Gigamon®

GigaVUE-OS Security Hardening Guide

GigaVUE Cloud Suite

Product Version: 6.5

Document Version: 1.1

Last Updated: Thursday, October 10, 2024

(See Change Notes for document updates.)

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.5.00	1.1	10/10/2024	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.5.00	1.0	12/11/2023	The original release of this document with 6.5.00 GA.

Contents

GigaVUE Security Hardening

This guide provides the best practices on securing the GigaVUE operating system.

Topics:

Introduction

This guide provides you information on the options that are available in the GigaVUE-OS to harden a device against attack by threat actors and other threat vectors, such as brute for attacks.

This document is intended for an audience who is familiar with the configuration of GigaVUE-OS Appliances.

Physical Control

Physical access to any device can result in equipment that has been tampered with, both in transit and also after it is deployed. Before deploying, you must ensure that the device must be stored in safe location and also verify that the device is not tampered with before installation.

Checking for tampering

When shipped from the factory, all GigaVUE appliances are provided in a sealed box. You must inspect the box before installation to ensure that it has not been opened.

Anti-tampering stickers

Tampering of the GigaVUE Appliance can be detected using Anti-Tampering Stickers which Gigamon provides for purchase. These ensure that any physical intrusion into the chassis of the device can be easily detected. Instructions for best placement of the Anti-

Tampering stickers is provided. Incorrect placement of sticker might result in closing of ventilation holes which can adversely affect the air flow required for cooling the appliance.

Disabling the Serial Interface

GigaVUE Appliance must be installed in a physically secure environment. It is recommended to disable the serial interface. The login to GigaVUE-OS using serial port is secured by authentication methods (i.e. local / TACACS+ / RADIUS).

By default, the serial port session does not log out when a serial port is disconnected. You must configure the session time.

NOTE: Access to the serial port is required to reset the device. If you lose the login credentials for the GigaVUE-OS appliance, you will not be able to factory-reset the device. It requires a RMA which will have associated costs.

To disable the Serial Interface, run the command `no serial enable`.

```
gigavue-appliance > enable
gigavue-appliance # configure terminal
gigavue-appliance (config) # no serial enable
Disable serial console will make serial connection unusable.
Only use this config command when you have available telnet/ssh connections.
Enter 'YES' to confirm this operation: YES
Serial Console disabled.
gigavue-appliance (config) #
```

You can enable the serial interface by running the command `serial enable`

```
gigavue-appliance (config) # serial enable
Serial Console enabled.
gigavue-appliance (config) #
```

Network Controls

Overview of IP Filter

The GigaVUE-OS Appliance allows the administrator to drop undesired connections from the network received on the management interface. It prevents unauthorized access to and from the interface. For example, you can restrict a syslog server that can communicate with the GigaVUE Appliance.

An IP filter is a chain of rules for the treatment of packets. It comprises of the following chains:

- FORWARD: It is used for forwarding the traffic from one interface to another. The forward chain is not used under normal operations. The default policy for this chain is DROP.
- INPUT: It is used for the traffic that is received by the interface and the destination of the traffic is the GigaVUE Appliance. The default policy for this chain is DROP.
- OUTPUT: It is used for the traffic being sent from the GigaVUE Appliance. This is used to restrict the remote systems that can be accessed by the GigaVUE appliance. For example, remote Syslog Servers or connecting to SCP/FTP/HTTP/HTTP Servers. The default policy for this chain is ACCEPT.

The Chain that is to be applied to the packet is determined by its source and destination. For example, a user connecting to the GigaVUE appliance using SSH will have the INPUT Chain and its rules applied to the session. A user logged into the GigaVUE appliance who is trying to connect from the GigaVUE appliance to a remote system will have the OUTPUT Chain and its rules applied to the session.

Each of the above Chains has a set of rules which are processed in order.

The INPUT Chain has a policy set to DROP. If there is no match in the rules for the packets, then the packets will be dropped.

There are six rules in this Chain. The function of each rule is:

1. Accepts all ICMP packets from any source to any destination.
2. Accepts all IGMP packets from any source to any destination.
3. Accepts all the packets where there is an established or related session. For example, accepting packets in both directions of a flow (SSH Client to GigaVUE Appliance / GigaVUE Appliance to SSH Client).

4. Allows all communications for the loopback (lo) interface.
5. Accepts all communications from the subnet 12.00.1.0/24 to any destination .
6. Accepts all communications to the subnet 12.00.1.0/24 from any destination.

Rules 5 and 6 allow connections from the subnet 12.00.1.0/24. This is being used internally within the GigaVUE Appliance to allow the Management Board to communicate with GigaSMART. The traffic to/from these IP's do not appear on the physical network and that these connections between the Management Board and GigaSMART are authenticated.

There is a Policy associated with each Chain, which can be set to ACCEPT or DROP the targets. If the Policy is set to DROP, and there are no matches for the incoming packets in the rules of the Chain, then the packet will be dropped. If the Policy is set to ACCEPT and if there are no matches for the incoming packets in the rules of the Chain, then the packet will be accepted.

