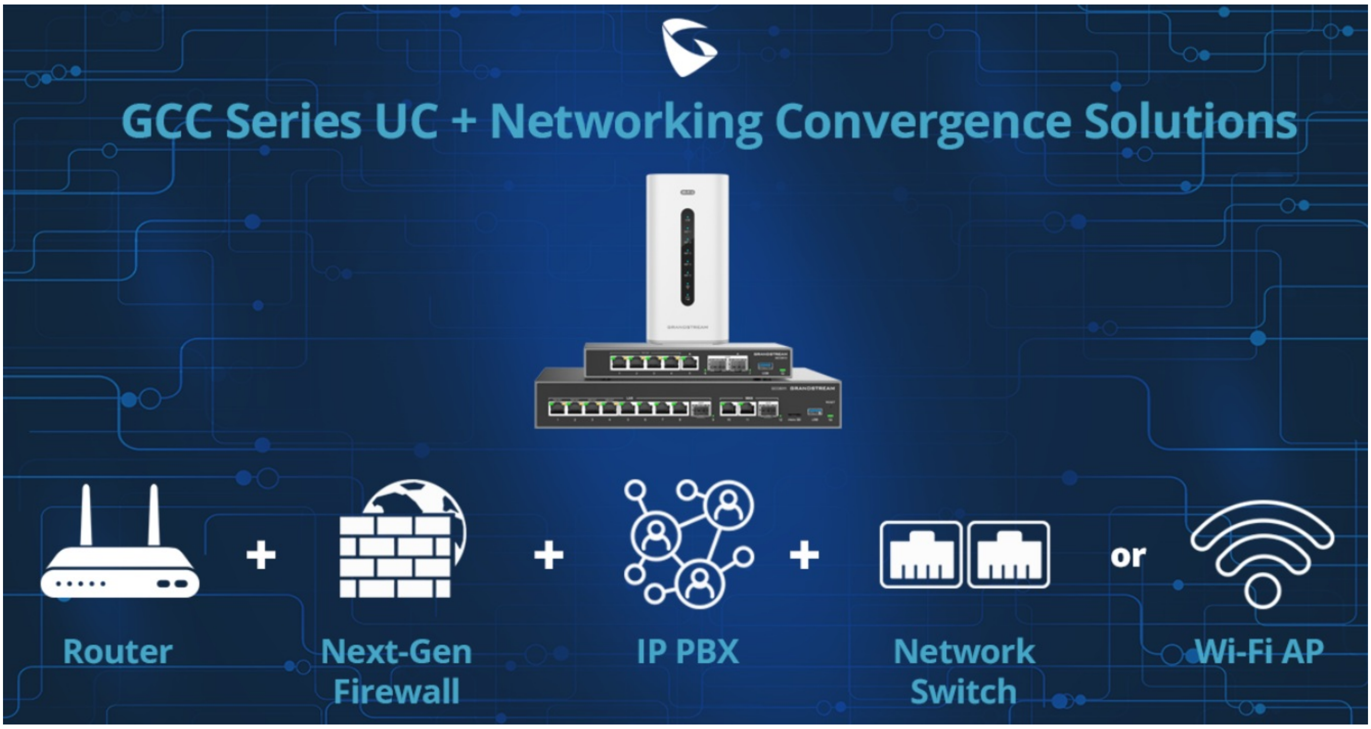
GRANDSTREAM
GRANDSTREAM GCC6000 Series
Intrusion Detection UC Plus
Networking Convergence Solutions
GCC Series UC + Networking Convergence Solutions
Router
Next-Gen Firewall
IP PBX
Network Switch
or
Wi-Fi AP
MANUALS.PLUS

GRANDSTREAM GCC6000 Series Intrusion Detection UC Plus Networking Convergence Solutions User Guide

Home » GRANDSTREAM » GRANDSTREAM GCC6000 Series Intrusion Detection UC Plus Networking Convergence Solutions User Guide

Contents

GRANDSTREAM GCC6000 Series Intrusion Detection UC Plus Networking Convergence Solutions



Product Specifications

- Brand: Grandstream Networks, Inc.
- Product Series: GCC6000 Series
- Features: IDS (Intrusion Detection System) and IPS (Intrusion Prevention System)

Product Usage Instructions

Introduction to IDS and IPS
The GCC convergence device is equipped with IDS and IPS for security purposes. IDS passively monitors traffic and alerts administrators of potential threats, while IPS intercepts harmful activities immediately.

