Grandstream Networks, Inc.

GCC6000 Series -

Security Defense Guide

GCC6000 Series - Security Defense Guide

Introduction

Security Defense is a mechanism implemented in the GCC convergence device, to protect the network from common cyber attacks, such as DoS attacks, Man-in-the-middle attack, ARP Spoofing…

Each tool will have a set of parameters and configuration items to either block, isolate or delete the source endpoint from where the attack is detected.

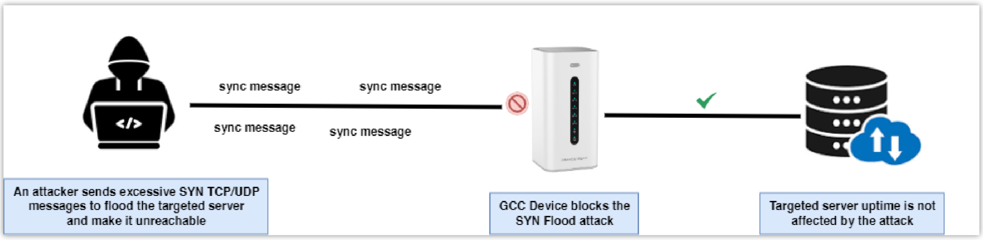
In this guide, we will go through some of the defense methods used by the GCC device to protect the network from potential down time or security vulnerabilities.

The guide will cover the following configurations:

- **DoS Defense**
- **ARP Protection**

DoS Defense

The Flood attack defense, as the name implies, is used to block connected endpoints from flooding the network with SYNC requests, this is achieved by performing a SYNC FLOOD defense on network service ports (port 443, port 80…), and if it notices that too many requests are being sent to a targeted device, it will block sync messages, or inform the network administrator, depending on the way it is configured.


sync message
sync message
sync message
sync message
An attacker sends excessive SYN TCP/UDP messages to flood the targeted server and make it unreachable
GCC Device blocks the SYN Flood attack
Targeted server uptime is not affected by the attack

DoS Attack Diagram

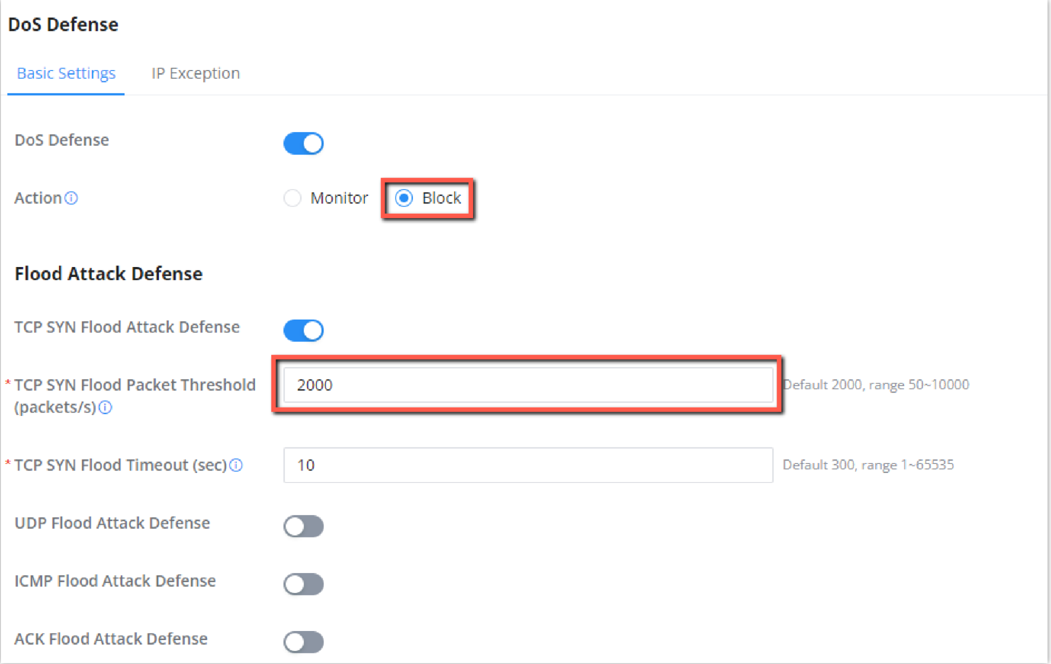
Some initial attack indications are: port scanning, where the GCC would signal an attempted scan for all internal service ports, and sees if any specific port is currently used, such as port 21 for FTP, port 22 for SSH access…, these kind of information can cause a vulnerability in the network if obtained by the wrong person, and can help him in some cases flood the network and launch a Denial-of-Service attack, to minimize the risks, we can enable the port scan detection feature to let us know, when a user is attempting a port scan.

