

# GCC601X(W) Firewall - User Manual

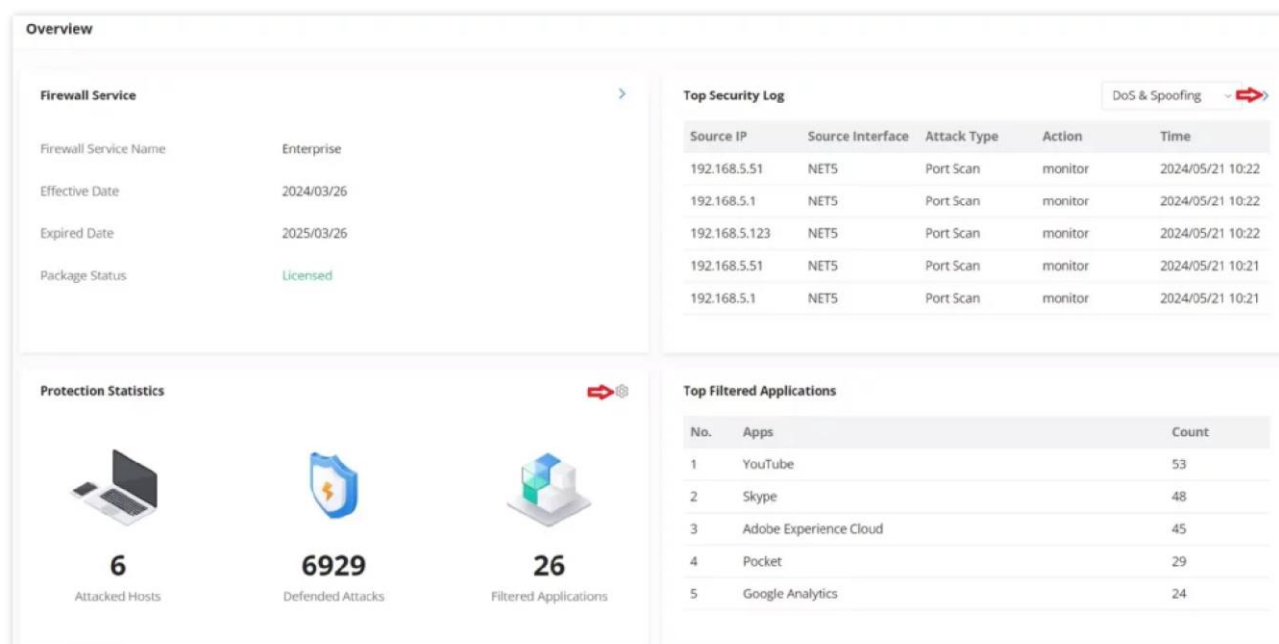
In this guide, we will introduce the configuration parameters of the GCC601X(W) Firewall Module.

## OVERVIEW

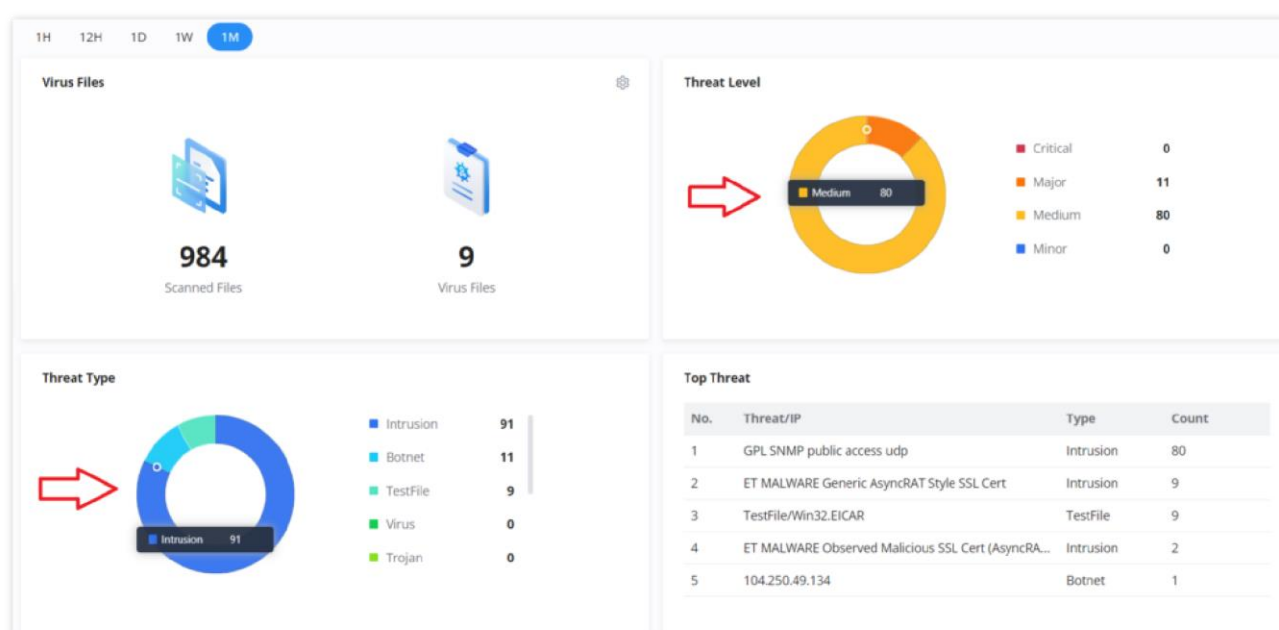
The overview page provides the users with a global insight into the GCC firewall module and also security threats and statistics, the overview page contains:

- **Firewall Service:** displays the firewall service and package status with effective and expired dates.
- **Top Security Log:** shows the top logs for each category, the user can select the category from the drop-down list or click on the arrow icon to get redirected to the security log page for more details.
- **Protection Statistics:** displays various protections statistics, there is an option to clear all the statistics by clicking on the settings icon.
- **Top Filtered Applications:** shows the top applications that have been filtered with count number.
- **Virus Files:** displays the scanned files and found virus files as well, to enable/disable the anti-malware the users can click on the settings icon.
- **Threat Level:** shows the threat level from critical to minor with color code.
- **Threat Type:** displays the threat types with color code and number of repetition, the users can hover the mouse cursor over the color to display the name and the number occurrence.
- **Top Threat:** shows top threats with type and count.

The users can easily spot the most important notifications and threats.



Overview part 1



Overview part 2

The users can click on the **arrow icon** under Top Security Log to get redirected to the Security Log section, or hover over the **gear icon** under Protection Statistics to clear the statistics or under Virus files to disable the Anti-malware. Under Threat Level and Threat Type, users can also hover over the graphs to show more details. Please refer to the figures above.

# FIREWALL POLICY

## Rules Policy

Rules policy allows to define of how the GCC device will handle the inbound traffic. This is done per WAN, VLAN, and VPN.

Group	Inbound Policy	IP Masquerading	MSS Clamping	Log Drop / Reject Traffic	Drop / Reject Traffic Limit	Operations
Default	Accept	Disabled	Disabled	Disabled	10/second	
WAN3	Reject	Enabled	Enabled	Disabled	10/second	
WAN2	Reject	Enabled	Enabled	Disabled	10/second	
WAN1	Reject	Enabled	Enabled	Disabled	10/second	
Guests	Accept	Disabled	Disabled	Disabled	10/second	
TechSupport	Accept	Disabled	Disabled	Disabled	10/second	

Rules Policy page

Rules Policy > WAN1

Inbound Policy  Accept  Reject  Drop

IP Masquerading

MSS Clamping

Log Drop / Reject Traffic

Drop / Reject Traffic Log Limit   The range is 1~99999999, if it is empty, there is no limit

- second
- minute
- hour
- day

Rules Policy – Edit

- **Inbound Policy:** Define the decision that the GCC device will take for the traffic initiated from the WAN or VLAN. The options available are Accept, Reject, and Drop.
- **IP Masquerading:** Enable IP masquerading. This will masquerade the IP address of the internal hosts.
- **MSS Clamping:** Enabling this option will allow the MSS (Maximum Segment Size) to be negotiated during the TCP session negotiation
- **Log Drop / Reject Traffic:** Enabling this option will generate a log of all the traffic that has been dropped or rejected.
- **Drop / Reject Traffic Log Limit:** Specify the number of logs per second, minute, hour or day. The range is 1~99999999, if it is empty, there is no limit.

## Inbound Rules

The GCC601X(W) allows to filtering of incoming traffic to networks group or port WAN and applies rules such as:

- **Accept:** To allow the traffic to go through.
- **Deny:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

Name	Status	IP Family	Protocol Type	Source Group	Source MAC Address	Source IP Address	Source Port	Dest	Operations
Anti-lockout-Rule	<input checked="" type="checkbox"/>	Any	TCP	Default (VLAN)	-	-	-	-	
Allow-DHCP-Ren...	<input checked="" type="checkbox"/>	IPv4	UDP	WAN1 (WAN)	-	-	-	-	
Allow-Ping	<input checked="" type="checkbox"/>	IPv4	ICMP	WAN1 (WAN)	-	-	-	-	
Allow-IGMP	<input checked="" type="checkbox"/>	IPv4	IGMP	WAN1 (WAN)	-	-	-	-	
Allow-DHCPv6	<input checked="" type="checkbox"/>	IPv6	UDP	WAN1 (WAN)	-	fe80::/10	-	fe80	
Allow-MLD	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN1 (WAN)	-	fe80::/10	-	-	
Allow-ICMPv6-In...	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN1 (WAN)	-	-	-	-	
Allow-DHCP-Ren...	<input checked="" type="checkbox"/>	IPv4	UDP	WAN2 (WAN)	-	-	-	-	
Allow-Ping	<input checked="" type="checkbox"/>	IPv4	ICMP	WAN2 (WAN)	-	-	-	-	
Allow-IGMP	<input checked="" type="checkbox"/>	IPv4	IGMP	WAN2 (WAN)	-	-	-	-	
Allow-DHCPv6	<input checked="" type="checkbox"/>	IPv6	UDP	WAN2 (WAN)	-	fe80::/10	-	fe80	
Allow-MLD	<input checked="" type="checkbox"/>	IPv6	ICMP	WAN2 (WAN)	-	fe80::/10	-	-	

Firewall Policy – Inbound Rules

Inbound Rules > Add Inbound Rule

**Name**  1-64 characters

**Status**

**IP Family**  Any  IPv4  IPv6

**Protocol Type**

**Source Group**

**Source MAC Address**

**Source IP Address**  Enter the IP address/mask length, such as "192.168.122.0/24"

**Source Port**  The valid range is 1-65535. You can enter a single port or a port range.

**Destination IP Address**  Enter the IP address/mask length, such as "192.168.122.0/24"

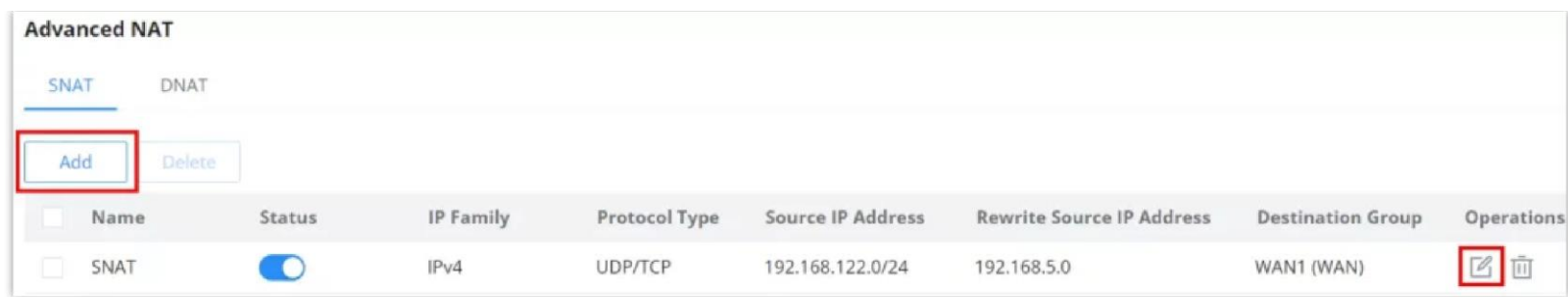
**Destination Port**  The valid range is 1-65535. You can enter a single port or a port range.

**Action**  Accept  Deny  Drop

Inbound Rules – Add/Edit

<b>Name</b>	Enter the name of the inbound rule.
<b>Status</b>	Toggle on/off the status of the inbound rule.
<b>IP Family</b>	Pick the IP family. <ul style="list-style-type: none"> <li>• Any</li> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Protocol Type</b>	Choose the protocol type. <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• UDP/TCP</li> <li>• ICMP</li> <li>• IGMP</li> <li>• All</li> </ul>
<b>Source Group</b>	If set to "All", rules will be matched in preference to other specific ones.
<b>Source MAC Address</b>	Specify the source MAC address.
<b>Source IP Address</b>	Specify the source IP address.
<b>Source Port</b>	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.





SNAT page

Add SNAT

Refer to the below table when creating or editing an SNAT entry:

<b>Name</b>	Specify a name for the SNAT entry
<b>IP Family</b>	Select the IP version, two options are available: IPv4 or Any.
<b>Protocol Type</b>	Select one of the protocols from dropdown list or All, available options are: UDP/TCP, UDP, TCP and All.
<b>Source IP Address</b>	Set the Source IP address.
<b>Rewrite Source IP Address</b>	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
<b>Source Port</b>	Set the Source Port
<b>Rewrite Source Port</b>	Set the Rewrite source port.
<b>Destination Group</b>	Select a WAN interface or a VLAN for Destination Group.
<b>Destination IP Address</b>	Set the Destination IP address.
<b>Destination Port</b>	Set the Destination Port

SNAT page

## DNAT

To add a DNAT click on the "Add" button to add a new DNAT or click on the "Edit" icon to edit a previously created one. Refer to the figures and table below:

*Advanced NAT – DNAT*

Refer to the below table when creating or editing a DNAT entry:

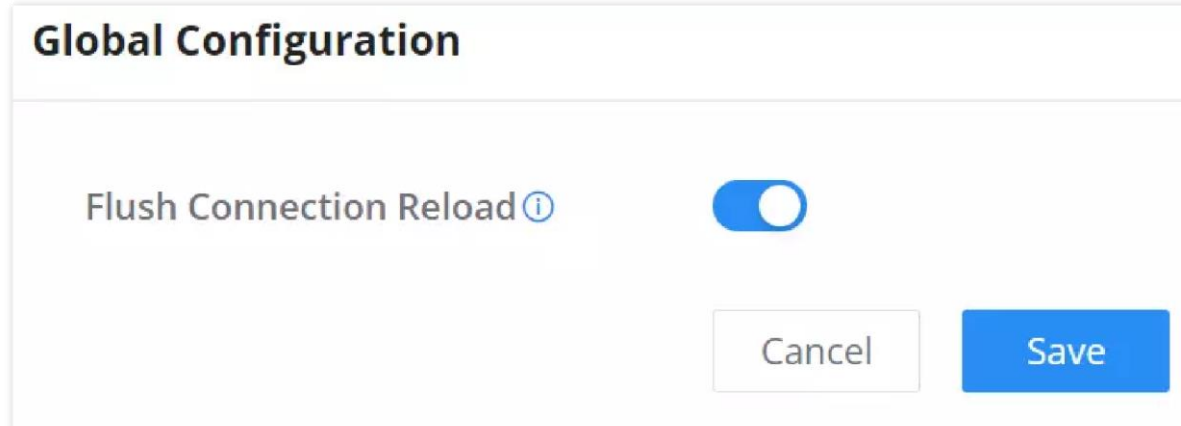
<b>Name</b>	Specify a name for the DNAT entry
<b>IP Family</b>	Select the IP version, three options are available: IPv4, IPv6 or Any.
<b>Protocol Type</b>	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
<b>Source Group</b>	Select a WAN interface or a LAN group for Source Group, or select All.
<b>Source IP Address</b>	Set the Source IP address.
<b>Source Port</b>	Set the Source Port.
<b>Destination Group</b>	Select a WAN interface or a LAN group for Destination Group, or select All. Make sure that destination and source groups are different to avoid conflict.
<b>Destination IP Address</b>	Set the Destination IP address.
<b>Rewrite Destination IP Address</b>	Set the Rewrite Destination IP Address.
<b>Destination Port</b>	Set the Destination Port.
<b>Rewrite Destination Port</b>	Set the Rewrite Destination Port
<b>NAT Reflection</b>	Click on " <b>ON</b> " to enable NAT Reflection
<b>NAT Reflection Source</b>	Select NAT Reflection either Internal or External.

