Gigamon GigaVUE

Security Target

ST Version: 1.0
December 11, 2015

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title:	Gigamon GigaVUE Security Target
ST Version:	1.0
ST Publication Date:	December 11, 2015
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1 and 1-2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator	The class of TOE user tasked with configuring the TOE beyond the forwarding policy. Embodies the "Super" 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.
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.

Table 1: Customer Specific Terminology

Term	Definition
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.
Security Administrator	Synonymous with Authorized Administrator.
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.

Table 2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

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

Table 3: Acronym Definition

1.1.5 Reference

[1] Protection Profile for Network Devices, version 1.1 (NDPP)
[2] Security Requirements for Network Devices, Errata #3
[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001

[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[6] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[7] NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009
[8] NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, December 2001
[9] FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[10] FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[11] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS) March 2012
[12] FIPS PUB 197 Advanced Encryption Standard November 26 2001
[13] FIPS PUB 198-1 Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[14] Gigamon Linux-Based Cryptographic Module CMVP certificate #2128
[15] Gigamon GigaVUE Supplemental Administrative Guidance v1.0
[16] GigaVUE-OS-CLIUsersGuide-v4400
[17] GigaVUE-OS-HVUE-UsersGuide-v4400
[18] GV-TA-Series-UpgradeGuide-v4400
[19] GV-H-Series-UpgradeGuide-v4400
[20] GV-HB-Series-HardwareInstallationGuide-v4400
[21] GV-HC-Series-HardwareInstallationGuide-v4400
[22] GV-HD-Series-HardwareInstallationGuide-v4400
[23] GV-TA-Series-HardwareInstallationGuide-v4400
[24] GV-OS-ReleaseNote-v4400

1.2 TOE Reference

The TOE is the Gigamon GigaVUE HD8, HD4, HC2, HB1, TA10 and TA40 with software version 4.4.03.

1.3 TOE Overview

The TOE includes the models HD8, HD4, HC2, HB1, TA10 and TA40 with software version 4.4.03. These models include modular components and can be configured per the tables defined in Section 2.4.1. These models allow an Authorized Administrator to access the TOE through a serial port, remote CLI via SSH, and a WebGUI via TLS/HTTPS. The TOE was evaluated against the requirements defined in Section 6.2 only. Refer to Section 2.5 for a summary of the functional claims tested.

The GigaVUE's primary functionality is to use 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.

A GigaVUE model:

- Receives a copy (or copies internally) network traffic
- Filters copied data based upon user selected criteria
- Forwards copied data to user selected ports

The TOE was evaluated as a network device only and the GigaVUE's network traffic capture, filter, and forwarding capabilities described above were not assessed during this evaluation.

The following figure depicts the TOE boundary:

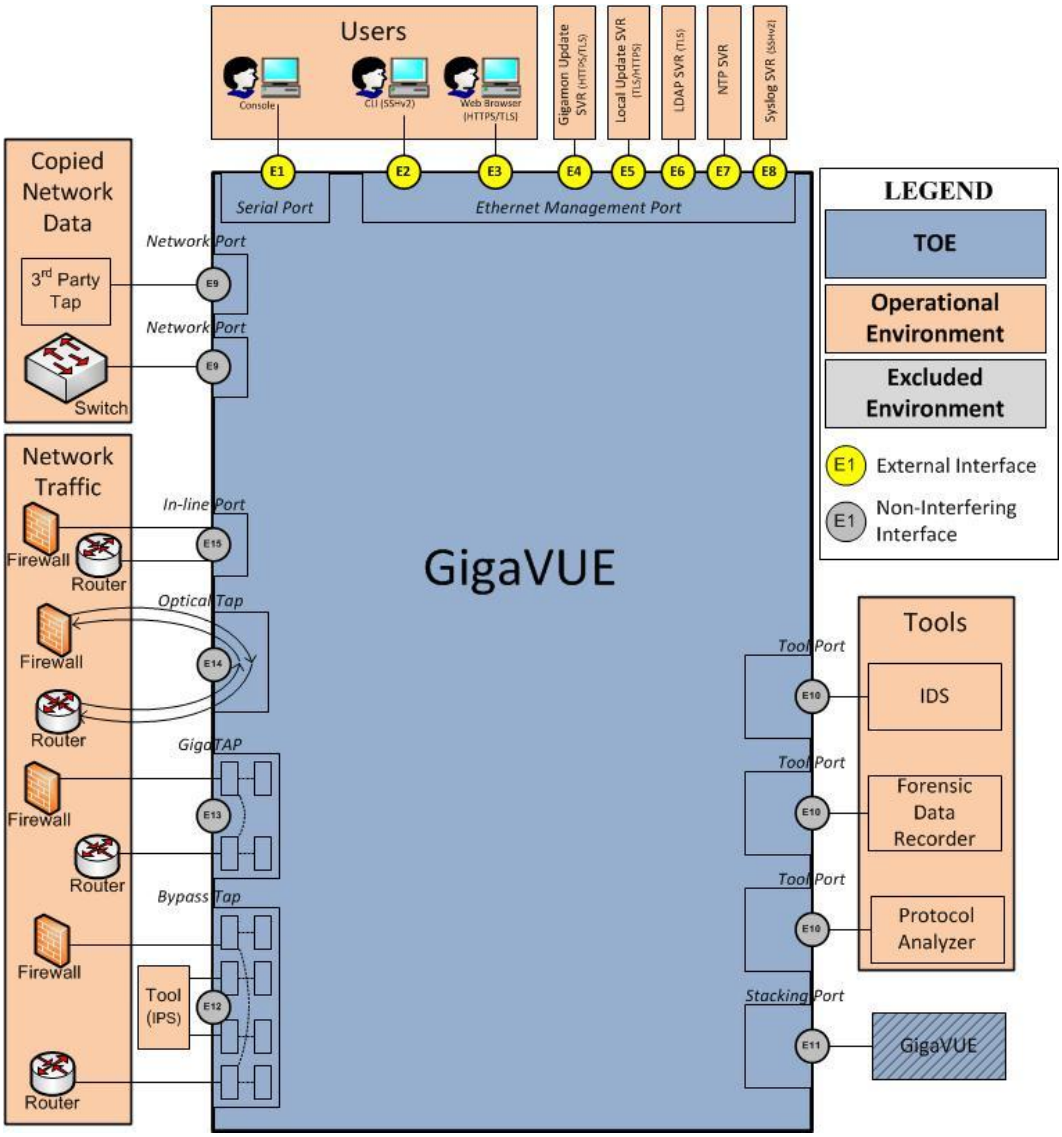

Figure 1: TOE Boundary for GigaVUE

As illustrated in Figure 1, the GigaVUE is a single hardware device that has management ports, network (or ingress) ports, and tool (or egress) ports. The TOE has management interfaces: a Serial Management Port and an Ethernet Management Port. The Ethernet Management Port allows authorized users to connect to the TOE via SSH or HTTPS to manage and use the TOE in an out of band environment. In addition, the Management Port is used to communicate to external authentication servers, if configured. The Ethernet Management Port is also used to communicate to other external servers such as the Syslog Server.

1.3.1 GigaVUE Purpose

The TOE was evaluated as a network device only and the GigaVUE's network traffic capture, filter, and forwarding capabilities described in Section 1.3.2 were not assessed during this evaluation. This information is only being provided to understand the primary purpose.

GigaVUE receives data from many sources, or networks. It can receive data from a 3rd party TAP or SPAN port. The GigaVUE can also be configured to be its own TAP. The internal TAP can be electrical so that it sits in line and copies the data, allowing the network traffic to continue to flow through unimpeded. GigaVUE also features an optical TAP that sits in line with production network and splits the light passing through the optical splitter making a copy of the network traffic.

GigaVUE can also act as a bypass TAP or a GigaTap. In this configuration, GigaVUE connects to both sides of an IPS or other in-line device and monitors both itself and the in-line device. Specifically, the GigaVUE copies network traffic creating copied network data, filters it, and sends it to tools. The GigaVUE Bypass TAP will then forward the data to the IPS or other in-line device, allow the device to perform its own designated functionality, and then receive the data again from the same device. The GigaVUE will then process the data a second time using the same functionality to copy the network traffic after the in-line device process. Then the GigaVUE Bypass TAP will send the network traffic out to the production network. The GigaTap is a TAP that has the ability to split and copy inbound or outbound data streams.

GigaVUE forwards the data received via a network port to a tool port based on user configured policy. Tool ports are physically connected to a packet capture or other analyzing tools. Any type of tool can be attached to the tool port such as an IDS, forensic data recorder, sniffer, or protocol analyzer.

1.3.2 **Deployments**

GigaVUE was evaluated as a network device only and the network traffic capture, filter, and forwarding capabilities described in Section 1.3.1 were not assessed during this evaluation. This information is only being provided to describe the operation in a multi-GigaVUE deployment.

As illustrated in Figures 1 and 2, the TOE can be deployed in a variety of ways. GigaVUE can be a standalone box, as represented in Figure 1, receiving network traffic or copied network data and forwarding it to the tools attached directly to it. This deployment configuration is used when there are a smaller number of sources or tools. This deployment configuration requires the authorized user to set up connections, flow maps, or filters to forward the received data to the tools directly attached to the GigaVUE.

