



**GRANDSTREAM  
GCC6000 Series  
Botnet Guide**



# GRANDSTREAM GCC6000 Series Botnet Guide User Guide

[Home](#) » [GRANDSTREAM](#) » **GRANDSTREAM GCC6000 Series Botnet Guide User Guide** 



## Contents

- [1 GRANDSTREAM GCC6000 Series Botnet Guide](#)
- [2 Product Usage Instructions](#)
- [3 Introduction](#)
- [4 Botnet Defense Action](#)
- [5 Supported Devices](#)
- [6 Documents / Resources](#)
  - [6.1 References](#)
- [7 Related Posts](#)

## GRANDSTREAM GCC6000 Series Botnet Guide



## Specifications

- Manufacturer: Grandstream Networks, Inc.
- Product Series: GCC6000 Series – Botnet Guide
- Supported Devices:
  - Device Model GCC6010W
  - Device Model GCC6010
  - Device Model GCC6011
- Firmware Required: 1.0.1.7+ for all supported device models

## **Product Usage Instructions**

### **Botnet Attack Prevention**

1. Navigate to Firewall Module > Intrusion Prevention > Botnet.
2. Set Botnet IP to Block.
3. You can also set Botnet Domain name to Block to prevent external users from launching attacks on a publicly accessible server.

### **Allowing Specific IP/Domain**

If there are specific external users (e.g., remote workers) that you want to allow access, follow these steps:

1. Add the public IP address or domain name of the allowed users to the exception list.
2. This ensures that legitimate users are not blocked by the Botnet defense mechanism.

### **FAQ**

#### **Q: What firmware version is required for the supported device models?**

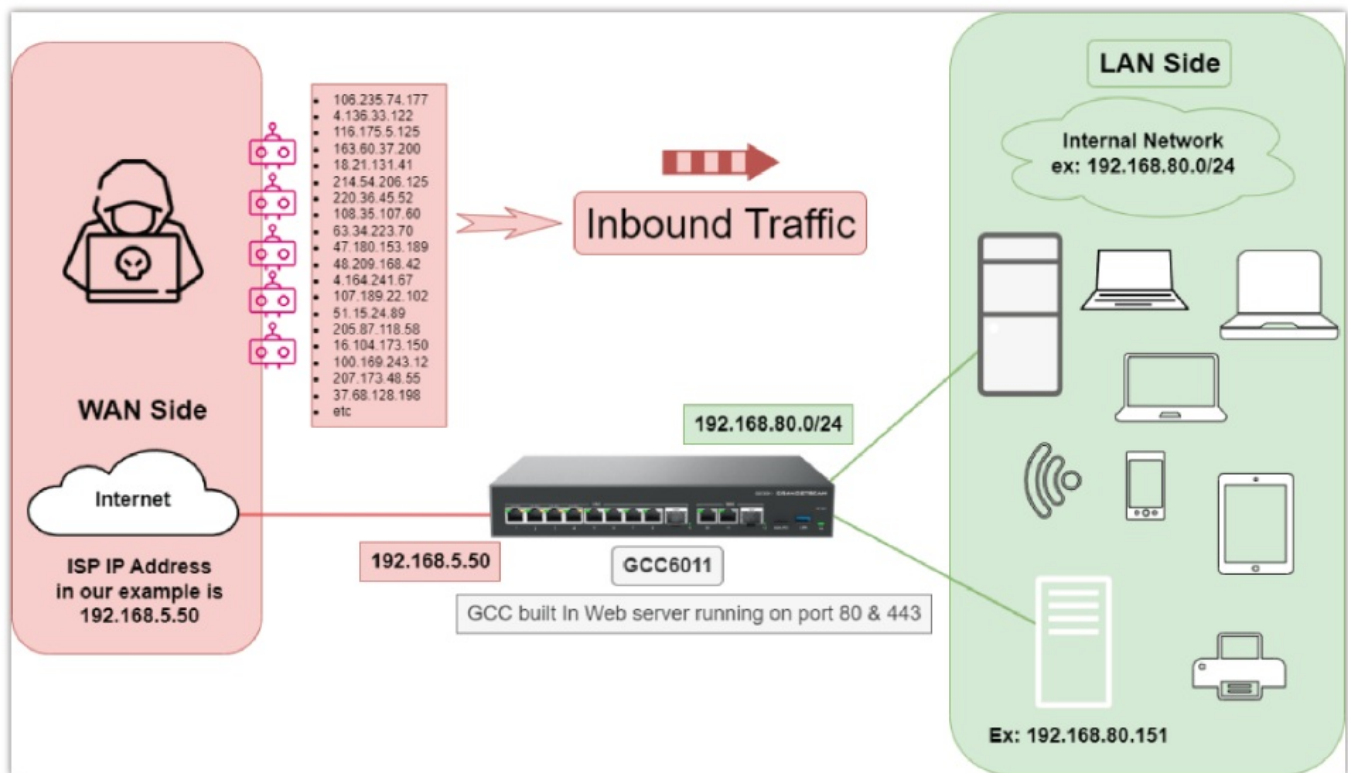
A: Firmware version 1.0.1.7 or higher is required for Device Models GCC6010W, GCC6010, and GCC6011.