## Global Configuration

- **Flush Connection Reload**

When this option is enabled and the firewall configuration changes are made, existing connections that had been permitted by the previous firewall rules will be terminated.

If the new firewall rules do not permit a previously established connection, it will be terminated and will not be able to reconnect. With this option disabled, existing connections are allowed to continue until they timeout, even if the new rules would not allow this connection to be established.



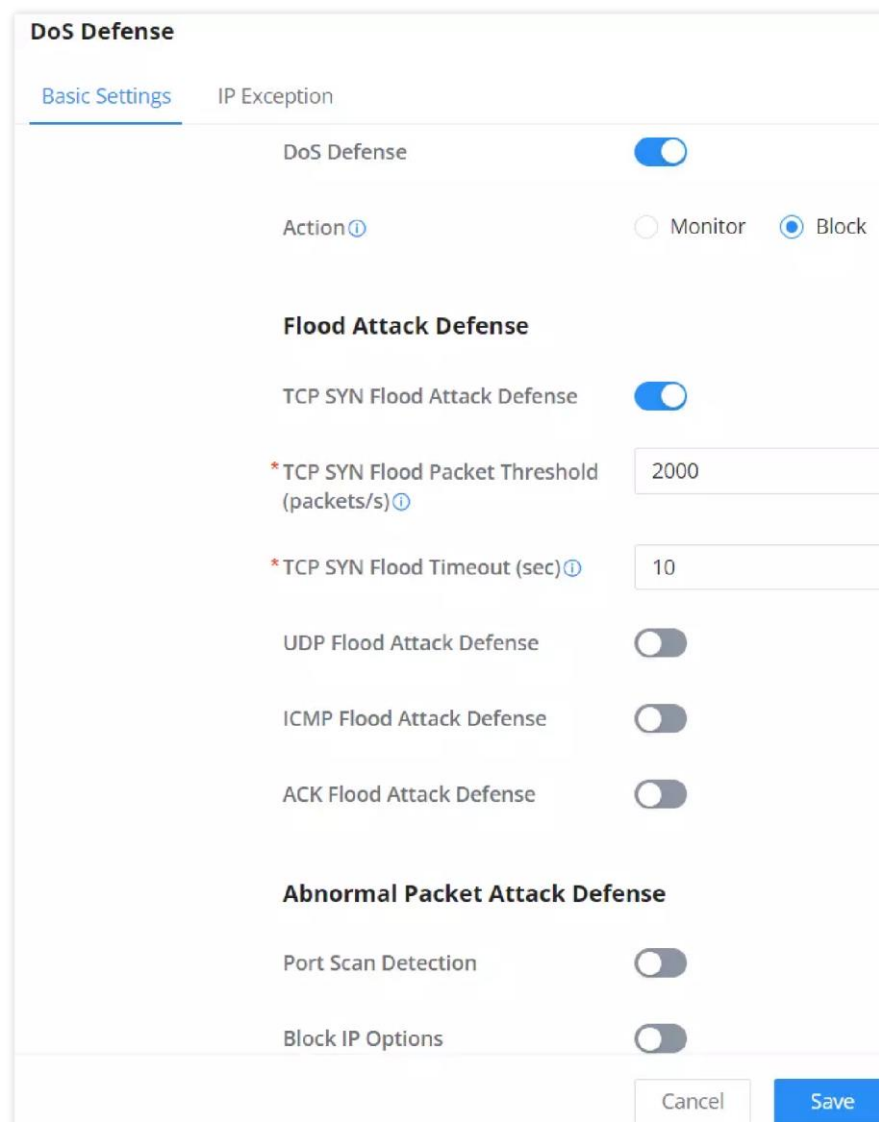
*Flush Connection Reload*

## SECURITY DEFENSE

### DoS Defense

#### Basic Settings – Security Defense

Denial-of-Service Attack is an attack aimed to make the network resources unavailable to legitimate users by flooding the target machine with so many requests causing the system to overload or even crash or shut down.



*DoS Defense – Basic Settings*

DoS Defence	Toggle on/off DoS Defence
-------------	---------------------------



<b>Action</b>	<p>Select the action:</p> <p><b>Monitor:</b> An alarm is generated but is not blocked.</p> <p><b>Block:</b> Monitor and block attacks.</p>
<b>Flood Attack Defense</b>	
<b>TCP SYN Flood Attack Defense</b>	<p>When this option is enabled, the router will take counter measures to SYN Flood Attack.</p> <ul style="list-style-type: none"> <li>● <b>TCP SYN Flood Packet Threshold (packets/s):</b> If the threshold of the TCP SYN packets from the Internet has exceeded the defined value, subsequent TCP SYN packets will be discarded within the specified timeout period.</li> <li>● <b>TCP SYN Flood Timeout (sec):</b> If the number of TCP SYN packets received per second exceeds the threshold within the specified timeout period, attack defense will start immediately.</li> </ul>
<b>UDP Flood Attack Defense</b>	<p>When this option is enabled, the router will take counter measures to the UDP Flood Attack.</p> <ul style="list-style-type: none"> <li>● <b>UDP Flood Packet Threshold (packets/s):</b> If the threshold of the UDP packets from the Internet has exceeded the defined value, subsequent UDP packets will be discarded within the specified timeout period.</li> <li>● <b>UTCP SYN Flood Timeout (sec):</b> If the average number of received UDP packets per second reaches the threshold within the timeout period, attack defense will start immediately.</li> </ul>
<b>ICMP Flood Attack Defense</b>	<p>When this option is enabled, the router will take counter measures to the ICMP Flood Attack.</p> <ul style="list-style-type: none"> <li>● <b>ICMP Flood Packet Threshold (packets/s):</b> If the threshold of the ICMP packets from the Internet has exceeded the defined value, subsequent ICMP packets will be discarded within the specified timeout period.</li> <li>● <b>ICMP Flood Timeout (sec):</b> If the average number of received ICMP packets per second reaches the threshold within the timeout period, attack defense will start immediately.</li> </ul>
<b>ACK Flood Attack Defense</b>	<p>When this option is enabled the router will take counter measures to ACK Flood Attack.</p> <ul style="list-style-type: none"> <li>● <b>ACK Flood Packet Threshold (packets/s):</b> If the threshold if the ACK packets from the Internet has exceeded the defined value, subsequent ACK packets will be discarded within the specified timeout period.</li> <li>● <b>ACK Flood Timeout (sec):</b> If the average number of received ACK packets per second reaches the threshold within the timeout period, attack defense will start immediately.</li> </ul>
<b>Abnormal Packet Attack Defense</b>	
<b>Port Scan Detection</b>	<p>When this option is enabled, the router will take counter measure to the port scanning attempts</p> <ul style="list-style-type: none"> <li>● <b>Port Scan Packet Threshold (packets/s):</b> If the port packets reach the threshold, port scanning detection will start immediately.</li> </ul>
<b>Block IP Options</b>	<p>When this option is enabled, the router will ignore any IP packets with Options field.</p>
<b>Block TCP Flag Scan</b>	<p>When this option is enabled, the router will ignore any packets with unexpected information in the TCP flags.</p>
<b>Block Land Attack</b>	<p>When this option is enabled, the router will block any SYN packets which may have been spoofed and modified to set the source and the destination address to the</p>

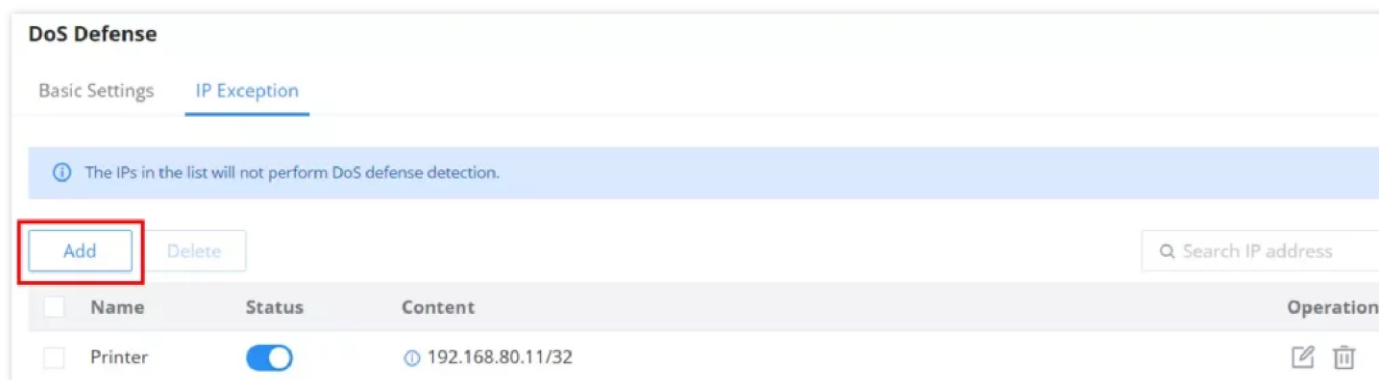


	address of the router. If this option is disabled, it might cause the router to be stuck in a loop of responding to itself.
<b>Block Smurf</b>	When this option is enabled, the router will drop any ICMP echo requests.
<b>Block Ping of Death</b>	When this option is enabled, the router will drop any abnormal or corrupted ping packets.
<b>Block Traceroute</b>	When this option is enabled, the router will not allow the traceroute requests initiated from the WAN side.
<b>Block ICMP Fragment</b>	When this option is enabled, the router will drop the ICMP packets which are fragmented.
<b>Block SYN Fragment</b>	When this option is enabled, the router will drop the SYN packets which are fragmented.
<b>Block Unassigned Protocol Numbers</b>	If enabled, the device will reject IP packets receiving IP protocol number greater than 133.
<b>Block Fraggle Attack</b>	If enabled, the router will drop any UDP broadcast packets initiate from the WAN side.

*DoS Defense*

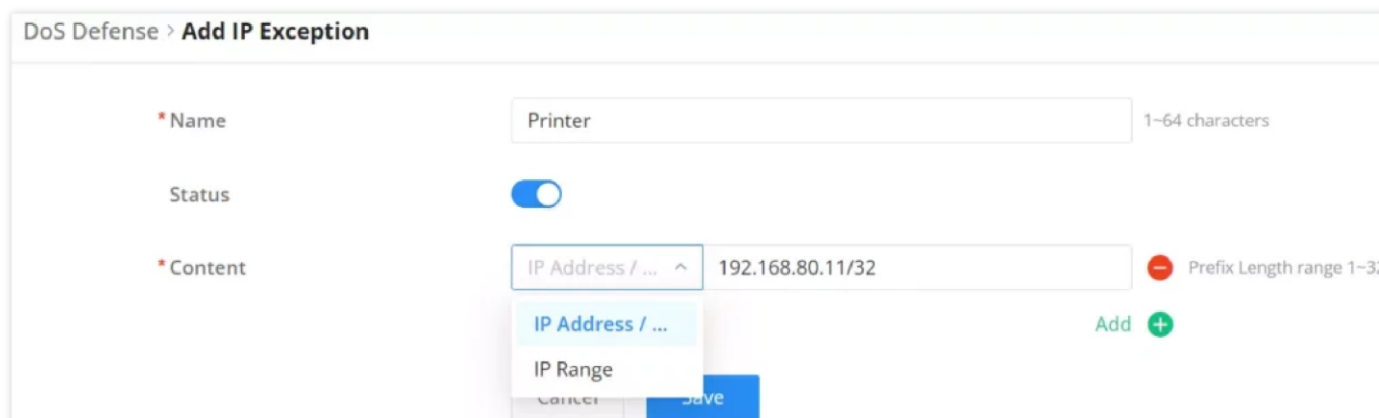
## IP Exception

On this page, users can add IP addresses or IP ranges to be excluded from the DoS Defense scan. To add an IP address or IP range to the list, click on the **"Add"** button as shown below:



*DoS Defense – IP Exception*

Specify a name, then toggle the status ON after that specify the IP address or IP range.



*DoS Defense – Add IP Exception*

## Spoofing Defense

The Spoofing defense section offers several counter-measures to the various spoofing techniques. To protect your network against spoofing, please enable the following measures to eliminate the risk of having your traffic intercepted and spoofed. GCC601X(W) devices offer measures to counter spoofing on ARP information, as well as on IP information.

**Spoofing Defense**

Spoofing Defense

Action ⓘ  Monitor  Block

**ARP Spoofing Defense**

Block ARP Replies with Inconsistent Source MAC Addresses

Block ARP Replies with Inconsistent Destination MAC Addresses

Decline VRRP MAC Into ARP Table

*Spoofing Defense*

### ARP Spoofing Defense

- **Block ARP Replies with Inconsistent Source MAC Addresses:** The GCC device will verify the destination MAC address of a specific packet, and when the response is received by the device, it will verify the source MAC address and it will make sure that they match. Otherwise, the GCC device will not forward the packet.
- **Block ARP Replies with Inconsistent Destination MAC Addresses:** The GCC601X(W) will verify the source MAC address when the response is received. The device will verify the destination MAC address and it will make sure that they match. Otherwise, the device will not forward the packet.
- **Decline VRRP MAC Into ARP Table:** The GCC601X(W) will decline including any generated virtual MAC address in the ARP table.

## ANTI-MALWARE

In this section, the users can enable Anti-malware and update their signature library information.

### Configuration

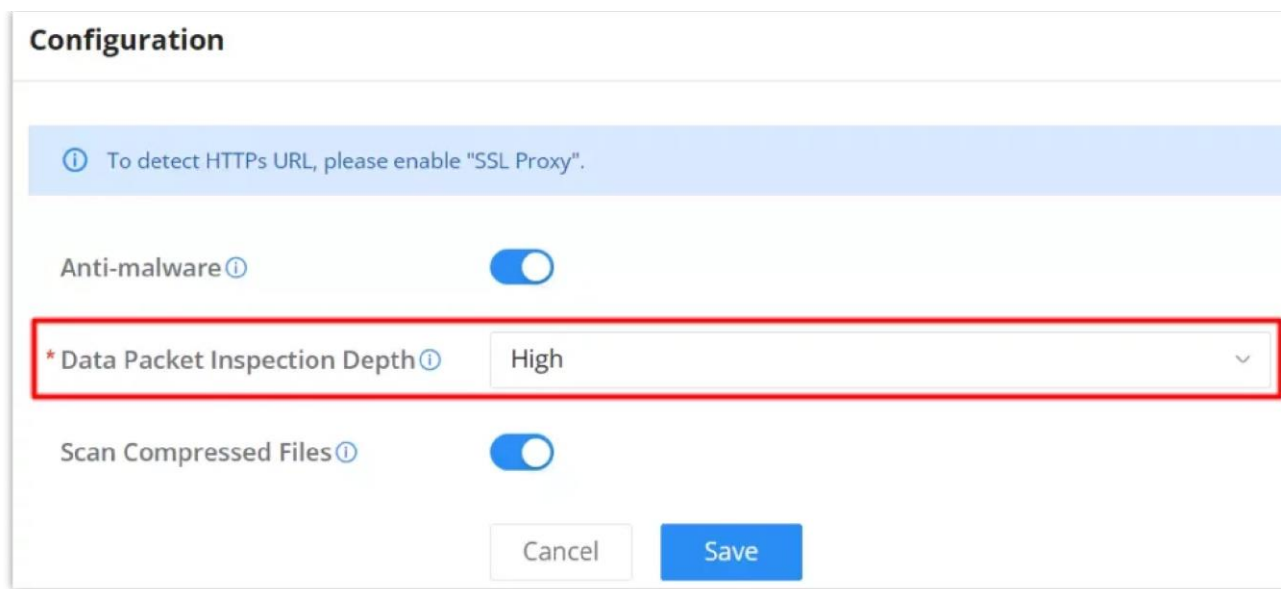
To enable Anti-malware, navigate to **Firewall module** → **Anti-Malware** → **Configuration**.