Preventing the DoS attack

To prevent a flooding attack, we can follow the below steps on the GCC device:

1. Under **"Firewall Module → Security Defense → DoS Defense",** Enable the DoS Defense option.
2. Set the action to "**Block**", this will notify the user of an attempted SYN FLOOD, and at the same time, block the user from sending SYN FLOOD attacks, setting the action to "Monitor" will only inform the user that an attack is attempted, the information can be viewed on the security logs of the GCC device.
3. Set the **TCP SYN Flood Packet Threshold (packets/s)** to 2000 packets per second, if the amount exceeds that, the system will consider it as a SYN Flood.

> In the same manner, you have the possibility to enable Flood attack defense for other protocols such as UDP, ICMP, or for the TCP Acknowlegments.



DoS Defense

Basic Settings | IP Exception

DoS Defense: ON

Action ⓘ: ○ Monitor ● Block

Flood Attack Defense

TCP SYN Flood Attack Defense: ON

* TCP SYN Flood Packet Threshold (packets/s) ⓘ: 2000 — Default 2000, range 50~10000

* TCP SYN Flood Timeout (sec) ⓘ: 10 — Default 300, range 1~65535

UDP Flood Attack Defense: OFF

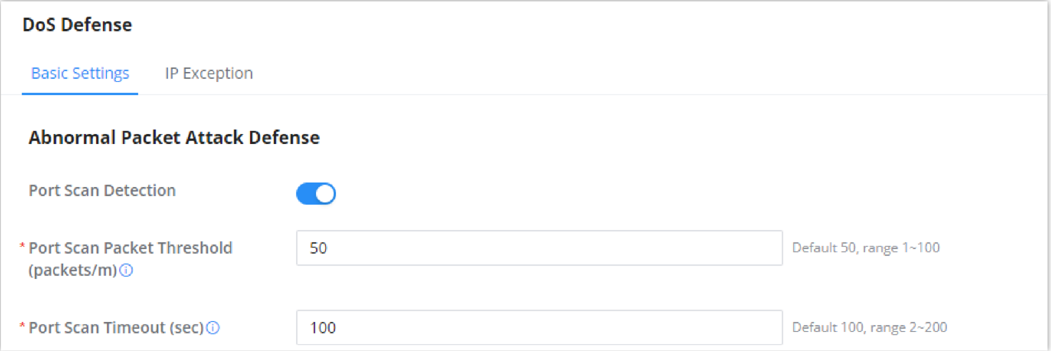
ICMP Flood Attack Defense: OFF

ACK Flood Attack Defense: OFF

Preventing Flood Attack

4. Additionally, we will enable the Port Scan detection option, the GCC device will notify us when a connected host is trying to launch a SYN flood attack, which can help us take preventive measures.

5. Define the **Port Scan Packet Threshold (packets/s)** to be 50 packets per second, If the port packets reach the threshold, port scanning detection will start immediately.