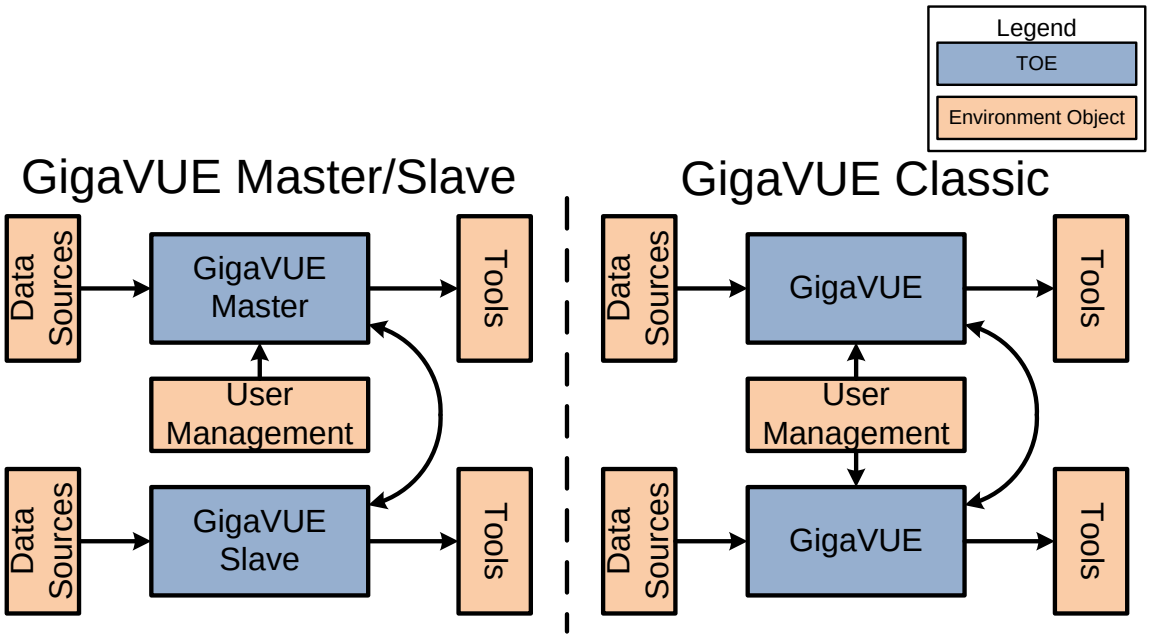

Figure 2 - Multi-GigaVUE Deployment

In addition to sending the copied network data to a specific tool port, the GigaVUE can forward the copied network data to another GigaVUE (crossbox) where it is forwarded to a tool (crossbox) connected to that GigaVUE, as is shown in the two deployments in Figure 2. The ability to connect multiple GigaVUEs is called stacking. The stacked GigaVUEs must be physically connected by one or more 10 GB or 40GB stacking links. Each stacking link uses one or more stacking ports from each GigaVUE. Multiple stacking links can be bundled together as a stack GigaStream to load balance the stack traffic. Both GigaVUEs must be configured with the same number of ports attached to each other. This connection provides two way communications between the two GigaVUEs. In this configuration the connections, flow maps and filters can be created for cross-box communication. One GigaVUE can receive data and, when a rule defines cross-box connection, forward it over to another GigaVUE and have that GigaVUE forward it to a directly connected tool. It is possible to connect more than two GigaVUEs together, for even greater flexibility, scalability, and throughput. The differences between the two deployments shown in Figure 2 are as follows: the GigaVUE can be set up in a Master/Slave configuration where a single GigaVUE is used to manage the other GigaVUEs or in a classic configuration where the GigaVUEs are connected but each TOE is managed separately.

1.4 TOE Type

The TOE is a network device that clearly meets the NDPP which states: “A network device in the context of this PP is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise. Examples of a ‘network device’ that should claim compliance to this PP include routers, firewalls, IDSs, audit servers, and switches that have Layer 3 functionality”. The TOE consists of the HD8, HD4, HC2, HB1, TA10 and TA40 models. The TOE is a network device composed of hardware and software that is connected to the network and accepts packets of data, filters them and passes them to tools for further analysis. Because the device operates at Layer 3 and serves a role in the enterprise network, this conformance claim is appropriate.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

Component	Definition
GigaVUE HD8	14RU fabric node, 8 line card slots, dual control cards
GigaVUE HD4	5RU fabric node, 4 line card slots, single control card
GigaVUE HC2	2RU fabric node, 4 front bays, 1 rear bay
GigaVUE HB1	1RU branch node
GigaVUE TA10	1RU traffic aggregator
GigaVUE TA40	1RU edge node

Table 4: Evaluated Components of the TOE

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
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.
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 (Microsoft Internet Explorer 11 or higher and Google Chrome 36 or higher) to access the WebGUI, 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.
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.
SPAN	This component provides the TOE with copied network data, but only if the TOE is configured to receive data from an external TAP or SPAN device.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
TAP	This component provides the TOE with copied network data, either from an internal GigaVUE TAP or an external TAP. The TOE can also be configured to receive data from an external source, meaning a TAP device or SPAN port.
Tool	This component is any analysis, capture or troubleshooting tool connected to a tool port. This component is required for the TOE to forward data. The connection to the tool is a physical connection.
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.

Table 5: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no components that are not installed.

2.3.2 Installed but Requires a Separate License

There are no excluded components that are installed and require a separate license.

2.3.3 Installed But Not Part of the TSF

This section contains functionality or components that are part of the purchased product but are not part of the TSF relevant functionality that is being evaluated as the TOE.

- Insecure mode of operation – GigaVUE provides an 'Enhanced Security Mode' that restricts the cryptographic algorithms and ciphersuites to what is claimed in the Security Target. Operating the product outside of this mode of operation is not within the scope of the TSF
- SCP/SFTP/FTP/TFTP mode of updating – GigaVUE provides several methods to download product updates from the Operational Environment. In the evaluated configuration, only the TLS/HTTPS method of downloading is permitted and the remaining methods are not part of the TOE.
- Port Blades, TAP Modules, Bypass Combo Modules and Port Modules – Modular components of the TOE used to capture traffic from the network in a variety of methods, for different scenarios, and to support different types of network media.
- Telnet – GigaVUE supports both Telnet and SSH2 for remote administration. In the evaluated configuration Telnet will be disabled.

2.4 Physical Boundary

2.4.1 Hardware

GigaVUE is a rack-mounted hardware device. The GigaVUE is a modular device to accommodate many variations of physical connectivity including copper, fiber, 1G, 10G, 40G and 100G ports.

The model specific hardware and their configurations are as follows:

Property	HD8	HD8	HD4	HD4
Model Number	GVS-HD8A1	GVS-HD8A2	GVS-HD4A1	GVS-HD4A2

	GigaVUE-HD8 base unit w/ chassis, CLI	GigaVUE-HD8 base unit w/ chassis, CLI	GigaVUE-HD4 base unit w/ chassis, CLI	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 6: HD8 and HD4 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 7: HC2 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 8: HB1 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 9: TA10 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

Table 10: TA40 Series

2.4.2 Software

- Gigamon GigaVUE with software version 4.4.03

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

2.5.1 Security Audit

Audit records are generated for various types of management activities and events. The audit records include the date and time stamp of the event, the event type and subject identity. The TOE generates audit records that can be configured to be pushed to the Syslog Server via an encrypted SSH channel. The audit records are stored locally and sent to the Syslog Server. If the Syslog Server connection is down, the TOE will try to automatically reconnect. The audit records are stored locally on the TOE until the connection is reestablished. Local audit records are stored in "message" files which are rotated to ensure a maximum limit of disk usage is enforced. Only users with the "Admin" privilege can access or delete the log files. Users with the Admin privilege are considered trusted users and are not expected to delete or modify the audit records.

2.5.2 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:

Algorithm	CAVP 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

Table 11 Cryptographic Algorithm Table

2.5.3 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, by writing zeros, the data upon allocation of memory. Residual data is never transmitted from the TOE.

2.5.4 Identification and Authentication

All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE. This is true of users accessing the TOE via the local console, or protected paths using the remote CLI via SSH or WebGUI via TLS 1.0. Users authenticate to the TOE using a username and password. However, for the remote CLI, users can authenticate using public-key based authentication or username and password. LDAP can be configured to provide a method of external authentication. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers and special characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates to the device, a warning banner is configured to be displayed.