## **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 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

Basic Settings

IP / Domain Name Exception

Botnet IP ⓘ

☐ Monitor ☒ Block ☐ No Action

Botnet Domain Name ⓘ

☐ Monitor ☒ Block ☐ No Action

Cancel

Save

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:

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 Botnet Advanced Filters

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

Total: 1

< 1 >

10 / page

Blocked Attack

Details

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

1 / 1

PrevNext

Page 1

Details on Security Logs

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.

Botnet > Add IP / Domain Name Exception

Name

Allow\_RemoteUser

1~64 characters

Enable

IP Address / Domain Name

IP Address

137.21.25.66

Add

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.

Signature Library

Update Interval

Auto (Updated Daily)

Auto (Updated Daily)

Create Schedule

Signature Library Information

Version

20241022.1416

Last Checked Time

2024/11/12 04:40:54 (UTC -06:00)

Update Time

2024/11/05 03:35:04 (UTC -06:00)

Expired Date

2025/03/25

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

Documents / Resources

    	<p><b><a href="#">GRANDSTREAM GCC6000 Series Botnet Guide</a></b> [pdf] User Guide GCC6010W, GCC6010, GCC6011, GCC6000 Series Botnet Guide, GCC6000 Series, Botnet Guide, Botnet</p>
--	--

References

- [documentation.grandstream.com/knowledge-base/gcc6000-series-botnet-guide/?hkb-redirect&nonce=04f52c5a7f&check=2nuf1&redirect=helpdesk.grandstream.com&otype=ht\\_kb\\_article&oid=04f52c5a7f](https://documentation.grandstream.com/knowledge-base/gcc6000-series-botnet-guide/?hkb-redirect&nonce=04f52c5a7f&check=2nuf1&redirect=helpdesk.grandstream.com&otype=ht_kb_article&oid=04f52c5a7f)
- [documentation.grandstream.com/wp-content/uploads/2024/11/allow-remote-User.png](https://documentation.grandstream.com/wp-content/uploads/2024/11/allow-remote-User.png)
- [documentation.grandstream.com/wp-content/uploads/2024/11/Botnet-Configuration-Confirmed.png](https://documentation.grandstream.com/wp-content/uploads/2024/11/Botnet-Configuration-Confirmed.png)
- [documentation.grandstream.com/wp-content/uploads/2024/11/Botnet.png](https://documentation.grandstream.com/wp-content/uploads/2024/11/Botnet.png)
- [documentation.grandstream.com/wp-content/uploads/2024/11/signature-library.png](https://documentation.grandstream.com/wp-content/uploads/2024/11/signature-library.png)
- [documentation.grandstream.com/wp-content/uploads/2024/12/Blocked-Attack.png](https://documentation.grandstream.com/wp-content/uploads/2024/12/Blocked-Attack.png)
- [documentation.grandstream.com/wp-content/uploads/2024/12/Details-on-Security-Logs.png](https://documentation.grandstream.com/wp-content/uploads/2024/12/Details-on-Security-Logs.png)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.