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.

irewall Service		>	Top Security I	og			DoS & Spoofing	- 5
irewall Service Name	Enterprise		Source IP	Source Interface	Attack Type	Action	Time	
			192.168.5.51	NET5	Port Scan	monitor	2024/05/21	10:2
ffective Date	2024/03/26		192.168.5.1	NETS	Port Scan	monitor	2024/05/21	10:2
xpired Date	2025/03/26		192.168.5.12	8 NET5	Port Scan	monitor	2024/05/21	10:2
ackage Status	Licensed		192.168.5.51	NET5	Port Scan	monitor	2024/05/21	10:2
			192.168.5.1	NET5	Port Scan	monitor	2024/05/21	10:2
votection Statistics		⇔ ©	Top Filtered A	pplications				
			No. App	s			Count	
			1 You	Tube			53	
	۶)		2 Skyr	oe			48	
			3 Ado	be Experience Cloud			45	
6	6929	26	4 Poc	tet			29	
	Defended Assesses	Filment Amelianian	5 Goo	ele Analytics			24	

Overview part 1

Virus Files	
Major	0 11



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.

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

Rules Policy page

ules Policy > WAN1				
Inbound Policy	🔵 Accept 🛛 💿 Reject	: O Drop		
IP Masquerading				
MSS Clamping				
Log Drop / Reject Traffic				
Drop / Reject Traffic Log Limit	10	second	^	The range is 1~99999999, if it is empty there is no limit
	Cancel	second		
	Cancel Save	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 masque 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.

Inbound Ru	ules											
Add									All Source	Groups		~
Name		Status	IP Family	Protocol Type	Source Group	Source MAC Address	Source IP Address	Source Port	Desi	Opera	ions	
Anti-lo	ockout-Rule		Any	TCP	Default (VLAN)			8		≢ 0	Î	
Allow-	DHCP-Ren		IPv4	UDP	WAN1 (WAN)			-		≢ 0	1 Ē	
Allow-	Ping		IPv4	ICMP	WAN1 (WAN)		*			≑ 0	î Ū	
Allow-	IGMP		IPv4	IGMP	WAN1 (WAN)	r.				≑ 0	10	
Allow	DHCPv6		IPv6	UDP	WAN1 (WAN)		fe80::/10	-	fe80	≢ 0	1	
Allow-	MLD		IPv6	ICMP	WAN1 (WAN)		fe80::/10	-		≑ 0	ŝ Ū	
Allow-	ICMPv6-In		IPv6	ICMP	WAN1 (WAN)		2	8		≢ 0	3 10	
Allow-	DHCP-Ren		IPv4	UDP	WAN2 (WAN)					≑ 0	î Ū	
Allow-	Ping		IPv4	ICMP	WAN2 (WAN)					≢ 0	ŝ Ū	
Allow-	IGMP		IPv4	IGMP	WAN2 (WAN)		2	2		≢ 0	Î	
Allow-	DHCPv6		IPv6	UDP	WAN2 (WAN)		fe80::/10		fe80	≢ 0	Î	
Allow-	MLD		IPv6	ICMP	WAN2 (WAN)		fe80::/10			≢ 0	3 10	

Firewall Policy – Inbound Rules

Inbound Rules > Add Inbound Rule		
*Name	SSH	1–64 characters
Status		
IP Family	Any IPv4 IPv6	
Protocol Type	TCP ~]
* Source Group ()	All	
Source MAC Address		
Source IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
Source Port ()	22	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 🕕	22	The valid range is 1-65535. You can enter a single port or a port range.
Action ()	Accept Deny Drop	
	Cancel Save	

Inbound Rules – Add/Edit

Name	Enter the name of the inbound rule.
Status	Toggle on/off the status of the inbound rule.
IP Family	 Pick the IP family. Any IPv4 IPv6
Protocol Type	Choose the protocol type. UDP UDP/TCP IGMP All
Source Group	If set to "All", rules will be matched in preference to other specific ones.
Source MAC Address	Specify the source MAC address.
Source IP Address	Specify the source IP address.
Source Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.