DoS Defense

Basic Settings | IP Exception

Abnormal Packet Attack Defense

Port Scan Detection: ON

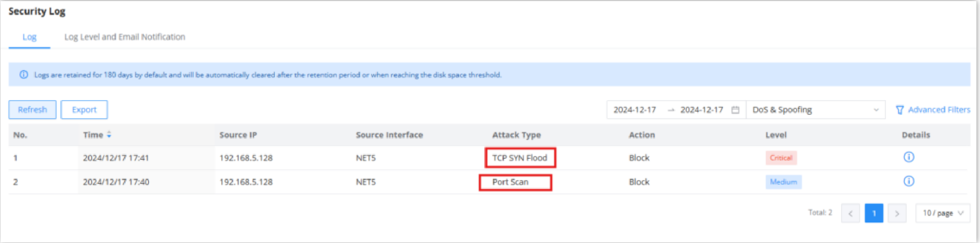
* Port Scan Packet Threshold (packets/m) ⓘ: 50 — Default 50, range 1~100

* Port Scan Timeout (sec) ⓘ: 100 — Default 100, range 2~200

Port Scan detection

After applying the above configuration, after a user attempts to flood the network, it will be blocked, and the GCC device will not experience any downtime.

You can view security logs displaying information about the exact time of the attack and the type of action, monitored only, or blocked



Security Log

Log | Log Level and Email Notification

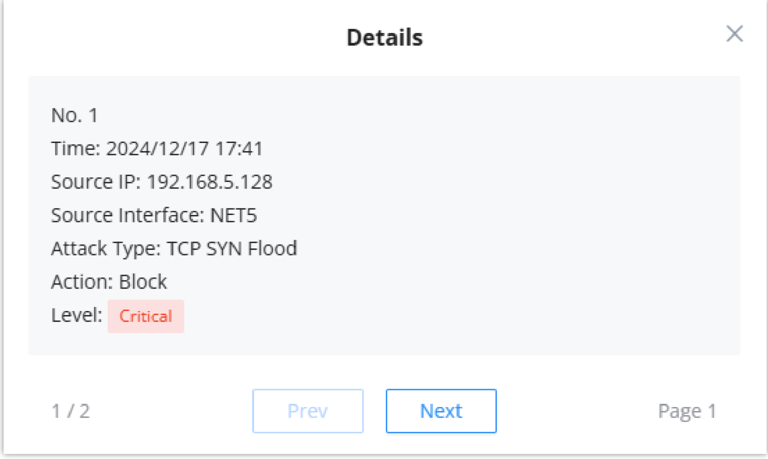
ⓘ Logs are retained for 180 days by default and will be automatically cleared after the retention period or when reaching the disk space threshold.

Refresh | Export | 2024-12-17 → 2024-12-17 | DoS & Spoofing | Advanced Filters

No.	Time	Source IP	Source Interface	Attack Type	Action	Level	Details
1	2024/12/17 17:41	192.168.5.128	NET5	TCP SYN Flood	Block	Critical	ⓘ
2	2024/12/17 17:40	192.168.5.128	NET5	Port Scan	Block	Medium	ⓘ

Total: 2 | ‹ 1 › | 10 / page

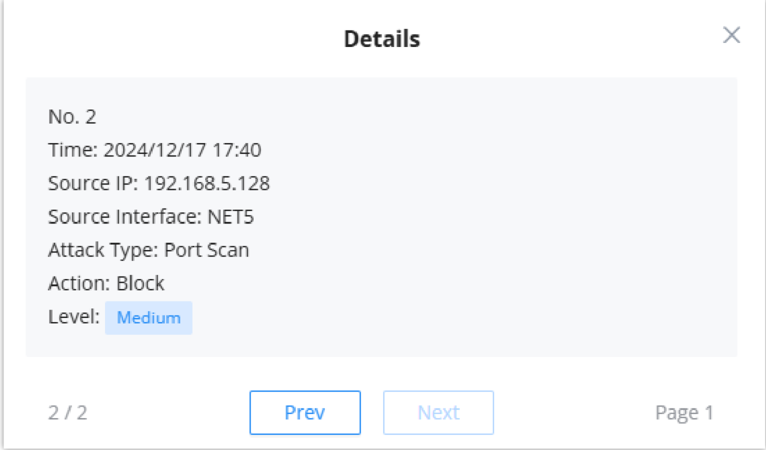
Security Log



Details

No. 1
Time: 2024/12/17 17:41
Source IP: 192.168.5.128
Source Interface: NET5
Attack Type: TCP SYN Flood
Action: Block
Level: Critical