2.5.5 Security Management

The TOE has role based authentication and only an Admin user can assign roles to users. Admin, Monitor and Operator are the default roles within the TOE. Only the Admin users are capable of performing SFR related management functions via the local console, remote CLI or WebGUI. The TOE's software can also be updated and is verified via a digital signature. In addition, the Admin has the ability to configure cryptographic functionality by placing the TOE in the "Enhanced Security Mode" of operation.

2.5.6 **Protection of the TSF**

The TOE stores usernames and passwords in a password file that cannot be viewed by any user on the TOE regardless of the user's role. The passwords are hashed using SHA-512. Public keys are stored in the configuration database which is integrity checked at boot time. The pre-shared, symmetric and private keys are stored in plaintext on the hard drive but cannot be accessed by any user. The TOE has an underlying hardware clock that is used for keeping time. In the evaluated configuration, the TOE can also use an NTP server to maintain accurate time information. Power-on self-tests are executed automatically when the FIPS validated cryptographic module is loaded into memory. The FIPS cryptographic module verifies its own integrity using an HMAC-SHA1 digest computed at build time. All binaries (e.g. executables, libraries), are located on a read-only partition and cannot be modified. In addition the TOE has a configuration database that is integrity checked at boot time.

The version of the TOE is verified from both the local console, remote CLI and the WebGUI.

The TOE is updated via the Gigamon update server or the local update server via an HTTPS protected connection. The updated image is verified via a digital signature.

2.5.7 **TOE Access**

The TOE can terminate inactive local console, remote CLI or WebGUI sessions after a specified time period. The default setting is 15 minutes. Users can also terminate their own interactive sessions. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also display a Security Administrator specified banner on the local console or remote CLI and the WebGUI prior to allowing any administrative access to the TOE.

2.5.8 **Trusted Path/Channels**

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a Syslog Server using SSH to encrypt the audit data that traverses the channel. The TOE also connects with an LDAP server using TLS and Gigamon update server using TLS/HTTPS to secure its data. The TOE connects to the local update server protected by TLS/HTTPS. Administrators authenticate to the TOE via the local console. The remote CLI is protected via SSH and the WebGUI is protected by TLS/HTTPS.

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through December 11, 2015.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through December 11, 2015.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- Protection Profile for Network Devices, version 1.1 [NDPP]
- Security Requirements for Network Devices, Errata #3

3.5 Package Claims

The TOE claims exact compliance to the Protection Profile for Network Devices, which is conformant with CC Part 3.

The TOE claims following optional SFRs that are defined in the appendices of the claimed PP:

- FCS_HTTPS_EXT.1
- FCS_SSH_EXT.1
- FCS_TLS_EXT.1

This does not violate the notion of exact conformance because the PP specifically indicates these as allowable options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the NDPP.

3.7 Conformance Claim Rationale

The NDPP states the following: “This is a Protection Profile (PP) for a network device. A network device in the context of this PP is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise. Examples of a ‘network device’ that should claim compliance to this PP include routers, firewalls, IDSs, audit servers, and switches that have Layer 3 functionality.”

The TOE is a network device composed of hardware and software that is connected to the network and accepts packets of data, filters them and passes them to tools for further analysis. Because the device operates at Layer 3 and serves a role in the enterprise network, this conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the NDPP.

Threat	Threat Definition
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.

Table 12 TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the NDPP.

Policy	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Table 13 TOE Organization Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the NDPP.

Assumption	Assumption Definition
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Table 14 TOE Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE. These objectives have been taken directly from the NDPP.

Objective	Objective Definition
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.

Table 15 TOE Objectives

4.4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives:

Objective	Objective Definition
OE.NO_GENERAL_PURPOSE	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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Table 16 TOE Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE

objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with bold and italicized text.
- **Refinement:** allows the addition of details. Indicated with italicized text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1	HTTPS
	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1	SSH
	FCS_TLS_EXT.1	TLS

Class Name	Component Identification	Component Name
User Data Protection	FDP_RIP.2	Full Residual Information Protection
Identification and Authentication	FIA_PMG_EXT.1	Password Management
	FIA_UAU_EXT.2	Password-Based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UIA_EXT.1	User Identification and Authentication
Security Management	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
TOE Access	FTA_SSL_EXT.1	TSF-Initiated Session Locking
	FTA_SSL.3	TSF-Initiated Termination
	FTA_SSL.4	User-Initiated Termination
	FTA_TAB.1	TOE Access Banner
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 17 Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 **Class FAU: Security Audit**

6.3.1.1 ***FAU_GEN.1 Audit Data Generation***

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) Specifically defined auditable events listed in Table *18*.

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of Table *18*.

Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM_EXT.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_RBG_EXT.1	None.	None.
FDP_RIP.2	None.	None.
FIA_PMG_EXT.1	None.	None.
FCS_TLS_EXT.1	Failure to establish an TLS session Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session. Establishment/Termination of an HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 18 Auditable Events

6.3.1.2 *FAU_GEN.2 User Identity Association*

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.3.1.3 *FAU_STG_EXT.1 External Audit Trail Storage*

FAU_STG_EXT.1.1

The TSF shall be able to [transmit the generated audit data to an external IT entity] using a trusted channel implementing the [SSH] protocol.

Application Note:

TCP tunneled via SSH is used to secure the audit data.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)*

FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with

[

- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;
- NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

6.3.2.2 *FCS_CKM_EXT.4 Cryptographic Key Zeroization*

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

6.3.2.3 *FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)*

FCS_COP.1.1(1)

The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [CBC] and cryptographic key sizes 128-bits, and 256-bits that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- [NIST SP 800-38A]

6.3.2.4 *FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)*

FCS_COP.1.1(2)

The TSF shall perform cryptographic signature services in accordance with a [

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater**]**

that meets the following:

- FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"

Application note:

In RSA cert# 1166, the rDSA algorithm that is being claimed is compliant with FIPS PUB 186-4, which superseded FIPS PUB 186-3.