Preventing SQL Injection Attacks
SQL injection attacks aim to insert malicious code into SQL statements to retrieve unauthorized information or harm the database. Follow these steps to prevent such attacks:

1. Navigate to Firewall Module > Intrusion Prevention > Signature Library.
2. Click on the update icon to ensure the Signature Library Information is up to date.
3. Set the mode to Notify & Block in Firewall Module > Intrusion Prevention > IDS/IPS.
4. Select a Security Protection Level (Low, Medium, High, Extremely High, or Custom) based on your needs.
5. Configure the Security Protection Level according to your preferences.

IDS/IPS Security Logs
After configuring the settings, any attempted SQL injection attack will be monitored and blocked by the GCC device. The corresponding information will be displayed in the security logs.

Frequently Asked Questions (FAQ)

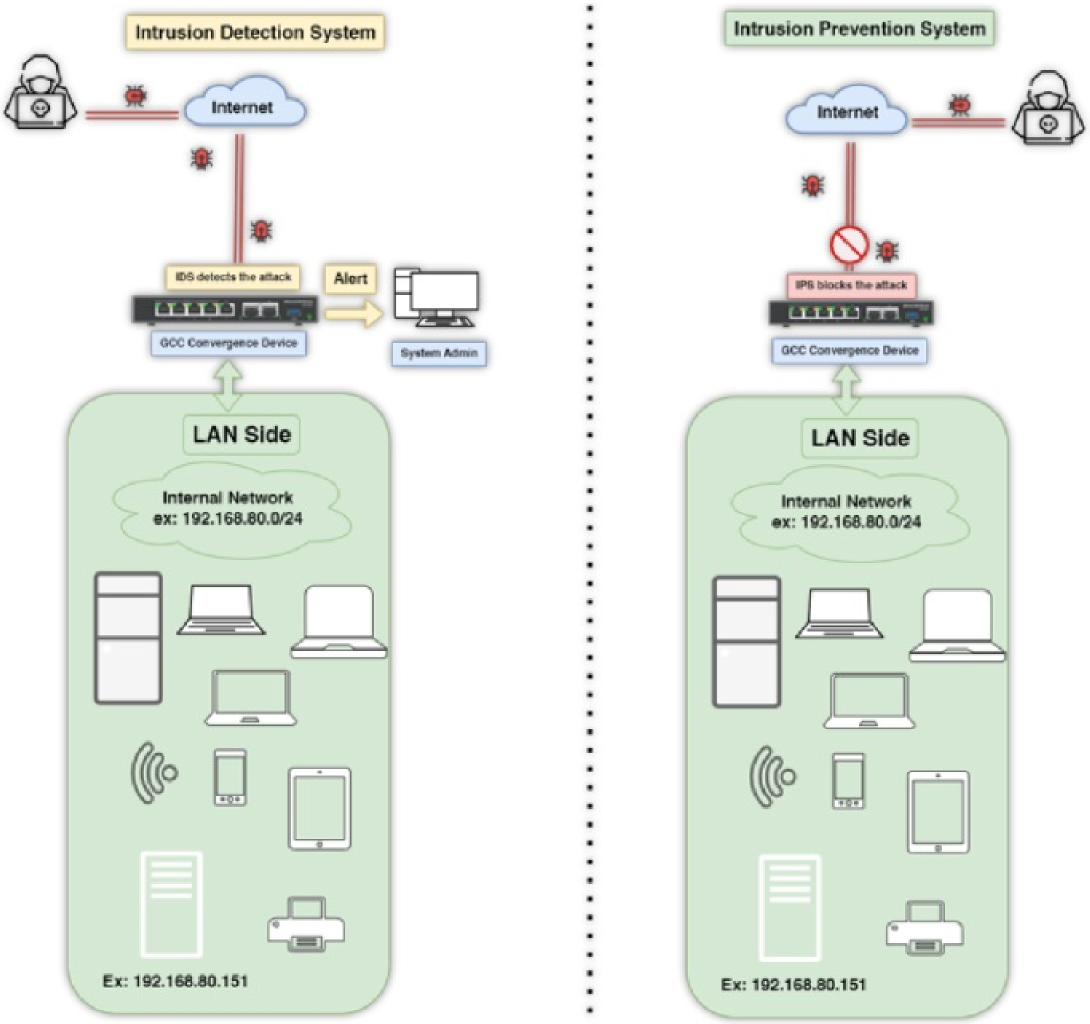
Q: How often is the threat database updated?
A: The threat database is regularly and automatically updated by the GCC depending on the purchased plan. Updates can be scheduled weekly or at a specific date/time.

