Gigamon LLC
GigaVUE version 7.2.29 Security Target

Version 3.0
August 26, 2011

Prepared for:

Gigamon LLC

598 Gibraltar Drive

Milpitas, CA 95035

Prepared by:

Booz Allen Hamilton

Common Criteria Testing Laboratory

900 Elkridge Landing Road, Suite 100

Linthicum, MD 21090-2950

Table of Contents

1 Security Target Introduction 9

1.1 ST Reference 9

1.1.1 ST Identification 9

1.1.2 Document Organization 9

1.1.3 Terminology 9

1.1.4 Acronyms 11

1.1.5 References 12

1.1.6 CC Concepts 13

1.2 TOE Reference 13

1.3 TOE Overview 13

1.4 TOE Type 16

2 TOE Description 17

2.1 Evaluated Components of the TOE 17

2.2 Components and Applications in the Operational Environment 17

2.3 Excluded from the TOE 18

2.3.1 Not Installed 18

2.3.2 Installed but Requires a Separate License 18

2.3.3 Installed But Not Part of the TSF 18

2.4 Physical Boundary 19

2.4.1 Hardware 19

2.4.2 Software 20

2.5 Logical Boundary 20

2.5.1 Security Audit 20

2.5.2 Cryptographic Support 21

2.5.3 User Data Protection 21

2.5.4 Identification and Authentication 21

2.5.5 Security Management 21

2.5.6 Protection of the TSF 22

2.5.7 Resource Utilization 22

2.5.8 TOE Access ... 22
2.5.9 Trusted Path/Channels ... 22
3 Conformance Claims ... 23
3.1 CC Version ... 23
3.2 CC Part 2 Conformance Claims ... 23
3.3 CC Part 3 Conformance Claims ... 23
3.4 PP Claims ... 23
3.5 Package Claims ... 23
3.6 Package Name Conformant or Package Name Augmented ... 23
3.7 Conformance Claim Rationale ... 23
4 Security Problem Definition ... 24
4.1 Threats ... 24
4.2 TOE Threats ... 24
4.3 Organizational Security Policies ... 24
4.4 Assumptions ... 24
4.4.1 Personnel Assumptions ... 24
4.4.2 Physical Assumptions ... 25
5 Security Objectives ... 26
5.1 TOE Security Objectives ... 26
5.2 Security Objectives for the operational environment of the TOE ... 26
6 Extended Security Functional and Assurance Requirements ... 28
6.1 Extended Security Functional Requirements for the TOE ... 28
6.2 Extended Security Assurance Requirements ... 28
7 Security Functional Requirements ... 29
7.1 Security Functional Requirements for the TOE ... 29
7.1.1 Class FAU: Security Audit ... 30
7.1.1.1 FAU_ARP.1 Security alarms ... 30
7.1.1.2 FAU_GEN.1 Audit data generation ... 30
7.1.1.3 FAU_GEN.2 User identity association ... 32
7.1.1.4 FAU_SAA.1 Potential violation analysis ... 32
7.1.1.5 FAU_SAR.1 Audit review ... 32
7.1.1.6 FAU_SAR.2 Restricted audit review ... 33

7.1.1.7 FAU_SAR.3 Selectable Audit Review 33
7.1.1.8 FAU_STG.2 Guarantees of audit data availability..33
7.1.2 Class FCS: Cryptographic Support.. 33
7.1.2.1 FCS_CKM.1 Cryptographic key generation 33
7.1.2.2 FCS_CKM.4 Cryptographic key destruction 34
7.1.2.3 FCS_COP.1 Cryptographic operation...34
7.1.3 Class FDP: User Data Protection... 34
7.1.3.1 FDP_IFC.1 Subset information flow control 34
7.1.3.2 FDP_IFF.1 Simple security attributes...34
7.1.4 Class FIA: Identification and Authentication 36
7.1.4.1 FIA_AFL.1(1) Authentication failure handling 36
7.1.4.2 FIA_AFL.1(2) Authentication failure handling 36
7.1.4.3 FIA_ATD.1 User attribute definition..36
7.1.4.4 FIA_SOS.1 Specification of Secrets 37
7.1.4.5 FIA_UAU.2 User authentication before any action 37
7.1.4.6 FIA_UAU.5 Multiple authentication mechanisms..37
7.1.4.7 FIA_UID.2 User identification before any action...37
7.1.4.8 FIA_USB.1 User-subject binding 37
7.1.5 Class FMT: Security Management 38
7.1.5.1 FMT_MOF.1 Management of security functions behavior...38
7.1.5.2 FMT_MSA.1 Management of security attributes 44
7.1.5.3 FMT_MSA.3 Static attribute initialization 45
7.1.5.4 FMT_MTD.1 Management of TSF data 45
7.1.5.5 FMT_REV.1(1) Revocation..45
7.1.5.6 FMT_REV.1(2) Revocation..45
7.1.5.7 FMT_SMF.1 Specification of Management Functions...46
7.1.5.8 FMT_SMR.1 Security roles 46
7.1.6 Class FPT: Protection of the TOE Security Functions.. 46
7.1.6.1 FPT_STM.1 Reliable time stamps 46
7.1.7 Class FRU: Resource Utilization.. 46
7.1.7.1 FRU_FLT.1 Fault Tolerance...46
7.1.8 Class FTA: TOE Access.. 46