Destination IP Address	Specify the destination IP address.
Destination Port	To enter multiple port/port ranges, separate them using commas (,), for example:4,5-10.
Action	If set to "Accept", the external devices are allowed to access the router; if set to "Deny", the access of the external devices is denied and the result is returned; if set to "Drop", the access request of the external device will be directly droped.

Traffic Rules – Inbound Rules

Forwarding Rules

GCC601X(W) offers the possibility to allow traffic between different groups and interfaces (WAN/VLAN/VPN).

To add a forwarding rule, please navigate to **Firewall Module** \rightarrow **Firewall Policy** \rightarrow **Forwarding Rules**, then click on the "**Add**" button to add a new forwarding rule or click on the "**Edit**" icon to edit a rule.

orwarding	Rules									
Add						All Source Groups	~	All Dest	tination Groups	
Name		Status	IP Family	Protocol Type	Source Group	Source MAC Address	Source IP Ad	ldress	5 Operations	
Allow-I	CMPv6		IPv6	ICMP	WAN1 (WAN)	•			· 章 🗹 🗇	
Allow-I	CMPv6		IPv6	ICMP	WAN2 (WAN)		*		· 章 🗹 🔟	
Allow-I	CMPv6		IPv6	ICMP	WAN3 (WAN)	ä.	÷		· 章 🗹 🗇	
Forwar	rding_r		Any	UDP	All				· 章 🗹 🔟	

Add Forwarding Rule

Forwarding Rules > Add Forwarding Rule		
*Name	Forwarding rule	1~64 characters
Status		
IP Family	Any IPv4 IPv6	
Protocol Type	All ~	
* Source Group ()	Default (VLAN)	
Source MAC Address		
Source IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
*Destination Group 🛈	TechSupport (VLAN) \times \checkmark	
Destination IP Address		Enter the IP address/mask length, such as "192.168.122.0/24"
Action ()	Accept Deny Drop	
	Cancel Save	

Add Forwarding Rule

Advanced NAT

NAT or Network address translation as the name suggests it's a translation or mapping of private or internal addresses to

public IP addresses or vice versa, and the GCC601X(W) supports both.

• **SNAT**: Source NAT refers to the mapping of clients' IP addresses (Private or Internal Addresses) to a public one.

• **DNAT:** Destination NAT is the reverse process of SNAT where packets will be redirected to a specific internal address.

The Firewall Advanced NAT page provides the ability to set up the configuration for source and destination NAT. Navigate to **Firewall Module** \rightarrow **Firewall Policy** \rightarrow **Advanced NAT**.

SNAT

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

Advanced NAT							
SNAT DNA	AT						
Add Del							
Name	Status	IP Family	Protocol Type	Source IP Address	Rewrite Source IP Address	Destination Group	Operations
SNAT		IPv4	UDP/TCP	192.168.122.0/24	192.168.5.0	WAN1 (WAN)	ľ

SNAT page

Add SNAT

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

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

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

Advanced NAT – DNAT

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.

Global Configuration					
Flush Connection Reload 🛈					
	Cancel	Save			

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	IP Exception	
	DoS Defense	
	Action ()	O Monitor 💿 Block
	Flood Attack Defense	
	TCP SYN Flood Attack Defense	
	*TCP SYN Flood Packet Threshold (packets/s)①	2000
	*TCP SYN Flood Timeout (sec) ①	10
	UDP Flood Attack Defense	
	ICMP Flood Attack Defense	
	ACK Flood Attack Defense	
	Abnormal Packet Attack Def	ense
	Port Scan Detection	
	Block IP Options	
		Cancel Save