Q: What types of attacks are monitored in each Security Protection Level?
A: Different protection levels (Low, Medium, High, Extremely High, Custom) monitor and block various attacks such as Injection, Brute Force, Path Traversal, DoS, Trojan, Webshell, Vulnerability Exploit, File Upload, Hacking Tools, and Phishing.

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.

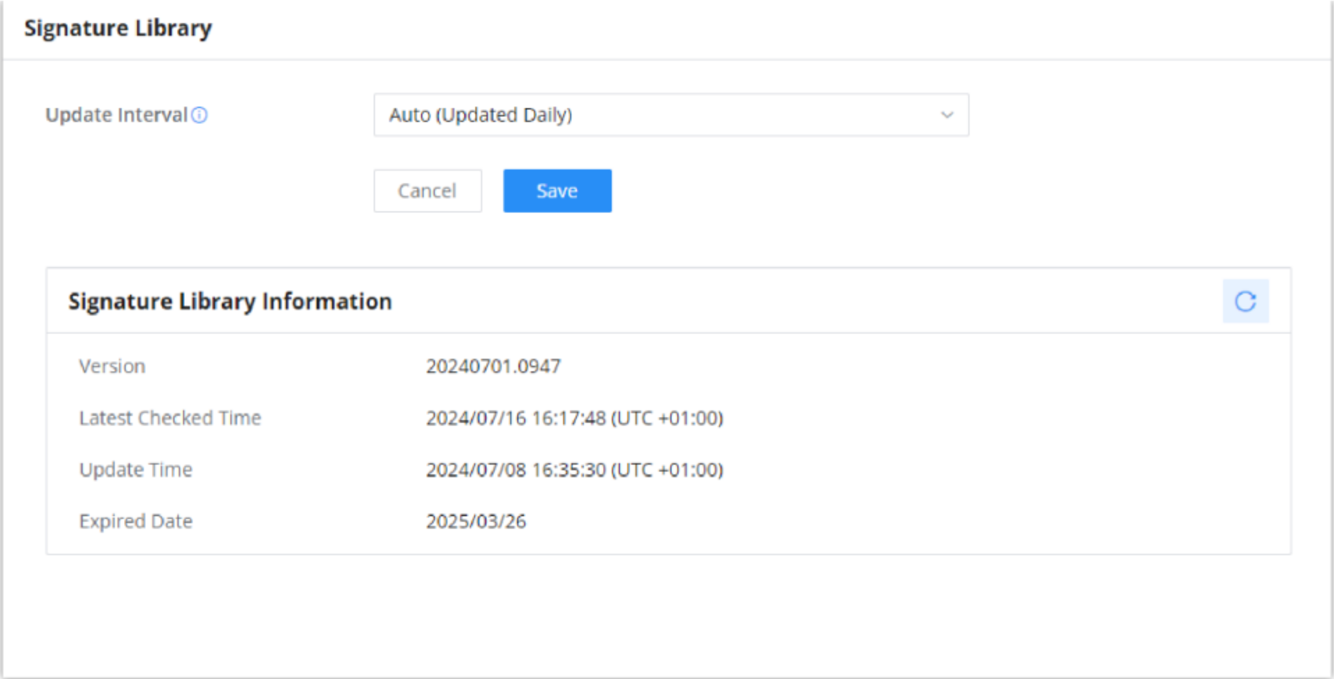


IDS vs IPS Diagram

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)

