addresses tab will be analyzed.*

Addresses

Address-type objects are used to identify hosts (machines) or networks (networks).

By default, the system brings some pre-registered objects, for example, objects referring to invalid network classes: “Class A reserved”, “Class B reserved”, “Class C reserved”.

All of these objects are available to be used in the processes of configuring and enabling services. Network address objects are classified into two types:

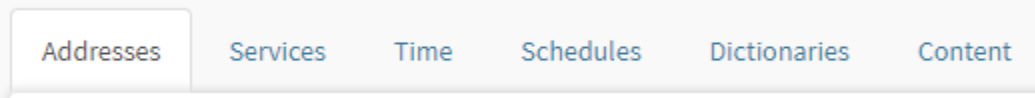
- *Unique IP*;
- LIST (support for multiple IP addresses / network address and Hosts).

This definition is applied at the time of registering the address object, which allows signaling if it will be unique or not.

Blockbit UTM allows the definition of three forms of identification of Address:

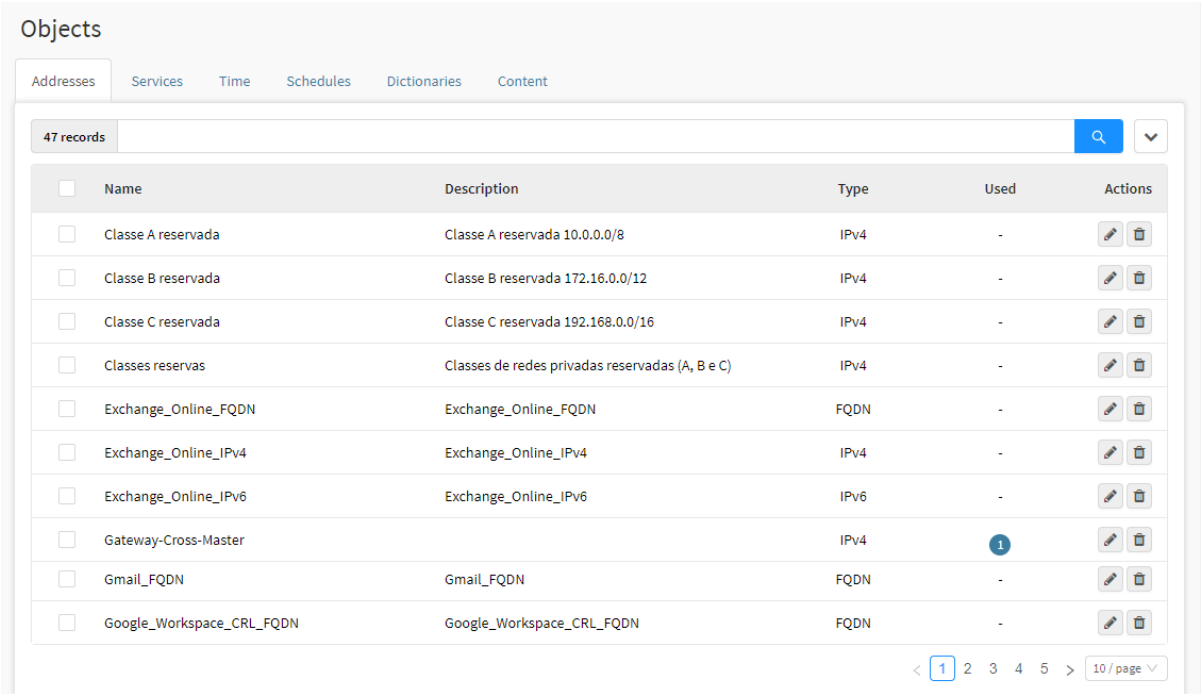
- ***IP address / Network address*:** They are objects that identify machines and networks through their IP addresses. Ex.: 172.16.102.235 ou 172.16.102.0/24;
- ***MAC address*:** They are objects that identify the machines through the physical addresses of their network cards. Ex.: 38:59:F9:1F:4E:16;
- ***FQDN address*:** They are objects that identify the machines through their DNS address. Ex.: blockbit.com or www.blockbit.com;

To access the screen, click on the “Addresses” tab:



Addresses tab

The “Adresses” screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the actions menu on the right.



Objects – Addresses

Dynamic base

The base of Address type objects is dynamic, which means that the servers address list comprehended by the object is constantly updated by the Blockbit database remotely.

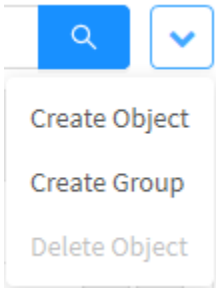
We will explain in detail the actions menu and later the columns of the "Addresses" tab.

Addresses - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions Menu

The menu consists of the following options:

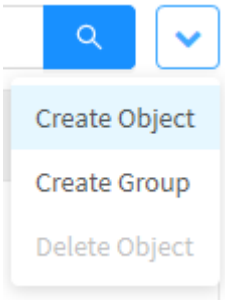
- *Create Object*;
- *Create Group*;
- *Delete Object*.

Next, each action menu option will be detailed.

Addresses - Actions menu - Create Object

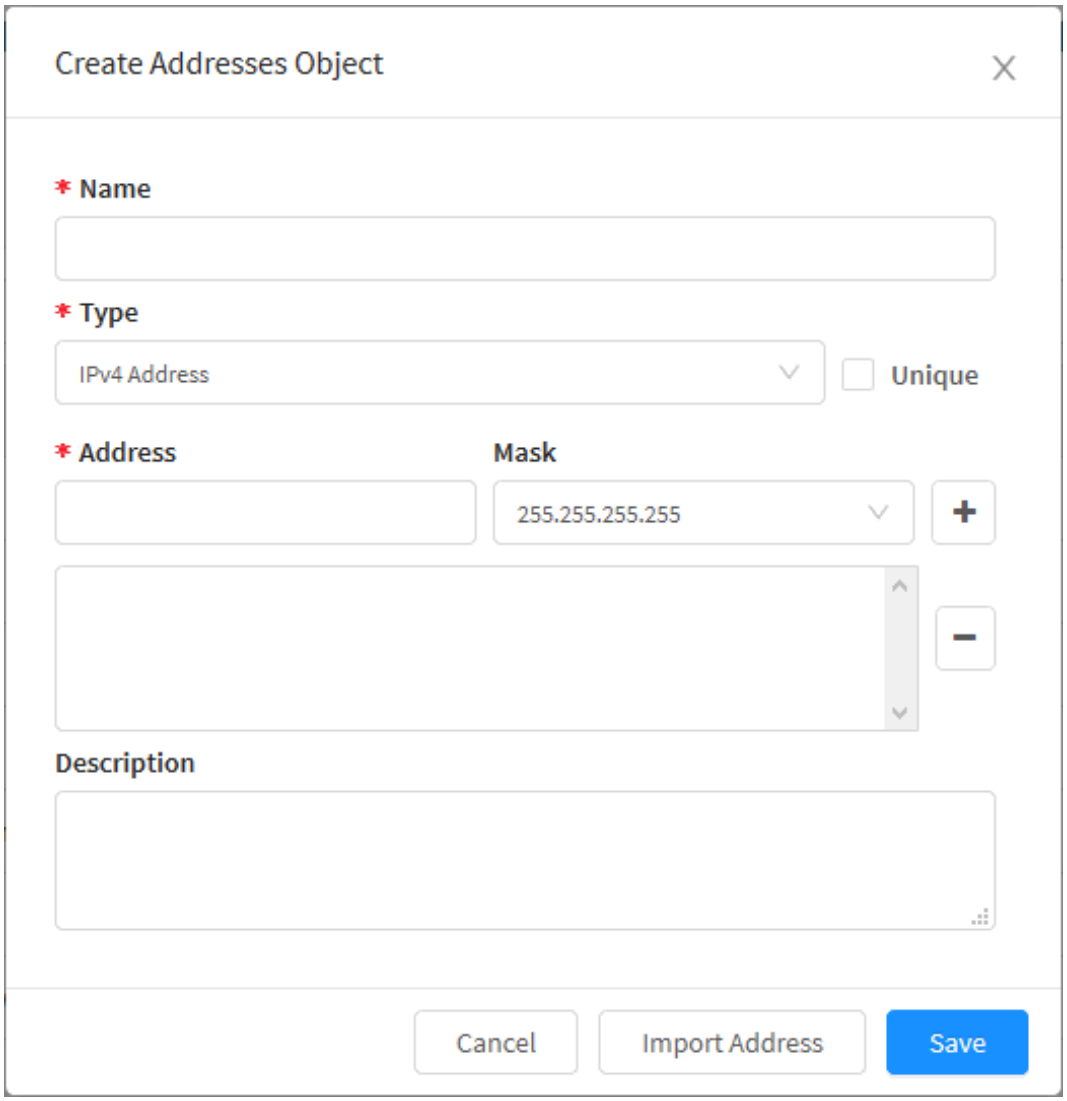
Through the option “Create Object” it is possible to create a new Object Address. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Addresses – Create Object

2. The Create Addresses Object screen will appear.



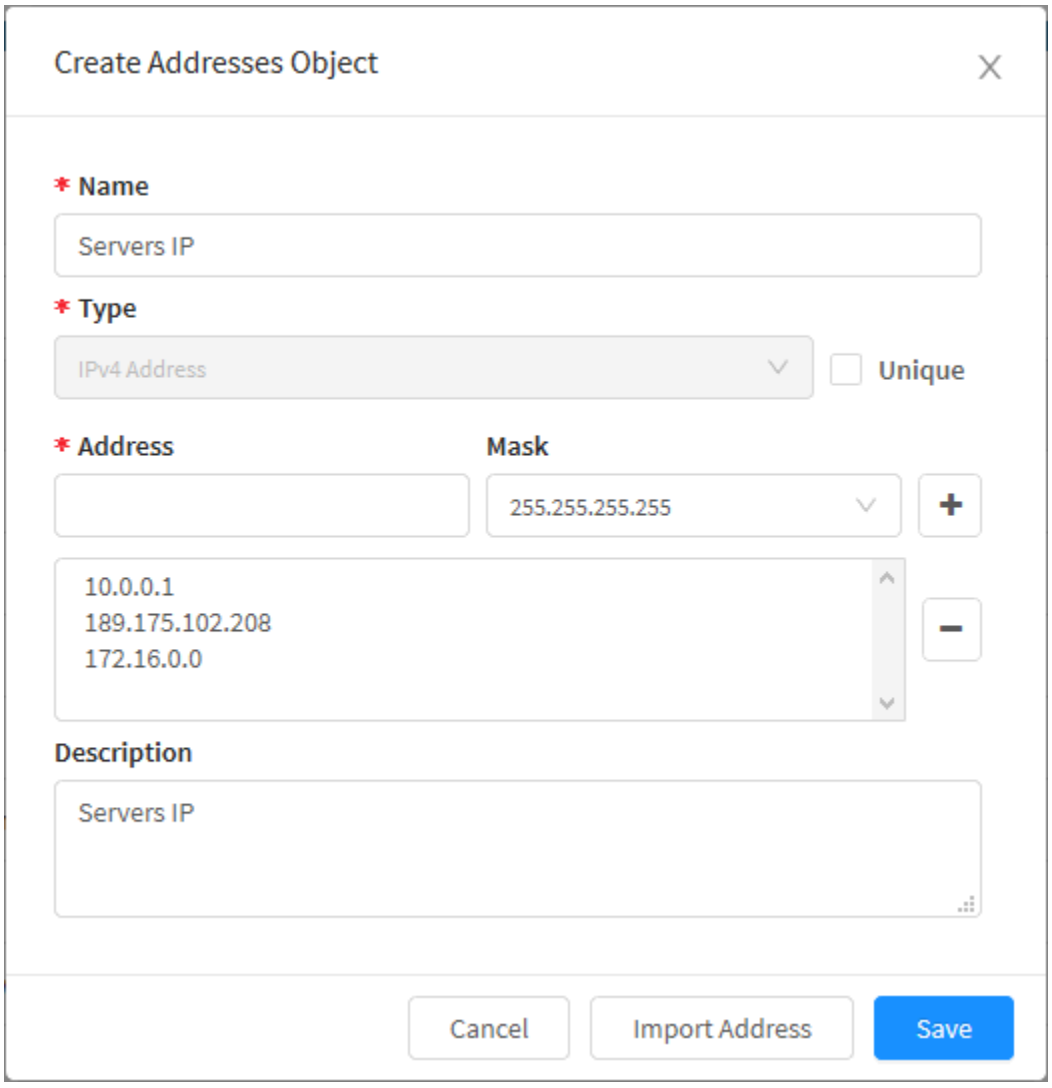
Objects – Create Addresses Object

It is possible to create IPv4, IPv6, Mac and FQDN addresses. Here are some examples on how to create address objects:

- Example 1 - Creating IPv4 Address Object;
- Example 2 - Creating IPv6 Address Object;
- Example 3 - Creating Physical Address Object.

Example 1 - Creating IPv4 Address Object

Here is a demonstration of how to create an IPv4 address object:



Objects – Create Addresses Object - IPv4

Attention: Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- ***Name*:** Object name. Ex.: *Servers IP*;
- ***Type*:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- ***Unique*[ ]:** Determines whether the address will be unique or not, disabling the Mask field;
- ***Address:*** The address of the type of connection object selected later. After entering an address, click **[+]** to add it to the list or select it and click **[−]** to remove it. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- ***Mask*:** This field will be available to add the IP address mask, if the type IPv4 Address or IPv6 Address is selected in the field "type";
- ***Description*:** This field is intended for the description of the object. Ex .: IP Servers.

When clicking on the Import Address [Import Address] button and selecting the file to be imported, clicking [+] to add the contents of the file inside the object, if you want to remove any registered address, select the IP address and click on the [−] button and the content will be removed.

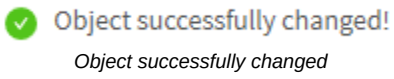
The supported format of the list is one IP or network address per line.

Ex.: 10.0.0.1

189.175.102.208

172.16.0.0/16

Click the [Cancel] button to Cancel or the [Save] button to save.

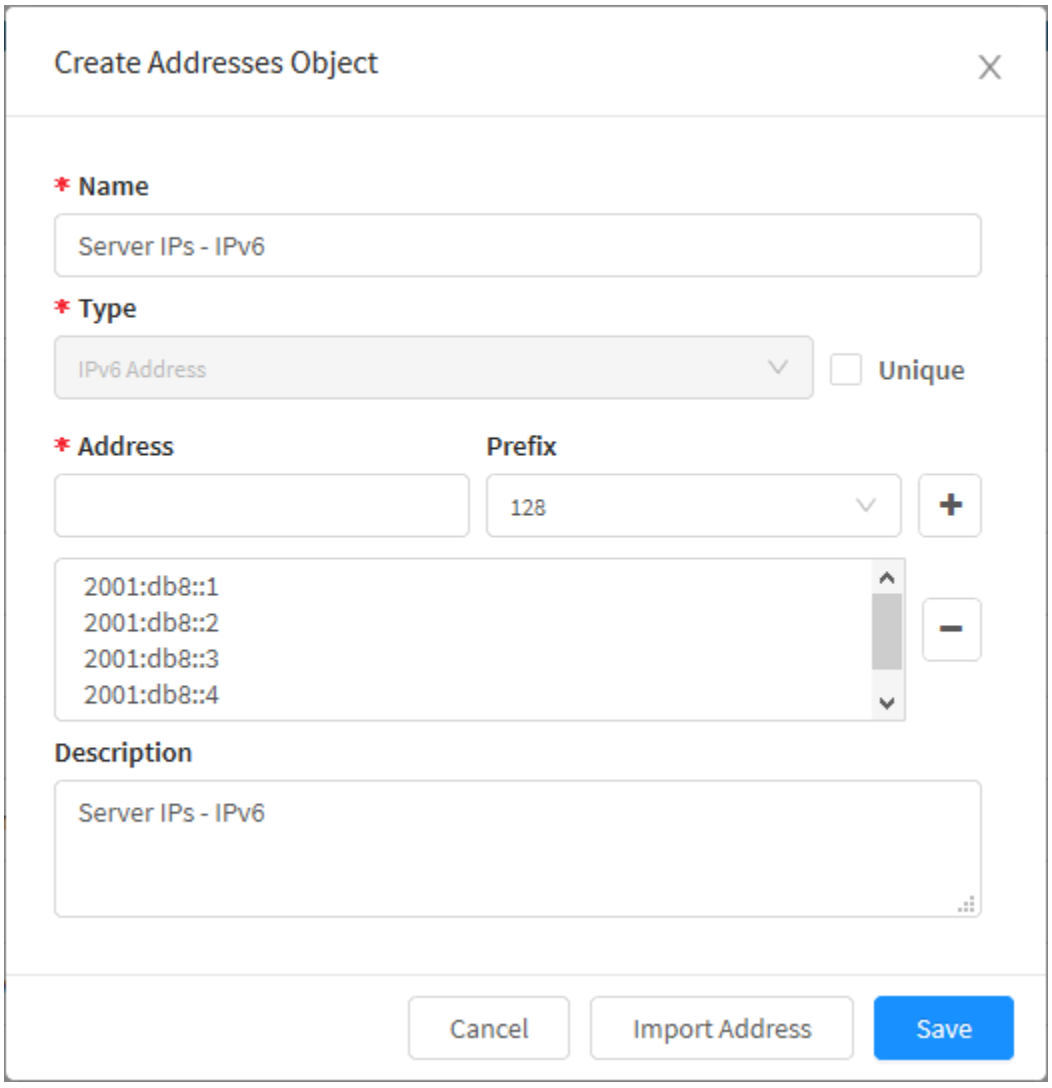


Object successfully changed

The object address was created successfully.

Example 2 - Creating IPv6 Address Object

Here is a demonstration of how to create an IPv6 address object:



Objects – Create Addresses Object - IPv6

Attention: Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- ***Name*:** Name of the object. Ex .: Server IPs - IPv6;
- ***Type*:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- ***Unique*[ ]:** Determines whether the address will be unique or not, disabling the Prefix field;
- ***Address:*** The address of the type of connection object selected later. After entering an address, click **[+]** to add it to the list or select it and click **[−]** to remove it. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- ***Prefix*:** Defines the prefix of the IP address that will be added to the object. Ex: 128;
- ***Description*:** This field is intended for the description of the object. Ex.: Server IPs - IPv6.

When clicking on the Import Address [Import Address] button and selecting the file to be imported, clicking [+] to add the contents of the file inside the object, if you want to remove any registered address, select the IP address and click on the [−] button and the content will be removed.

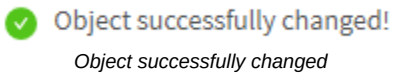
The supported format of the list is one IP or network address per line.

Ex.: 2001::FF:01/68

::FF:0A/128

2001:abcd:172.16.102.0/120

Click the [Cancel] button to Cancel or the [Save] button to save.



Object successfully changed

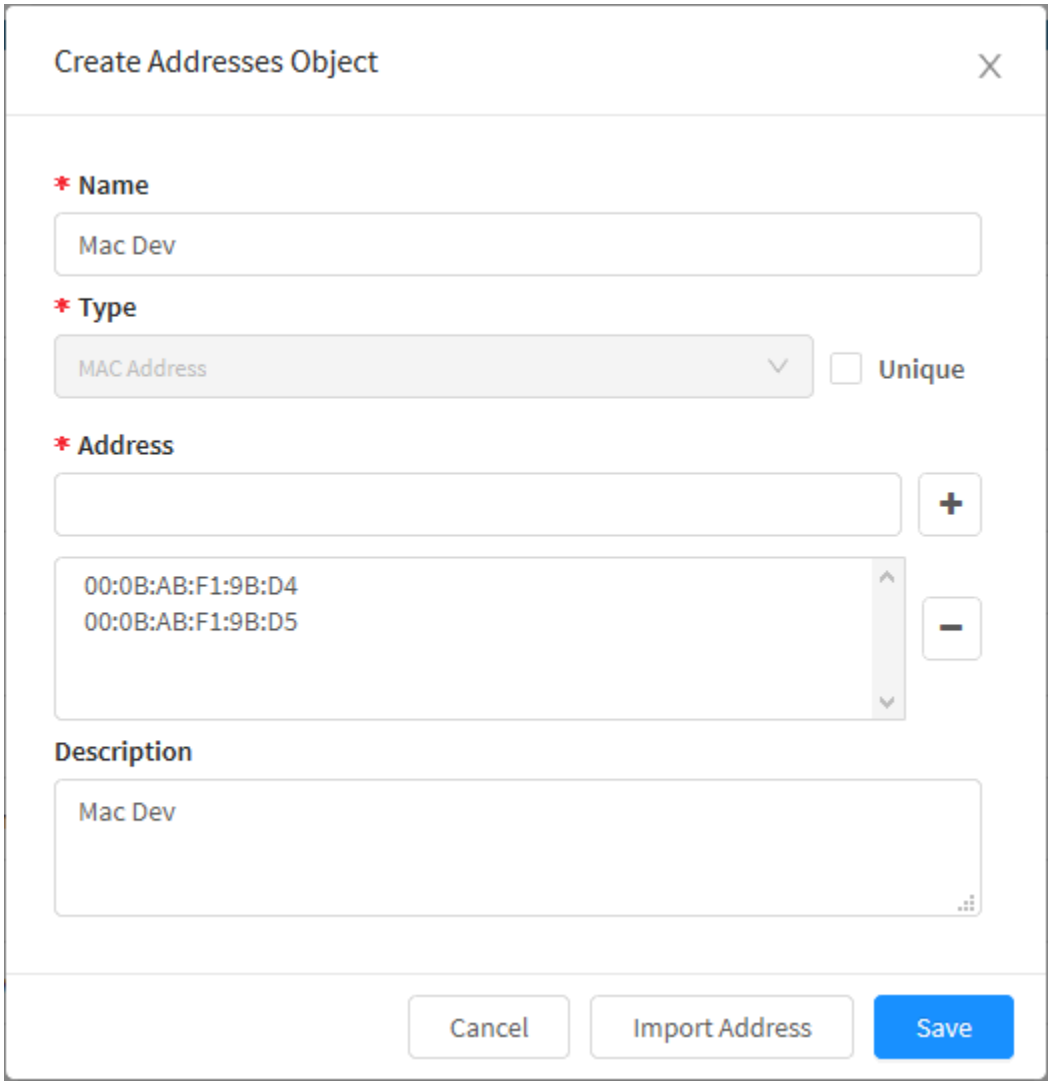
The object address was created successfully.

Exemplo 3 - Creating Physical Address Object

The registered objects are available to be used in the process of configuring the “DHCP” service and by the “Compliance Policies”. MAC address objects can comprise a single MAC address or a list of addresses.

Through this panel it is possible to configure the object according to the settings of the host address and also, make the necessary adjustments according to your applications in the settings of the respective services of the solution.

Here is a demonstration of how to create a MAC Address object:



Objects – Create Addresses Object - Mac Address

Attention: Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- ***Name*:** Name of the object. Ex.: Mac Dev;
- ***Type*:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- ***Unique*[ ]:** Determines whether the address will be unique or not;

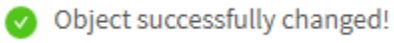
- ***Address:*** The address of the type of connection object selected later. After entering an address, click **[** + **]** to add it to the list or select it and click **[** − **]** to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- ***Description*:** This field is intended for the description of the object. Ex.: Mac Dev.

When clicking on the Import Address **[** Import Address **]** button and selecting the file to be imported, clicking **[** + **]** to add the contents of the file inside the object, if you want to remove any registered address, select the IP address and click on the **[** − **]** button and the content will be removed.

The definition of the MAC address is composed of 48 bits and its format is completely specific, it has 12 hexadecimal digits, grouped two by two separated by colons.

Object syntax: *00:01:02:AA:CC:FF*

Click the **[** Cancel **]** button to Cancel or the **[** Save **]** button to save.



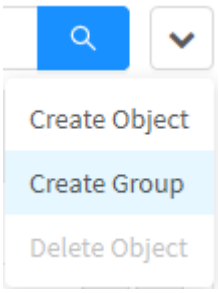
Object successfully changed

The object address was created successfully.

Addresses - Actions Menu - Create Group

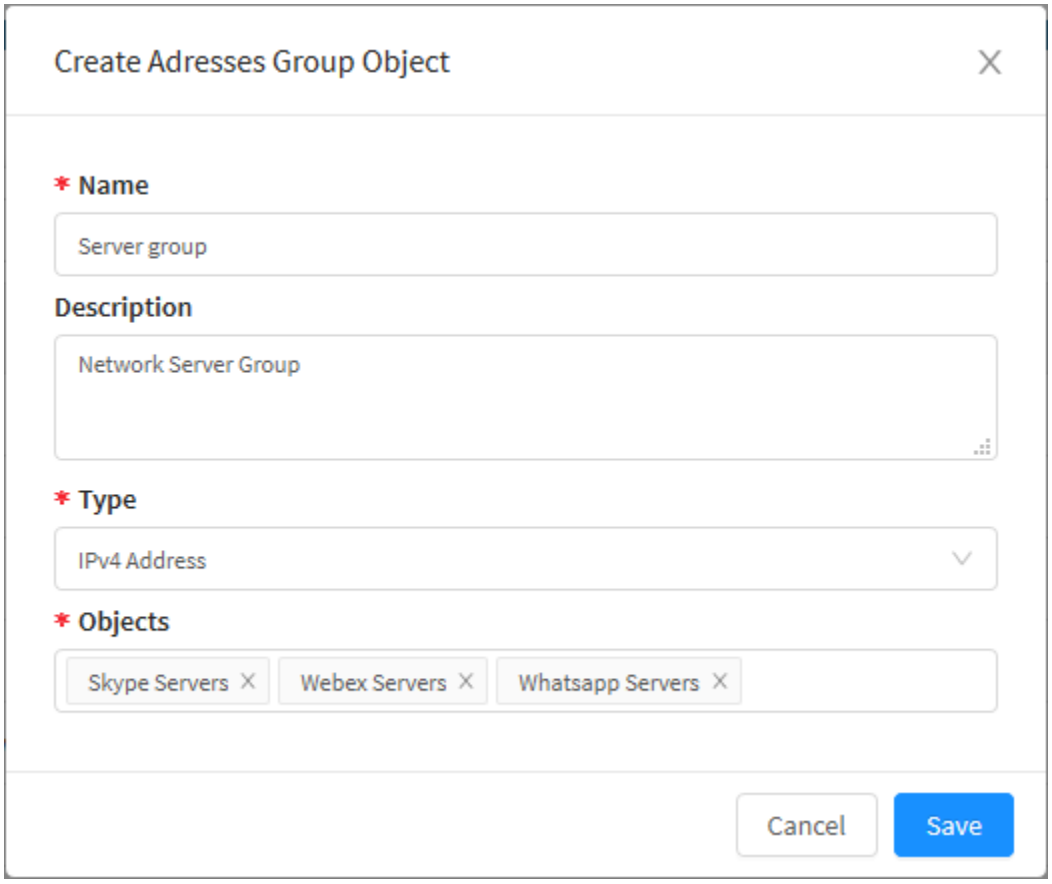
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the actions menu **[**  **]**, click on the option “Create Group”;



Objects – Addresses – Create Group

2. Fill in the information on the Create Addresses Group Object screen:

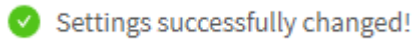


Objects – Create Addresses Group Object

- ***Name*:** Object group name. Ex.: *Server group*;
- ***Description*:** This field is intended for the description of the group. Ex.: *Network Server Group*;
- ***Type*:** Connection object type, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address;

- ***Objects*:** It allows selecting the objects that were previously added in the Addresses - Actions menu - Create Object. The objects added in this field will be inserted as tags.

Click the **[** Cancel **]** button to Cancel or the **[** Save **]** button to save.



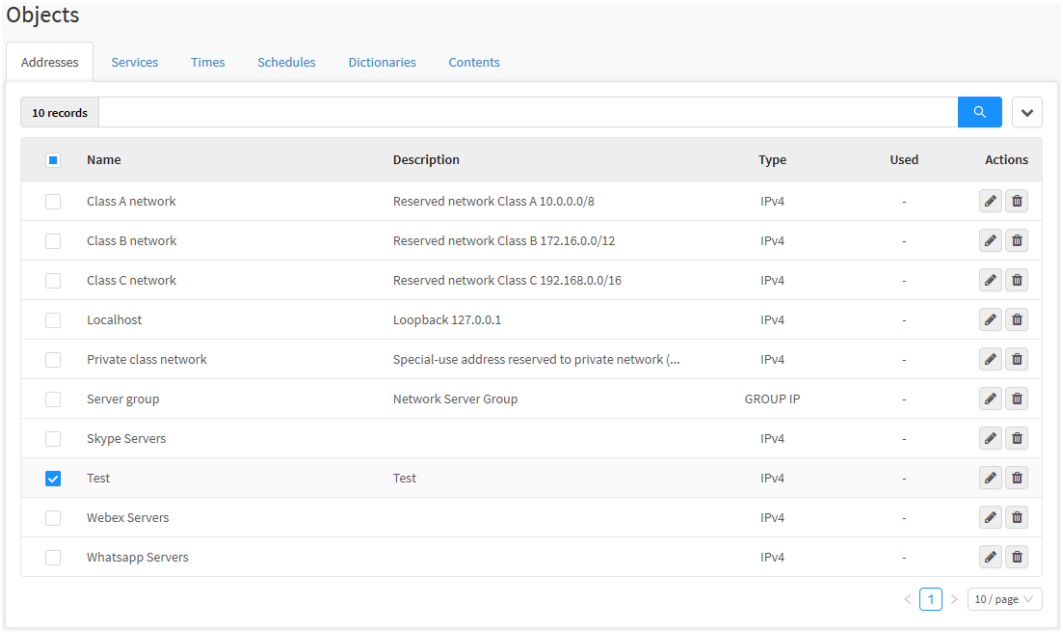
Settings successfully changed

The group was created successfully.

Addresses - Actions Menu - Delete Object

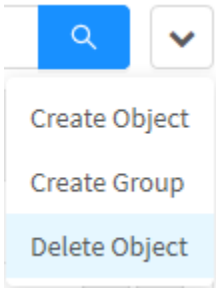
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the **checkbox[ ]** .Ex .: Test;



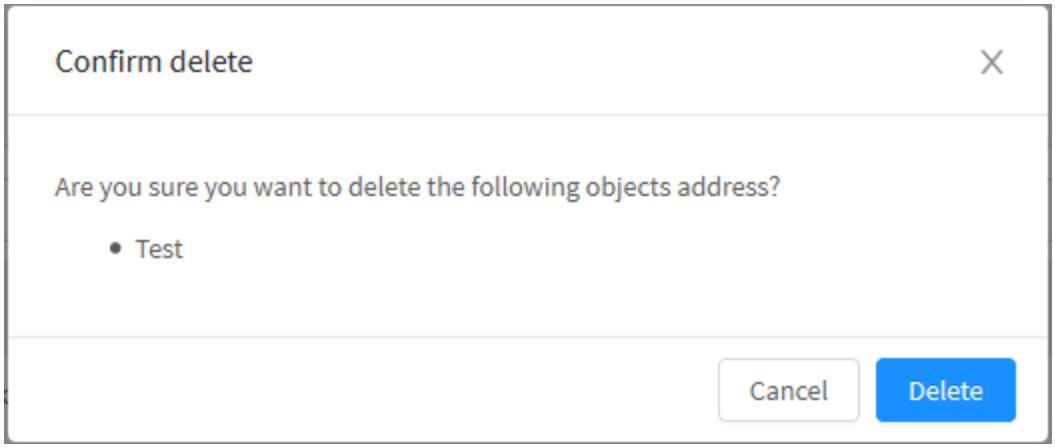
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following objects address

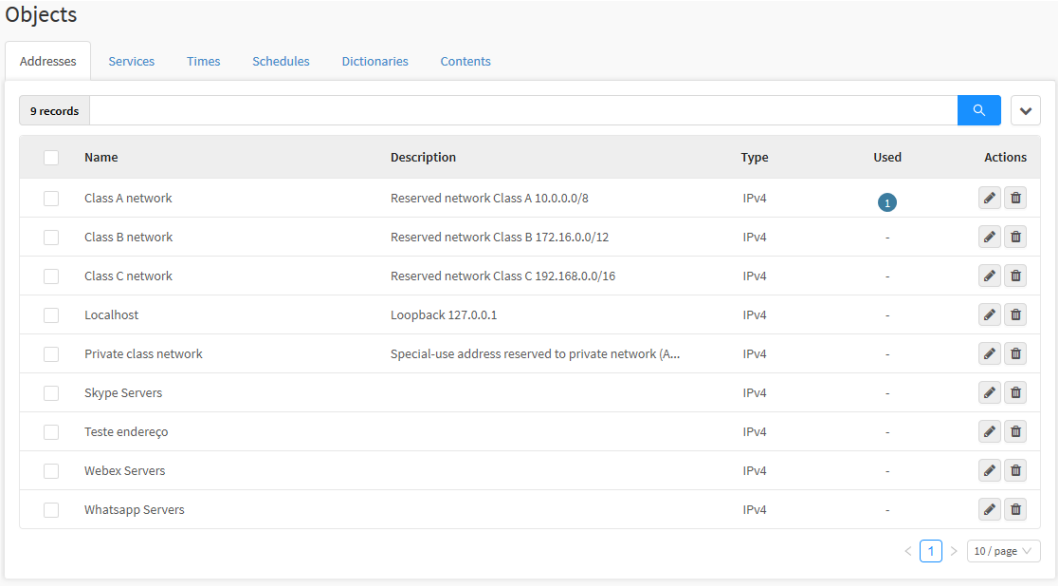
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Addresses - Columns

In the “Addresses” tab, it is possible to view the actions menu and six columns:



Objects – Aba *Addresses*.

Next we will explain each column of the *Addresses* tab:

- **Select[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** Displays the object's description;
- ***Type*:** Object Type;
- ***Used[1]*:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed;
- ***Actions*:** Allows you to edit, select and delete the object;
    - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the action menu;
    - **Deletar[ ]:** Allows you to remove the Object.

Addresses - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

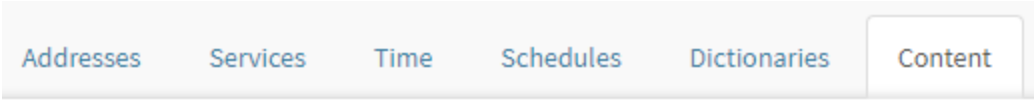
Content

This panel is composed of groupings of types of applications based on the type of content that specify their characteristic.

By default, the system brings some pre-registered objects that group some types of applications in order to facilitate their applicability in the system. Eg: "ActiveX", "Compressed", "Executables", "images", "javascript", "Multimedia" and "Office".

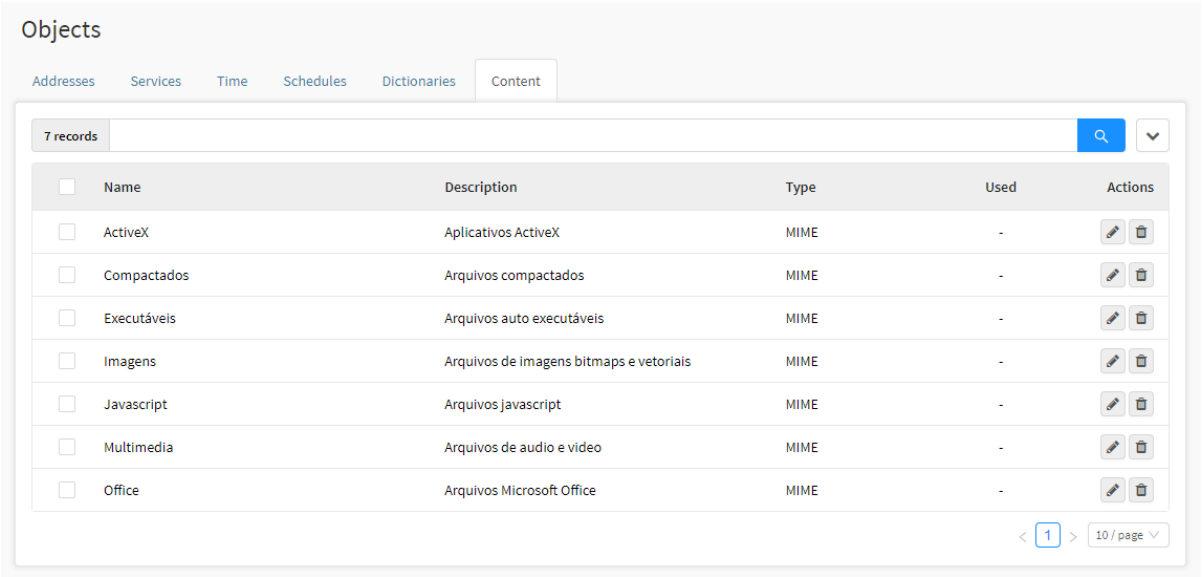
All of these objects are available for use in the configuration and policy setting processes.

To access the screen, click on the “Content” tab.



Objects – Content

The “Content” screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the actions menu on the right.



Objects - Content

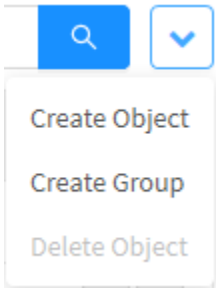
We will explain in detail the actions menu and later the columns of the "*Content*" tab.

Contents - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions Menu

The menu consists of the following options:

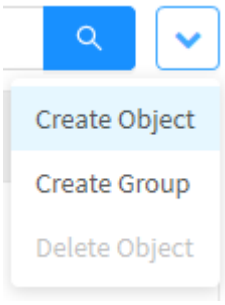
- *Create Object*;
- *Create Group*;
- *Delete Object*.

Next, each action menu option will be detailed.

Contents - Actions Menu - Create Object

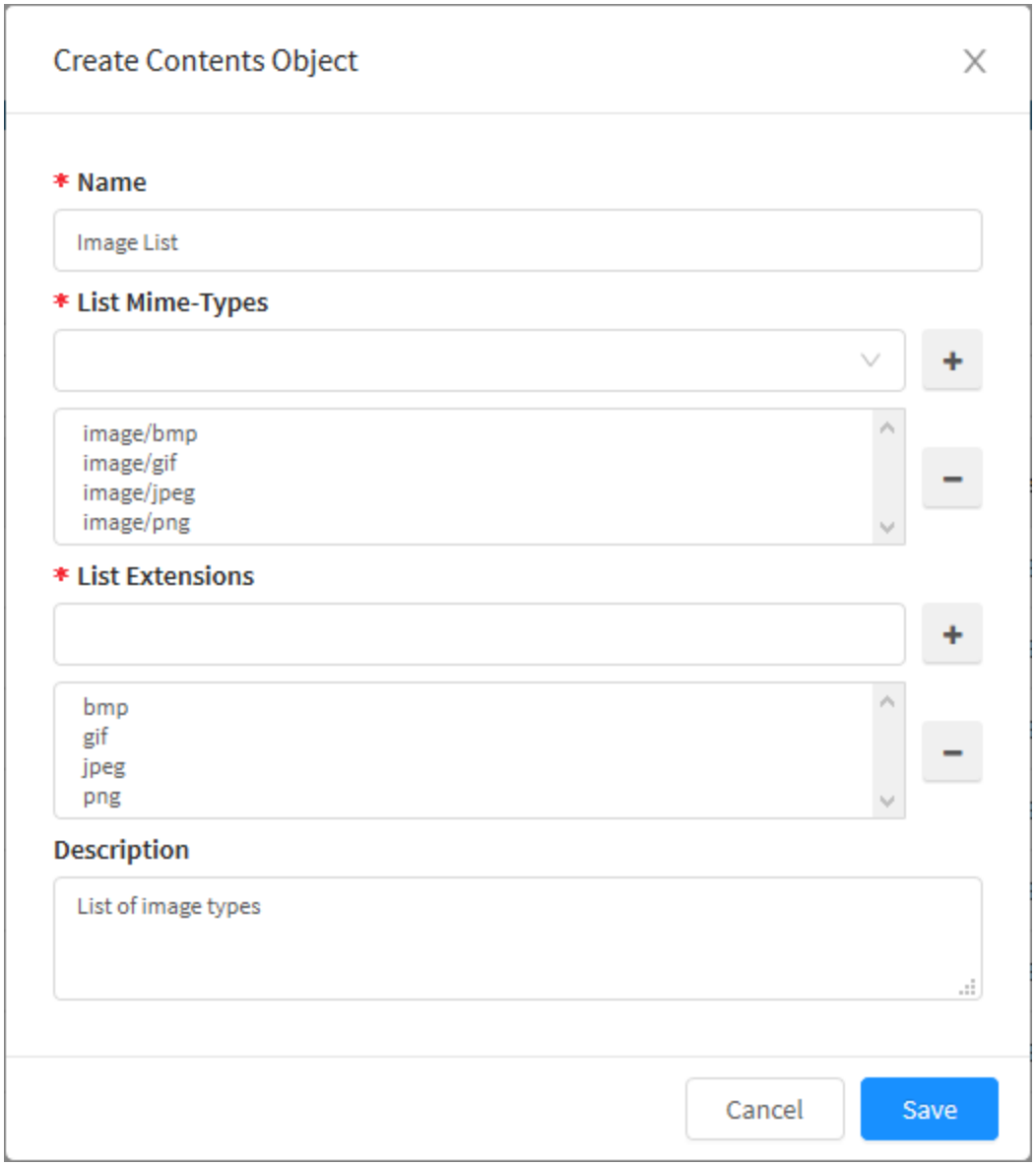
Through the option “Create Object” it is possible to create a new object Contents. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Contents – Create Object

2. The Create Contents Objects screen will appear. Fill in the fields:

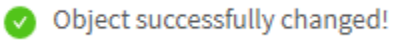


Objects – Create Contents Object

- ***Name*:** Object name. Ex.: *Image List*;
- ***List Mime-Types*:** Displays the list of mime-types for the object. To add, click **[** + **]**, to delete any value entered, select it and click the **[** − **]** button;
- ***List Extensions*:** Displays the list of object extensions. To add, click **[** + **]**, to delete any value entered, select it and click the **[** − **]** button;
- ***Description*:** Object description. Ex.: "*List of image types*".

The specifications of new content-types can be identified from surveys of records in the detailed logs

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



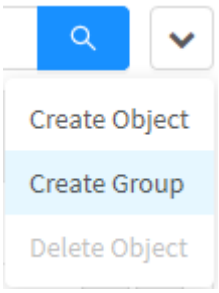
Object successfully changed

The contents object was created successfully.

Contents - Actions Menu - Create Group

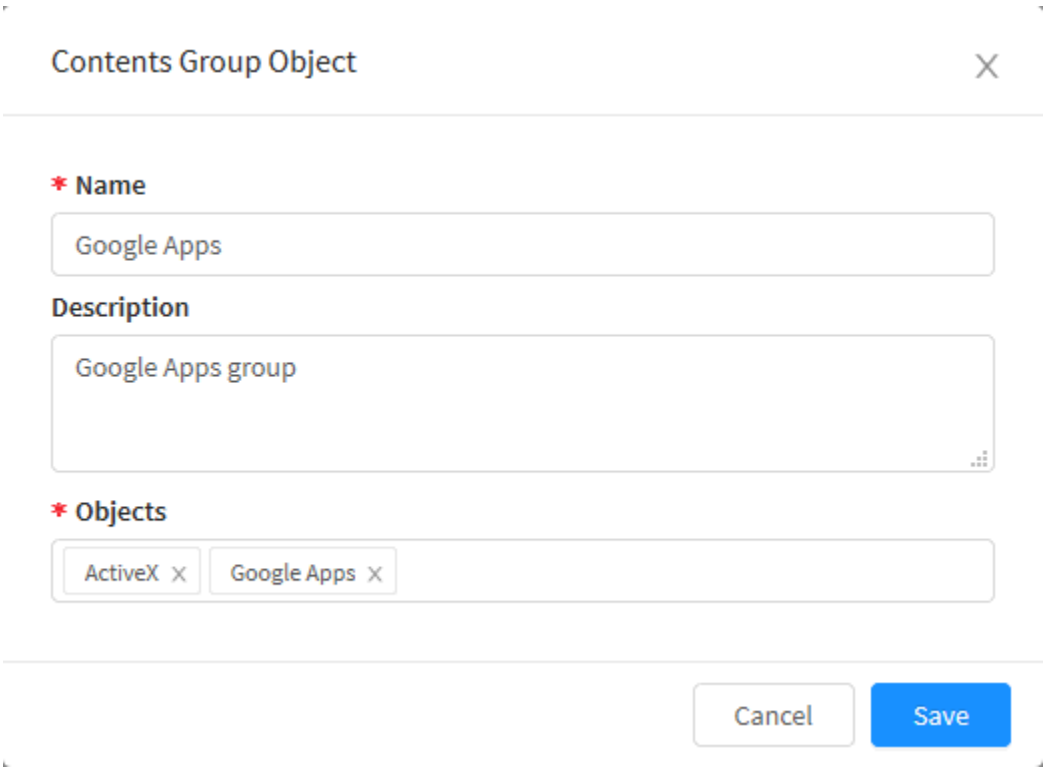
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Group”;



Objects – Contents – Create Group

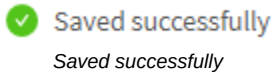
2. Fill in the information on the Contents Group Object screen:



Objects – Contents Group Object

- ***Name*:** Object group name. Ex.: *Image group*;
- ***Description*:** This field is intended for the description of the group. Ex.: *Google Apps Group*;
- ***Objects*:** It allows selecting the objects that were previously added in Contents - Actions Menu - Create Object. The objects added in this field will be inserted as tags.

Click the **[** Cancel **]** button to Cancel or the **[** Save **]** button to save.



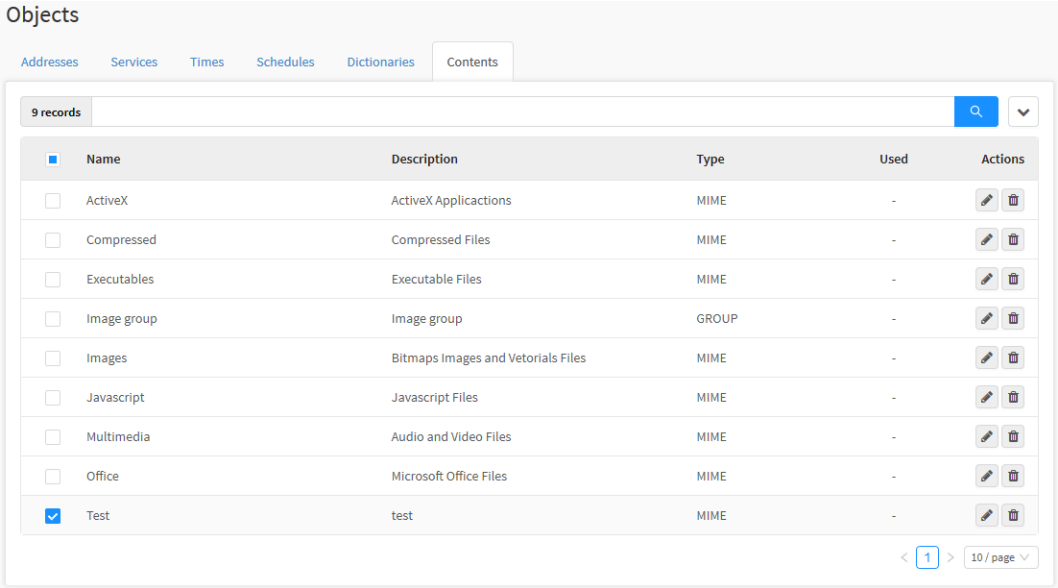
Saved successfully

The group was created successfully.

Contents - Actions Menu - Delete Object

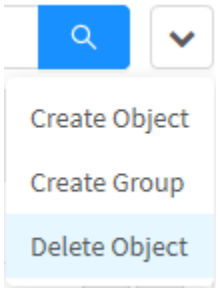
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the ***checkbox*** **[ ]**.Ex.: *Test*;



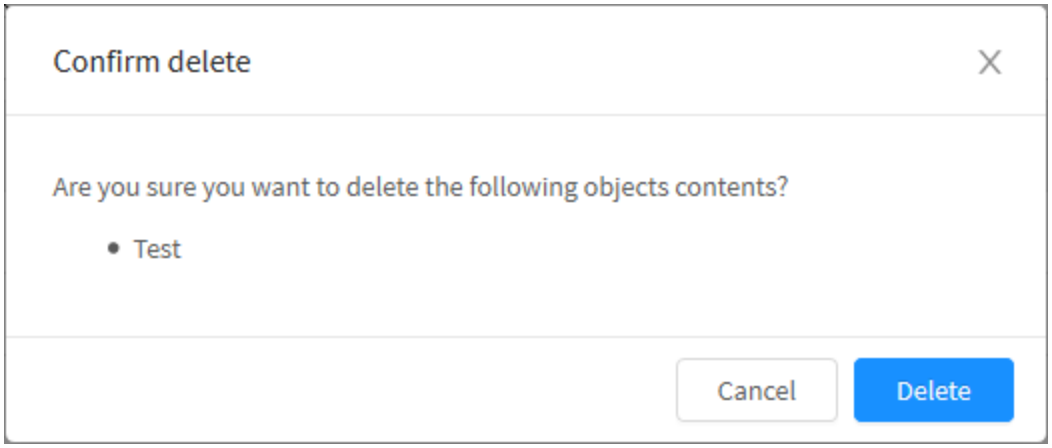
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following object contents

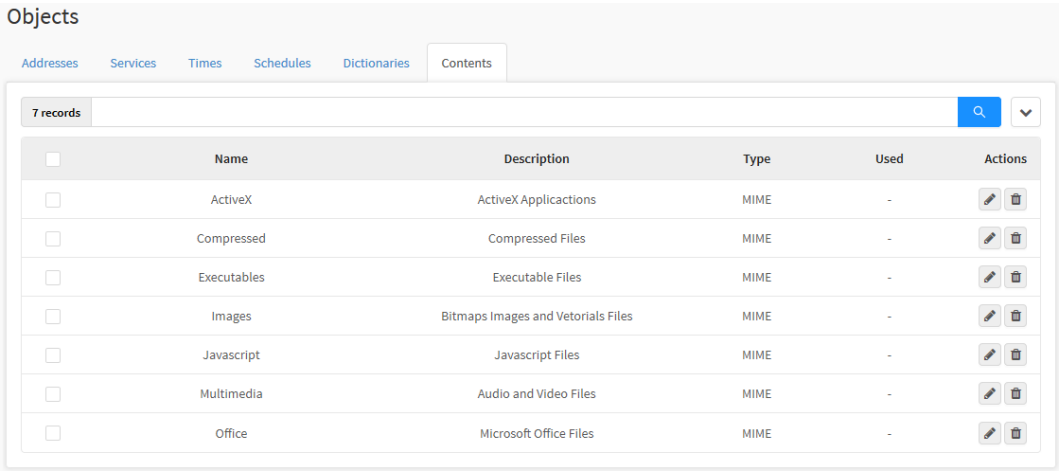
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Contents - Columns

In the “Contents” tab, it is possible to view the actions menu and six columns:



Objects – Contents tab

Below we will explain each column of the Contents tab:

- **Checkbox[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** The object description;
- ***Type*:** Object Type;
- ***Used[ ]*:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed.
- ***Actions*:** Allows you to edit, select and delete the object;
  - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the action menu;
  - **Delete[ ]:** Allows you to remove the Object.

Contents - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

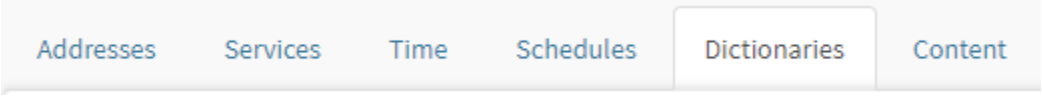
Dictionaries

Dictionary-type objects are made up of “word lists” or a set of “regular expression” combinations, and it is also possible to create groups containing several “Dictionary” objects.

By default, the system brings some pre-registered objects. Ex.: “Alphanumeric”, “Email Address”, “HTML Link”, “URL”.

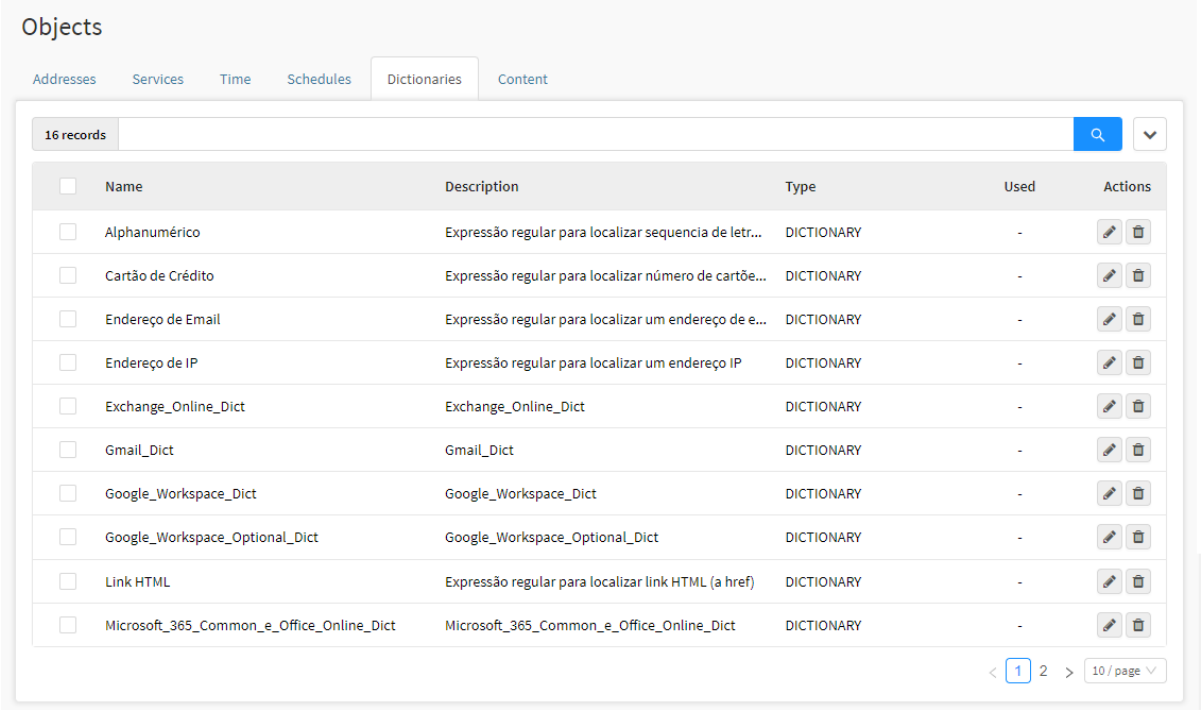
All of these objects are available for use in policy configuration and definition processes.