6.3.2.5 *FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)*

FCS_COP.1.1(3)

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-512] and message digest sizes [160, 256, 512] bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

6.3.2.6 *FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)*

FCS_COP.1.1(4)

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[SHA-1, SHA-256, SHA-512], key size [*160 bits, 256 bits, 512 bits*], and message digest sizes [160, 256, 512] bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

6.3.2.7 *FCS_HTTPS_EXT.1 HTTPS*

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.3.2.8 *FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)*

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using [CTR_DRBG (AES)]] seeded by an entropy source that accumulated entropy from [a software-based noise source].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

6.3.2.9 *FCS_SSH_EXT.1 SSH*

FCS_SSH_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [5656, 6668].

FCS_SSH_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [***65535***] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [no other algorithms].

FCS_SSH_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [SSH_RSA] and [no other public key algorithms] as its public key algorithm(s).

FCS_SSH_EXT.1.6

The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha2-256, hmac-sha2-512].

FCS_SSH_EXT.1.7

The TSF shall ensure that diffie-hellman-group14-sha1 and [no other methods] are the only allowed key exchange method used for the SSH protocol.

6.3.2.10 *FCS_TLS_EXT.1 TLS*

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

]

6.3.3 Class FDP: User Data Protection

6.3.3.1 *FDP_RIP.2 Full Residual Information Protection*

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] all objects.

6.3.4 Class FIA: Identification and Authentication

6.3.4.1 *FIA_PMG_EXT.1 Password Management*

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

6.3.4.2 *FIA_UAU_EXT.2 Password-Based Authentication Mechanism*

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, [**an *LDAP authentication mechanism, a public-key based authentication mechanism***] to perform administrative user authentication.

6.3.4.3 *FIA_UAU.7 Protected Authentication Feedback*

FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

6.3.4.4 *FIA_UIA_EXT.1 User Identification and Authentication*

FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions]

FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.3.5 Class FMT: Security Management

6.3.5.1 *FMT_MTD.1 Management of TSF Data (for general TSF data)*

FMT_MTD.1.1

The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

6.3.5.2 *FMT_SMF.1 Specification of Management Functions*

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- [Ability to configure the cryptographic functionality]

6.3.5.3 *FMT_SMR.2 Restrictions on Security Roles*

FMT_SMR.2.1

The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

6.3.6 Class FPT: Protection of the TSF

6.3.6.1 *FPT_APW_EXT.1 Protection of Administrator Passwords*

FPT_APW_EXT.1.1

The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext passwords.

6.3.6.2 *FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)*

FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.3.6.3 *FPT_STM.1 Reliable Time Stamps*

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

6.3.6.4 *FPT_TST_EXT.1 TSF Testing*

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

6.3.6.5 *FPT_TUD_EXT.1 Trusted Update*

FPT_TUD_EXT.1.1

The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2

The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3

The TSF shall provide a means to verify firmware/software updates to the TOE using a [digital signature mechanism] prior to installing those updates.

6.3.7 Class FTA: TOE Access

6.3.7.1 *FTA_SSL_EXT.1 TSF-initiated Session Locking*

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [terminate the session] after a Security Administrator-specified time period of inactivity.

6.3.7.2 *FTA_SSL.3 TSF-initiated Termination*

FTA_SSL.3.1

The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

6.3.7.3 *FTA_SSL.4 User-initiated Termination*

FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.3.7.4 *FTA_TAB.1 TOE Access Banner*

FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

6.3.8 Class FTP: Trusted Path/Channels

6.3.8.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

FTP_ITC.1.1

The TSF shall use [SSH, TLS, TLS/HTTPS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [authentication server, **[*Local Update Server and Gigamon Update Server*]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2

The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [***authentication requests, transferring audit records, and downloading software updates***]**.**

6.3.8.2 *FTP_TRP.1 Trusted Path*

FTP_TRP.1.1

The TSF shall use [SSH, TLS/HTTPS] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured

identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data**.**

FTP_TRP.1.2

The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the PPs against which exact conformance is claimed and a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PP.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are in exact conformance with the NDPP.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 **Operational User Guidance (AGD_OPE.1)**

7.2.1.1 ***Developer action elements:***

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 ***Content and presentation elements:***

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 ***Evaluator action elements:***

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 ***Evaluator action elements:***

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 ***Developer action elements:***

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 ***Content and presentation elements:***

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 ***Evaluator action elements:***

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 ***Developer action elements:***

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 ***Content and presentation elements:***

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 ***Evaluator action elements:***

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 **Vulnerability Survey (AVA_VAN.1)**

7.5.1.1 ***Developer action elements:***

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 ***Content and presentation elements:***

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 ***Evaluator action elements:***

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. They include Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, TOE Access and Trusted Path / Channels.

8.1 Security Audit

8.1.1 **FAU_GEN.1:**

The TOE contains mechanisms to generate audit data based upon successful and unsuccessful management actions by all authorized users of the TOE. Each audit record contains identifying information of the subject performing the action. The audit records are generated and stored in the form of syslog records which are sent securely to the Syslog Server protected by SSHv2. The TOE maintains log levels which determine the set of events that are logged. The log level is set using the following command: `config system log-level`. Setting the log-level to "info" captures all the necessary logs defined in the NDPP.

The TOE allows viewing of the audit records through the local console with the following command: `show log <logfile> start <value>`

where logfile is the name of file to be used and value is used to filter out entries by date and time. Users of any role can view audit log files, however, only Admin users can delete audit log files. If an Admin deletes a log file, an audit record of that action is also recorded. In addition, audit records can be viewed from the WebGUI.

