National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Gigamon GigaVUE 4.4

Report Number: CCEVS-VR-VID10648-2016
Version 1.0
March 4, 2016

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Luke Florer, Lead Validator
Aerospace Corporation

Jerome Myers, Senior Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Jeff Barbi
Justin Fisher
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Gigamon GigaVUE version 4.4.03 provided by Gigamon Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in January 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP).

The Target of Evaluation (TOE) is the Gigamon GigaVUE HD8, HD4, HC2, HB1, TA10, and TA40 with software version 4.4.03 standalone network device. This device is used to receive out-of-band copied network data from external sources and forward that data to one or many tool ports for packet capture and/or analysis based on selected criterial. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDPP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDPP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Gigamon GigaVUE Security Target, Version 1.0*, dated December 11, 2015 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Gigamon GigaVUE devices with software version 4.4.03 *Refer to Table 2 for Models and Specifications
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional HTTPS, SSH, and TLS requirements) and Errata #3
Security Target	Gigamon GigaVUE Security Target, Version 1.0, December 11, 2015
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Gigamon GigaVUE" Evaluation Technical Report v1.0 dated January 29, 2016
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Gigamon, Inc.
Developer	Gigamon, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Luke Florer, Aerospace Corporation Jerome Myers, Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNDETECTED_ACTIONS** — Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.PROTECTED_COMMUNICATIONS —** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- **O.VERIFIABLE_UPDATES —** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- **O.SYSTEM_MONITORING —** The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- **O.DISPLAY_BANNER —** The TOE will display an advisory warning regarding use of the TOE.

- **O.TOE_ADMINISTRATION —** The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.RESIDUAL_INFORMATION_CLEARING —** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.SESSION_LOCK —** The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.TSF_SELF_TEST —** The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly**.**

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional HTTPS, TLS, and SSH requirements) with Errata #3 to which this evaluation claimed exact conformance.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Section 6 of the Security Target. The traffic forwarding functionality included in the product and described in Section 1.3 of the Security Target was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated configuration of the TOE includes the Gigamon GigaVUE product that is comprised of one or more of the product models listed in Table 2 and includes version 4.4.03 of its software. There are no separately purchased licenses or components that must be acquired in order to operate the product in its evaluated configuration. The TOE includes all the code that enforces the policies identified (see Section 5). The SCP, SFTP, FTP, and TFTP interfaces to the update server in order to download product updates and Telnet for remote administration are excluded from the evaluated configuration. Additionally, the TOE must be configured into its enhanced security mode in order to enforce the cryptographic algorithms and ciphersuites that are claimed in the Security Target.

The exclusion of these functionalities do not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

GigaVUE HD8, HD4, HC2, HB1, TA10 and TA40 with software version 4.4.03 (herein referred to as GigaVUE or the TOE) uses the Gigamon Forwarding Policy to receive out-of-band copied network data from external sources (TAP or SPAN port) and forward that copied network data to one or many tool ports for packet capture or analyzing tools based on user selected criteria. GigaVUE can also copy the network traffic itself when sitting in-line with the network flow using passive, inline and bypass taps or any combination. GigaVUE features extensive filtering abilities enabling authorized users to forward precise customized data flows of copied data from many sources to a single tool, from a single source to many tools, or from many sources to many tools.

The TOE consists of one or more models as specified below. Each of the models includes software version 4.4.03.

4.2 Physical Boundaries

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Table 2 – Hardware Models and Specifications (HD8 and HD4 Series)