- **Anti-malware:** toggle ON/OFF to enable/disable the Anti-malware.

**Note:**

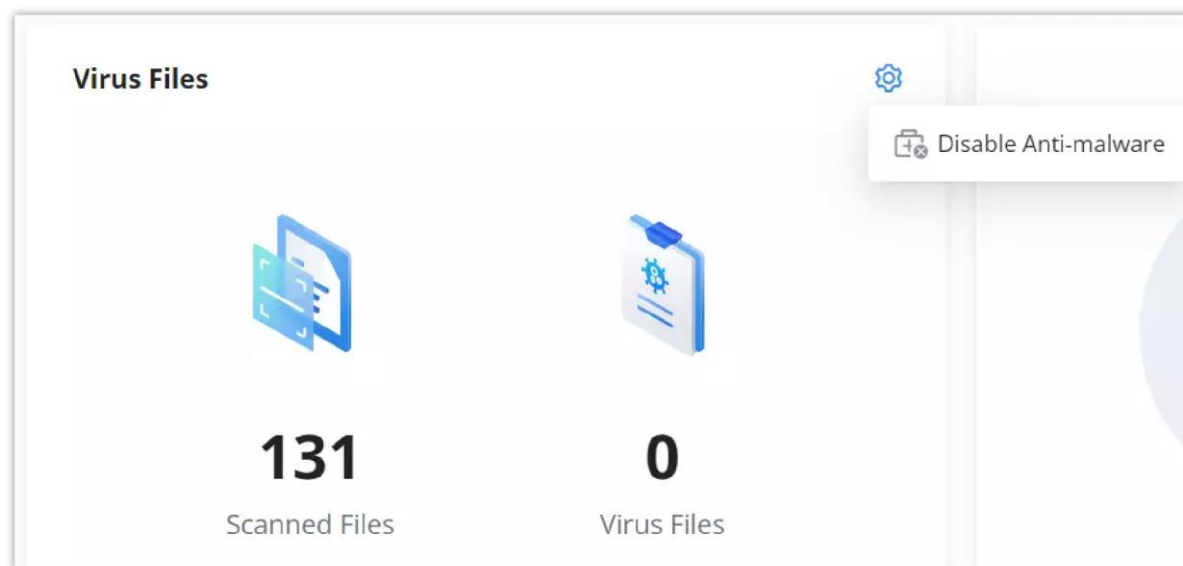
To filter HTTPs URL, please enable "[SSL Proxy](#)".

- **Data Packet Inspection Depth:** Check the packet content of each traffic according to the configuration. The deeper the depth, the higher the detection rate and the higher the CPU consumption. There are 3 level of depth low, medium and high.
- **Scan Compressed Files:** supports scanning of compressed files.



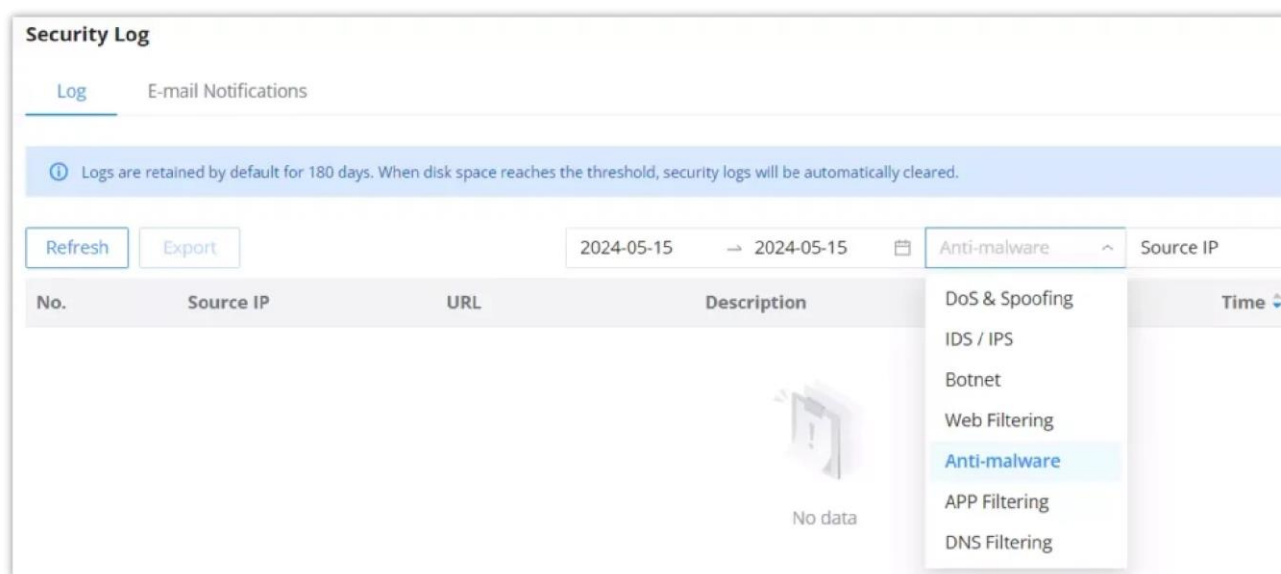
Anti-Malware Configuration

On the Overview page, users can check the statistics and have an [overview](#). Also, it's possible to disable the Anti-malware directly from this page by clicking on the settings icon as shown below:



Overview page – Anti-malware statistics

It's also possible to check the [security log](#) for more details:



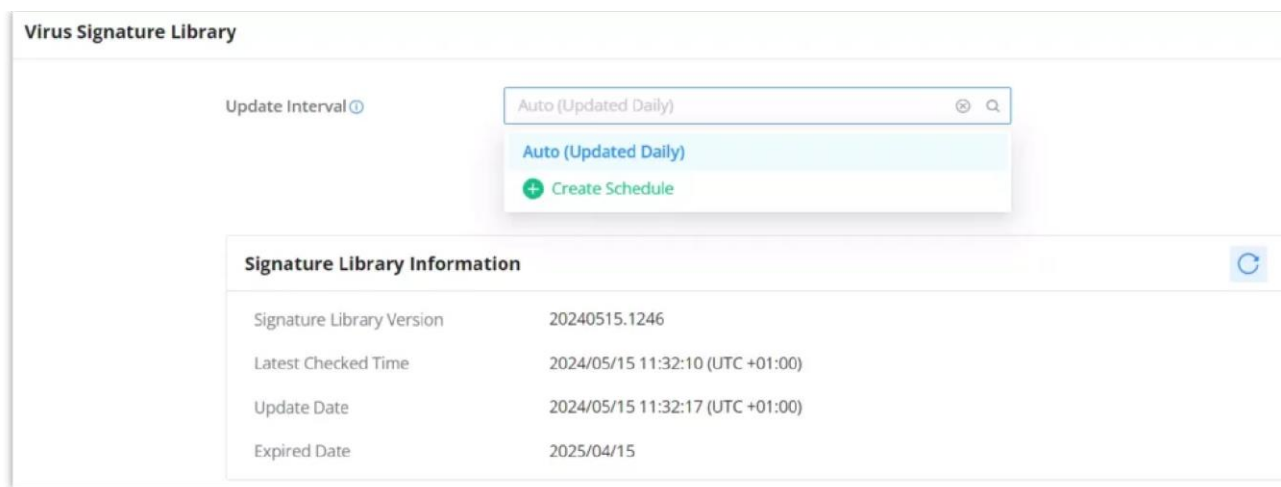
Security log – Anti-malware

## Virus Signature Library

On this page, the users can update the anti-malware signature library information manually, update daily or create a schedule, please refer to the figure below:

**Note:**

By default, it is updated at a random time point (00:00-6:00) every day.



Virus Signature Library

## INTRUSION PREVENTION

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are security mechanisms that monitor network traffic for suspicious activities and unauthorized access attempts. IDS identifies potential security threats by analyzing network packets and logs, while IPS actively prevents these threats by blocking or mitigating malicious traffic in real time. Together, IPS and IDS provide a layered approach to network security, helping to protect against cyberattacks and safeguard sensitive information. A botnet is a network of compromised computers infected with malware and controlled by a malicious actor, typically used to carry out large-scale cyberattacks or illicit activities.

### IDS/IPS

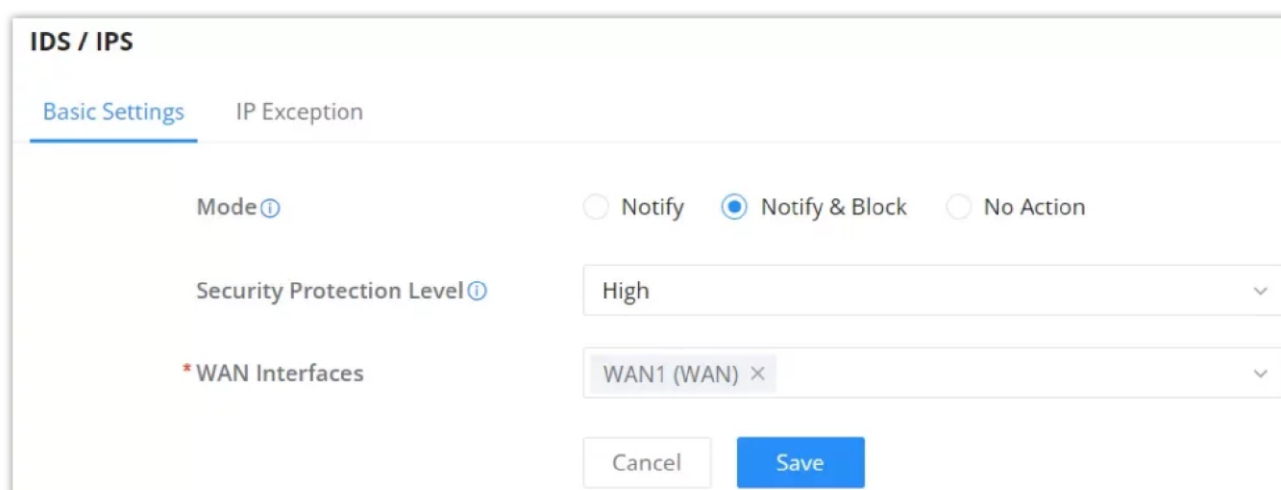
#### Basic Settings – IDS/IPS

On this tab, the users can select IDS/IPS mode, Security Protection Level.

#### IDS/IPS Mode:

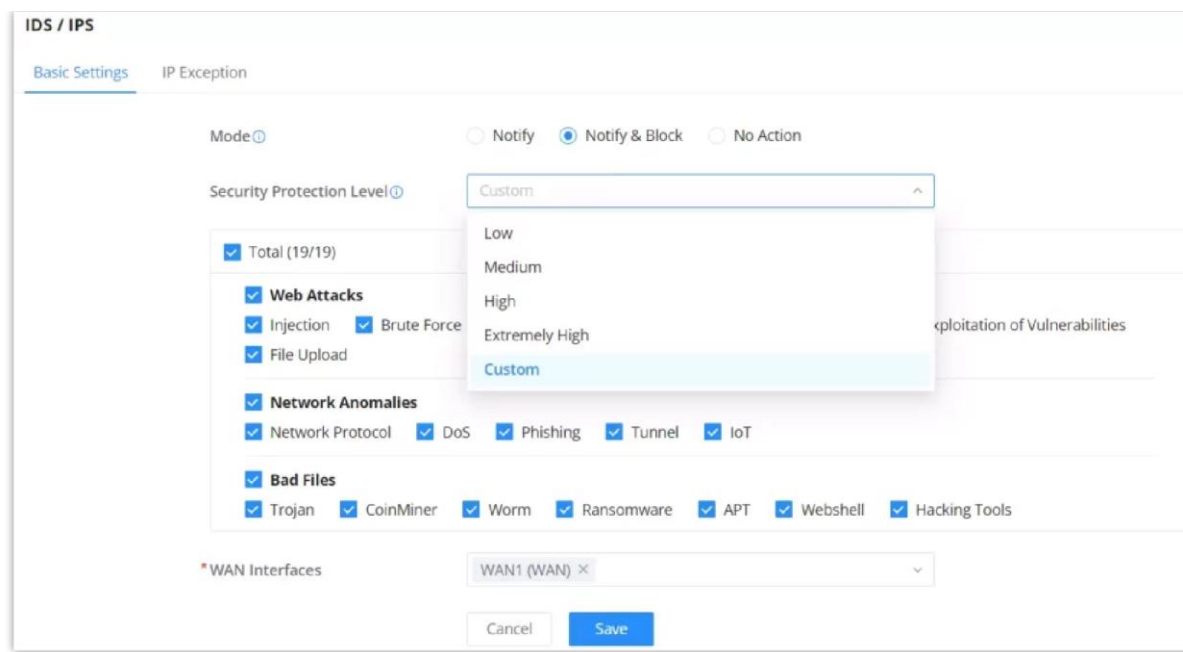
- **Notify:** detect traffic and only notify the users without blocking it, this is equal to IDS (Intrusion Detection System).
- **Notify & Block:** detects or blocks traffic and notifies about the security issue, this is equal to IPS (Intrusion Prevention System).
- **No Action:** no notifications or prevention, IDS/IPS is disabled in this case.

**Security Protection Level:** Select a protection level (Low, Medium, High, Extremely high and Custom). Different protection levels correspond to different protection levels. Users can customize the protection type. The higher the protection level, the more protection rules, and Custom will enable the users to select what to IDS/IPS will detect.