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

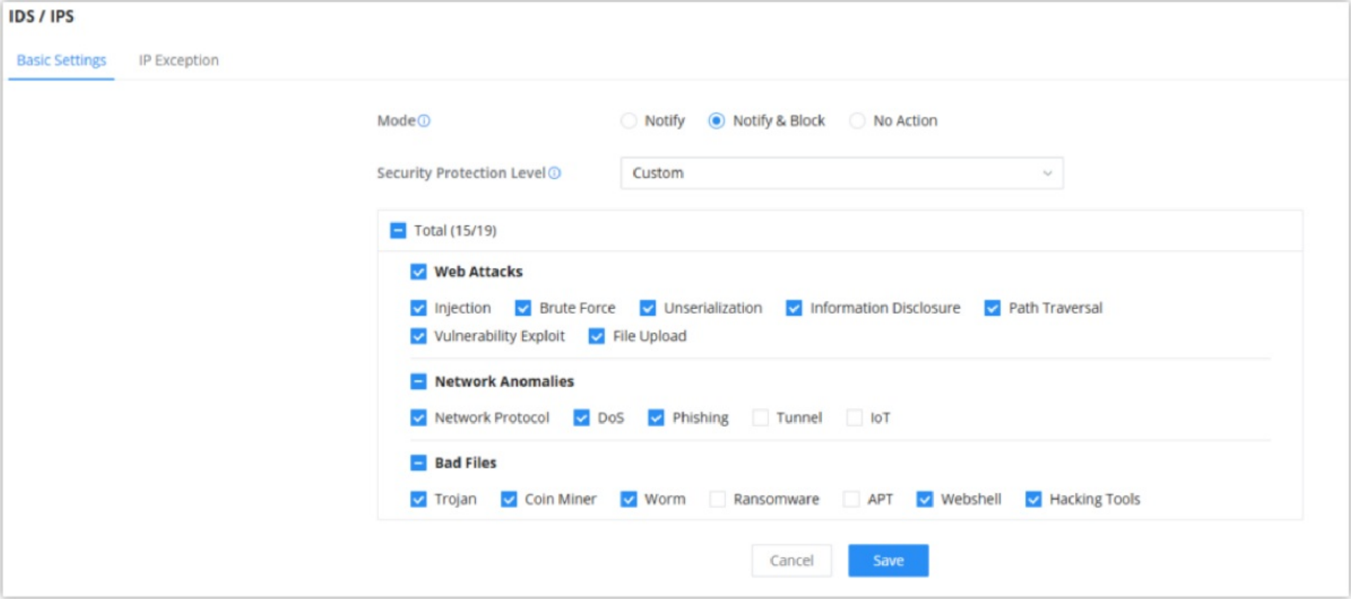
Note

- 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

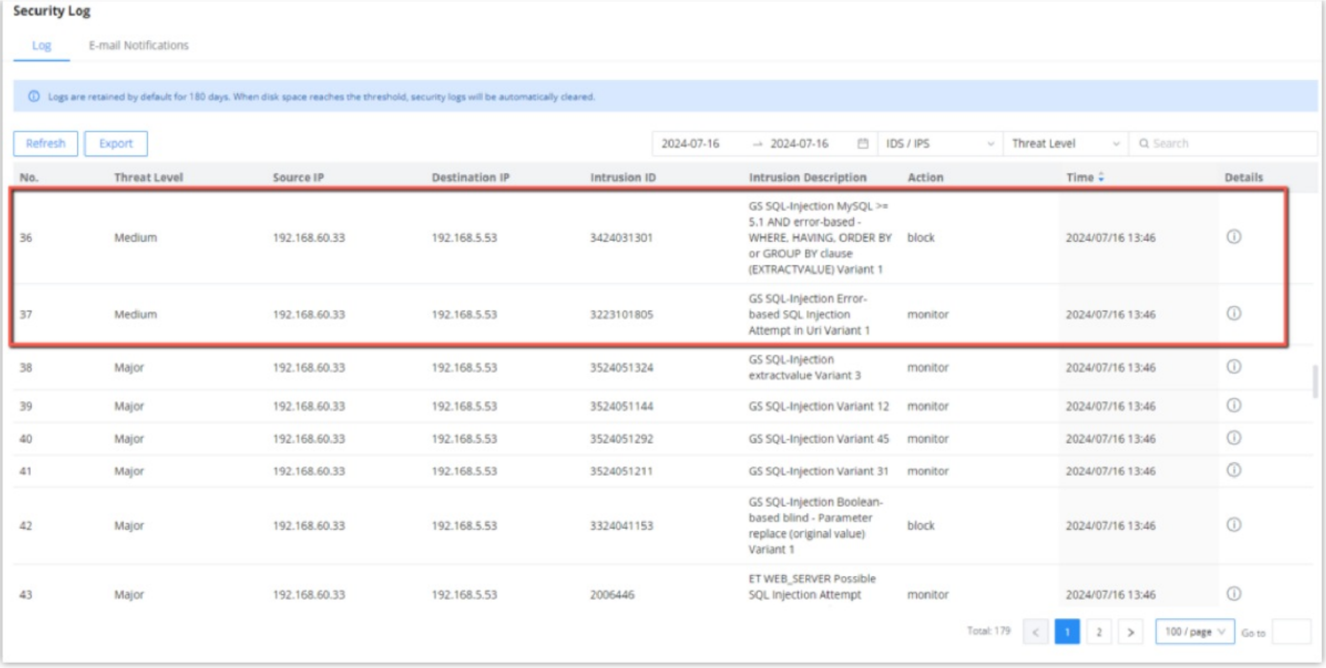
Mode: ○ Notify ● Notify & Block ○ No Action