7.1.8.1 FTA_SSL.3(1) TSF-initiated termination 46
7.1.8.2 FTA_SSL.3(2) TSF-initiated termination 47
7.1.8.3 FTA_SSL.4 User-initiated termination 47
7.1.8.4 FTA_TAB.1 Default TOE access banners 47
7.1.9 Class FTP: Trusted Paths/Channels 47
7.1.9.1 FTP_TRP.1 Trusted Paths....47
7.2 Operations Defined....47
8 Security Assurance Requirements....49
8.1 Security Architecture....49
8.1.1 Security Architecture Description (ADV_ARC.1) 49
8.1.2 Security-enforcing functional specification (ADV_FSP.2) 49
8.1.3 Basic Design (ADV_TDS.1) 50
8.2 Guidance Documents 50
8.2.1 Operational user guidance (AGD_OPE.1).... 50
8.2.2 Preparative Procedures (AGD_PRE.1).... 51
8.3 Lifecycle Support 51
8.3.1 Use of a CM system (ALC_CMC.2) 51
8.3.2 Parts of the TOE CM coverage (ALC_CMS.2).... 51
8.3.3 Delivery Procedures (ALC_DEL.1) 52
8.3.4 Flaw reporting procedures (ALC_FLR.1) 52
8.4 Security Target Evaluation....52
8.4.1 Conformance Claims (ASE_CCL.1) 52
8.4.2 Extended Components Definition (ASE_ECD.1).... 53
8.4.3 ST Introduction (ASE_INT.1) 53
8.4.4 Security objectives (ASE_OBJ.2).... 54
8.4.5 Derived security requirements (ASE_REQ.2) 54
8.4.6 Security Problem Definition (ASE_SPD.1).... 55
8.4.7 TOE Summary Specification (ASE_TSS.1) 55
8.5 Tests 55
8.5.1 Evidence of Coverage (ATE_COV.1) 55
8.5.2 Functional Testing (ATE_FUN.1).... 55
8.5.3 Independent Testing - Sample (ATE_IND.2).... 56

8.6 Vulnerability Assessment 56
8.6.1 Vulnerability Analysis (AVA_VAN.2) 56
9 TOE Summary Specification 57
9.1 TOE Security Functions 57
9.1.1 Security Audit 57
9.1.1.1 Syslog 57
9.1.1.2 Alerting 57
9.1.1.3 Log-level 58
9.1.2 Cryptographic Support 58
9.1.3 User Data Protection 58
9.1.3.1 Gigamon Forwarding Policy 59
9.1.3.2 Forwarding Rules 60
9.1.3.2.1 Receiving Data 60
9.1.3.2.2 Filtering and Forwarding Data 61
9.1.3.2.3 Moving the Data 62
9.1.4 Identification and Authentication 63
9.1.4.1 User attributes 63
9.1.4.2 Authentication Methods 63
9.1.4.3 Failed Authentication Attempts 64
9.1.4.4 Password Policy 64
9.1.5 Security Management 64
9.1.5.1 Roles 65
9.1.5.2 Lock-level 65
9.1.5.3 Connection Locking 65
9.1.5.4 User-group 65
9.1.6 Protection of the TSF 66
9.1.7 Resource Utilization 66
9.1.8 TOE Access 66
9.1.9 Trusted Path/Channels 67
9.1.10 Security Architecture 67
9.1.10.1 Separation of Roles 67
9.1.10.2 Domain Separation 67