To access the screen, click on the “Dictionaries” tab.



Dictionaries tab

The "Dictionaries" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the actions menu on the right.



Objects – Dictionaries

Dynamic base

The base of Dictionaries type objects is dynamic, which means that the expressions and characters list comprehended by the object is constantly updated by the Blockbit database remotely.

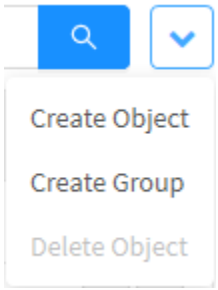
We will explain in detail the action menu and then the columns of the "Dictionaries" tab.

Dictionaries - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions menu

The menu consists of the following options:

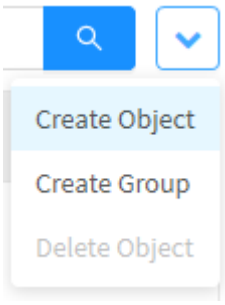
- Create Object;
- Create Group;
- Delete Object.

Next, each action menu option will be detailed.

Dictionaries - Actions Menu - Create Object

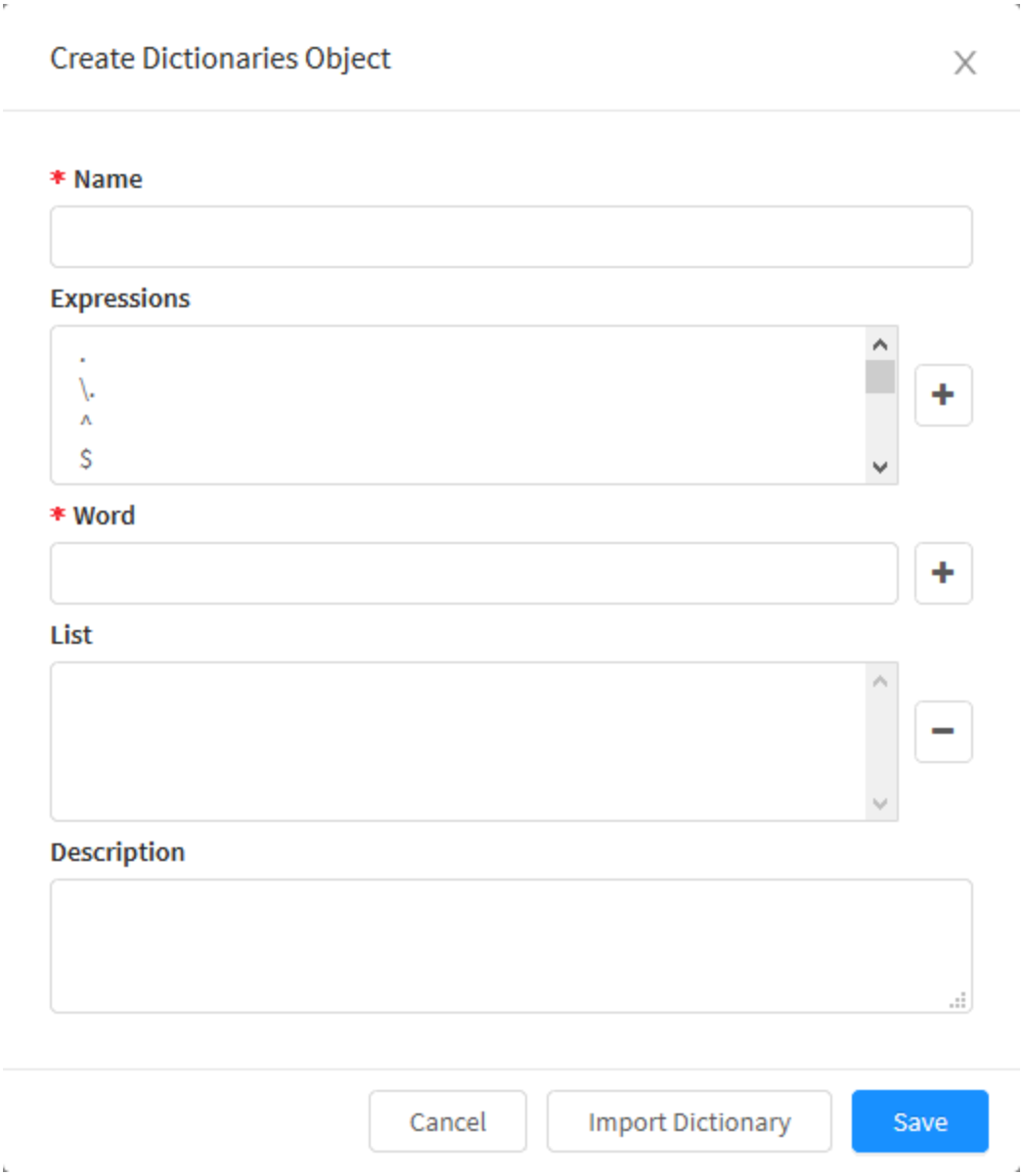
Through the option “Create Object” it is possible to create a new object Dictionaries. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Dictionaries – Create Object

2. The Create Dictionaries Objects screen will appear:



Objects – Create Dictionaries Object

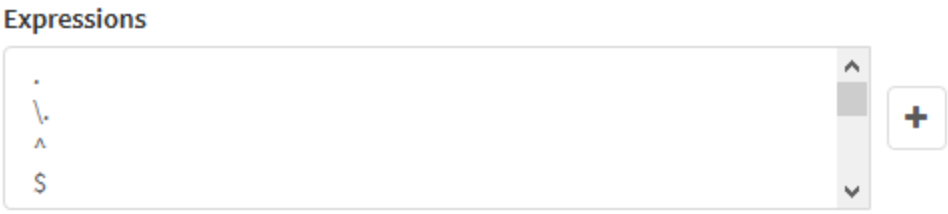
Here are some examples on how to create service objects:

- Example 1 - Adding a dictionary object to access the Blockbit website;
- Example 2 - Adding a dictionary object to access Facebook;
- Example 3 - Adding dictionary objects for Microsoft Update servers - WSUS Servers;
- Example 4 - Adding a dictionary object for Symantec Update servers.

Below some notes regarding the selection of the types of protocols in some fields of the form.

Expressions

Note that the Expressions field includes a list of “regex” that we can combine to build a regular expression and add it to the keyword list.



Objects - Dictionary Expressions

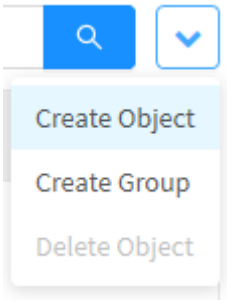
Check this page to see an example of a dictionary object created using "regex".

Example 1 - Adding a dictionary object to access the Blockbit website

Next we will exemplify the creation of a dictionary object to access the Blockbit website.

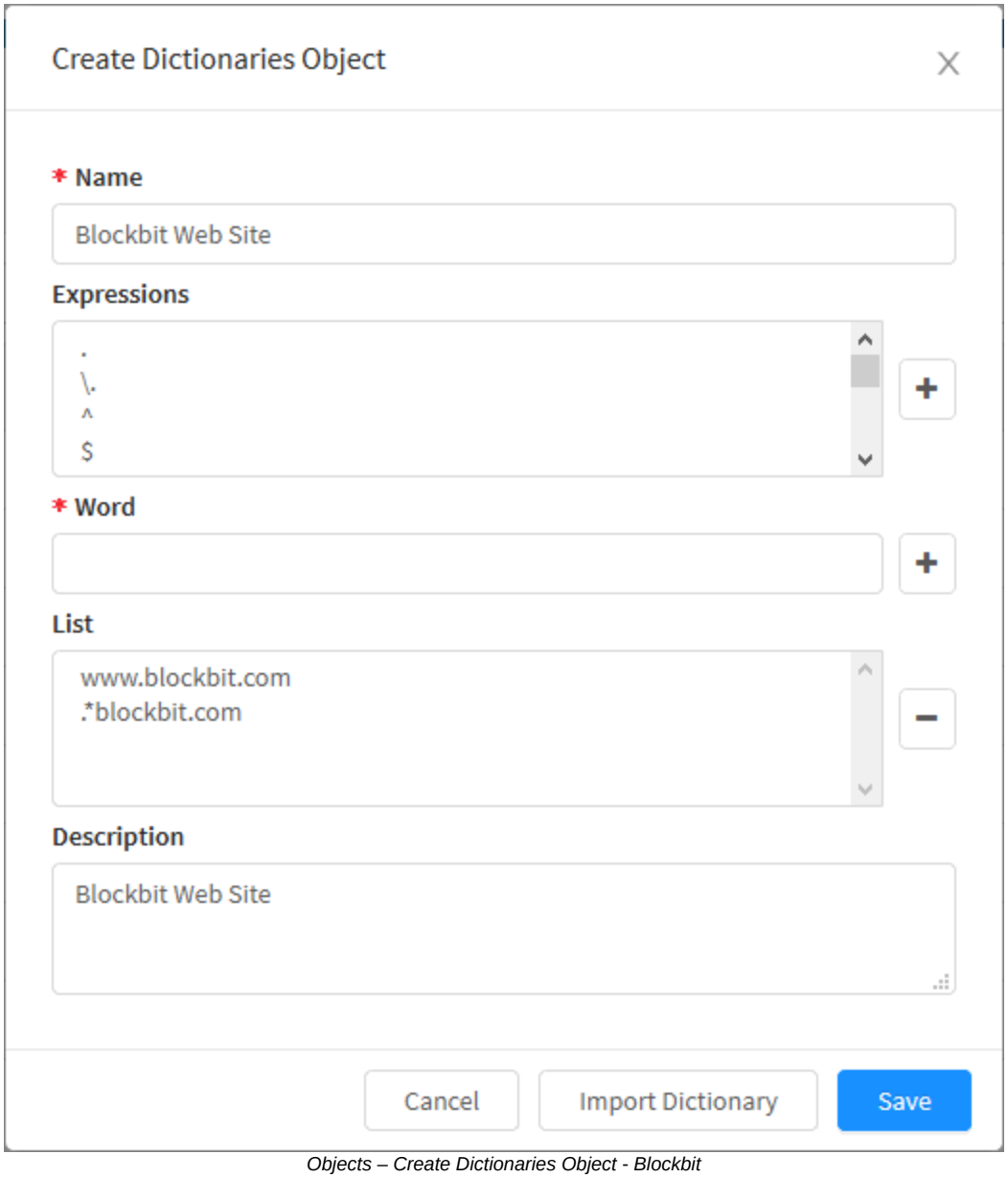
Through the option “Create Object” it is possible to create a new object Dictionaries. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Dictionaries – Create Object

2. The Create Dictionaries Objects screen will appear. Fill in the fields:



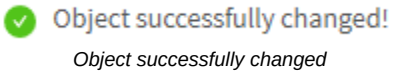
Objects – Create Dictionaries Object - Blockbit

- ***Name*:** Object Name. Ex.: Blockbit Web Site;
- ***Expressions*:** It includes a list of "regex", which we can combine to build a regular expression and add to the list of keywords. Select the code and click **[** + **]** to add it to the Word field;
- ***Word*:** This field defines the regular expression to identify the desired item. To add click **[** + **]**. Ex: "www.blockbit.com" and ". * Blockbit.com";
- ***List Extensions*:** Displays the list of regular expressions. To delete any value entered, select it and click the **[** − **]** button;
- ***Description*:** Object description. Ex.: *Blockbit Web Site*.

If you prefer to import a list of regular expressions, click the **[** Import Dictionary **]** button, the file must contain one item per line.

We can include the desired "keywords" in the word list of the "Dictionary" object by a list of "simple words" without spaces, adding "one per line" or combining "Regular expressions".

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



Object successfully changed

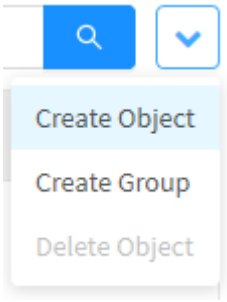
The dictionaries object was created successfully.

Example 2 - Adding dictionary object for access to Facebook

Next we will exemplify the creation of a dictionary object to access Facebook.

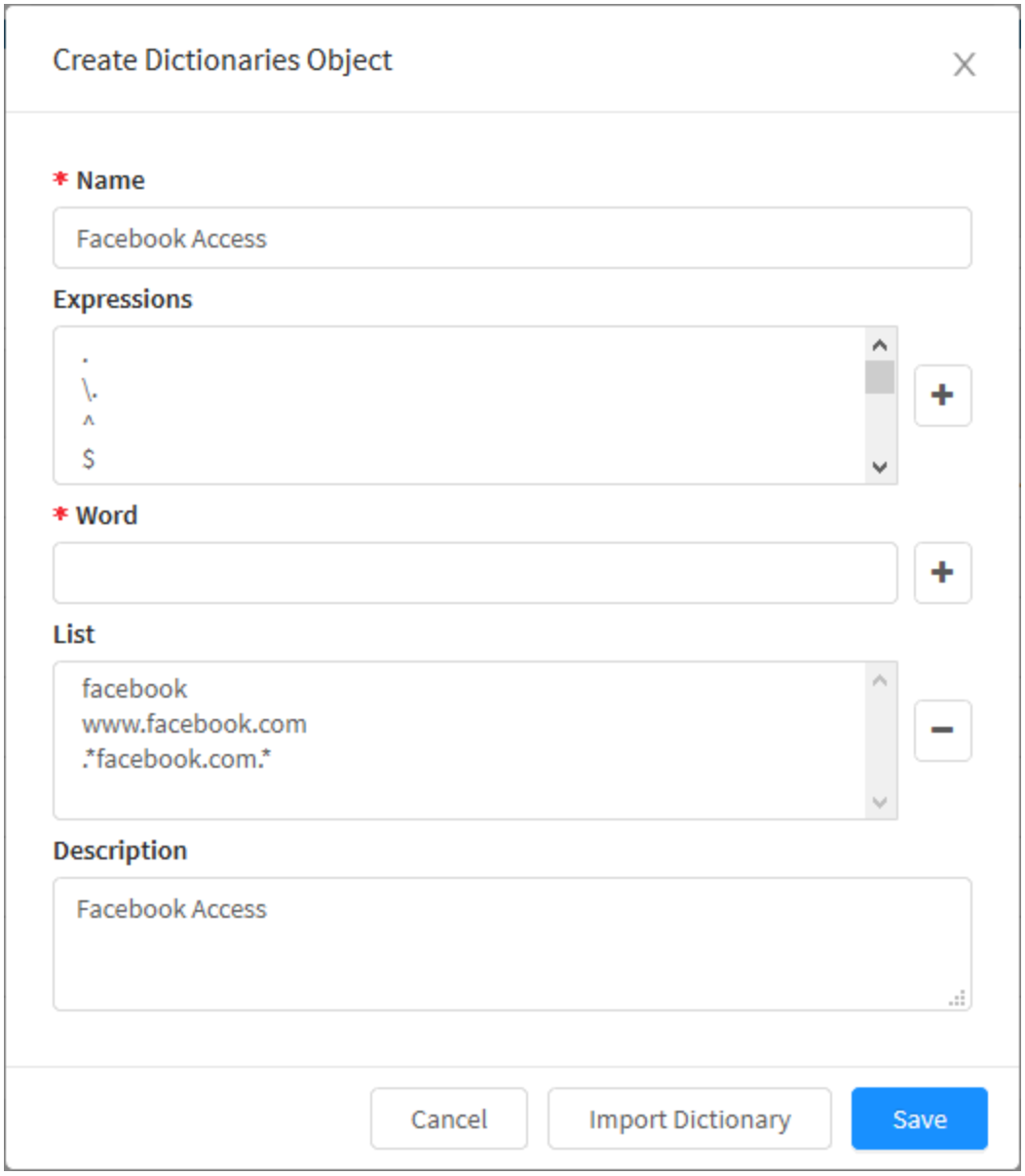
Through the option “Create Object” it is possible to create a new object Dictionaries. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Dictionaries – Create Object

2. The Create Dictionaries Objects screen will appear. Fill in the fields:



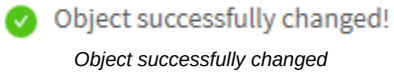
Objects – Create Dictionaries Object - Facebook

- ***Name*:** Object Name. Ex.: *Facebook Access*;
- ***Expressions*:** It includes a list of "regex", which we can combine to build a regular expression and add to the list of keywords. Select the code and click **[** + **]** to add it to the Word field;
- ***Word*:** This field defines the regular expression to identify the desired item. To add click **[** + **]**. Ex.: "facebook", "www.facebook.com" and ".*facebook.com.*";
- ***List Extensions*:** Displays the list of regular expressions. To delete any value entered, select it and click the **[** − **]** button;
- ***Description*:** Object description. Ex.: *Facebook Access*.

If you prefer to import a list of regular expressions, click the **[** Import Dictionary **]** button, the file must contain one item per line.

We can include the desired "keywords" in the word list of the "Dictionary" object by a list of "simple words" without spaces, adding "one per line" or combining "Regular expressions".

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



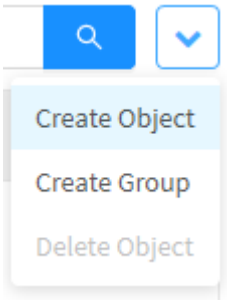
Object successfully changed

The dictionaries object was created successfully.

Example 3 - Adding a dictionary object to Microsoft Update servers - WSUS Servers

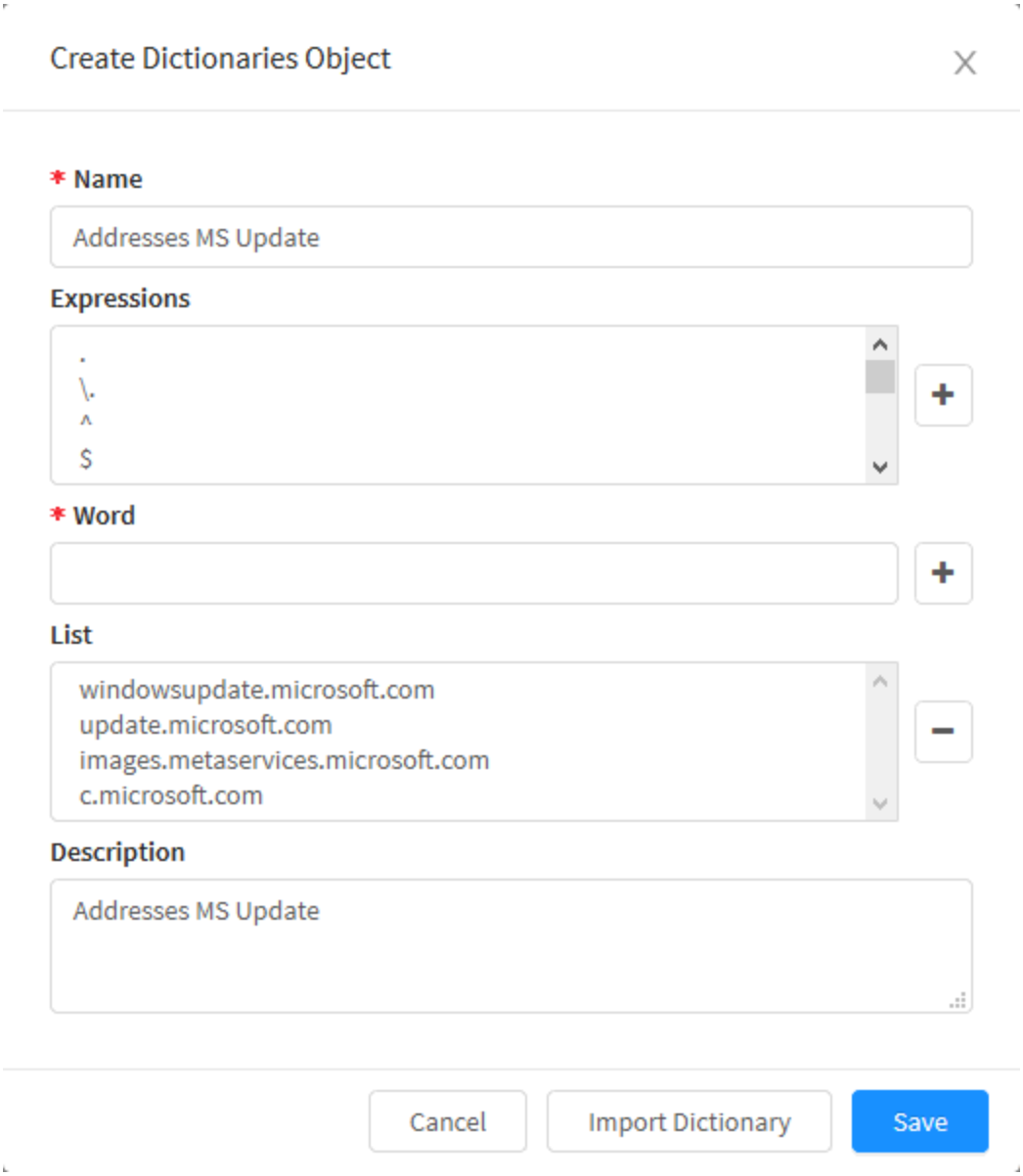
Let's exemplify the registration of a Dictionary object with the list of simple words: "addresses of Microsoft Update servers - WSUS Servers", let's add the addresses manually one word per line.

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Dictionaries – Create Object

2. The Create Dictionaries Objects screen will appear. Fill in the fields:



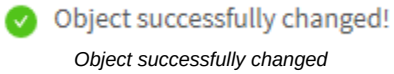
Objects - Dictionary Address WSUS

- ***Name*:** Object Name. Ex.: *Addresses MS Update*;
- ***Expressions*:** It includes a list of “regex”, which we can combine to build a regular expression and add to the list of keywords. Select the code and click **[** + **]** to add it to the Word field;
- ***Word*:** This field defines the regular expression to identify the desired item. To add click **[** + **]**. Ex.: "Windowsupdate.microsoft.com", "update.microsoft.com", "images.metaservices.microsoft.com", "c.microsoft.com" and etc;
- ***List Extensions*:** Displays the list of regular expressions. To delete any value entered, select it and click the **[** − **]** button;
- ***Description*:** Object description. Ex.: *Addresses MS Update*.

If you prefer to import a list of regular expressions, click the**[** Import Dictionary **]** button, the file must contain one item per line.

We can include the desired "keywords" in the word list of the "Dictionary" object by a list of "simple words" without spaces, adding "one per line" or combining "Regular expressions".

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



Object successfully changed

The dictionaries object was created successfully.

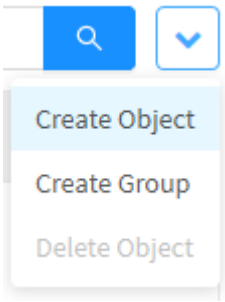
Example 4 - Adding a dictionary object for Symantec Update servers

Another example, let's register a list of words using “regular expressions”: To create the desired regular expression combination. Ex.:

"The regex.: "\." corresponds to a period character ("."), therefore, when we have the following expression: "ftp\.symantec\.com/public" the registered object corresponds to the keyword "FTP.symantec.com/public" in order to specify a server address."

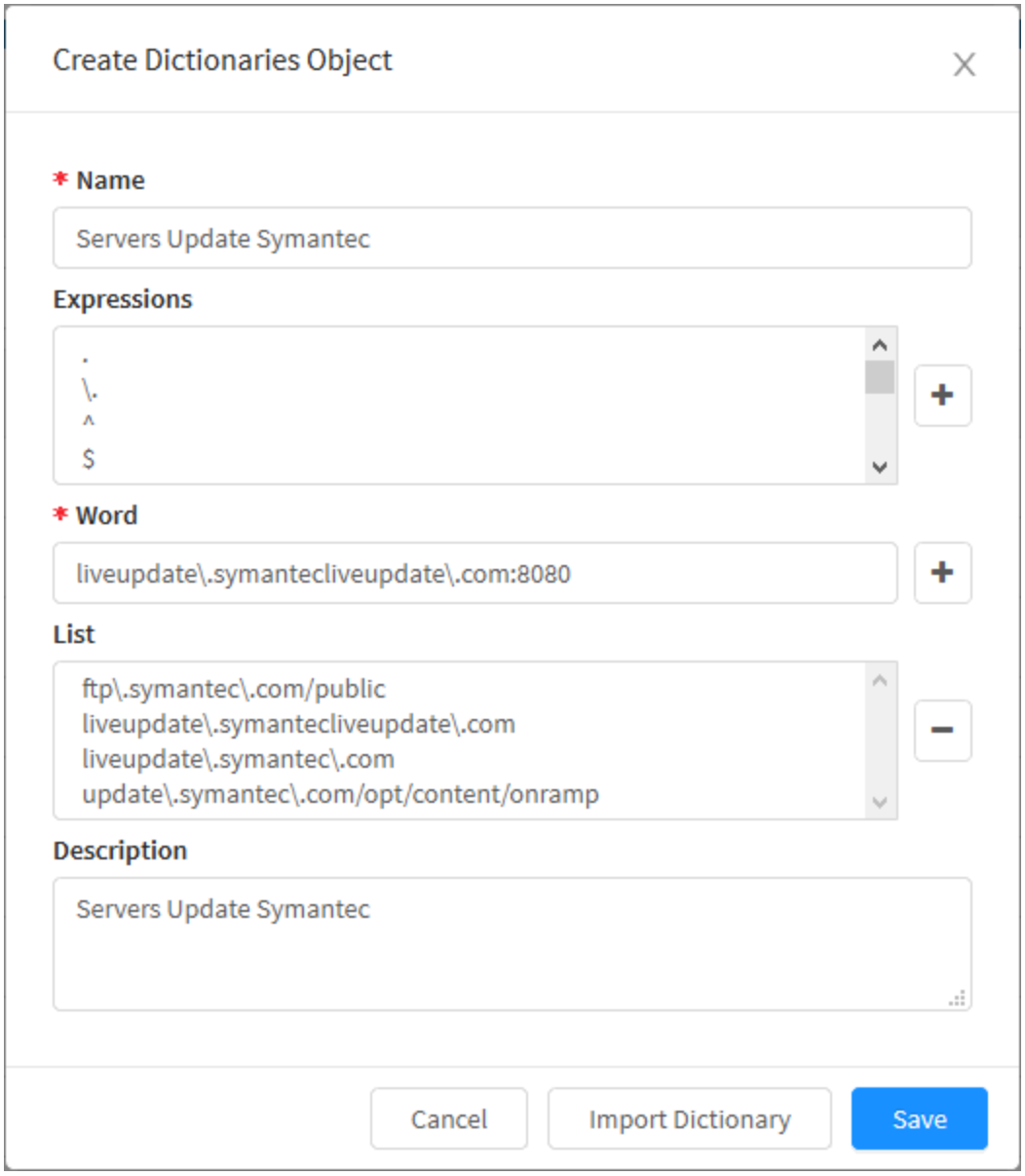
Let's use this example and add a new dictionary object.

1. In the actions menu **[**  **]**, click on the option “Create Object”;



Objects – Dictionaries – Create Object

2. The Create Dictionaries Objects screen will appear. Fill in the fields:



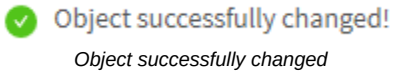
Objects - Regex Symantec Register

- ***Name*:** Object Name. Ex.: *Servers Update Symantec*;
- ***Expressions*:** It includes a list of "regex", which we can combine to build a regular expression and add to the list of keywords. Select the code and click **[** + **]** to add it to the Word field;
- ***Word*:** This field defines the regular expression to identify the desired item. To add click **[** + **]**. Ex.: "liveupdate\.symanteclive update\.com: 8080", "ftp\.symanted\.com/public", "liveupdate\.symantec\.com", "update\.symantec\.com/opt/contentinramp" and etc;
- ***List Extensions*:** Displays the list of regular expressions. To delete any value entered, select it and click the**[** − **]** button;
- ***Description*:** Description of the object. Ex.: Symantec Servers Update.

If you prefer to import a list of regular expressions, click the **[** Import Dictionary **]** button, the file must contain one item per line.

We can include the desired "keywords" in the word list of the "Dictionary" object by a list of "simple words" without spaces, adding "one per line" or combining "Regular expressions".

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



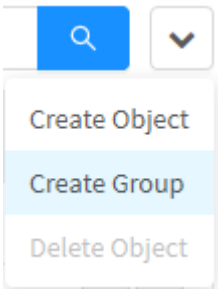
Object successfully changed

The dictionaries object was created successfully.

Dictionaries - Actions Menu - Create Group

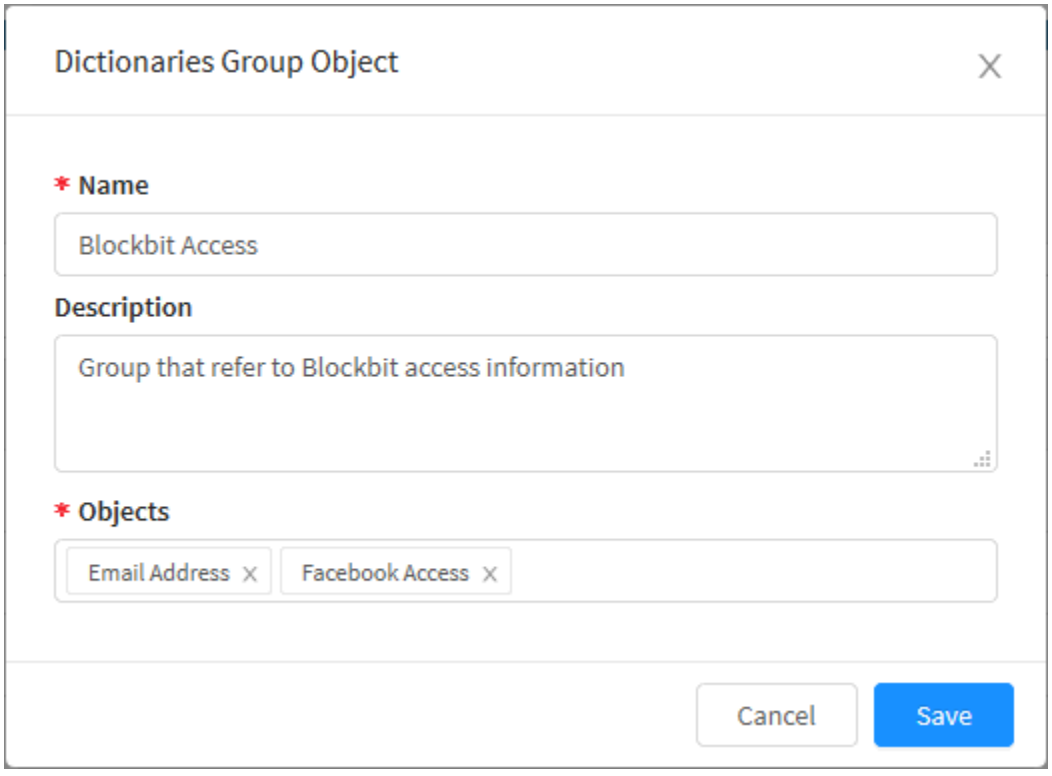
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Group”;



Objects – Dictionaries – Create Group

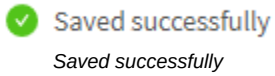
2. Fill in the information for the Dictionaries Group Object screen:



Objects – Dictionaries Group Object

- ***Name*:** Object group name. Ex.: *Blockbit Access*;
- ***Description*:** This field is intended for the description of the group. Ex.: *Group that refer to Blockbit access information*;
- ***Objects*:** Allows you to select objects that were previously added in Objects - Dictionaries - Menu de ações - Create Object. The objects added in this field will be inserted as tags.

Click the **[** Cancel **]** button to Cancel or the **[** Save **]** button to save.



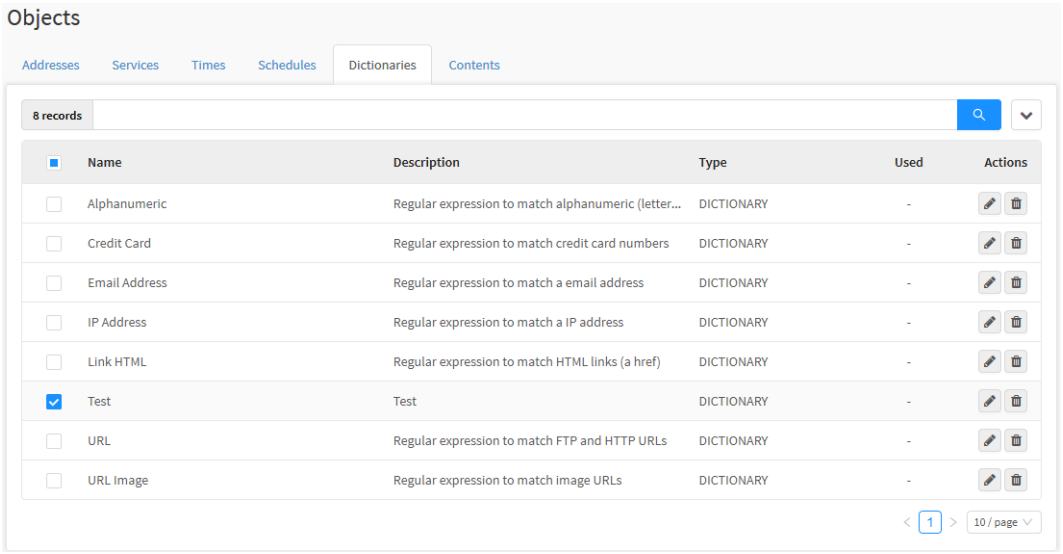
Saved successfully

The group was created successfully.

Dictionaries - Actions Menu - Delete Object

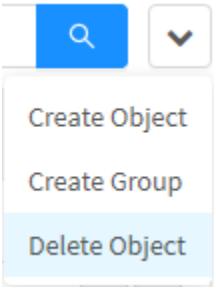
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the checkbox **[ ]**.Ex.: *Test*;



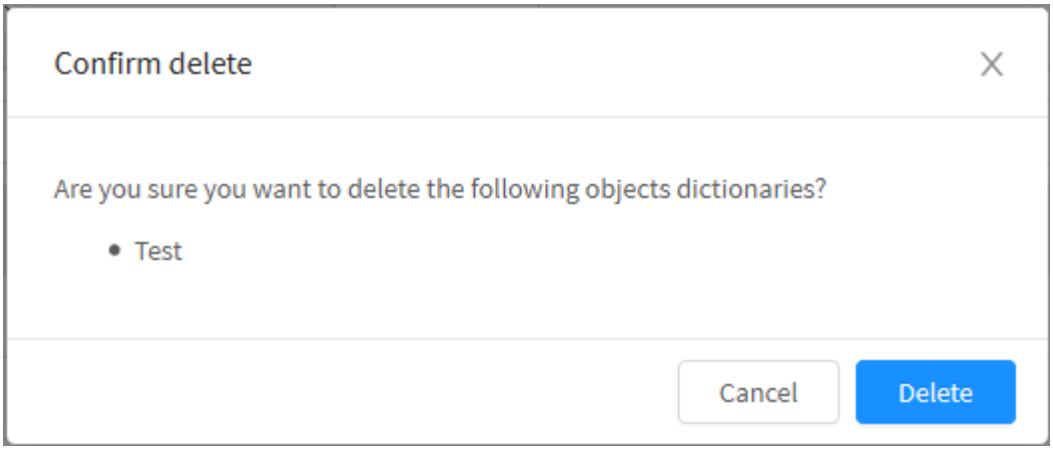
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following object dictionaries?

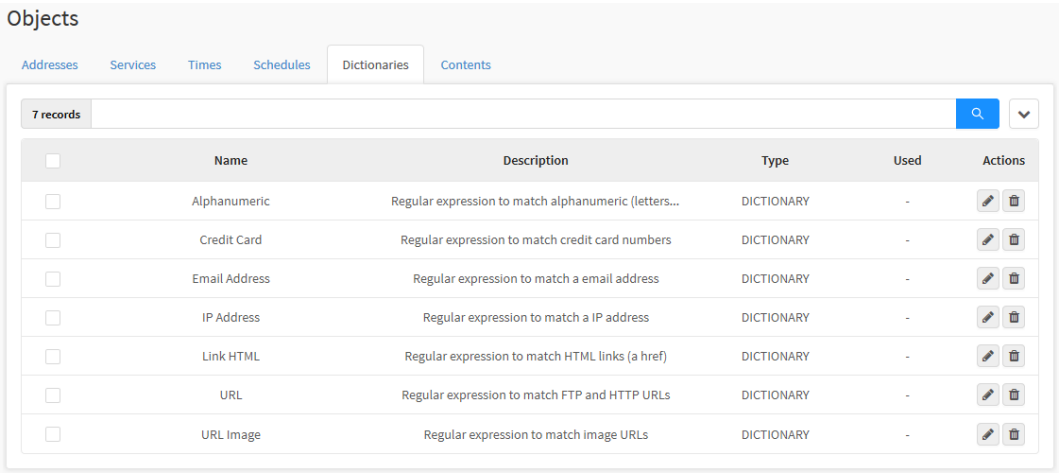
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Dictionaries - Columns

In the “Dictionaries” tab it is possible to view the actions menu and six columns:



Objects – Dictionaries tab

In the following we will explain each column of the Dictionaries tab:

- **Checkbox[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** The object description;
- ***Type*:** Object Type;
- ***Used*[1]:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed.
- ***Actions*:** Allows you to edit, select and delete the object;
  - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the actions menu;
  - **Delete[ ]:** Allows you to remove the Object.

Dictionaries - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

Object Mapping

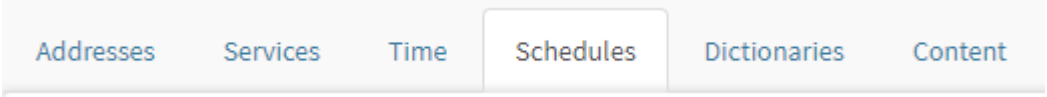
In addition, when clicking on the link, a redirection is made directly to where the object is being used.

Schedules

Schedules objects are made up of the definitions of a period that competes “Start date / time” and “End date / time”. Ex.: 2017-05-11 8:00 AM until 2017-05-30 5:00 PM.

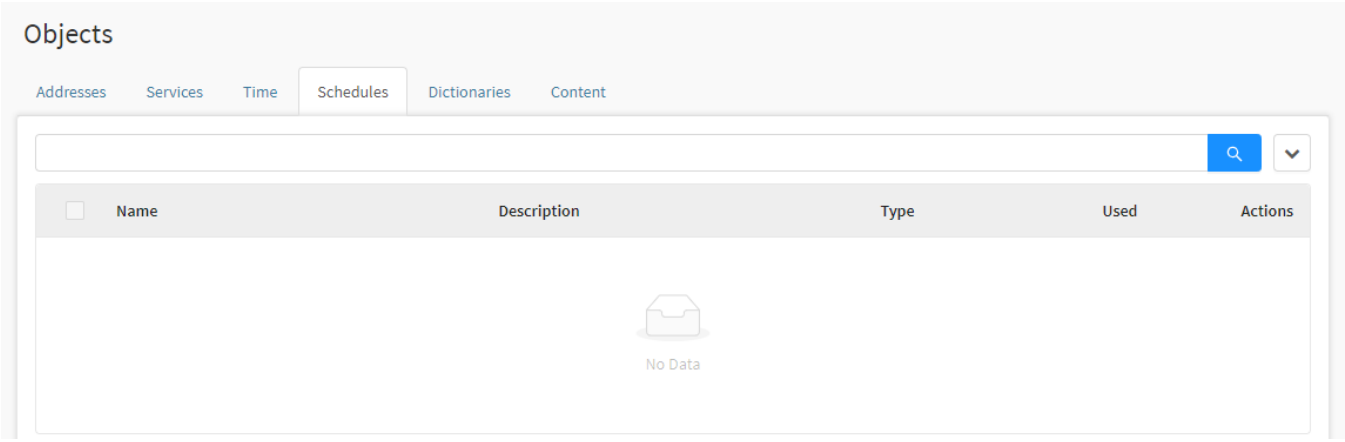
The registered objects are available to be used in the configuration and enabling processes of some "Services" and also, in the definitions of the "Policy".

To access the screen, just select the “Schedules” tab.



Schedules tab

The "Schedules" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the actions menu on the right.



Objects - Schedules

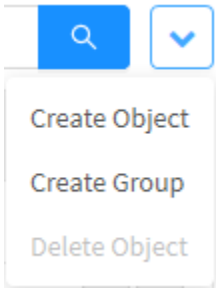
We will explain in detail the actions menu and later the columns of the "*Schedules*" tab.

Schedules - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions menu

The menu consists of the following options:

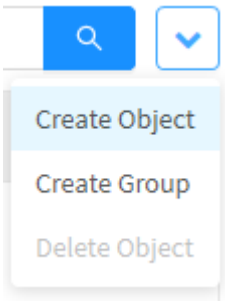
- Create Object;
- Create Group;
- Delete Object.

Next, each action menu option will be detailed.

Schedules - Actions Menu - Create Object

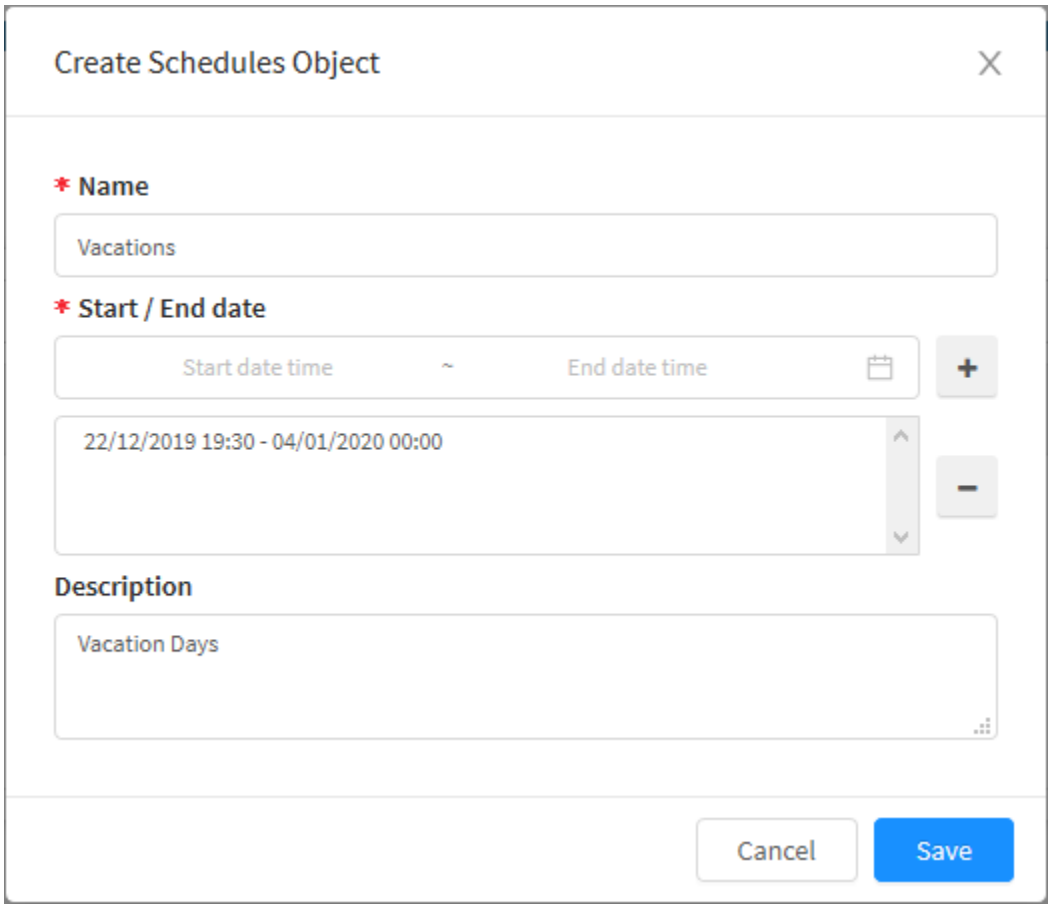
Through the option “Create Object” it is possible to create a new object Schedules. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Schedules – Create Object

2. The Create Schedule Objects screen will appear. Fill in the fields:

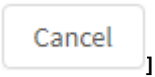


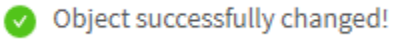
Schedules Objects – Create Schedules Object

- ***Name*:** Object name. Ex.: *Vacations*;

- **Start / End date:** Defines the period between the start date and time and the end date and time, to add click **[**  **]**. Ex.: 22/12/2019 19:30 - 04/01/2020 00:00;
- ***List*:** Displays the list of added periods. To delete an entered value, select it and click the**[** **]** button;
- ***Description*:** Object description. Ex.: *Vacation Days*.

 It is worth mentioning that Schedules objects have a very unique purpose. Ex .: When defining policies with expiration time, "Start date / time" - "End date / time".

Click the **[**  **]** button to cancel. Click the **[**  **]** button to save.



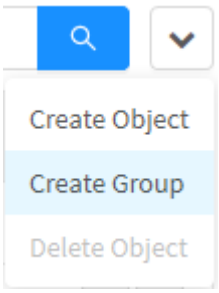
Object successfully changed

The schedule object was created successfully.

Schedules - Actions Menu - Create Group

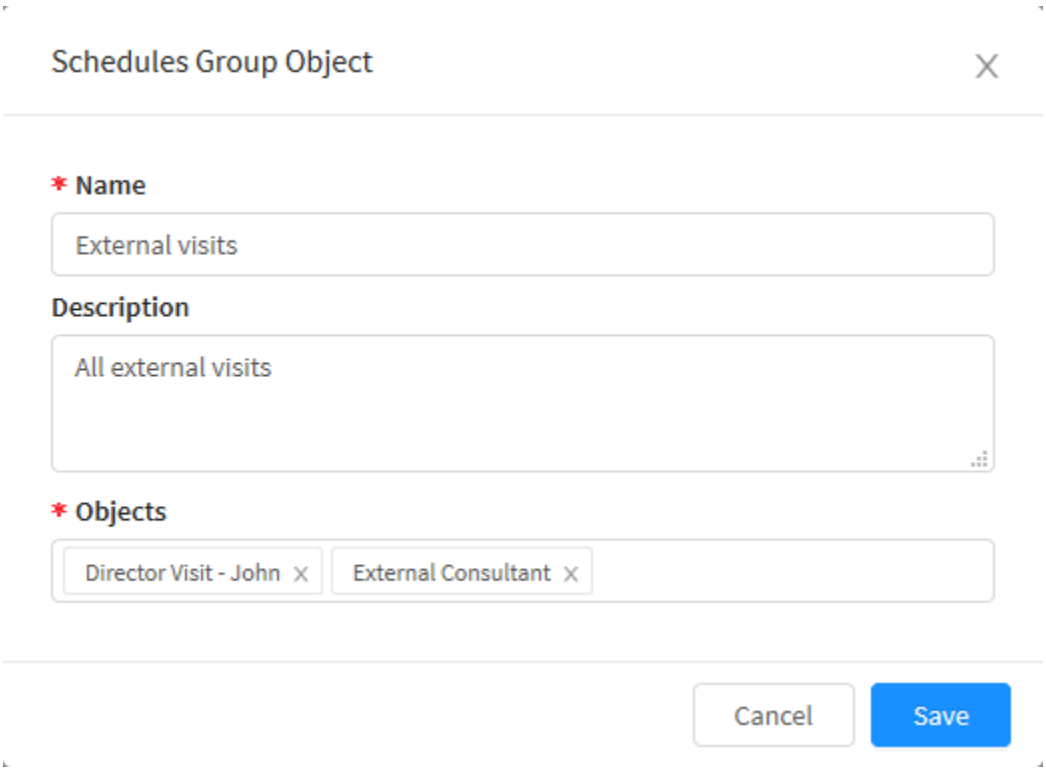
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Group”;



Objects – Schedules – Create Group

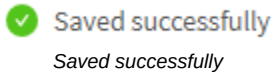
2. Fill in the information on the Schedules Group Object screen:



Objects – Schedules Group Object

- ***Name*:** Object group name. Ex.: *External visits*;
- ***Description*:** This field is intended for the description of the group. Ex.: *All external visits*;
- ***Objects*:** It allows selecting the objects that were previously added in Objects - Schedules - Menu de ações - Create Object. The objects added in this field will be inserted as tags.

Click the **[** Cancel **]** button to Cancel or the **[** Save **]** button to save.



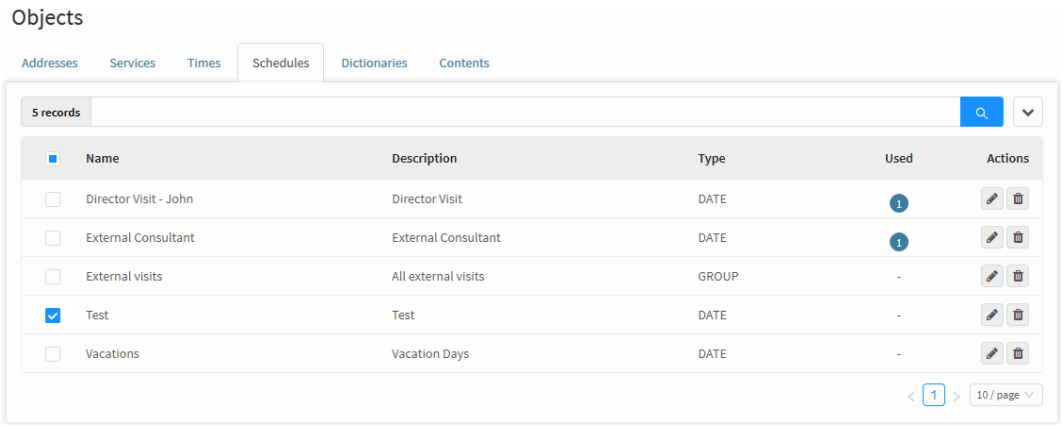
Saved successfully

The group was created successfully.

Schedules - Actions Menu - Delete Object

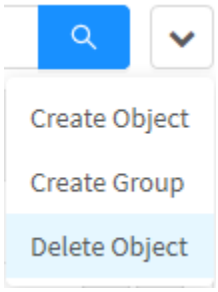
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking the checkbox **[ ]**.Ex.: *Test*;



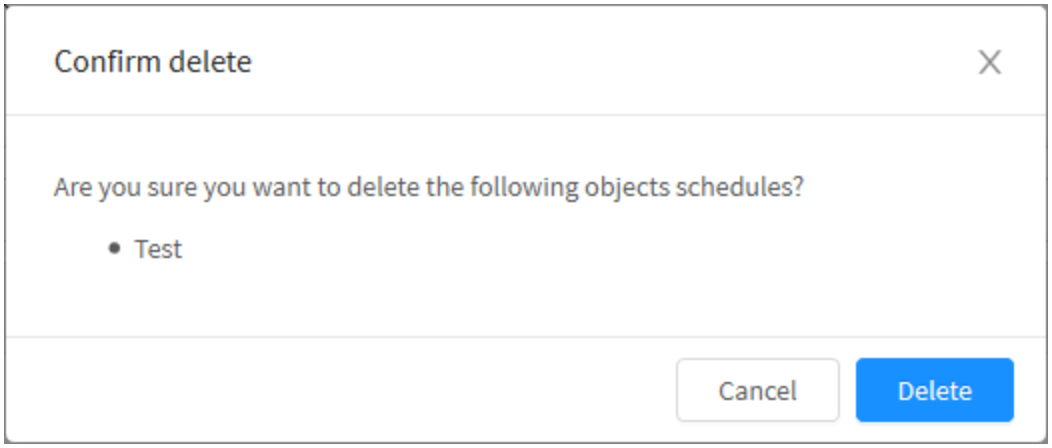
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following object schedules?

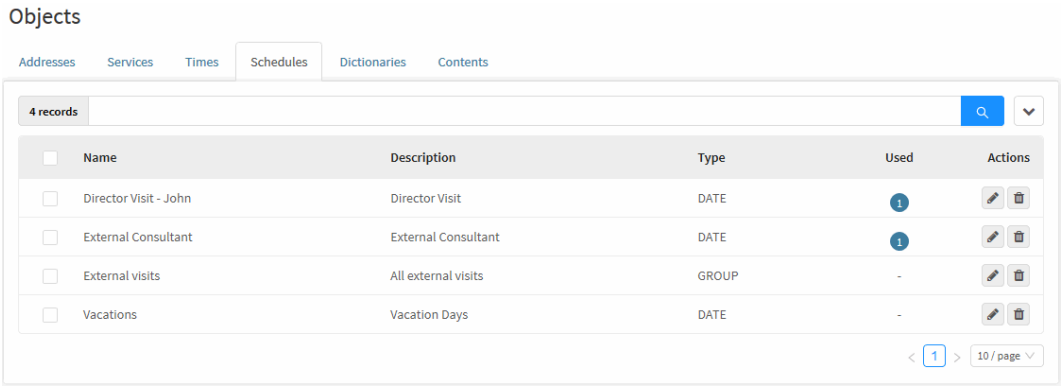
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Schedules - Columns

In the “Schedules” tab it is possible to view the actions menu and six columns:



Objects – Schedules tab

Below we will explain each column of the Schedules tab:

- **Checkbox[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** The object description;
- ***Type*:** Object Type;
- ***Used*[1]:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed;
- ***Actions*:** Allows you to edit, select and delete the object:
  - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the actions menu;
  - **Delete[ ]:** Allows you to remove the Object.