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

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:



Security Log

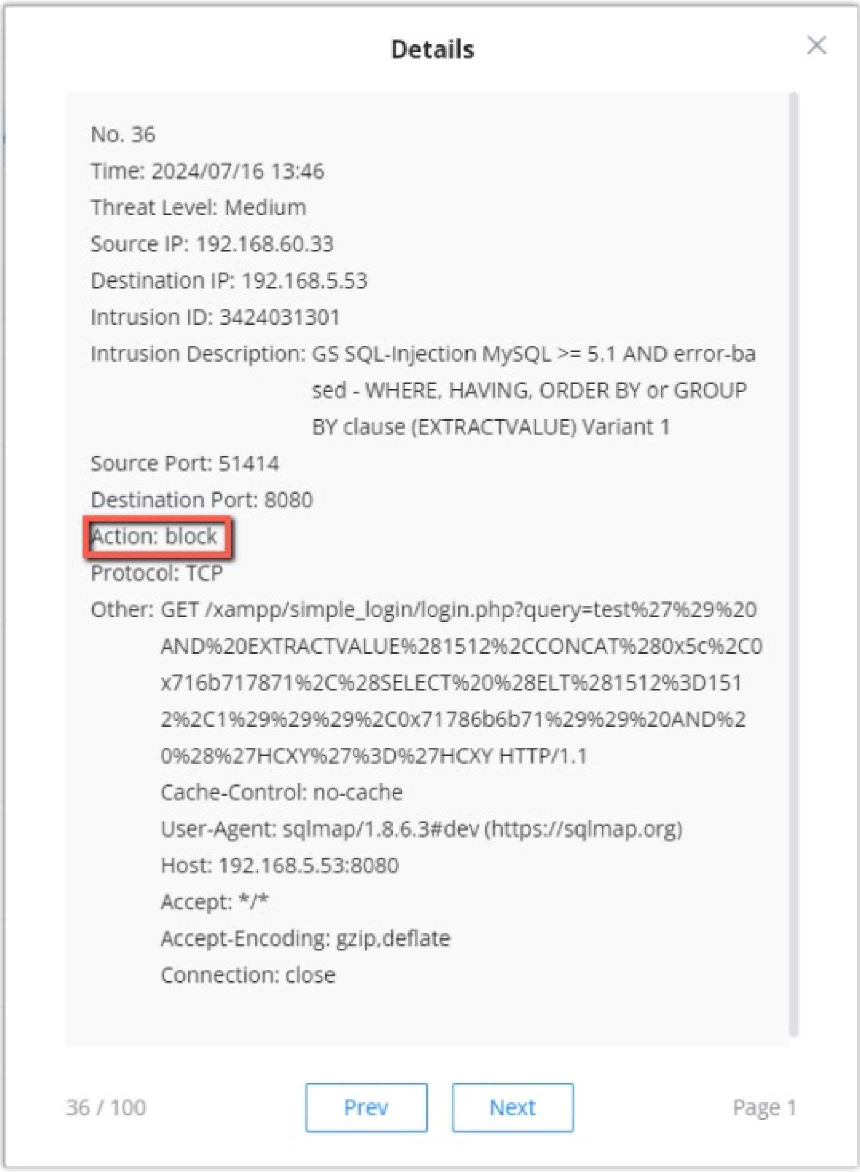
Log | E-mail Notifications

ⓘ Logs are retained by default for 180 days. When disk space reaches the threshold, security logs will be automatically cleared.