Details about the TCP SYN FLOOD log



Details

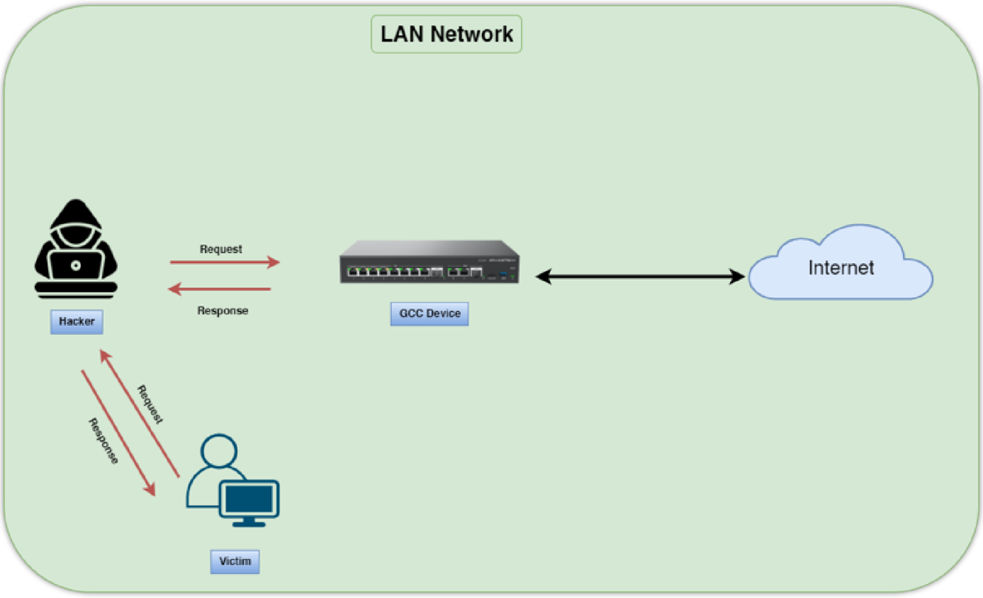
No. 2
Time: 2024/12/17 17:40
Source IP: 192.168.5.128
Source Interface: NET5
Attack Type: Port Scan
Action: Block
Level: Medium

Details about the Port Scan log

ARP Protection

Spoofing Defense is a security mechanism used to prevent connected users, to alter and modify their network information, in our case, we will focus on taking preventive measures against MAC spoofing attacks.

A MAC spoofing attack involves changing the MAC address of a network interface on a device to impersonate another device on the network. This can be used to bypass network access controls, such as the 802.1X authentication, disguise the attacker's device, or intercept network traffic intended for another device.