Schedules - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

Services

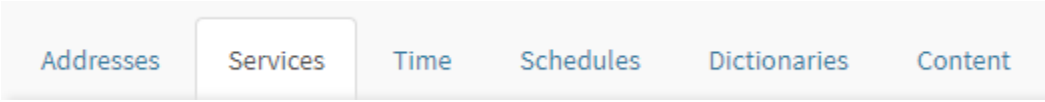
On this screen we have the administrative panel of the Services objects, which comprises port and protocols.

In its initial configuration, by default, the system brings some pre-registered objects (ports / protocols), the objects referring to the most common protocols and services: Example: "DHCP", "DNS", "HTTP", "HTTPS".

All of these objects are available to be used in the configuration and enabling processes of the services. Service objects can be composed of a set of different protocols and services, it is also possible to create groups containing different service objects as a common resource to be applied to any Blockbit UTM functionality, eg: “Compliance policies”, “ Services ”, among others.

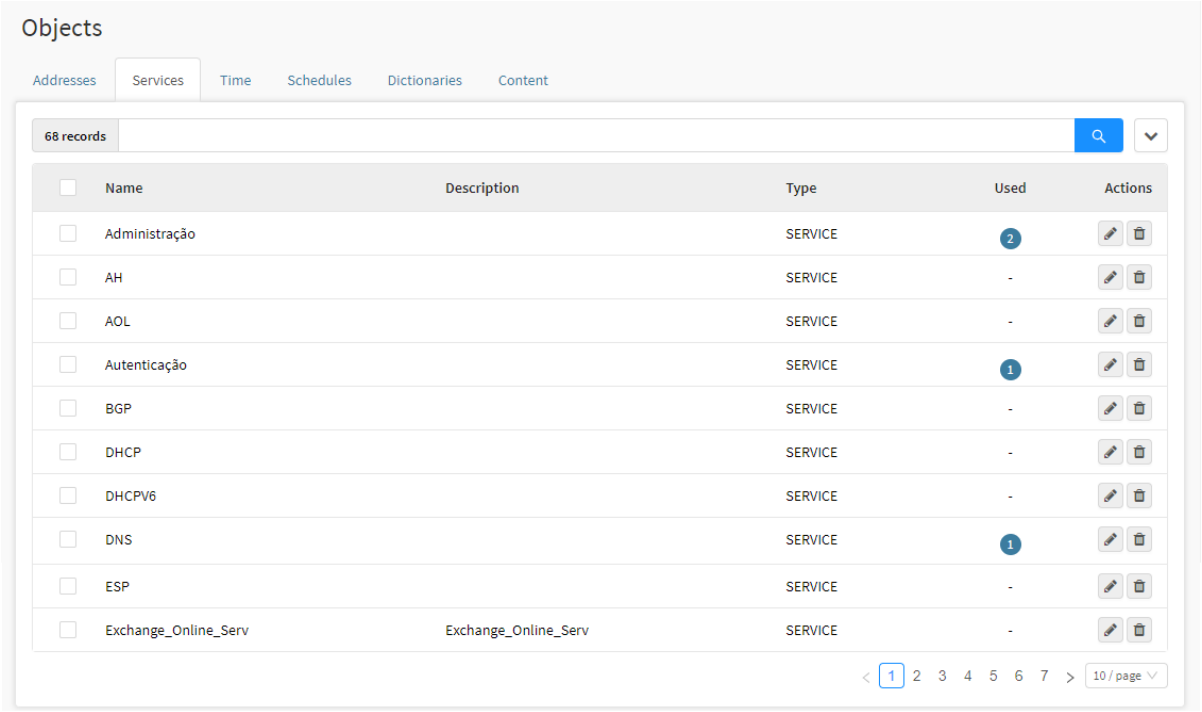
Services type objects identify protocols and applications based on their TCP, UDP, IP and ICMP ports.

To access the screen, click on the "Services" tab.



Services Tab

The "Services" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and “Actions”. In addition, at the top of the screen is the search bar and the action menu on the right.



Objects – Services

Dynamic Base

The base of Services type objects is dynamic, which means that the protcols and ports comprehended by the object is constantly updated by the Blockbit database remotely.

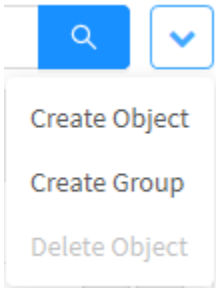
We will explain in detail the actions menu and later the columns of the "Services" tab.

Services - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions Menu

The menu consists of the following options:

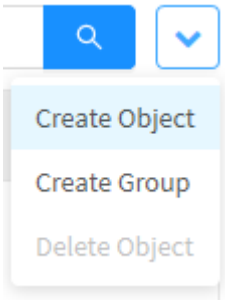
- Create Object;
- Create Group;
- Delete Object.

Next, each action menu option will be detailed.

Services - Actions Menu - Create Object

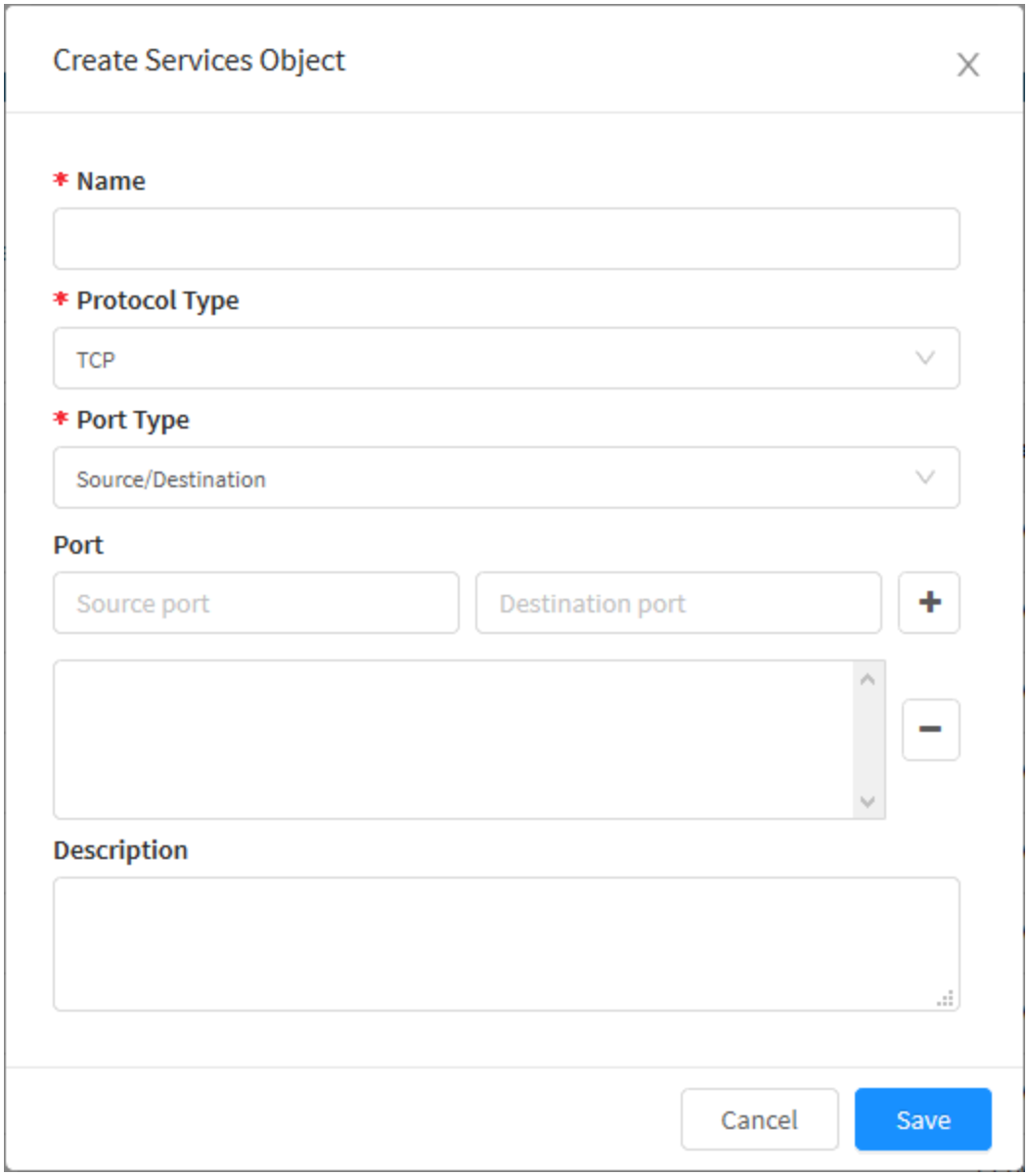
Through the option “Create Object” it is possible to configure the object according to the definitions of the policies that you want to apply for specific hosts.
To create a new Object Services, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”;



Objects – Services – Create Object

2. The Create Service Objects screen will appear.



Objects – Services – Create Service Objects

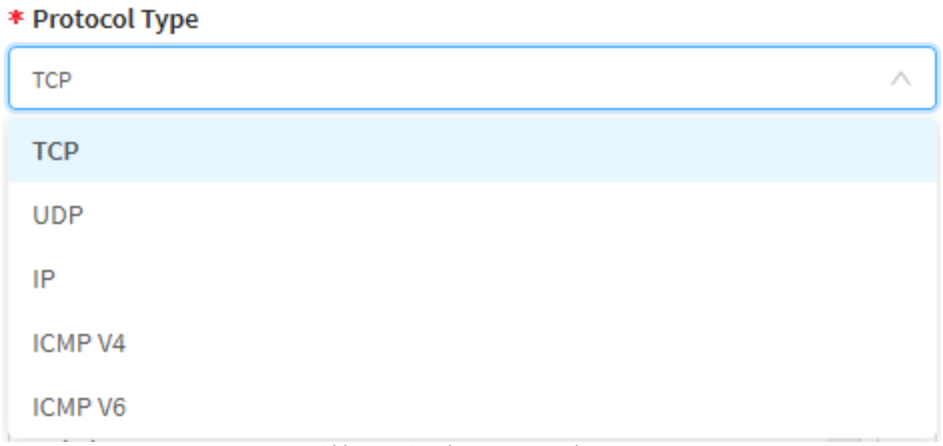
Here are some examples on how to create service objects:

- Example 1 - Creating service object;
- Example 2 - Creating VPN Client service object using MAC iOS.

Below some notes regarding the selection of the types of protocols in some fields of the form.

Protocol Type

The administrator can select between the types of protocol to compose the object, this selection allows to determine different protocols and to group them in the same object:



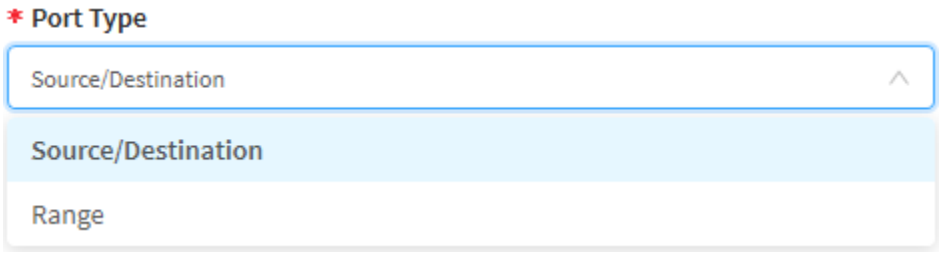
Objects – Services – Protocol Type

Follow the options in this checkbox:

- ***TCP***: It is associated with ports and port ranges for the various services that run your applications under the TCP protocol. Ex.: “Vpn pptp (1723), http (80), https (443), dns (53)”;
- ***UDP***: It is associated with ports and port ranges for the various services that run your applications under the UDP protocol. Ex.: “Vpn ike-isakmp (500), Vpn l2tp (1701), Vpn Nat-t (4500), dns (53)”.;
- ***IP***: Associates with other IP layer protocols. Ex.: “ah, egp, esp, gre, icmp, igmp, sctp, tcp e udp”;
- ***ICMP v4 and ICMP v6*:** Associated with types of treatment and/or expected response related to ICMP v4 or ICMP v6 traffic. *Ex.: “Echo Request”, “Echo Replay”, “Destination unreachable”, “time exceeded”.*

Port Type

The administrator can select between 2 (two) types of ports (services) that will compose the object.



Objects – Services – Port Type

Follow the options in this checkbox:

- ***Source/Destination*:** Definition of the [Source port] / [Destination port] fields, referring to services that normally follow RFC's standards and perform the service on a specific port (Destination port), usually on services that run under the TCP protocol. Ex. “*HTTP* (80); *HTTPS* (443), *DNS* (53)”. There are cases of services that also run under the UDP protocol. Ex. “*DNS* (53)”;
- ***Range*:** Definition of the ports or services that normally run within a class of ports [Initial port] / [End port], usually on services that run under the UDP protocol. Services that typically run in port ranges. Ex.: “*VOIP* - starting port 4500/*UDP*; final port 5500/*UDP*.; Cameras - starting port 10000/*UDP*; final port 20000/*UDP*”.

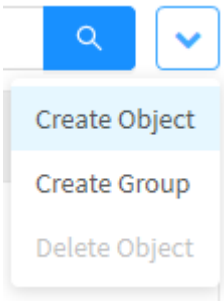
The **[Source port]** field is an optional field. Usually runs under a random high [1024: 65535] port runs at service start.

The range of ports even for applications of the same type may vary according to the specification of each application.

Example 1 - Creating service object

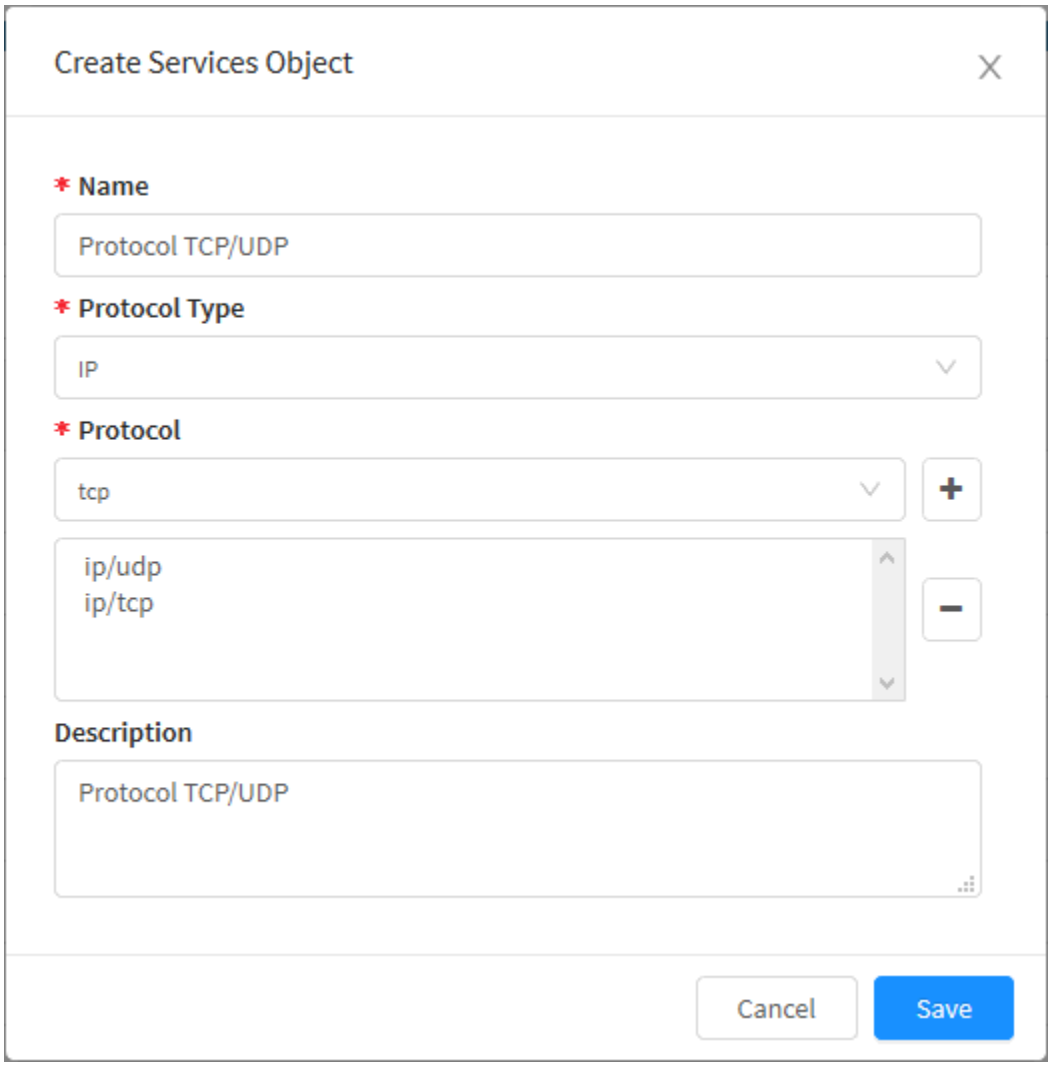
Through the option “Create Object” it is possible to create a new Object Services. To access, follow the steps:

1. In the action menu **[**  **]**, click on the “Create Object” option;



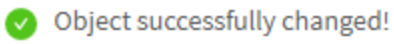
Objects – Services – Create Object

2. The Create Service Objects screen will appear. Fill in the fields:



- ***Name*:** Object name. Ex.: *HTTP*;
- ***Protocol Type*:** Select the object's protocol, among the options: “TCP”, “UDP”, “IP” and “ICMP”. Ex .: TCP;
- **Port Type:** Determines whether the port type will be of origin/destination or within an IP range. If you selected the range option, you will need to determine the range in the following text fields;
- **Port:** Determines the source and destination port of the addresses, to be added to the list of service objects;
- ***List*:** Lists the added ports. To delete an entered value, select it and click the **[** − **]** button, otherwise click the **[** + **]** button to make an addition to the list;
- ***Description*:** Object description. Ex.: *HTTP Protocol*.

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.

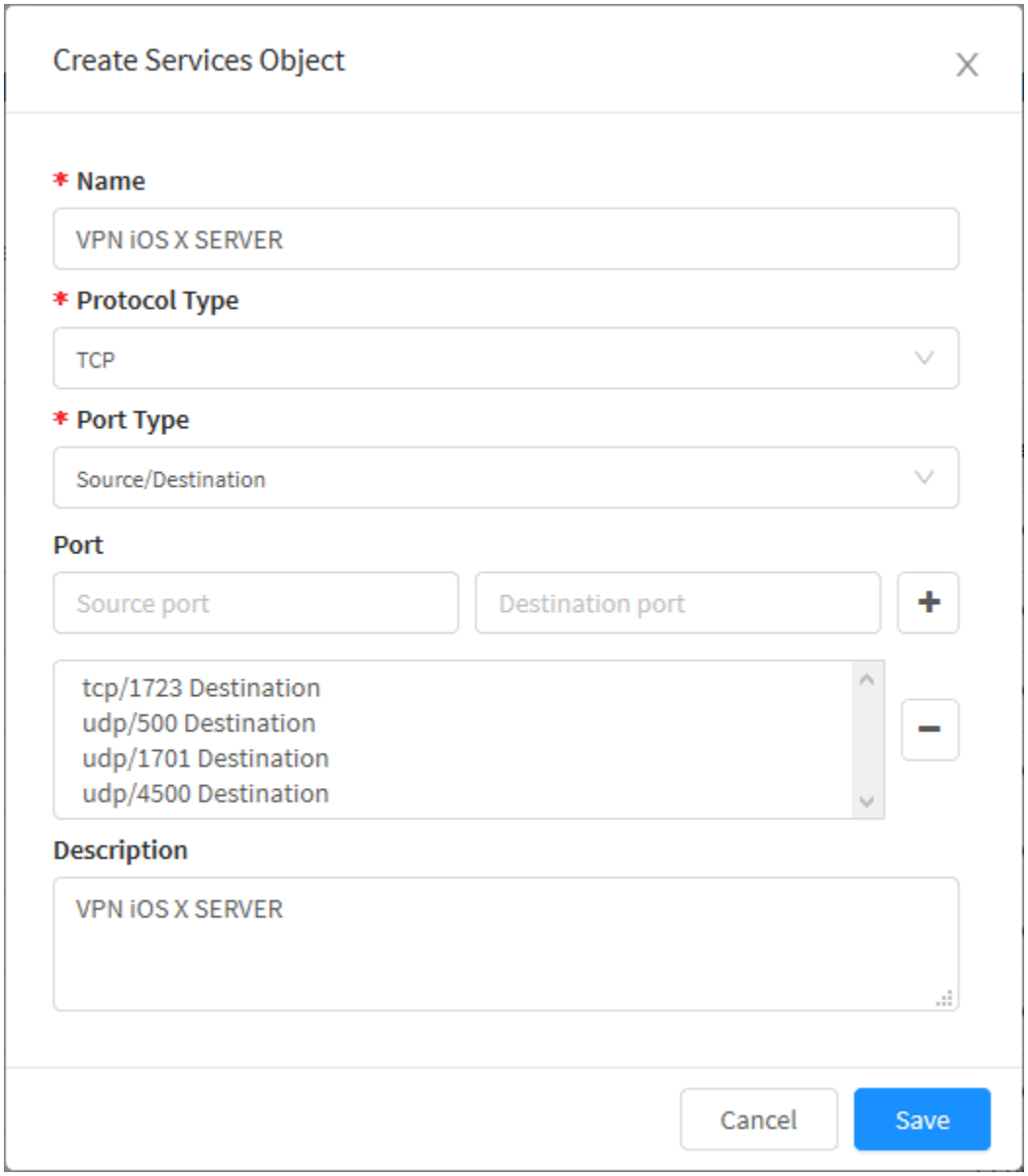


Object successfully changed

The service object was created successfully.

Example 2 - Creating VPN Client service object using MAC iOS

Let's exemplify the registration of a Service object for VPN Client application using MAC iOS. Ex.: “iOS X Server VPN - Ports 500 / UDP; 1701 / UDP; 4500 / UDP; 1723 / TCP ”.



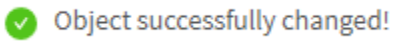
Object Service - VPN iOS X Server

- ***Name*:** Object name. Ex.: VPN iOS X SERVER;
- ***Protocol Type*:** Select the object's protocol, among the options: “TCP”, “UDP”, “IP” and “ICMP”. In this example we will use the TCP and UDP protocol;
- **Port Type:** Determines whether the port type will be of origin/destination or within an IP range. If you selected the range option, you will need to determine the range in the following text fields. In this example, only the "Source/Destination" option will be used;
- **Port:** Determines the source and destination port of the addresses, to be added to the list of service objects. In this example we will specifically use the destination ports, as shown in the image, add:
    - **Protocol Type:** TCP; **Destination Port:** 1723 and click **[+]** to add the value to the list;

- **Protocol Type:** UDP; **Destination Port:** 500 and click **[+]** to add the value to the list;
- **Protocol Type:** UDP; **Destination Port:** 1701 and click **[+]** to add the value to the list;
- **Protocol Type:** UDP; **Destination Port:** 4500 and click **[+]** to add the value to the list.

- ***List*:** Lists the added ports. To delete an entered value, select it and click the **[−]** button, otherwise click the **[+]** button to make an addition to the list. After the previous step, we should have 4 inserts already listed, as shown in the image;
- ***Description*:** Object description. Ex.: VPN iOS X SERVER.

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



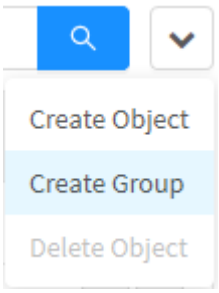
Object successfully changed

The service object was created successfully.

Services - Actions Menu - Create Group

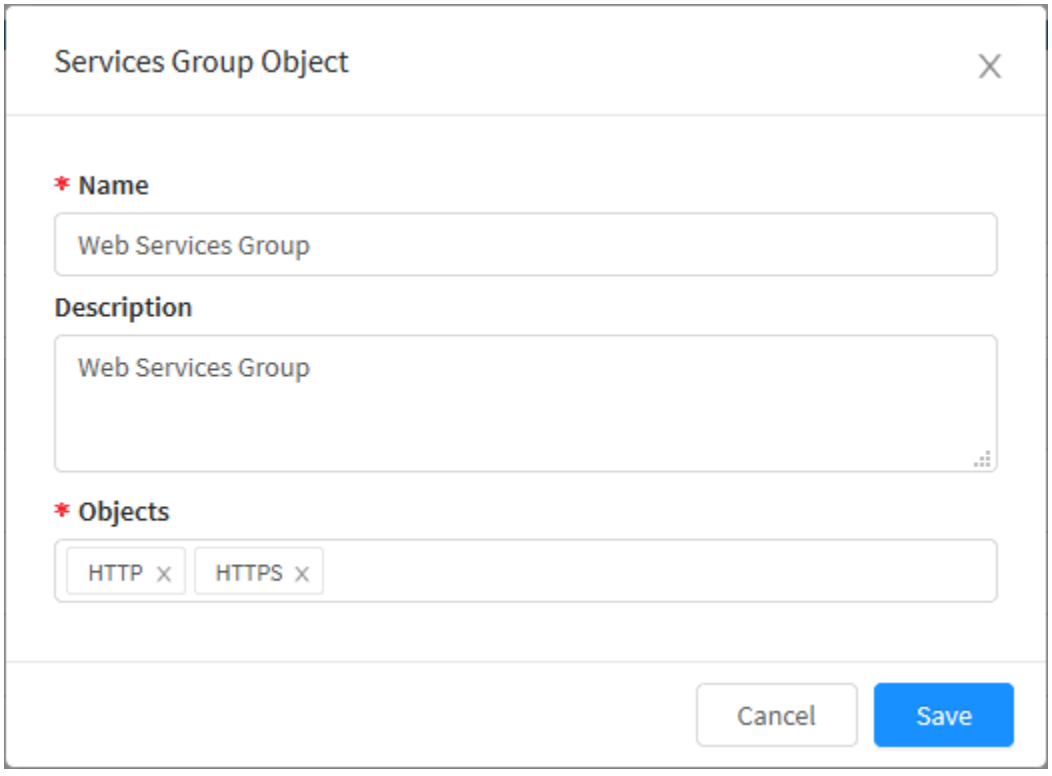
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Group”;



Objects – Services – Create Group

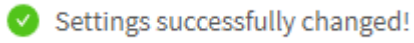
2. Fill in the information on the Services Group Object screen:



Objects – Services Group Object

- ***Name*:** Object group name. Ex.: Web Services Group;
- ***Description*:** This field is intended for the description of the group. Ex.: Web Services Group;
- ***Objects*:** It allows to select the objects that were previously added in Services - Actions Menu - Create Object. The objects added in this field will be inserted as tags.

Click the [Cancel] button to Cancel or the [Save] button to save.



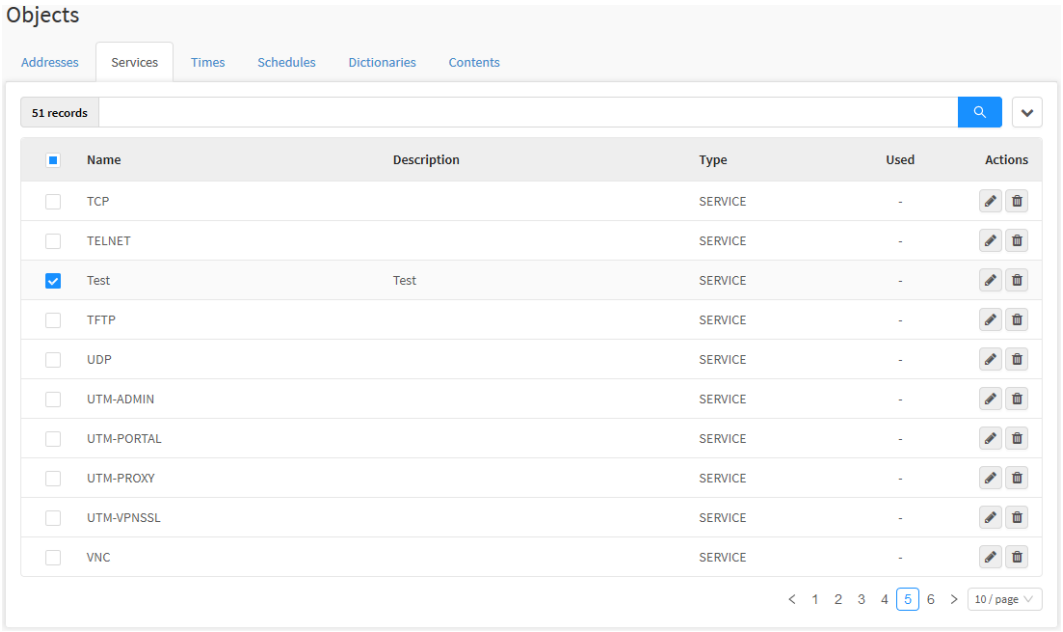
Settings successfully changed

The group was created successfully.

Services - Actions Menu - Delete Object

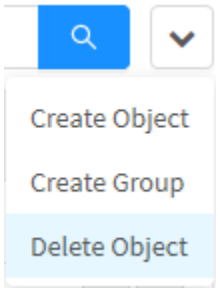
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the checkbox **[ ]** .Ex .: Test;



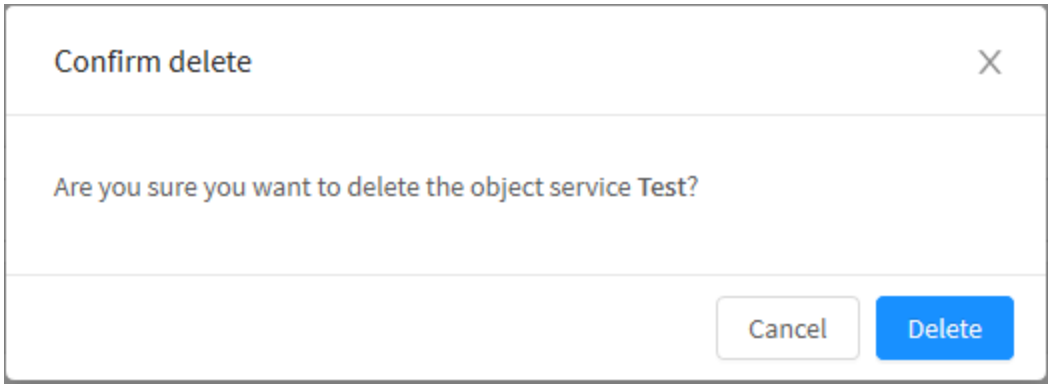
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - *Are you sure you want to delete the object service?*

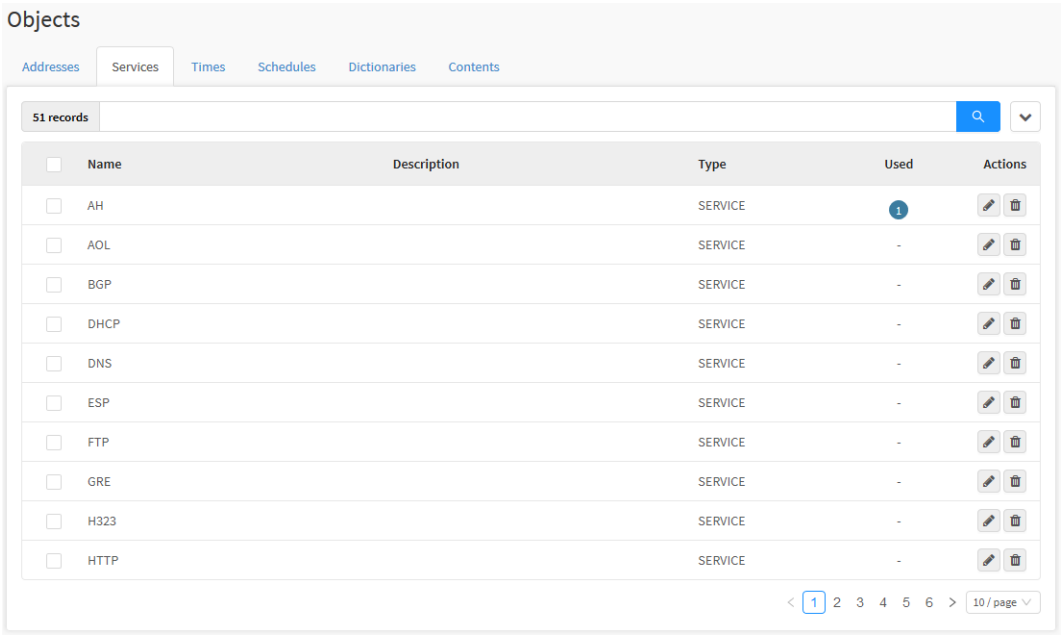
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Services - Columns

In the "Services" tab, you can view the actions menu and six columns:



Objects – Services tab

Below we will explain each column of the Services tab:

- **Checbox[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** The object description;
- ***Type*:** Object Type;
- ***Used*[1]:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed.
- ***Actions*:** Allows you to edit, select and delete the object;
    - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the action menu;
    - **Delete[ ]:** Allows you to remove the Object.

Services - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

Time

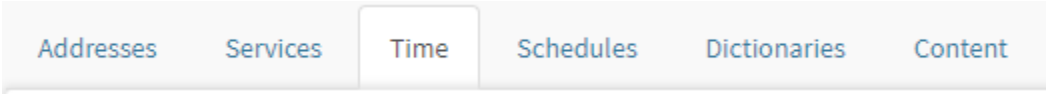
Time-type objects are made up of the “days of the week” and the “start and end time”. Ex .: “Business Hours - start: Monday from 8:00 AM until Friday at 6: 00 PM.

By default, the system brings 2 (two) pre-registered TIME objects.

- *Business*;
- *Weekend.*

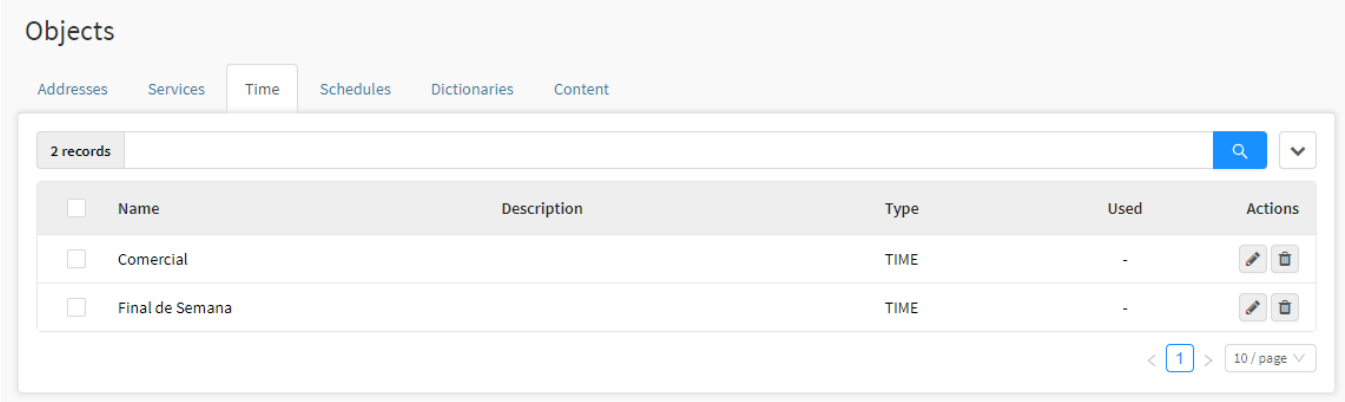
These objects are available to be used in service configuration processes and by “Policy”.

Click on the "Time" tab.



Time

The "Time" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the actions menu on the right.



Objects - Time

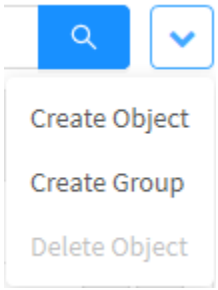
We will explain in detail the action menu and later the columns of the "*Time*" tab.

Times - Actions Menu

At the top right of the screen we have the actions menu:

Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects – Actions menu

The menu consists of the following options:

- Create Object;
- Create Group;
- Delete Object.

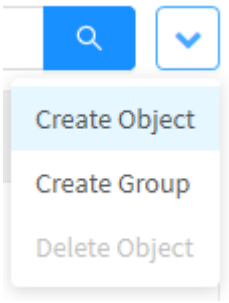
Next, each action menu option will be detailed.

Times - Actions Menu - Create Object

Through the option “Create Object” it is possible to create a new object Time and configure it according to the definitions of the policies to be applied.

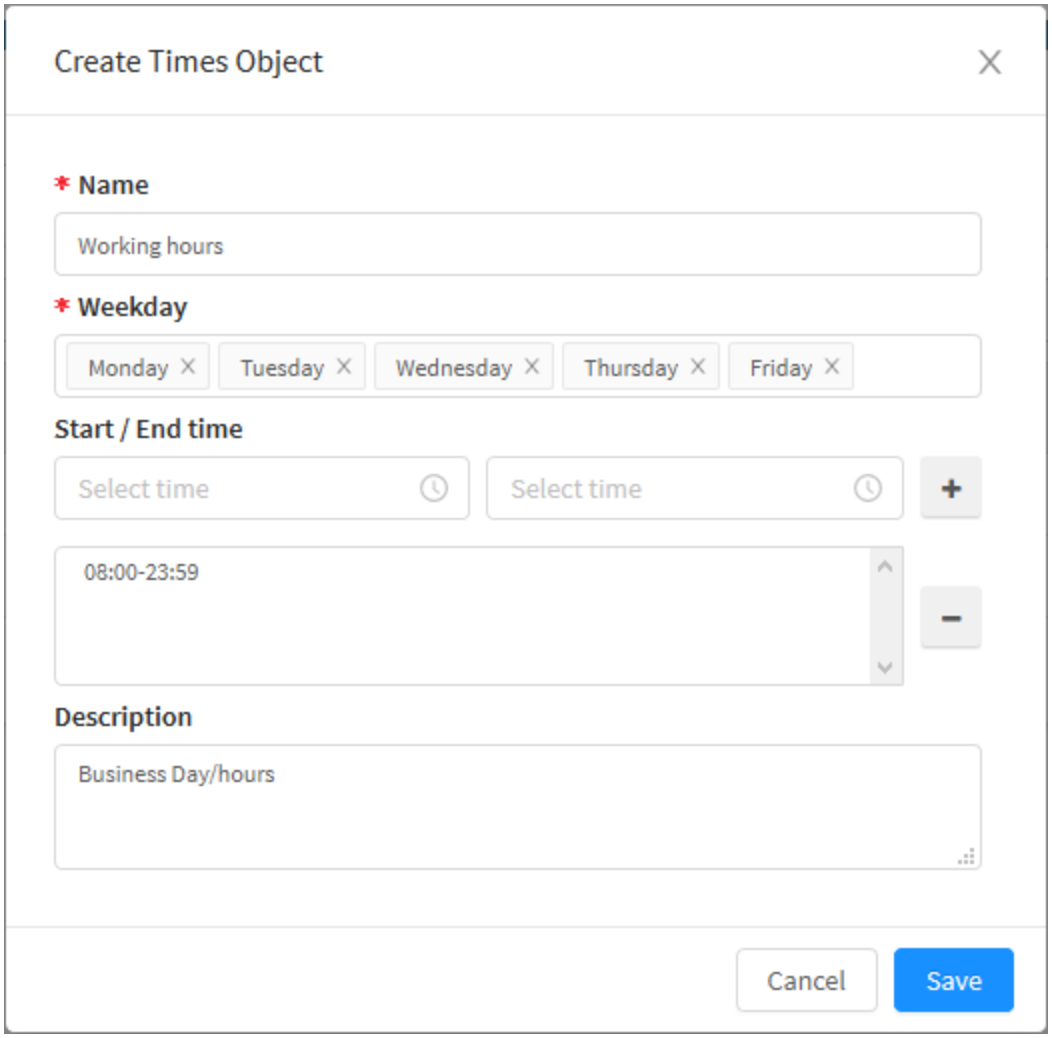
Let's exemplify adding a time object, for that, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Object”:



Objects – Times – Create Object

2. The Create Times Objects screen will appear. Fill in the fields:

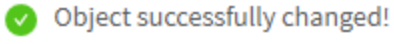


Service Objects – Create Times Object

- ***Name*:** Object name. Ex.: *Working hours*;
- ***Weekday*:** Allows you to select the days of the week. Ex.: "*Monday*", "*Tuesday*", "*Wednesday*", "*Thursday*" and "*Friday*";
- **Start / End time:** Defines the object's time bands. The end time cannot be earlier than the start time and vice versa. Ex.: "08:00 – 23:59";
- ***List*:** Lists the times added. To delete an entered value, select it and click the [−] button, otherwise click the **[** + **]** button to make an addition to the list;
- ***Description*:** Description of the object. Ex.: HTTP Protocol.

The definition of the time object allows to include several ranges of start time/end time in the same object.

Click the **[** Cancel **]** button to cancel. Click the **[** Save **]** button to save.



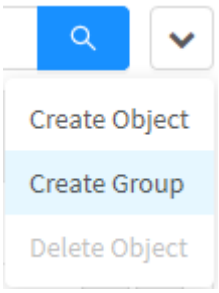
Object successfully changed

The object time was created successfully.

Times - Actions Menu - Create Group

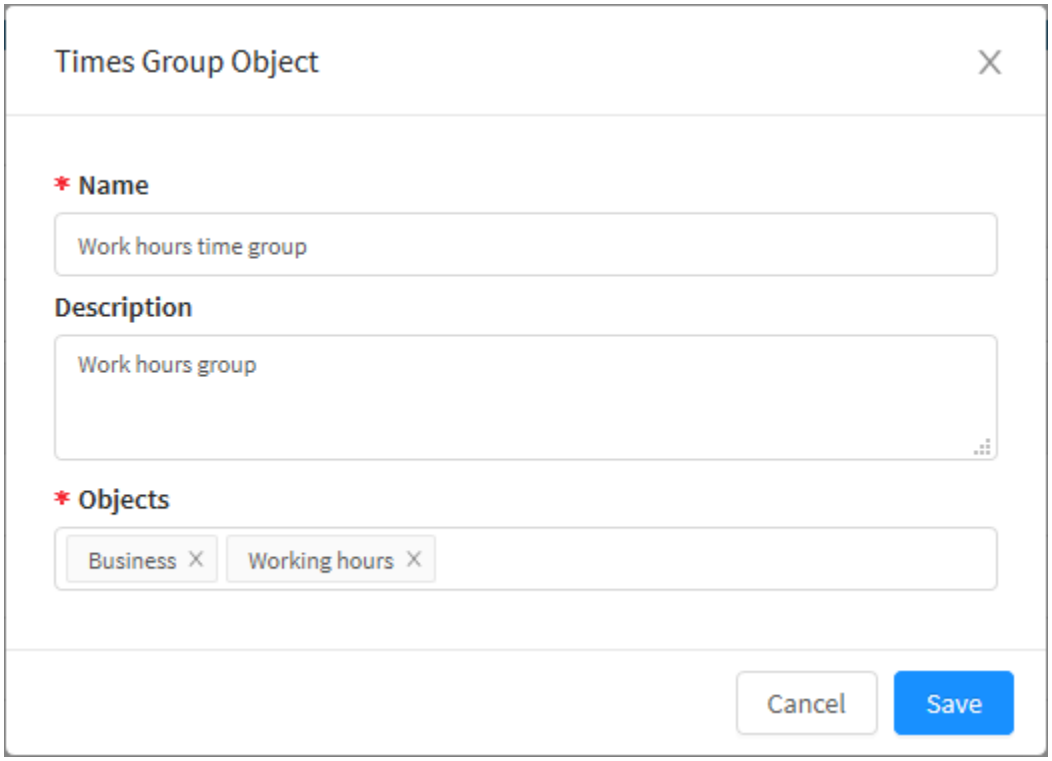
Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:

1. In the action menu **[**  **]**, click on the option “Create Group”;



Objects – Times – Create Group

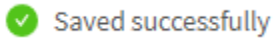
2. Fill in the information on the Times Group Object screen:



Objects – Times Group Object

- ***Name*:** Object group name. Ex.: *Work hours time group*;
- ***Description*:** This field is intended for the description of the group. Ex.: *Work hours group*;
- ***Objects*:** Allows you to select objects that were previously added in Objects - Times - Menu de ações - Create Object. The objects added in this field will be inserted as tags.

Click the [Cancel] button to Cancel or the [Save] button to save.



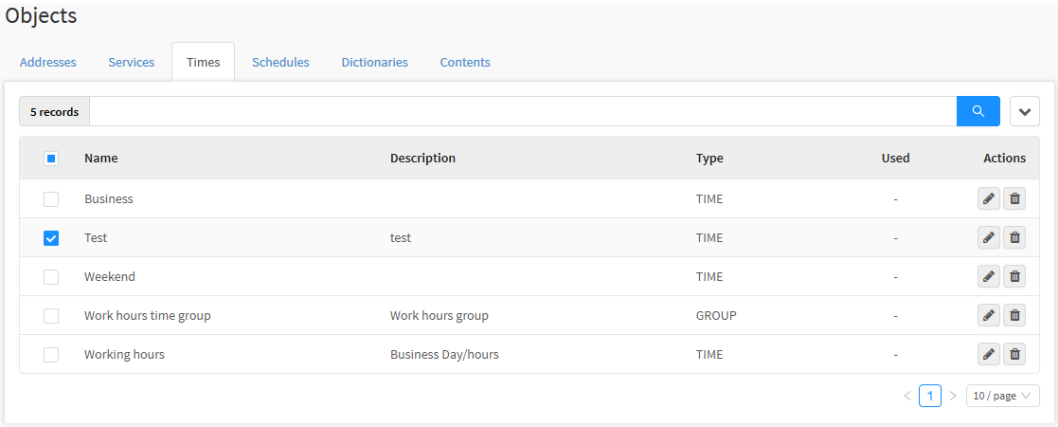
Saved successfully

The group was created successfully.

Times - Actions Menu - Delete Object

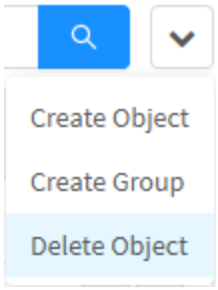
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the ***checkbox*[ ]**.Ex.: *Test*;



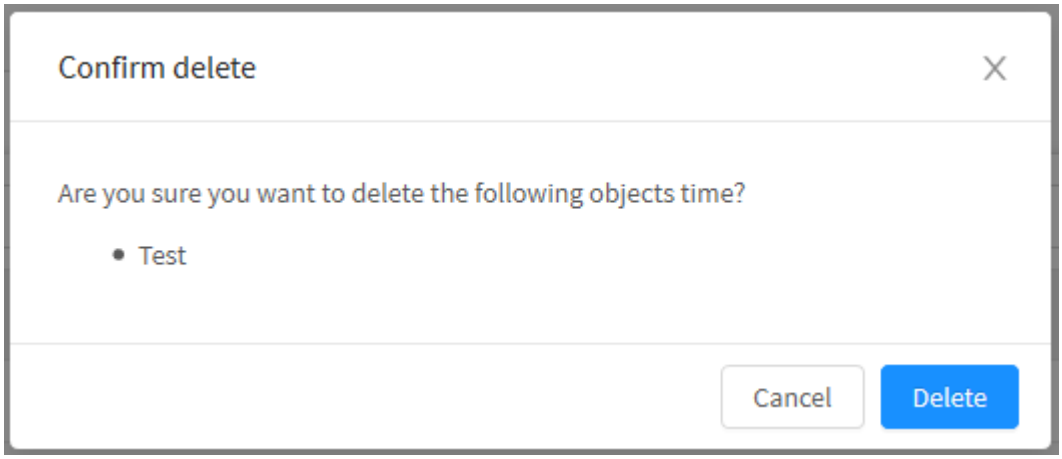
Objects - Objects selected for deletion

2. Enter the actions menu **[ ]** and click on the “Delete Object” button.



Objects - Actions Menu - *Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following object time?

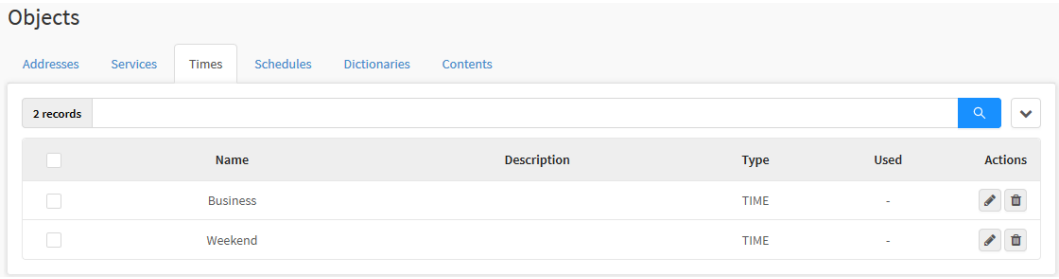
If you want to cancel, click the **[** Cancel **]** button. To finish, click the **[** Delete **]** button.

Object deleted successfully

After performing these procedures the packages will have been successfully deleted.

Times - Columns

In the "Times" tab it is possible to view the actions menu and six columns:



Objects – Times tabs

Next we will explain each column of the Times tab:

- **Checkbox[ ]:** Select the desired objects;
- ***Name*:** Object Name;
- ***Description*:** The object description;
- ***Type*:** Object Type;
- ***Used*[1]:** Enumerates the number of times this object is being used. By clicking on this number, the *Object Mapping* window is displayed.
- ***Actions*:** Allows you to edit, select and delete the object;
    - ***Edit*[ ]:** Allows you to edit the settings of the Object added in the Create Object option of the action menu;
    - **Delete[ ]:** Allows you to remove the Object.

Times - Object Mapping

By clicking on the icon of how many times an object has been used [1] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.

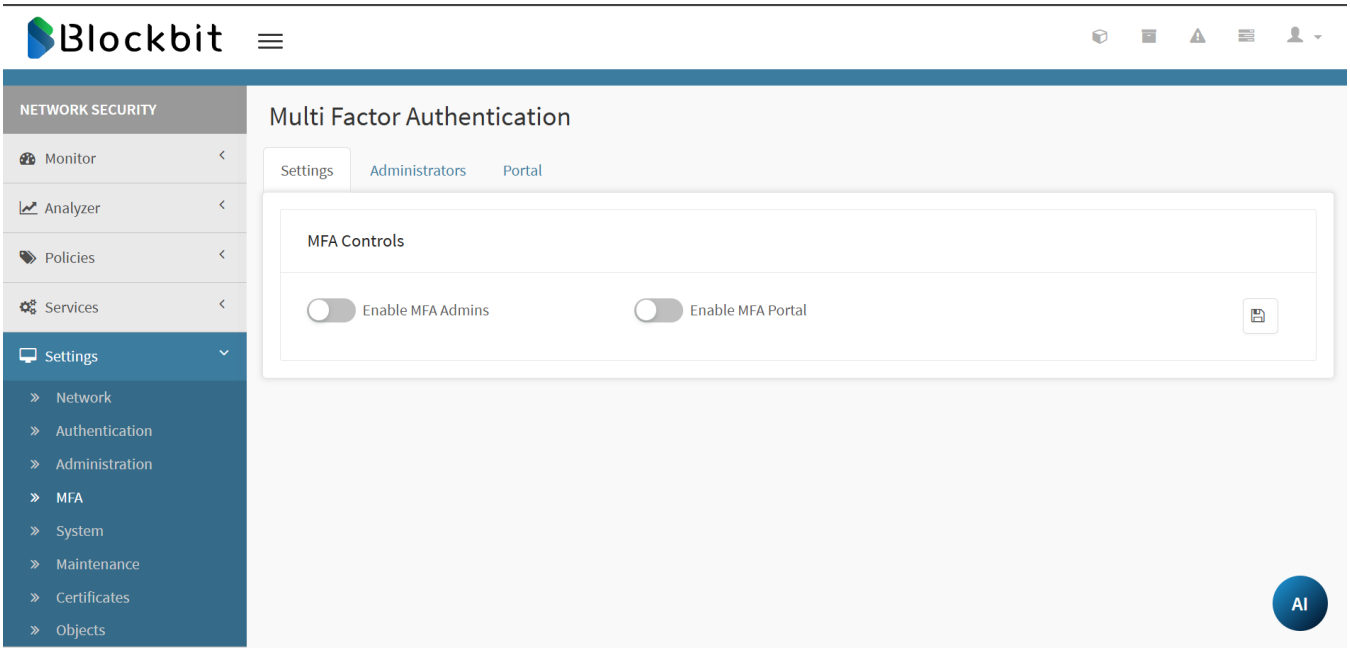
Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

NGFW - Settings - Multi Factor Authentication

Multi-factor authentication (MFA) is a way to enhance access security by requiring more than one factor to verify a user's identity.

In the NGFW, you can enable MFA for administrators and Captive Portal users.



To enable MFA for administrators, click **Enable MFA Admins**.

To enable MFA for Captive Portal users, click **Enable MFA Portal**.

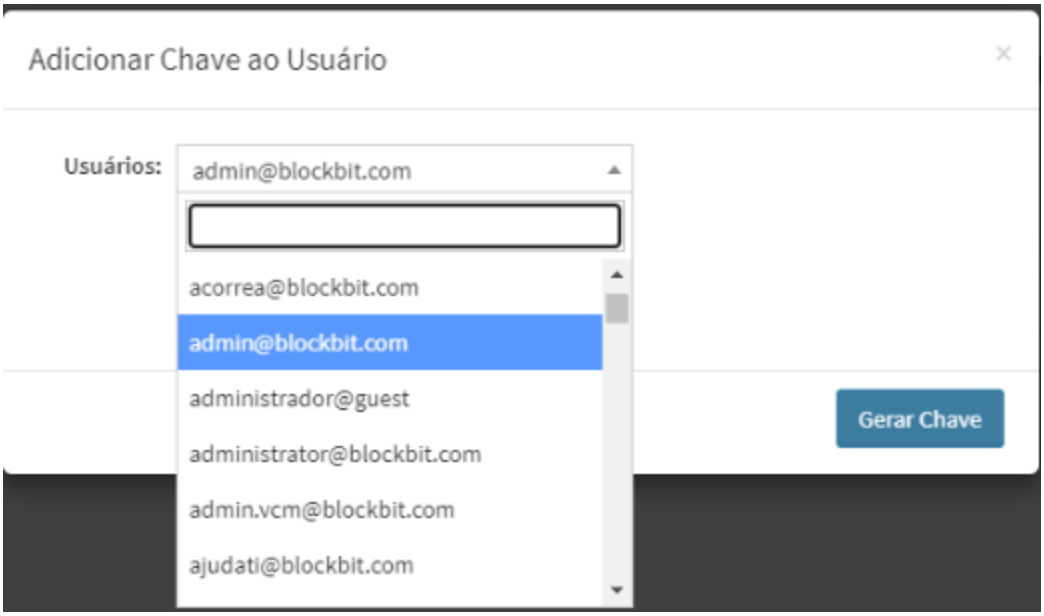
Under the **Administrators** and **Portal** tabs, there is a list of users and their respective keys.