For more information on IP Security Chain, refer the IP Filter Chains for Security topics in the GigaVUE-OS CLI Reference Guide.

Best Practices for Security Hardening

The following sections list best practices for security:

- Use of SNMPv1 and SNMPv2 are Not Recommended
- Use of Self-Signed Certificates are Not Recommended
- Use of FTP and TFTP are Not Recommended
- Use of Enhanced Cryptography Mode to Run Scans is Recommended

Use of SNMPv1 and SNMPv2 are Not Recommended

Using SNMPv1 and SNMPv2 are not recommended because they authenticate using unencrypted, plaintext community strings.

Using SNMPv3 is recommended for access to the SNMP agent, as well as to SNMP traps. SNMPv3 authenticates using encrypted community strings. For more information, refer to Use SNMP.

Use of Self-Signed Certificates are Not Recommended

Using self-signed TLS/SSL certificates are not recommended.

Certificates generated by a third party certification authority are recommended because they are issued by a Certification Authority (CA). Refer to SHA2-Based Signature in TLS/SSL Server X.509 Certificate for how to obtain a third party certificate.

Use of FTP and TFTP are Not Recommended

Using FTP or TFTP for file transfers is not recommended.

Using SFTP, SCP, or HTTPS is recommended for uploading or downloading files to or from GigaVUE Cloud Suite nodes.

Use of Enhanced Cryptography Mode to Run Scans is Recommended

Using secure cryptography mode to run scans is recommended.

Refer to Configure Enhanced Cryptography Mode for more information.

When a scan includes password brute force testing, it is recommended to disable locking users due to many attempts.

To disable lockout of accounts based on failed authentication attempts, select **Settings > Authentication > AAA**. Under Lockout, unselect **Enable Lockout**. For more information about Lockout, refer to Lockout.

GigaVUE-OS Security Hardening

To harden the GigaVUE Cloud Suite operating system, GigaVUE-OS, against security threats, Gigamon fixes known vulnerabilities, keeps up-to-date any OS components that provide remote access (such as Apache, SSH, SSHD, and OpenSSL), and analyzes the system for attack vectors.

GigaVUE Cloud Suite nodes run the GigaVUE-OS, which is hardened against the following:

- SHA2-Based Signature in TLS/SSL Server X.509 Certificate
- ICMP Timestamp Response
- TCP Timestamp Response
- Non-Standard SNMP Community Name

SHA2-Based Signature in TLS/SSL Server X.509 Certificate

Certificates generated by a third party certification authority are more secure than self-signed certificates. High strength ciphers with key lengths equal to or greater than 112 bits are also more secure than ciphers with less than 112 bits.

GigaVUE-OS supports TLS/SSL server X.509 certificates, including SHA2-256 and SHA2-512-based certificates, as well as SHA1-based certificates.

However, SHA1 has known weaknesses that expose it to collision attacks, which may allow an attacker to generate additional X.509 certificates with the same signature as the original.

Therefore, when a third party certificate is requested, SHA2-256 or SHA2-512 should be requested as the signature algorithm, and not SHA1.

Obtain Third Party Certificate

To obtain a third party certificate, on Linux or Linux app (such as Cygwin), generate a private key as follows:

- openssl req -new -key privkey.pem -out cert.csr

The file, cert.csr is sent to a third party certificate authority, which will generate a certificate.

Supported Ciphers

The ciphers supported with TLS v1.2 are listed in the following table:

Table 1: Supported Ciphers with TLS v1.2.

Authenticated Encryption with Additional Data (AEAD) Ciphers
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Authenticated Encryption with Additional Data (AEAD) Ciphers
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)

ICMP Timestamp Response

The GigaVUE-OS does not respond to Internet Control Message Protocol (ICMP) timestamp requests.

The response to such a request is an ICMP timestamp response. The response can contain the date and time from a GigaVUE Cloud Suite node, which could be used to exploit weak time-based random number generators in other services on the node, therefore this is disabled.

In addition, ICMP echo broadcasts, including timestamp requests and responses, are disabled, since ICMP echo requests may be used for Denial of Service (DoS) attacks, such as packet flooding.

TCP Timestamp Response

The GigaVUE-OS does not respond to Transmission Control Protocol (TCP) timestamp requests.

The response to such a request is a TCP timestamp response. The response can be used to approximate the uptime of the GigaVUE Cloud Suite node, which can then be used in is DoS attacks.

In addition, some operating systems can be fingerprinted based on the behavior of their TCP timestamps, therefore this is disabled.

Non-Standard SNMP Community Name

Gigamon does not recommend using the default SNMP community string, public. It recommends using a non-standard SNMP community name, gigamon.

For steps to protect against SNMP vulnerabilities, refer to Recommendations for Vulnerabilities in the Use SNMP chapter.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)