DoS Defense – Basic Settings

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

ActionSelect the action:ActionMonitor: An alarm is generated but is not blocked.Block: Monitor and block attacks.		
	Flood Attack Defense	
TCP SYN Flood Attack Defense	 When this option is enabled, the router will take counter measures to SYN Flood Attack. TCP SYN Flood Packet Threshold (packets/s): 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. TCP SYN Flood Timeout (sec): If the number of TCP SYN packets received per second exceeds the threshold within the specified timeout period, attack defense will start immediately. 	
UDP Flood Attack Defense	 When this option is enabled, the router will take counter measures to the UDP Flood Attack. UDP Flood Packet Threshold (packets/s): 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. UTCP SYN Flood Timeout (sec): If the average number of received UDP packets per second reaches the threshold within the timeout period, attack defense will start immediately. 	
ICMP Flood Attack Defense	 When this option is enabled, the router will take counter measures to the ICMP Flood Attack. ICMP Flood Packet Threshold (packets/s): 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. ICMP Flood Timeout (sec): If the average number of received ICMP packets per second reaches the threshold within the timeout period, attack defense will start immediately. 	
ACK Flood Attack Defense	 When this option is enabled the router will take counter measures to ACK Flood Attack. ACK Flood Packet Threshold (packets/s): 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. ACK Flood Timeout (sec): If the average number of received ACK packets per second reaches the threshold within the timeout period, attack defense will start immediately. 	
	Abnormal Packet Attack Defense	

Port Scan Detection	 When this option is enabled, the router will take counter measure to the port scanning attempts Port Scan Packet Threshold (packets/s): If the port packets reach the threshold, port scanning detection will start immediately.
Block IP Options	When this option is enabled, the router will ignore any IP packets with Options field.
Block TCP Flag Scan	When this option is enabled, the router will ignore any packets with unexpected information in the TCP flags.
Block Land Attack	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

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

Basic Settings IP Exception IP Exception Image: The IPs in the list will not perform DoS defense detection. Add Delete Name Status Content Oper				DoS Defense
The IPs in the list will not perform DoS defense detection. Add Delete Q Search IP address Name Status Content Oper			IP Exception	Basic Settings
Add Delete Q. Search IP address Name Status Content Operation		defense detection.	ist will not perform DoS	① The IPs in the list
Name Status Content Ope	Search IP address			Add Dele
	Operations	Content	Status	Name
Printer 🔘 0 192.168.80.11/32	CA m	() 192.168.80.11/32		Printer

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 Exc	ception	
*Name	Printer	1–64 characters
Status		



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

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** \rightarrow **Anti-Malware** \rightarrow **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.

Configuration	
① To detect HTTPs URL, please enable	'SSL Proxy".
Anti-malware 🛈	
* Data Packet Inspection Depth ①	High ~
Scan Compressed Files ①	
	Cancel Save

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 L	og							
Log	E-mail Notifications							
Logs a	re retained by default for 180 da	ys. When disk space reac	hes the threshold, secu	rity logs will be automati	cally cle	ared.		
Refresh	Export		2024-05-15	→ 2024-05-15	₿	Anti-malware	^	Source IP
No.	Source IP	URL		Description		DoS & Spoofing		Time
						IDS / IPS		
				3 PM		Botnet		
				1		Web Filtering		
						Anti-malware		
				No data		APP Filtering		
				NO Uata				

Security log – Anti-malware

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			
Update Interval ①	Auto (Updated Daily)	⊗ Q.	
	Auto (Updated Daily)		
	Create Schedule		
Signature Library Info	mation		C
Signature Library Version	20240515.1246		
Latest Checked Time	2024/05/15 11:32:10 (UTC +01:00)		
Update Date	2024/05/15 11:32:17 (UTC +01:00)		
Expired Date	2025/04/15		

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.

ings IP Exception	
Mode () Notify	Notify & Block O No Action
Security Protection Level () High	~
Security Protection Level () High	



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:

asic Settings	IP Exception		
	Mode ①	Notify Notify Notify & Block No Action	
	Security Protection Level	Custom	^
	V Total (19/19)	Low Medium	
	 ✓ Web Attacks ✓ Injection ✓ Brute Force ✓ File Upload 	High Extremely High Custom	cploitation of Vulnerabilities
	Vetwork Anomalies	S 🔽 Phishing 🔽 Tunnel 🔽 IoT	
	 ✓ Bad Files ✓ Trojan ✓ CoinMiner 	🗹 Worm 🔽 Ransomware 💟 APT 💟 Webshell	✓ Hacking Tools
	* WAN Interfaces	WAN1 (WAN) \times	~