Property	HD8	HD8	HD4	HD4
Model Number	GVS-HD8A1 GigaVUE-HD8 base unit w/ chassis, CLI	GVS-HD8A2 GigaVUE-HD8 base unit w/ chassis, CLI	GVS-HD4A1 GigaVUE-HD4 base unit w/ chassis, CLI	GVS-HD4A2 GigaVUE-HD4 base unit w/ chassis, CLI
Size	14RU	14RU	5RU	5RU
Total Slots	8	8	5	5
Power	AC	DC	AC	DC
Control Cards	1 or 2	1 or 2	1	1
Port Blades	PRT-H00-X12G04 Port Blade, HD Series, 12x10G 4x1G PRT-H00-X12TS Port Blade, HD Series, 12x10G Time Stamp PRT-H00-X04G44 Port Blade, HD Series, 4x10G 44x1G PRT-H00-Q02X32 Port Blade, HD Series, 2x40G 32x10G (24 10G + 2 40G or 32 10G active) PRT-HD0-Q08 Port Blade, HD Series, 8x40G PRT-HD0-C01 Port Blade, HD Series, 1x100G PRT-HD0-C02X08 Port Blade, HD Series, 2x100G CFP cages + 8x10G cages PRT-HD0-C02X08A Port Blade, HD Series, 2x100G CFP2 cages + 8x10G cages GigaSMART Module: SMT-HD0-GigaSMART, HD Series blade (includes Slicing, Masking, Source Port,& GigavuE Tunneling De-Encapsulation SW			
Power Supplies	4	4	2	2
Processor	PowerPC 600	PowerPC 600	PowerPC 600	PowerPC 600
Memory (RAM)	CCv1: 2GB CCv2: 4GB	CCv1: 2GB CCv2: 4GB	CCv1: 2GB CCv2: 4GB	CCv1: 2GB CCv2: 4GB
Logical Drive Capacity	CCv1: 2GB CCv2: 8GB	CCv1: 2GB CCv2: 8GB	CCv1: 2GB CCv2: 8GB	CCv1: 2GB CCv2: 8GB

Fixed Ports	None	None	None	None
Configurable Ports	Provided by Port Blades	Provided by Port Blades	Provided by Port Blades	Provided by Port Blades

Table 3 – Hardware Models and Specifications (HC2 Series)

Property	HC2	HC2
Model Number	GVS-HC201 GigaVUE-HC2 base unit w/ chassis, CLI,	GVS-HC202 GigaVUE-HC2 base unit w/ chassis, CLI
Size	2RU	2RU
Front Bays	4	4
Rear Bays	1	1
Power	AC	DC
Main Board	1	1
TAP Modules	TAP-HC0-D25AC0 TAP module, HC Series, SX/SR Internal TAP Module 50/125, 12 TAPs TAP-HC0-D25BC0 TAP module, HC Series, SX/SR Internal TAP Module 62.5/125, 12 TAPs TAP-HC0-D35CC0 TAP module, HC Series, LX/LR Internal TAP Module, 12 TAPs TAP-HC0-G100C0 TAP and Bypass module, HC Series, Copper, 12 TAPs or BPS pairs	
Bypass Combo Modules	BPS-HC0-D25A4G Bypass Combo Module, HC Series, 4 SX/SR 50/125 BPS pairs, 16 10G cages BPS-HC0-D25B4G Bypass Combo Module, HC Series, 4 SX/SR 62.5/125 BPS pairs, 16 10G cages BPS-HC0-D35C4G Bypass Combo Module, HC Series, 4 LX/LR BPS pairs, 16 10G cages	
Port Modules	PRT-HC0-X24 Port Module, HC Series, 24x10G PRT-HC0-Q06 Port Module, HC Series, 6x40G GigaSMART Modules: SMT-HC0-R GigaSMART, HC Series rear module (includes Slicing, Masking, Source Port & GigaVUE Tunneling De-Encapsulation SW) SMT-HC0-X16 GigaSMART, HC Series, Front Module, 16 10G cages (includes Slicing, Masking, Source Port & GigaVUE Tunneling De-Encapsulation SW	
Power Supplies	2	2
Processor	PowerPC 600	PowerPC 600
Memory (RAM)	4GB	4GB
Logical Drive Capacity	8GB	8GB
Fixed Ports	PTP IEEE 1588 Stack Mgmt Port Mgmt Console	PTP IEEE 1588 Stack Mgmt Port Mgmt Console
Configurable Ports	Provided by TAP Modules, Bypass combo modules, Port Modules	Provided by TAP Modules, Bypass combo modules, Port Modules

Table 4 – Hardware Models and Specifications (HB1 Series)

Property	HB1	HB1
Model Number	GVS-HB101-0416 branch node	GVS-HB102-0416 branch node
Size	1RU	1RU
Cages	4 10G cages 8 1G cages	4 10G cages 8 1G cages

Copper	8 1G	8 1G
Power	AC	DC
Power Supplies	1	1
Processor	PowerPC 600	PowerPC 600
Memory (RAM)	2GB	2GB
Logical Drive Capacity	2GB	2GB
Fixed Ports	PTP 1588 Mgmt Console 8 10/100/1000 Ports, 8 1G Ports (SFP), 4 1G/10G (SFP+)	PTP 1588 Mgmt Console 8 10/100/1000 Ports, 8 1G Ports (SFP), 4 1G/10G (SFP+)
Configurable Ports	None	None