To copy a key, click **Copy (**  **)**.

To delete a key, click **Delete (**  **)**.

To generate a new key, click the **+** button in the upper right corner.

Select the user and click **Create key**.


Adicionar Chave ao Usuário
Usuários:
admin@blockbit.com
acorrea@blockbit.com
admin@blockbit.com
administrador@guest
administrator@blockbit.com
admin.vcm@blockbit.com
ajudati@blockbit.com
Gerar Chave

UTM - SNAPSHOT

The Snapshot option offers a faster and more compact way to save the BLOCKBIT UTM settings.

The Snapshot contains the UTM database and services configuration files dumped by the system:

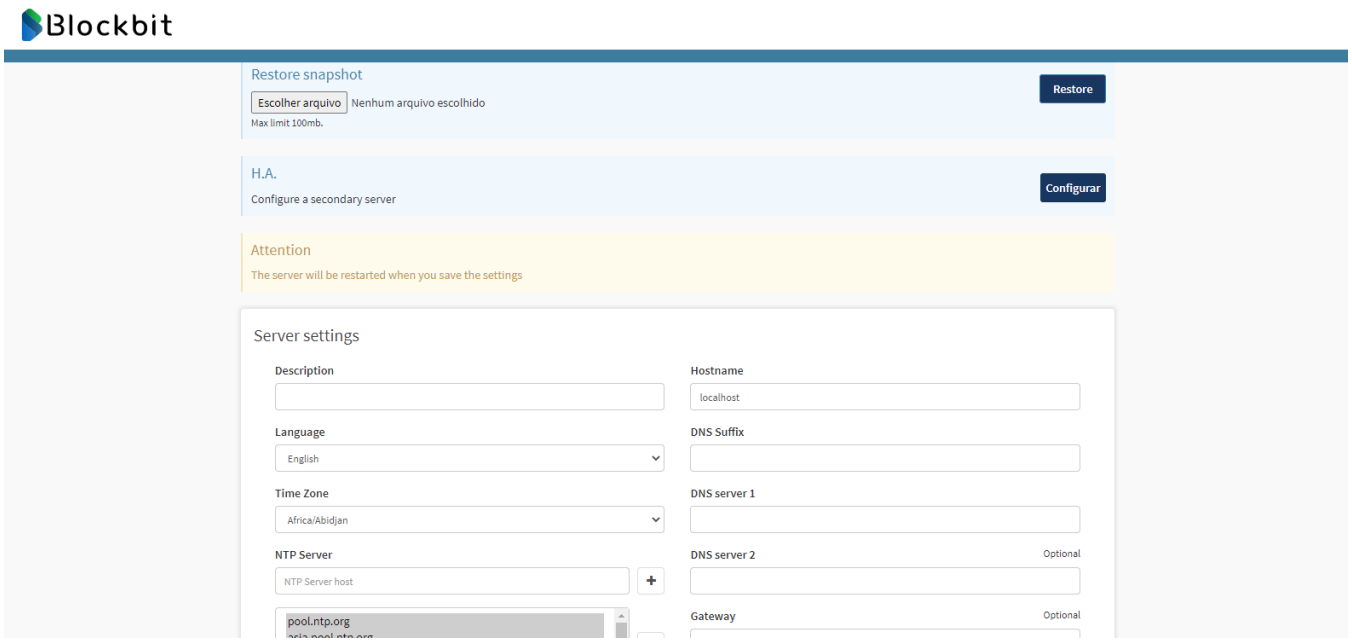
- Operating system service configuration files:
  - Network (Ex.: Network Interfaces, IPs, Routes etc.);;
  - Services (Ex.: Firewall, Proxy, IPS, VPN etc.);
  - Others OS datas.

The snapshot does not include specific files that could cause problems when restoring to a new installation or another machine.

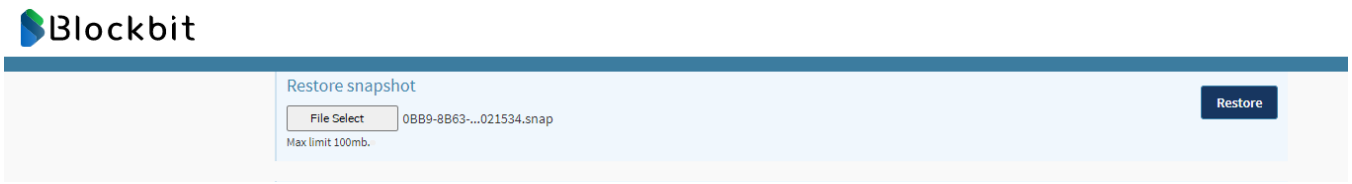
- In your web browser access: https://<IP address>:98. In case the IP address has been changed, use the latter;

Wizard page

After accessing the recovery page, select the "Configure manually" option to set it up manually. The following page will be displayed:



Manual wizard page



".snap" file select

Select the ".snap" file that shall be used and the system will run the recovery process, without the necessity of filling the remaining information.

After this process, the UTM should restore all the settings saved on the Snapshot.

Keep in mind that in case the device's UUID or machine is different, or the license is invalid it will be necessary to reissue the solution's license. However, if the restore is being made in the same machine and the license is still valid, then it is NOT necessary to reissue the solution's license.

The Snapshot that will be used in the NGFW's restore process must be from the same version of the NGFW that will be used, otherwise it won't work.

UTM - TERMINAL

The action button “Terminal” allows the administrator to access the text interface (shell) directly through the UTM:

Terminal

When accessing the option, a new window will open in the browser. To access the terminal, use the user “admin” and the personalized “password”.

By default, access credentials are:

- *Login*: admin;
- *Password*: admin.

Upon logging in, the following output will be displayed:

```
utm login: admin
admin@utm.blockbit.com's password:
Last login: Wed Jan 22 10:40:29 2020 from 172.16.100.144
Welcome to BlockBit
Type '?' or 'help' to get the list of allowed commands

admin  >
```

Terminal - Loged in successfully

For more information about CLI, check UTM - INTERFACE BLOCKBIT CLI - COMMAND LINE.

UTM - INTERFACE BLOCKBIT CLI - COMMAND LINE

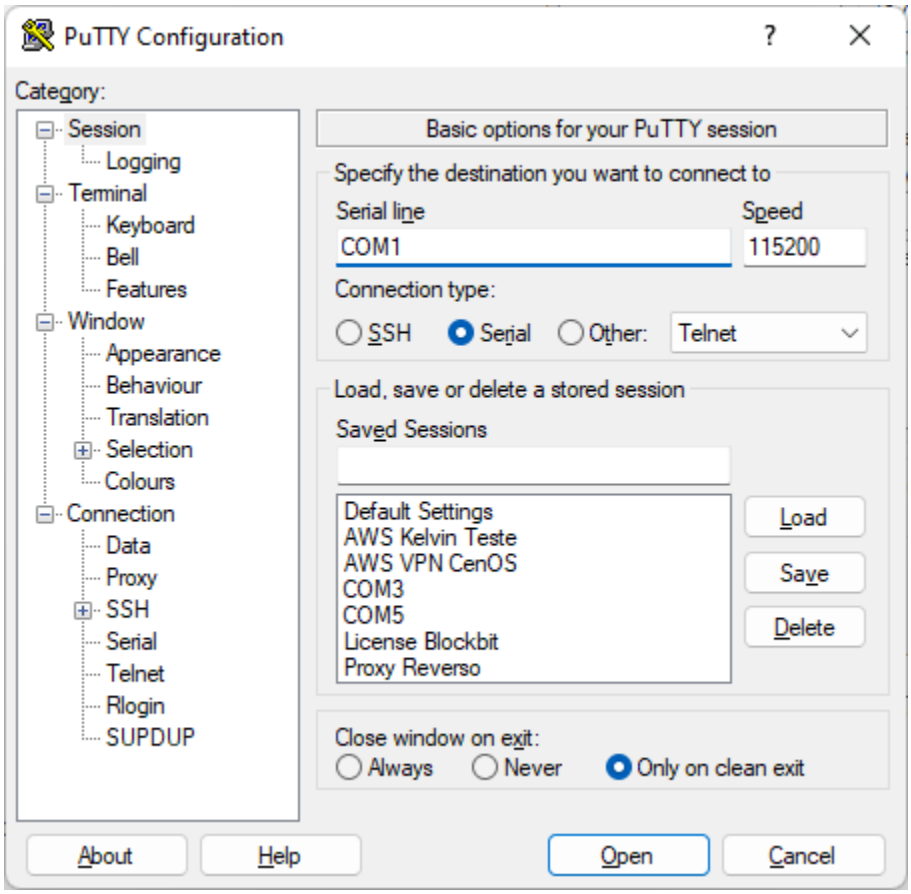
Blockbit UTM provides a Command Line Interface - CLI console feature, which allows the administrator to execute administrative and troubleshooting commands for the main system services. To perform the configuration, an SSH client and Console are required. The minimum recommended applications are:

- *PUTTY*;
- *CygWin*;
- *Mobaxterm*.

Next we will present step by step how to access the Blockbit UTM CLI console:

1. Check that the access device has a recommended SSH client already installed. In this case, we will exemplify the process using the “PUTTY” application;
2. Access the SSH console and fill in the fields:

- ***Host Name* (or *IP Address*):** Enter the IP address of the Blockbit UTM. Ex.: 172.16.102.136;



PuTTY Configuration

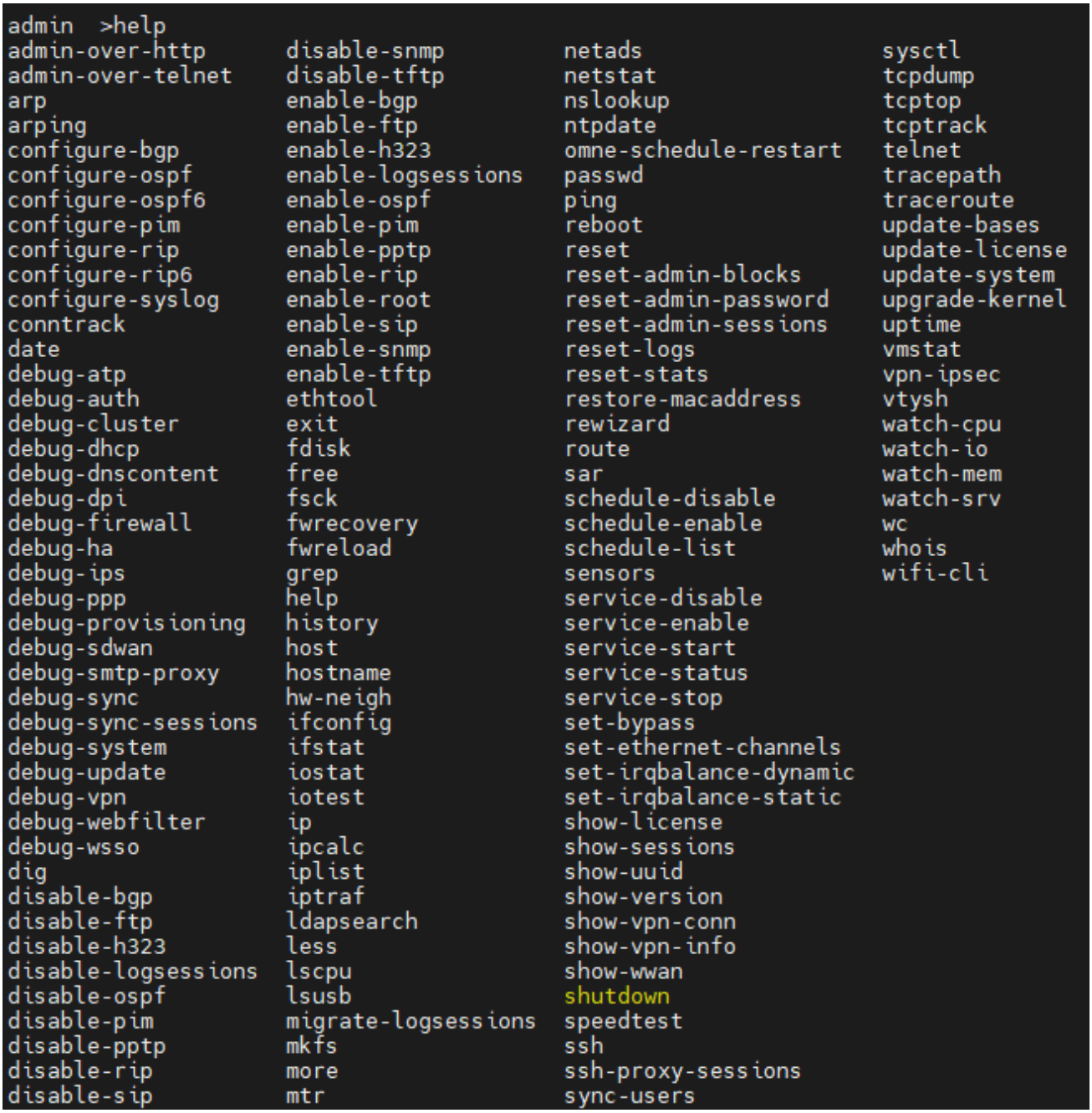
- Click the “Open” button.

3. The console will be displayed, prompting for user and password;

```
In "login as:" type the user admin
and press "Enter".
```

It is also possible to access the CLI interface by the USB Port, which makes it a COM Port.

The image below shows the commands of the main system services.



Blockbit UTM – *Command Line Interface*

Next, we'll introduce each command:

- *[arp]*;
- *[arping]*;
- *[configure-bgp]*;
- *[configure-ospf]*;
- *[configure-ospf6]*;
- *[configure-pim]*;
- *[configure-rip]*;
- *[configure-rip6]*;
- *[configure-syslog]*;
- *[conntrack]*;
- *[date]*;

- *[debug-auth];*
- *[debug-cluster];*
- *[debug-dhcp];*
- *[debug-events];*
- *[debug-firewall];*
- *[debug-sdwan];*
- *[debug-smtp-proxy];*
- *[debug-sync];*
- *[debug-threats];*
- *[debug-vpn];*
- *[debug-webfilter]*
- *[dig];*
- *[disable-bgp];*
- *[disable-logsessions];*
- *[disable-ospf];*
- *[disable-pim];*
- *[disable-rip];*
- *[disable-sip];*
- *[disable-snmp];*
- *[enable-bgp];*
- *[enable-logsessions];*
- *[enable-ospf];*
- *[enable-pim];*
- *[enable-rip];*
- *[enable-root];*
- *[enable-sip];*
- *[enable-snmp];*
- *[ethtool];*
- *[exit];*
- *[fdisk];*
- *[free];*
- *[fsck];*
- *[fwrecovery];*
- *[fwreload];*
- *[grep];*
- *[help];*
- *[history];*
- *[host];*
- *[hostname];*
- *[ifconfig];*
- *[ifstat];*
- *[iostat];*
- *[iotest];*
- *[ip];*
- *[ipcalc];*
- *[iplist];*
- *[iptraf];*
- *[ldapsearch];*
- *[less];*
- *[lscpu]*
- *[lsusb];*
- *[migrate-logsessions];*
- *[mkfs];*
- *[more];*
- *[mtr];*
- *[netads];*
- *[netstat];*
- *[nslookup];*
- *[ntpdate];*
- *[passwd];*
- *[ping];*
- *[reboot];*
- *[reset];*
- *[reset-admin-blocks];*
- *[reset-admin-password];*
- *[reset-admin-sessions];*
- *[reset-logs];*
- *[reset-stats];*
- *[rewizard];*
- *[route];*
- *[sar];*
- *[schedule-restart]*
- *[sensors]*
- *[service-disable];*
- *[service-enable];*
- *[service-start];*
- *[service-status];*
- *[service-stop];*
- *[set-bypass];*

- [set-ethernet-channels];
- *[set-irqbalance-dynamic];*
- *[set-irqbalance-static];*
- *[show-license];*
- *[show-sessions];*
- *[show-uuid];*
- *[show-version];*
- *[show-vpn-conn];*
- *[show-vpn-info];*
- *[shutdown];*
- *[speedtest];*
- [ssh-client];
- [ssh-proxy-sessions];
- *[sync-users];*
- *[sysctl];*
- *[tcpdump];*
- *[tcptop];*
- *[tcptrack];*
- *[telnet];*
- *[tracepath];*
- *[traceroute];*
- *[update-license];*
- *[update-system];*
- *[uptime];*
- *[vmstat];*
- *[vtysh];*
- *[watch-cpu];*
- *[watch-io];*
- *[watch-mem];*
- *[watch-srv];*
- *[wc];*
- *[whois].*
- *[wifi-cli]*

UTM - [arp]

Used to map the network address (for example, an IPv4 address) to a physical address, such as an Ethernet address (also called MAC address). View and modify this list of Internet address lists for Ethernet addresses. ARP has been implemented with many combinations of network technologies and data link layer. IPv4 is the most common case.

Use this command to identify a network communication problem or to identify connected IP events and status.

How to use:

```
Modo de uso
admin  >arp -h
Usage:
  arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>] <-Display ARP cache
  arp [-v]          [-i <if>] -d  <host> [pub]  <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f  [<filename>]  <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s  <host> <hwaddr> [temp] <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub <-''-

        -a  display (all) hosts in alternative (BSD) style
        -e  display (all) hosts in default (Linux) style
        -s, --set               set a new ARP entry
        -d, --delete            delete a specified entry
        -v, --verbose           be verbose
        -n, --numeric           don't resolve names
        -i, --device            specify network interface (e.g. eth0)
        -D, --use-device        read <hwaddr> from given device
        -A, -p, --protocol      specify protocol family
        -f, --file              read new entries from file or from /etc/ethers

  <HW>=Use '-H <hw>' to specify hardware address type. Default: ether
  List of possible hardware types (which support ARP):
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
    dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) x25 (generic X.25) infiniband (InfiniBand)
    eui64 (Generic EUI-64)
admin  >
```

Command Line Interface – arp

Example: Presenting the table of IP addresses and addresses of physical hosts (devices) on the network:

```
admin  >arp -a
? (172.16.12.85) at 00:26:8b:04:eb:bd [ether] on eth0
? (192.168.254.15) at 00:30:48:c2:02:a4 [ether] on eth2.254
? (172.16.13.248) at 0c:c4:7a:11:0f:96 [ether] on eth0
? (172.16.12.81) at 00:30:48:de:78:ae [ether] on eth0
? (192.168.254.4) at e6:9c:1f:89:11:32 [ether] on eth2.254
? (192.168.253.34) at 7e:49:6f:55:42:00 [ether] on eth2.253
? (172.16.12.92) at <incomplete> on eth0
? (172.16.12.90) at 10:98:36:fb:c9:1b [ether] on eth0
? (172.16.20.22) at 00:0b:ab:f1:9b:bc [ether] on eth3
? (172.16.12.71) at <incomplete> on eth0
? (172.16.20.20) at 00:0c:29:b7:34:cf [ether] on eth3
? (172.16.20.19) at 04:7d:7b:fd:53:d7 [ether] on eth3
? (172.16.12.65) at 78:2b:cb:c4:e7:12 [ether] on eth0
? (172.16.12.64) at <incomplete> on eth0
? (172.16.12.77) at 90:b1:1c:f6:2f:e2 [ether] on eth0
? (192.168.254.22) at 00:e0:4c:68:19:bf [ether] on eth2.254
admin  >
```

Command Line Interface – arp – Example

UTM - [arping]

Discover and identify the connected hosts, using the association of the ARP table with the ping-like response that adopts the ICMP protocol.

How to use:

```
admin  >arping -h
Usage: arping [-fqbDUAV] [-c count] [-w timeout] [-I device] [-s source] destination
  -f : quit on first reply
  -q : be quiet
  -b : keep broadcasting, don't go unicast
  -D : duplicate address detection mode
  -U : Unsolicited ARP mode, update your neighbours
  -A : ARP answer mode, update your neighbours
  -V : print version and exit
  -c count : how many packets to send
  -w timeout : how long to wait for a reply
  -I device : which ethernet device to use
  -s source : source ip address
  destination : ask for what ip address
admin  >
```

Command Line Interface – arping

Example: Finding the MAC address of a given IP:

```
admin  >arping -c 5 -I eth0 172.16.12.85
ARPING 172.16.12.85 from 172.16.12.1 eth0
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  6.465ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  2.099ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  0.773ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD]  0.761ms
^CSent 4 probes (1 broadcast(s))
Received 4 response(s)
admin  >
```

Command Line Interface – arping - Example

UTM - [configure-bgp]

Dynamic BGP routing configuration.

How to use:

By default the user password and privileged is admin.

```
admin  >configure-bgp
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
localhost>
```

Command Line Interface – configure-bgp

In the web interface, under **[System] >> [Network] >> [Dynamic Routing]**, by clicking on the **[ ]** icon, you can view the configuration example:

```
Example: BGP

configure-bgp

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# bgp multiple-instance
utm-bb(config)# router bgp 180
utm-bb(config)# bgp router-id 0.0.0.180
utm-bb(config-router)# network 172.16.0.0/24
utm-bb(config-router)# timers bgp 1 5
utm-bb(config-router)# neighbor 192.168.20.2 remote-as 181
utm-bb(config-router)# neighbor 172.15.0.1 remote-as 181
utm-bb(config-router)# do wr
utm-bb(config)# exit
Connection closed by foreign host
```

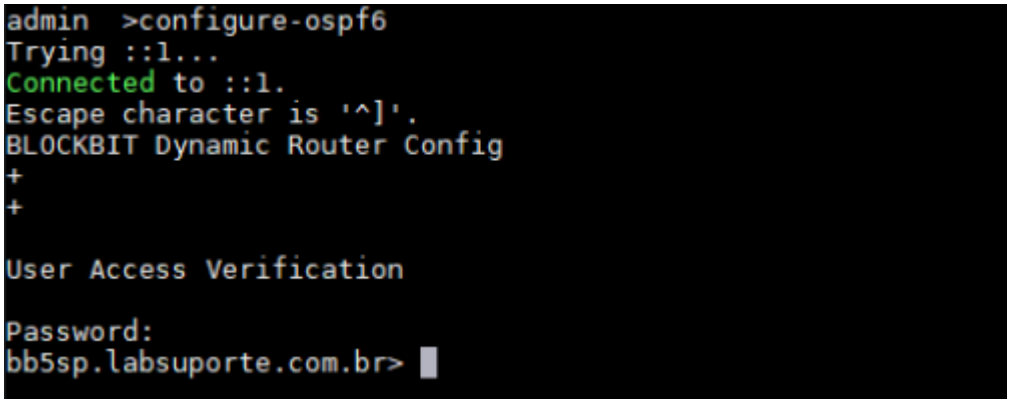
Command Line Interface – BGP configuration example

UTM - [configure-ospf6]

Configures dynamic routing from OSPF to IPv6.

How to use:

By default the user password and privileged is admin.



Command Line Interface – configure-ospf6

UTM - [configure-ospf]

Configures dynamic OSPF routing.

How to use:

By default the user password and privileged is admin.

```
admin  >configure-ospf
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
BLOCKBIT Dynamic Router Config
+
+

User Access Verification

Password:
localhost>
```

Command Line Interface – configure-ospf

In the web interface, under **[System] >> [Network] >> [Dynamic Routing]**, by clicking on the **[ ]** icon, you can view the configuration example:

```
Example: OSPF

configure-ospf

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# router ospf
utm-bb(config-router)# network 192.168.10.0/24 area 0
utm-bb(config-router)# network 172.16.0.0/24 area 0
utm-bb(config-router)# network 192.168.20.0/24 area 0
utm-bb(config-router)# exit
utm-bb(config)# do wr
utm-bb# exit
Connection closed by foreign host
```

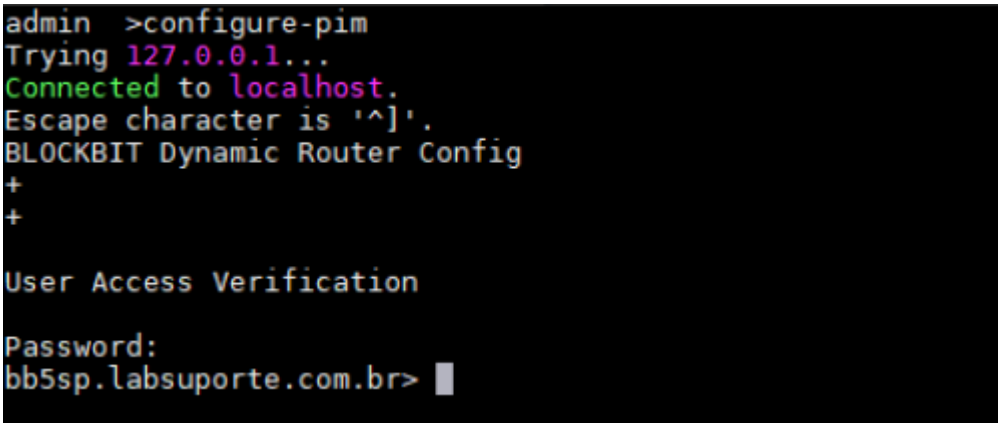
Command Line Interface – OSPF configuration example

UTM - [configure-pim]

Configures PIM-SM dynamic routing.

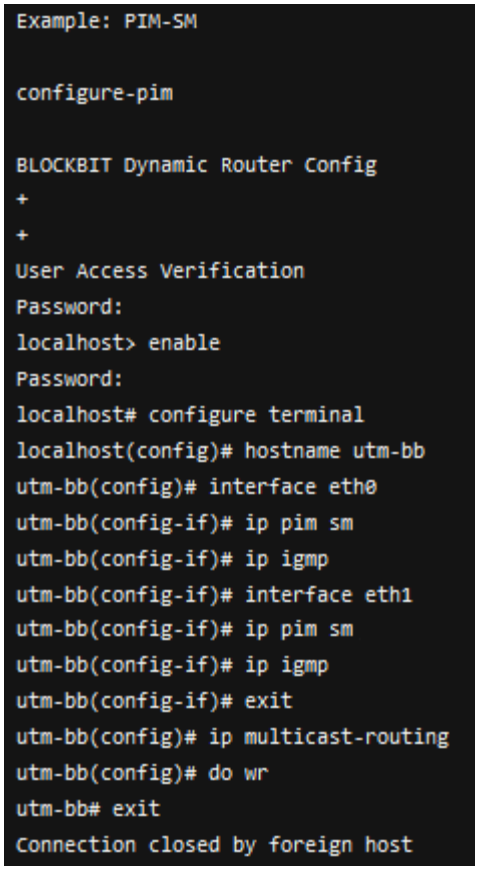
How to use:

By default the user password and privileged is admin.



Command Line Interface – configure-pim

In the web interface, under **[System] [Network] [Dynamic Routing]**, clicking on the **[ ]** icon, You can view the configuration example:



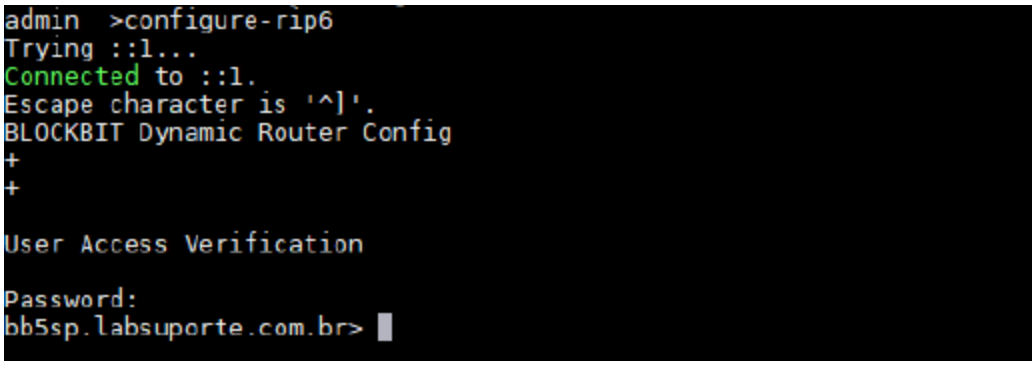
Command Line Interface – PIM configuration example

UTM - [configure-rip6]

Configures dynamic RIP routing for IPv6.

How to use:

By default the user password and privileged is admin.



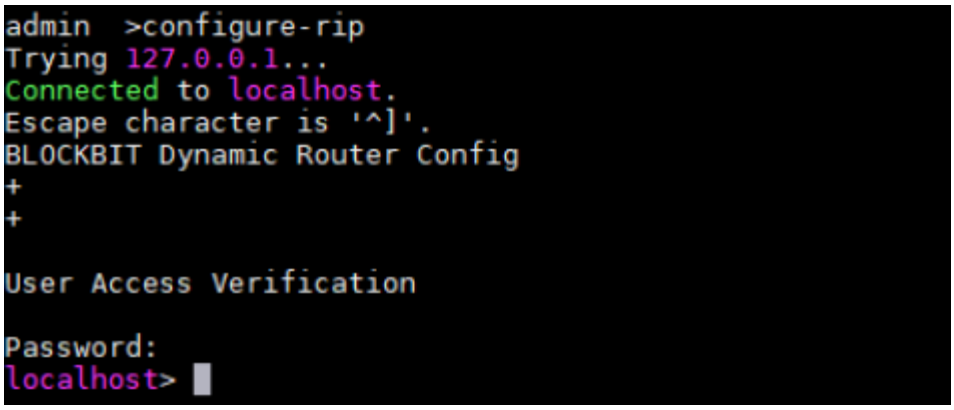
Command Line Interface – configure-rip6

UTM - [configure-rip]

Configures dynamic RIP routing.

How to use:

By default the user password and privileged is admin.



Command Line Interface – configure-rip

In the web interface, under **[System] >> [Network] >> [Dynamic Routing]**, clicking on the **[ ]** icon, You can view the configuration example:

```
Example: RIP

configure-rip

BLOCKBIT Dynamic Router Config
+
+
User Access Verification
Password:
localhost> enable
Password:
localhost# configure terminal
localhost(config)# hostname utm-bb
utm-bb(config)# router rip
utm-bb(config-router)# version 2
utm-bb(config-router)# network 10.0.0.0/8
utm-bb(config-router)# passive-interface eth0
utm-bb(config-router)# interface eth0
utm-bb(config-if)# no ip rip authentication mode text
utm-bb(config-if)# exit
utm-bb(config)# do wr
utm-bb# exit
Connection closed by foreign host
```

Command Line Interface - Example of RIP configuration

UTM - [configure-syslog]

This command has the function of configuring the syslog. Here is a summary of the function of each of its parameters:

[-i] *Interval*

Specifies the time interval in seconds that determines the limit rate for transferring files between “Syslog” servers. Recommended value: 600;

Atenção: Ao aplicar o valor 0 o *ratelimiting* é desativado. O que não é recomendável.

[-b] *Burst*

Specifies the maximum number of messages that will be exported at each "interval" time interval to the "remote" syslog server. Recommended value: 20000;

[-r] *Restore-default*

Restores the syslog default values;

[-c] *Configure*

Apply the settings determined in the previous parameters {Mandatory parameter};

[-d] *Debug*

Activates the [debug] mode, displaying a printout of all procedures applied by the ***configure-syslog*** command;

[-h] *Help*

Displays the help message.

How to use:

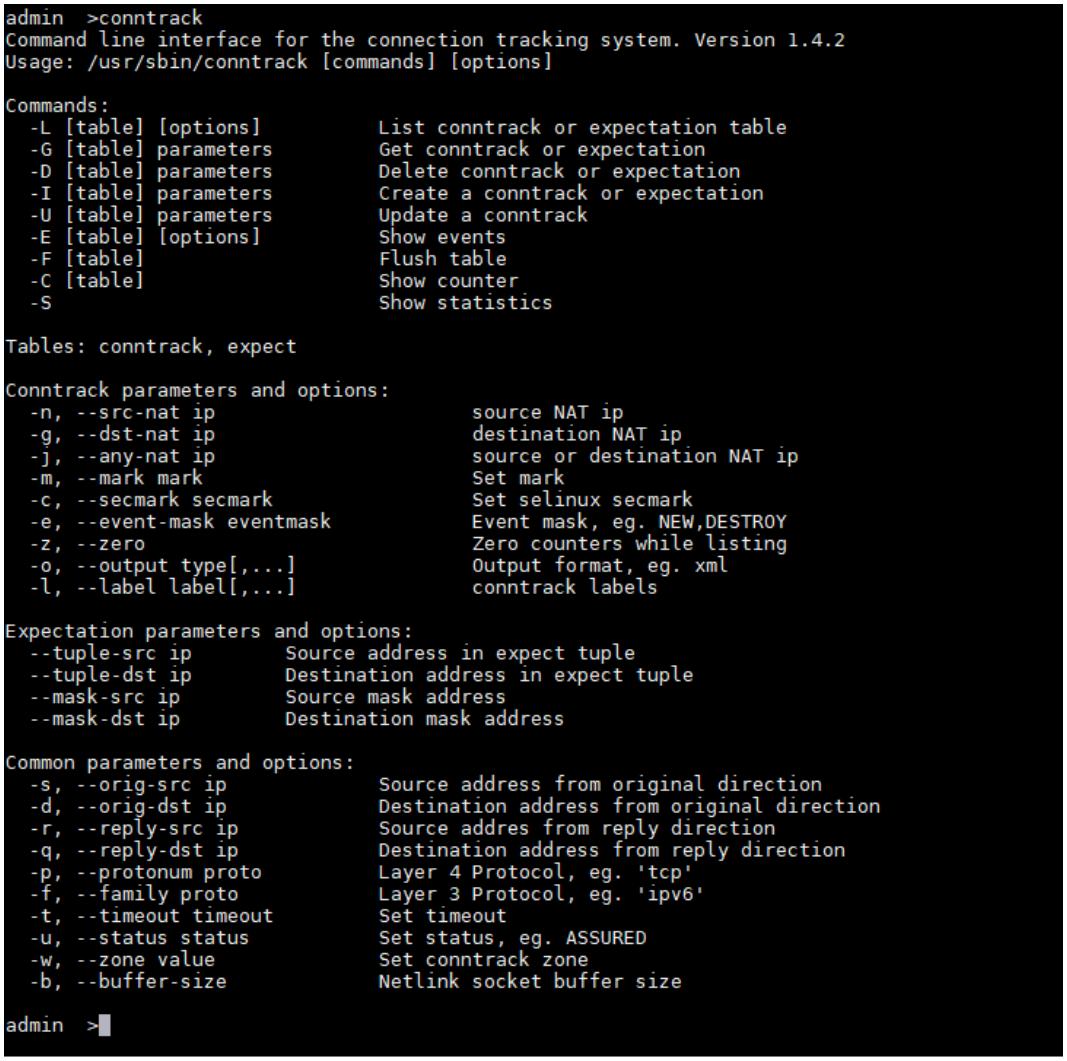
```
admin  >configure-syslog
Usage: omne-apply-syslog [OPTIONS]
Script that configures remote syslog service.

Optional Arguments
      -i, --interval             Rate Limit Interval, in seconds
      -b, --burst                Rate Limit Burst
      -r, --restore-default      Restore default values
      -c, --configure            Configure rate-limit options
      -d, --debug    Switch on|off debug mode
      -h, --help     Display this help message and exit

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com.br>

Generated at Nov 23 2018 10:32:42
admin  >
```

Command Line Interface – configure-syslog

UTM - [conntrack]

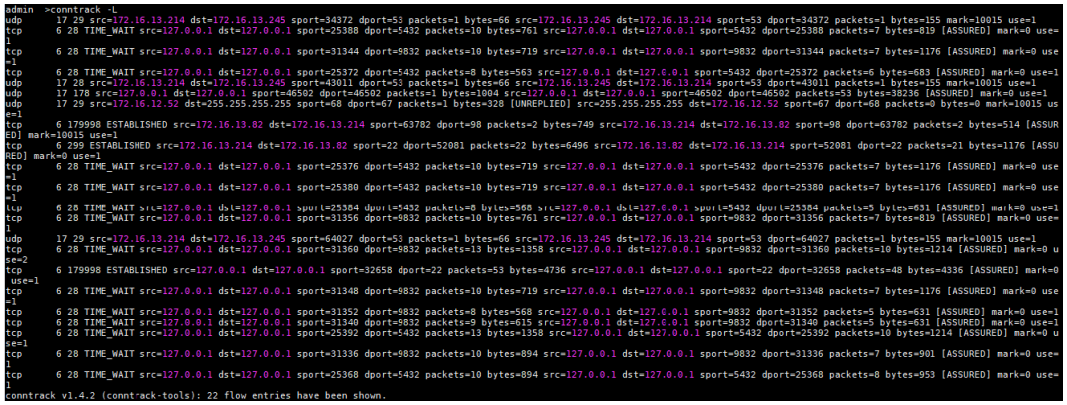
View and manage the server's connection table.

How to use:



Command Line Interface – conntrack

Example: Display all records in the connection table:



Command Line Interface – conntrack - Example

NGFW - [crypto-optimization]

Manages cryptography on IPSec and AES packages.

How to use

- To show the status, use:
  `crypto-optimization status <paralel-crypto|hw-crypto>`

- To enable, use:
  `crypto-optimization enable <paralel-crypto|hw-crypto>`

- To disable, use:
  `crypto-optimization disable <paralel-crypto|hw-crypto>`

The system will reboot after running the command crypto-optimization.

UTM - [date]

Lists and allows you to change the current date and time.

How to use:

```
admin  >date --help
Usage: date [OPTION]... [+FORMAT]
  or:  date [-u|--utc|--universal] [MMDDhhmm[[CC]YY][.ss]]
Display the current time in the given FORMAT, or set the system date.
...
Mandatory arguments to long options are mandatory for short options too.
  -d, --date=STRING         display time described by STRING, not 'now'
  -f, --file=DATEFILE       like --date once for each line of DATEFILE
  -I[TIMESPEC], --iso-8601[=TIMESPEC]  output date/time in ISO 8601 format.
                            TIMESPEC='date' for date only (the default),
                            'hours', 'minutes', 'seconds', or 'ns' for date
                            and time to the indicated precision.
  -r, --reference=FILE      display the last modification time of FILE
  -R, --rfc-2822            output date and time in RFC 2822 format.
                            Example: Mon, 07 Aug 2006 12:34:56 -0600
```

Command Line Interface – date

```
      --rfc-3339=TIMESPEC   output date and time in RFC 3339 format.
                            TIMESPEC='date', 'seconds', or 'ns' for
                            date and time to the indicated precision.
                            Date and time components are separated by
                            a single space: 2006-08-07 12:34:56-06:00
  -s, --set=STRING          set time described by STRING
  -u, --utc, --universal    print or set Coordinated Universal Time (UTC)
      --help     display this help and exit
      --version  output version information and exit

admin  >
```

Command Line Interface – date 1

Example 1: Listing the current date and time:

```
admin  >date
Thu Sep  1 09:59:08 BRT 2016
admin  >
```

Command Line Interface – date – Example 1

Example 2: Updating date and time based on the America / São Paulo time zone:

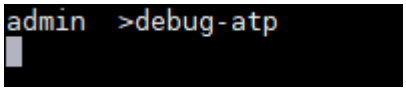
```
admin  > date --date='TZ="America/Sao_Paulo" 11:00'
Thu Sep  1 11:00:00 BRT 2016
admin  >
_OK ticket:57ddcb336098c149eebca22604e3a01a
```

Command Line Interface – date – Example 2

UTM - [debug-atp]

Displays Advanced Threat Protection debug logs in real time.

How to use:



Command Line Interface – debug-atp

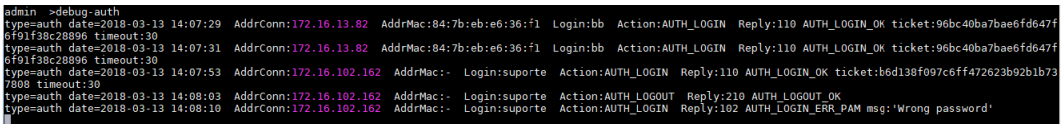
UTM - [debug-auth]

Displays authentication debug logs (login, logout, keepalive and errors) in real time.

How to use:

Command Line Interface – debug-auth

Example:



Command Line Interface – debug-auth - example

UTM - [debug-cluster]

Shows the *debug logs* of High Availability (H.A.) service.

How to use:

debug-cluster -h to see the filtering options;

```
admin  >debug-cluster -h
Usage: debug-cluster [OPTIONS]
Displays and copies debug messages related to the cluster service.

Optional arguments:
        -h, --help
                Print this help message.

        -e, --every-line
                Prints all lines found (that pass the criteria of the
                other parameters). By default, some lines are omitted
                because they are too repetitive. If more than one of
                these lines (of the same type) are found in sequence,
                only the last one is shown (the others are overwritten
                by the last one). In case of ucarp bad digest warnings
                all lines are removed by default.

                origin          | lines starting with
                ----------------------------------------
                ucarp           | '[WARNING] Bad digest - '
                cluster_bin     | 'Sync progress: '

                Note: This parameter does not affect the number of
                lines written in the output file when defined.

        -f, --file-output <file_path>
                File path to save output.

        -o, --origin <s|a|b|p|o|u>
                Origin of log messages. Takes a combination of the
                following options:
                's'     Shows messages coming from the systemd about
                        cluster_ha and cluster-restore service.
                'a'     Shows messages coming from the cluster_apply.
                'b'     Shows messages coming from the cluster binary.
                'p'     Shows messages coming from postgres.
                'o'     Shows messages coming from omne-apply-queue.
                'u'     Shows messages coming from ucarp.
                'sabou' Default origin combination.

        -s, --show-from <point_of_start>
                Print this help message. Takes one of the following
                options:
                'first_line'    Show all stored output lines.
                'last_start'    [default] Shows messages from the last
                                start of the cluster binary.
                'end'           Show only the most recent entries.

        -t, --tail
                Continuously print new entries as they are appended.
                to the log.

Usage examples:
        debug-cluster -o sabou -s last_start
                Default behavior, the same as running the command
                without a parameter. Shows all messages logged since
                the last start of the cluster binary that came from
                systemd (cluster service related messages only),
                cluster binary, conntrackd, ommne-apply-queue and ucarp.

        debug-cluster -f /tmp/logout.log
                Saves a copy of log messages in the /tmp/logout.log file.

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

Generated at Mar 10 2023 12:17:51
```

Command Line Interface – debug-cluster

The debug-cluster command must be executed in both devices, for they show different results in the primary and secondary device.

Example 1

debug-cluster -t (primary device)

debug-cluster -t (primary device)

Example 2

debug-cluster -t (secundary device)

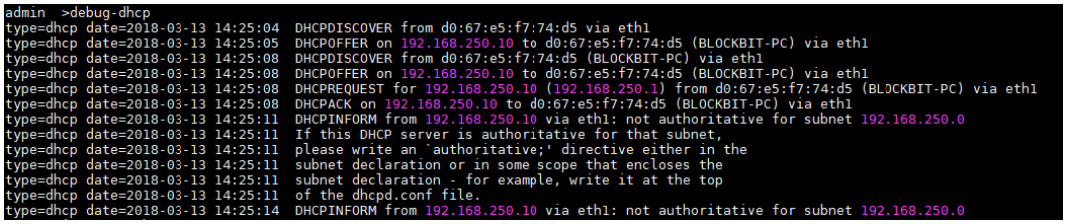
UTM - [debug-dhcp]

Displays DHCP service debug logs in real time.

How to use:

Command Line Interface – debug-dhcp

Example:



Command Line Interface – debug-dhcp - example

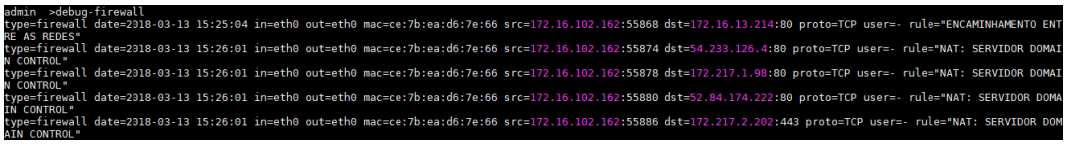
UTM - [debug-firewall]

Displays the Firewall debug logs in real time.

How to use:

Command Line Interface – debug-firewall

Example:



Command Line Interface – debug-auth - example

UTM - [debug-ha]

Displays the High Availability (H.A.) service debug logs.

How to use:

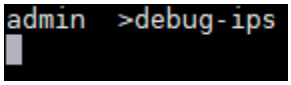
```
admin  >debug-ha
type=ha date=2018-03-17 11:54:49 Mar  1 11:54:49 master.blockbit.com blockbit-apply-cluster-master-notifyVI_2: conntrack primary
type=ha date=2018-03-17 11:54:50 Mar  1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: reconfigure macaddr: eth7 (00:90:28:01:2f:48)
type=ha date=2018-03-17 11:54:50 Mar  1 11:54:50 master.blockbit.com blockbit-apply-cluster-master-notifyVI_1: conntrack primary
```

Command Line Interface – debug-ha

UTM - [debug-ips]

Displays the Intrusion Prevention System debug logs in real time.

How to use:



Command Line Interface – debug-ips

Example:

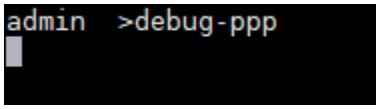
```
admin  >debug-ips
date="Fri Mar 13 15:28:25 2020" src="172.16.100.173" dst="74.119.119.145" proto="tcp" profile="Prevenção de Intrusão" devin="eth3" rule="
Controle e Proteção" devout="eth5" dport="443" sessionID="27826EBE361267F6D8B4290315DA0108" blocked="0" category="SCAN" log="true" geosrc
="" geodst="US" threat_impact="2" threat_class="Attempted Information Leak" threat_name="nmap TCP" service="https" login="wlima@blockbit.
com" threat_sid="2100628" sport="64015" threat_payload="450000293F3B4000400628CEAC1064AD4A777791FA0F01BB1CC0D23BE11C46B350102013AA6300000
0"
date="Fri Mar 13 15:28:29 2020" src="172.16.100.173" dst="208.185.50.80" proto="tcp" profile="Prevenção de Intrusão" devin="eth3" rule="C
ontrole e Proteção" devout="eth5" dport="443" sessionID="BACECF9A2D75D4D477374DEC8949DC04" blocked="0" category="SCAN" log="true" geosrc=
"" geodst="US" threat_impact="2" threat_class="Attempted Information Leak" threat_name="nmap TCP" service="https" login="wlima@blockbit.c
om" threat_sid="2100628" sport="64018" threat_payload="450000299B34400040068BD3AC1064ADD0B93250FA1201BBBC966540589D2BDE50102014D9D7000000
"
date="Fri Mar 13 15:31:29 2020" src="172.32.0.6" dst="99.84.30.170" proto="icmp" profile="Prevenção de Intrusão" devin="eth2" rule="Defau
lt (Allow)" devout="eth5" dport="443" sessionID="9B42A4E2C8A2220DF51956E7CFEB4197" blocked="0" category="ICMP_INFO" log="true" geosrc="US
" geodst="US" threat_impact="3" threat_class="Misc activity" threat_name="PING" service="443" login="-" threat_sid="2100384" sport="64018
" threat_payload="450000544B7440003F01C210AC20000663541EAA080018EF68390000AD88C94E0000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000"
date="Fri Mar 13 15:31:29 2020" src="172.32.0.6" dst="99.84.30.170" proto="icmp" profile="Prevenção de Intrusão" devin="eth2" rule="Defau
lt (Allow)" devout="eth5" dport="443" sessionID="9B42A4E2C8A2220DF51956E7CFEB4197" blocked="0" category="PROTOCOL-ICMP" log="true" geosrc
="US" geodst="US" threat_impact="2" threat_class="Information Leak" threat_name="Unusual PING detected" service="443" login="-" threat_si
d="29456" sport="64018" threat_payload="450000544B7440003F01C210AC20000663541EAA080018EF68390000AD88C94E0000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000"
date="Fri Mar 13 15:31:29 2020" src="172.32.0.6" dst="99.84.30.170" proto="icmp" profile="Prevenção de Intrusão" devin="eth2" rule="Defau
lt (Allow)" devout="eth5" dport="443" sessionID="9B42A4E2C8A2220DF51956E7CFEB4197" blocked="0" category="PROTOCOL-ICMP" log="true" geosrc
="US" geodst="US" threat_impact="3" threat_class="Misc activity" threat_name="PING" service="443" login="-" threat_sid="384" sport="64018
" threat_payload="450000544B7440003F01C210AC20000663541EAA080018EF68390000AD88C94E0000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000"
```

Command Line Interface – debug-ips- example

UTM - [debug-ppp]

Displays debug logs for interfaces using Point-to-Point Protocol in real time.

How to use:



Command Line Interface – debug-ppp

UTM - [debug-sdwan]

This command is used to display the debug logs of the SD-WAN service performed in the time stipulated in the option “Monitoring interval” in the panel for creating an SD-WAN profile (see chapter SD-WAN). There are two types of log available: Targets and Results and it is possible to raise a log based on a specific date.

Targets

Displays the debug log for all monitoring targets. Is composed of:

- ***date*****:** *The date and time the log was run*. The date is displayed in Year-Month-Day format. Ex.: 2019-02-12 10:02:09;
- ***profile*****:** The name of the SD-WAN profile from which this log was generated. Ex.: QA-Internet;
- ***dev*****:** The web interface from which this log was generated. Ex.: eth0;
- ***target*****:** The monitoring target that generated this log. Ex.: 8.8.8.8;
- ***port*****:** The output port used. Ex.: 80;
- ***protocol*****:** The protocol that was used. Ex.: tcp;
- ***latency*****:** The result of the Latency performance indicator. It is displayed in milliseconds. Ex.: 9.42;
- ***jitter*****:** The result of the Jitter performance indicator. It is displayed in milliseconds. Ex.: 7.54;
- ***packet_loss*****:** The result of the Packet Loss performance indicator. It is displayed in whole numbers. Ex.: 0;
- ***bandwidth*****:** The result of the Band Limit performance indicator. It is displayed in bytes per second. Ex.: 467711.73;
- ***connection_error*****:** Represents all connection errors. It is displayed in whole numbers. Ex.: 0;
- ***total_error*****:** Represents the number of times that a link availability test (using the values determined by the performance indicators) returned an error and also the connection errors. It is displayed in whole numbers. Ex.: 0.

Results

Displays the monitoring log according to the results of the performance indicator tests. Is composed of:

- ***date*****:** *The date and time the log was run*. The date is arranged in Year-Month-Day format. Ex.: 2019-02-10 10:25:07;
- ***profile*****:** The name of the SD-WAN profile from which this log was generated. Ex.: QA-Internet;
- ***dev*****:** The web interface from which this log was generated. Ex.: eth1;
- ***latency*****:** The result of the Latency performance indicator. It is displayed in milliseconds. Ex.: 12.835;
- ***jitter*****:** The result of the Jitter performance indicator. It is displayed in milliseconds. Ex.: 1.0275;
- ***packet_loss*****:** The result of the Packet Loss performance indicator. It is displayed in percentage. Ex.: 0;
- ***bandwidth*****:** The result of the Band Limit performance indicator. It is displayed in bytes. Ex.: 1818958.07;
- ***total_error*****:** Represents the number of times that a link availability test (using the values determined by the performance indicators) returned an error and also the connection errors. It is arranged in whole numbers. Ex.: 0;
- ***total_error_percent*****:** Represents the percentage of failure (Equivalent to the Fail Rate field of the visual interface). It is arranged in percentage. Ex.: 0;
- ***weight*****:** Weight of network consumption through the web interface. It is arranged in percentage. Ex.: 100.00;
- ***status*****:** *The status of this interface, whether it is on or off*. Ex.: *on*.