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 L	og								
Log	E-mail Notifications								
Refresh	Export					IDS/IPS ^ T	fhreat Level 🗸 🗸	Q Search	
No.	Threat Level	Source IP	Destination IP Address	Intrusion ID	Intrusion	DoS & Spoofing	Time 🗘		Details
1	Medium	192.168.5.103	192.168.5.141	2013929	ET POLICY on port 44	Botnet Web Filtering	2024-03	8-19 15:21:00	0
2	Medium	192.168.5.103	192.168.5.141	2101411	GPL SNMP access udp	Anti-virus	2024-03	1-19 15:20:53	()
3	Medium	192.168.5.113	192.168.5.141	2013929	ET POLICY on port 44	APP Filtering DNS Filtering	2024-03	1-19 13:30:56	(i)
4	Medium	192.168.5.113	192.168.5.141	2101411	GPL SNMP p access udp	public monitor	2024-03	8-19 13:30:49	0

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				
Basic Settings	Exception			
The IPs in this list	t will not be detected	t by IPS.		
		a uy n o.		
Add Delet				Q. Search Name / IP Address
Name	Status	Туре	Content	Operations
Local_NAS		Source	0 192.168.5.0/24	۵ d



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 > Edit IP Exception			

* Name	Local_NAS	1~64 characters
Status		
Туре	Source ~]
* Content	IP Address / > 192.168.5.0/24	Prefix Length range 1~32
	Add	• •
	Cancel Save	

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.

Botnet				
Basic Settings	IP / Domain Name Exception			
	Botnet IP 🕕	 Monitor 	O Block	O No Action
	Botnet Domain Name 🛈	O Monitor	 Block 	O No Action
		Cancel	Save	

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:

Botnet			
Basic Settings	P / Domain Name	Exception	
① The IP and doma	ain names in the list	vill not be detected by threat intelligence. Valid for WAN botnet IP.	
Add Dele			Q Search Name / IP Address /
Name	Status	IP Address / Domain Name	Operations
Local_Printer		① 192.168.5.11	Ē
			Total: 1 < 1 > 10 / page V

Botnet – IP/Domain name exception

Botnet > Edit IP / Domain Name Exception				
*Name	Local_Printer	1~64 characters		



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:

1 Note:

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

Signature Library		
Update Interval 🕕	Auto (Updated Daily)	×
	Cancel Save	
Signature Library Info	rmation	C
Version	20240516.1035	
Latest Checked Time	2024/05/16 12:59:13 (UTC +01:00)	
Update Date	2024/05/16 10:10:58 (UTC +01:00)	
Expired Date	2025/04/15	

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** \rightarrow **Content Control** \rightarrow **DNS Filtering**. Click on the "**Add**" button to add a new DNS Filtering as shown below:

DNS Filtering						
Add Delete	Add Delete					DNS
Priority	Name	Status	DNS		Action	Operations
□ 1	DNS_Filter		(i) *example*		e Block	≐ 🗹 🗇

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.

DNS Filtering > Add DNS Filtering		
*Name	DNS_Filter	1~64 characters
Status		



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:

			L		
Source IP	DNS Domain	Description	Action	DoS & Spoofing	
192.168.80.235	example.org	DNS_Filtering	block	IDS / IPS	14
192.168.80.235	example.org	DNS_Filtering	block	Botnet Web Filtering	14
192.168.80.235	example.org	DNS_Filtering	block	Anti-virus	14
192.168.80.235	example.org	DNS_Filtering	block	APP Filtering	14
192.168.80.235	example.org	DNS_Filtering	block	DNS Filtering	14

DNS Filtering on the overview page

Security L	og					
Log	E-mail Notifications					
Refresh	Export			DNS Filtering ^ Se	ource IP v Q. Search	
No.	Source IP	DNS Domain Name	Description	DoS & Spoofing	Time 🗘	Details
1	192.168.80.235	example.org	DNS_Filtering	IDS / IPS	2024-03-19 14:30:15	0
2	192.168.80.235	example.org	DNS_Filtering	Botnet Web Filtering	2024-03-19 14:29:36	(j)
3	192.168.80.235	example.org	DNS_Filtering	Anti-virus	2024-03-19 14:28:12	()
4	192.168.80.235	example.org	DNS_Filtering	APP Filtering	2024-03-19 14:25:35	()
5	192.168.80.235	example.org	DNS_Filtering	DNS Filtering	2024-03-19 14:23:35	(1)