All actions performed on the TOE are logged. These include the following auditable events defined in Table 18:

- Startup and shutdown of the audit functions
- All management activities performed via the WebGUI
- All CLI commands for local users
- All CLI commands for remote users
- All authentication attempts
- All session information
- Updates and modifications of the logging levels
- Initiation and termination of Trusted Paths
- Initiation and termination of Trusted Channels
- Inactivity due to auto-logout

The following is an example of an audit record generated by the TOE for the Failed Login From Serial Port event:

```
Feb 11 20:22:43 ta1 login: pam_unix(login:auth): authentication
failure; logname=LOGIN uid=0 euid=0 tty=ttyS0 ruser= rhost=
user=admin
```

```
Feb 11 20:22:47 ta1 login: FAILED LOGIN 1 FROM (null) FOR admin,
Authentication failure
```

The audit records that the TOE creates include the following information: Date and time of the event (Feb 11 20:22:43), Event type (e.g. authentication failure), Subject identity (e.g. user admin (System Administrator), Process crond (Cron Daemon), Launched crond (Cron Daemon)), success or failure of the event, source of the event (e.g. ttyS0).

8.1.2 **FAU_GEN.2:**

The TOE records the identity of the user (e.g. username, system name, IP address) associated with each audited event in the audit record. The following are examples:

username=admin,

system name= Process crond (Cron Daemon),

IP address= 10.115.0.108.

8.1.3 **FAU_STG_EXT.1:**

The TOE generates audit records which are stored locally until the Syslog Server is initially configured. Once the Syslog Server is configured, the audit records are stored both locally and also immediately pushed to the Syslog Server via an encrypted SSH channel over the Ethernet Management Port. If the connection to the Syslog Server is down, the audit records cannot be sent to the Syslog Server and during this time period are only stored locally. Once the connection to the Syslog Server is restored, new audit records will be both stored locally and sent to the Syslog Server. The audit records that were generated during the time the Syslog Server was down remain stored locally and are not sent to the Syslog Server.

The audit records are stored locally on the TOE under the /var/log directory in files named “messages, messages.1.gz”, “messages.2.gz”,…,”messages.8.gz”. The message files are archived when they reach a specific size (8MB). These 8 files are rotated so that the 8 most recent log files are saved. This mechanism guarantees a maximum limit of disk usage used by the log files. Only a user with the “Admin” privilege can delete or modify the log files. Users with the Admin privilege are considered trusted users and are not expected to delete or modify the audit records.

8.2 Cryptographic Support

8.2.1 **FCS_CKM.1:**

The TOE implements a NIST SP 800-56A conformant key generation mechanism for Diffie-Hellman key establishment schemes. Specifically, the TOE complies with the NIST SP 800-56A key agreement scheme (KAS) primitives that are defined in section 5.6 of the SP. This is used to generate the keys for diffie-hellman-group14-sha1. In addition, the TOE implements RSA key establishment, conformant to NIST SP 800-56B. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in NIST SP 800-56B. The TOE is able to generate RSA key pairs with a modulus of at least 2048 bits which has an equivalent key strength of 112 bits.

8.2.2 **FCS_CKM_EXT.4:**

The TOE zeroizes all plaintext secret and private cryptographic keys by overwriting the memory location the keys occupy. This overwrite occurs during shutdown and power cycle of the TOE. Keys are also immediately zeroized upon deallocation using the function cleanse(), which overwrites the keys with pseudo-random data. This combined approach protects the keys from being compromised. The following table is taken from Table 6 of the Security Policy of CMVP FIPS certificate #2128 and identifies the keys and CSPs that are applicable to the TOE:

Keys and CSPs	Storage Location
AES Key	RAM
RSA Public Key	RAM
RSA Private Key	RAM
HMAC Key	RAM
CTR_DRBG Entropy	RAM
CTR_DRBG V	RAM
CTR_DRBG Key	RAM
CTR_DRBG Seed	RAM

8.2.3 **FCS_COP.1(1)**

The TOE performs encryption and decryption using the AES algorithm in CBC mode with key sizes of 128 and 256 bits. This algorithm has CAVP AES certificate #2273 that meets FIPS PUB 197 and NIST SP 800-38A. The TOE has an "Enhanced Security Mode" to restrict the AES algorithm modes to meet this requirement.

8.2.4 **FCS_COP.1(2):**

The TOE performs cryptographic digital signature verification and generation in accordance with FIPS PUB 186-4: RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater.

The algorithm has CAVP RSA certificate #1166. Note that FIPS 186-4 supersedes FIPS 186-3. The TOE has an "Enhanced Security Mode" to restrict the SHA algorithm modes to meet this requirement.

8.2.5 **FCS_COP.1(3):**

The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-512 with message digest sizes of 160, 256 and 512 bits respectively, as specified in FIPS PUB 180-3. The algorithm has CAVP SHA certificate #1954. The TOE has an "Enhanced Security Mode" to restrict the SHA algorithm modes to meet this requirement.

8.2.6 **FCS_COP.1(4):**

The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512 with key sizes and digest sizes of 160, 256 and 512 bits as specified in FIPS PUB 198-1 and FIPS PUB 180-3. The algorithm has CAVP HMAC certificate #1391. The TOE has an "Enhanced Security Mode" to restrict the HMAC-SHA algorithm modes to meet this requirement.

8.2.7 **FCS_HTTPS_EXT.1:**

The TOE invokes HTTPS, as specified in RFC 2818, to provide a secure management interactive interface via the WebGUI for administrative functions, and to support secure exchange of user authentication parameters during login, including using 2048-bit certificates for authentication. In addition, HTTPS is used to secure the connection to the Gigamon update server and local update server for downloading images to the TOE. All HTTPS user session traffic, Gigamon update server or local update server traffic is sent and received over the Ethernet Management Port.

HTTPS uses TLS 1.0 (as specified in FCS_TLS_EXT.1) to securely establish the AES encrypted session. TLS uses the following ciphersuites:

- TLS_RSA_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

By default, the HTTPS port used is port 443.

8.2.8 **FCS_RBG_EXT.1:**

The TOE performs random bit generation services in accordance with NIST SP 800-90 using CTR_DRBG with AES-256. The algorithm has CAVP DRBG certificate #281. The DRBG is seeded with at least 256 bits of entropy from the software-based entropy source.