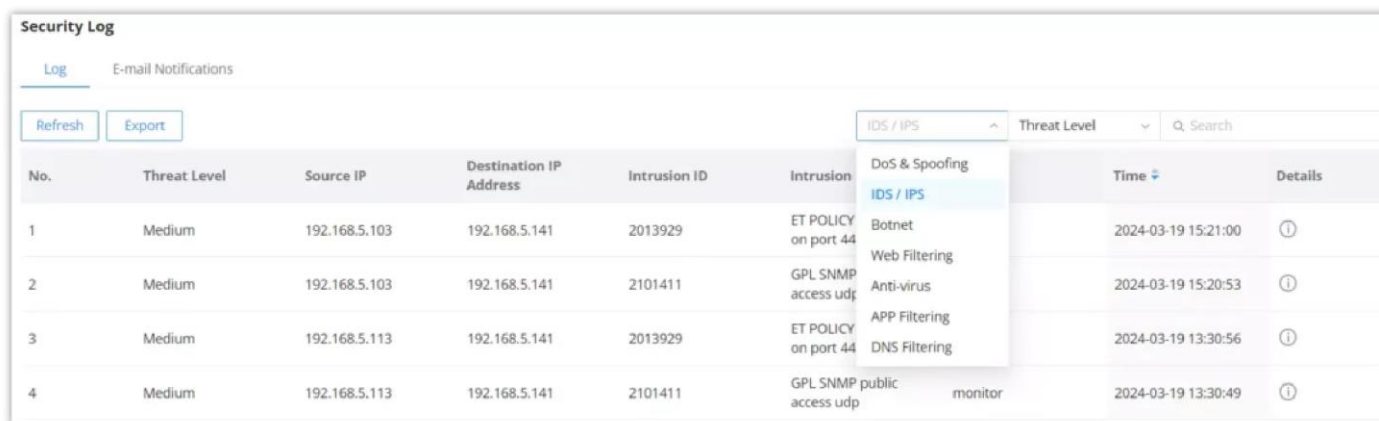
IDS/IPS – Basic settings

It's also possible to select a custom security protection level and then select from the list the specific threats. Please refer to the figure below:



IDS/IPS – Security protection level set to custom

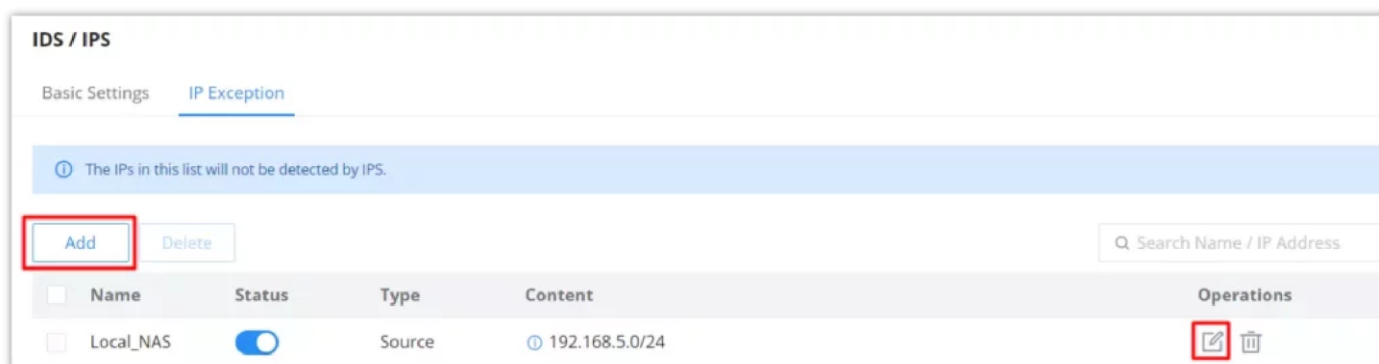
To check the notifications and the actions taken, under the [Security log](#), select IDS/IPS from the drop-down list as shown below:



Security log – IDS/IPS

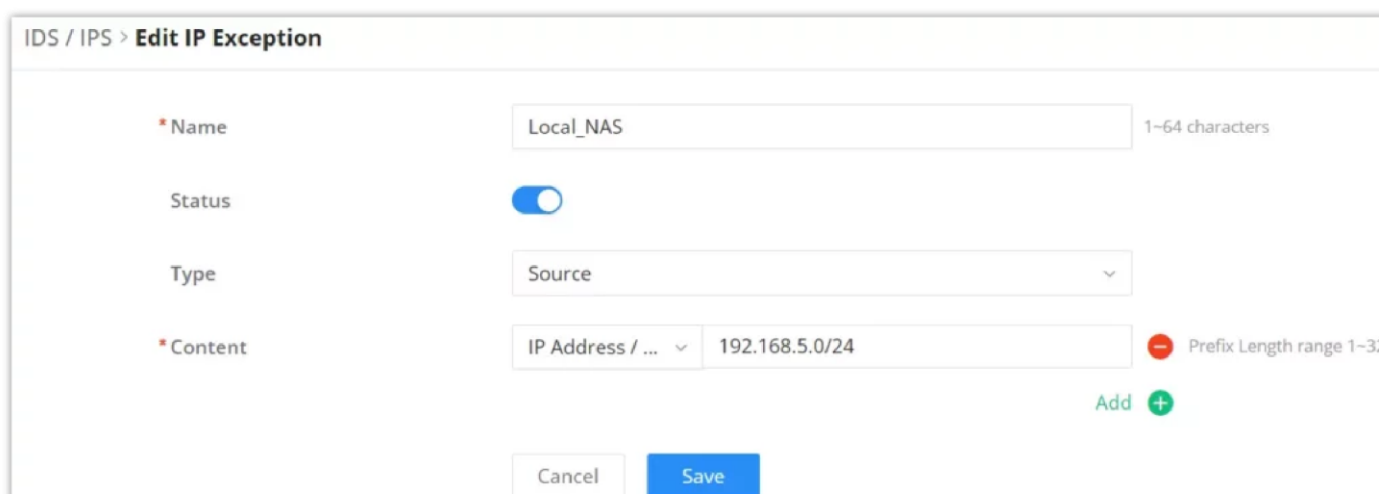
## IP Exception

The IP addresses on this list will not be detected by IDS/IPS. To add an IP address to the list, click on the **“Add”** button as shown below:



IDS/IPS – IP Exception

Enter a name, then enable the status, and then select the type (Source or Destination) for the IP address(s). To add an IP address click on the **“+”** icon and to delete an IP address click on the **“-”** icon as shown below:



IDS/IPS – Add IP Exception

## Botnet

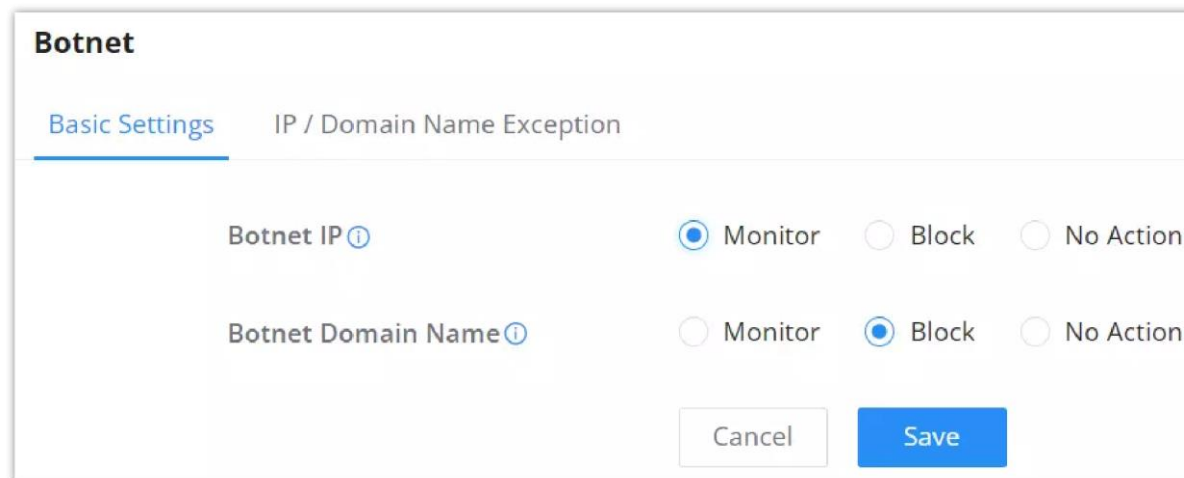
### Basic Settings – Botnet

On this page, users can configure the basic settings for monitoring the outbound Botnet IP and Botnet Domain Name and there are three options:

**Monitor:** alarms are generated but are not blocked.

**Block:** monitors and blocks outbound IP addresses/Domain names that access botnets.

**No Action:** The IP address/Domain name of the outbound botnet is not detected.



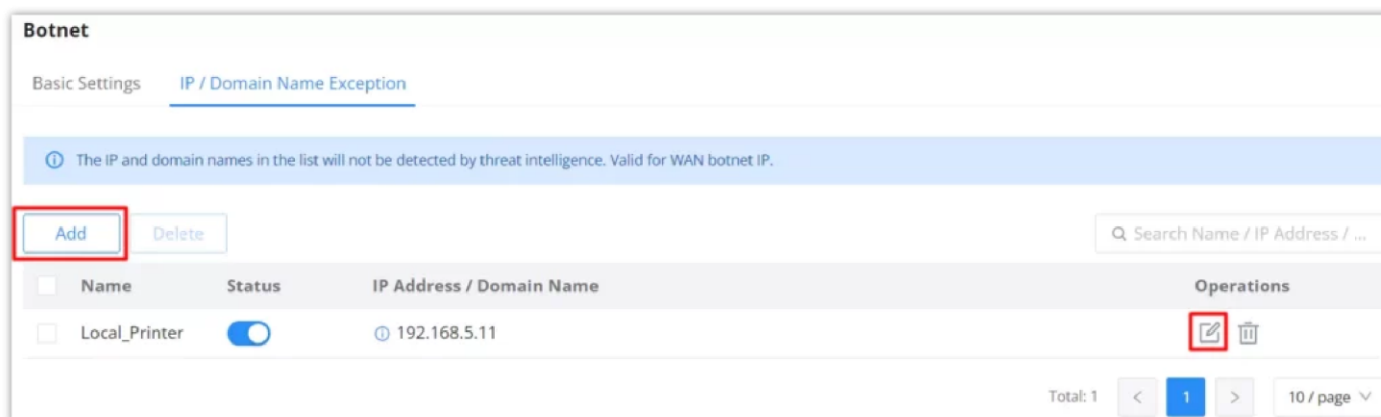
The screenshot shows the 'Botnet' configuration page with two tabs: 'Basic Settings' (active) and 'IP / Domain Name Exception'. Under 'Basic Settings', there are two rows of radio button options. The first row is for 'Botnet IP' with 'Monitor' selected. The second row is for 'Botnet Domain Name' with 'Block' selected. At the bottom are 'Cancel' and 'Save' buttons.

Botnet – Basic Settings

### IP/Domain Name Exception

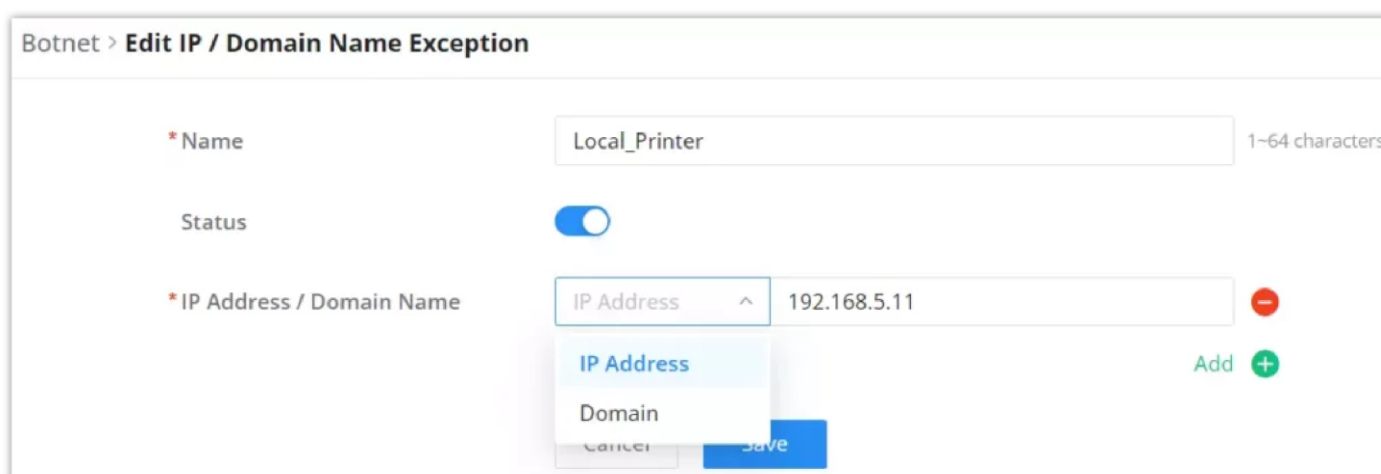
The IP addresses on this list will not be detected for Botnets. To add an IP address to the list, click on the “Add” button as shown below:

Enter a name, then enable the status. To add an IP address/Domain name click on the “+” icon and to delete an IP address/Domain name click on the “-” icon as shown below:



The screenshot shows the 'Botnet' configuration page with the 'IP / Domain Name Exception' tab active. A blue banner at the top states: 'The IP and domain names in the list will not be detected by threat intelligence. Valid for WAN botnet IP.' Below this are 'Add' and 'Delete' buttons. A search bar is on the right. A table lists exceptions with columns for Name, Status, IP Address / Domain Name, and Operations. One entry is 'Local\_Printer' with status 'On' and IP '192.168.5.11'. The 'Add' button in the table is highlighted with a red box. At the bottom right, there are pagination controls showing 'Total: 1' and '10 / page'.

Botnet – IP/Domain name exception



The screenshot shows the 'Botnet > Edit IP / Domain Name Exception' form. It has three main fields: '\* Name' with the value 'Local\_Printer' (1-64 characters), 'Status' with a toggle switch turned on, and '\* IP Address / Domain Name' with a dropdown menu set to 'IP Address' and the value '192.168.5.11'. There are 'Add' and 'Cancel' buttons at the bottom.

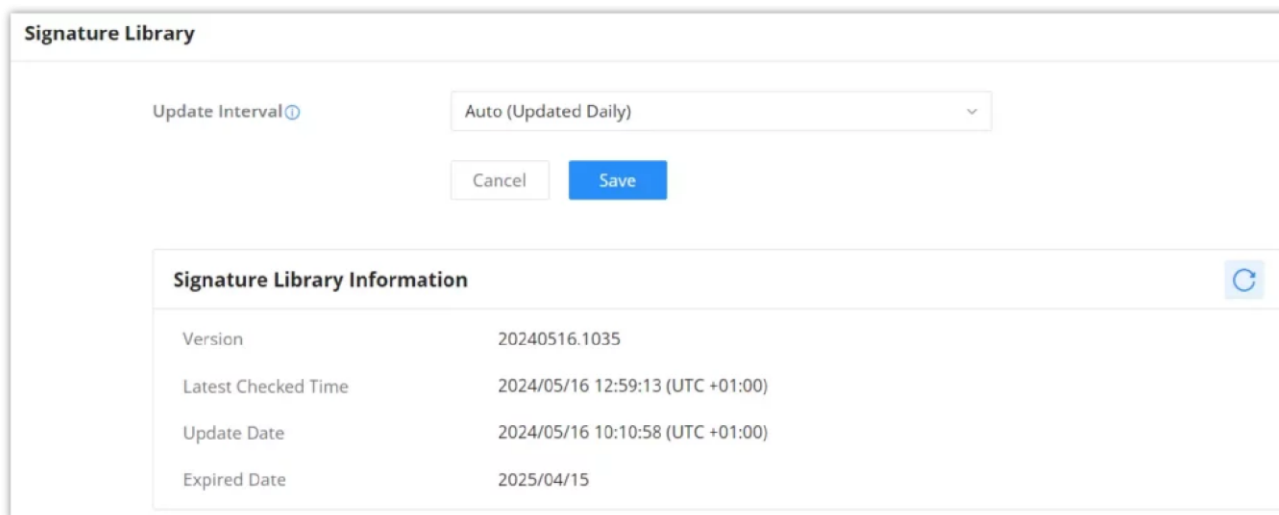
Botnet – IP/Domain name exception

### Signature Library – Botnet

On this page, the users can update the IDS/IPS and Botnet signature library information manually, update daily or create a schedule, please refer to the figure below:

**Note:**

By default, it is updated at a random time point (00:00-6:00) every day.