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	D			
		Cancel	/e	

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 \rightarrow Content Filtering \rightarrow Web Filtering page \rightarrow URL Filtering tab, then

click on the "**Add**" button as shown below:

eb Filtering					
Basic Settings	URL Filtering URL	Category Filtering	Keywords Filtering URL Signature Library		
Add Dele				Q Search	URL
Priority	Name	Status	URL	Action	Operations
1	URL_Filering		① *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	
*URL①	Wildcard ~ *example*	e 1~128 characters
	Add	•
	Cancel Save	

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:

Veb Filtering Basic Settings URL	Filtering URL Categor	ry Filtering Keywords Filter	ring URL Signature Lib	rary		
Adult	All BLOCK 🕎	🗢 🗸 Adult	🗢 🗸 Lingerie	Mixed Adult	Sexual Education	3
Advertisement	All BLOCK	 Marketingwa re 	🥑 🗸 Publicite			
Attacks and Threats	All BLOCK v	● ∨ Agressif	🗢 🗸 DDoS	🕒 🗸 Hacking	🗢 🗸 Phishing	
Bad Websites	Mix ~	✓ Bitcoin	⊘ ∽ Cryptojackin g	Dangerous M aterial	🗢 🗸 Drogue	🖨 🗸 Gamblin
		🥑 🗸 Stalkerware				
Entertainment	All Allow ~	🥥 🤟 Audio Video	🥥 🗸 Manga	🖉 ~ Mobile Phon e	🥥 🗸 Radio	
Finance	All Allow ~	🥑 🗸 Bank	🥏 ~ Financial			
Game	All Allow ~	Sames	🥥 🜱 Games			
Network	All Allow 🗸	🥑 🗸 Redirector	⊘ ∨ Remote Cont	🕑 🗸 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** \rightarrow **Content Filtering** \rightarrow **Web Filtering page** \rightarrow **Keywords Filtering tab**, then click on the "**Add**" button as shown below:



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:

Web Filtering > Edit Keywords Filterin	g	
* Name	Keywords_Filtering	1-64 characters
Status		
Action	Allow 💿 Block	
* Filtered Content 🛈	Wildcard ^ *youtube*	😑 1~128 character
	Wildcard	Add 🕕
	Regular Expression	

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:

 Grandstream Firewall Alert 	× +	
← → C 😫 youtube.com		
6		
		The web page you visit is risky.
	The pa	ge you have requested has been blocked because it contains a banned word.
	URL:	https://www.youtube.com/
	Detail:	Match content filter:Keywords_Filtering
	For more is	nformation, contact the administrator.

Example of keywords_filtering on the Browser

For more details about the alert, the users can navigate to the **Firewall module** \rightarrow **Security Log**.

ecurity L	og					
Log	E-mail Notifications					
Refresh	Export			Web Filtering	~ URL ~ Q Search	
No.	Source IP	URL	Description	Action	Time ÷	Details
21	192.168.80.235	Name and Address of the Address of the	Match content filter:Keywords_Filtering	block	2024-03-19 13:25:19	(
22	192.168.80.235	The second se	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:34	0
23	192.168.80.235		Match content filter:Keywords_Filtering	block	2024-03-19 13:23:31	0
24	192.168.80.235	The second s	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:17	0
25	192.168.80.235	1000 - 1000 - 1000 - 1000	Match content filter:Keywords_Filtering	block	2024-03-19 13:23:10	0
26	192.168.80.235	here and a set of the	Match content filter:Keywords_Filtering	block	2024-03-19 13:22:56	0
27	192.168.80.235	https://www.youtube.com/	Match content filter:Keywords_Filtering	block	2024-03-19 13:19:40	0