8.2.9 **FCS_SSH_EXT.1:**

SSHv2 is used to secure the remote CLI management connection and Syslog communications. The remote CLI management traffic is sent over the Ethernet Management Port.

The TOE implements the SSHv2 protocol that complies with the following RFCs: 4251, 4252, 4253, 4254, 5656 and 6668. The TOE supports password based and public key based authentication methods as described in RFC 4252 and RSA public keys can be used for the authentication methods. The SSHv2 connection will be dropped upon detection of any packet greater than 65535 bytes being transported, as described in RFC 4253. Data encryption is provided by the AES-CBC-128 and AES-CBC-256 algorithms and data integrity by the HMAC-SHA1, HMAC-SHA2-256 and HMAC-SHA2-512 algorithms. The key exchange method used in SSHv2 is Diffie-Hellman Group14 SHA-1. By default the SSHv2 port used is port 22.

The SSH public/private key pairs are generated using the following command;

```
config system hostkey
```

The TOE has an “Enhanced Security Mode” to restrict the key exchange methods to meet this requirement.

8.2.10 **FCS_TLS_EXT.1:**

The TOE uses the TLS 1.0 protocol to secure the following connections and channels: WebGUI management interface connection using HTTPS, Gigamon update server or local update server connections using HTTPS used for TOE image updates, and LDAP server connection used for

authentication requests. When the TOE is operating in "Enhanced Security mode", TLS uses the following ciphersuites:

- TLS_RSA_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

When the TOE is not operating in the evaluated configuration, other optional ciphersuites are available.

8.3 User Data Protection

8.3.1 **FDP_RIP.2:**

The TOE ensures that packets transmitted from the product do not contain any residual information by zeroizing the data upon allocation of memory. This ensures that if a new packet reuses the same memory location as a previous packet, the location is zeroized first before the new packet is constructed.

8.4 Identification and Authentication

8.4.1 **FIA_PMG_EXT.1:**

Passwords maintained by the TSF can be composed using any combination of upper case and lower case letters, numbers and special characters including the following: "!","@","#","$","%","^","&","*","(",")". The password policy is configurable by the Admin and supports the minimum password length of 8 characters and a maximum password length of 30 characters.

8.4.2 **FIA_UAU_EXT.2:**

Users can authenticate to the TOE locally or remotely. Local users log in to the local console using a username and password via the serial port. Remote users can log in to the TOE via the remote CLI using username and password or public-key via the Ethernet Management Port. User authentication information that is sent remotely via the remote CLI is protected using SSHv2. Users may also authenticate remotely via a WebGUI that is protected using TLS/HTTPS via the Ethernet Management Port. External authentication is possible using an LDAP server. The username and password are defined in the LDAP directory and the authentication request is redirected from the TOE to the LDAP server and this connection is protected by TLS v1.0.

8.4.3 **FIA_UAU.7:**

While authenticating locally to the TOE, the user's password does not appear in the password field. Instead, asterisks will appear thus masking the password to prevent the password from being shared. In the case that a user enters invalid credentials (valid/invalid username or valid/invalid password), the TOE does not reveal any information about the invalid component of the credential.

8.4.4 **FIA_UIA_EXT.1:**

In the evaluated configuration the warning banner is displayed when the user logs on via the local console, the remote CLI or the WebGUI. The administrative user is authenticated by a username and password via the local console. The administrative user is also authenticated using a username and

password or public key via the remote CLI which is protected by SSH. The WebGUI authentication requires a username and password to be entered over the TLS/HTTPS protected connection. The username and password can be defined locally on the TOE or externally on an LDAP server. The only service that can be run prior to authentication is the display of a warning banner otherwise the TOE does not allow a user to perform any other actions prior to authentication.

8.5 Security Management

8.5.1 **FMT_MTD.1:**

GigaVUE provides three roles and of these, only the Admin role is relevant to the TOE. The TOE restricts the access to the SFR relevant management functions to the Admin role which corresponds to the PP Authorized Administrator definition.

8.5.2 **FMT_SMF.1:**

A user with the Admin role is capable of performing management functions on the TOE locally and remotely. Admins can perform management functions via the local console or remotely via the remote CLI or WebGUI.

The Admin also has the ability to update the TOE's software. Prior to installing the update on the TOE, updates are verified using a digital signature using rDSA with a key size of 2048 bits.

The Admin has the ability to configure the cryptographic functionality. This is accomplished by entering a command into the CLI which places the TOE into "Enhanced Security Mode" of operation. When this command is entered, the TOE limits the cryptographic algorithms to meet the requirements within this Common Criteria evaluation.

8.5.3 **FMT_SMR.2:**

All security management functions available to authorized users of the TOE are mediated by a role-based access control system.

Each user has the following security attributes associated with them:

- Username
- Password
- SSH public key (optional - used for remote CLI login only)
- role or roles, which grants privileges for user activities (including TSF management)

The username is contained within whatever authentication mechanism is configured for the TOE. This means that the TOE will store all user data if local authentication is used, and the LDAP enterprise server will store only the authentication data in the event of LDAP enterprise authentication being used. The roles are always stored locally, and when LDAP is used the LDAP validated username is used to query these attributes. The username and password are for authenticating to the TOE.

There are three roles which can be Admin, Operator, or Monitor, depending on the role assigned by an Authorized Administrator and each has different levels of authorization in terms of the functions that can be performed by them. All SFR relevant management activity is performed by the Admin role. The Admin user corresponds to the PP’s definition of Authorized Administrator. Only Admin users have the

ability to assign roles to users and more than one role may be assigned to a user. Admin users can administer the TOE both locally and remotely.

8.6 Protection of the TSF

8.6.1 **FPT_APW_EXT.1:**

The TOE stores usernames and passwords in a password file. All passwords stored on the TOE are stored in hashed form using the SHA-512 hash. The password file cannot be viewed by any user on the TOE regardless of the user's role.