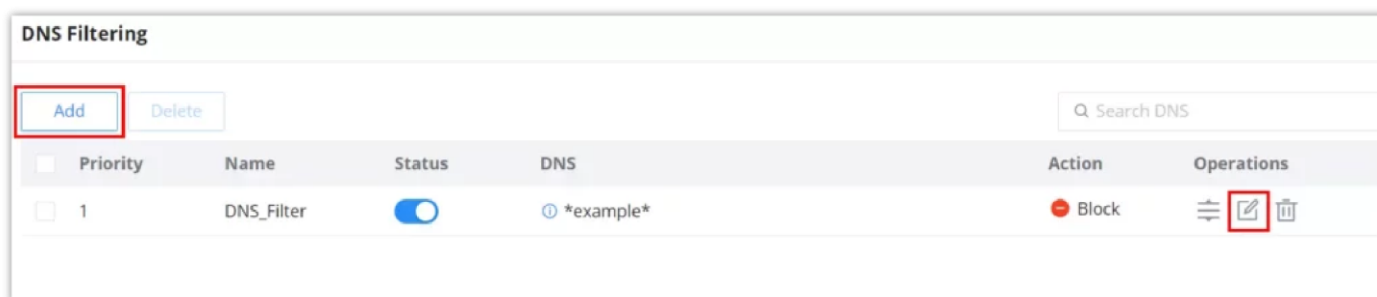
IDS/IPS & Botnet – Signature Library

## CONTENT CONTROL

The Content Control feature provides users with the ability to filter (allow or block) traffic based on DNS, URL, keywords, and application.

### DNS Filtering

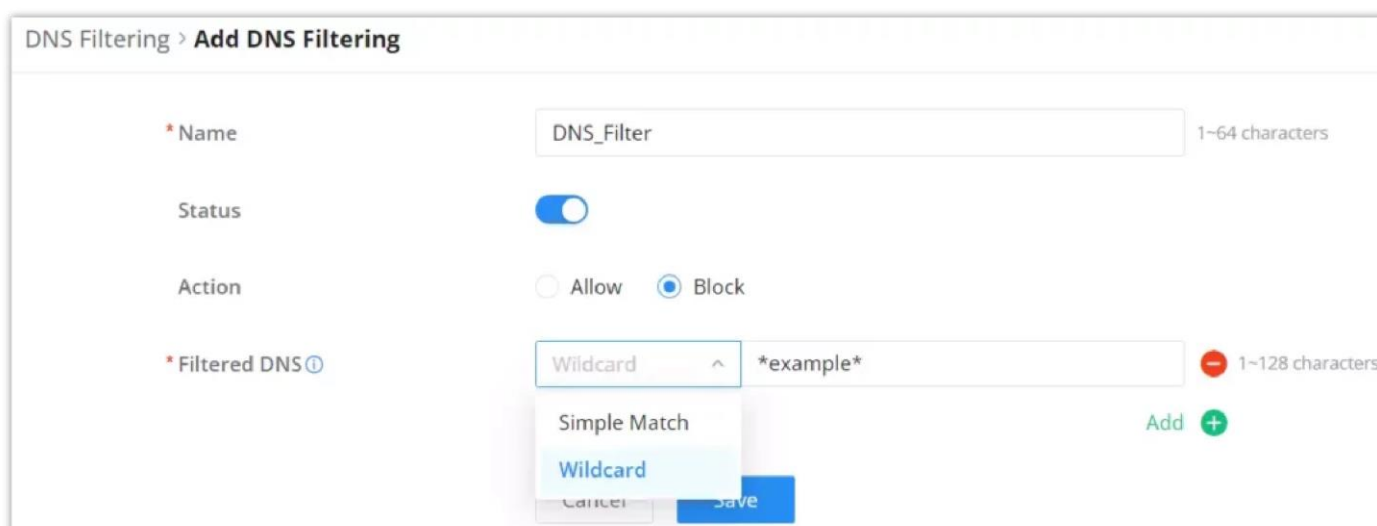
To filter traffic based on DNS, navigate to **Firewall module** → **Content Control** → **DNS Filtering**. Click on the **“Add”** button to add a new DNS Filtering as shown below:



DNS Filtering page

Then, enter the name of the DNS filter, enable the status, and select the action (Allow or Block) as for Filtered DNS, there are two options:

- **Simple Match:** the domain name supports multi-level domain name matching.
- **Wildcard:** keywords and wildcard \* can be entered, wildcard \* can only be added before or after the entered keyword. For example: \*.imag, news\*, \*news\*. The \* in the middle is treated as a normal character.



Add DNS Filter

To check the filtered DNS, the users can either find it on the [Overview](#) page or under the [Security log](#) as shown below:



**Top Security Log**

Source IP	DNS Domain ...	Description	Action
192.168.80.235	example.org	DNS_Filtering	block
192.168.80.235	example.org	DNS_Filtering	block
192.168.80.235	example.org	DNS_Filtering	block
192.168.80.235	example.org	DNS_Filtering	block
192.168.80.235	example.org	DNS_Filtering	block

Dropdown menu options: DNS Filtering, DoS & Spoofing, IDS / IPS, Botnet, Web Filtering, Anti-virus, APP Filtering, DNS Filtering.

DNS Filtering on the overview page

**Security Log**

Log | E-mail Notifications

Refresh | Export

Dropdown menu: DNS Filtering, DoS & Spoofing, IDS / IPS, Botnet, Web Filtering, Anti-virus, APP Filtering, DNS Filtering.

No.	Source IP	DNS Domain Name	Description	Time	Details
1	192.168.80.235	example.org	DNS_Filtering	2024-03-19 14:30:15	ⓘ
2	192.168.80.235	example.org	DNS_Filtering	2024-03-19 14:29:36	ⓘ
3	192.168.80.235	example.org	DNS_Filtering	2024-03-19 14:28:12	ⓘ
4	192.168.80.235	example.org	DNS_Filtering	2024-03-19 14:25:35	ⓘ
5	192.168.80.235	example.org	DNS_Filtering	2024-03-19 14:23:35	ⓘ

DNS Filtering – Security Log

## Web Filtering

### Basic Settings – Web Filtering

On the page, the users can enable/disable the global web filtering, then the users can enable or disable web URL filtering, URL category filtering and keyword filtering independently and to filter HTTPs URLs, please enable “[SSL Proxy](#)”.

**Web Filtering**

Basic Settings | URL Filtering | URL Category Filtering | Keywords Filtering | URL Signature Library

Web Filtering ⓘ

Cancel Save

Web Filtering – Basic Settings

### URL Filtering

URL filtering enables users to filter URL addresses using either a Simple match (domain name or IP address) or using a Wildcard (e.g. \*example\*).

To create a URL filtering, navigate to **Firewall Module** → **Content Filtering** → **Web Filtering page** → **URL Filtering tab**, then click on the “**Add**” button as shown below:

**Web Filtering**

Basic Settings | URL Filtering | URL Category Filtering | Keywords Filtering | URL Signature Library

Add Delete Search URL

Priority	Name	Status	URL	Action	Operations
1	URL_Filtering	<input checked="" type="checkbox"/>	*example*	Block	⋮

Web Filtering – URL Filtering

Specify a name, then toggle the status ON, select the action (Allow, Block), and finally specify the URL either using a simple domain name, IP address (Simple match), or using a wildcard. Please refer to the figure below:

Web Filtering > **Add URL Filtering**

\* Name: URL\_Filtering (1-64 characters)

Status:

Action:  Allow  Block

\* URL: Wildcard (1-128 characters) \*example\*

Buttons: Cancel, Save, Add (+)

Web Filtering – URL Filtering

## URL Category Filtering

The users also have the option not to only filter by specific domain/IP address or wildcard, but also to filter by categories for example Attacks and Threats, Adult, etc.

To block or allow the whole category, click on the first option on the row and select All Allow or All Block. It's also possible to block/allow by sub-categories as shown below:

Web Filtering

Basic Settings | URL Filtering | **URL Category Filtering** | Keywords Filtering | URL Signature Library

<b>Adult</b>	All BLOCK	Adult	Lingerie	Mixed Adult	Sexual Education	
<b>Advertisement</b>	All BLOCK	Marketingware	Publicite			
<b>Attacks and Threats</b>	All BLOCK	Agressif	DDoS	Hacking	Phishing	
<b>Bad Websites</b>	Mix	Bitcoin	Cryptojackin g	Dangerous M aterial	Drogue	Gambling
<b>Entertainment</b>	All Allow	Audio Video	Manga	Mobile Phon e	Radio	
<b>Finance</b>	All Allow	Bank	Financial			
<b>Game</b>	All Allow	Educational Games	Games			
<b>Network</b>	All Allow	Redirector	Remote Cont rol	Shortener	VPN	

Web Filtering – URL Filtering

## Keywords Filtering

Keyword filtering enables users to filter using either a regular expression or a Wildcard (e.g. \*example\*).

To create a keywords filtering, navigate to **Firewall Module** → **Content Filtering** → **Web Filtering page** → **Keywords Filtering tab**, then click on the "Add" button as shown below:

Web Filtering

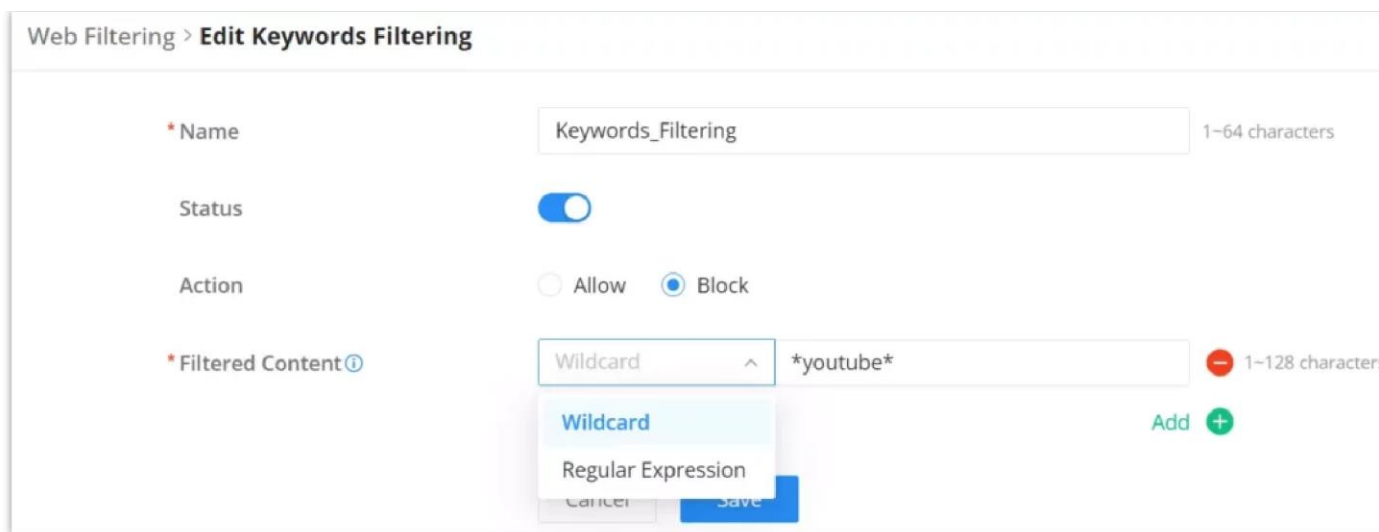
Basic Settings | URL Filtering | URL Category Filtering | **Keywords Filtering** | URL Signature Library

Buttons: Add, Delete, Search filtered content

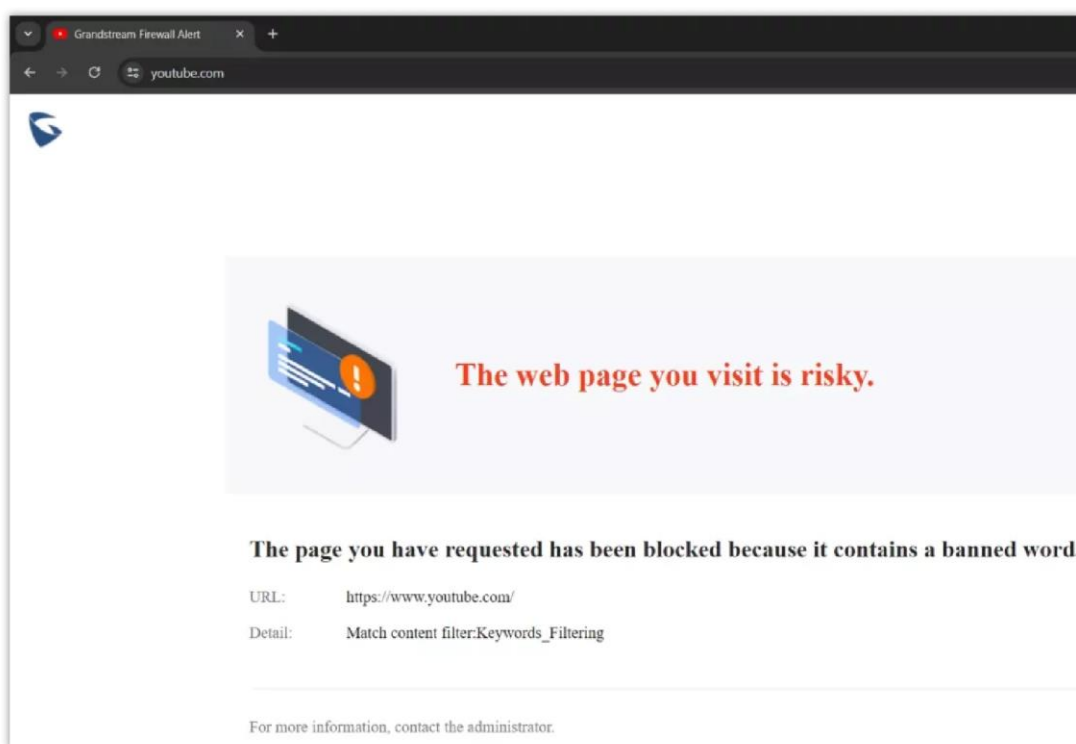
Priority	Name	Status	Filtered Content	Action	Operations
1	Keywords_FILT...	<input checked="" type="checkbox"/>	*example*	Block	[Edit] [Delete]

Web Filtering – Keywords Filtering

Specify a name, then toggle the status ON, select the action (Allow, Block), and finally specify the filtered content either using a regular expression or a wildcard. Please refer to the figure below:



When the keywords filtering is ON and the action is set to Block. If the users try to access for example “YouTube” on the browser, they will be prompted with a firewall alert as shown below:



Example of keywords\_filtering on the Browser

For more details about the alert, the users can navigate to the [Firewall module](#) → [Security Log](#).