How to use:

```
admin  >debug-sdwan
Usage:  [OPTIONS] [TYPE] Pattern
  debug-sdwan [OPTION] -i [TYPE] targets Show debug logs for Targets
  debug-sdwan [OPTION] -i [TYPE] results Show debug logs for Results

Optional Arguments
  -i, --info      Log type (results, targets)
  -p, --profile   Set the profile name
  -s, --specific  Search for specific text on log
  -h, --help      Display this help message and exit

Examples:
  debug-sdwan -i targets
  debug-sdwan -i targets -p PROFILE_NAME -s "2019-02-20 19:47"
  debug-sdwan -i results -p PROFILE_NAME
  debug-sdwan -i results -p PROFILE_NAME -s "2019-02-20 19:47"

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

Command Line Interface – debug-sdwan

Example 1: Using the log type “targets” in a specific profile:

```
admin  >debug-sdwan -i targets -p FAILOVER
date="2019-02-11 15:30:57" profile="FAILOVER" dev="eth4" target="www.uol.com.br" port="443" protocol="tcp" latency="13.89" jitter="3.12"
packet_loss="0" bandwidth="13299.11" connection_error="0" total_error="0"
date="2019-02-11 15:30:59" profile="FAILOVER" dev="eth4" target="186.192.81.31" port="-" protocol="icmp" latency="6.59" jitter="3.05" pac
ket_loss="0" bandwidth="12260.23" connection_error="0" total_error="0"
date="2019-02-11 15:31:00" profile="FAILOVER" dev="eth2" target="g1.globo.com" port="80" protocol="tcp" latency="6.53" jitter="2.93" pack
et_loss="0" bandwidth="59150247.15" connection_error="0" total_error="0"
date="2019-02-11 15:31:00" profile="FAILOVER" dev="eth2" target="8.8.8.8" port="-" protocol="icmp" latency="50.70" jitter="0.76" packet_l
oss="0" bandwidth="59119868.60" connection_error="0" total_error="0"
date="2019-02-11 15:31:01" profile="FAILOVER" dev="eth4" target="g1.globo.com" port="80" protocol="tcp" latency="4.36" jitter="2.26" pack
et_loss="0" bandwidth="11740.65" connection_error="0" total_error="0"
admin  >
```

Command Line Interface – debug-sdwan -i targets

Example 2: Using the log type “results” in a specific profile:

```
admin  >debug-sdwan -i results -p FAILOVER
date="2019-02-11 15:40:52" profile="FAILOVER" dev="eth4" latency="19.7625" jitter="3.4925" packet_loss="0" bandwidth="17238.58" total_err
or="0" total_error_percent="0" weight="100.00" status="on"
date="2019-02-11 15:40:52" profile="FAILOVER" dev="eth2" latency="19.91" jitter="4.773125" packet_loss="0" bandwidth="1272036.29" total_e
rror="0" total_error_percent="0" weight="0" status="on"
date="2019-02-11 15:40:57" profile="FAILOVER" dev="eth4" latency="17.74" jitter="4.365" packet_loss="0" bandwidth="16119.98" total_error=
"0" total_error_percent="0" weight="100.00" status="on"
date="2019-02-11 15:40:58" profile="FAILOVER" dev="eth2" latency="21.375" jitter="3.54125" packet_loss="0" bandwidth="4827743.80" total_e
rror="0" total_error_percent="0" weight="0" status="on"
admin  >
```

Command Line Interface – debug-sdwan -i results

Example 3: Using the log type "targets" in a given profile within a specific date:

```
admin  >debug-sdwan -i targets -p FAILOVER "2019-02-20 20:00"
date="2019-02-22 11:48:41" profile="FAILOVER" dev="eth4" target="8.8.8.8" port="-" protocol="icmp" latency="54.63" jitter="0.14" packet_l
oss="0" bandwidth="139596.71" connection_error="0" total_error="0"
date="2019-02-22 11:48:42" profile="FAILOVER" dev="eth4" target="g1.globo.com" port="80" protocol="tcp" latency="9.57" jitter="1.33" pack
et_loss="0" bandwidth="107272.91" connection_error="0" total_error="0"
date="2019-02-22 11:48:44" profile="FAILOVER" dev="eth4" target="186.192.81.31" port="-" protocol="icmp" latency="8.02" jitter="0.40" pac
ket_loss="0" bandwidth="51387.60" connection_error="0" total_error="0"
date="2019-02-22 11:48:44" profile="FAILOVER" dev="eth2" target="186.192.81.31" port="-" protocol="icmp" latency="8.13" jitter="0.20" pac
ket_loss="0" bandwidth="400260.79" connection_error="0" total_error="0"
date="2019-02-22 11:48:44" profile="FAILOVER" dev="eth2" target="www.uol.com.br" port="443" protocol="tcp" latency="14.11" jitter="0.20"
packet_loss="0" bandwidth="397354.96" connection_error="0" total_error="0"
date="2019-02-22 11:48:45" profile="FAILOVER" dev="eth4" target="www.uol.com.br" port="443" protocol="tcp" latency="15.53" jitter="0.31"
packet_loss="0" bandwidth="64543.17" connection_error="0" total_error="0"
date="2019-02-22 11:48:45" profile="FAILOVER" dev="eth2" target="8.8.8.8" port="-" protocol="icmp" latency="50.74" jitter="0.14" packet_l
oss="0" bandwidth="424981.19" connection_error="0" total_error="0"
admin  >
```

Command Line Interface – debug-sdwan -s

UTM - [debug-smtp-proxy]

This command shows the *debug logs* of Proxy SMTP. It shows what was blocked by the Proxy SMTP service.

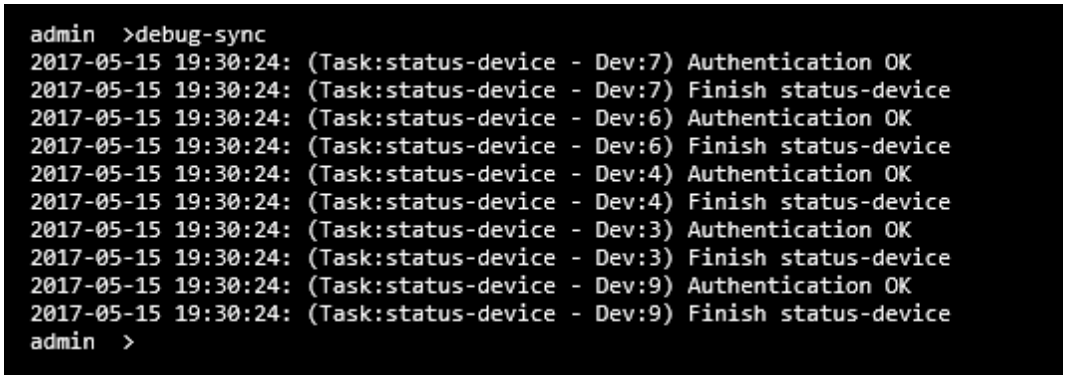
Usage example and command message.

```
admin  >debug-smtp-proxy
--------------------------------
 Debug SMTP proxy - Blockbit
--------------------------------
Debugging...


Feb  7 18:12:42 ngfw45-lab proxy-smtp[29066]: NEW (1/0) on=127.0.0.1:10026, src=127.0.0.1:58756, ident=, dst=127.0.0.1:10026, smtp, user=, id=1675804362.29066
Feb  7 18:14:12 ngfw45-lab proxy-smtp[1123]: NEW (1/0) on=127.0.0.1:10026, src=10.40.150.60:50879, ident=, dst=64.233.190.108:465, smtps, user=Unknown, id=1675804451.11
23
Feb  7 18:14:13 ngfw45-lab proxy-smtp[1123]: MAIL FROM <lab.socialtest@gmail.com>
Feb  7 18:14:13 ngfw45-lab atp: /var/spool/proxy-smtp/msg/1675804451.1123: Eicar-Test-Signature FOUND
Feb  7 18:17:13 ngfw45-lab proxy-smtp[15904]: NEW (1/0) on=127.0.0.1:10026, src=10.40.150.60:61362, ident=, dst=64.233.190.108:465, smtps, user=Unknown, id=1675804633.1
5904
Feb  7 18:17:15 ngfw45-lab proxy-smtp[15904]: MAIL FROM <lab.socialtest@gmail.com>
Feb  7 18:17:24 ngfw45-lab proxy-smtp[15904]: CLOSE by=server, rcv=2088825/637, trns=1, rcpts=1, auth=2, time=11, src=10.40.150.60, ident=, user=Unknown
Feb  7 18:18:13 ngfw45-lab proxy-smtp[18391]: NEW (1/0) on=127.0.0.1:10026, src=10.40.150.60:61372, ident=, dst=64.233.190.108:465, smtps, user=Unknown, id=1675804693.1
8391
Feb  7 18:18:15 ngfw45-lab proxy-smtp[18391]: MAIL FROM <lab.socialtest@gmail.com>
Feb  7 18:18:15 ngfw45-lab atp: /var/spool/proxy-smtp/msg/1675804693.18391: Eicar-Test-Signature FOUND
```

UTM - [debug-sync]

Used to monitor BLOCKBIT GSM communication with devices. Displays device updates and status.

How to use:



Command Line Interface – debug-sync

UTM - [debug-update]

Displays debug logs for updates generated by installing Hotfix packages.

How to use:

```
admin  >debug-update -a
2023/08/29 15:44:43 The file was successfully validated
2023/08/29 15:44:48 Running pre.sh bash script from hotfix ID: 20
2023/08/29 15:44:48
2023/08/29 15:44:49 Running post.sh bash script from hotfix ID: 20
2023/08/29 15:44:49
2023/08/29 15:44:49 Clean executed
2023/08/29 15:44:49 The package was successfully installed.
```

Command Line Interface – debug-update

UTM - [debug-vpn]

Displays debug logs for the IPSEC VPN service in real time. To use this command it is necessary to pass the argument -t and define which type of VPN will be debugged:

How to use:

```
admin  >debug-vpn -t ipsec
Aug 20 19:17:28.958 05[NET] <tun16|4389> received packet: from 172.31.240.241[500] to 172.31.208.40[500] (36 bytes)
Aug 20 19:17:28.958 05[ENC] <tun16|4389> parsed IKE_SA_INIT response 0 [ N(NO_PROP) ]
Aug 20 19:17:28.958 05[IKE] <tun16|4389> received NO_PROPOSAL_CHOSEN notify error
Aug 20 19:19:28.956 12[CFG] vici initiate 'tun16', me 172.31.208.40, other 172.31.240.241, limits 0
Aug 20 19:19:28.956 12[IKE] <tun16|4390> initiating IKE_SA tun16[4390] to 172.31.240.241
Aug 20 19:19:28.957 12[ENC] <tun16|4390> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(
REDIR_SUP) ]
Aug 20 19:19:28.957 12[NET] <tun16|4390> sending packet: from 172.31.208.40[500] to 172.31.240.241[500] (332 bytes)
Aug 20 19:19:28.960 15[NET] <tun16|4390> received packet: from 172.31.240.241[500] to 172.31.208.40[500] (36 bytes)
Aug 20 19:19:28.960 15[ENC] <tun16|4390> parsed IKE_SA_INIT response 0 [ N(NO_PROP) ]
Aug 20 19:19:28.960 15[IKE] <tun16|4390> received NO_PROPOSAL_CHOSEN notify error
```

Command Line Interface – debug-vpn -t ipsec

Example: If the service is not enabled and configured, the message below will be displayed:

```
admin  >debug-vpn
log not found
admin  >
```

Command Line Interface – debug-vpn – Log not found

UTM - [debug-webfilter]

Displays the debug logs of the Web Filter service in real time.

How to use:

```
admin  >debug-webfilter
date="Fri Mar 13 15:43:19 2020" src="172.16.100.173" dst="20.185.212.106" proto="tcp" web_protocol="HTTPS" devin="eth3" src_geo="" web_cu
stom_cat="-" devout="eth5" dport="443" dst_geo="US" sessionID="A9F557549786AE3CC7B412A36E8AE378" user="wlima@blockbit.com" mac="64:1c:67:
7d:49:d1" web_explicit="false" reason="appcontrol" service="https" web_cat_name_pt_br="Sistemas de troca instantânea de mensagens" up_byt
es="0" down_bytes="22" rule="Controle e Proteção" web_cat_name_en_us="Instant Messaging" zonein="LAN" web_method="POST" web_url="https://
azeus1-client-s.gateway.messenger.live.com/v1/users/ME/endpoints/%257B8dc65d35-ffff-ffff-dcb0-b1cde7fd763e%257D/subscriptions/6/poll?ackI
d=2989" web_referer="-" log="true" web_cat_id="18.3" web_agent="Mozilla/5.0%20(Windows%20NT%2010.0;%20WOW64)%20AppleWebKit/537.36%20(KHTM
L,%20like%20Gecko)%20Skype/8.57.0.116%20Chrome/78.0.3904.130%20Electron/7.1.8%20Safari/537.36" web_profile="QA - Security Ethics" web_mim
e="application/json" action="allow" sport="65031" zoneout=""
date="Fri Mar 13 15:43:19 2020" src="172.32.250.21" dst="20.185.212.106" proto="tcp" web_protocol="HTTPS" devin="eth2" src_geo="US" web_c
ustom_cat="-" devout="eth4" dport="443" dst_geo="US" sessionID="5FE01B6E39DC96FF9A3BCCDB573AE550" user="-" mac="" web_explicit="false" re
ason="appcontrol" service="https" web_cat_name_pt_br="Sistemas de troca instantânea de mensagens" up_bytes="0" down_bytes="22" rule="Cont
role e Proteção Wifi" web_cat_name_en_us="Instant Messaging" zonein="LAN" web_method="POST" web_url="https://azeus1-client-s.gateway.mess
enger.live.com/v1/users/ME/endpoints/%257Bd3727ec3-ffff-ffff-ff03-629623a5e360%257D/subscriptions/6/poll?ackId=2634" web_referer="-" log=
"true" web_cat_id="18.3" web_agent="Mozilla/5.0%20(Windows%20NT%2010.0;%20WOW64)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Skype/8
.57.0.116%20Chrome/78.0.3904.130%20Electron/7.1.8%20Safari/537.36" web_profile="QA - Security Ethics" web_mime="application/json" action=
"allow" sport="55414" zoneout=""
date="Fri Mar 13 15:43:20 2020" src="172.16.100.243" dst="20.185.212.106" proto="tcp" web_protocol="HTTPS" devin="eth3" src_geo="" web_cu
stom_cat="-" devout="eth5" dport="443" dst_geo="US" sessionID="64AA2C03EF9E398AF54C10BF519AB326" user="-" mac="84:7b:eb:e4:d8:c4" web_exp
licit="false" reason="appcontrol" service="https" web_cat_name_pt_br="Sistemas de troca instantânea de mensagens" up_bytes="0" down_bytes
="22" rule="Controle e Proteção" web_cat_name_en_us="Instant Messaging" zonein="LAN" web_method="POST" web_url="https://azeus1-client-s.g
ateway.messenger.live.com/v1/users/ME/endpoints/%257Bfde1d7ce-ffff-ffff-0fb9-00fd886aba2a%257D/subscriptions/6/poll?ackId=2051" web_refer
er="-" log="true" web_cat_id="18.3" web_agent="Mozilla/5.0%20(X11;%20Linux%20x86_64)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Sky
pe/8.56.0.103%20Chrome/78.0.3904.130%20Electron/7.1.6%20Safari/537.36" web_profile="QA - Security Ethics" web_mime="application/json" act
ion="allow" sport="44568" zoneout=""
```

Command Line Interface – debug-webfilter

To display the Web Filter's tuning options: "debug-webfilter -t":

```
admin  >debug-webfilter -h
Usage:  [OPTIONS] Pattern

Optional Arguments
  -s, --specific  Search for specific text on log
  -h, --help      Display this help message and exit
  -t, --tunning   Show webfilter tunning options messages

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

Command Line Interface - debug-webfilter -h

```
admin  >debug-webfilter -t
2023/04/03 17:45:41 kid4| WARNING: external ACL 'webfilter' queue overload. Request rejected '- acl_webfilter_access assets.msn.com - assets.msn.com:443 172.29.21.148 62062 assets.msn.com 443 74:
27:ea:78:93:fb - - - - 443 23.205.127.155 - CONNECT -'.
2023/04/03 17:46:11 kid4| WARNING: external ACL 'webfilter' queue overload. Request rejected '- acl_webfilter_access assets.msn.com - assets.msn.com:443 172.29.21.148 62062 assets.msn.com 443 74:
27:ea:78:93:fb - - - - 443 23.205.127.155 - CONNECT -'.
```

Command Line Interface - debug-webfilter -t

UTM - [dig]

Displays information about domains.

How to use:

```
admin  >dig -h
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
            {global-d-opt} host [@local-server] {local-d-opt}
            [ host [@local-server] {local-d-opt} [...]]
Where:  domain    is in the Domain Name System
        q-class   is one of (in,hs,ch,...) [default: in]
        q-type    is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
                  (Use ixfr=version for type ixfr)
        q-opt     is one of:
                  -x dot-notation     (shortcut for reverse lookups)
                  -i                  (use IP6.INT for IPv6 reverse lookups)
                  -f filename         (batch mode)
                  -b address[#port]   (bind to source address/port)
                  -p port             (specify port number)
                  -q name             (specify query name)
                  -t type             (specify query type)
                  -c class            (specify query class)
                  -u                  (display times in usec instead of msec)
                  -k keyfile          (specify tsig key file)
                  -y [hmac:]name:key  (specify named base64 tsig key)
                  -4                  (use IPv4 query transport only)
                  -6                  (use IPv6 query transport only)
                  -m                  (enable memory usage debugging)
        d-opt     is of the form +keyword[=value], where keyword is:
                  +[no]vc             (TCP mode)
                  +[no]tcp            (TCP mode, alternate syntax)
                  +time=###           (Set query timeout) [5]
                  +tries=###          (Set number of UDP attempts) [3]
                  +retry=###          (Set number of UDP retries) [2]
                  +domain=###         (Set default domainname)
                  +bufsize=###        (Set EDNS0 Max UDP packet size)
                  +ndots=###          (Set NDOTS value)
                  +subnet=addr        (Set edns-client-subnet option)
                  +[no]edns[=###]     (Set EDNS version) [0]
                  +[no]search         (Set whether to use searchlist)
                  +[no]showsearch     (Search with intermediate results)
                  +[no]defname        (Ditto)
                  +[no]recurse        (Recursive mode)
                  +[no]ignore         (Don't revert to TCP for TC responses.)
                  +[no]fail           (Don't try next server on SERVFAIL)
                  +[no]besteffort     (Try to parse even illegal messages)
```

Command Line Interface – dig

```
                +[no]aaonly         (Set AA flag in query (+[no]aaflag))
                +[no]adflag         (Set AD flag in query)
                +[no]cdflag         (Set CD flag in query)
                +[no]cl             (Control display of class in records)
                +[no]cmd            (Control display of command line)
                +[no]comments       (Control display of comment lines)
                +[no]rrcomments     (Control display of per-record comments)
                +[no]crypto         (Control display of cryptographic fields in records)
                +[no]question       (Control display of question)
                +[no]answer         (Control display of answer)
                +[no]authority      (Control display of authority)
                +[no]additional     (Control display of additional)
                +[no]stats          (Control display of statistics)
                +[no]short          (Disable everything except short
                                     form of answer)
                +[no]ttlid          (Control display of ttls in records)
                +[no]all            (Set or clear all display flags)
                +[no]qr             (Print question before sending)
                +[no]nssearch       (Search all authoritative nameservers)
                +[no]identify       (ID responders in short answers)
                +[no]trace          (Trace delegation down from root [+dnssec])
                +[no]dnssec         (Request DNSSEC records)
                +[no]expire         (Request time to expire)
                +[no]nsid           (Request Name Server ID)
                +[no]split=##       (Split hex/base64 fields into chunks)
                +[no]multiline      (Print records in an expanded format)
                +[no]onesoa         (AXFR prints only one soa record)
                +[no]keepopen       (Keep the TCP socket open between queries)
        global d-opts and servers (before host name) affect all queries.
        local d-opts and servers (after host name) affect only that lookup.
        -h                          (print help and exit)
        -v                          (print version and exit)
admin  >
```

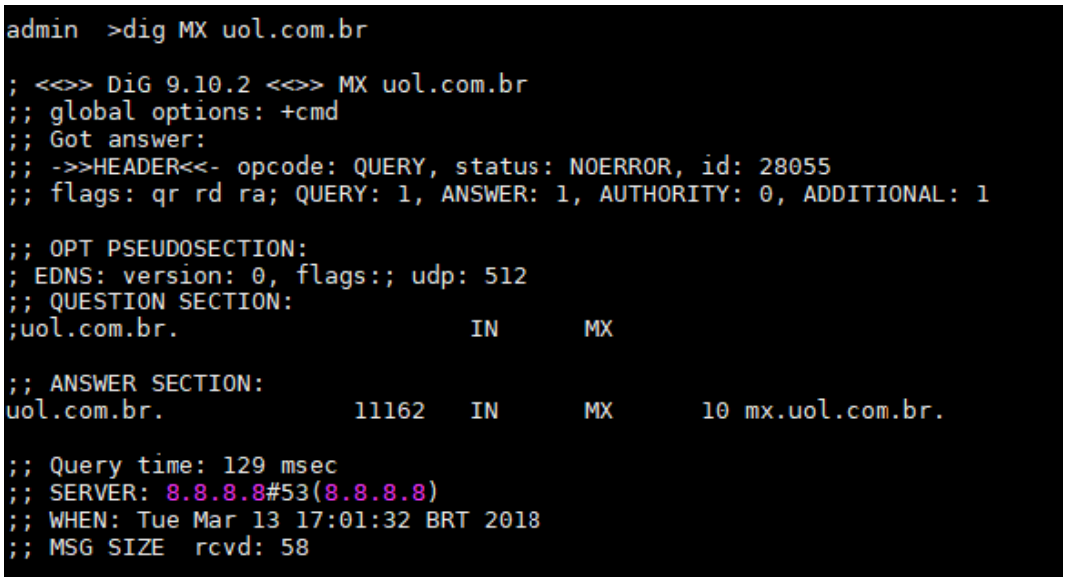
Command Line Interface – dig 2

Example: Checks the site type A note:

```
admin  >dig A www.uol.com.br

; <<>> DiG 9.10.2 <<>> A www.uol.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6375
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.uol.com.br.                        IN      A

;; ANSWER SECTION:
www.uol.com.br.         9       IN      CNAME   homeuol-ib.uol.com.br.
homeuol-ib.uol.com.br.  9       IN      A       200.221.2.45

;; Query time: 130 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Mar 13 17:01:04 BRT 2018
;; MSG SIZE  rcvd: 84
```

Command Line Interface – dig - example

Example 2: Checks MX (Mail Exchanger) notes for the domain:



Command Line Interface – dig – example 2

UTM - [disable-bgp]

Disables the BGP dynamic routing service.

How to use:

Command Line Interface – disable-bgp

Disables only the service, the settings will remain.

UTM - [disable-logsessions]

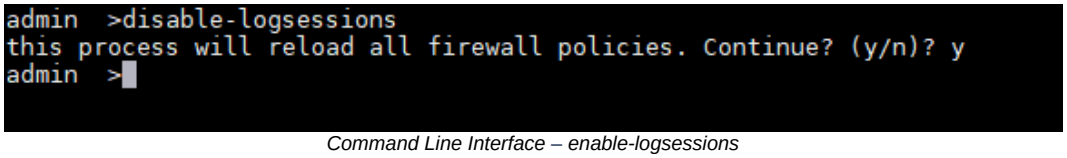
This command disables the sending of session information to the reporter service (report generator), effectively interrupting the logs and summary.

ATTENTION: When executing this command, all information in the graphical interface in: Dashboard, Live Sessions, Analyzer and Security Events, will be unavailable.

In addition, the **[debug-firewall]** and **[debug-webfilter]** commands will be disabled, since they depend on the logs to function normally.

To reactivate all these features, run the command **[enable-logsessions]**, for more information, see this page.

Command standard output:



Command Line Interface – enable-logsessions

Note that when executing the command, all firewall rules will need to be reloaded.

UTM - [disable-ospf]

Disables the OSPF dynamic routing service for both IPv4 and IPv6.

How to use:

Command Line Interface – disable-ospf

Disables only the service, the settings will remain.

UTM - [disable-pim]

Disables the PIM-SM dynamic routing service.

How to use:

Command Line Interface – disable-pim

Disables only the service, the settings will remain.

UTM - [disable-rip]

Disables the dynamic RIP routing service for both IPv4 and IPv6.

How to use:

Command Line Interface – disable-rip

Disables only the service, the settings will remain.

UTM - [disable-sip]

Disables the SIP protocol (VOIP Communication Protocol).

How to use:

Command Line Interface – disable-sip

Disables only the service, the settings will remain.

UTM - [disable-snmp]

Disables the SNMP service.

How to use:

```
admin  >disable-snmp
snmpd is disabled!
admin  >
```

Command Line Interface – disable-snmp

Disables only the service, the settings will remain.

UTM - [enable-bgp]

Enables the BGP dynamic routing service.

How to use:

Command Line Interface – enable-bgp

UTM - [enable-logsessions]

This command enables the sending of session information to the reporter service (report generator), effectively activating the logs and summarization if the command [disable-logsesions] has been previously executed and these services have been disabled.

If it is necessary to control system performance and reserve equipment resources for basic Firewall and Routing functionality without the need to generate reports, it is possible to execute the command **[disable-logsessions]**, for more information, see this page.

Command standard output:

```
admin  >enable-logsessions
this process will reload all firewall policies. Continue? (y/n)? y
admin  >
```

Command Line Interface – enable-logsessions

Note that when executing the command, all firewall rules will need to be reloaded.

UTM - [enable-ospf]

Enables the OSPF dynamic routing service for both IPv4 and IPv6.

How to use:

Command Line Interface – enable-ospf

UTM - [enable-pim]

Enables the PIM-SM dynamic routing service.

How to use:

Command Line Interface – enable-pim

UTM - [enable-rip]

Enables the dynamic RIP routing service for both IPv4 and IPv6.

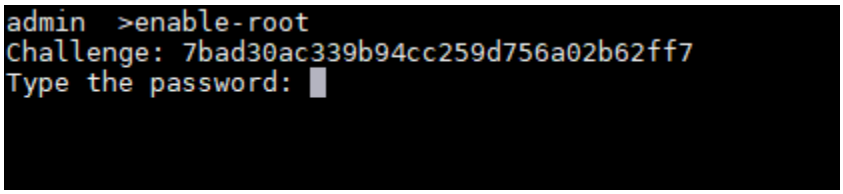
How to use:

Command Line Interface – enable-rip

UTM - [enable-root]

Enables root access to the system, it will be necessary to enter the password that will appear on the screen with the compatible password.

How to use:



Command Line Interface – enable-root

UTM - [enable-sip]

Activates the SIP protocol (VOIP Communication Protocol).

How to use:

Command Line Interface – enable-sip

UTM - [enable-snmp]

Enables and configures SNMP (SNMPv1, SNMPv2 or SNMPv3).

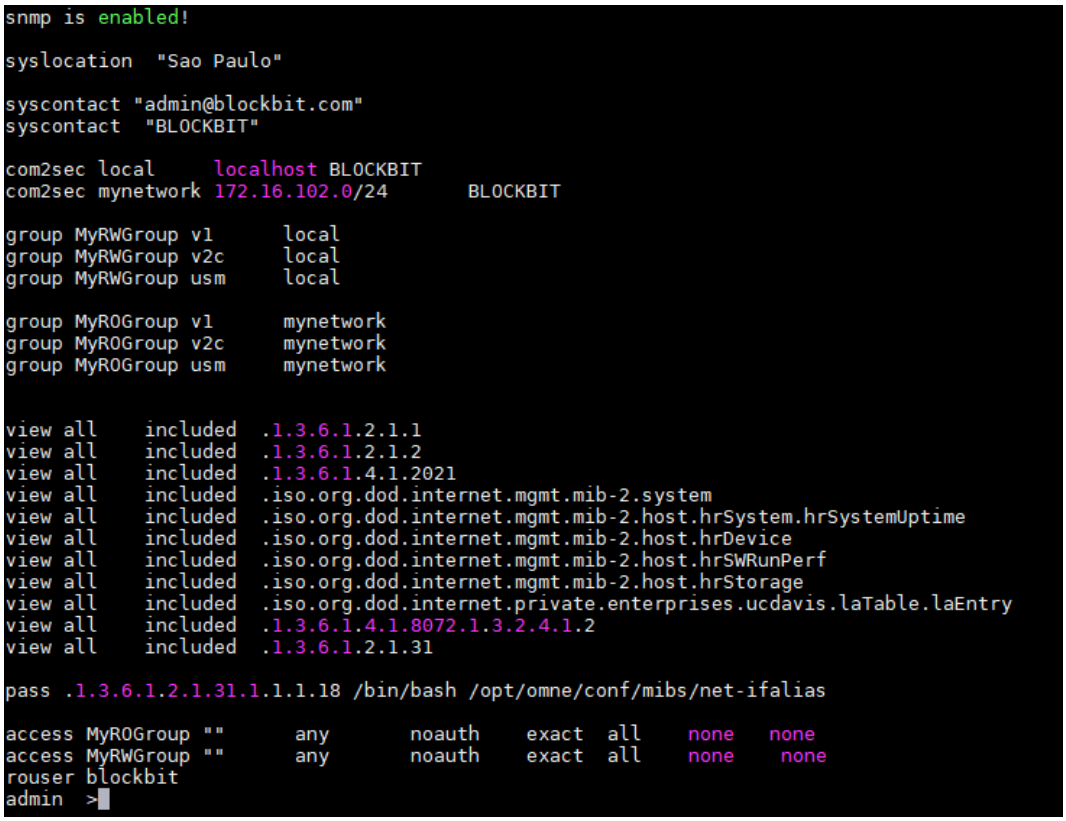
It is necessary to access **Services >> Firewall**, click on the option Edit of **Administration** (located inside the Services box) and activate the check box **[SNMP port]** for the command to work correctly.

How to use:

```
admin  >enable-snmp
Location: Sao Paulo
Organization: BLOCKBIT
E-mail: admin@blockbit.com
Enable SNMPv1 (Y/N)? Y
Enable SNMPv2 (Y/N)? Y
Community name: BLOCKBIT
Network Access (Leave blank to default 0.0.0.0/0): 172.16.102.0/24
Enable SNMPv3 (Y/N)? Y
Auth Protocol (MD5 or SHA): MD5
Username: blockbit
User password (minimum of 8 characters): password
Encryption Protocol (3DES or DES): 3DES
Encryption Password: password
Enable SNMPv1
Enable SNMPv2
Comunity: BLOCKBIT
Network Access: 172.16.102.0/24
Enable SNMPv3
Auth Protocol: MD5
Username: blockbit
Encryption Protocol: 3DES

Confirm (Y/N)? Y
```

Command Line Interface – enable-snmp

After confirming the above configuration, the following settings are displayed:



Command Line Interface – enable-snmp – Settings example

The information obtained through SNMP can be better viewed through Zabbix, for more information about this access this page. Note that if you want to use Zabbix, your community name cannot have spaces. Ex.: Community Name: Blockbit Community.

If you want to use a community name with spaces in Zabbix, you will need to name it in quotes. Eg: Community Name: "Blockbit Community"

UTM - [ethtool]

Used to present and detail information regarding network interfaces, check online and offline interfaces, change speed, change the way of negotiation and check which interface is physically located.

How to use:

```
admin  >ethtool -h
ethtool version 3.15
Usage:
        ethtool DEVNAME Display standard information about device
        ethtool -s|--change DEVNAME     Change generic options
                [ speed %d ]
                [ duplex half|full ]
                [ port tp|aui|bnc|mii|fibre ]
                [ mdix auto|on|off ]
                [ autoneg on|off ]
                [ advertise %x ]
                [ phyad %d ]
                [ xcvr internal|external ]
                [ wol p|u|m|b|a|g|s|d... ]
                [ sopass %x:%x:%x:%x:%x:%x ]
                [ msglvl %d | msglvl type on|off ... ]
```

Command Line Interface – ethtool

Example: Identify a specific network interface:

```
admin  >ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: Symmetric
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: Symmetric
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        MDI-X: off (auto)
        Supports Wake-on: pumbg
        Wake-on: g
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
Admin >
```

Command Line Interface – ethtool - Example

UTM - [exit]

Abandon the session.

How to use:

```
Modo de uso
admin  >exit
```

Command Line Interface – exit

UTM - [fdisk]

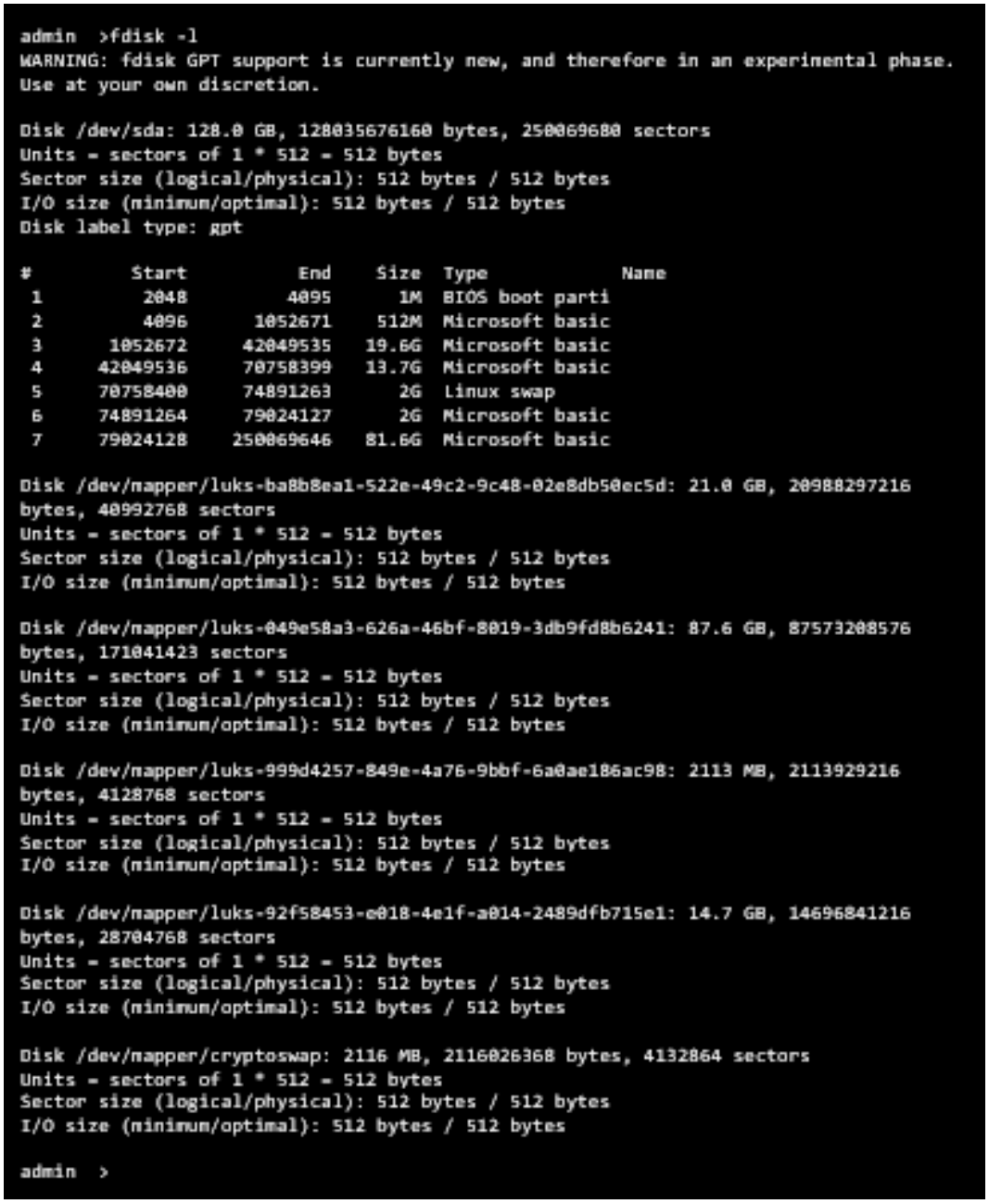
Used for managing hard disk partitions. It is possible to list and identify HDD-SSD type storage devices, create physical, logical partitions, delete, display information, etc.

How to use:

```
admin  >fdisk -h
Usage:
 fdisk [options] <disk>    change partition table
 fdisk [options] -l <disk> list partition table(s)
 fdisk -s <partition>      give partition size(s) in blocks
Options:
 -b <size>             sector size (512, 1024, 2048 or 4096)
 -c[=<mode>]           compatible mode: 'dos' or 'nondos' (default)
 -h                    print this help text
 -u[=<unit>]           display units: 'cylinders' or 'sectors' (default)
 -v                    print program version
 -C <number>           specify the number of cylinders
 -H <number>           specify the number of heads
 -S <number>           specify the number of sectors per track
admin  >
```

Command Line Interface – fdisk

Example: List the existing disks and partitions:



Command Line Interface – fdisk – Example

UTM - [free]

Displays the system's RAM usage status.

How to use:

```
admin  >free --h
free: option '--h' is ambiguous; possibilities: '--human' '--help'

Usage:
 free [options]

Options:
 -b, --bytes         show output in bytes
 -k, --kilo          show output in kilobytes
 -m, --mega          show output in megabytes
 -g, --giga          show output in gigabytes
     --tera          show output in terabytes
 -h, --human         show human-readable output
     --si            use powers of 1000 not 1024
 -l, --lohi          show detailed low and high memory statistics
 -t, --total         show total for RAM + swap
 -s N, --seconds N   repeat printing every N seconds
 -c N, --count N     repeat printing N times, then exit
 -w, --wide          wide output

     --help     display this help and exit
 -V, --version  output version information and exit

For more details see free(1).
admin  >
```

Command Line Interface – free

Example: Checking memory consumption:

```
admin  >free -m
               total        used        free      shared  buff/cache   available
Mem:            3952         172         186         216        3593        3324
Swap:           1995          80        1915
admin  >
```

Command Line Interface – free – Example

UTM - [fsck]

Used to check and correct errors on disks and file systems.

How to use:

```
admin  >fsck -h
/usr/sbin/fsck.ext4: invalid option -- 'h'
Usage: /usr/sbin/fsck.ext4 [-panyrcdfvtDFV] [-b superblock] [-B blocksize]
                [-I inode_buffer_blocks] [-P process_inode_size]
                [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
                [-E extended-options] device

Emergency help:
 -p                   Automatic repair (no questions)
 -n                   Make no changes to the filesystem
 -y                   Assume "yes" to all questions
 -c                   Check for bad blocks and add them to the badblock list
 -f                   Force checking even if filesystem is marked clean
 -v                   Be verbose
 -b superblock        Use alternative superblock
 -B blocksize         Force blocksize when looking for superblock
 -j external_journal  Set location of the external journal
 -l bad_blocks_file   Add to badblocks list
 -L bad_blocks_file   Set badblocks list
admin  >
```

Command Line Interface – fsck

Example: Check for possible errors on a given partition:

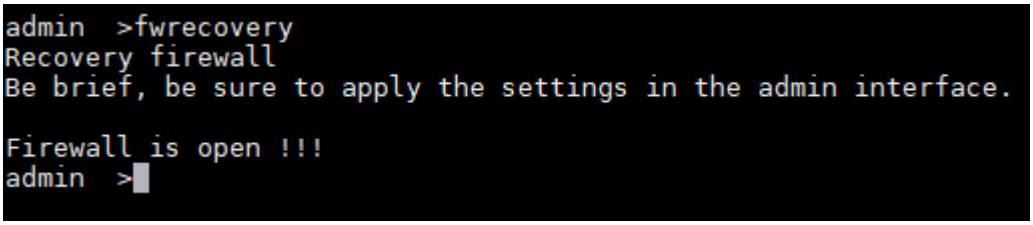
```
Admin  >fsck /dev/sda3
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/sda3: clean, 702/192000 files, 52661/768000 blocks
...
reloading firewall chains
reloading firewall zones
reloading firewall input
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
reloading firewall redirects
reloading firewall security rules
reloading firewall multilink rules
reloading firewall vpn rules
reloading firewall atp rules
admin >
```

Command Line Interface – fsck - Example

UTM - [fwrecovery]

Temporarily releases all Firewall input and routing.

How to use:



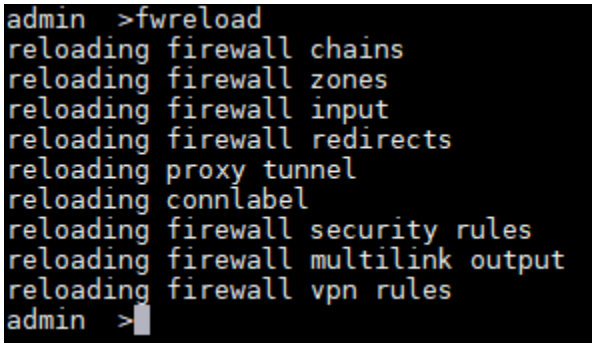
Command Line Interface – fwrecovery

ATTENTION: As soon as possible, access the WEB interface and click on “apply” (upper right corner) so that the temporary rules are removed.

UTM - [fwreload]

Reload the firewall.

How to use:



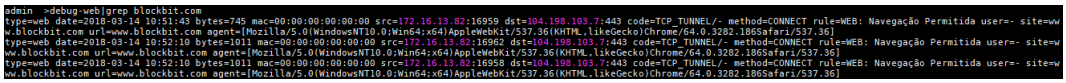
Command Line Interface – fwreload

ATTENTION: *When executing this command, a brief interruption in the accesses will occur.*

UTM - [grep]

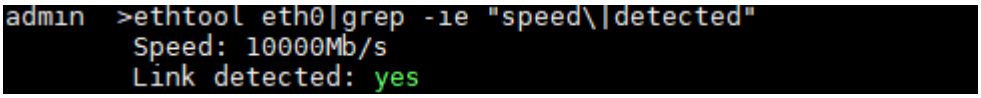
This command is intended to perform a search for the occurrence of regular expressions that match the pattern searched. It is used in conjunction with other commands to filter the output results.

Example: Filter debug-web output to view only requests destined for a specific URL:



Command Line Interface – grep - example

Example 2: Filter the output of the ethtool command using regex:

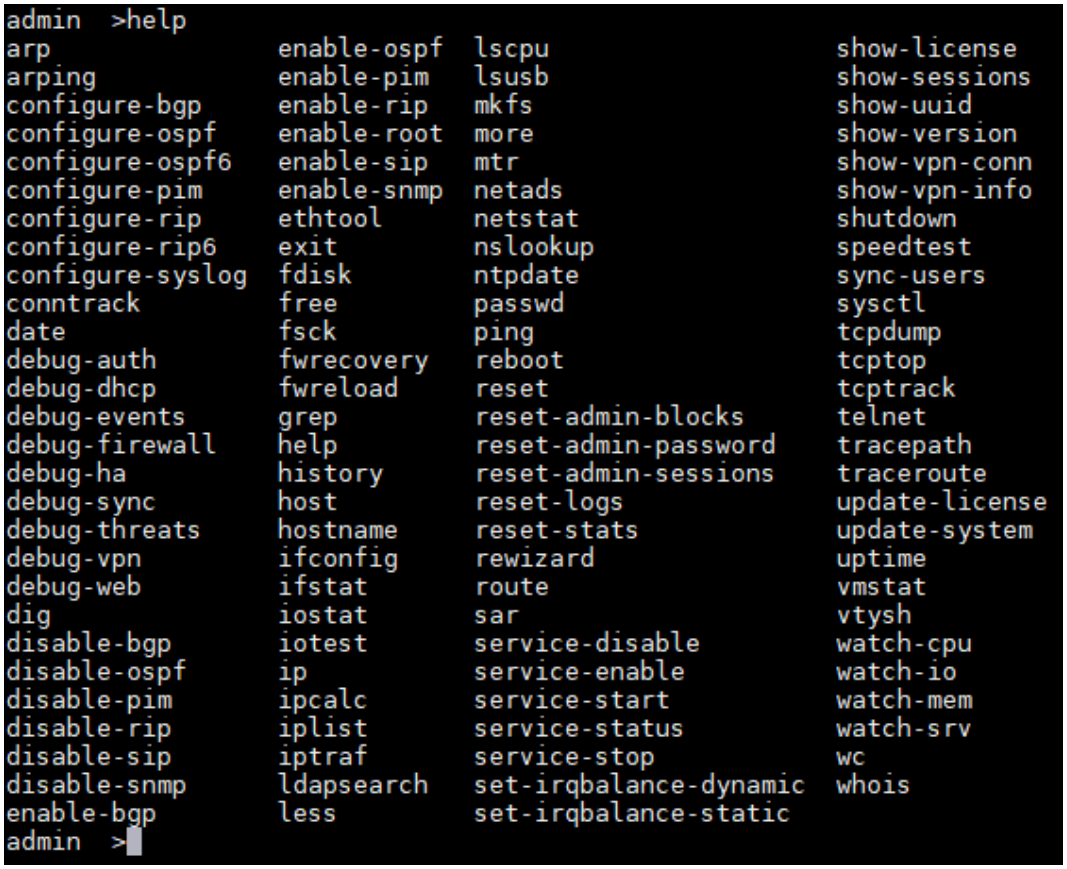


Command Line Interface – grep – example 2

UTM - [help]

Lists all commands available on the CLI interface.

How to use:

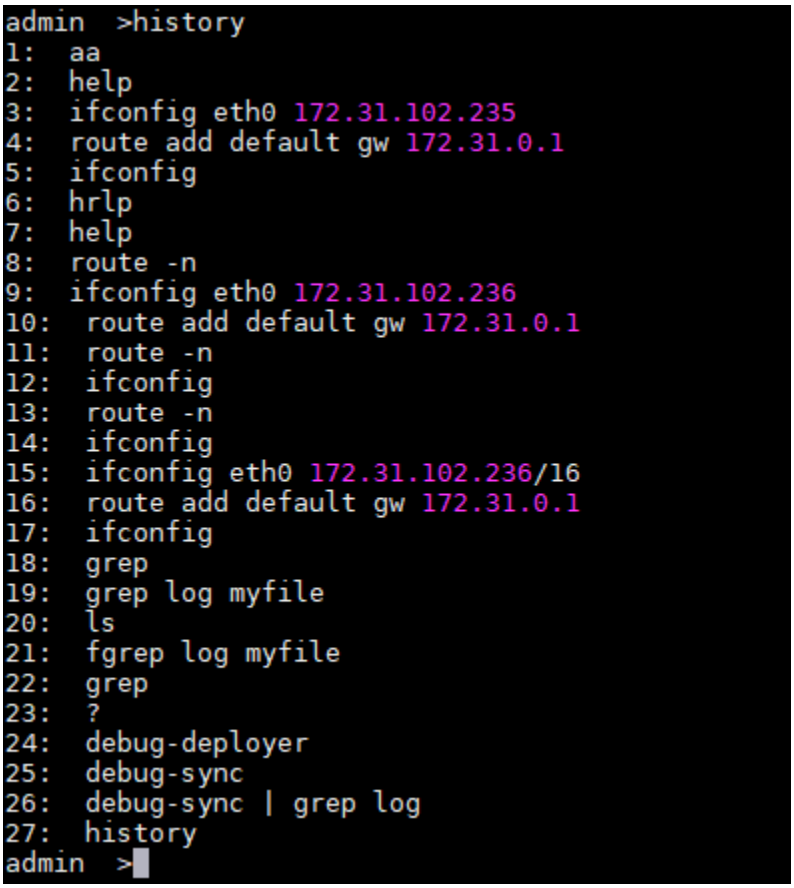


Command Line Interface – help

UTM - [history]

When using this command, a history of all the last used commands is displayed.

How to use:

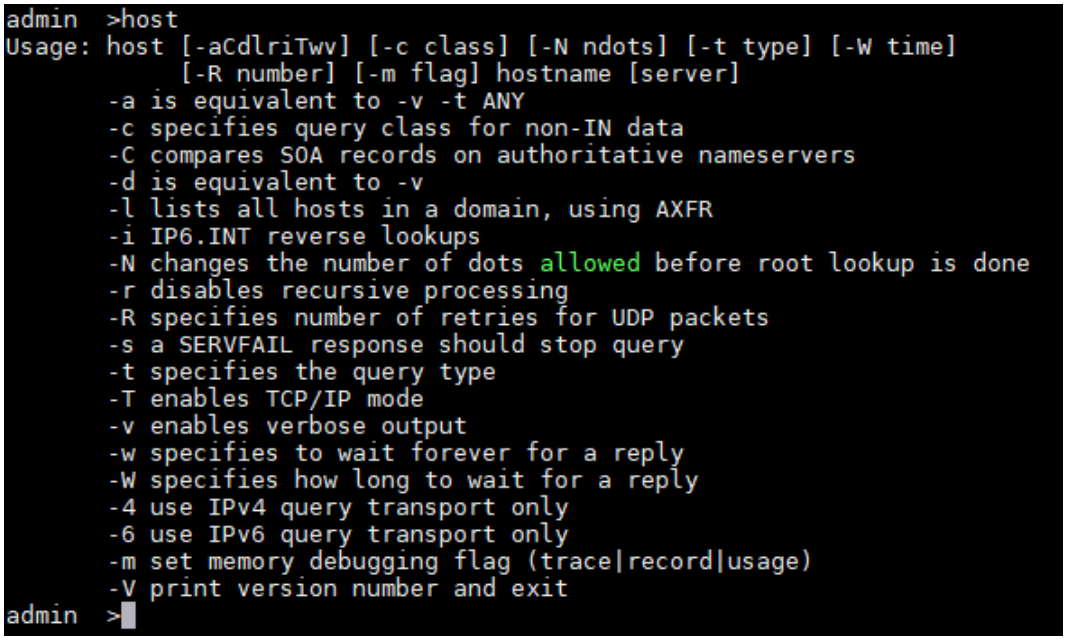


Command Line Interface – history

UTM - [host]

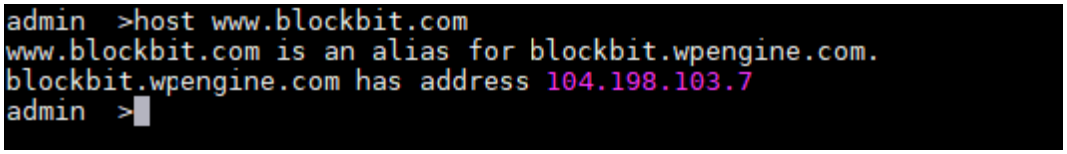
This command is used to perform DNS lookups, being able to convert names to IP addresses and vice versa.

How to use:



Command Line Interface – host

Example:



Command Line Interface – host - example

UTM - [hostname]

Displays or changes the host name of your BLOCKBIT UTM device.

How to use:

```
blockbit >hostname --help
Usage: hostname [-b] {hostname|-F file}         set host name (from file)
       hostname [-a|-A|-d|-f|-i|-I|-s|-y]       display formatted name
       hostname                                 display host name

       {yp,nis,}domainname {nisdomain|-F file}  set NIS domain name (from file)
       {yp,nis,}domainname                      display NIS domain name

       dnsdomainname                            display dns domain name

       hostname -V|--version|-h|--help          print info and exit

Program name:
       {yp,nis,}domainname=hostname -y
       dnsdomainname=hostname -d

Program options:
    -a, --alias            alias names
    -A, --all-fqdns        all long host names (FQDNs)
    -b, --boot             set default hostname if none available
    -d, --domain           DNS domain name
    -f, --fqdn, --long     long host name (FQDN)
    -F, --file             read host name or NIS domain name from given file
    -i, --ip-address       addresses for the host name
    -I, --all-ip-addresses all addresses for the host
    -s, --short            short host name
    -y, --yp, --nis        NIS/YP domain name

Description:
   This command can get or set the host name or the NIS domain name. You can
   also get the DNS domain or the FQDN (fully qualified domain name).
   Unless you are using bind or NIS for host lookups you can change the
   FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
   part of the FQDN) in the /etc/hosts file.
blockbit >
```

Command Line Interface – hostname

Example: Using the command to display the current name of your BLOCKBIT UTM device:

```
blockbit >hostname -f
vcm.blockbit.com
blockbit >
```

Command Line Interface – hostname - Example

UTM - [ifconfig]

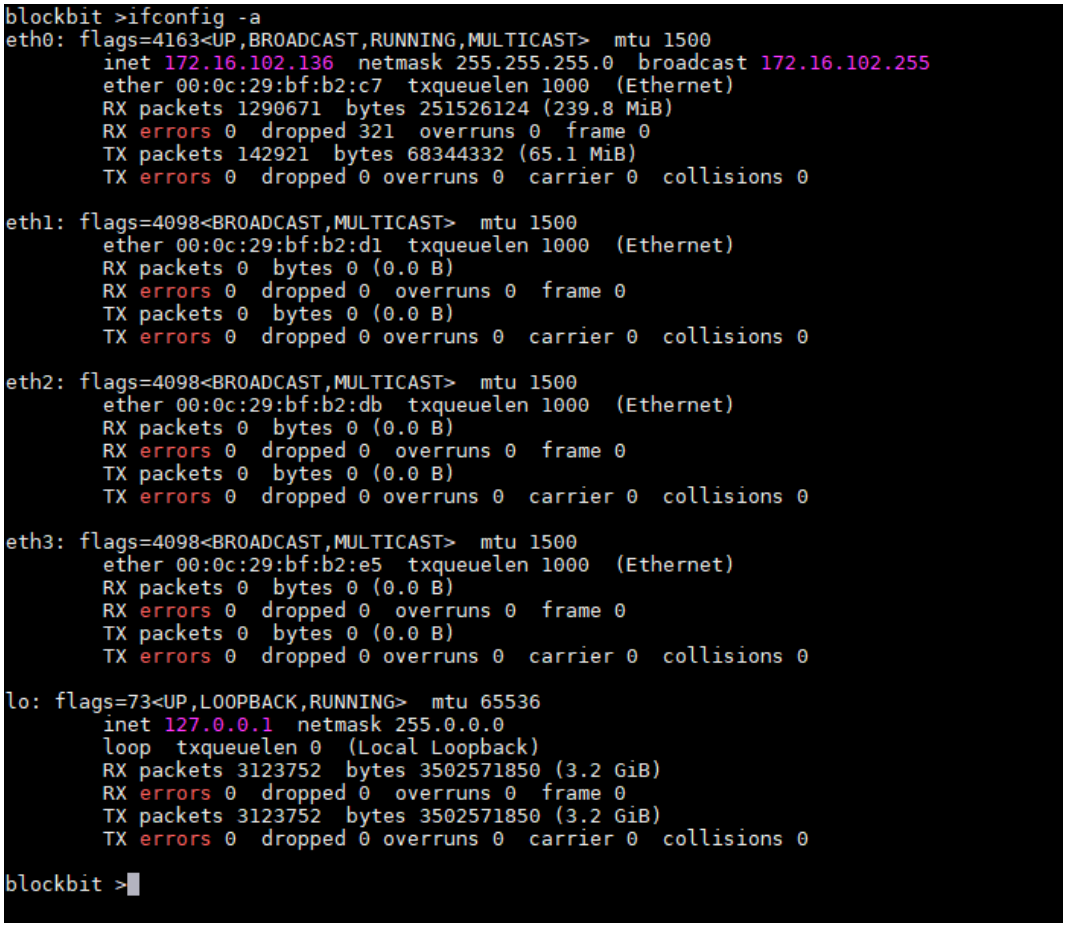
Configure and maintain the interface settings, you can enable, disable and list the status of each interface. It can also be used to optimize the system configuration.

How to use:

```
blockbit >ifconfig -h
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast [<address>]]  [[-]pointopoint [<address>]]
  [netmask <address>]  [dstaddr <address>]  [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>]  [mtu <NN>]
  [[-]trailers]  [[-]arp]  [[-]allmulti]
  [multicast]  [[-]promisc]
  [mem_start <NN>]  [io_addr <NN>]  [irq <NN>]  [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...

  <HW>=Hardware Type.
  List of possible hardware types:
    loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
    slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
    ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
    arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
    sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) ec (Econet) x25 (generic X.25)
    infiniband (InfiniBand) eui64 (Generic EUI-64)
  <AF>=Address family. Default: inet
  List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
blockbit >
```

Command Line Interface

Example: Displaying information about all network interfaces, both active and disabled:



Command Line Interface – ifconfig - Example

UTM - [ifstat]

Displays network traffic statistics.

