

Grandstream Networks, Inc.

GCC6000 Series -

Intrusion Detection and Prevention Guide

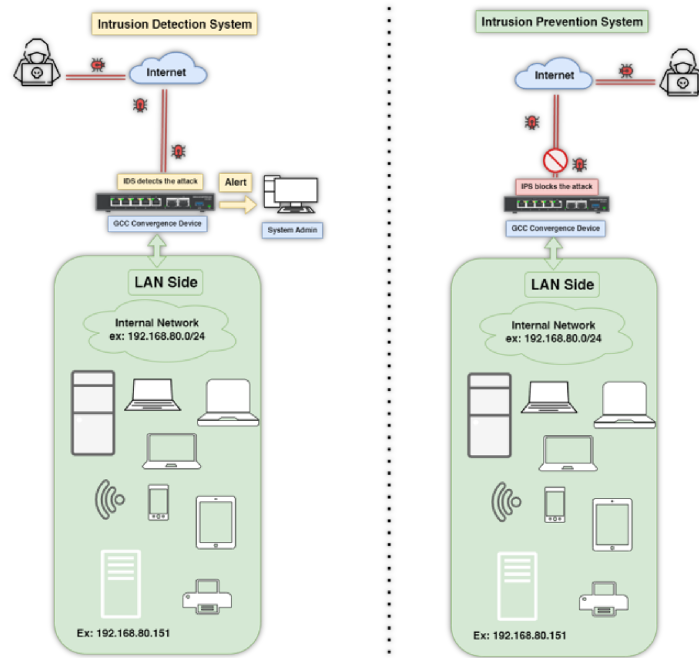


GCC6000 Series - Intrusion Detection and Prevention Guide

Introduction

The GCC convergence device comes equipped with two main important security features which are the IDS (Intrusion detection System) and IPS (Intrusion Prevention System), each serves a specific purpose to actively monitor and prevent malicious activities by identifying and blocking various types and levels of threat in real time.

- **Intrusion Detection Systems (IDS):** passively monitor traffic and alert administrators of potential threats without direct intervention.
- **Intrusion Prevention Systems (IPS):** intercept harmful activities immediately.




IDS vs IPS Diagram

In this guide, we will configure an intrusion detection and prevention protection against one common type of web attacks known as SQL injections.

Preventing attacks using IDS/IPS

SQL injection attack, is a type of attack designated to place malicious code in SQL statements, in the goal of retrieving unauthorized information from the web server's database, or break the database by entering a harmful command or input.

Please follow the below steps to prevent the injection attack:

- Navigate to **Firewall Module** → **Intrusion Prevention** → **Signature Library**.
- Click the icon  to make sure the **Signature Library Information** is up to date.

Signature Library

Update Interval ⓘ

Auto (Updated Daily) ▾

Cancel

Save

Signature Library Information ⓘ

Version	20240701.0947
Latest Checked Time	2024/07/16 16:17:48 (UTC +01:00)
Update Time	2024/07/08 16:35:30 (UTC +01:00)
Expired Date	2025/03/26

Update Library

Note

- The threat database is regularly and automatically updated by the GCC depending on the purchased plan.
 - The update interval can be scheduled to be triggered either weekly, or on an absolute date/time.
- Navigate to **Firewall Module** → **Intrusion Prevention** → **IDS/IPS**.
 - Set the mode to **Notify & Block**, this will monitor for any suspicious action and save it in the security log, it will also block the source of the attack.
 - Select the Security Protection Level, different protection levels are supported:
 1. **Low**: When the protection is set to “**Low**”, the following attacks will be monitored and/ or blocked: Injection, Brute Force, Path Traversal, DoS, Trojan, Webshell.
 2. **Medium**: When the protection is set to “**Medium**”, the following attacks will be monitored and/or blocked: Injection, Brute Force, Path Traversal, DoS, Trojan, Webshell, Vulnerability Exploit, File Upload, Hacking Tools, Phishing.
 3. **High**: When the protection is set to “**High**”, the following attacks will be monitored and/or blocked: Injection, Brute Force, Path Traversal, DoS, Trojan, Webshell, Vulnerability Exploit, File Upload, Hacking Tools, Phishing.
 4. **Extremely High**: All the attack vectors will be blocked.
 5. **Custom**: the custom protection level allows the user to select only specific types of attacks to be detected and blocked by the GCC device, please refer to [[Attack Types Definitions](#)] section for more information, we will set the security Protection Level to **Custom**.