No.	Threat Level	Source IP	Destination IP	Intrusion ID	Intrusion Description	Action	Time	Details
36	Medium	192.168.60.33	192.168.5.53	3424031301	GS SQL-Injection MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE) Variant 1	block	2024/07/16 13:46	ⓘ
37	Medium	192.168.60.33	192.168.5.53	3223101805	GS SQL-Injection Error-based SQL Injection Attempt in Uri Variant 1	monitor	2024/07/16 13:46	ⓘ
38	Major	192.168.60.33	192.168.5.53	3524051324	GS SQL-Injection extractvalue Variant 3	monitor	2024/07/16 13:46	ⓘ
39	Major	192.168.60.33	192.168.5.53	3524051144	GS SQL-Injection Variant 12	monitor	2024/07/16 13:46	ⓘ
40	Major	192.168.60.33	192.168.5.53	3524051292	GS SQL-Injection Variant 45	monitor	2024/07/16 13:46	ⓘ
41	Major	192.168.60.33	192.168.5.53	3524051211	GS SQL-Injection Variant 31	monitor	2024/07/16 13:46	ⓘ
42	Major	192.168.60.33	192.168.5.53	3324041153	GS SQL-Injection Boolean-based blind - Parameter replace (original value) Variant 1	block	2024/07/16 13:46	ⓘ
43	Major	192.168.60.33	192.168.5.53	2006446	ET WEB_SERVER Possible SQL Injection Attempt	monitor	2024/07/16 13:46	ⓘ