How to use:

```
blockbit >ifstat -h
Usage: ifstat [OPTION] [ PATTERN [ PATTERN ] ]
   -h, --help           this message
   -a, --ignore ignore history
   -d, --scan=SECS      sample every statistics every SECS
   -e, --errors show errors
   -n, --nooutput       do history only
   -r, --reset          reset history
   -s, --noupdate       don;t update history
   -t, --interval=SECS  report average over the last SECS
   -V, --version        output version information
   -z, --zeros          show entries with zero activity
blockbit >
```

Command Line Interface – ifstat

Example: Listing the general traffic statistics report for all network interfaces:

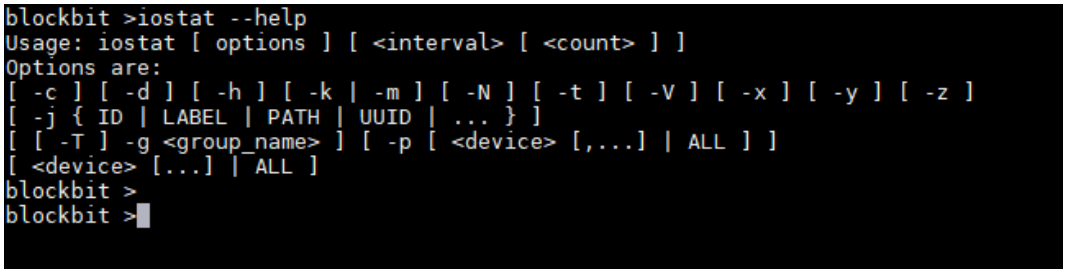
```
blockbit >ifstat
#kernel
Interface        RX Pkts/Rate    TX Pkts/Rate    RX Data/Rate    TX Data/Rate
                 RX Errs/Drop    TX Errs/Drop    RX Over/Rate    TX Coll/Rate
lo                 34054 0         34054 0        84632K 0        84632K 0
                       0 0             0 0             0 0             0 0
eth0               18848 0          3665 0         1700K 0         1466K 0
                       0 10            0 0             0 0             0 0
blockbit >
```

Command Line Interface – ifstat - Example

UTM - [iostat]

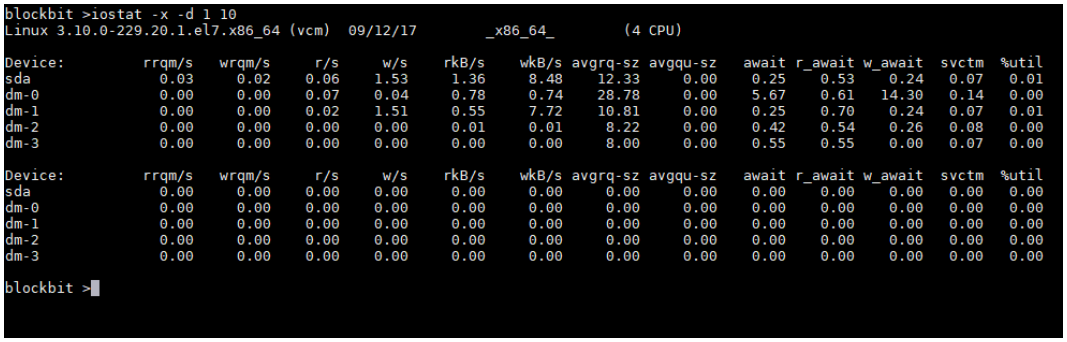
Monitors input and output (I / O) writing on the “file system” partition structure of the BLOCKBIT UTM disk.

How to use:



Command Line Interface – iostat

Example: Listing the (I / O) usage of BLOCKBIT UTM partitions.

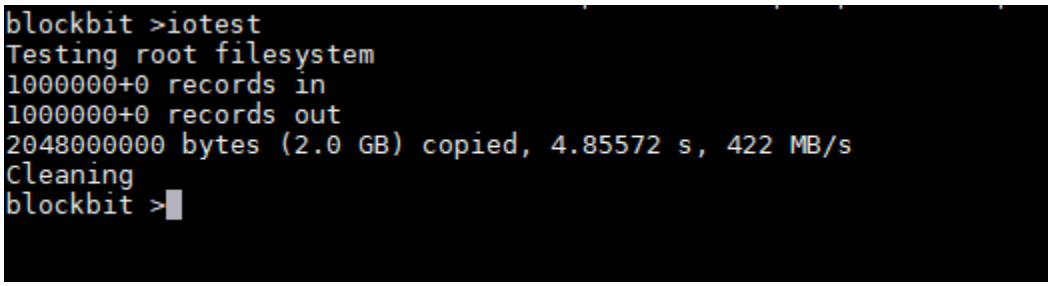


Command Line Interface – iostat - Example

UTM - [iotest]

Perform a write test for input and output (I / O) on the “file system” partition structure of the BLOCKBIT UTM disk.

How to use:



Command Line Interface – iotest

UTM - [ip]

Through this command it is possible to perform the display, manipulation and routing of devices, interfaces and network tunnels.

How to use:

```
admin  >ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | addr | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddr | mroute | mrule | monitor | xfrm |
                   netns | l2tp | tcp_metrics | token }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -f[amily] { inet | inet6 | ipx | dnet | bridge | link } |
                    -4 | -6 | -I | -D | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } |
                    -o[neline] | -t[imestamp] | -b[atch] [filename] |
                    -rc[vbuf] [size]}
admin  >
```

Command Line Interface – ip

UTM - [ipcalc]

Used for calculating IPv4 and IPv6 network / subnets. It has options to identify the prefix (mask), the network and broadcast address.

How to use:

```
admin  >ipcalc -h
ipcalc: ip address expected
Usage: ipcalc [OPTION...]
  -c, --check         Validate IP address for specified address family
  -4, --ipv4          IPv4 address family (default)
  -6, --ipv6          IPv6 address family
  -b, --broadcast     Display calculated broadcast address
  -h, --hostname      Show hostname determined via DNS
  -m, --netmask       Display default netmask for IP (class A, B, or C)
  -n, --network       Display network address
  -p, --prefix        Display network prefix
  -s, --silent        Don't ever display error messages

Help options:
  -?, --help          Show this help message
  --usage             Display brief usage message
admin  >
```

Command Line Interface – ipcalc

Example: Calcular uma *subnet*, seu endereço de rede e *broadcast*:

```
admin  >ipcalc -n -b -p 192.168.7.0/23
PREFIX=23
BROADCAST=192.168.7.255
NETWORK=192.168.6.0
admin  >
```

Command Line Interface – ipcalc – Example

UTM - [iplist]

Lists one or all network interfaces, zone, and physical connection status.

How to use:

```
admin  >iplist eth0
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 10000
    link/ether 00:0c:29:53:3d:16 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.78/24 brd 172.16.102.255 scope global eth0
       valid_lft forever preferred_lft forever
SIOCGMIIPHY on 'eth0' failed: Operation not supported
```

Command Line Interface – iplist

UTM - [iptraf]

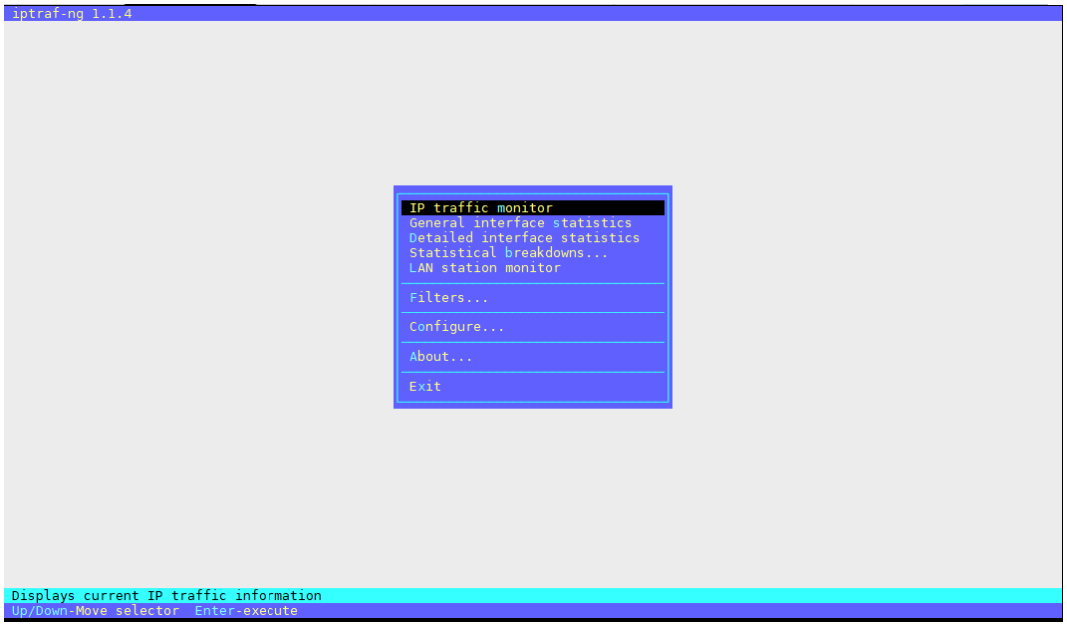
Network traffic monitor with GUI (Graphical User Interface).

How to use:

```
admin  >iptraf --help
usage: iptraf-ng [options]
   or: iptraf-ng [options] -B [-i <iface> | -d <iface> | -s <iface> | -z <iface> | -l <iface> | -g]

    -h, --help            show this help message

    -i <iface>            start the IP traffic monitor (use '-i all' for all interfaces)
    -d <iface>            start the detailed statistics facility on an interface
    -s <iface>            start the TCP and UDP monitor on an interface
    -z <iface>            shows the packet size counts on an interface
    -l <iface>            start the LAN station monitor (use '-l all' for all LAN interfaces)
    -g                    start the general interface statistics

    -B                    run in background (use only with one of the above parameters
    -f                    clear all locks and counters
    -t <n>                run only for the specified <n> number of minutes
    -L <logfile>          specifies an alternate log file
```

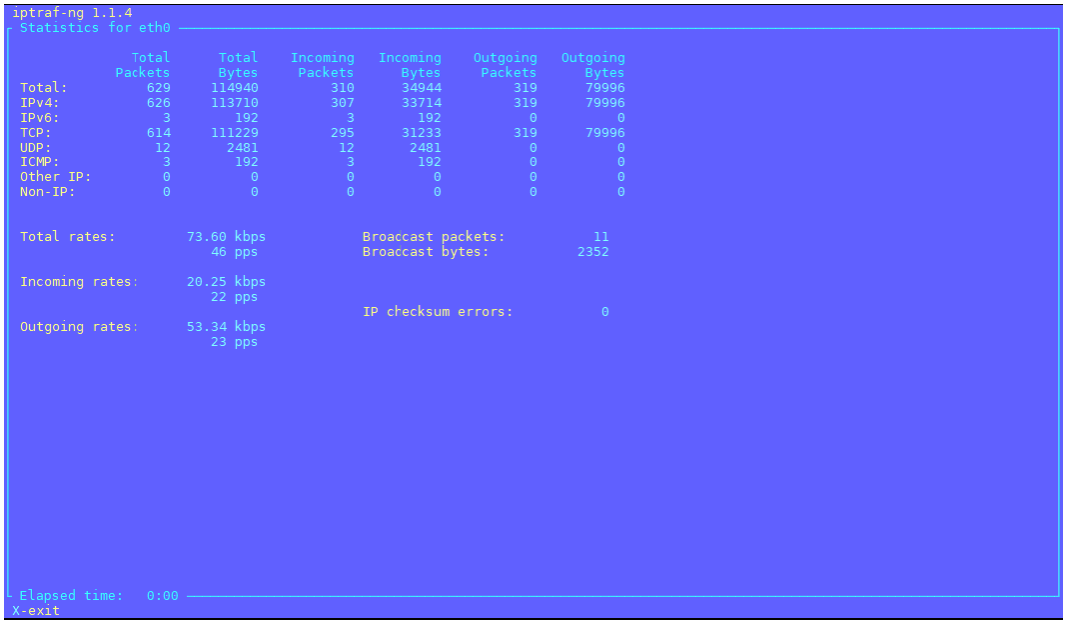
Command Line Interface – iptraf

Example: When you run the **iptraf** command, the interactive interface opens:



Command Line Interface – iptraf - Example

Example 2: iptraf -d eth0 - Detailed real-time statistics for the eth0 interface:



Command Line Interface – *iptraf* – Example 2

UTM - [ldapsearch]

LDAP based query tool.

How to use:

```
admin  >ldapsearch --help
ldapsearch: invalid option -- '-'
ldapsearch: unrecognized option --
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter        RFC 4515 compliant LDAP search filter
  attributes    whitespace-separated list of attribute descriptions
    which may include:
      1.1   no attributes
      *     all user attributes
      +     all operational attributes
Search options:
  -a deref   one of never (default), always, search, or find
  -A         retrieve attribute names only (no values)
  -b basedn  base dn for search
  -c         continuous operation mode (do not stop on errors)
  -E [!]<ext>[=<extparam>] search extensions (! indicates criticality)
             [!]domainScope              (domain scope)
             !dontUseCopy                (Don't Use Copy)
             [!]mv=<filter>              (RFC 3876 matched values filter)
             [!]pr=<size>[/prompt|noprompt] (RFC 2696 paged results/prompt)
             [!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...]
                                         (RFC 2891 server side sorting)
             [!]subentries[=true|false]  (RFC 3672 subentries)
             [!]sync=ro[/<cookie>]       (RFC 4533 LDAP Sync refreshOnly)
                     rp[/<cookie>][/<slimit>] (refreshAndPersist)
             [!]vlv=<before>/<after>(/<offset>/<count>|:<value>)
                                         (ldapv3-vlv-09 virtual list views)
             [!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]
             [!]<oid>[=:<b64value>] (generic control; no response handling)
  -f file    read operations from `file'
  -F prefix  URL prefix for files (default: file:///tmp/)
  -l limit   time limit (in seconds, or "none" or "max") for search
  -L         print responses in LDIFv1 format
  -LL        print responses in LDIF format without comments
  -LLL       print responses in LDIF format without comments
             and version
  -M         enable Manage DSA IT control (-MM to make critical)
  -P version protocol version (default: 3)
  -s scope   one of base, one, sub or children (search scope)
   S attr    sort the results by attribute `attr'
  -t         write binary values to files in temporary directory
  -tt        write all values to files in temporary directory
  -T path    write files to directory specified by path (default: /tmp)
  -u         include User Friendly entry names in the output
  -z limit   size limit (in entries, or "none" or "max") for search
```

Command Line Interface – ldapsearch

```
Common options:
  -d level   set LDAP debugging level to `level'
  -D binddn  bind DN
  -e [!]<ext>[=<extparam>] general extensions (! indicates criticality)
             [!]assert=<filte>     (RFC 4528; a RFC 4515 Filter string)
             [!]authzid=<authzid>   (RFC 4370; "dn:<dn>" or "u:<user>")
             [!]chaining[=<resolveBehavior>[/<continuationBehavior>]]
                    one of "chainingPreferred", "chainingRequired",
                    "referralsPreferred", "referralsRequired"
             [!]manageDSAit         (RFC 3296)
             [!]noop
             ppolicy
             [!]postread[=<attrs>]  (RFC 4527; comma-separated attr list)
             [!]preread[=<attrs>]   (RFC 4527; comma-separated attr list)
             [!]relax
             [!]sessiontracking
             abandon, cancel, ignore (SIGINT sends abandon/cancel,
             or ignores response; if critical, doesn't wait for SIGINT.
             not really controls)
  -h host    LDAP server
  -H URI     LDAP Uniform Resource Identifier(s)
  -I         use SASL Interactive mode
  -n         show what would be done but don't actually do it
  -N         do not use reverse DNS to canonicalize SASL host name
  -O props   SASL security properties
  -o <opt>[=<optparam>] general options
             nettimeout=<timeout> (in seconds, or "none" or "max")
             ldif-wrap=<width> (in columns, or "no" for no wrapping)
  -p port    port on LDAP server
  -Q         use SASL Quiet mode
  -R realm   SASL realm
  -U authcid SASL authentication identity
  -v         run in verbose mode (diagnostics to standard output)
  -V         print version info (-VV only)
  -w passwd  bind password (for simple authentication)
  -W         prompt for bind password
  -x         Simple authentication
  -X authzid SASL authorization identity ("dn:<dn>" or "u:<user>")
  -y file    Read password from file
  -Y mech    SASL mechanism
  -Z         Start TLS request (-ZZ to require successful response)
```

Command Line Interface – ldapsearch 2

Example: List the attributes of the OU and its members:

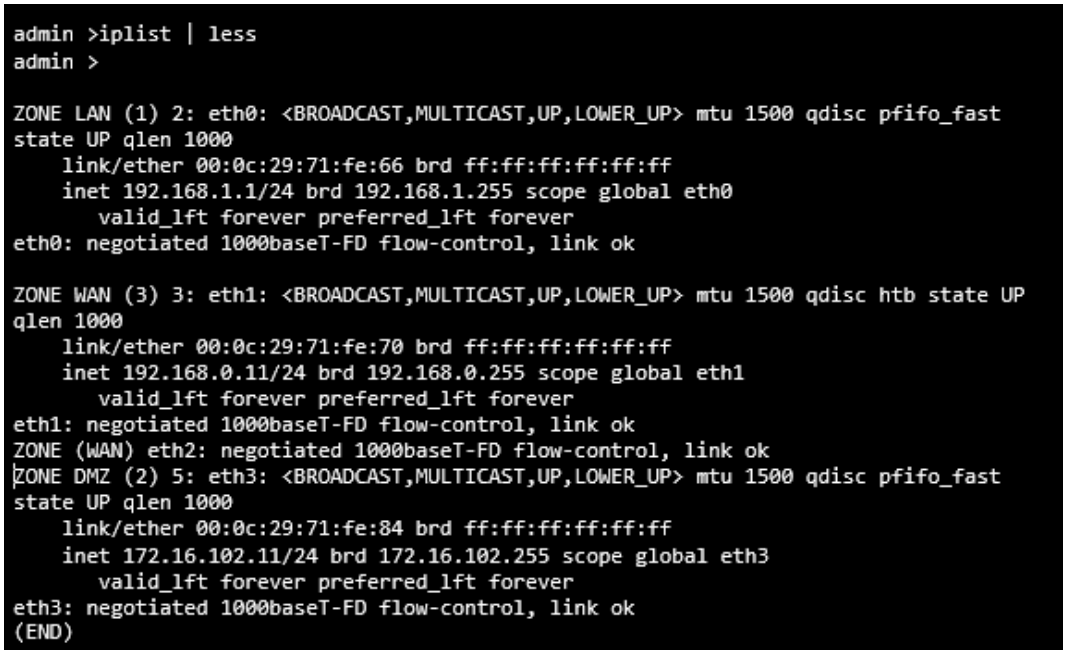
```
admin  >ldapsearch -z0 -x -b "OU=suporte,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br" -D "administrador@labsuporte.com.br" -h 172.16.102.161 -p 389 -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <OU=suporte,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# SUPORTE, BLOCKBIT, labsuporte.com.br
dn: OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
objectClass: top
objectClass: organizationalUnit
ou: SUPORTE
distinguishedName: OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
instanceType: 4
whenCreated: 20180314161706.0Z
whenChanged: 20180314161707.0Z
uSNCreated: 23679
uSNChanged: 23680
name: SUPORTE
objectGUID:: EaEgpi7FMUqKQD5rSSOktg==
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=labsuport
 e,DC=com,DC=br
dSCorePropagationData: 20180314161707.0Z
dSCorePropagationData: 20180314161707.0Z
dSCorePropagationData: 16010101000000.0Z

# charlie, SUPORTE, BLOCKBIT, labsuporte.com.br
dn: CN=charlie,OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=br
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: charlie
givenName: Charlie
distinguishedName: CN=charlie,OU=SUPORTE,OU=BLOCKBIT,DC=labsuporte,DC=com,DC=b
 r
instanceType: 4
whenCreated: 20171214114002.0Z
whenChanged: 20180314161856.0Z
displayName: Charlie
uSNCreated: 2265501
memberOf: CN=Marketing,OU=Usuarios,OU=Suporte,DC=labsuporte,DC=com,DC=br
uSNChanged: 23683
wWWHomePage: www.blockbit.com
name: charlie
```

Command Line Interface – ldapsearch - example

UTM - [less]

Used to paginate files or standard input. It is possible to direct the output of another command using the pipe "|".

How to use: Use the less command as output from another command that returns a very extensive amount of information.

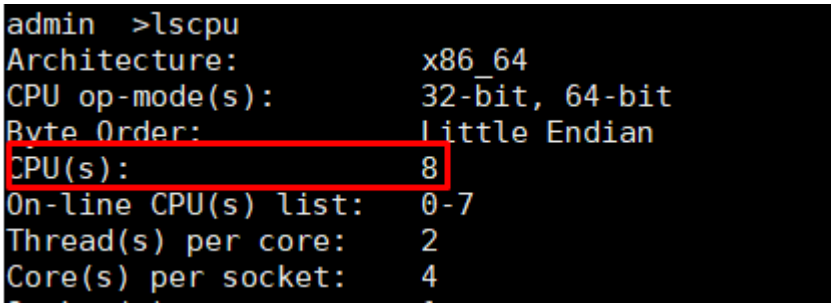


Command Line Interface – less

UTM - [lscpu]

Displays the specifications of the machine in use, alongside the number of CPUs.

How to use:



Command Line Interface – lscpu

UTM - [lsusb]

Displays information about the USB ports and the devices connected to them.

How to use:

```
admin  >lsusb --help
Usage: lsusb [options]...
List USB devices
  -v, --verbose
      Increase verbosity (show descriptors)
  -s [[bus]:][devnum]
      Show only devices with specified device and/or
      bus numbers (in decimal)
  -d vendor:[product]
      Show only devices with the specified vendor and
      product ID numbers (in hexadecimal)
  -D device
      Selects which device lsusb will examine
  -t, --tree
      Dump the physical USB device hierarchy as a tree
  -V, --version
      Show version of program
  -h, --help
      Show usage and help
```

Command Line Interface – lsusb

Example:

```
admin  >lsusb
Bus 001 Device 002: ID 8087:07e6 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 058f:6387 Alcor Micro Corp. Flash Drive
```

Command Line Interface – lsusb - example

UTM - [migrate-logsessions]

This command has the function of migrating the logs from the old Firewall structure to the new version. This command is performed in the background and its progress can be checked through the "status" attribute.

The migration service checks each batch of data if there is enough disk space, if a lack of space is detected, the migration is interrupted.

```
apply-migrate-log: no action, please set(start, stop, status or delete)
admin  >
```

CLI - migrate-logsessions

How to use:

- **start:** This attribute starts the log migration process;

```
admin  >migrate-logsessions start
admin  >migrate-logsessions status
2021-02-27 success 100.0%
2021-02-28 running 0.0%
2021-03-01 pending 0%
2021-03-02 pending 0%
2021-03-03 pending 0%
2021-03-04 pending 0%
2021-03-05 pending 0%
admin  >
```

CLI - migrate-logsessions start

- **stop:** Serves to interrupt the migration process;

If you have already run the command "migrate-logsessions start" and you need to shut down or restart the server, it is recommended to run "migrate-logsessions stop" to prevent data from being compromised.

```
admin  >migrate-logsessions stop
admin  >migrate-logsessions status
2021-02-27 stopped 0%
2021-02-28 pending 0%
2021-03-01 pending 0%
2021-03-02 pending 0%
2021-03-03 pending 0%
2021-03-04 pending 0%
2021-03-05 pending 0%
admin  >
```

CLI - migrate-logsessions stop

- **delete:** This command deletes entries in the database of old logs, it is possible to delete by date or delete all records.

```
admin  >migrate-logsessions delete
apply-migrate-logdelete: invalid delete action value:, please set(all or YYYY-MM-DD)
admin  >migrate-logsessions delete all
admin  >
```

CLI - migrate-logsessions delete

Below is an example of removing all records:

```
admin  >migrate-logsessions delete all
Delete all from old database, confirm (Y/N)? y
drop day 2021-02-27
drop day 2021-02-28
drop day 2021-03-01
drop day 2021-03-02
drop day 2021-03-03
drop day 2021-03-04
drop day 2021-03-05
admin  >
```

CLI - migrate-logsessions delete all

- **status:** This attribute displays the current status of the migration, it is possible to track the progress when using it:

```
admin  >migrate-logsessions status
2021-02-27 deleted 15.8%
2021-02-28 deleted 15.8%
2021-03-01 deleted 15.8%
2021-03-02 deleted 15.8%
2021-03-03 deleted 15.8%
2021-03-04 deleted 15.8%
2021-03-05 deleted 15.8%
admin  >
```

CLI - migrate-logsessions status

UTM - [mkfs]

Used to perform a format. It will be necessary to determine the device to be formatted. Eg: mkfs -t ext4 / dev / sdb;

How to use:

```
admin  >mkfs
Usage: mkfs.ext4 [-c|-l filename] [-b block-size] [-C cluster-size]
        [-i bytes-per-inode] [-I inode-size] [-J journal-options]
        [-G flex-group-size] [-N number-of-inodes]
        [-m reserved-blocks-percentage] [-o creator-os]
        [-g blocks-per-group] [-L volume-label] [-M last-mounted-directory]
        [-O feature[,...]] [-r fs-revision] [-E extended-option[,...]]
        [-t fs-type] [-T usage-type ] [-U UUID] [-jnqvDFKSV] device [blocks-count]
admin  >
```

Command Line Interface – mkfs

UTM - [more]

Used to paginate files or standard input. It is possible to direct the output of another command using the pipe "|".

How to use: Use the more command as output from another command that returns a very extensive amount of information.

```
admin  >iplist | more
ZONE LAN (1) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.16.20.1/24 brd 172.16.20.255 scope global eth3
       valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 8: eth0.102@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.1/24 brd 172.16.102.255 scope global eth0.102
       valid_lft forever preferred_lft forever
eth0.102: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 7: eth0.101@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.1/24 brd 172.16.101.255 scope global eth0.101
       valid_lft forever preferred_lft forever
eth0.101: negotiated 1000baseT-FD flow-control, link ok
ZONE LAN (1)
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.12.1/23 brd 172.16.13.255 scope global eth0
       valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok
[--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns]
                [--show-ips] [--address interface] [--filename=FILE|-F]
                [--ipinfo=item_no|-y item_no] [--aslookup|-z]
                [--psize=bytes/-s bytes] [--order fields]
                [--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-
ttl=NUM]
                [--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--
timeout=SECONDS]
                [--interval=SECONDS] HOSTNAME
admin  >
```

Command Line Interface – more

Example: Routing test for a specific destination.

UTM - [mtr]

Diagnostic tool that combines ping and traceroute tests to identify packet loss and high latency.

How to use:

```
admin  >mtr --help
usage: /usr/sbin/mtr [-BfhvrwctglxspQomniuT46] [--help] [--version] [--report]
               [--report-wide] [--report-cycles=COUNT] [--curses] [--gtk]
               [--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns] [--show-ips]
               [--address interface] [--filename=FILE|-F]
               [--ipinfo=item_no|-y item_no]
               [--aslookup|-z]
               [--psize=bytes/-s bytes] [--order fields]
               [--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-ttl=NUM]
               [--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--timeout=SECONDS]
               [--interval=SECONDS] HOSTNAME
```

Command Line Interface – mtr

UTM - [netads]

Displays and manages LDAP server information.

How to use:

```
admin  >netads --help
Usage:
net ads info
    Display details on remote ADS server
net ads join
    Join the local machine to ADS realm
net ads testjoin
    Validate machine account
net ads leave
    Remove the local machine from ADS
net ads status
    Display machine account details
net ads user
    List/modify users
net ads group
    List/modify groups
net ads dns
    Issue dynamic DNS update
net ads password
    Change user passwords
net ads changetrustpw
    Change trust account password
net ads printer
    List/modify printer entries
net ads search
    Issue LDAP search using filter
net ads dn
    Issue LDAP search by DN
net ads sid
    Issue LDAP search by SID
net ads workgroup
    Display the workgroup name
net ads lookup
    Find the ADS DC using CLDAP lookups
net ads keytab
    Manage local keytab file
net ads gpo
    Manage group policy objects
net ads kerberos
    Manage kerberos keytab
net ads enctypes
    List/modify enctypes
```

Command Line Interface – netads

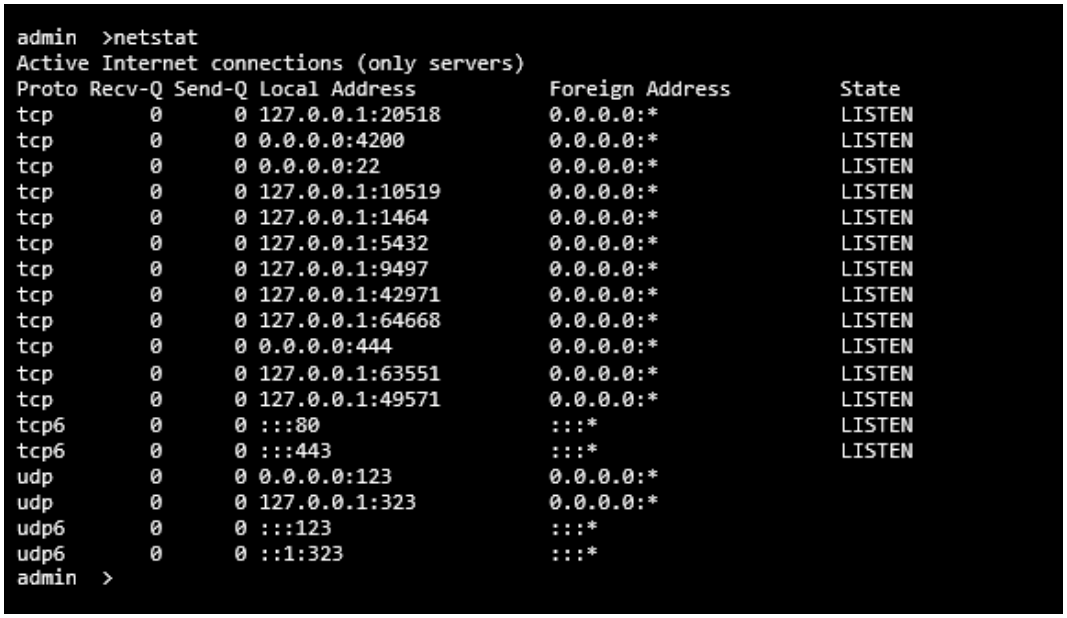
Example: View LDAP server information:

```
admin  >netads info
LDAP server: 172.16.102.161
LDAP server name: WIN-KUJ3AT9LI1Q.labsuporte.com.br
Realm: LABSUPORTE.COM.BR
Bind Path: dc=LABSUPORTE,dc=COM,dc=BR
LDAP port: 389
Server time: Wed, 14 Mar 2018 14:12:13 BRT
KDC server: 172.16.102.161
Server time offset: 35
```

UTM - [netstat]

Used to display the listening ports on the server.

How to use:

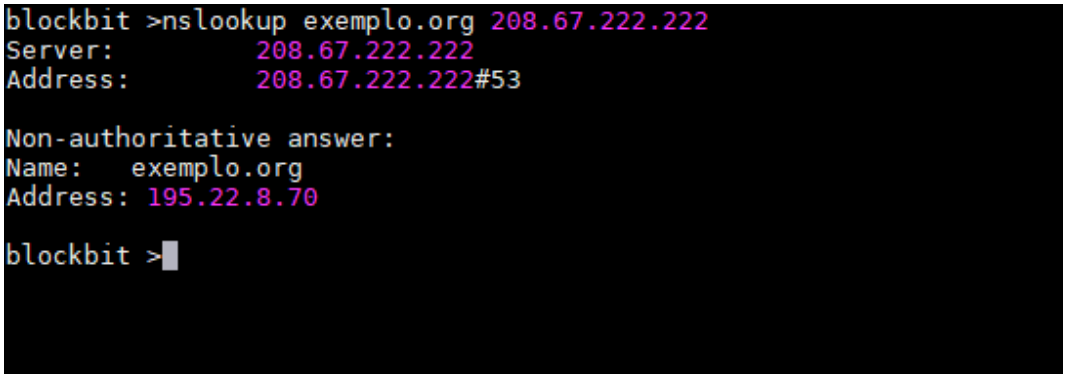


Command Line Interface – netstat

UTM - [nslookup]

Sends DNS lookups to a remote DNS server.

How to use:

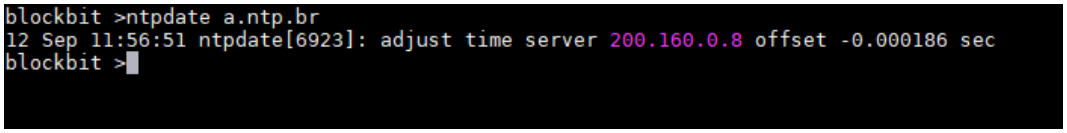


Command Line Interface – nslookup

UTM - [ntpdate]

Adjusts your device's local date and time by querying NTP (Network Time Protocol) servers available on the network.

How to use:

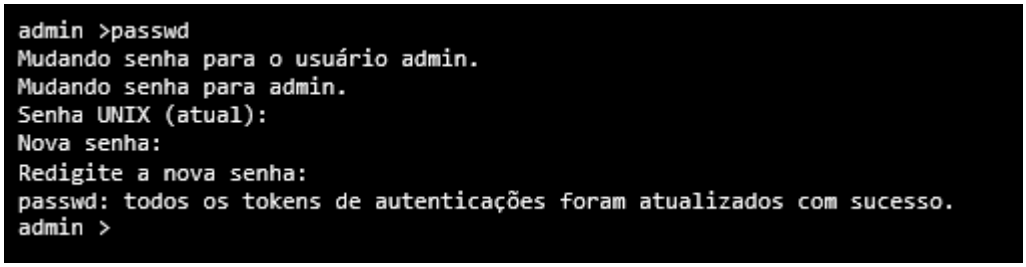


Command Line Interface – ntpdate

UTM - [passwd]

Used to set or change the password of the default “admin” user of the console.

How to use:

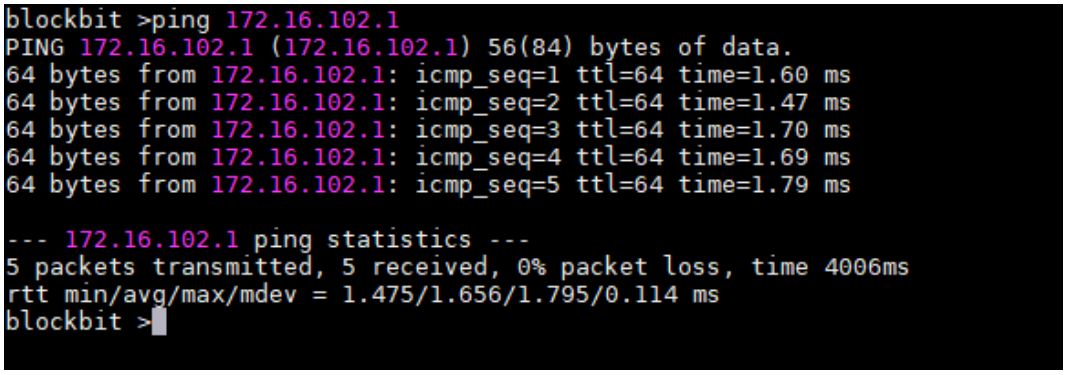


Command Line Interface – passwd

UTM - [ping]

Tests connectivity between devices on the network. Uses the ICMP protocol datagram.

How to use:

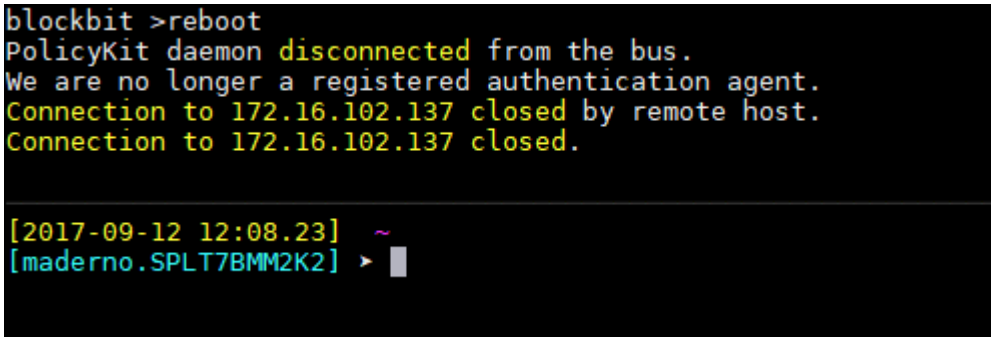


Command Line Interface – ping

UTM - [reboot]

Reboots the system.

How to use:

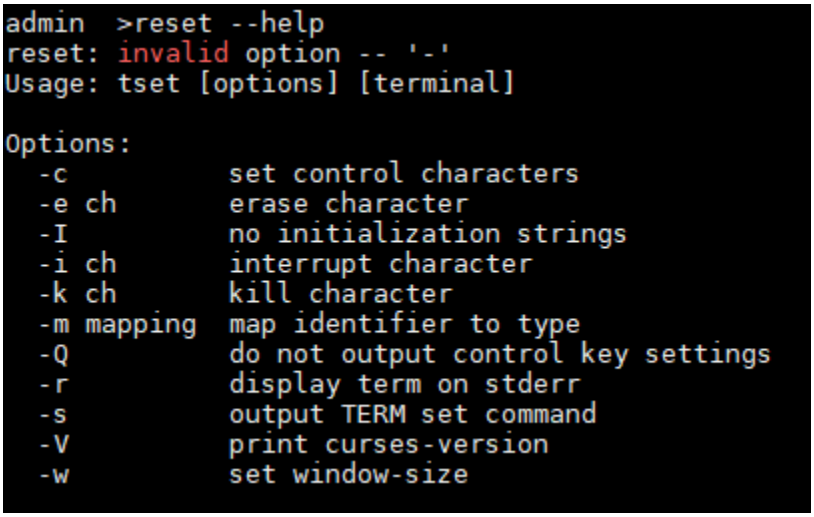


Command Line Interface – reboot

UTM - [reset]

Reset the variables of the current session in the terminal.

How to use:

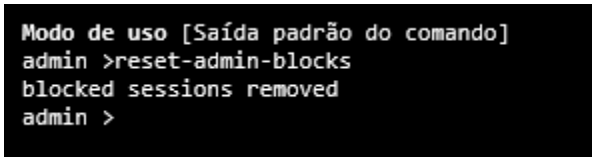


Command Line Interface – reset

UTM - [reset-admin-blocks]

Releases blocked sessions from the “admin” user of the WEB interface.

How to use:

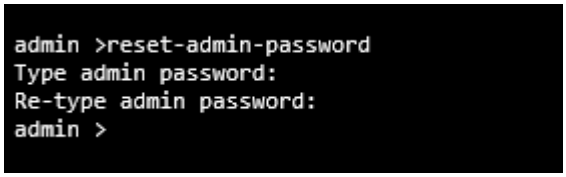


Command Line Interface – reset-admin-blocks – Example

UTM - [reset-admin-password]

Used to reset (cancel) the password for the “admin” user of the WEB interface. Automatically, you are asked to create a new password.

How to use: [Command standard output]:

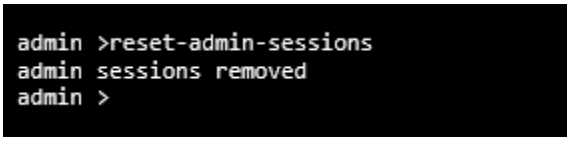


Command Line Interface – reset-admin-password

UTM - [reset-admin-sessions]

Used to remove the “Active” sessions from the “admin” user of the WEB interface.

How to use: [Command standard output]:

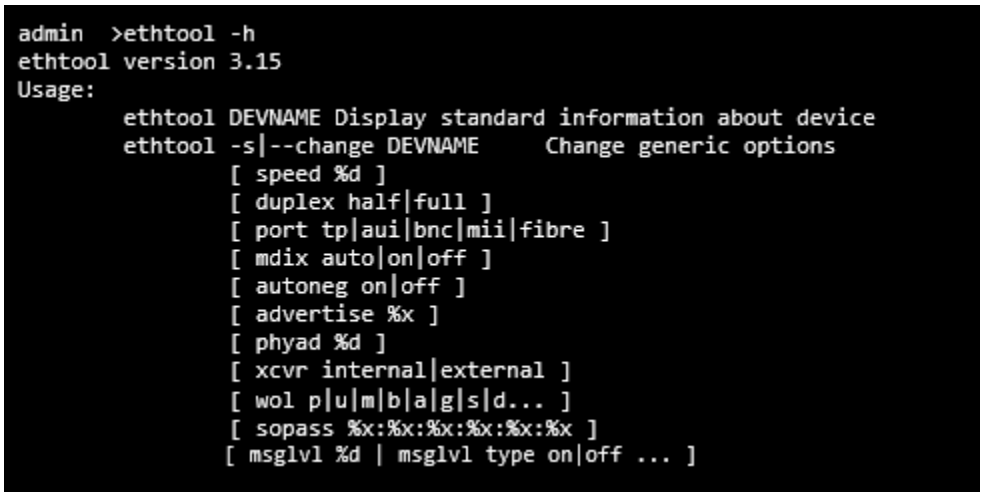


Command Line Interface – reset-admin-sessions

UTM - [reset-logs]

Deletes all UTM logs.

How to use:



Command Line Interface – ethtool

UTM - [reset-stats]

Removes all summaries for specific services or all.

How to use:

```
admin  >reset-stats
usage: reset-stats <module>
modules: [all, web, network, atp, ips, firewall, antimalware]
admin  >
```

Command Line Interface – reset-stats

Example: Remove all summaries (statistics):

```
admin  >reset-stats all
Do you really want remove (Y/N)? Y
removed web stats
removed network stats
removed atp stats
removed ips stats
removed firewall stats
removed antimalware stats
```

Command Line Interface – reset-stats - example

UTM - [restore-macaddress]

Restores the Mac Address of a determined device, after the restore of a snapshot from a different device:

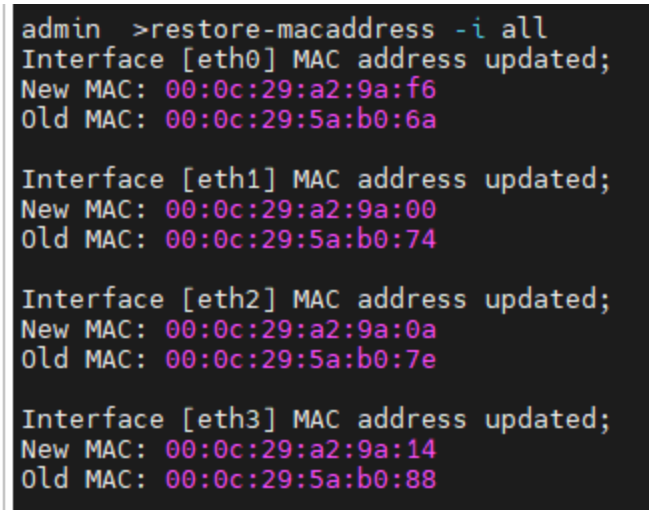
[restore-macaddress -h]: Displays the commands available in the "restore-macaddress" option.

[restore-macaddress -i ethX]: Used to restore the Mac Address of a single eth interface, in which "x" must be replaced by the number of the interface one whishes to restore the Mac Address of.

[restore-macaddress -i all]: Used to restore all of the Mac Address' interfaces.

```
[root@ngfw240-36 admin]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.23.31.36  netmask 255.255.0.0  broadcast 172.23.255.255
        ether 00:0c:29:a2:9a:f6  txqueuelen 10000  (Ethernet)
        RX packets 335  bytes 31030 (30.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 140  bytes 15451 (15.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ngfw240-36 admin]# ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 180.190.150.1  netmask 255.255.255.0  broadcast 180.190.150.255
        ether 00:0c:29:a2:9a:00  txqueuelen 10000  (Ethernet)
        RX packets 187  bytes 13248 (12.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 84 (84.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ngfw240-36 admin]# ifconfig eth2
eth2: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:a2:9a:0a  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@ngfw240-36 admin]# ifconfig eth3
eth3: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:a2:9a:14  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Command line interface: *[restore-macaddress -i ethx]*

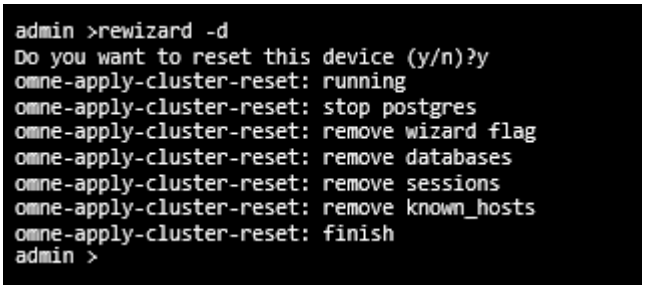


Command line interface: *[restore-macaddress -i all]*

UTM - [rewizard]

Used to reset (cancel) the BLOCKBIT GSM device settings. This command should only be used in cases of real need for total system reconfiguration.

How to use [Command standard output]:



Command Line Interface – rewizard

UTM - [route]

Displays and manipulates the IP address routing table.

How to use:

```
blockbit >route -h
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables
       route [-v] [-FC] {add|del|flush} ...  Modify routing table for AF.

       route {-h|--help} [<AF>]              Detailed usage syntax for specified AF.
       route {-V|--version}                  Display version/author and exit.

        -v, --verbose            be verbose
        -n, --numeric            don't resolve names
        -e, --extend             display other/more information
        -F, --fib                display Forwarding Information Base (default)
        -C, --cache              display routing cache instead of FIB

  <AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
blockbit >
```

Command Line Interface – route

Static routes added by the CLI (command line) console are not saved or loaded after boot.

Example 1:

```
blockbit >route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.102.1    0.0.0.0         UG    100    0        0 eth0
172.16.102.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
blockbit >
```

Command Line Interface – route – Example 1

Example 2: Configuring static routing for an extended network:

```
blockbit >route add -net 192.168.254.0/24 gw 172.16.102.1 dev eth0
blockbit >route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.102.1    0.0.0.0         UG    100    0        0 eth0
172.16.102.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
192.168.254.0   172.16.102.1    255.255.255.0   UG    0      0        0 eth0
blockbit >
```

Command Line Interface – route – Example 2

UTM - [sar]

Used to display system activity reports.

How to use:

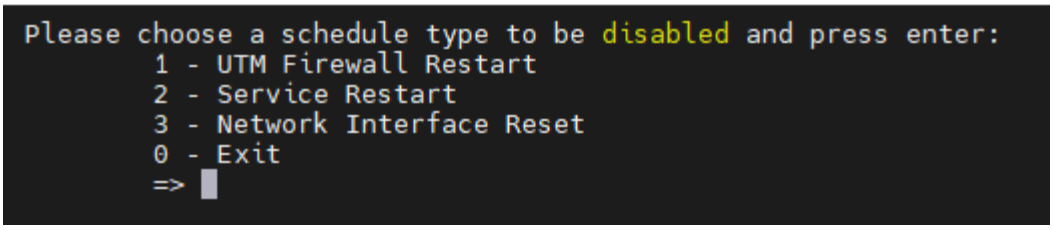
```
admin  >sar
Linux 3.10.0-229.20.1.el7.x86_64 (host.blockbit.com)    11/22/18        _x86_64_        (4 CPU)

00:00:01        CPU     %user     %nice   %system   %iowait    %steal     %idle
00:10:01        all      1.45      0.00      0.98      0.06      0.00     97.51
00:20:01        all      1.44      0.00      0.97      0.01      0.00     97.58
00:30:01        all      1.44      0.00      0.99      0.11      0.00     97.46
00:40:01        all      1.41      0.00      1.01      0.03      0.00     97.55
00:50:01        all      1.39      0.00      0.96      0.01      0.00     97.65
01:00:01        all      1.41      0.00      0.96      0.01      0.00     97.63
01:10:01        all      1.12      0.00      0.77      0.01      0.00     98.10
01:20:01        all      1.44      0.00      1.04      0.01      0.00     97.51
01:30:01        all      1.42      0.00      1.01      0.01      0.00     97.56
01:40:01        all      1.49      0.00      1.03      0.01      0.00     97.47
01:50:01        all      1.50      0.00      1.03      0.01      0.00     97.47
02:00:01        all      1.39      0.00      0.98      0.15      0.00     97.48
02:10:01        all      1.40      0.00      0.98      0.04      0.00     97.58
02:20:01        all      1.43      0.00      0.97      0.01      0.00     97.60
02:30:01        all      1.36      0.00      0.94      0.01      0.00     97.70
02:40:01        all      1.39      0.00      0.95      0.01      0.00     97.65
02:50:02        all      1.39      0.00      0.97      0.01      0.00     97.64
03:00:01        all      1.43      0.00      0.99      0.01      0.00     97.58
03:10:01        all      1.43      0.00      1.00      0.01      0.00     97.56
03:20:01        all      1.49      0.00      1.07      0.01      0.00     97.43
03:30:01        all      1.45      0.00      1.02      0.01      0.00     97.52
03:40:01        all      1.37      0.00      0.95      0.01      0.00     97.66
03:50:01        all      1.32      0.00      0.94      0.03      0.00     97.71
04:00:01        all      1.49      0.00      1.09      0.02      0.00     97.39
04:10:01        all      1.46      0.00      1.02      0.01      0.00     97.51
04:20:01        all      1.45      0.00      1.04      0.02      0.00     97.49
04:30:01        all      1.42      0.00      0.97      0.03      0.00     97.58
04:40:01        all      1.42      0.00      0.98      0.01      0.00     97.59
04:50:01        all      1.39      0.00      0.97      0.01      0.00     97.63
05:00:01        all      1.43      0.00      1.00      0.01      0.00     97.57
05:10:01        all      1.47      0.00      1.05      0.01      0.00     97.47
05:20:01        all      1.49      0.00      1.10      0.01      0.00     97.40
05:30:01        all      1.49      0.00      1.06      0.09      0.00     97.35
05:40:01        all      1.46      0.00      1.05      0.04      0.00     97.44
05:50:01        all      1.46      0.00      1.03      0.01      0.00     97.51
06:00:01        all      1.46      0.00      1.03      0.01      0.00     97.50

06:00:01        CPU     %user     %nice   %system   %iowait    %steal     %idle
06:10:01        all      1.43      0.00      1.03      0.01      0.00     97.53
06:20:01        all      1.43      0.00      0.98      0.01      0.00     97.59
06:30:02        all      1.45      0.00      1.01      0.01      0.00     97.53
06:40:01        all      1.38      0.00      0.94      0.01      0.00     97.68
06:50:01        all      1.21      0.00      0.85      0.01      0.00     97.93
07:00:01        all      1.41      0.00      1.02      0.01      0.00     97.57
07:10:01        all      0.98      0.00      0.68      0.01      0.00     98.33
07:20:01        all      1.41      0.00      1.03      0.01      0.00     97.55
07:30:01        all      1.44      0.00      0.97      0.01      0.00     97.59
07:40:01        all      1.42      0.00      0.98      0.01      0.00     97.59
07:50:01        all      1.38      0.00      0.94      0.01      0.00     97.66
08:00:01        all      1.41      0.00      0.95      0.01      0.00     97.63
08:10:01        all      1.40      0.00      0.95      0.01      0.00     97.64
08:20:01        all      1.42      0.00      0.97      0.01      0.00     97.60
08:30:01        all      1.42      0.00      0.98      0.07      0.00     97.53
08:40:01        all      1.43      0.00      1.00      0.07      0.00     97.50
08:50:01        all      1.43      0.00      0.98      0.01      0.00     97.58
09:00:01        all      1.45      0.00      1.00      0.01      0.00     97.55
09:10:01        all      1.45      0.00      1.03      0.01      0.00     97.52
09:20:01        all      1.48      0.00      1.03      0.01      0.00     97.48
09:30:01        all      1.49      0.00      1.07      0.01      0.00     97.43
09:40:01        all      1.49      0.00      1.03      0.01      0.00     97.47
Average:        all      1.41      0.00      0.99      0.02      0.00     97.58
admin  >
```

Command Line Interface – sar

UTM - [schedule-disable]

These commands are used to schedule the NGFW's reboot, restart the NGFW's services and restart the network board, since these network interfaces are enabled.

When using a command in the CLI interface, the following scheduling canceling options will be available for each command, respectively:



CLI - schedule-disable

[schedule-disable]: Cancels the schedule of one of the items below:

Select the desired canceling option inserting the number option shown.

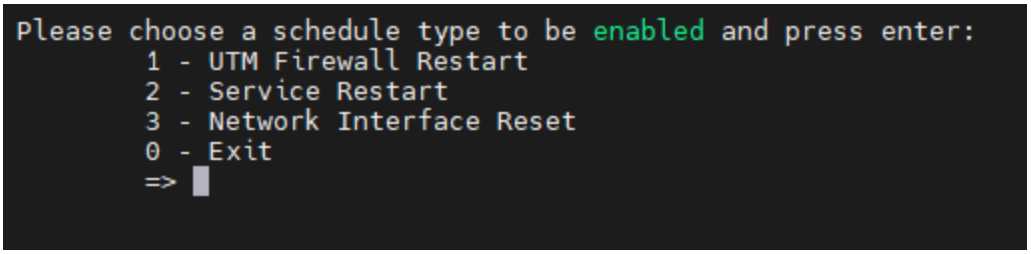
1. Resets the NGFW Firewall
2. Service restart
3. Network interface restart
0. Exit

The schedule will have been canceled and the following message will be displayed: *Appointment successfully canceled.*

UTM - [schedule-enable]

These commands are used to schedule the NGFW's reboot, restart the NGFW's services and restart the network board, since these network interfaces are enabled.

When using a command in the CLI interface, the following scheduling options will be available for each command, respectively:



CLI - schedule-enable

[schedule-enable]: Schedules the restart of the following item (enter item number):

1. Resets the NGFW Firewall
2. Service restart
3. Network interface restart

Choose an option by entering 1, 2 or 3. Next. we will analyze each one of the paths:

1.Resets the Firewall:

Enter the type of scheduling (Ex: Single/Recurring): The scheduling options are a single time "Single" (S) or as often as set "Recurring" (R).

Enter the appointment time (Ex: 23:59): The supported time is from 00:00 to 23:59.

Enter the day of the appointment (Ex: 05): The supported days are from 01 to 31.

Enter the month of the appointment (Ex: 01): The supported months are from 01 to 12.

Confirm the Firewall restart on 01/05 at 23:59 (Y - N)?: Confirmation message displayed in case of a single time event.

Confirm the the Firewall restart on the 5 of every month at 23:59 (Y - N)? Confirmation message displayed in case of a recurring event.

Confirm by entering "Y" or refuse by entering "N".

After the confirmation, the following message will be displayed: *Scheduling successfully completed*.

2. Service Restart:

Enter the type of scheduling (Ex: Single/Recurring): The scheduling options are a single time "Single" (S) or as often as set "Recurring" (R).

*Which service do you want to select (Ex: **proxy-http**)?:* Select the service to be restarted.

Enter the appointment time (Ex: 23:59): The supported time is from 00:00 to 23:59.

Enter the day of the appointment (Ex: 05): The supported days are from 01 to 31.

Enter the month of the appointment (Ex: 01): The supported months are from 01 to 12.

Confirm the Proxy-HTTP restart on 01/05 at 23:59 (Y - N)?: Message displayed in case of a single time event.

Confirm the restart of the Proxy-HTTP service on the 5 of every month at 23:59 (Y - N)?: Message displayed in case of a recurring event.

Confirm by entering "Y" or refuse by entering "N".

After the confirmation, the following message will be displayed: *Scheduling successfully completed*.

3. Network Interface

Enter the type of scheduling (Ex: Single/Recurring): The scheduling options are a single time "Single" (S) or as often as set "Recurring" (R).

The currently enabled network interfaces will be displayed, from the types: Phisycal, Alias, Virtual, VLAN, DSL, LAG, BRIDGE or TUNNEL;

Which interface do you want to restart? (Ex: eth0): Set the network interface which it will restart during the schedule.

Enter the appointment time (Ex: 23:59): The supported time is from 00:00 to 23:59.

Enter the day of the appointment (Ex: 05): The supported days are from 01 to 31.

Enter the month of the appointment (Ex: 01): The supported months are from 01 to 12.

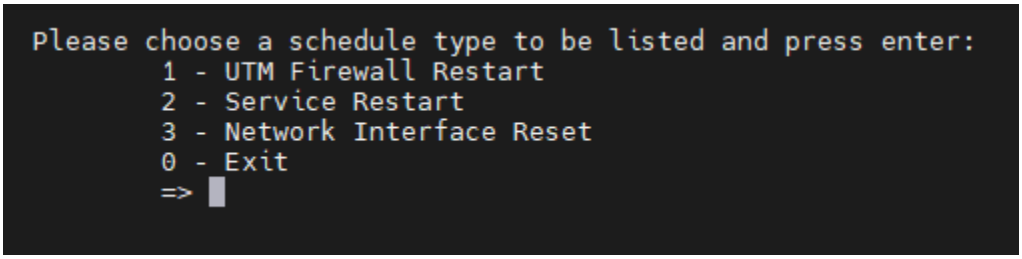
Do you want to confirm the eth0 interface restart schedule on 01/05 at 23:59?: (Yes – Y or No – N): Y

After the confirmation the following message will be displayed: *Scheduling successfully completed.*

UTM - [schedule-list]

These commands are used to schedule the NGFW's reboot, restart the NGFW's services and restart the network board, since these network interfaces are enabled.

When using a command in the CLI interface, the following list options will be available for each command, respectively:



CLI - schedule-list

[schedule-list]: Displays the appointments done for each one of the options below:

Select the schedule type inserting the number option shown.

1. Resets the NGFW Firewall
2. Service restart
3. Network interface restart
0. Exit

Example of scheduling to be displayed, in case option 1 is chosen:

- *15:00 01/05 Restart NGFW*

Example of scheduling to be displayed, in case option 2 is chosen:

- *15:00 01/05 proxy-http Service Restart*

Example of scheduling to be displayed, in case option 3 is chosen:

- *15:00 01/05 eth0 Interface Restart*

UTM - [sensors]

This command is used to display the current temperature detected by the appliance's sensors.