ARP Spoofing Attack

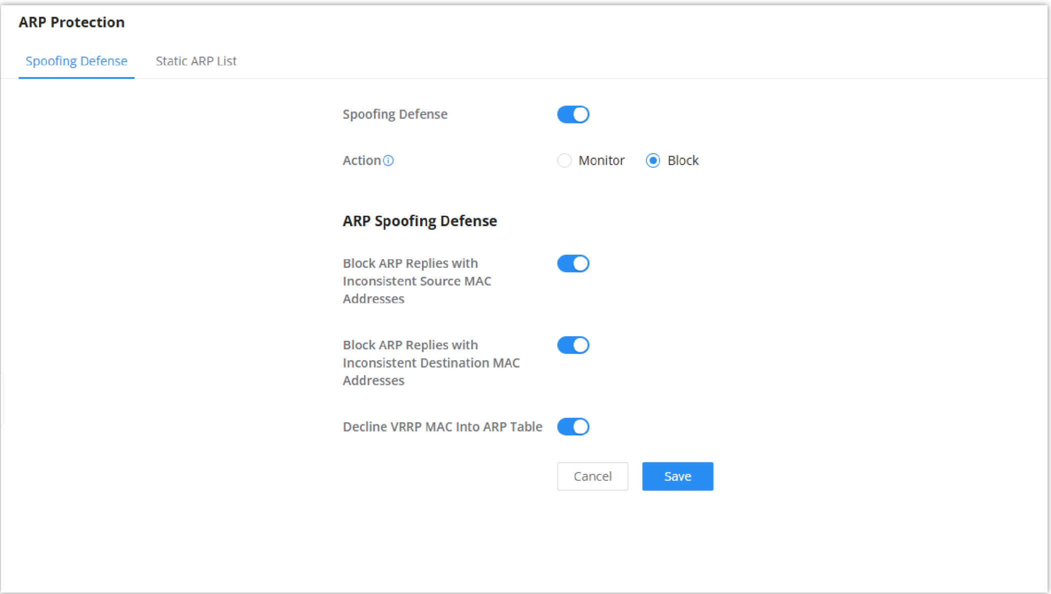
Preventing the ARP Spoofing

The GCC device allows its users to prevent such ARP spoofing attacks, by implementing specific rules to block the device from reconnecting and obtaining the modified MAC address, this can be done by following the below steps:

1. Under **"Firewall Module → Security Defense →ARP Protection",** Enable the Spoofing Defense option.
2. Set the action to "**Block**", this will block the device from sniffing the traffic between the victim device and the router, it will also notify the user that an ARP spoofing attempt happened, this can be viewed in the security log.
3. Enable the ARP Spoofing Defense, by enabling the following options, "**Block ARP Replies with Inconsistent Source MAC Addresses**" , and "**Block ARP Replies with Inconsistent Destination MAC Addresses**"

4. Additionally you can enable "**Decline VRRP MAC Into ARP Table**" to decline including any generated virtual MAC address in the ARP table.

> **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**: Virtual Router Redundancy Protocol (VRRP) allows multiple routers to manage a single virtual IP address for high availability. This defense ensures that VRRP MAC addresses are not accepted into the ARP table, which can prevent certain types of attacks that involve VRRP.