IDS / IPS

Basic Settings

IP Exception

Mode ⓘ

☐ Notify
 ☒ Notify & Block
 ☐ No Action

Security Protection Level ⓘ

Custom ▾

Total (15/19)

Web Attacks

☒ Injection
 ☒ Brute Force
 ☒ Unserialization
 ☒ Information Disclosure
 ☒ Path Traversal

☒ Vulnerability Exploit
 ☒ File Upload

Network Anomalies

☒ Network Protocol
 ☒ DoS
 ☒ Phishing
 ☐ Tunnel
 ☐ IoT

Bad Files

☒ Trojan
 ☒ Coin Miner
 ☒ Worm
 ☐ Ransomware
 ☐ APT
 ☒ Webshell
 ☒ Hacking Tools

Cancel

Save

Configure Security Protection Level

Once the configuration is set, If an attacker attempts to launch an SQL injection, it will be monitored and blocked by the GCC device, and the corresponding action information will be displayed on the security logs as shown below:

Details

No. 37

Time: 2024/07/16 13:46

Threat Level: Medium

Source IP: 192.168.60.33

Destination IP: 192.168.5.53

Intrusion ID: 3223101805

Intrusion Description: GS SQL-Injection Error-based SQL Injection Att
empt in Uri Variant 1

Source Port: 51414

Destination Port: 8080

Action: monitor

Protocol: TCP

Other: GET /xampp/simple_login/login.php?query=test%27%29%20AND%20EXTRACTVALUE%281512%2C%28CONCAT%280x5c%2C0x716b717871%2C%28SELECT%20%28ELT%281512%3D1512%2C1%29%29%29%2C0x71786b6b71%29%29%20AND%20%28%27HCXY%27%3D%27HCXY HTTP/1.1

Cache-Control: no-cache

User-Agent: sqlmap/1.8.6.3#dev (https://sqlmap.org)

Host: 192.168.5.53:8080

Accept: */*

Accept-Encoding: gzip,deflate

Connection: close

37 / 100

PrevNext

Page 1

Monitor IDS

Attack Types Definitions

The IDS/IPS tool has the ability to protect against various attack vectors, we will briefly explain each one of them on the below table:

Attack Type	Description	Example
Injection	Injection attacks occur when untrusted data is sent to an interpreter as part of a command or query, tricking the interpreter into executing unintended commands or accessing unauthorized data.	SQL Injection in a login form can allow an attacker to bypass authentication.
Brute Force	Brute force attacks involve trying many passwords or passphrases with the hope of eventually guessing correctly by systematically checking all possible passwords.	Attempting multiple password combinations on a login page.
Unserialize	Unserialization attacks occur when untrusted data is deserialized, leading to arbitrary code execution or other exploitations.	An attacker providing malicious serialized objects.
Information	Information disclosure attacks aim to gather information about the target system to facilitate further attacks.	Exploiting a vulnerability to read sensitive configuration files.

Path Traversal	Path traversal attacks aim to access files and directories stored outside the web root folder by manipulating variables that reference files with "../" sequences.	Accessing /etc/passwd on a Unix system by traversing directories.
Exploitation of Vulnerabilities	Exploitation involves taking advantage of software vulnerabilities to cause unintended behavior or gain unauthorized access.	Exploiting a buffer overflow vulnerability to execute arbitrary code.
File Upload	File upload attacks involve uploading malicious files to a server to execute arbitrary code or commands.	Uploading a web shell script to gain control over the server.
Network Protocol	Monitoring and detecting anomalies in network protocols to identify potentially malicious traffic.	Unusual use of protocols such as ICMP, ARP, etc.
DoS (Denial of Service)	DoS attacks aim to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of internet traffic.	Sending a high volume of requests to a web server to exhaust its resources.
Phishing	Phishing involves tricking individuals into divulging confidential information through deceptive emails or websites.	A fake email that appears to be from a trusted source, prompting users to enter their credentials.
Tunnel	Tunneling attacks involve encapsulating one type of network traffic within another to bypass security controls or firewalls.	Using HTTP tunneling to send non-HTTP traffic through an HTTP connection.
IoT (Internet of Things)	Monitoring and detecting anomalies in IoT devices to prevent potential attacks targeting these devices.	Unusual communication patterns from IoT devices indicating a possible compromise.
Trojan	Trojan horses are malicious programs that mislead users of their true intent, often providing a backdoor to the attacker.	A seemingly harmless program that gives an attacker access to the system when executed.
CoinMiner	CoinMiners are malicious software designed to mine cryptocurrency using the infected machine's resources.	A hidden mining script that utilizes CPU/GPU power to mine cryptocurrency.
Worm	Worms are self-replicating malware that spread across networks without the need for human intervention.	A worm that spreads through network shares to infect multiple machines.
Ransomware	Ransomware encrypts a victim's files and demands a ransom payment to restore access to the data.	A program that encrypts files and displays a ransom note demanding payment in cryptocurrency.
APT (Advanced Persistent Threat)	APTs are prolonged and targeted cyberattacks where an intruder gains access to a network and remains undetected for an extended period.	A sophisticated attack targeting sensitive data of a specific organization.
Webshell	Web shells are scripts that provide a web-based interface for attackers to execute commands on a compromised web server.	A PHP script uploaded to a web server that allows the attacker to run shell commands.
Hacking Tools	Hacking tools are software designed to facilitate unauthorized access to systems.	Tools like Metasploit or Mimikatz used for penetration testing or malicious hacking.

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](#)