8.6.2 **FPT_SKP_EXT.1:**

Public keys are stored in the configuration database which is integrity checked at boot time. The pre-shared, symmetric and private keys are stored in plaintext on the hard drive but cannot be accessed via the local console, remote CLI or the WebGUI by any user.

8.6.3 **FPT_STM.1:**

The TOE has an underlying hardware clock that is used for keeping time. A user with the Admin role has the ability to set the clock's time manually. In the evaluated configuration, the TOE can also use an NTP server for time. The TOE is configurable to use either NTP version 3 or 4 and has the ability to upload a key for server authentication. The TOE has several uses for time that include:

- Audit record timestamps
- Inactivity timeout for sessions
- Prevent numerous authentication in short period of time (4 second delay - hard coded)
- User lockout based on time (admin configurable)
- LDAP timeouts (CLI "ldap-server", configurable)
- Web session timeout (CLI "web session")

8.6.4 **FPT_TST_EXT.1:**

Power-on self-tests are executed automatically when the cryptographic module is loaded into memory. The FIPS cryptographic module verifies its own integrity using an HMAC-SHA1 digest computed at build time. If the integrity test passes, the power-up self-tests are then performed. If the power-up self-tests are successful, a flag is set to place the cryptographic module in FIPS mode. All of the cryptographic algorithms that are used by the TOE are tested. See the FIPS Security Policy for CMVP certificate #2128 for details of the FIPS power-on self-tests.

All binaries (e.g. executables, libraries), are located on a read-only partition and cannot be modified. In addition the TOE has a configuration database that is integrity checked at boot time.

In addition, the following functions are run and perform further power-on self-tests:
udiag is run under u-boot (microcode boot loader) which runs power-on self-tests of all the major components (memory, CPU, UART, Ethernet controllers...) on the motherboard, including the components that connect to the i2c buses. This includes all transceivers used by the dataplane.

The pci_diag component is a Linux component that runs when the kernel is loading that is responsible for testing and checking the components connected to the PCIe interfaces. It is also responsible for Line card type detection.

These tests are sufficient to validate the correct operation of the TSF because they verify that the cryptographic module is operating correctly, the configuration database does an integrity check, and that the underlying hardware does not have any anomalies that would cause the software to be executed in an unpredictable or inconsistent manner.

8.6.5 **FPT_TUD_EXT.1:**

TOE Admin users can query the current version of software on the local console, remote CLI interface and the WebGUI interface. On the local console and remote CLI interface a user can enter the "show version" command to show the current version. Within the WebGUI interface, the user can navigate to the "Systems" tab where the current version of software will be visible.

In order to update the TOE, the Admin can point the TOE directly to the Gigamon update server which is a Gigamon hosted site and enter a username and password to download the image. Alternatively, the Admin can download the image themselves and install it on a local server. In both instances, the connection to download the image is secured using TLS/HTTPS. When the TOE downloads the image from the local update server, the TOE will do this with TLS/HTTPS in the evaluated configuration.

The image that is downloaded is compressed and stored in a tar file and signed with a digital signature. Before the actual installation occurs, the signature is verified. If the signature is successfully verified, the update will be installed on an inactive partition and the Admin will have to enter a command in the local console or remote CLI in order to boot off of the inactive partition on which the updated was installed; making it the Active partition. If the update fails to be verified and the signature does not match, the Admin will receive an error and the Admin will select not to install the update.

8.7 TOE Access

8.7.1 **FTA_SSL_EXT.1:**

The TOE is designed to terminate a local session after a specific period of time. The default setting is 15 minutes and it is configurable by an Admin. Once a session has been terminated the local user must re-authenticate to start a new session.

8.7.2 **FTA_SSL.3:**

The TOE is able to terminate remote interactive sessions that are inactive in two different ways. In the event that the inactivity setting is met while users are logged into the CLI, the TOE tears down the SSH connection. This setting can be configured between 0-35791 minutes. The value of 0 means that this setting is disabled and there is no timeout configured. In the event that the inactivity setting is reached while a user is logged into the WebGUI, the user's session will end. This setting can be configured between 0-999999999 minutes. The value of 0 means that this setting is disabled and there is no timeout configured.

The Admin users authenticated to the local console or remote CLI may configure this setting for both the local console, remote CLI and WebGUI. However, Admin users authenticated to the WebGUI can only configure the timeout setting for the WebGUI.

8.7.3 **FTA_SSL.4:**

The Admin is able to terminate their own session by entering the "Exit" command when logged into the local console or remote CLI. The Admin can terminate their own session by clicking on the "logout" tab when logged into the WebGUI.

8.7.4 **FTA_TAB.1:**

There are three possible ways to login to the TOE: local console, remote CLI, and WebGUI. Each of these interfaces has a configurable login banner that is displayed prior to the user authenticating to the TOE.

The banner is configured using the “banner local” command for the local console, “banner remote” for both the remote CLI and WebGUI. The command “banner login” configures the banner for all login methods.

8.8 Trusted Path/Channels

8.8.1 **FTP_ITC.1:**

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a Syslog Server using SSHv2 to encrypt the audit data that traverses the channel. The TOE also connects with an LDAP server using TLS and Gigamon update server using TLS/HTTPS to secure its data. The TOE connects to the local update server using TLS/HTTPS.

In each of these instances, the TOE initiates communication using the protocols discussed in the SFRs. These protocols are used to protect the data traversing the channel from disclosure and/or modification.

8.8.2 **FTP_TRP.1:**

The Admin users are required to authenticate to the TOE in order to be able to perform any management functions. By initiating the trusted path via a WebGUI or remote CLI, Admin users are able to perform management activities remotely. The WebGUI path is protected by TLS/HTTPS (TLS v1.0) and the remote CLI is protected using SSHv2. These protocols are used to protect the data traversing the channel from disclosure and/or modification.