

Grandstream Networks, Inc.

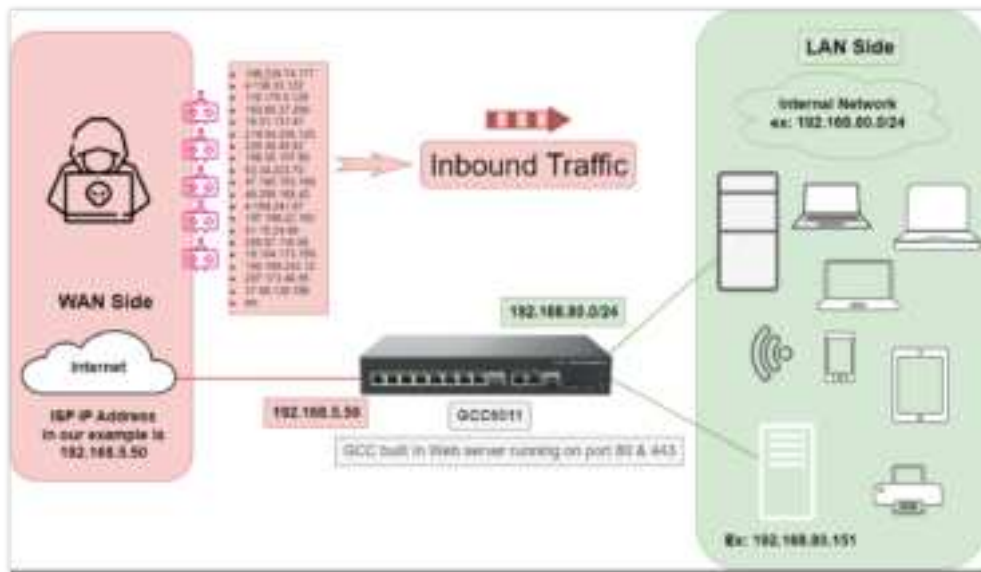
GCC6000 Series - **Botnet Guide**

GCC6000 Series - Botnet Guide

Introduction

The GCC convergence device includes a protection feature against botnet attacks, the way the attack works is when an attacker, either from outside the network (WAN side) or inside the network (LAN side), coordinates multiple hosts infected with malware (bots), to perform a specific action while managed by a command-and-control (C&C) server.

The attacker can do that by either infecting many computers with malware, and controlling them using a C&C server to flood the target and make it unresponsive, or by performing the action from one powerful computer that sends web requests to the target from randomized different source IP addresses, both methods will have the same effect on the target: harm the availability of the service.



Botnet Attack

Botnet Defense Action

To prevent a Botnet Attack, Follow the below steps:

1. Navigate to **Firewall Module** → **Intrusion Prevention** → Botnet
2. Set Botnet IP to Block
3. Additionally, you can set Botnet Domain name to Block, this will block external users from launching a Botnet attack on a locally hosted server accessible publicly with a domain name.

Botnet Configuration Confirmed

Once the prevention is enabled, if an external user attempts to flood your network by targeting the public IP of the gateway, it will be blocked and will be recorded in the security logs as shown below:



The screenshot shows the 'Security Log' interface with a table of log entries. The first entry is highlighted, showing details of a blocked attack.

No.	Time	Source IP	Destination IP address / Domain name	Protocol	Description	Action	Level	Report
1	2024/12/17 17:29	47.237.79.198	192.168.6.32	tcp	Inbound	Block	Critical	

Blocked Attack



The 'Details' window shows the following information for the selected log entry:

- No. 1
- Time: 2024/12/17 17:29
- Source IP: 47.237.79.198
- Destination IP address / domain name: 192.168.6.32
- Protocol: tcp
- Description: inbound
- Action: Block
- Level: Critical

Navigation buttons: Prev, Next, Page 1

Details on Security Logs

In some cases, you will have a specific IP address or domain name, making several requests from outside the LAN to your internal network, and that you want to allow, for example, a remote worker who has the job of retrieving multiple information for an internal secured database, what you can do, is to add the public IP address of the remote worker that is connected through a VPN tunnel, to the list of IP/Domain name exception list.



The form is titled 'Botnet - Add IP / Domain Name Exception'. It contains the following fields and controls:

- Name: Allow_RemoteUser (1-64 characters)
- Enable: ☒
- IP Address / Domain Name: IP Address (dropdown) with value 192.21.25.66 (Add button)
- Buttons: Cancel, Save

It is advised to regularly update the protection database under **Intrusion Prevention** → **Signature Library** to ensure that all attack vectors and attack types are up to date. You can also create a schedule for the update.



The 'Signature Library' interface shows a table of signatures and a 'Signature Library Information' section.

Signature	Version
Example 1	1.0
Example 2	1.0
Example 3	1.0
Example 4	1.0

Signature Library Information:

- Version: 1.0
- Last Updated Time: 2024/12/17 17:29
- Update Time: 2024/12/17 17:29
- Update Size: 100MB

Signature Library

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](#)