ARP Protection

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 ●

Preventing ARP Spoofing

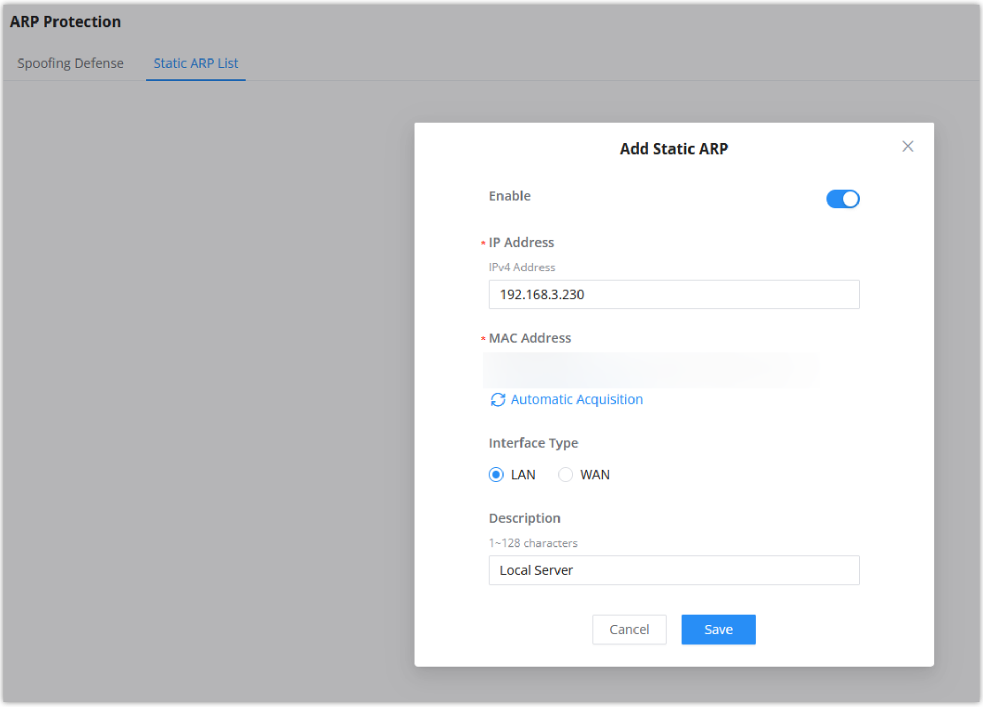
Static ARP List

In addition to the above mentioned tools and options used, another useful approach would be to map MAC to IP address, this is done by stating to the GCC firewall, a list of IP addresses in your local network, and their corresponding allowed MAC addresses, this means that if an attacker, within your LAN tries to impersonate one of the IP addresses added but with a different MAC address, it will be detected as a spoofing attempt and will be blocked, This is achieved through the feature called **Static ARP List**.

We will take the below example for better understanding:

For a connected internal server with the local static IP address 192.168.3.230, we will do the following:

1. Go to **Firewall Module** → **Security Defense** →**ARP Protection** →**Static ARP List**, before that make sure Spoofing defense is enabled under **Firewall Module** → **Security Defense** →**ARP Protection** →**Spoofing Defense**
2. Click Add to Add a new Mapping rule.
3. Define the local IP address of the endpoint, in our case it is "192.168.3.230".
4. You have the option to either manually enter the MAC address of the connected unit, or click on "Automatic Acquisition" to be able to retrieve the MAC address of the device automatically from the list of connected devices. this will map the MAC address with the local IP address
5. Defining the Interface type depends on your set up scenario, in our case we will select **LAN**:
   - **LAN:** Selecting the LAN interface is used when you want to protect your internal devices against internal spoofing attempts, by mapping each device in the LAN to its corresponding IP address, it is important to note that the IP address must be set statically to avoid having to update the mapping rule each time with the new IP address.
   - **WAN:** The WAN interface will be selected when we want to protect our Internal network by defining to the Firewall the public IP address of the ISP gateway provided , and its corresponding MAC address, which is the MAC address of the gateway device used, this is useful if you have a server hosted on your network and that is exposed to the internet, and you want to ensure that only traffic coming from the gateway is allowed to communicate with it.
6. Define a description that matches the device.



ARP Protection

Spoofing Defense | Static ARP List

Add Static ARP

Enable: ●

* IP Address
IPv4 Address
192.168.3.230

* MAC Address

Automatic Acquisition

Interface Type
● LAN ○ WAN

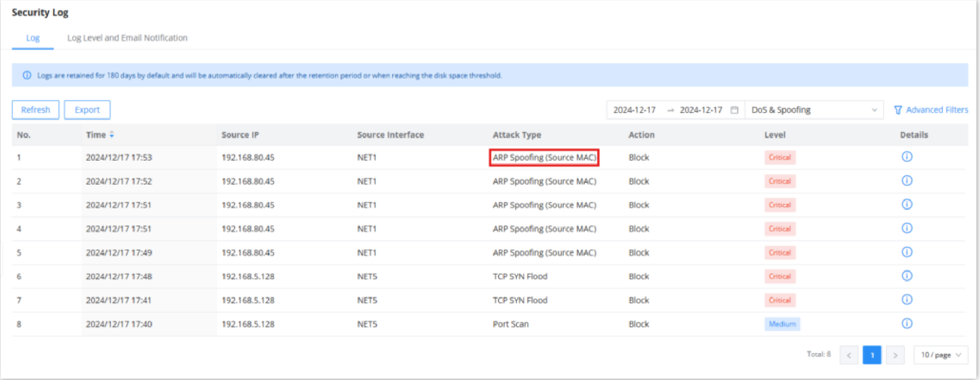
Description
1~128 characters
Local Server