No.	Source IP	URL	Description	Action	Time	Details
21	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:25:19	ⓘ
22	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:34	ⓘ
23	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:31	ⓘ
24	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:17	ⓘ
25	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:10	ⓘ
26	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:22:56	ⓘ
27	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:19:40	ⓘ

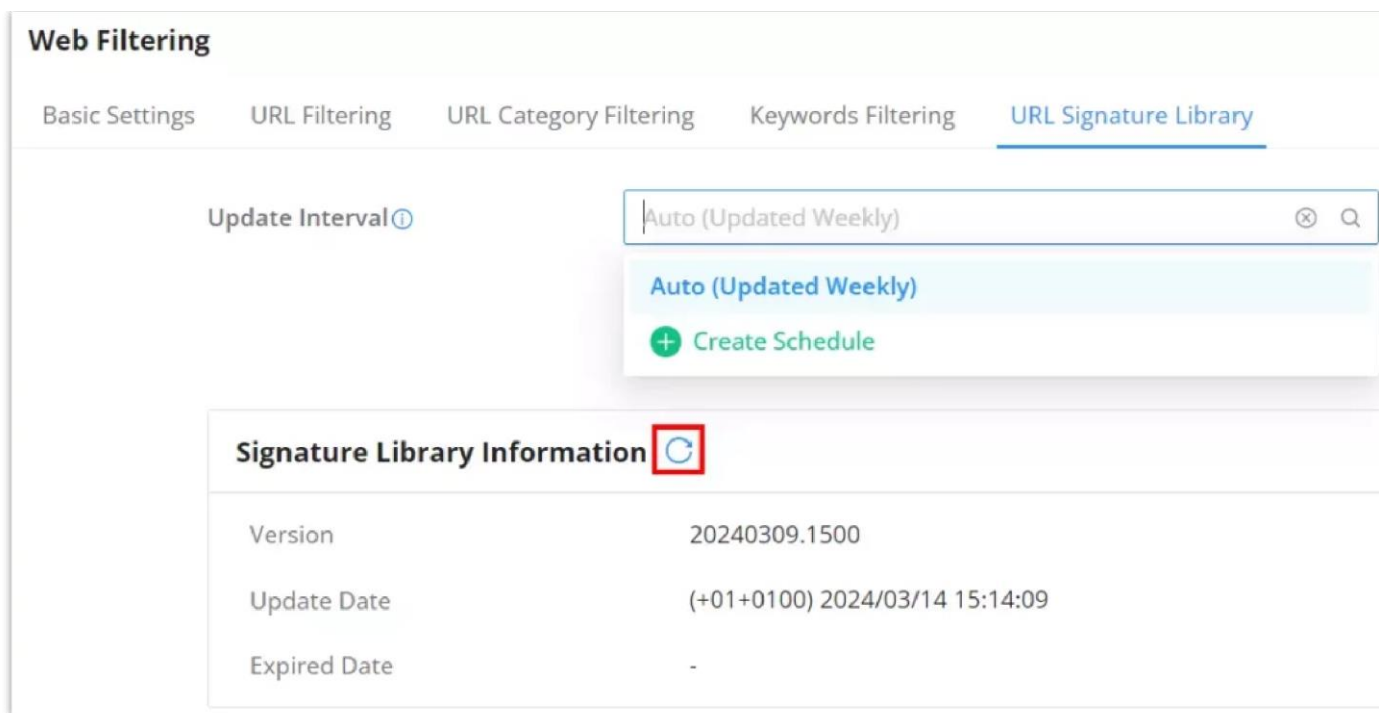
Example of keywords\_filtering on GCC security log

## URL Signature Library

On this page, the users can update the Web Filtering signature library information manually, update daily, or create a schedule, please refer to the figure below:

**Note:**

By default, it is updated at a random time point (00:00-6:00) every day.



Web Filtering – URL Signature Library

## Application Filtering

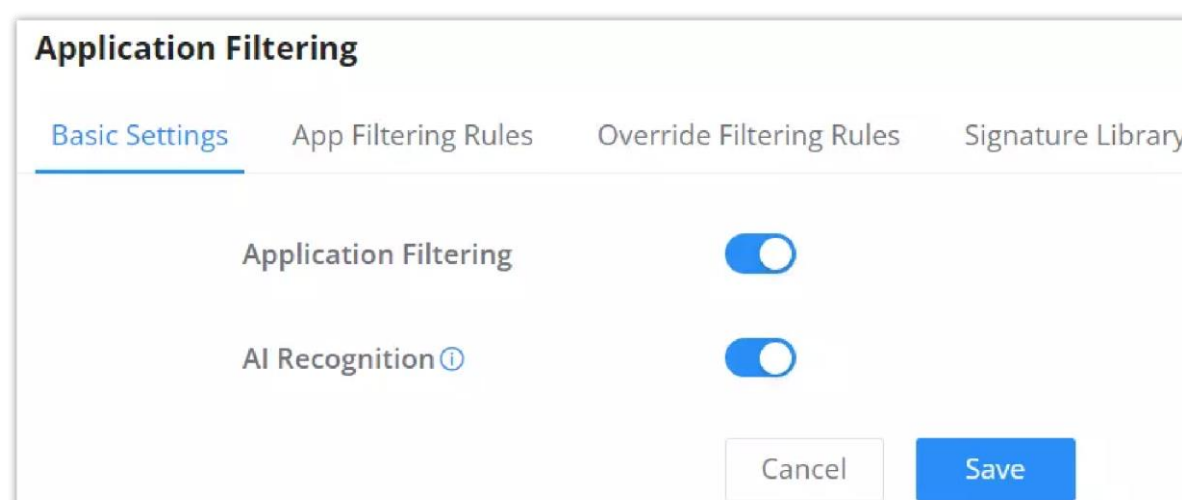
### Basic Settings – Application Filtering

On the page, the users can enable/disable the global application filtering, then the users can enable or disable by app categories.

Navigate to **Firewall module** → **Content Control** → **Application Filtering**, and on the basic settings tab, enable Application Filtering globally, it's also possible to enable AI Recognition for better classification.

**Note:**

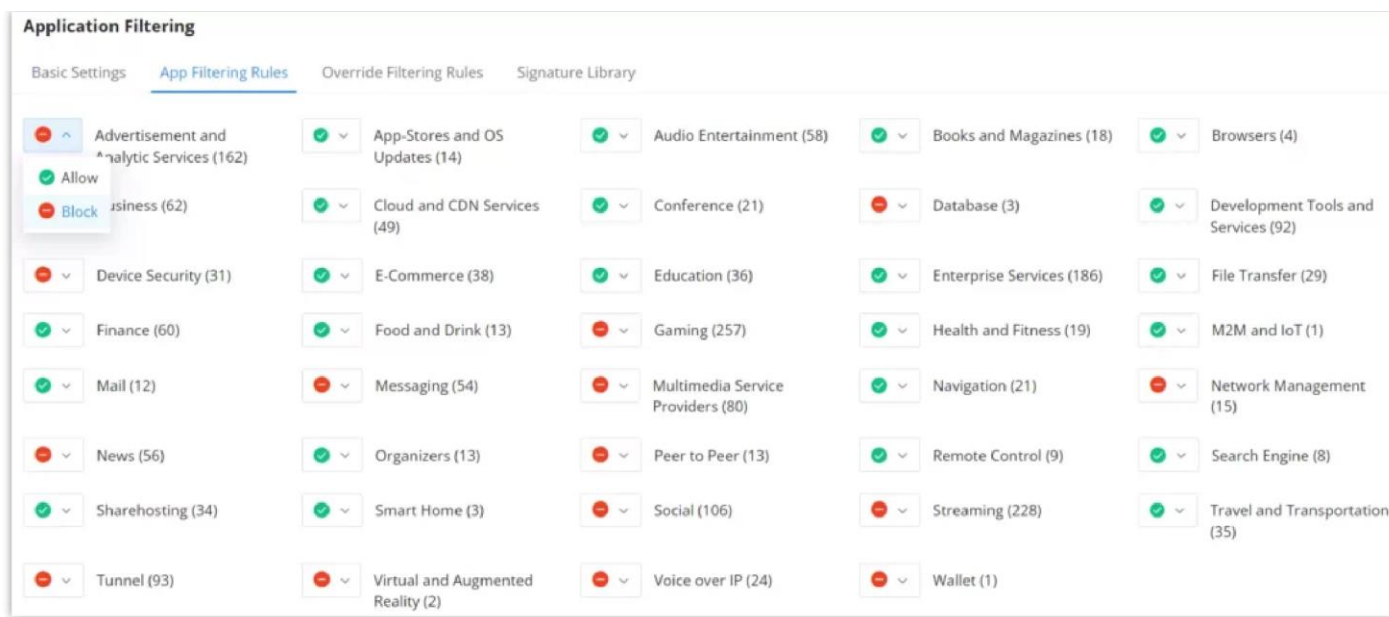
when AI Recognition is enabled, AI deep learning algorithms will be used to optimise the accuracy and reliability of application classification, which may consume more CPU and memory resources.



Application Filtering – Basic Settings

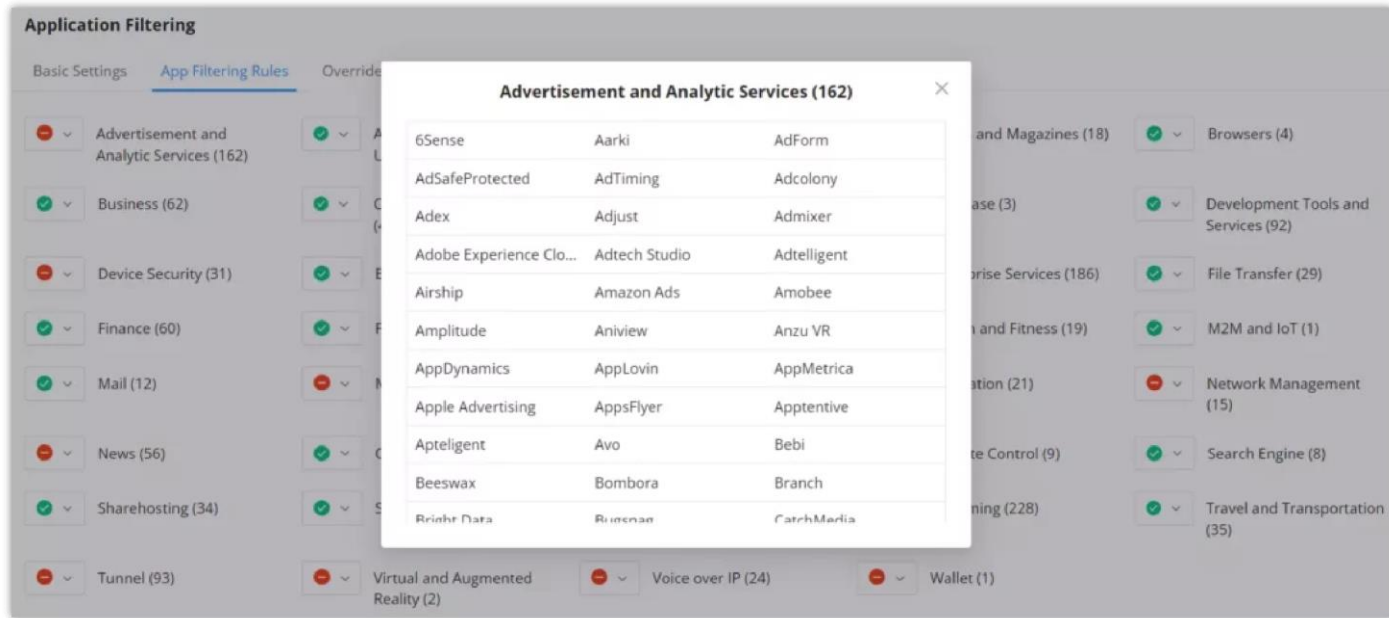
### App Filtering Rules

On the App Filtering Rules tab, the users can Allow/Block by app category as shown below:



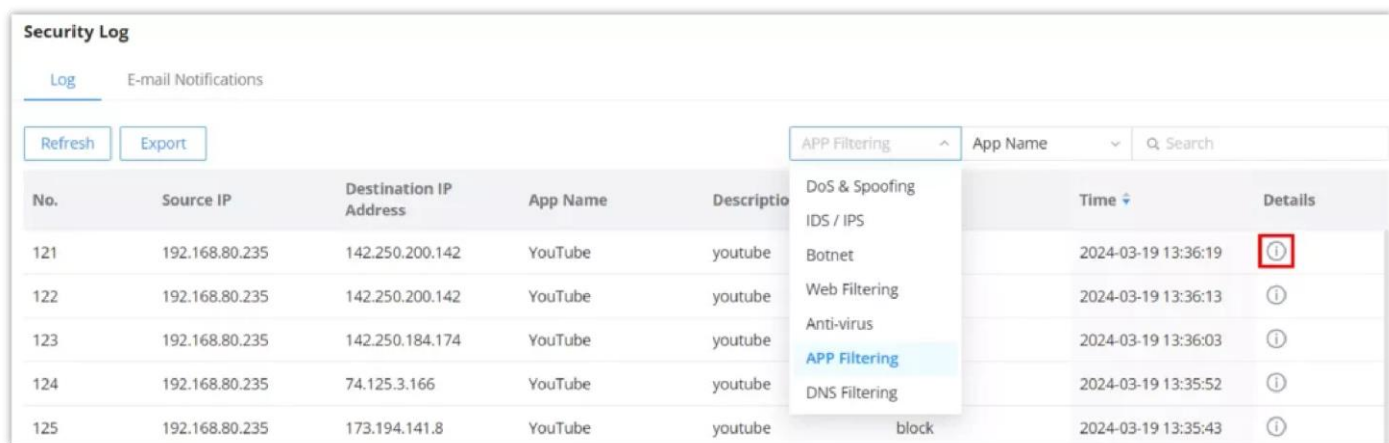
Application Filtering – App Filtering Rules

To view what the app category includes, click on the text and a list of apps will be displayed. Refer to the figure below:



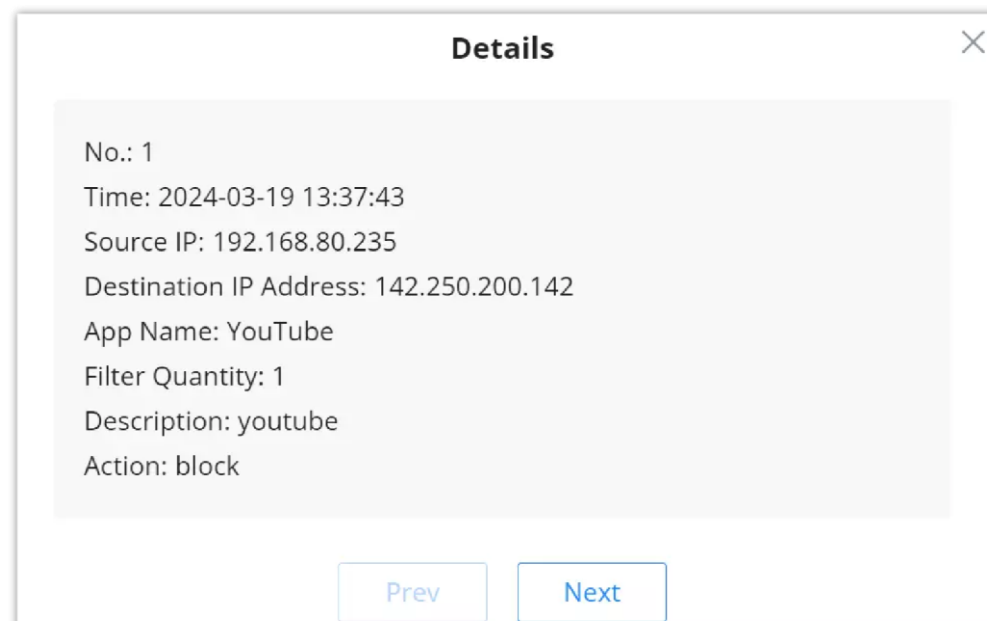
Application Filtering – category

An example of application filtering is used on the app "YouTube" and the action set to "Block", this information will be displayed under the Security Log.



Example of application filtering on GCC security log

For more details, click on the **exclamation icon** as shown above:



Example of application filtering on GCC security log – details

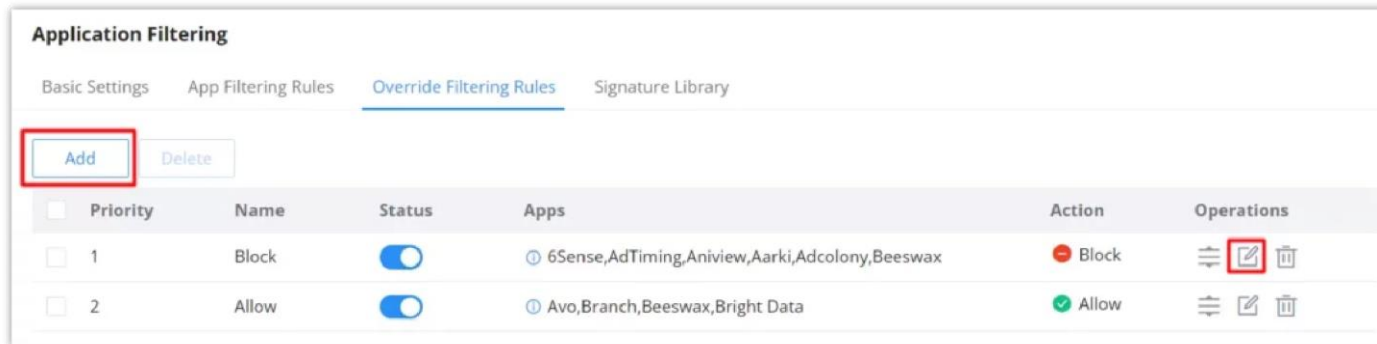


## Override Filtering Rules

If an app category is selected, the users will still have the option to override the general rule (app category) with the override filtering rules feature.