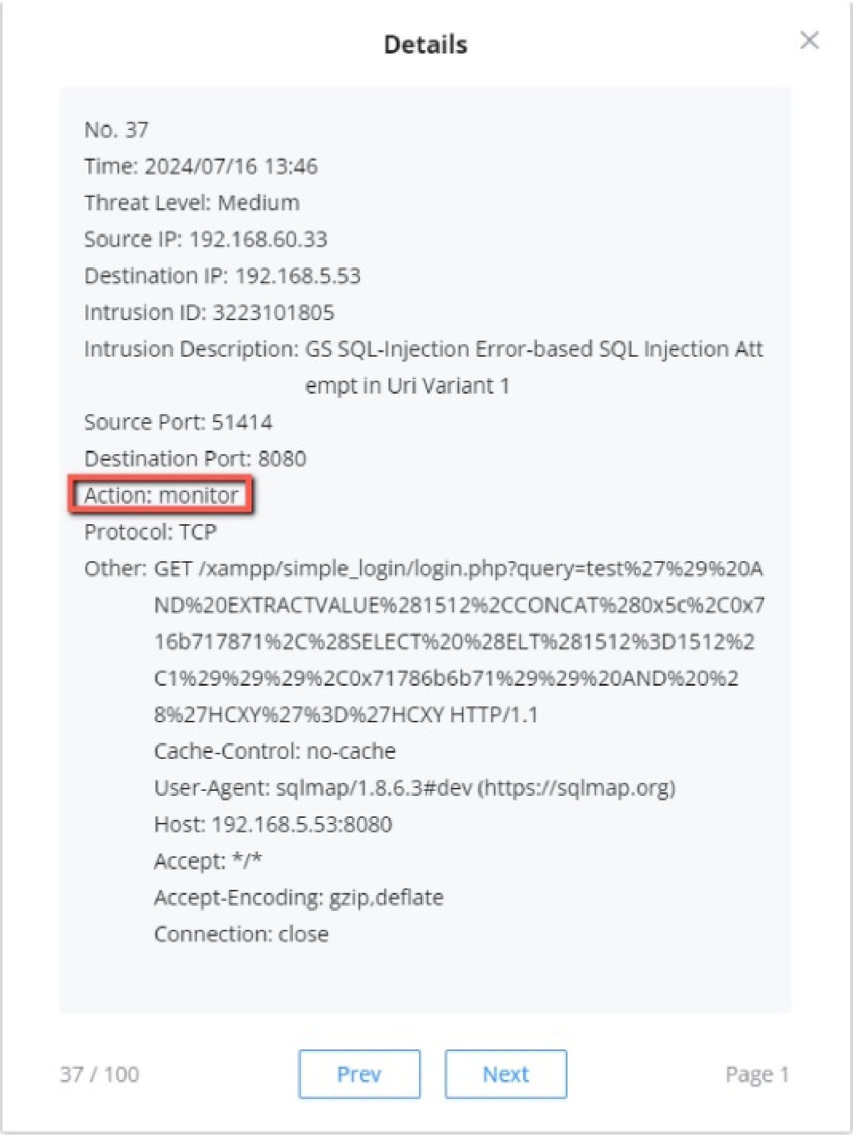
IDS/IPS Security Logs Examples

To view more information on each log, you can click the icon corresponding to the log entry:



```
No. 36
Time: 2024/07/16 13:46
Threat Level: Medium
Source IP: 192.168.60.33
Destination IP: 192.168.5.53
Intrusion ID: 3424031301
Intrusion Description: GS SQL-Injection MySQL >= 5.1 AND error-ba
                       sed - WHERE, HAVING, ORDER BY or GROUP
                       BY clause (EXTRACTVALUE) Variant 1
Source Port: 51414
Destination Port: 8080
Action: block
Protocol: TCP
Other: GET /xampp/simple_login/login.php?query=test%27%29%20
       AND%20EXTRACTVALUE%281512%2CCONCAT%280x5c%2C0
       x716b717871%2C%28SELECT%20%28ELT%281512%3D151
       2%2C1%29%29%29%2C0x71786b6b71%29%29%20AND%2
       0%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
```

IPS Block



```
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%20A
       ND%20EXTRACTVALUE%281512%2CCONCAT%280x5c%2C0x7
       16b717871%2C%28SELECT%20%28ELT%281512%3D1512%2
       C1%29%29%29%2C0x71786b6b71%29%29%20AND%20%2
       8%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   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.

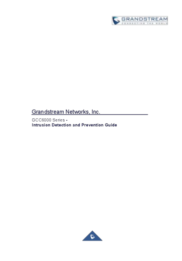
Tunnel	Tunneling attacks involve encapsulating one type of network traffic within another to bypass security controls or firewalls.	Using HTTP tunneling to send non-HTTP traffic through an HTTP connection.
IoT (Internet of Things)	Monitoring and detecting anomalies in IoT devices to prevent potential 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!

Documents / Resources

 Grandstream Networks, Inc. GCC6000 Series - Intrusion Detection and Prevention Guide	**GRANDSTREAM GCC6000 Series Intrusion Detection UC Plus Networking Convergence Solutions** [pdf] User Guide GCC6000, GCC6000 Series, GCC6000 Series Intrusion Detection UC Plus Networking Convergence Solutions, Intrusion Detection UC Plus Networking Convergence Solutions, Detection UC Plus Networking Convergence Solutions, Networking Convergence Solutions, Solutions

References

- **documentation.grandstream.com/knowledge-base/gcc6000-series-intrusion-detection-and-prevention-guide/?hkb-redirect&nonce=04f52c5a7f&check=2nufl&redirect=helpdesk.grandstream.com&otype=ht_kb_article&oid=**
- **documentation.grandstream.com/wp-content/uploads/2024/07/IDS_IPS-difference.png**
- **documentation.grandstream.com/wp-content/uploads/2024/11/IDS_IPS-Security-Logs.png**
- **documentation.grandstream.com/wp-content/uploads/2024/11/IPS-Block.png**
- **documentation.grandstream.com/wp-content/uploads/2024/11/monitor-IDS.png**
- **documentation.grandstream.com/wp-content/uploads/2024/11/update-interval.png**
- **documentation.grandstream.com/wp-content/uploads/2024/12/IDS-IPS-basic-Settings.png**
- User Manual