Table 5 – Hardware Models and Specifications (TA10 Series)

Property	TA10	TA10
Model Number	GigaVUE-TA10 Edge Traffic Aggregation Node (SKU GVS-TAX01)	GigaVUE-TA10 Edge Traffic Aggregation Node (SKU GVS-TAX01)
Size	1RU	1RU
Power	AC	DC
Power Supplies	2	2
Processor	PowerPC e500	PowerPC e500
Memory (RAM)	4GB	4GB
Logical Drive Capacity	8GB	8GB
Fixed Ports	Mgmt Console 48 1G/10G Ports (SFP+) 4 10G/40G QSFP Ports	Mgmt Console 48 1G/10G Ports (SFP+) 4 10G/40G QSFP Ports
Configurable Ports	None	None

Table 6 – Hardware Models and Specifications (TA40 Series)

Property	**TA40**	**TA40**
Model Number	GigaVUE-TA40 Edge Traffic Aggregation Node (SKU GVS-TAQ01)	GigaVUE-TA40 Edge Traffic Aggregation Node (SKU GVS-TAQ01)
Size	1RU	1RU
Power	AC	DC
Power Supplies	2	2
Processor	PowerPC e500	PowerPC e500
Memory (RAM)	4GB	4GB
Logical Drive Capacity	8GB	8GB
Fixed Ports	Mgmt Console 32 10G/40G QSFP Ports	Mgmt Console 32 10G/40G QSFP Ports
Configurable Ports	None	None

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 7 – Operational Environment Components

Component	Usage/Purpose Description for TOE performance
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or a web browser to access the web GUI, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
Update Server	A general-purpose computer that includes a web server and is used to store software update packages that can be retrieved by the TOE using TLS/HTTPS. The update server can be a server maintained by Gigamon or it can be set up locally in the Operational Environment by an administrator if the TOE's deployment prevents it from being able to access Gigamon's web domain.
LDAP Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory.
NTP Server	A server that provides reliable time data to the TOE's system clock so that the timestamps on its audit records can be synchronized with other devices in the Operational Environment that connect to the same server.
Syslog Server	An SFTP server that can be used by the TOE to transfer its stored syslog audit data to using SSH.

5 Security Policy

5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record includes timestamp, event type, and subject identity where applicable. The audit records are stored locally and sent securely to the environmental syslog server using SSH. The TOE's local audit data storage is used to continue recording audit data in the event that communications between the TOE and the syslog server fail. Only authorized administrators can delete locally stored audit data.

5.2 Cryptographic Support

The TOE uses sufficient security measures to protect its data in transmission by implementing cryptographic methods and trusted channels. The TOE uses SSH to secure the remote CLI and Syslog Server trusted channels. The TOE also uses TLS/HTTPS to secure the trusted channels for the secure WebGUI, update server and LDAP server. SSH and TLS/HTTPS protocols implement Diffie-Hellman and RSA based key generation and key establishment methods. The cryptographic algorithms are provided by a FIPS validated cryptographic module (CMVP certificate #2128). Cryptographic keys are generated using the CTR_DRBG provided by this module. The TOE zeroizes all plaintext secret and private keys by overwriting the memory location occupied by the keys and deallocating their memory locations. In the evaluated configuration the TOE operates in "Enhanced Security Mode" which is used to restrict algorithms to meet the PP requirements.

The following table contains the CAVP algorithm certificates.

Table 4 CAVP References

Algorithm	Cert. #
AES-CBC-128, AES-CBC-256	2273
RSA	1166
CTR_DRBG (AES)	281
SHA-1, SHA-256, SHA-512	1954
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512	1391

5.3 User Data Protection

The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. The TOE ensures this by zeroizing the data upon allocation of memory. Residual data is never transmitted from the TOE.

5.4 Identification and Authentication

Users authenticate to the TOE as administrators via the local console, remote CLI, or remote web GUI. Administrators are authenticated through a username and password defined on the TOE, a username and password defined on an environmental LDAP server, or username and SSH public key. The TOE does not allow any TSF functionality to be performed prior to successful authentication other than a display of the warning banner. When authenticating via the local console, any input credential data is not echoed back to the screen by the TSF.