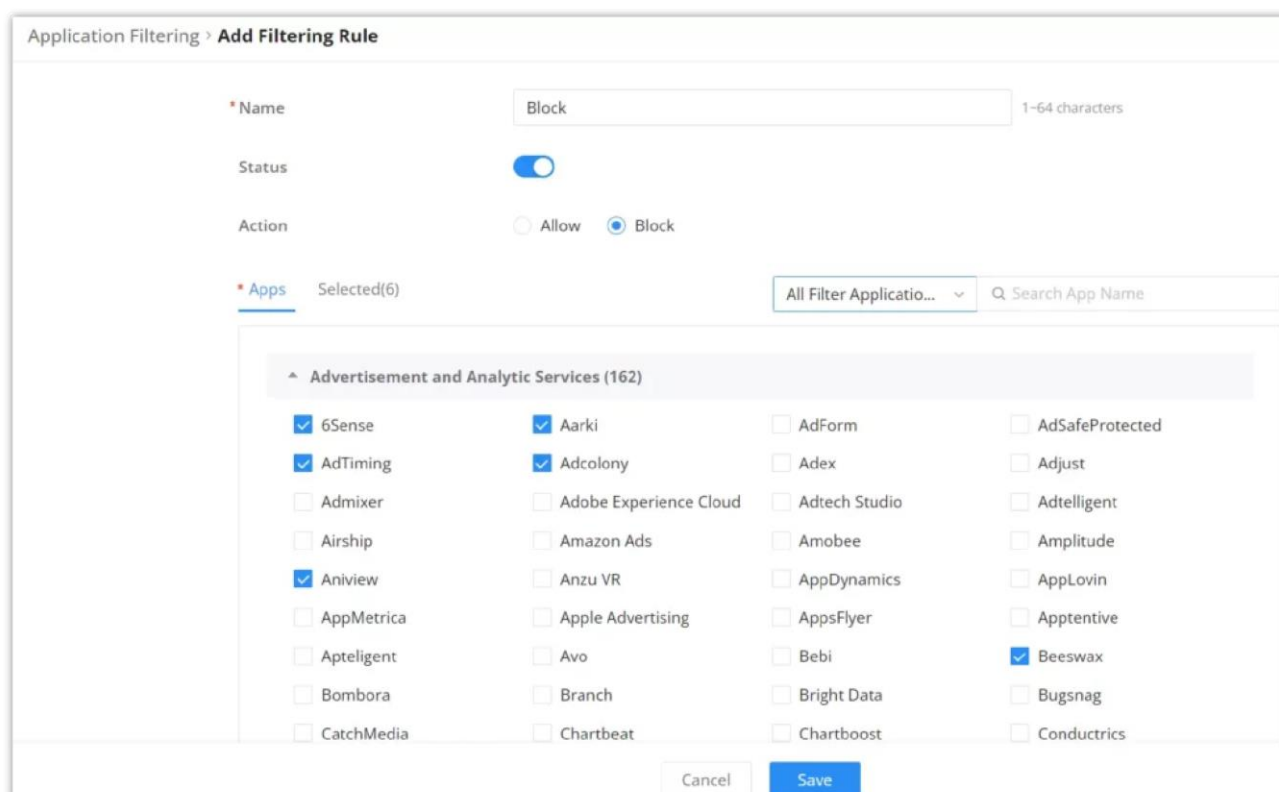
**For example**, if the Browsers app category is set to Block, then we can add an override filtering rule to allow Opera Mini, this way the whole browser app category is blocked except Opera Mini.

To create an override Filtering rule, click on the **"Add"** button as shown below:



Application Filtering – Override filtering rules

Then, specify a name and toggle the status ON, set the action to Allow or Block and finally select from the list the apps that will be allowed or blocked. Please refer to the figure below:



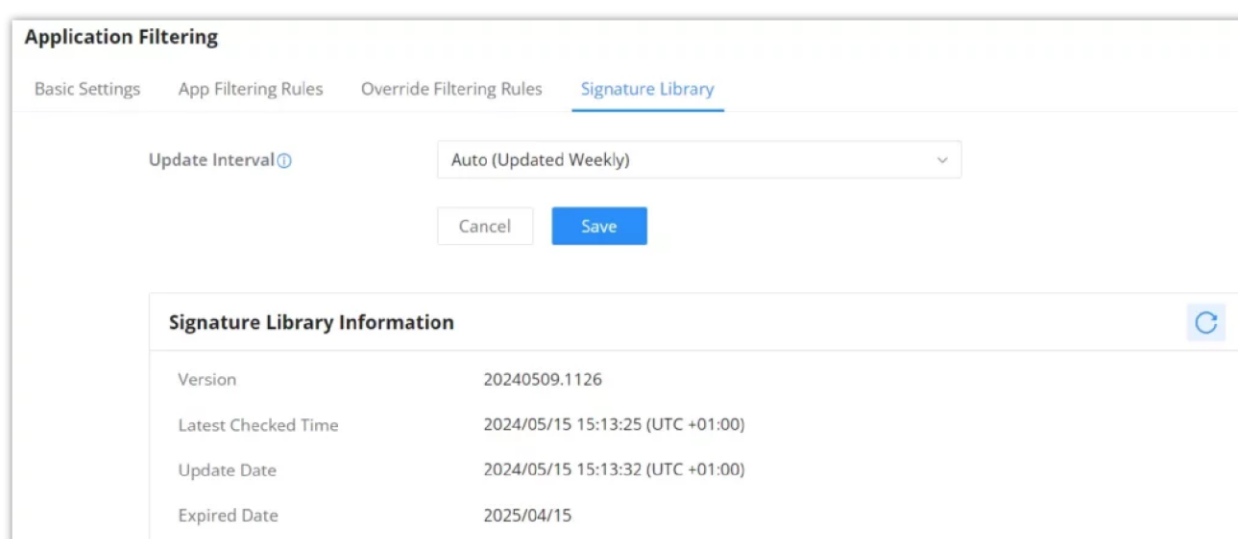
Add/Edit filtering rule

## Signature Library – Application Filtering

On this page, the users can update the Application Filtering signature library information manually, update daily or create a schedule, please refer to the figure below:

### Note:

By default, it is updated at a random time point (00:00-6:00) every day.



## SSL PROXY

An SSL proxy is a server that uses SSL encryption to secure data transfer between a client and a server. It operates transparently, encrypting and decrypting data without being detected. Primarily, it ensures the safe delivery of sensitive information over the internet.

When the SSL Proxy is enabled, the GCC601x(w) will act as an SSL Proxy server for the connected clients.

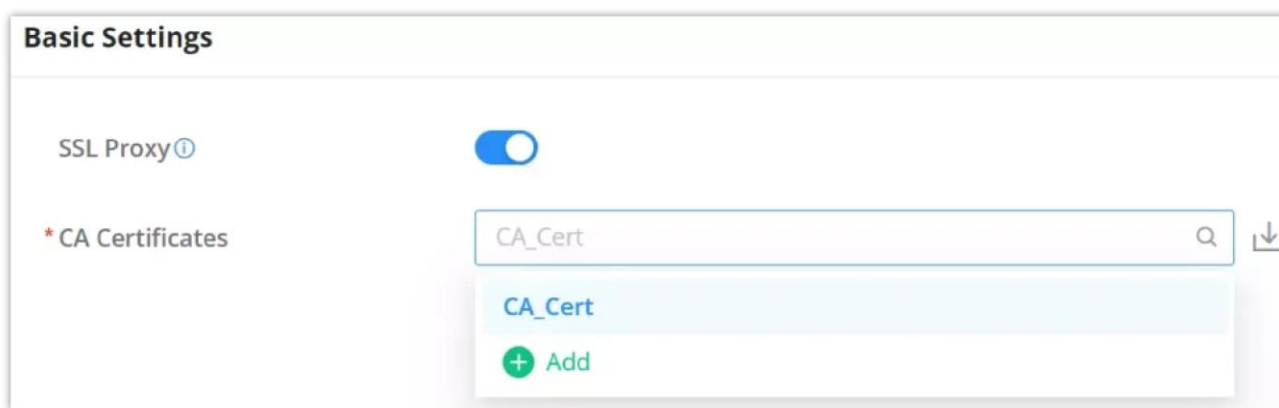
### Basic Settings – SSL Proxy

Turning on features like SSL Proxy, Web Filtering, or Anti-malware helps detect certain types of attacks on websites, such as SQL injection and cross-site scripting (XSS) attacks. These attacks try to harm or steal information from websites.

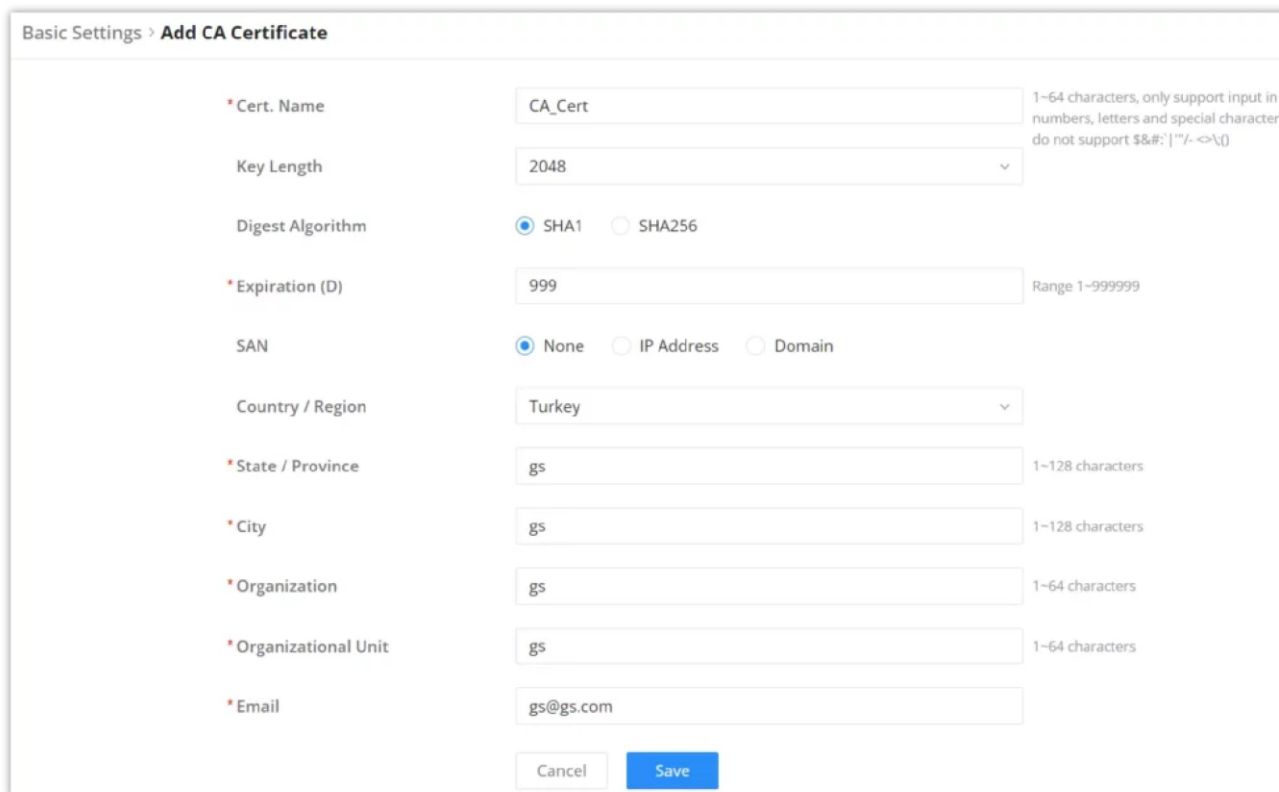
When these features are active, they generate alert logs under **Security Log**.

However, when these features are turned on, users might see warnings about certificates when they browse the web. This happens because the browser doesn't recognize the certificate being used. To avoid these warnings, users can install the certificate in their browser. If the certificate isn't trusted, some applications might not work correctly when accessing the internet

For HTTPS filtering, users can enable SSL proxy by navigating to **Firewall module** → **SSL Proxy** → **Basic Settings**, then toggle ON SSL proxy, after either selecting the CA Certificate from the drop-down list or clicking on the **"Add"** button to create a new CA certificate. Please refer to the figures and table below:



Enable/disable SSL Proxy



SSL Proxy – Add CA Certificate

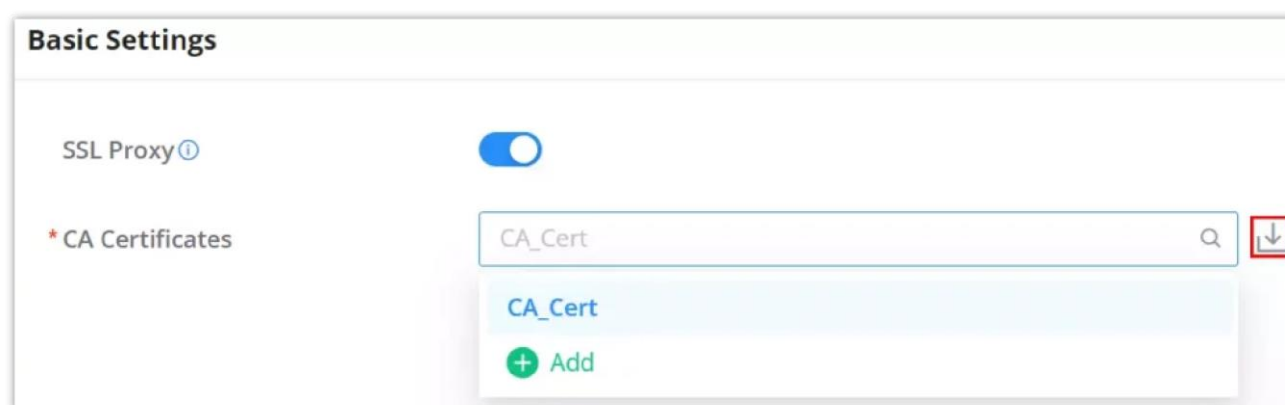
<b>Cert. Name</b>	Enter the Certificate name for the CA. <b>Note:</b> It could be any name to identify this certificate. Example: "CATest".
<b>Key Length</b>	Choose the key length for generating the CA certificate. The following values are available:



	<ul style="list-style-type: none"> <li>• <b>1024:</b> 1024-bit keys are no longer sufficient to protect against attacks.</li> <li>• <b>2048:</b> 2048-bit keys are a good minimum. (Recommended).</li> <li>• <b>4096:</b> 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.</li> </ul>
<b>Digest Algorithm</b>	<p>Choose the digest algorithm:</p> <ul style="list-style-type: none"> <li>• <b>SHA1:</b> This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input.</li> <li>• <b>SHA256:</b> This digest algorithm generates an almost unique, fixed-size 256 bit hash.</li> </ul> <p><b>Note:</b> Hash is a one-way function, it cannot be decrypted back.</p>
<b>Expiration (D)</b>	<p>Enter the validity date for the CA certificate in days. The valid range is 1~999999..</p>
<b>SAN</b>	<p>Enter the address IP or the domain name of the SAN (Subject Alternate Name).</p>
<b>Country / Region</b>	<p>Select a country code from the dropdown list. Example: "United Stated of America".</p>
<b>State / Province</b>	<p>Enter a state name or province. Example: "Casablanca".</p>
<b>City</b>	<p>Enter a city name. Example: "SanBern".</p>
<b>Organization</b>	<p>Enter the organization's name. Example: "GS".</p>
<b>Organizational Unit</b>	<p>This field is the name of the department or organization unit making the request. Example: "GS Sales".</p>
<b>Email</b>	<p>Enter an email address. Example: "EMEAregion@grandstream.com"</p>