```
admin  > sensors -h
Usage: sensors [OPTION]... [CHIP]...
  -c, --config-file     Specify a config file
  -h, --help            Display this help text
  -s, --set             Execute `set' statements (root only)
  -f, --fahrenheit      Show temperatures in degrees fahrenheit
  -A, --no-adapter      Do not show adapter for each chip
      --bus-list        Generate bus statements for sensors.conf
  -u                    Raw output
  -v, --version         Display the program version

Use `-' after `-c' to read the config file from stdin.
If no chips are specified, all chip info will be printed.
Example chip names:
        lm78-i2c-0-2d   *-i2c-0-2d
        lm78-i2c-0-*    *-i2c-0-*
        lm78-i2c-*-2d   *-i2c-*-2d
        lm78-i2c-*-*    *-i2c-*-*
        lm78-isa-0290   *-isa-0290
        lm78-isa-*      *-isa-*
        lm78-*
```

Command Line Interface – sensors - h

The system may need to recognize the sensors. To do this, use the command **[sensors -detect]**

How to use:

```
admin  > sensors
coretemp-isa-0000
Adapter: ISA adapter
Physical id 0:  +44.0°C  (high = +88.0°C, crit = +98.0°C)
Core 0:         +43.0°C  (high = +88.0°C, crit = +98.0°C)
Core 1:         +41.0°C  (high = +88.0°C, crit = +98.0°C)
Core 2:         +44.0°C  (high = +88.0°C, crit = +98.0°C)
Core 3:         +42.0°C  (high = +88.0°C, crit = +98.0°C)
Core 4:         +41.0°C  (high = +88.0°C, crit = +98.0°C)
Core 8:         +41.0°C  (high = +88.0°C, crit = +98.0°C)
Core 9:         +39.0°C  (high = +88.0°C, crit = +98.0°C)
Core 10:        +41.0°C  (high = +88.0°C, crit = +98.0°C)
Core 11:        +40.0°C  (high = +88.0°C, crit = +98.0°C)
Core 12:        +41.0°C  (high = +88.0°C, crit = +98.0°C)

coretemp-isa-0001
Adapter: ISA adapter
Physical id 1:  +40.0°C  (high = +88.0°C, crit = +98.0°C)
Core 0:         +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 1:         +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 2:         +40.0°C  (high = +88.0°C, crit = +98.0°C)
Core 3:         +36.0°C  (high = +88.0°C, crit = +98.0°C)
Core 4:         +39.0°C  (high = +88.0°C, crit = +98.0°C)
Core 8:         +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 9:         +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 10:        +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 11:        +37.0°C  (high = +88.0°C, crit = +98.0°C)
Core 12:        +37.0°C  (high = +88.0°C, crit = +98.0°C)
```

Command Line Interface – sensors

UTM - [service-disable]

Disables a particular service from being automatically loaded when restarting the server.

How to use:

```
admin  >service-disable
usage: service-disable <service-name>
admin  >
```

Command Line Interface – service-disable

***Service Names*:**

```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Command Line Interface – service-disable – service-names

UTM - [service-enable]

Enables a specific service to be loaded automatically when restarting the server.

How to use:

```
admin  >service-enable
usage: service-enable <service-name>
admin  >
```

Command Line Interface – service-enable

***Service names*:**

```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Command Line Interface – service-enable – service-names

UTM - [service-start]

Initializes a particular service.

How to use:

```
admin  >service-start
usage: service-start <service-name>
admin  >
```

Command Line Interface – service-start

***Service names*:**

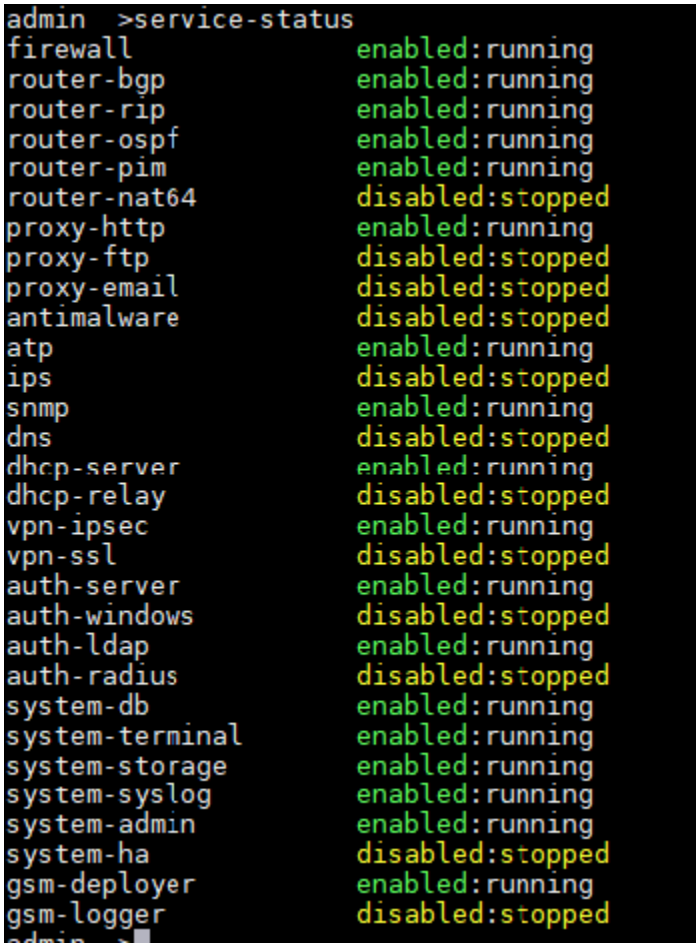
```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Command Line Interface – service-start – service-names

UTM - [service-status]

Displays the status of all monitored services.

How to use:



Command Line Interface – service-status

UTM - [service-stop]

Stops a particular service.

How to use:

```
admin  >service-stop
usage: service-stop <service-name>
admin  >
```

Command Line Interface – service-stop

***Service names*:**

```
antimalware
atp
auth-ldap
auth-radius
auth-server
auth-windows
dhcp-relay
dhcp-server
dns
firewall
gsm-deployer
gsm-logger
ips
proxy-email
proxy-ftp
proxy-http
router-bgp
router-nat64
router-ospf
router-pim
router-rip
snmp
system-admin
system-db
system-ha
system-storage
system-syslog
system-terminal
vpn-ipsec
vpn-ssl
```

Command Line Interface – service-stop – service-names

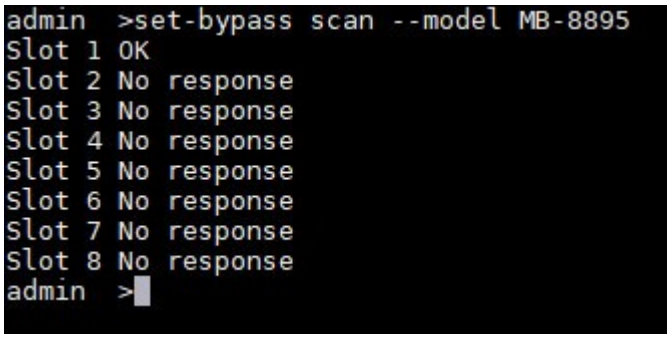
UTM - [set-bypass]

This command has the function of configuring the UTM bypass feature. When using this command it is necessary to pass the hardware model of the appliance, here is a summary of the function of each of the arguments of this command:

Command Action Arguments:

[*scan*]

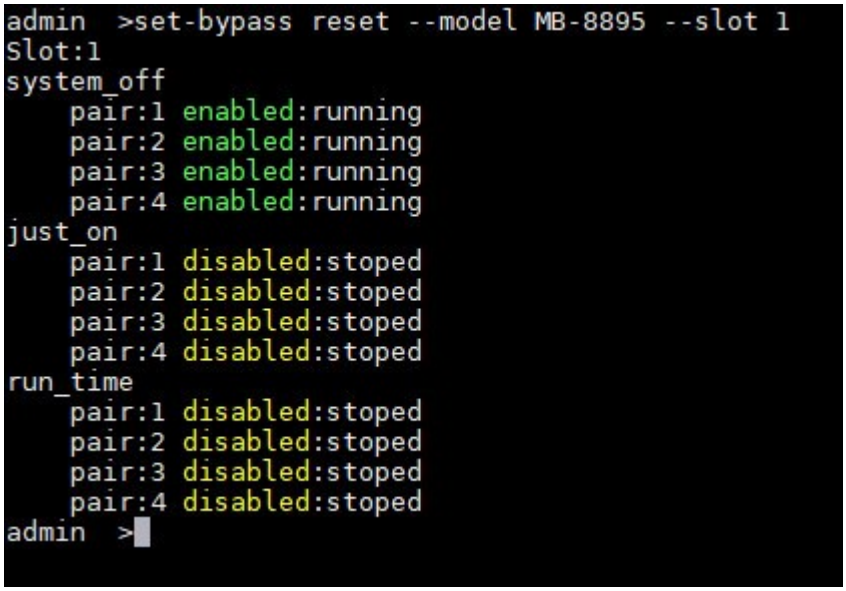
Scans the appliance to detect which slot is available and which has not returned a response;



Command Line Interface – set-bypass – scan

[*reset*]

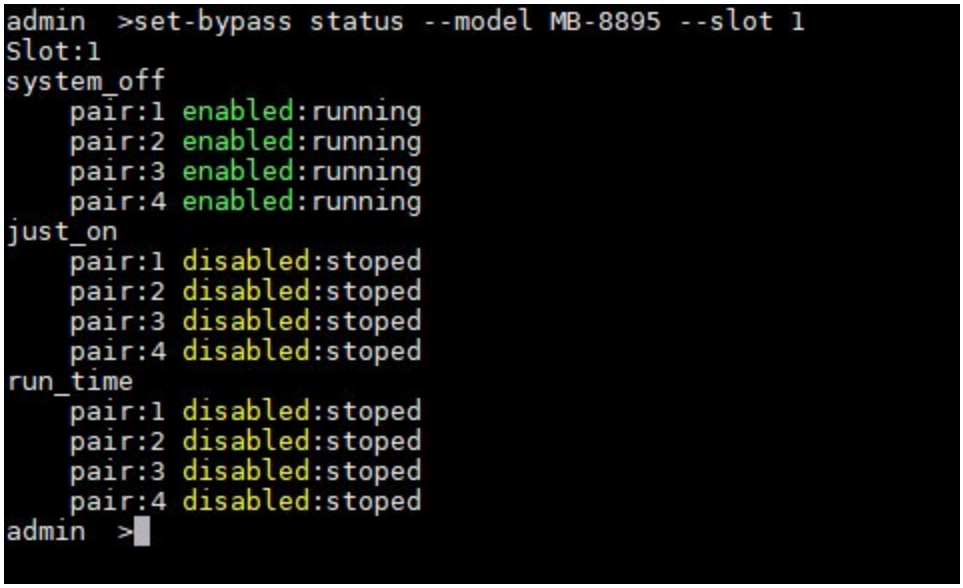
Restores factory settings, by default, system_off mode is enabled;



Command Line Interface – set-bypass – reset

[*status*]

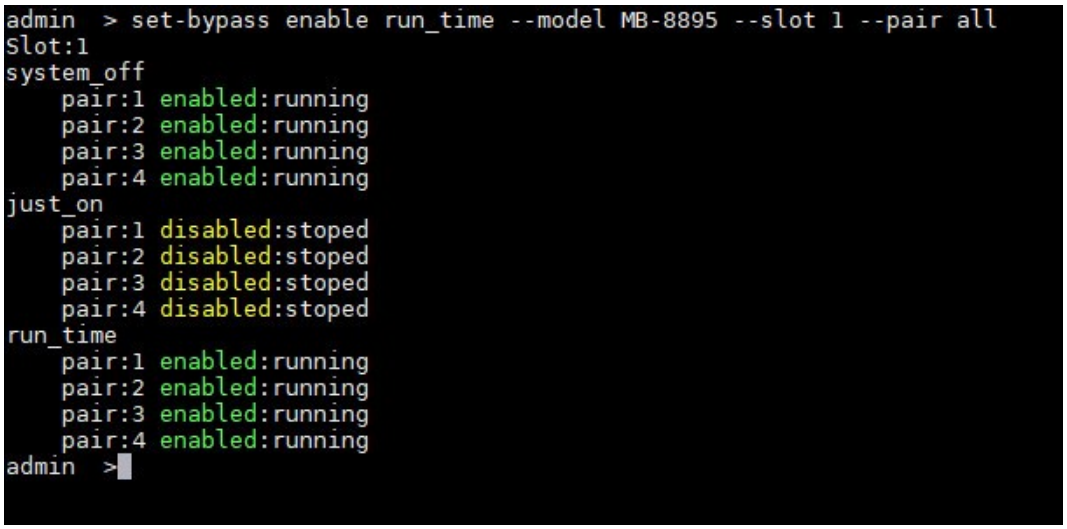
Determines which type of bypass is configured for which pair and the current state of each of these pairs;



Command Line Interface – set-bypass – status

[*enable*]

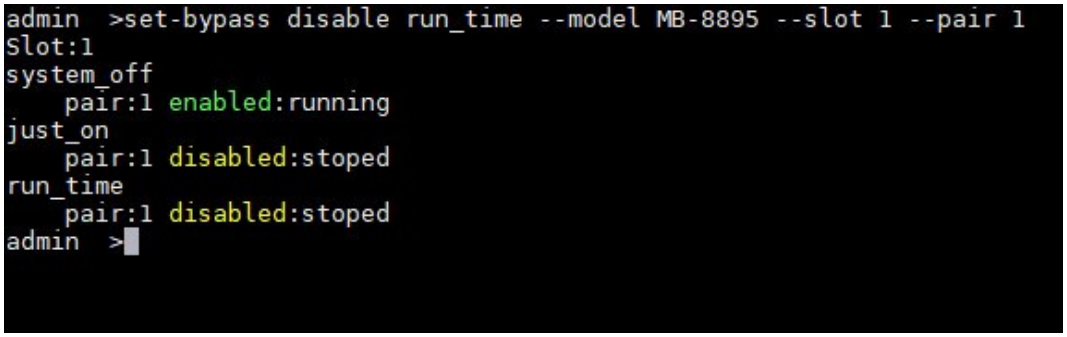
This parameter is used to enable the type of bypass that will be applied to the selected pair;



Command Line Interface – set-bypass – enable

[*disable*]

This parameter is used to disable the type of bypass that will be applied to the selected pair*;*



Command Line Interface – set-bypass – disable

Bypass Mode Arguments:

[*system_off*]

The bypass will be activated when the system has turned off.

[*just_on*]

The bypass will be activated when the system is in the boot process.

[*run_time*]

The bypass will be activated when the system is running.

[*all*]

The bypass will be active in all situations mentioned above.

Bypass option arguments:

[-m] *--model*

It determines the hardware model of the appliance, it is a necessary argument to pass most commands. As shown in the examples shown by the command, use the MB-8895 model.

[-s] *--slot*

Determines in which slot the command will be executed.

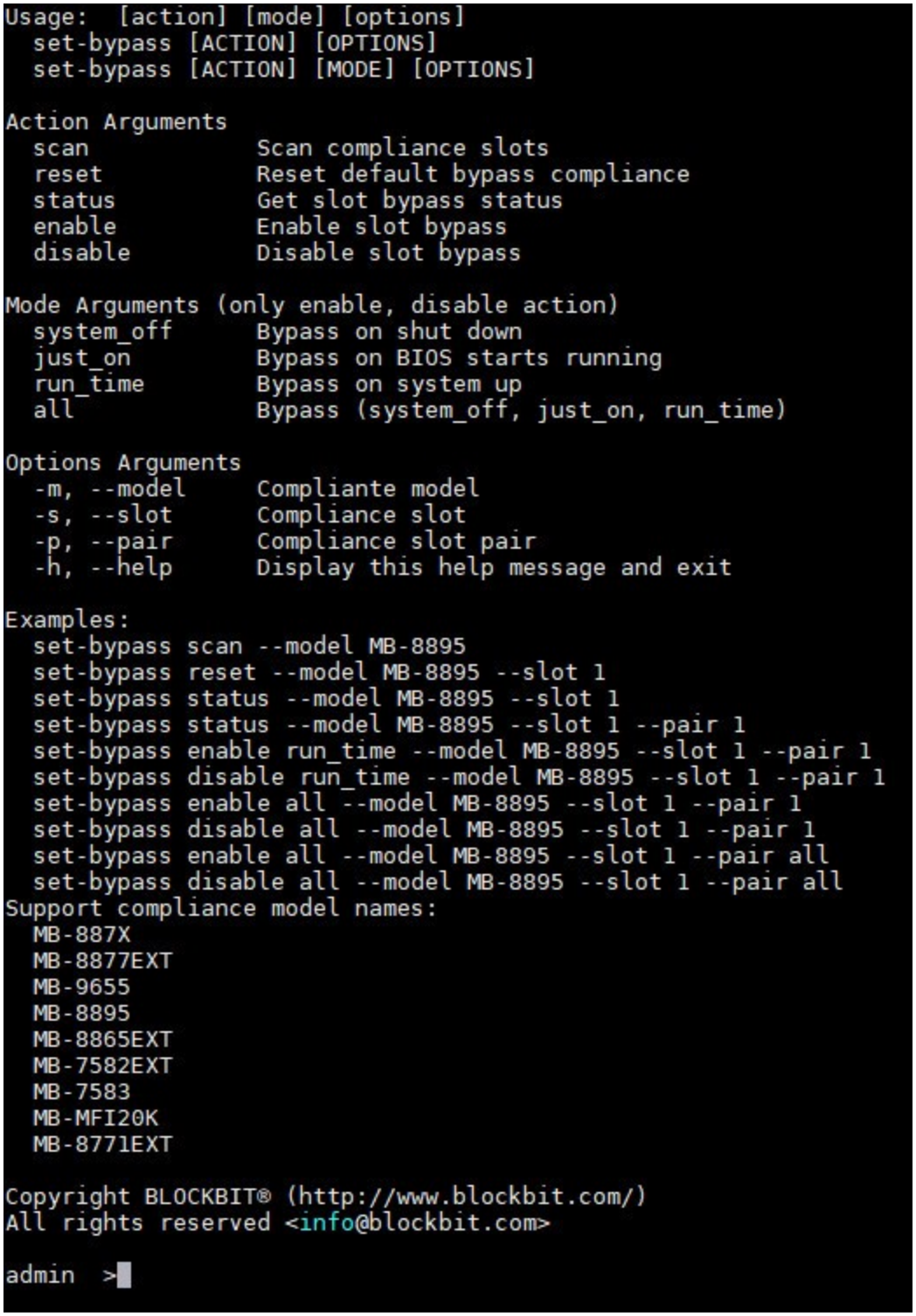
[-p] *--pair*

Determines which pair the command will be executed on.

[-h] *--help*

Displays the standard help message.

How to use:



Command Line Interface – set-bypass

UTM - [set-ethernet-channels]

By default, network cards use a specific queue, the **[set-ethernet-channels]** command has the function of enabling the user to increase the number of queues that will be used on the physical interfaces.

Note that this command is used specifically on physical interfaces. It does NOT apply to virtual interfaces.

Attention: This command may not be supported depending on the equipment's network card.

How to use:

```
admin  >set-ethernet-channels eth1 3
admin  >
```

Command Line Interface - set-ethernet-channels - Standard command output

```
admin  >set-ethernet-channels eth1 3
admin  >set-ethernet-channels eth1 3
combined unmodified, ignoring
no channel parameters changed, aborting
current values: tx 0 rx 0 other 1 combined 3
admin  >
```

Command Line Interface - set-ethernet-channels - Output if you have already configured a certain channel on the same interface

Command Action Arguments:

[-h]

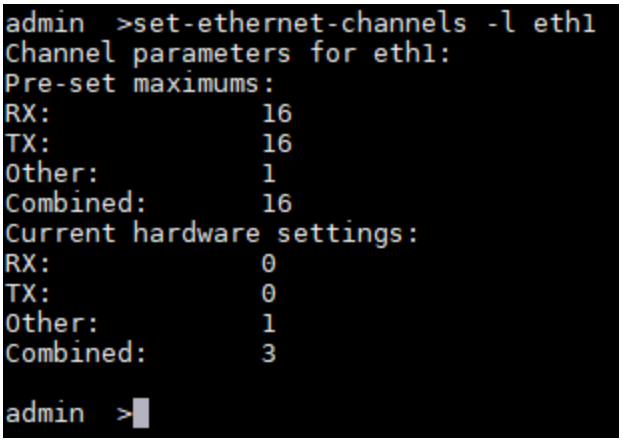
Displays the default help message.

```
admin  >set-ethernet-channels
Usage: set-ethernet-channels <eth0> [1-9]

Optional Arguments
  -h,              Display this help message and exit
  -l <eth0>,       Show channel device
  -p,              Configuration persist
admin  >
```

Command Line Interface – set-ethernet-channels

[-l]

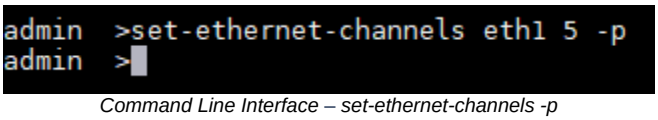
Its function is to list relevant information of the determined interface.



Command Line Interface – set-ethernet-channels -l

[-p]

When adding this attribute, configuration persistence will be implemented.

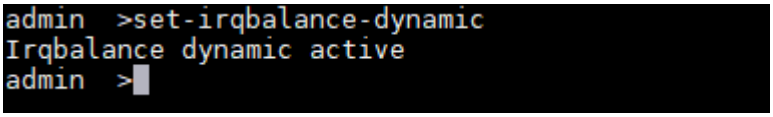


Command Line Interface – set-ethernet-channels -p

UTM - [set-irqbalance-dynamic]

Enables Dynamic IRQ Balance.

How to use:

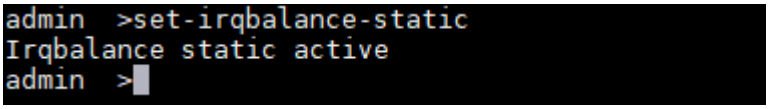


Command Line Interface – set-irqbalance-dynamic

UTM - [set-irqbalance-static]

Enables the Static IRQ Balance.

How to use:

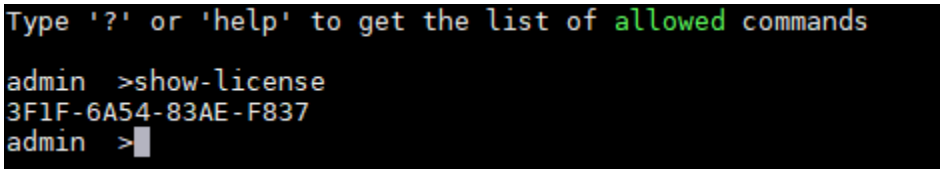


Command Line Interface – set-irqbalance-static

UTM - [show-license]

Displays information about the license.

How to use:

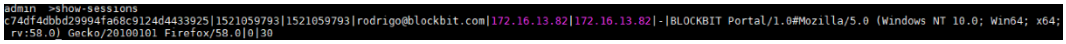


Command Line Interface – show-license

UTM - [show-sessions]

Displays authentication sessions.

How to use:

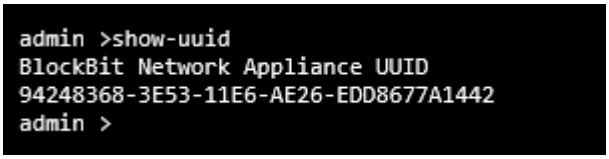


Command Line Interface – show-sessions

UTM - [show-uuid]

Used to display the BLOCKBIT UTM identification number. This ID is used to identify the hardware for validating the use license.

How to use: [Standard command output]

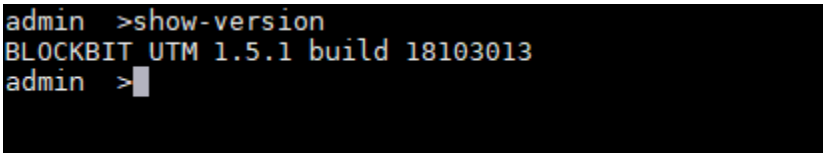


Command Line Interface – show-uuid

UTM - [show-version]

Command to obtain version information.

How to use:

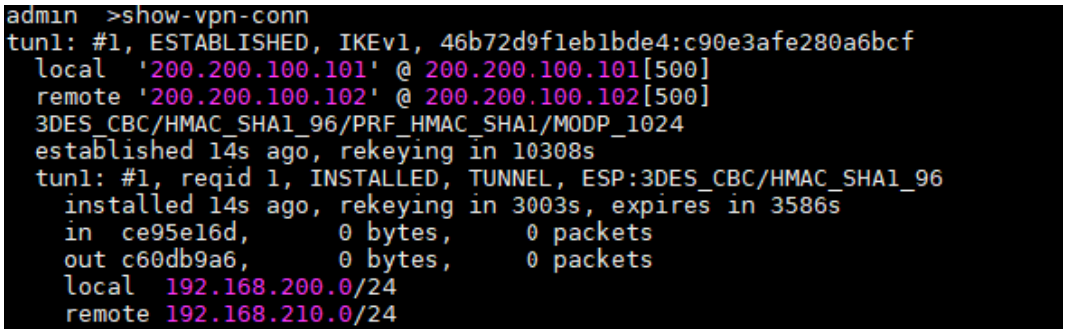


Command Line Interface – show-version

UTM - [show-vpn-conn]

Displays the IPSEC VPN tunnels that are in the air, the encryption used, connection time, source network, destination network and packets trafficked.

How to use:



Command Line Interface – show-vpn-conn

UTM - [show-vpn-info]

Displays the IPSEC VPN tunnels that are in the air, encryption used, connection time, originating network, destination network and packets trafficked. In addition, it also displays the time the service is on the air, the number of workers and the IP (s) the service is listening to (listen).

How to use:

```
admin  >show-vpn-info
  uptime: 16 seconds, since Mar 15 09:31:28 2018
  malloc: sbrk 2703360, mmap 0, used 576032, free 2127328
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
Listening IP addresses:
  172.16.102.78
  200.200.100.101
  192.168.222.1
Connections:
       tun1:  200.200.100.101...200.200.100.102,0.0.0.0/0,::/0  IKEv1
       tun1:   local:  [200.200.100.101] uses pre-shared key authentication
       tun1:   remote: [200.200.100.102] uses pre-shared key authentication
       tun1:   child:  192.168.200.0/24 === 192.168.210.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
       tun1[1]: ESTABLISHED 16 seconds ago, 200.200.100.101[200.200.100.101]...200.200.100.102[200.200.100.102]
       tun1[1]: IKEv1 SPIs: 46b72d9f1eb1bde4_i* c90e3afe280a6bcf_r, rekeying in 2 hours
       tun1[1]: IKE proposal: 3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
       tun1{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ce95e16d_i c60db9a6_o
       tun1{1}:  3DES_CBC/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 50 minutes
       tun1{1}:   192.168.200.0/24 === 192.168.210.0/24
```

Command Line Interface – show-vpn-info

UTM - [show-wwan]

This command has the function to display information of the 3G / 4G / LTE connection its current state and properties of the device:

How to use

```
admin  >show-wwan -h
Usage: show-wwan [COMMAND]
Show WWAN device info

Options:
  modem-info                Query modem general information
  sim-info                  Query SIM information
  connection-status         Query connection status


Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

Command Line Interface – show-wwan -h

This command also has the following parameters:

modem-info

The command displays information about the modem.

```
admin  >show-wwan modem-info

BB-WWAN/Modem/0 (device id '25e0ad644e62365be25250466fb3d0d28ef0fe08')
  ------------------------
  Hardware |   manufacturer: 'QUALCOMM INCORPORATED'
           |          model: 'QUECTEL Mobile Broadband Module'
           |       revision: 'EC25AUFAR06A03M4G'
           |      supported: 'gsm-umts
           |                  lte
           |                  gsm-umts, lte'
           |        current: 'gsm-umts, lte'
           |   equipment id: '861585045180203'
  ------------------------
  System   |         device: '/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3'
           |        drivers: 'option1, qmi_wwan'
           |         plugin: 'Generic'
           |   primary port: 'cdc-wdm0'
           |          ports: 'ttyUSB0 (qcdm), ttyUSB2 (at), cdc-wdm0 (qmi), wwan0 (net), ttyUSB3 (at)'
  ------------------------
  Numbers  |            own : 'unknown'
  ------------------------
  Status   |           lock: 'sim-pin2'
           | unlock retries: 'sim-pin (3), sim-pin2 (3), sim-puk (10), sim-puk2 (10)'
           |          state: 'connected'
           |    power state: 'on'
           |    access tech: 'lte'
           | signal quality: '67' (recent)
  ------------------------
  Modes    |      supported: 'allowed: 2g, 3g, 4g; preferred: none'
           |        current: 'allowed: 2g, 3g, 4g; preferred: none'
  ------------------------
  Bands    |      supported: 'dcs, egsm, pcs, g850, u2100, u1900, u850, u900, eutran-i, eutran-ii, eutran-iii, eutran-iv, eutran-v, eutran-vii, eutran-viii, eutran-xl'
           |        current: 'dcs, egsm, pcs, g850, u2100, u1900, u850, u900, eutran-i, eutran-ii, eutran-iii, eutran-iv, eutran-v, eutran-vii, eutran-viii, eutran-xl'
  ------------------------
  IP       |      supported: 'ipv4, ipv6, ipv4v6'
  ------------------------
  3GPP     |           imei: '861585045180203'
           |  enabled locks: 'none'
           |    operator id: '72403'
           |  operator name: 'TIM'
           |   subscription: 'unknown'
           |   registration: 'home'
  ------------------------
  SIM      |           path: 'BB-WWAN/SIM/0'

  ------------------------
  Bearers  |          paths: 'BB-WWAN/Bearer/0'

admin  >
```

Command Line Interface – show-wwan modem-info

sim-info

It serves to determine the status of the SIM card.

```
admin  >show-wwan sim-info
SIM 'BB-WWAN/SIM/0'
  ------------------------
  Properties |          imsi : 'unknown'
             |            id : 'unknown'
             |   operator id : '72403'
             | operator name : 'TIM'
```

Command Line Interface – show-wwan sim-info

connection-status

It is used to determine the connection status.

```
admin  >show-wwan connection-status
Bearer 'BB-WWAN/Bearer/0'
  ------------------------
  Status              |   connected: 'yes'
                      |   suspended: 'no'
                      |   interface: 'wwan0'
                      |  IP timeout: '20'
  ------------------------
  Properties          |         apn: 'vivo.com.br'
                      |     roaming: 'allowed'
                      |     IP type: 'ipv4v6'
                      |        user: 'vivo'
                      |    password: 'vivo'
                      |      number: 'none'
                      | Rm protocol: 'unknown'
  ------------------------
  IPv4 configuration  |   method: 'static'
                      |  address: '100.66.59.216'
                      |   prefix: '28'
                      |  gateway: '100.66.59.217'
                      |      DNS: '189.40.198.81', '189.40.198.80'
                      |      MTU: '1500'
  ------------------------
  IPv6 configuration  |   method: 'static'
                      |  address: '2804:214:812d:f524:a4fa:b46f:7f46:a3e7'
                      |   prefix: '64'
                      |  gateway: '2804:214:812d:f524:f8b3:7c0f:90c0:c756'
                      |      DNS: '2804:214:8000:ffff::81', '2804:214:8000:ffff::80'
                      |      MTU: '1500'
  ------------------------
  Stats               |          Duration: '6720'
                      |    Bytes received: '111201476'
                      | Bytes transmitted: '10330353'
admin  >
```

Command Line Interface – show-wwan connection-status

-h ou --help

Displays the help menu with information about all attributes.

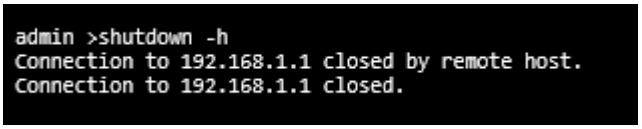
```
admin  >show-wwan -h
Usage: show-wwan [COMMAND]
Show WWAN device info

Options:
  modem-info                Query modem general information
  sim-info                  Query SIM information
  connection-status         Query connection status


Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

Command Line Interface – show-wwan -h

UTM - [shutdown]

Used to shut down the system.

How to use: [Standard command output]



Command Line Interface – shutdown

UTM - [speedtest]

Speedtest is a command to measure internet connection speed using the Speedtest.net service. You can check download speed, upload speed, and latency (ping) directly in the terminal without accessing the website.

The connection speed is estimated and relative, and it may differ from the actual performance experienced when using the internet. The value given by Speedtest should not be used for documentation purposes.

The difference between the estimated and actual speed can be due to server location (closer servers provide higher speeds), network congestion and routing (tests do not capture traffic variation), equipment limitations (devices may limit speed), traffic priority, or bandwidth usage by other devices.

To obtain a more realistic measure, you can:

- Test at different times;
- Test with different servers;
- Test browsing with different content (streaming, downloads, etc.).

How to use:

```
admin  >speedtest -h
usage: speedtest [-h] [--bytes] [--share] [--simple] [--list] [--server SERVER] [--mini MINI] [--source SOURCE] [--version]

Command line interface for testing internet bandwidth using speedtest.net. ------------------------------------------------------------------------
https://github.com/sivel/speedtest-cli

optional arguments:
  -h, --help            show this help message and exit
  --bytes               Display values in bytes instead of bits. Does not affect the image generated by --share
  --share               Generate and provide a URL to the speedtest.net share results image
  --simple              Suppress verbose output, only show basic information
  --list                Display a list of speedtest.net servers sorted by distance
  --server SERVER       Specify a server ID to test against
  --mini MINI           URL of the Speedtest Mini server
  --source SOURCE       Source IP address to bind to
  --version             Show the version number and exit
```

Command Line Interface – speedtest

Example:

```
admin  >speedtest
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from Vivo (191.13.128.45)...
Selecting best server based on latency...
Hosted by CenturyLink (Sao Paulo) [14.70 km]: 69.484 ms
Testing download speed.....................................
Download: 59.95 Mbits/s
Testing upload speed.......................................................
Upload: 49.07 Mbits/s
```

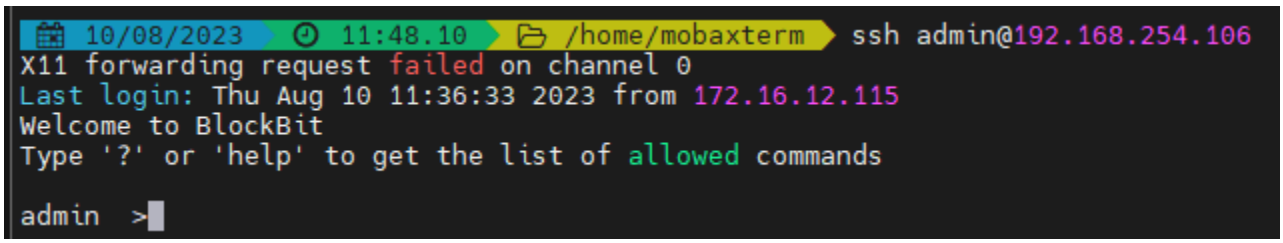
Command Line Interface – speedtest - example

UTM - [ssh]

This command makes it possible to make an SSH connection between Blockbit servers.

This command can only be used specifically by an "admin" user

How to use:



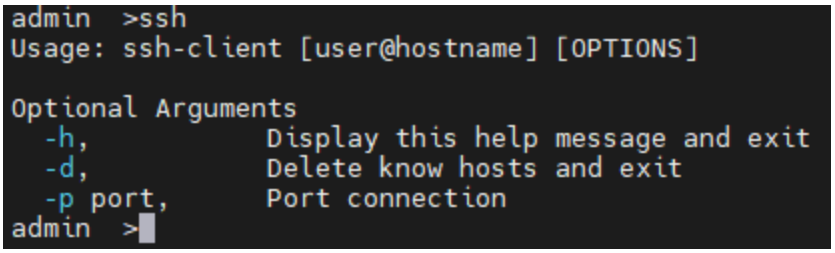
Command Line Interface – ssh - Command standard output

When making the connection, the command performs a fingerprint validation in the accesses between the servers. In order to continue, you will need a confirmation from the user.

Command Action Arguments:

[-h]

Displays the default help message.



Command Line Interface – ssh - help

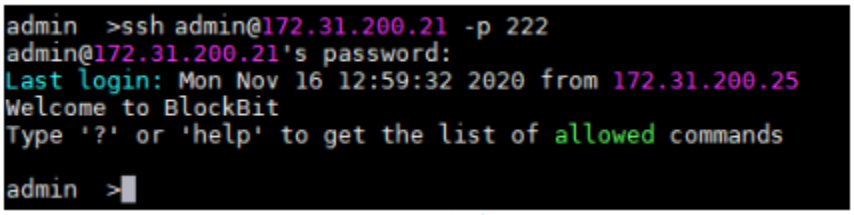
[-d]

Removes known hosts and exits the command.

Command Line Interface - ssh -d

[-p]

This command is used to access a Blockbit server that uses a non-standard port (for example, in a *port forward* scenario).



Command Line Interface - ssh -p

UTM - [ssh-proxy-sessions]

This command makes it possible to list the SSH Proxy users and their sessions history.

How to use:

Type 'ssh-proxy-session' and the users found will be listed.

Type the same command and pass one of the listed users as a parameter (e.g. 'ssh-proxy-sessions user_1') to verify the activity from this user.

```
admin  >ssh-proxy-sessions
You have to run the command 'ssh-proxy-sessions' and the user
Example:  'show_ssh_proxy_sessions jonsnow'
we found this user(s):
        user.mano1
        user_1
        user_3
        user_4
        user_5
admin  >
admin  >ssh-proxy-sessions user_1
SSH Session session authorized by user_1 between Feb 13 15:29:18 2023-Feb 14 10:44:24 2023

  SSH User       Destination    From Source   Login at       Duration
  administrator  172.23.21.185  10.40.150.61  Today   10:44  0d 00:00:03

SSH Session session authorized by user_1 between Feb 14 10:47:12 2023- No logout

  SSH User       Destination    From Source   Login at       Duration
  administrator  172.23.21.185  10.40.150.61  Today   10:46  -
  administrator  172.23.21.185  10.40.150.61  Today   10:46  0d 00:00:05
  administrator  172.23.21.185  10.40.150.61  Today   10:44  0d 00:01:06
  administrator  172.23.21.185  10.40.150.61  Today   10:44  0d 00:00:06
  administrator  172.23.21.185  10.40.150.61  Today   10:44  0d 00:00:03

admin  >
```

Command Line - Interface - ssh-proxy-sessions

UTM - [sync-users]

Performs user synchronism.

How to use:

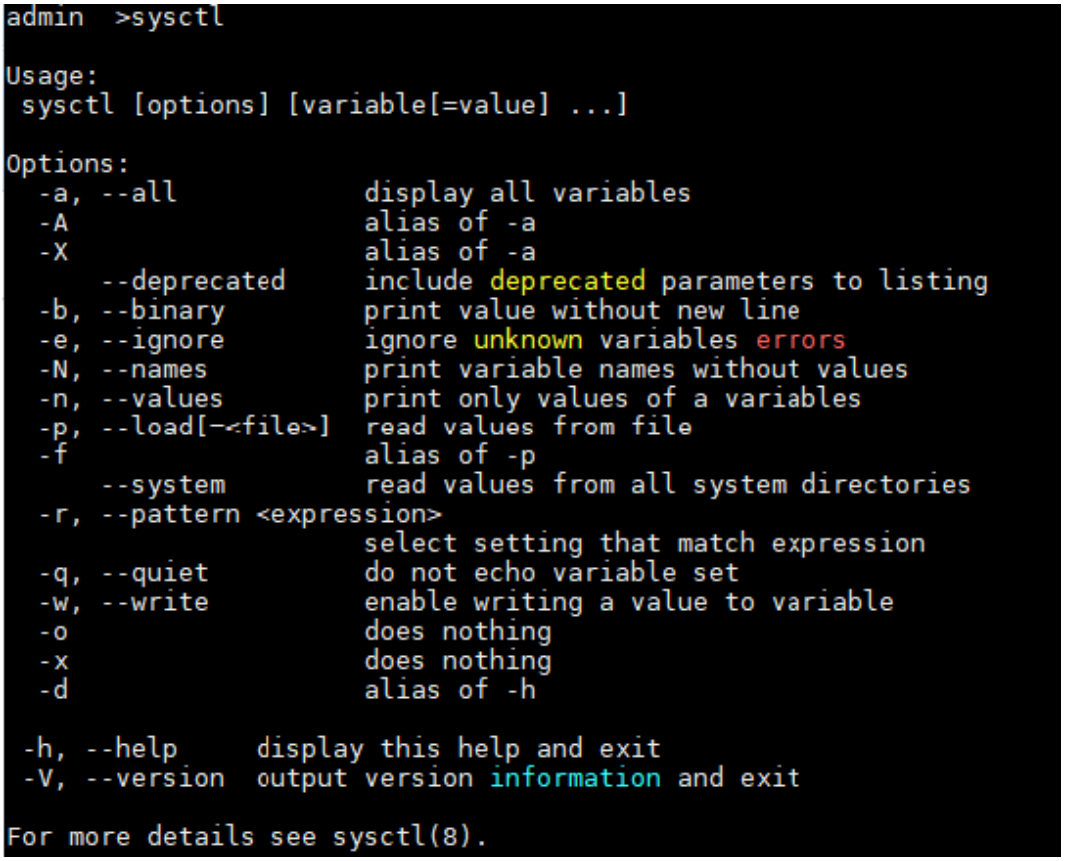
```
admin  >sync-users
```

Command Line Interface – sync-users

UTM - [sysctl]

Modifica parâmetro do kernel em tempo de execução.

Modo de uso:



Command Line Interface – sysctl

Parâmetros alterados por esse comando não são mantidos após reiniciar o servidor.

UTM - [tcpdump]

Monitors, captures and analyzes packets transmitted over the network. Thus, it allows the administrator to analyze the behavior of the network, helping to identify problems, infected stations, malicious traffic, bottlenecks, etc.

How to use:

```
blockbit >tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ]
                [ -P in|out|inout ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ -V file ] [ -w file ]
                [ -W filecount ] [ -y datalinktype ] [ -z command ]
                [ -Z user ] [ expression ]
blockbit >
```

Command Line Interface – tcpdump

Example: Monitoring all traffic on the local network interface (Eth0 interface):

```
blockbit >tcpdump -i eth0 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:55:48.261189 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 655814578:655814738, ack 1349706053, win 203, length 160
13:55:48.261316 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 160:240, ack 1, win 203, length 80
13:55:48.261359 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 240:288, ack 1, win 203, length 48
13:55:48.261404 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 288:336, ack 1, win 203, length 48
13:55:48.261445 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 336:384, ack 1, win 203, length 48
13:55:48.261477 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 384:432, ack 1, win 203, length 48
13:55:48.261491 IP 172.16.100.15.59005 > 172.16.102.136.22: Flags [.], ack 160, win 2048, length 0
13:55:48.261531 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 432:496, ack 1, win 203, length 64
13:55:48.261560 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 496:544, ack 1, win 203, length 48
13:55:48.261585 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 544:592, ack 1, win 203, length 48
13:55:48.261610 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 592:640, ack 1, win 203, length 48
13:55:48.261637 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 640:688, ack 1, win 203, length 48
13:55:48.261663 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 688:736, ack 1, win 203, length 48
13:55:48.261694 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 736:784, ack 1, win 203, length 48
13:55:48.261972 IP 172.16.100.15.59005 > 172.16.102.136.22: Flags [.], ack 640, win 2053, length 0
13:55:48.261978 IP 172.16.102.136.22 > 172.16.100.15.59005: Flags [P.], seq 784:832, ack 1, win 203, length 48
```

Command Line Interface – tcpdump – Example

UTM - [tcptop]

Extracts and displays traffic information from network interfaces, such as: Total captured packets, received packets, packets blocked by the kernel and packets trafficked by the TOP 10 IP addresses.

How to use:

```
Modo de uso
admin  >tcptop
you must specify the interface: [eth0,eth1 ...]
admin  >
```

Command Line Interface – tcptop

Example: Displaying top 10 traffic information on the eth0 interface:

```
admin  >tcptop eth1
Wait capturing frames ...
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
10000 packets captured
10070 packets received by filter
21 packets dropped by kernel
   3268 IP 177.185.5.137
   3090 IP 192.168.0.2
   1626 IP 192.168.3.2
    481 IP 201.86.139.109
    290 IP 8.8.8.8 > 192
    288 IP 192.168.3.2 > 8
    246 IP 201.31.172.3
admin  >
```

Command Line Interface – tcptop – Example

UTM - [tcptrack]

Displays information about TCP connections for a given network interface. It monitors connections, displays status, source address, destination address and bandwidth consumption.

How to use:

```
admin  >tcptrack
Usage: /usr/bin/tcptrack [-dfhvp] [-r <seconds>] -i <interface> [<filter expression>] [-T <pcap file]
admin  >
```

Command Line Interface – tcptrack

UTM - [telnet]

Used for remote access, terminal simulation tests, service connection response and sending an e-mail message.

How to use:

```
blockbit >telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
 [host-name [port]]
blockbit >
```

Command Line Interface – telnet

Example 1:

```
blockbit >telnet
telnet> ?
Commands may be abbreviated.  Commands are:

close           close current connection
logout          forcibly logout remote user and close the connection
display         display operating parameters
mode            try to enter line or character mode ('mode ?' for more)
open            connect to a site
quit            exit telnet
send            transmit special characters ('send ?' for more)
set             set operating parameters ('set ?' for more)
unset           unset operating parameters ('unset ?' for more)
status          print status information
toggle          toggle operating parameters ('toggle ?' for more)
slc             change state of special charaters ('slc ?' for more)
z               suspend telnet
!               invoke a subshell
environ         change environment variables ('environ ?' for more)
?               print help information
telnet>
```

Command Line Interface – telnet – Example 1

Example 2: Connection tests with a remote service (Terminal Service) on a specific port:

```
blockbit >telnet 172.16.13.245 3389
Trying 172.16.13.245...
Connected to 172.16.13.245.
Escape character is '^]'.
^]

telnet>
```

Command Line Interface – telnet – Example 2

UTM - [tracepath]

Trace a path to a designated network address, stating the “lifetime” (or TTL lag) and the maximum transmission unit (MTU) along the way.

How to use:

```
blockbit >tracepath -h
Usage: tracepath [-n] [-b] [-l <len>] [-p port] <destination>
blockbit >tracepath -p 3389 172.16.13.245
 1?: [LOCALHOST]                                         pmtu 1500
 1:  gateway                                               1.684ms
 1:  gateway                                               3.150ms
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  no reply
 8:  no reply
 9:  no reply
10:  no reply
11:  no reply
12:  no reply
13:  no reply
14:  no reply
15:  no reply
16:  no reply
17:  no reply
18:  no reply
19:  no reply
20:  no reply
21:  no reply
22:  no reply
23:  no reply
24:  no reply
25:  no reply
26:  no reply
27:  no reply
28:  no reply
29:  no reply
30:  no reply
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
blockbit >
```

Command Line Interface – tracepath

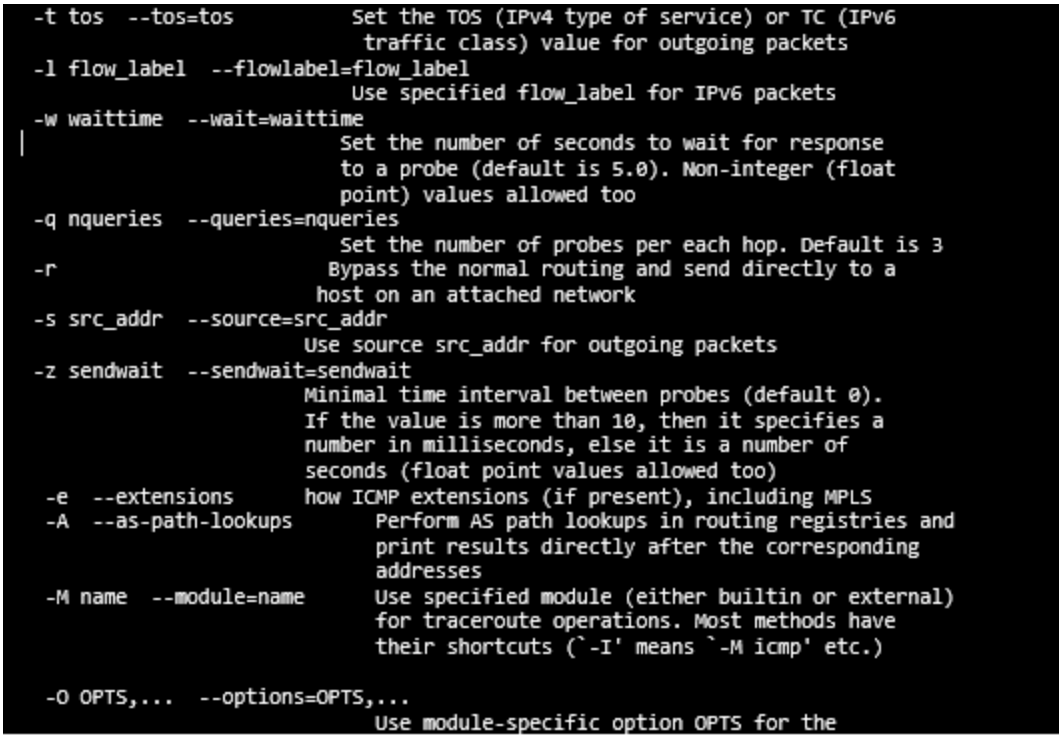
UTM - [traceroute]

Plots a path to a designated network address. The “traceroute” command supports some advanced parameters (which differentiates it from “tracepath”) including the selection of protocols: TCP, UDP or ICMP.