5.5 Security Management

The TOE maintains the roles of Admin, Monitor, and Operator. Of these roles, only the Admin role is authorized to manage the behavior of the TSF. The other roles are used to perform actions that are entirely outside the scope of the claimed Protection Profile. All administration of the TOE can be performed locally using a management workstation connected to the serial console, remotely using a CLI from a management workstation that communicates with the TOE using SSH, or remotely using a web GUI from a management workstation that communicates with the TOE using TLS/HTTPS.

5.6 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE stores password data as SHA-512 hashes and does not provide a mechanism to access any pre-shared keys, symmetric keys, or private keys. The TOE maintains system time with either its local hardware clock or with NTP server synchronization. At start-up, the TOE performs an integrity test of its cryptographic module, known answer tests for cryptographic services, self-tests of all components connected to the motherboard (memory, CPU, Ethernet controllers, etc.), and any components that are connected to the device via PCIe interfaces. Software updates are securely downloaded from a remote server using TLS/HTTPS and are verified using a digital signature prior to being applied.

5.7 TOE Access

The TOE can terminate inactive sessions after an administrator-configurable time period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE also displays a configurable warning banner prior to use of the TSF.

5.8 Trusted Path/Channels

The TOE establishes trusted channels to the Operational Environment using TLS for LDAP server communications, SSH for syslog server communications, and TLS/HTTPS for update server communications. Administrators can establish trusted paths to the TOE using SSH for remote CLI administration and TLS/HTTPS for remote web GUI administration. All cryptographic functionality supporting the use of these trusted channels and paths is facilitated by the FIPS-validated cryptographic module contained within the TOE. In the evaluated configuration, the TOE will be configured into its enhanced security mode, which limits the cryptographic algorithms and cipher suites used for trusted communications to those that are specified in the Security Target.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Gigamon GigaVUE Supplemental Administrative Guidance, Version 1.0
- GigaVUE-OS-CLIUsersGuide-v4400
- GigaVUE-OS-HVUE-UsersGuide-v4400
- GV-TA-Series-UpgradeGuide-v4400
- GV-H-Series-UpgradeGuide-v4400
- GV-HB-Series-HardwareInstallationGuide-v4400
- GV-HC-Series-HardwareInstallationGuide-v4400
- GV-HD-Series-HardwareInstallationGuide-v4400
- GV-TA-Series-HardwareInstallationGuide-v4400
- GV-OS-ReleaseNote-v4400

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Gigamon GigaVUE standalone network hardware appliances that run version 4.4.03 of its operational software.

To use the product in the evaluated configuration, the product must be configured as specified in the *Gigamon GigaVUE Supplemental Administrative Guidance, Version 1.0* (AGD) document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation "Gigamon GigaVUE" Evaluation Technical Report v1.0 dated January 29, 2016,* as summarized in the publicly available *Assurance Activity Report* for a Target of Evaluation *"Gigamon GigaVUE" Assurance Activities Report v1.0 dated January 29, 2016* .

8.1 Test Configuration

The evaluation team configured each tested model of the TOE according the *Gigamon GigaVUE Supplemental Administrative Guidance, Version 1.0* (AGD) document for testing.

The evaluation team set up a test environment for the independent functional testing that allowed them to perform all test assurance activities across the GigaVUE HD4 and TA-40 models over the SFR relevant interfaces. A sampling of test assurance activities were also tested multiple times on the GigaVUE HB1, HC2, and TA-10 models over all SFR relevant interfaces. The testing performed has a complete overlap between the tested models and interfaces to validate that the TOE performs the same regardless of the specific model.

The selection of models for testing was based upon ensuring that all of the SFR relevant interfaces and all TOE software images were tested and that they produced the same results when tested. The AC power supplied GigaVUE HD4, HC2, HB1, TA-10, and TA-40 models running Gigamon GigaVUE-OS were deployed in the test laboratory as a representative set of the TOE's models. These models were used for the execution of the independent functional testing and vulnerability testing.

The evaluation team performed testing of the TSF functionality across all of the sampled models as well as each of the three available management interfaces (local console, remote CLI, remote GUI). The full set of tests were replicated for each model and the tests were developed to stimulate each applicable TSF relevant interface; which would fully test all combinations of the selected models and their TSF relevant interfaces. The testing performed on each physical interface of each sampled model, with the same logical interface SFR functionality, validated that the internal processing of the TOE would produce the same results regardless of the specific model or physical interface used to initiate or perform the processing. The testing is consistent with the use of the interfaces defined within the ST. Thus, the testing of the interfaces was based upon testing SFR functionality related to user actions over each interface.