9.1.10.3 Secure Operation 67
9.2 TOE Summary Specification Rationale 68
9.2.1 Security Audit 69
9.2.2 Cryptographic Support 69
9.2.3 User Data Protection 69
9.2.4 Identification and Authentication 69
9.2.5 Security Management 70
9.2.6 Protection of the TSF 70
9.2.7 Resource Utilization 70
9.2.8 TOE Access 70
9.2.9 Trusted Path/Channels 71
10 Security Problem Definition Rationale 72
10.1 Security Objectives Rationale 72
10.2 Operational Security Policy Rationale 75
10.3 Security Functional Requirements Rationale 75
10.4 EAL2 Justification 80
10.5 Requirement Dependency Rationale 80
10.6 Assurance Measures 81

List of Figures

Figure 1 – TOE Boundary 14
Figure 2 – Multi-TOE Deployments 15

List of Tables

Table 1-1: Customer Specific Terminology 11
Table 1-2: CC Specific Terminology 11
Table 1-3: Acronym Definitions 12
Table 2-1: Evaluated Components of the TOE 17

Table 2-2: Evaluated Components of the Operational Environment 18
Table 7-1: Security Functional Requirements for the TOE 29
Table 7-2: Auditable Events 31
Table 7-3: Management of TSF Data 43
Table 7-4: Connection Locking Policy 44
Table 9-1: Gigamon Forwarding Policy Attributes 60
Table 9-2: Security Functional Components for the TOE 69
Table 10-1: Assumption to Objective Mapping 72
Table 10-2: Threat to Objective Mapping 75
Table 10-3: Security Functional Requirements Rationale 80
Table 10-4: Requirement Dependencies 81
Table 10-5: Assurance Requirements Evidence 84

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. This ST targets Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1.

1.1.1 ST Identification

ST Title:	Gigamon LLC GigaVUE version 7.2.29 Security Target
ST Version:	3.0
ST Publication Date:	August 26, 2011
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this ST provides identifying information for the TOE. It includes an ST Introduction, ST Reference, ST Identification, TOE Reference, TOE Overview, and TOE Type.

Chapter 2 describes the TOE Description, which includes the physical and logical boundaries, and describes the components and/or applications that are excluded from the evaluated configuration.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the Security Problem Definition as it relates to threats, Operational Security Policies, and Assumptions met by the TOE.

Chapter 5 identifies the Security Objectives of the TOE and of the Operational Environment.

Chapter 6 describes the Extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 7 describes the Security Functional Requirements.

Chapter 8 describes the Security Assurance Requirements.

Chapter 9 is the TOE Summary Specification (TSS), a description of the functions provided by the TOE to satisfy the SFRs and SARs.

Chapter 10 is the Security Problem Definition Rationale and provides a rationale or pointers to a rationale, for security objectives, assumptions, threats, requirements, dependencies, and PP claims for the chosen EAL, any deviations from CC Part 2 concerning SFR dependencies, and a mapping of threats to assumptions, objectives, and SFRs. It also identifies the items used to satisfy the Security Assurance Requirements for the evaluation.

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.

Terminology	**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.
Collector	The ‘Everything Else Bucket’. A location where all packets can be sent that do not match the criteria specified in a map rule and are not included in the map rules of a specific flow map.
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.
Lock-Level	A settable value that provides the administrator the ability to restrict the management functions used and the data accessible by users. Can be set to “none,” “medium,” or “high.”
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.
Map Rule	Map rules direct traffic into the TOE by including and excluding data from a network port to a tool port.
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.
Pass-All	Command that can be used to send ‘all data’ from a network or tool port to another tool port, regardless of the filters or flow maps assigned to those ports.
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.
User-Group	A user attribute that provides a method for an administrator to assign port permissions to users.
Virtual Drop Port	Where packets are sent to be discarded. Virtual drop ports are part of a flow map.

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized user	A user who, in accordance with proper authentication/authorization, is allowed to perform an operation.
External IT entity	Any IT product or system, trusted or not, outside of the TOE that interacts with the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Table 1-2: 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
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CLI	Command-line Interface
CPU	Central Processing Unit
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol

IT	Information Technology
NIAP	National Information Assurance Partnership
NP	Network Port
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RBAC	Role Based Access Control
RGN	Randomly Generated Number
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSL	Secure Sockets Layer
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TP	Tool Port
TSF	TOE Security Function
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator

Table 1-3: Acronym Definitions

1.1.5 References

[1] GigaVUE 7.2 User Guide

[2] GigaVUE 7.2 CLI Summary

1.1.6 CC Concepts

The following are CC concepts as used in this document. A Subject is any user of the TOE (account, user, administrative user). An Object (i.e., resource or entity) can be a dataset, volume, command issued by a user, etc. An Operation is any action on a resource (e.g. read, write, create, fetch, update, control, alter, or scratch). A Security Attribute is information such as username, groups, profiles, facilities, passwords, etc. that is kept in the security file for the user. An External Entity is anything outside of the TOE that affects the TOE.