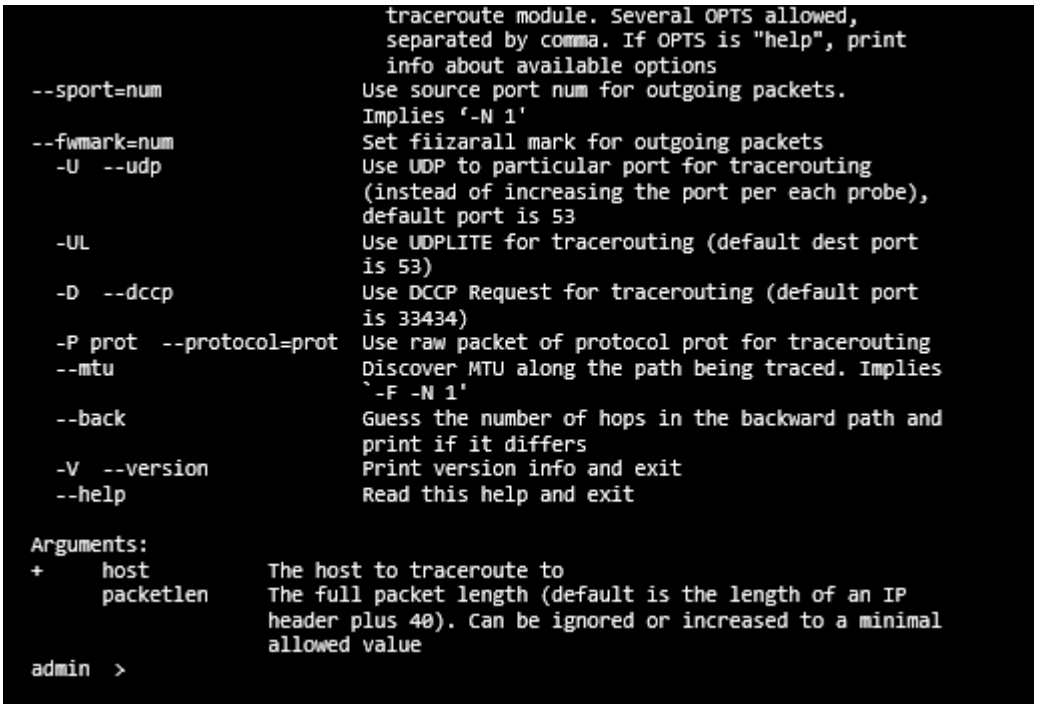
How to use:

```
admin  >traceroute --help
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m
max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [
-q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]


Options:
  -4                          Use IPv4
  -6                          Use IPv6
  -d  --debug                 Enable socket level debugging
  -F  --dont-fragment         Do not fragment packets
  -f first_ttl  --first=first_ttl
                              Start from the first_ttl hop (instead from 1)
  -g gate,...  --gateway=gate,...
                              Route packets through the specified gateway
                              (maximum 8 for IPv4 and 127 for IPv6)
  -I  --icmp                  Use ICMP ECHO for tracerouting
  -T  --tcp                   Use TCP SYN for tracerouting (default port is 80)
  -i device  --interface=device
                              Specify a network interface to operate with
  -m max_ttl  --max-hops=max_ttl
                              Set the max number of hops (max TTL to be
                              reached). Default is 30
  -N squeries  --sim-queries=squeries
                              Set the number of probes to be tried
                              simultaneously (default is 16)
  -n                          Do not resolve IP addresses to their domain names
  -p port  --port=port
                           Set the destination port to use. It is either
                              initial udp port value for "default" method
                              (incremented by each probe, default is
                              33434), or initial seq for "icmp" incremented
                              as well, default from 1), or some constant
                             destination port for other methods (with default of 80
for "tcp", 53 for "udp", etc.)
```

Command Line Interface – traceroute_1

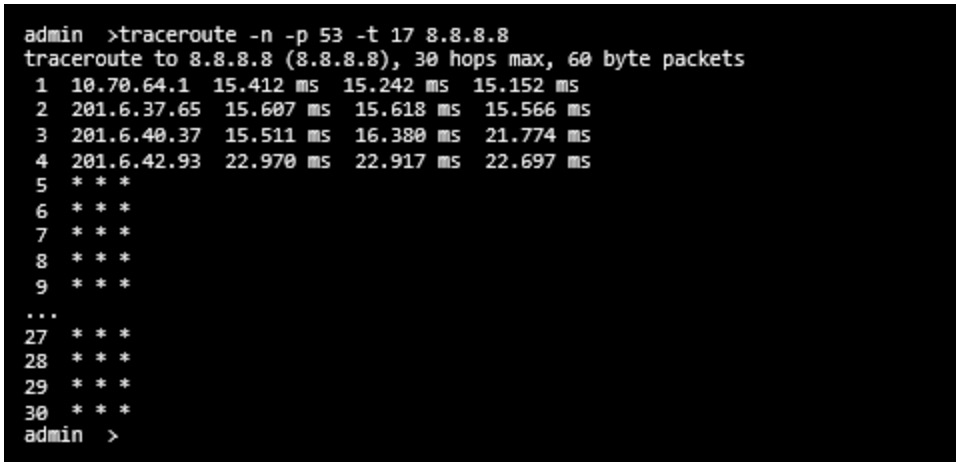


Command Line Interface – traceroute_2



Command Line Interface – traceroute_3

Example: Tests to map the routing or path to Google's DNS IP address, IP 8.8.8.8 in the UDP protocol (17):

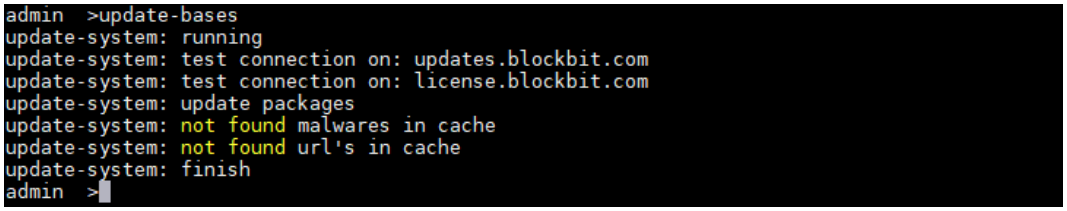


Command Line Interface – traceroute – Example 1

UTM - [update-bases]

Used for verification, Download and installation of Blockbit UTM bases.

How to use:



Command Line Interface – update-bases

UTM - [update-license]

Used to register the BLOCKBIT UTM through the CLI. The license must be typed in front of the command. The **[update-license]** should only be used if the license is deactivated and released by BLOCKBIT for activation, it is extremely important to keep in mind that: If this command is executed when the license is already activated it will be DEACTIVATED.

How to use:

Command Line Interface – update-license

Attention to the proper use of the [update-license] command: If the command is executed twice, or if it is executed when the license is active, it will be DISABLED. In addition, for the correct use of this command, it must be released to be able to register it correctly.

UTM - [update-system]

Used to check, Download and install the update packages for Blockbit NGFW.

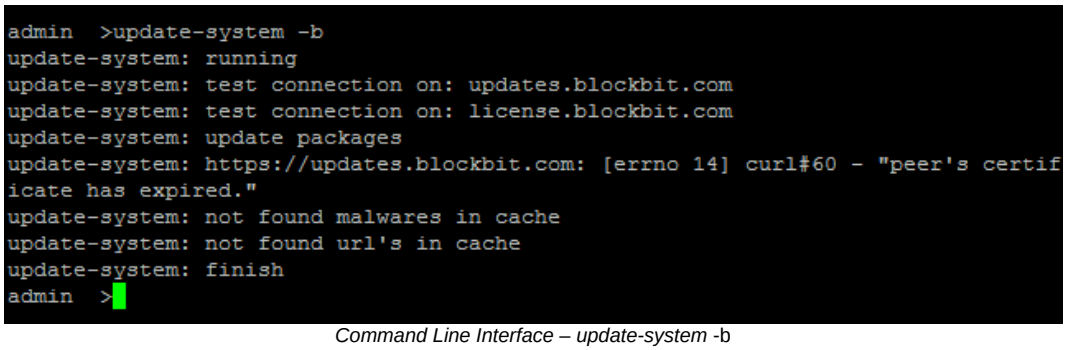
How to use:

Command Line Interface – update-system

This command also has the following parameters:

update-system -b

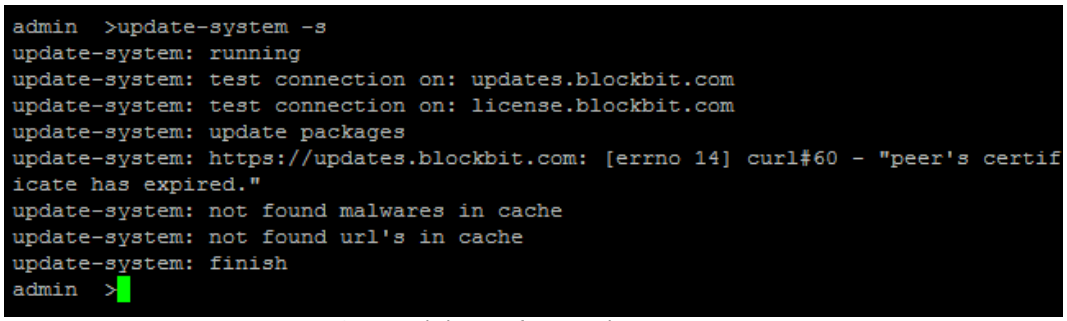
Used to specifically update the system's subscription base and security feeds;



Command Line Interface – update-system -b

update-system -s

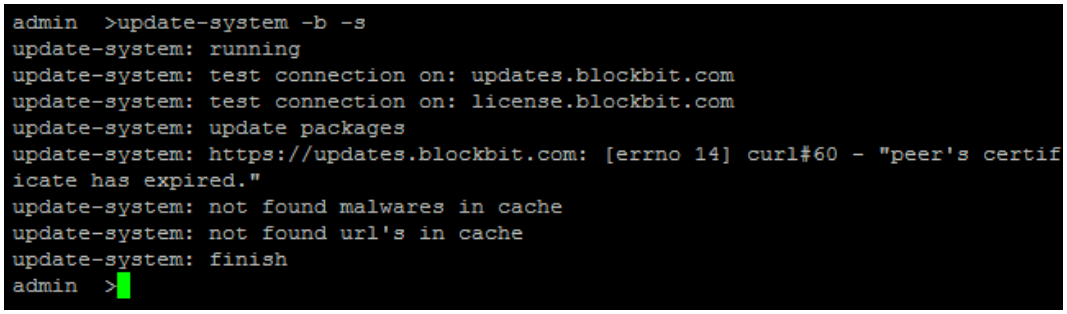
It is used to update the system, bug fixes and new features;



Command Line Interface – update-system -s

update-system -b -s

Performs the complete system update: Performs system updates, bug fixes, new features, subscription base and security feeds.



Command Line Interface – update-system -b -s

UTM - [upgrade-blockbit]

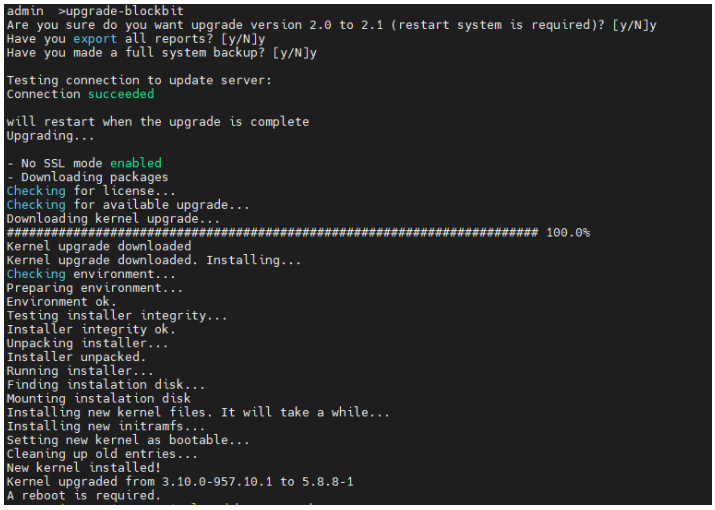
This command is used to check, download and upgrade Blockbit UTM to the most current version.

ATTENTION: We ALWAYS recommend that a FULL BACKUP of the latest system version and reports be made before any update or upgrade procedure is performed and that the files are saved in a safe place.

When running the command, the system will ask the user to confirm that all reports have been exported and that a system backup has been generated. For the command to be executed, this double confirmation from the user will be necessary.

WARNING: At the end of the execution of this command, it will be necessary to restart your UTM.

How to use:



Command Line Interface – upgrade-blockbit

Important:

During the upgrade process of the Blockbit Platform version 2.2.2 to the Blockbit Platform version 2.4.0, a message informing that the upgrade was not successfully completed may be shown. **This message occurs due to a change done in our upgrade repository,** which causes the system to upgrade straight to the 2.4.0 version instead of the 2.3.0, as the upgrade command expects to receive by the end of the process.

Here is an example:

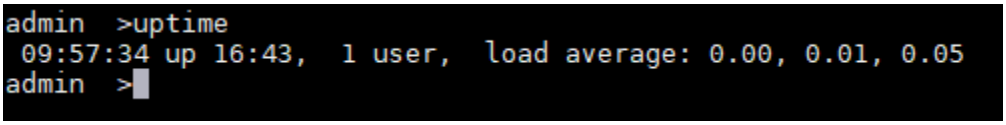
1. The first rectangle shows both the current version and build of the system:2.2.2;
2. The second highlighted area shows that the command requests a confirmation for upgrading the system from the 2.2 version to the 2.3 from the user;
3. On the third, the error message, because the system did not identify that the new version is the 2.3;
4. However, the system has been successfully upgraded to the 2.4.0 version.

And so, the upgrade has been successfully completed, and the message can be ignored. However, in case there is any doubts or problems, we kindly ask you to check your services' status and, if necessary, please contact our Customer Support.

UTM - [uptime]

Displays how long the server has been in operation.

How to use:



Command Line Interface – uptime

UTM - [vmstat]

Reports information about processes, memory, pagination, block I / O and CPU activities.

How to use:

```
[root@vcm bin]# vmstat --help

Usage:
 vmstat [options] [delay [count]]

Options:
 -a, --active           active/inactive memory
 -f, --forks            number of forks since boot
 -m, --slabs            slabinfo
 -n, --one-header       do not redisplay header
 -s, --stats            event counter statistics
 -d, --disk             disk statistics
 -D, --disk-sum         summarize disk statistics
 -p, --partition <dev>  partition specific statistics
 -S, --unit <char>      define display unit
 -w, --wide             wide output
 -t, --timestamp        show timestamp

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see vmstat(8).
[root@vcm bin]#
```

Command Line Interface – vmstat

Example:

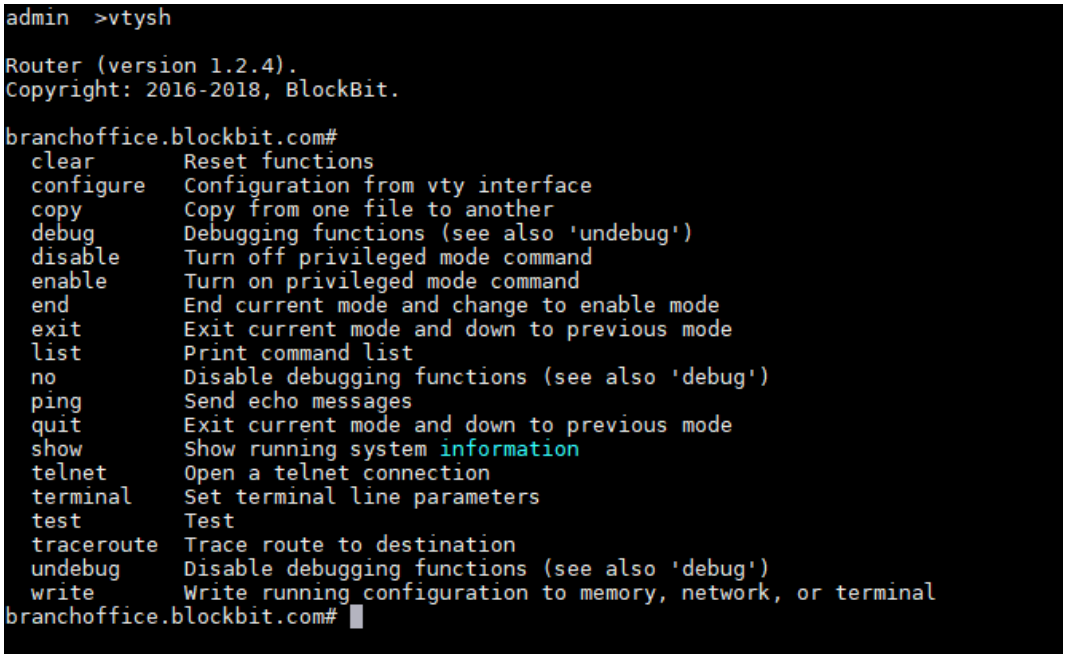
```
[root@vcm bin]# vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 1  0      0 1816712 182256 1040896    0    0     0     2   23    5  0  0 100  0  0
[root@vcm bin]#
```

Command Line Interface – vmstat - Example

UTM - [vtysh]

This command is used to open a shell interface integrated in the dynamic routing engines.

How to use:

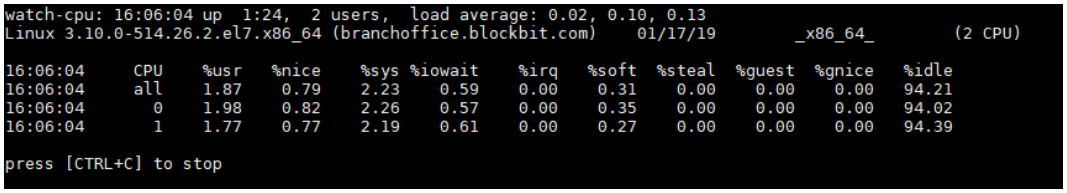


Command Line Interface – vtysh

UTM - [watch-cpu]

Monitors real-time usage of server processors.

How to use:

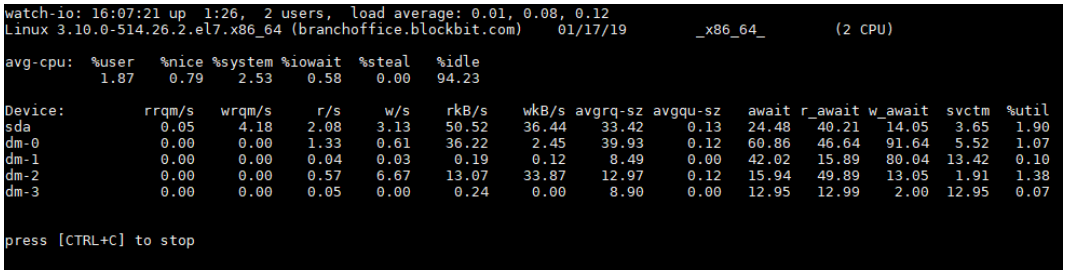


Command Line Interface – watch-cpu

UTM - [watch-io]

Monitors in real time the use of server I / O (use of writing and reading from disk).

How to use:



Command Line Interface – watch-io

UTM - [watch-mem]

Monitors server memory usage in real time.

How to use:

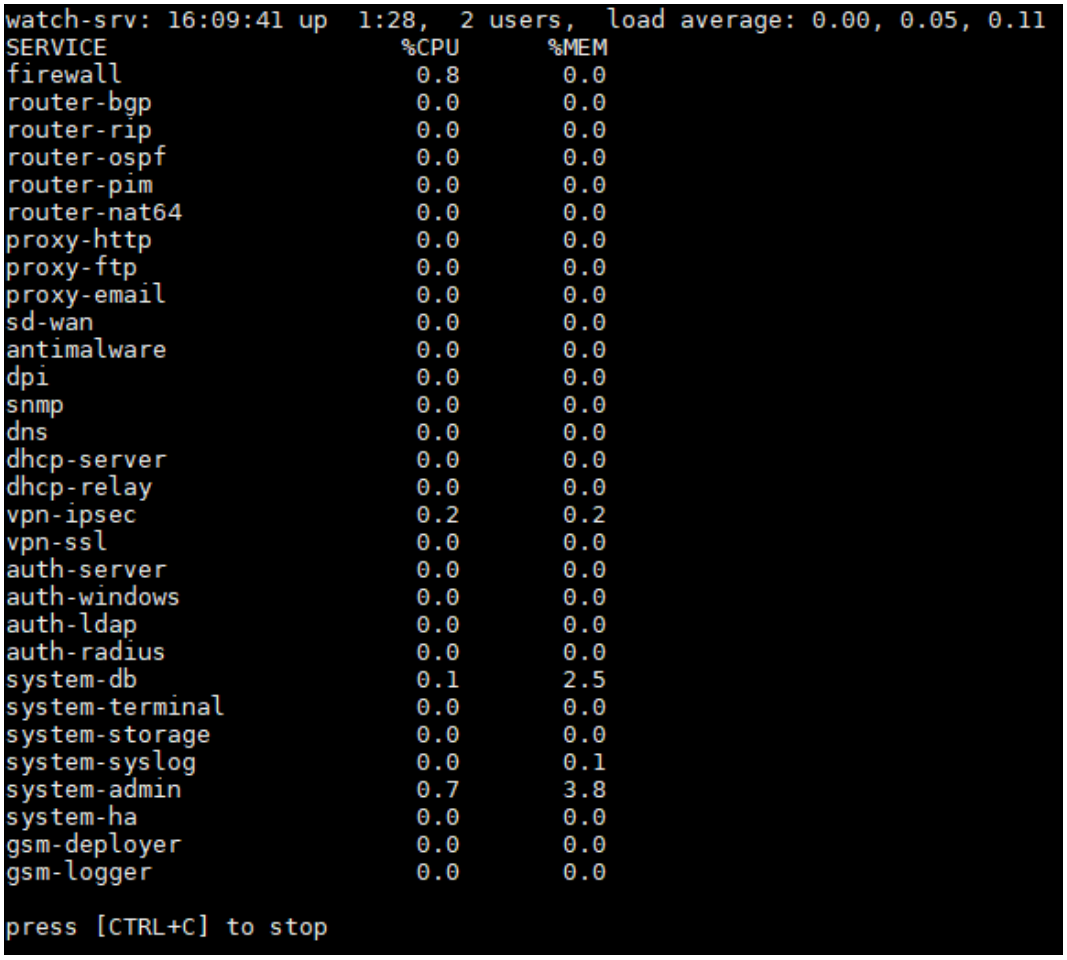
```
watch-mem: 16:08:38 up  1:27,  2 users,  load average: 0.00, 0.06, 0.11
              total        used        free      shared  buff/cache   available
Mem:        4047164      331804     3268380       94588      446980     3352132
Swap:       1653756           0     1653756

press [CTRL+C] to stop
```

Command Line Interface – watch-mem

UTM - [watch-srv]

Monitors the processing and memory usage of each service in real time.

How to use:



Command Line Interface – watch-srv

UTM - [wc]

Line count counter for the output of a command.

Example: Check the number of authenticated users on the server:

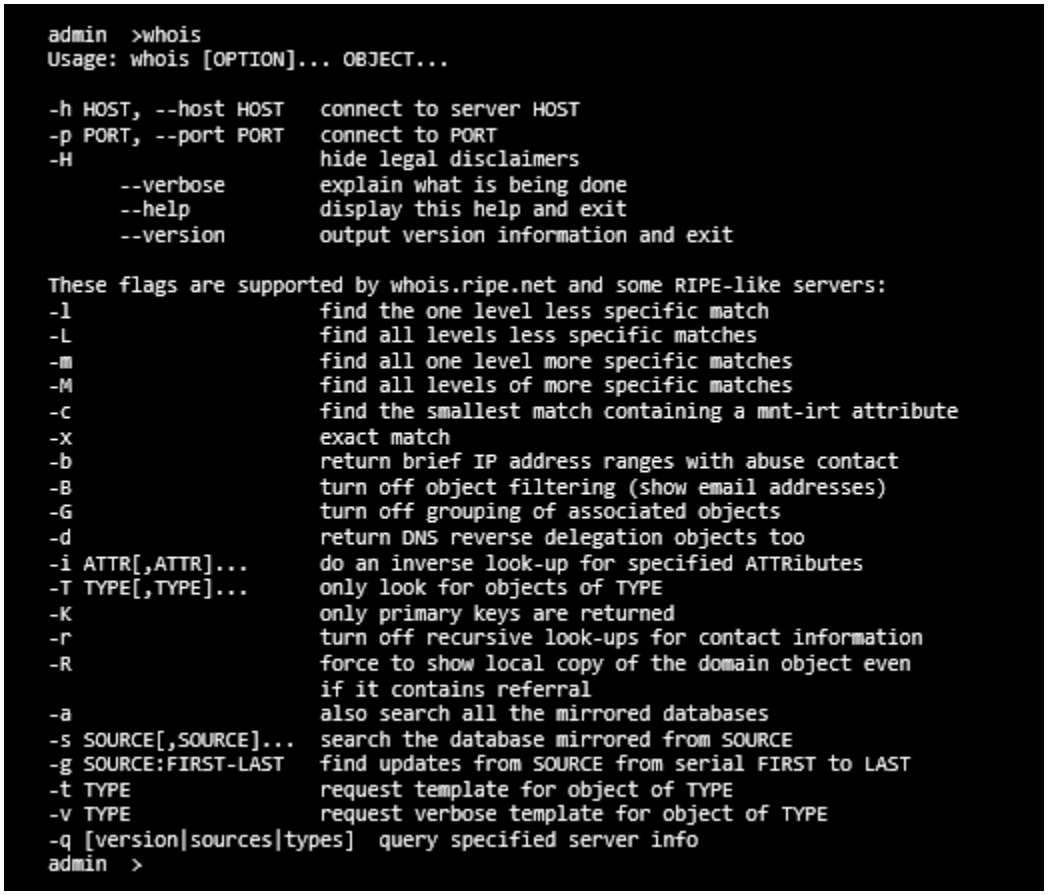
```
admin  >show-sessions|wc -l
1
```

Command Line Interface – wc

UTM - [whois]

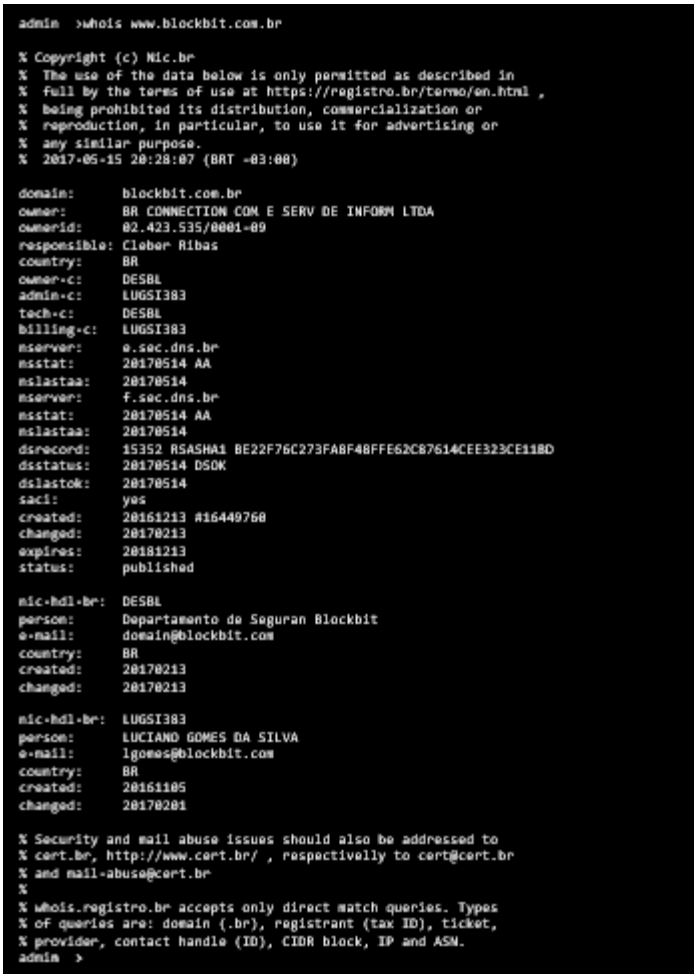
Utilizado para consultar a informação sobre um domínio de *Internet*.

Modo de uso:



Command Line Interface – whois

Exemplo: Saída padrão do comando:



Command Line Interface – whois – Example

Blockbit

it's easy to be secure

www.blockbit.com

UTM - [wifi-cli]

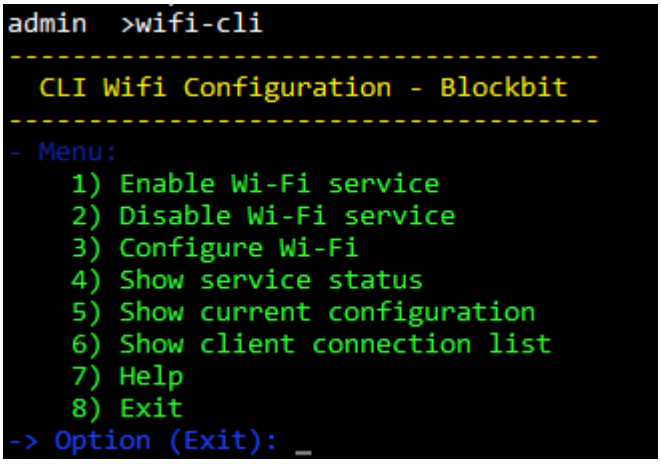
Allows access to the service's configuration:

How to use:

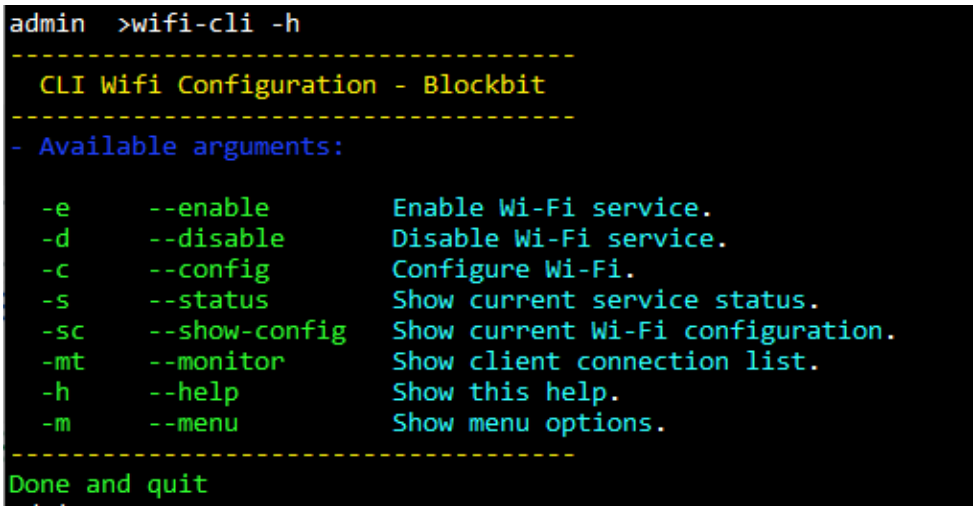
admin > wifi-cli

Uso: wifi-cli <enable|disable|status|config|monitor>

--enable: Enables the service
--disable: Disables the service
--status: Checks the service status
--config: Interactive configuration
--monitor: Displays the connected users



Command Line Interface – wifi-cli



Command Line Interface - wifi-cli -h

Next, we have a description with the variations of the command:

-e --enable: Enables the service.

-d --disable: Disables the service.

-c --config: Shows the Wi-Fi settings.

-s --status: Shows the services' current status.

-sc --show-config: Displays the current Wi-Fi settings.

-mt --monitor: Displays the list of connected hosts.

-h --help: Shows this help menu.

-m --menu: Displays the options menu.

NGFW - [logoff-wmi]

This command controls the number of accesses from the same IP by enabling the WMI Logoff function. When active, the WMI takes down the session at the logoff. When other user logins using the same IP, his last session will resume.

Commands

`enable-logoff-wmi`

Enables WMI Logoff.

`disable-logoff-wmi`

Disables WMI Logoff.

NGFW - [deepinspect]

This command manages the nDPI (Deep Packet Inspection), that monitors the network and does advanced traffic analysis.

To run this command, you have to first integrate the GSM/Analyzer, where the nDPI logs will be stored.

Commands:

Enable nDPI:

```
enable-deepinspect
```

Disable nDPI.

```
disable-deepinspect
```

NGFW - [AdminCoreReserv]

This command reserves the system last used CPU for critical system administration components. Ex: web server or database.

```
AdminCoreReserve --enable
```

Enable

```
AdminCoreReserve --disable
```

Disable (default)

```
AdminCoreReserve --status
```

Show status.

NGFW - [recovery]

If an Admin user has lost its password, access the CLI and follow these steps:

1 - type the following command in the "user" field:

```
recovery
```

2 - A Challenge will be generated.
Example:

```
 03e613782e10d5b4bc41473312f1bf65
```

3 - Contact Blockbit and provide the Challenge.

4 - A provisory password will be given to you.
 - Insert your username and provisory password.

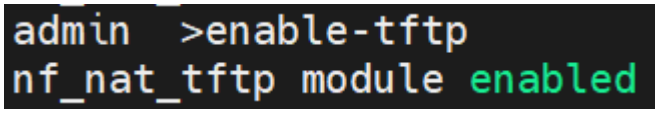
5 - You will be asked to create a new password.

6 - After creating a new password, logoff and enter again with your username and new password.

UTM - [enable-tftp]

Enable file transfer, similar to FTP protocol.

How to use:



Command Line Interface – [enable-tftp]

UTM - [enable-pptp]

Enable the usage of virtual private networks.

How to use:

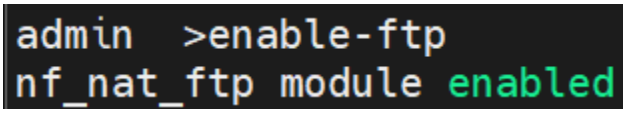
```
admin  >enable-pptp
nf_nat_pptp module enabled
```

Command Line Interface – [enable-pptp]

UTM - [enable-ftp]

Enable file tranfer between client/server connections.

How to use:

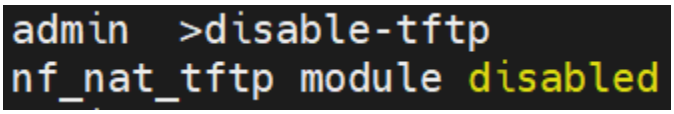


Command Line Interface – [*enable-ftp]*

UTM - [disable-tftp]

Disable file transfer, similar to FTP protocol.

How to use:



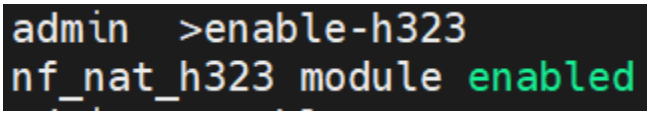
Command Line Interface – [disable-tftp]

Disables only the service, the settings will remain.

UTM - [enable-h323]

Enable multimedia communication systems.

How to use:



Command Line Interface – [enable-h323]

NGFW - [simet]

Simet is a command to measure internet connection speed using the simet.nic.br service. You can check download speed, upload speed, and latency (ping) directly from the terminal without accessing the website.

Command	Description
simet -e	Enables the service in the network.
simet -d	Disables the service.
simet -s	Shows the service status.
simet -r	Saves the test URL.
simet -u	Shows the test URL.
simet -t	Executes the speed test.

Simet uses two services:

- **simet-ma**: measures internet connection availability. For service logs, use the command **simet -m**.
- **simet-lmapd**: measures in the background. For service logs, use the command **simet -l**.

The connection speed is estimated and relative, and it may differ from the performance you experience when using the internet. The value provided by Simet should not be used for documentation purposes.

The difference between the estimated and experienced speed can be due to the following factors:

- **Server location**: The closer the server, the higher the speed.
- **Network congestion and routing**: Tests do not capture traffic variation.
- **Equipment limitations**: Devices may limit speed.
- **Traffic prioritization or bandwidth usage by other devices**.

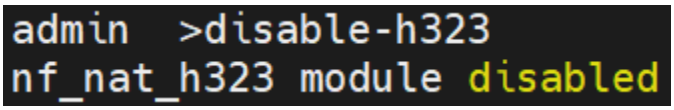
To obtain a more realistic measure, you can:

- Test at different times.
- Test with different servers.

UTM - [disable-h323]

Disable multimedia communication systems.

How to use:



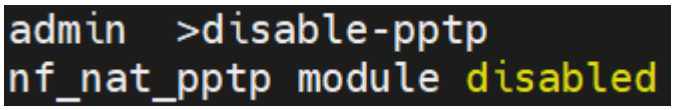
Command Line Interface – [disable-h323]

Disables only the service, the settings will remain.

UTM - [disable-pptp]

Disable the usage of virtual private networks.

How to use:



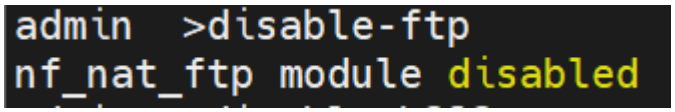
Command Line Interface – [*disable-pptp]*

Disables only the service, the settings will remain.

UTM - [disable-ftp]

Disable file tranfer between client/server connections.

How to use:



Command Line Interface – [disable-ftp]

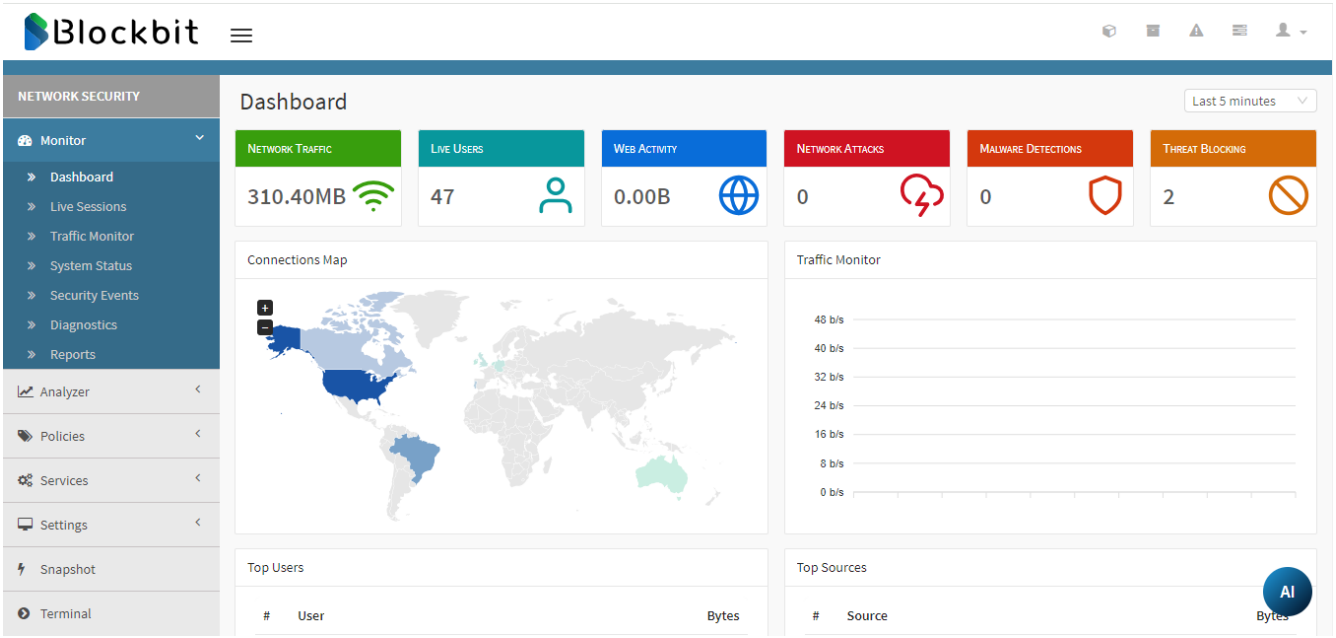
Disables only the service, the settings will remain.

NGFW - CHAT AI

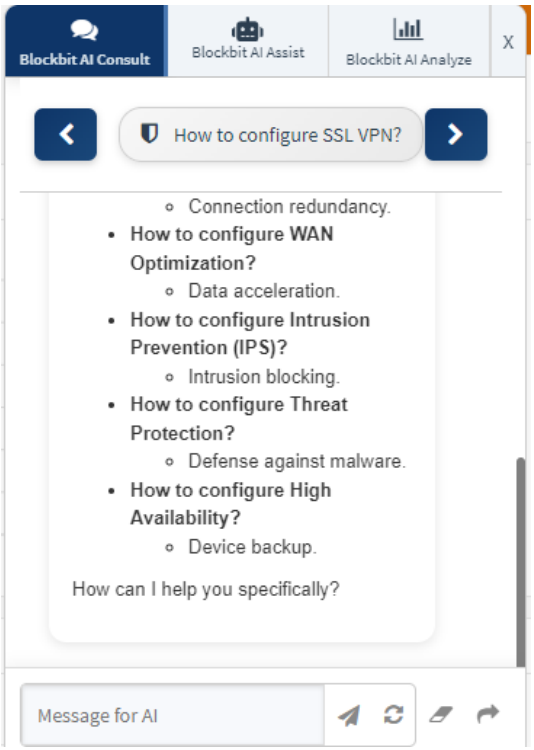
To make your network security even easier, the Blockbit NGFW provides Chat AI.

The artificial intelligence of the Blockbit NGFW answers questions, configures your network, and even compares configurations so you know exactly what has been changed.

To access Chat AI, click the button  in the bottom right corner of the screen.



A message box will open:



The box has 3 tabs. To learn more, visit:

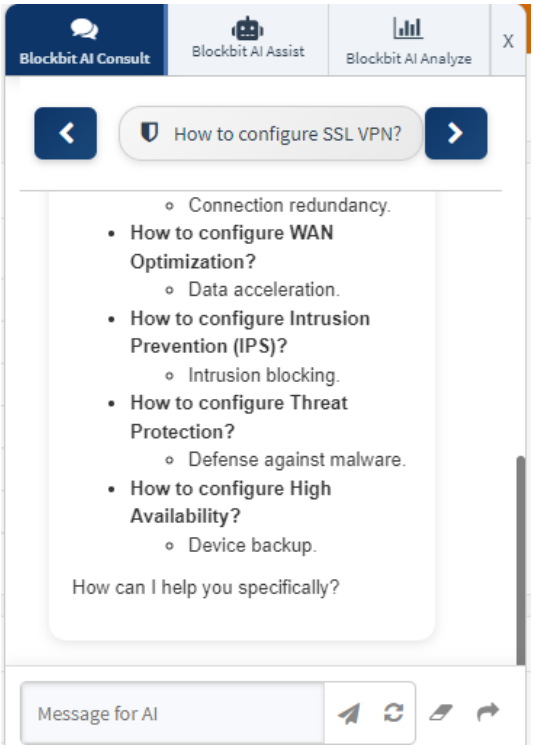
Blockbit AI Consult

Blockbit AI Assist

Blockbit AI Analyze

Blockbit AI Consult

This tab answers questions by applying Artificial Intelligence to the Blockbit knowledge base.



To ask Blockbit AI, use the Message for AI field. After typing a question, press **Enter** for the AI to respond to your question.

Next to the field, there are 4 buttons:

Send Message ( ): send a message to the AI. Once a message is sent, the button changes to stop ( ). Clicking it aborts the action;

New Chat ( ): clears messages and responses in the chat;

Clear Memory ( ): erases the learning from the last chat session;

Export Rules ( ): downloads a file with the rules created in the session.

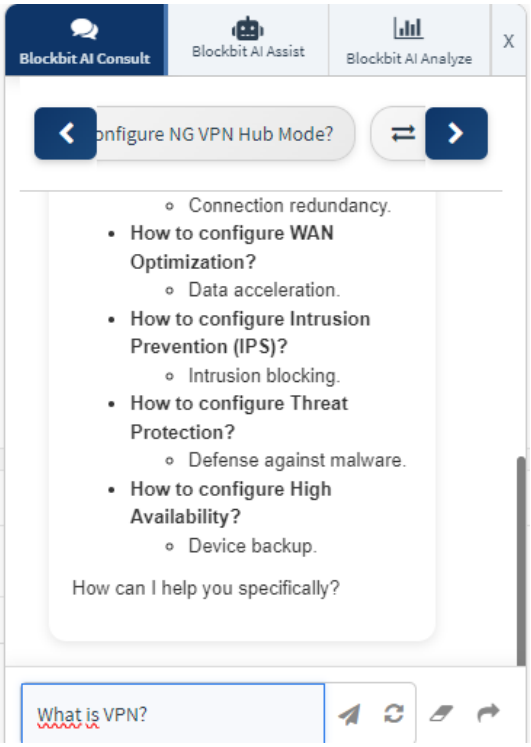
At the top of the message box, there are some frequently asked questions.

Clicking on any of the questions will prompt the AI to respond as usual.

For an example, visit the How To.

Blockbit AI Consult - How to

To search in Chat AI, enter your question in the message box;



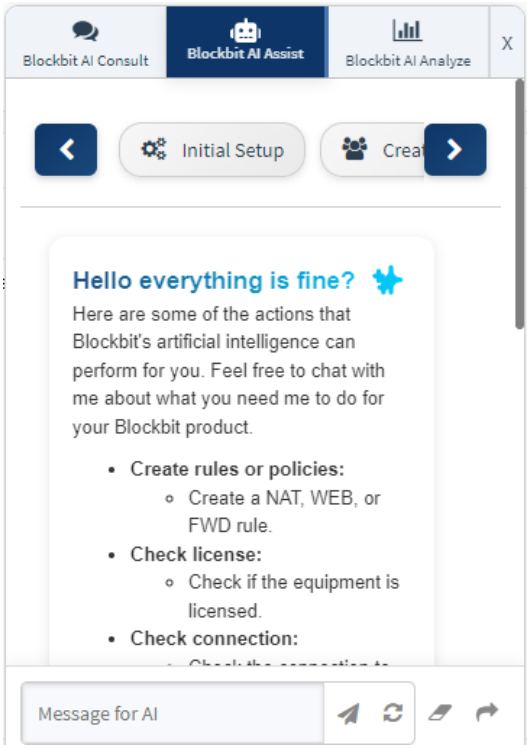
Here, a question about what a VPN is was asked to the AI.

Press **Enter** or click on **Send Message** ( ).

The AI will respond according to the knowledge base.

Blockbit AI Assist

This tab creates configurations automatically.



To ask Blockbit AI to create a configuration, use the Message for AI field.

After typing a request, press **Enter** to automatically create the configuration.

If the request is unclear, the Artificial Intelligence will ask more questions to create accurate configurations.

Next to the field, there are 4 buttons:

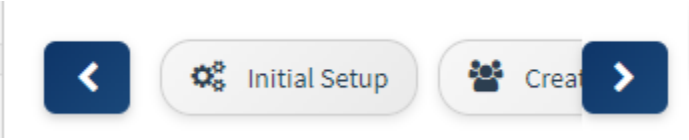
Send Message ( ): send a request to the AI. Once a request is sent, the button changes to stop ( ). Clicking it aborts the action;

New Chat ( ): clears messages and responses in the chat;

Clear Memory ( ): erases the learning from the last chat session;

Export Rules ( ): downloads a file with the rules created in the session.

At the top of the message box, there are some frequent requests.



Clicking on any of the requests will prompt the AI to create a configuration.

For an example, visit the How To.

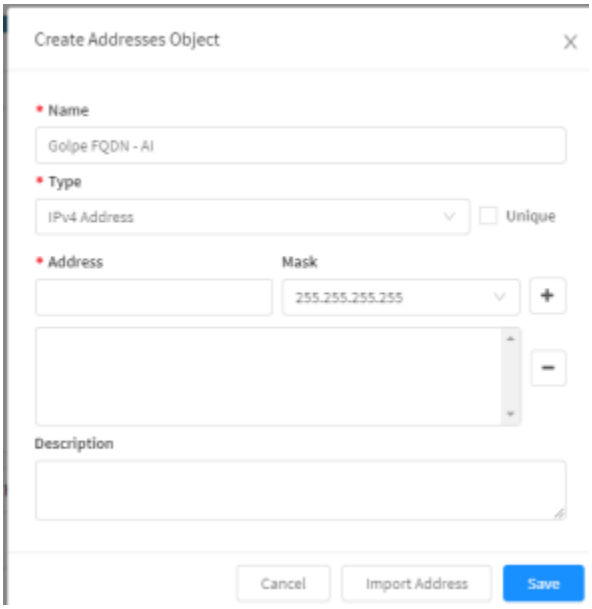
Blockbit AI Assist- How to

To create a policy, click on the Blockbit AI Assist tab and type your request:

In the example, a request was made to block the fictional site www.golpe.com.

Press **Enter** or click on **Send Message** ( ).

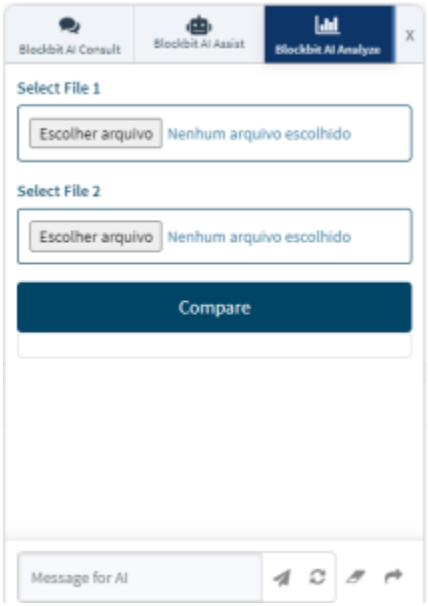
The AI will automatically create an object for the site and a blocking policy.



Click save and apply it in the queue.

Blockbit AI Analyze

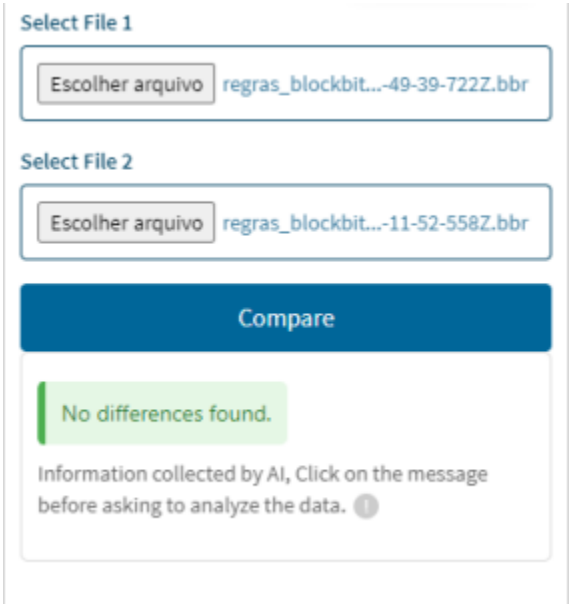
This tab allows you to compare configuration files.



The chat only compares **.bbr** type files. These files contain policies created by Blockbit AI and are downloaded using the **Export Rules** ( ) button.

To compare, click **Choose file** in the first field and select file 1. Then, click Choose file in the **second field** and select file 2.

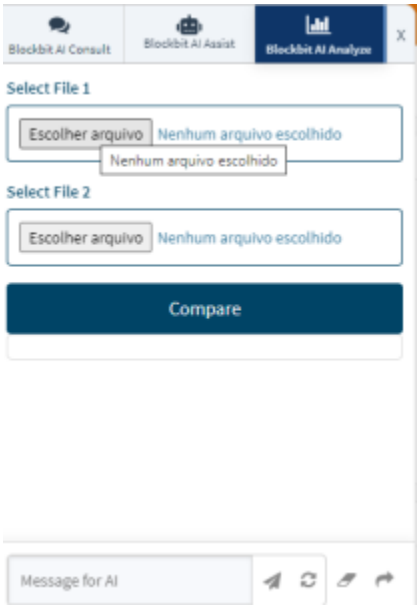
When you click **Compare**, the AI will list the differences between the files.



For an example, visit the How To.

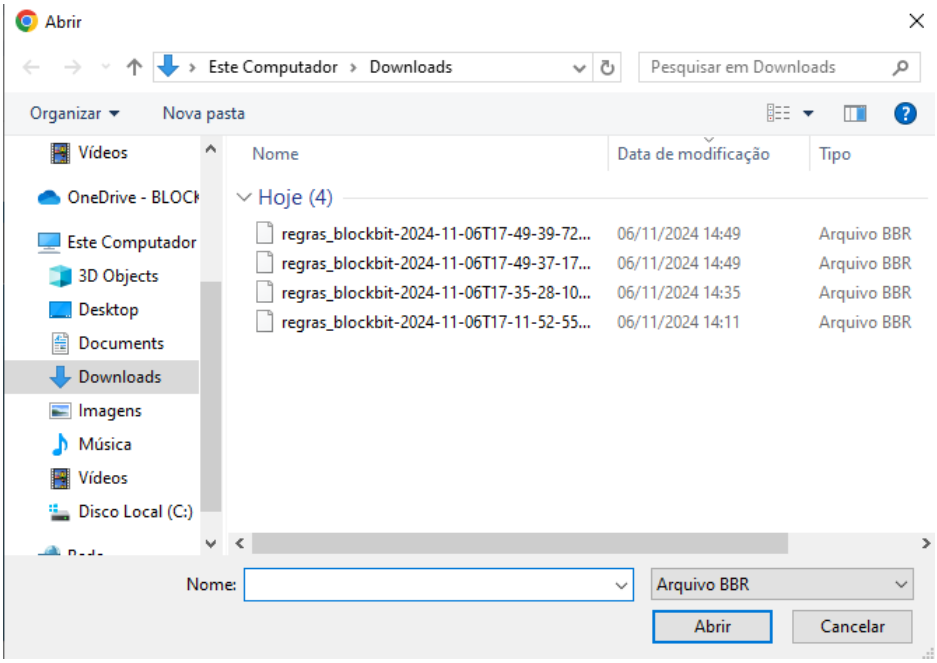
Blockbit AI Analyze - How to

To compare two files, click on the Blockbit AI Analyze tab.



In the Select File 1 field, click **Choose file**.

Your local directory will open.



Select a file.

Repeat these steps in the Select File 2 field, choosing a different file.

Press **Compare**.

The AI will compare the two files and show the differences.

In this case, the two files have no differences.