The TOE was configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- NTP Server to acquire the time
- Local Update Server to perform TOE software updates
- LDAP Server to perform external authentication
- Syslog Server to transfer audit records remotely from the TOE

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 1.12.6
- Bitvise SSH Client: version 6.43

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Ciena CES models by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov. Near the completion of the evaluation, the evaluators revisited their search for known vulnerabilities and identified a memory leak vulnerability and the vendor updated the TOE to incorporate a patch to address the vulnerability.

Upon the completion of the vulnerability analysis research and initially discovering no known vulnerabilities, the team identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  The TOE’s implementation of trusted communications protocols should be correct and should not use weak ciphers or expose sensitive data in a way that would allow an attacker to break the security of the channel and gain access to TSF data in transit.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- Web Interface Vulnerability Identification
  The WebGUI that is used to manage the TOE should not contain implementation flaws such as cross-site scripting or SQL database injection vulnerabilities that would allow a user to gain or escalate their privileges on the system or to inject data into the TOE that may interfere with its functionality and cause it to enter an unknown state.
- SSH Timing Attack

The CLI interface to the TOE should not behave differently whether a valid or invalid username is supplied to it so that an attacker with no knowledge of the user database cannot enumerate valid user accounts on the TOE.

- CLI Privilege Escalation
  The TOE software is built on the Linux kernel, so an attacker should not be able to successfully ‘break out’ of the management CLI into a general-purpose Linux shell such as bash or ksh.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2.

The TOE successfully prevented any attempts of subverting its security.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Assurance Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Ciena CES TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Gigamon GigaVUE product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Security Requirements for Network Devices Protection Profile (NDPP).

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Gigamon GigaVUE Supplemental Administrative Guidance, Version 1.0* document.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Gigamon GigaVUE Security Target v1.0* dated December 11, 2015.

13 List of Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command-line Interface
CPU	Central Processing Unit
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RU	Rack Unit
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SPAN	Switch Port Analyzer
SSL	Secure Sockets Layer
SSH	Secure Shell
ST	Security Target
TAP	Test Access Point
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TP	Tool Port
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Administrator	The class of TOE user tasked with configuring the TOE beyond the forwarding policy. Embodies the “Super” role.
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the ‘admin’ role.
Connection	One to One simple flows between a network port and a tool port.
Copied Network Data	The copied network traffic that is filtered and forwarded by the TOE to a physically connected analysis tool.
Filter	Rules used to create customized data streams which include or exclude data between connections. ‘Pre’ filters operate at the Network Port (ingress to TOE) ‘Post’ filters operate at the Tool Port (egress from the TOE).
GigaStream	A grouping of multiple ports (based on IEEE 802.1 specification) into a logical bundle to increase bandwidth.
GigaVUE	The TOE; it provides secure out-of-band data access for enterprise networks.
Flow Map	Provide greater capabilities than connections by allowing the distribution of network traffic based on a set of user-defined rules, with each rule directing the traffic to one or more tool ports.
Module	Swappable hardware devices that are inserted into the expansion slots of the TOE. Modules can change the functionality of the TOE to include an internal TAP, bypass TAP, Gigabit Ethernet ports, and stacking ports.
Network Port	Where data arrives into the TOE. The ports which receive copied network data for the TOE. SPAN or TAPs are connected to a network port to provide data into the TOE.
Production Network	The network(s) which the GigaVUE receives or copies network traffic from. Note: The TOE takes no action on this traffic. When the TOE is in-line with the production network traffic, the traffic received by the TOE is the same traffic that is sent back out to the production network. During internal GigaVUE processes, this traffic is copied becoming the Copied Network Data.
Security Administrator	Synonymous with Authorized Administrator.
Stacking	The ability to connect one TOE to another TOE and have data flow between them.
System Administrator	The class of TOE administrators that are tasked with managing the TOE’s deployment and configuration.
Tool Port	Where data leaves the TOE. The ports to which the TOE sends data that has been filtered and directed. Tools are connected to the tool ports and receive copied data from the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Gigamon GigaVUE Security Target v1.0
6. Gigamon GigaVUE Supplemental Administrative Guidance, Version 1.0