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								
Basic Settings	URL Filtering	URL Category Fil	ltering	Keywords Filterin	ig l	JRL Signature Library		
l	Update Interval 🕕		Auto (U	Ipdated Weekly)			\otimes	Q
			Auto (Updated Weekly)				
			🕂 Cre	eate Schedule				
	Signature Libr	ary Informatio	on 🖸					
	Version		202	240309.1500				
	Update Date		(+0	1+0100) 2024/03/14	4 15:14	:09		
	Expired Date		-					

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

1 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

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

Basic Settings App Filtering Rules	s Overri	de Filtering Rules Signatu	ure Library					
Advertisement and Advertisement	• ~	App-Stores and OS Updates (14)	•	Audio Entertainment (58)	o ~	Books and Magazines (18)	•	Browsers (4)
Block Jsiness (62)	0 ~	Cloud and CDN Services (49)	e ~	Conference (21)	• ~	Database (3)	•	Development Tools and Services (92)
Device Security (31)	•	E-Commerce (38)	o ~	Education (36)	0 ~	Enterprise Services (186)	•	File Transfer (29)
🥑 🗸 Finance (60)	•	Food and Drink (13)	• ~	Gaming (257)	o ~	Health and Fitness (19)	•	M2M and IoT (1)
🥝 🗸 Mail (12)	• •	Messaging (54)	• •	Multimedia Service Providers (80)	•	Navigation (21)	• •	Network Management (15)
9 ~ News (56)	o ~	Organizers (13)	• ~	Peer to Peer (13)	0 ~	Remote Control (9)	•	Search Engine (8)
Sharehosting (34)	•	Smart Home (3)	• ~	Social (106)	• ~	Streaming (228)	•	Travel and Transportatio (35)
• v Tunnel (93)	• ~	Virtual and Augmented Reality (2)	• ~	Voice over IP (24)	• •	Wallet (1)		

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:

Jasic Se	ttings App Hitering Kule	S Override	Advertise	ment and Analyti	: Services (162) $ imes$			
• •	Advertisement and	• ~ A	6Sense	Aarki	AdForm	and Magazines (18)	•	Browsers (4)
	Analytic Services (102)	-	AdSafeProtected	AdTiming	Adcolony			
9 ~	Business (62)	⊘ ~ C (•	Adex	Adjust	Admixer	ase (3)	0 ~	Development Tools and Services (92)
	_		Adobe Experience Clo	Adtech Studio	Adtelligent		-	
• •	Device Security (31)	O ~ E	Airship	Amazon Ads	Amobee	orise Services (186)	• •	File Transfer (29)
•	Finance (60)	O ~ F	Amplitude	Aniview	Anzu VR	and Fitness (19)	•	M2M and IoT (1)
	Mail (12)	0 v 1	AppDynamics	AppLovin	AppMetrica	ation (21)	•	Network Management
			Apple Advertising	AppsFlyer	Apptentive		-	(15)
	News (56)	• · · ·	Apteligent	Avo	Bebi	te Control (9)	0 ~	Search Engine (8)
			Beeswax	Bombora	Branch			
3 ~	Sharehosting (34)	o ~ s	Reight Data	Rumanan	CatchMadia	ning (228)	0 ~	Travel and Transportation (35)

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.

Security L	og								
Log	E-mail Notifications								
Refresh	Export			[APP Filtering	App Name	Ŷ	Q Search	
No.	Source IP	Destination IP Address	App Name	Descriptio	DoS & Spoofing IDS / IPS		Time 🗘		Details
121	192.168.80.235	142.250.200.142	YouTube	youtube	Botnet		2024-03	3-19 13:36:19	
122	192.168.80.235	142.250.200.142	YouTube	youtube	Web Filtering		2024-03	3-19 13:36:13	(j)
123	192.168.80.235	142.250.184.174	YouTube	youtube	Anti-virus		2024-03	3-19 13:36:03	0
124	192.168.80.235	74.125.3.166	YouTube	youtube	DNS Filtering		2024-03	3-19 13:35:52	0
125	192.168.80.235	173.194.141.8	YouTube	youtube	block		2024-03	3-19 13:35:43	()