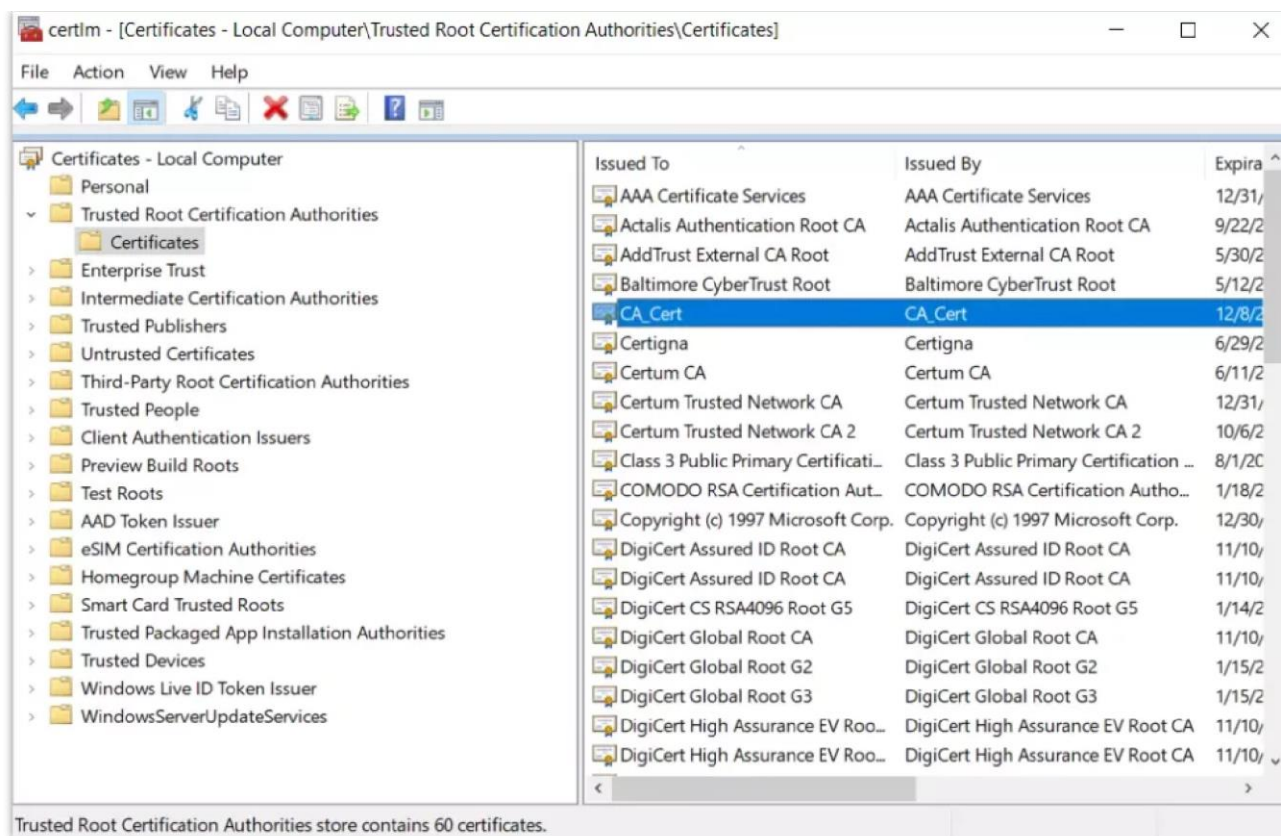
SSL Proxy – Add CA Certificate

For the SSL Proxy to take effect, users can manually download the CA certificate by clicking on the download icon as shown below:

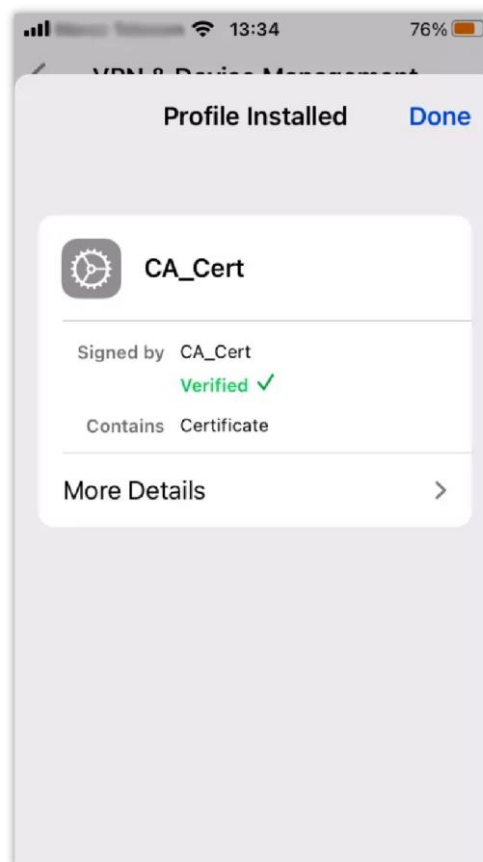


SSL Proxy – Download the CA certificate

Then, the CA certificate can be added to the intended devices under the trusted certificates.



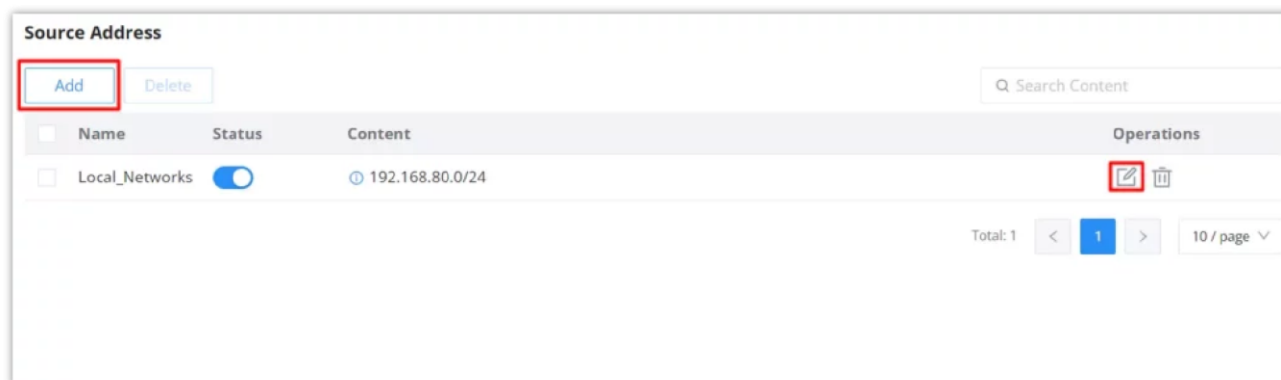
SSL Proxy – add CA certificate to Windows



SSL Proxy – add CA certificate to a phone

## Source Address

When no source addresses are specified, all outgoing connections are automatically routed through the SSL proxy. However, upon manually adding new source addresses, only those specifically included will be proxied through SSL, ensuring selective encryption based on user-defined criteria.



SSL Proxy – Source Address

SSL Proxy – add/edit source address

## SSL Proxy Exemption List

SSL proxy involves intercepting and inspecting SSL/TLS encrypted traffic between a client and a server, which is commonly done for security and monitoring purposes within corporate networks. However, there are certain scenarios where SSL proxy may not be desirable or practical for specific websites or domains.

The exemption list allows users to specify their IP address, domain, IP range, and web category to be exempted from SSL proxy.

Click on the **“Add”** button to add an SSL exemption as shown below:

SSL proxy exemption list

Under the “Content” option, the users can add content by clicking on the “+ icon” button and delete by clicking on the “– icon” as shown below:

Add/edit SSL Exempted Address

## SECURITY LOG

### Log

On this page, security logs will listed with many details such as Source IP, Source interface, Attack Type, Action, and Time. Click on the **“Refresh”** button to refresh the list and the **“Export”** button to download the list to the local machine.

The users have also the option to filter the logs by:

1. Time

2. Attack

Sort log entries by:

- 1. Source IP
- 2. Source Interface
- 3. Attack Type
- 4. Action

**Security Log**

Log E-mail Notifications

Logs are retained by default for 180 days. When disk space reaches the threshold, security logs will be automatically cleared.

Refresh Export 2024-05-16 → 2024-05-16 DoS & Spoofing Source IP Search

No.	Source IP	Source Interface	Attack Type	Action	Time	Details
1	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:35	ⓘ
2	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:34	ⓘ
3	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:34	ⓘ
4	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:33	ⓘ
5	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:33	ⓘ
6	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:32	ⓘ
7	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:32	ⓘ
8	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:31	ⓘ
9	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:31	ⓘ

Total: 796 1 2 3 ... 80 10 / page Go to

Security log

**Note:**

Logs are retained by default for 180 days. When disk space reaches the threshold, security logs will be automatically cleared.

For more details, click on the “**exclamation icon**” under the Details column as shown above:

**Details**

No.: 1  
Time: 2024-03-19 13:36:50  
Source IP: 192.168.80.235  
DNS Domain Name: example.org  
Filter Quantity: 2  
Description: DNS\_Filtering  
Action: block

Prev Next

Security log – details

When the users click on “**Export**” button, an Excel file will be downloaded to their local machine. Please refer to the figure below:

	A	B	C	D	E	F
1	Time	Source IP	Source Interface	Attack Type	Filter Quantity	Action
2	####	192.168.5.128	NET5	Port Scan	35	block
3	####	192.168.5.222	NET5	Port Scan	7	block
4	####	192.168.5.222	NET5	Port Scan	23	block
5	####	192.168.5.222	NET5	Port Scan	2	block
6	####	192.168.5.222	NET5	Port Scan	21	block
7	####	192.168.5.222	NET5	Port Scan	23	block
8	####	192.168.5.222	NET5	Port Scan	12	block
9	####	192.168.5.222	NET5	Port Scan	24	block
10	####	192.168.5.222	NET5	Port Scan	22	block
11	####	192.168.5.222	NET5	Port Scan	23	block
12	####	192.168.5.222	NET5	Port Scan	15	block
13	####	192.168.5.222	NET5	Port Scan	11	block
14	####	192.168.5.222	NET5	Port Scan	25	block
15	####	192.168.5.222	NET5	Port Scan	11	block
16	####	192.168.5.222	NET5	Port Scan	23	block
17	####	192.168.5.222	NET5	Port Scan	25	block
18	####	192.168.5.222	NET5	Port Scan	23	block
19	####	192.168.5.222	NET5	Port Scan	11	block
20	####	192.168.5.222	NET5	Port Scan	23	block
21	####	192.168.5.222	NET5	Port Scan	23	block
22	####	192.168.5.1	NET5	ARP Spoofing (Source MAC)	1	block
23	####	192.168.5.222	NET5	Port Scan	11	block
24	####	192.168.5.1	NET5	ARP Spoofing (Source MAC)	1	block
25	####	192.168.5.222	NET5	Port Scan	23	block
26	####	192.168.5.222	NET5	Port Scan	24	block
27	####	192.168.5.70	NET5	Port Scan	224	block
28	####	192.168.5.70	NET5	Port Scan	277	block

Security log – Export (Excel file)

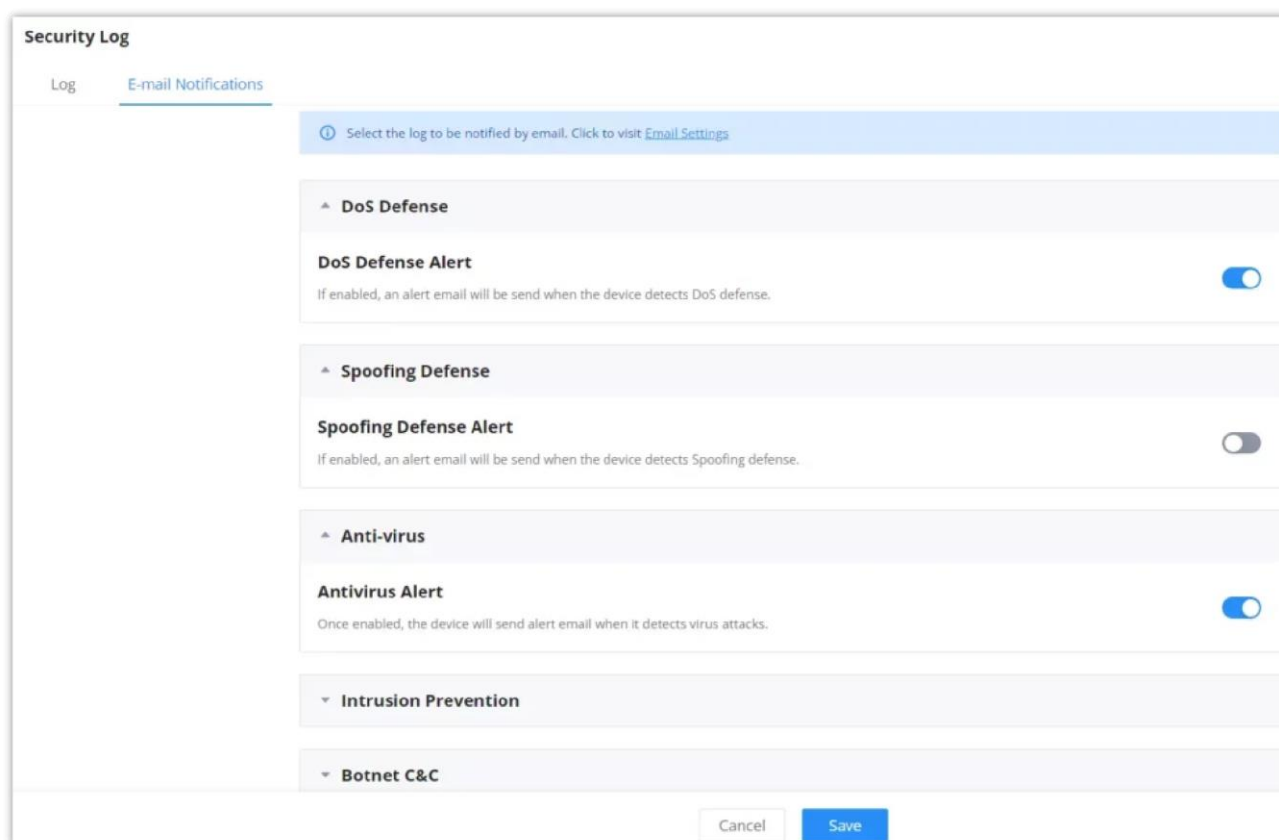
## E-mail Notifications

On the page, the users can select what security threats to be notified of using E-mail addresses.

Select what you want to be notified about from the list.

### Note:

Email Settings must be configured first, click on “**Email Settings**” to enable and configure E-mail notifications. Please refer to the figure below:



The screenshot shows the 'Security Log' configuration page with the 'E-mail Notifications' tab selected. A blue banner at the top says 'Select the log to be notified by email. Click to visit Email Settings'. Below this, there are three main sections:

- DoS Defense:** 'DoS Defense Alert' is enabled (toggle is on). Description: 'If enabled, an alert email will be send when the device detects DoS defense.'
- Spoofing Defense:** 'Spoofing Defense Alert' is disabled (toggle is off). Description: 'If enabled, an alert email will be send when the device detects Spoofing defense.'
- Anti-virus:** 'Antivirus Alert' is enabled (toggle is on). Description: 'Once enabled, the device will send alert email when it detects virus attacks.'

At the bottom, there are two more collapsed sections: 'Intrusion Prevention' and 'Botnet C&C'. 'Cancel' and 'Save' buttons are located at the bottom right of the configuration area.

E-mail Notifications