1.2 TOE Reference

GigaVUE version 7.2.29

1.3 TOE Overview

GigaVUE 7.2.29 (herein referred to as GigaVUE or the TOE) receives out-of-band copied network data from external sources (tap or SPAN port) and forwards that copied network data to one or many 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:

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

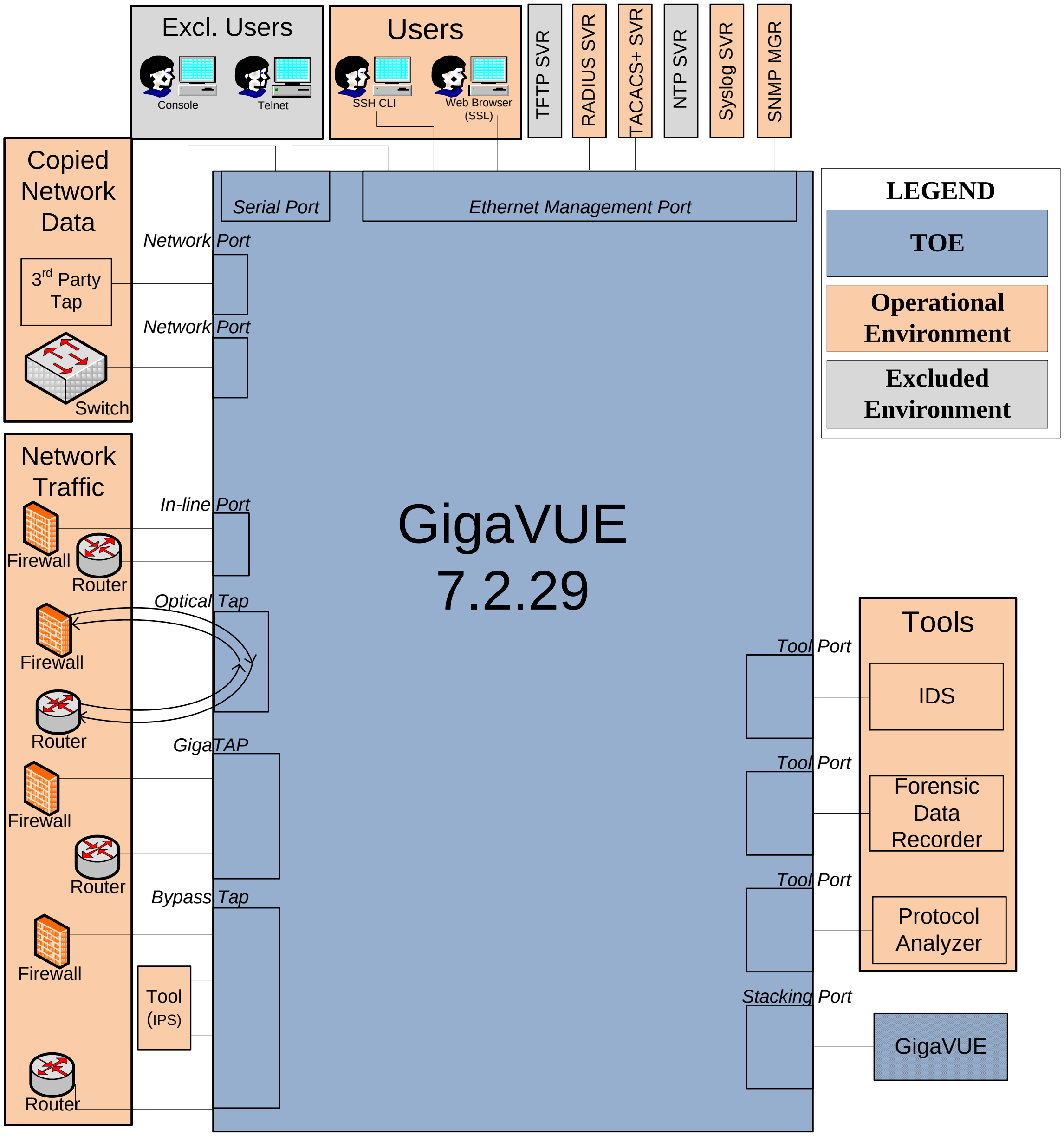

Figure 1 – TOE Boundary

As illustrated in Figure 1, the TOE is a single hardware device that has management ports, network (or ingress) ports, and tool (or egress) ports. The TOE has two 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 Syslog, and SNMP Manager.