Example of application filtering on GCC security log

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

Details ×

No.: 1
Time: 2024-03-19 13:37:43
Source IP: 192.168.80.235
Destination IP Address: 142.250.200.142
App Name: YouTube
Filter Quantity: 1
Description: youtube
Action: block
Prev Next

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						
App Filtering Rules	Override Filte	ring Rules Signature Library				
Name	Status	Apps	Action	Operations		
Block		⑤ 6Sense,AdTiming,Aniview,Aarki,Adcolony,Beeswax	😑 Block	≡ 🗹 🗇		
Allow		① Avo,Branch,Beeswax,Bright Data	Allow	≡ ⊠ ⊡		
	ring App Filtering Rules te Name Block Allow	App Filtering Rules Override Filter Name Status Block O Allow O	Name Status Apps Block Image:	Name Status Apps Action Block Image: I		

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:

Application Filtering > Add F	iltering Rule			
* Nar	ne	Block		1-64 characters
Star	tus			
Act	ion	Allow 🖲 Block		
- AF	Selected(6)		All Filter Applicatio 🗸	Q Search App Name
	 Advertisement and A 	nalytic Services (162)		
	6Sense	🔽 Aarki	AdForm	AdSafeProtected
	AdTiming	Adcolony	Adex	Adjust
	Admixer	Adobe Experience Cloud	Adtech Studio	Adtelligent
	Airship	Amazon Ads	Amobee	Amplitude
	Aniview	Anzu VR	AppDynamics	AppLovin
	AppMetrica	Apple Advertising	AppsFlyer	Apptentive
	Apteligent	Avo	Bebi	Beeswax
	Bombora	Branch	Bright Data	Bugsnag
	CatchMedia	Chartbeat	Chartboost	Conductrics
		Cancel	Save	

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:

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

Application Filtering		
Basic Settings App Filtering Re	ules Override Filtering Rules Signature Libra	ary
Update Interval ()	Auto (Updated Weekly)	~
	Cancel Save	
Signature Lib	orary Information	C
Version	20240509.1126	
Latest Checked	d Time 2024/05/15 15:13:25 (UTC +	-01:00)
Update Date	2024/05/15 15:13:32 (UTC +	-01:00)
Expired Date	2025/04/15	

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** \rightarrow **SSL Proxy** \rightarrow **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:

Basic Settings		
SSL Proxy ①		
* CA Certificates	CA_Cert	م ل√
	CA_Cert	
	🕀 Add	

Enable/disable SSL Proxy

Basic Settings > Add CA Certificate		
* Cert. Name	CA_Cert	1~64 characters, only support input in numbers, letters and special characters. do not support \$£#:\!"/- <>\()
Key Length	2048 ~	
Digest Algorithm	● SHA1 ○ SHA256	
* Expiration (D)	999	Range 1~999999
SAN	None IP Address Domain	
Country / Region	Turkey ~	
* State / Province	gs	1~128 characters
* City	gs	1~128 characters
* Organization	gs	1~64 characters
* Organizational Unit	gs	1~64 characters
* Email	gs@gs.com	
	Cancel Save	

SSL Proxy – Add CA Certificate

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

	 1024: 1024-bit keys are no longer sufficient to protect against attacks. 2048: 2048-bit keys are a good minimum. (Recommended). 4096: 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.
Digest Algorithm	 Choose the digest algorithm: SHA1: This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. SHA256: This digest algorithm generates an almost unique, fixed-size 256 bit hash. Note: Hash is a one-way function, it cannot be decrypted back.
Expiration (D)	Enter the validity date for the CA certificate in days. The valid range is 1~999999
SAN	Enter the address IP or the domain name of the SAN (Subject Alternate Name).
Country / Region	Select a country code from the dropdown list. Example: "United Stated of America".
State / Province	Enter a state name or province. Example: "Casablanca".
City	Enter a city name. Example: "SanBern".
Organization	Enter the organization's name. Example: "GS".
Organizational Unit	This field is the name of the department or organization unit making the request. <i>Example: "GS Sales"</i> .
Email	Enter an email address. Example: "EMEAregion@grandstream.com"

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:

Basic Settings		
SSL Proxy ①		
*CA Certificates	CA_Cert	م 🛃
	CA_Cert	



SSL Proxy – Download the CA certificate

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

File Action View Help ← ←	issued By	_
← ➡ Ż 🗊 ¼ 🖻 🗙 🗑 🔒 🛛 ज	ssued By	
Gertificates - Local Computer Issued To Is	ssued By	
 Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Untrusted Certificates Untrusted Certificates Certum Trusted Network CA Certum Trusted Network CA Certum Trusted Network CA Control Control Contrupol Control Control Control Control Control Control Control	AAA Certificate Services Actalis Authentication Root CA AddTrust External CA Root Baltimore CyberTrust Root CA_Cert Certigna Certum CA Certum Trusted Network CA Certum Trusted Network CA 2 Class 3 Public Primary Certification COMODO RSA Certification Autho COMODO RSA Certification Autho COMODO RSA Certification Autho Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert SSA4096 Root G5 DigiCert Global Root G2 DigiCert Global Root G3 DigiCert High Assurance EV Root CA	Expira ^ 12/31/ 9/22/2 5/30/2 5/12/2 6/29/2 6/11/2 12/8/2 6/29/2 6/11/2 12/31/ 10/6/2 8/1/2C 1/18/2 12/30/ 11/10/ 11/10/ 1/15/2 11/10/ 11/10/ 11/10/ >

SSL Proxy – add CA certificate to Windows

all ? 13:34	76% 🛑
Profile Installed	Done
CA_Cert	
Signed by CA_Cert	
Contains Certificate	
More Details	>

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.

Source Addr	ress
Add	



SSL Proxy – Source Address

Basic Settings > Edit Source Address		
* Name	Local_Networks	1~64 characters
Status		
* Content	IP Address / > 192.168.80.0/24	Prefix Length range 1~32
		Add 🛨
	Cancel Save	

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		
Add Delete		Q, Search IP address/domain name
Name Status	Content	Operations
SSL Exempted	① 192.168.7.0/24,example.com,192.168.80.2-192.168.80.50,Adult	Ľ Ó
		Total: 1 < 1 > 10 / page ∨

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:

SSL Proxy Exemption List > Add SS	5L Exempted Address	
*Name	SSL Exempted Address	1~64 characters
Status		
* Content	IP Address / \vee 192.168.7.0/24	Prefix Length range 1~3
	Domain v example.com	•
	IP Range v 192.168.80.2 - 192.168.80.50	•
	Web Category \lor Adult \times	•
	Adult	0
	Cancel S-	
	Attacks and Threats	
	Bad Websites	
	Entertainment	
	Finance	
	Game	
	Network	

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 Lo	og					
Log	E-mail Notifications					
O Logs an	re retained by default for 180 day	s. When disk space reaches the threshold	security logs will be automatically	r cleared.		
00	, , , , , , , , , , , , , , , , , , , ,		· · · · · · · · · · · · · · · · · · ·			
Refresh	Export	2024-	05-16 2024-05-16	📋 🛛 DoS & Spoofing 🗸 🗸	Source IP v Q 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	0
5	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:33	0
6	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:32	0
7	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:32	0
8	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:31	0
9	192.168.5.222	NET5	Port Scan	block	2024/05/16 14:31	0
				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	
Source IP: 192.168.80.235	
DNS Domain Name: example.org Filter Quantity: 2	
Description: DNS_Filtering	
Action: DIOCK	
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:

	А	В	С	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	PortScan	23	block
5	####	192.168.5.222	NET5	PortScan	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	PortScan	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	PortScan	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.

1 Note:

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

Security	Log		
Log	E-mail Notifications		
		Select the log to be notified by email. Click to visit <u>Email Settings</u>	
		* DoS Defense	
		DoS Defense Alert If enabled, an alert email will be send when the device detects DoS defense.	
		* Spoofing Defense	
		Spoofing Defense Alert If enabled, an alert email will be send when the device detects Spoofing defense.	
		* Anti-virus	
		Antivirus Alert Once enabled, the device will send alert email when it detects virus attacks.	
		* Intrusion Prevention	

* Botnet C&C			
	Cancel	Save	

E-mail Notifications