Static ARP List

Results

With the ARP spoofing defense mechanism applied, the GCC device can help you prevent many security threats, such as Man-in the middle attack, and altering MAC address to bypass the NAC authentication.

The security logs will display the information about the blocked ARP spoofing attempt, make sure to set the type of attack to DoS & Spoofing to view the logs, as shown below:



Security Log

Log | Log Level and Email Notification

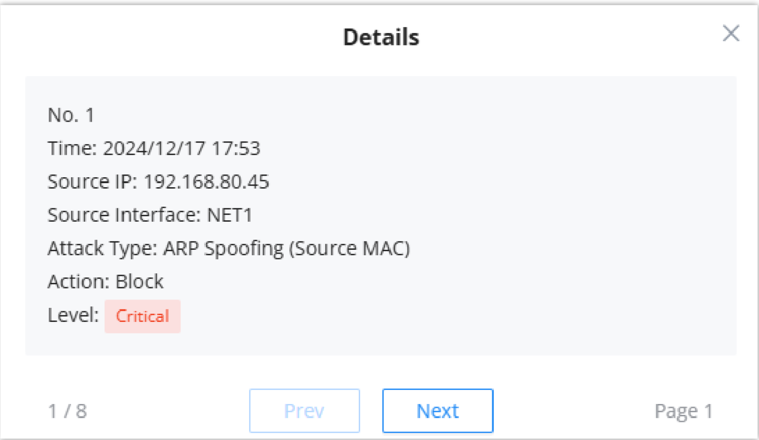
Logs are retained for 180 days by default and will be automatically cleared after the retention period or when reaching the disk space threshold.

2024-12-17 → 2024-12-17 | DoS & Spoofing

No.	Time	Source IP	Source Interface	Attack Type	Action	Level	Details
1	2024/12/17 17:53	192.168.80.45	NET1	ARP Spoofing (Source MAC)	Block	Critical	ⓘ
2	2024/12/17 17:52	192.168.80.45	NET1	ARP Spoofing (Source MAC)	Block	Critical	ⓘ
3	2024/12/17 17:51	192.168.80.45	NET1	ARP Spoofing (Source MAC)	Block	Critical	ⓘ
4	2024/12/17 17:51	192.168.80.45	NET1	ARP Spoofing (Source MAC)	Block	Critical	ⓘ
5	2024/12/17 17:49	192.168.80.45	NET1	ARP Spoofing (Source MAC)	Block	Critical	ⓘ
6	2024/12/17 17:48	192.168.5.128	NET5	TCP SYN Flood	Block	Critical	ⓘ
7	2024/12/17 17:41	192.168.5.128	NET5	TCP SYN Flood	Block	Critical	ⓘ
8	2024/12/17 17:40	192.168.5.128	NET5	Port Scan	Block	Medium	ⓘ

Total: 8 < 1 > 10 / page

ARP Spoofing Security Log



No. 1
Time: 2024/12/17 17:53
Source IP: 192.168.80.45
Source Interface: NET1
Attack Type: ARP Spoofing (Source MAC)
Action: Block
Level: Critical

Detailed Spoofing Log

Supported Devices

Device Model	Firmware Required
GCC6010W	1.0.1.7+
GCC6010	1.0.1.7+
GCC6011	1.0.1.7+

Need Support?

Can’t find the answer you’re looking for? Don’t worry we’re here to help!

CONTACT SUPPORT