The TOE receives data from many sources, or networks. It can receive data from a 3rd party tap or SPAN port. The TOE 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. The TOE 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.

The TOE forwards the data received via a network port to a tool port based on the flow maps, filters, connections, pass-alls, collectors, and GigaStreams that the authorized users have configured in the 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.

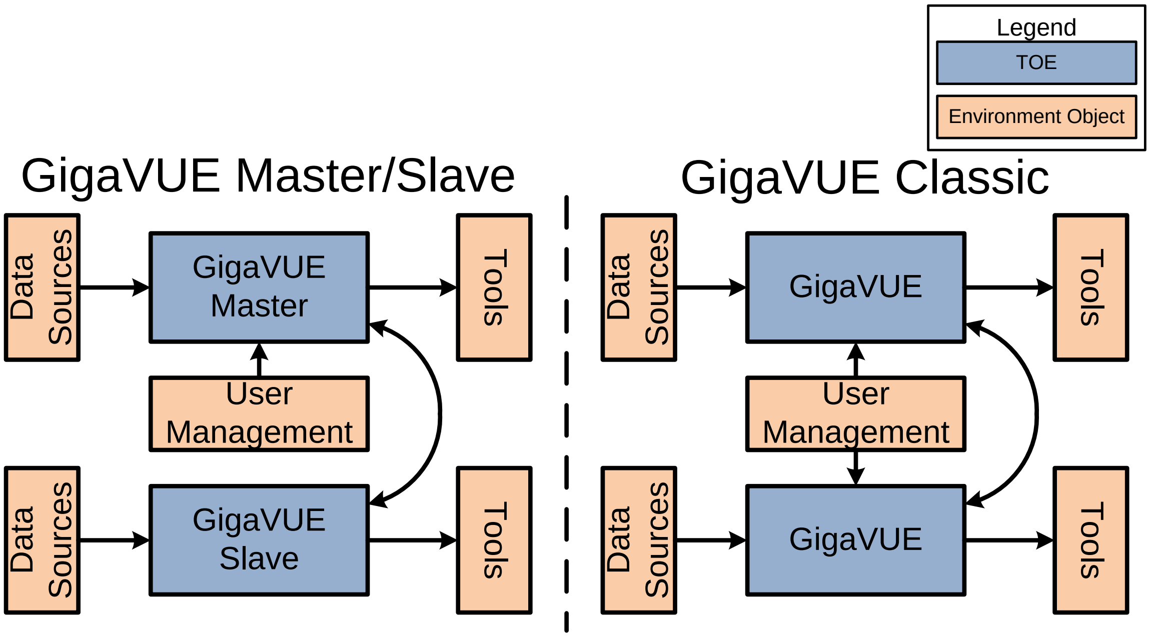

Figure 2 – Multi-TOE Deployments

As illustrated in Figures 1 and 2, the TOE can be deployed in a variety of ways. The TOE 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 TOE.

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

1.4 TOE Type

The TOE type for GigaVUE is Security Management. Security Management is defined by CCEVS as “a set of pervasive security mechanisms which support the security services by direct and supervisory administration, automated processes, and by the activities of all information users.”

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 212	GigaVUE chassis with 10 ports standard with optional 4 additional ports. There are (2) 10 Gb ports and (8) 1 Gb ports. There are 4 additional (1) Gb optional ports that can be inserted or can be replaced with an electrical tap or an in-line bypass tap.
GigaVUE 420	GigaVUE chassis with 4 ports standard and an optional 20 additional ports. There are (4) optional 10 Gb ports and (16) optional 1 Gb ports. The additional (4) 10 Gb ports can house an optical tap, or a stacking module used for stacking multiple TOE's together. The additional (20) 1G ports are inserted via modules. The GigaVUE 420 chassis is expandable to 4 internal 1G modules. Optional modules can include 2 x 1G optical or electrical full duplex taps, 1 x electrical Bypass Tap or a 4 Port expansion module. All ports can be configured as either a Network or Tool ports with no restrictions or licenses. Hot swappable redundant power supplies and fans are also included.
GigaVUE 2404	GigaVUE chassis with 28 ports. This model has (24) 10 Gb ports and (4) 1 Gb ports. This model has 3 blades which can be swapped out: 2 blades, each with 8 expansion ports and 1 system blade with 4 x 10/100/1000 ports & 8 x 10G ports. Different/optional blades can also be installed with 4 x Full duplex Taps and can be either 1G or 10G optical. All GigaVUE ports are available for use as either a Network or Tool port with no restrictions or licenses. All 10 Gb ports can also be used as 1 Gb ports with the corresponding SFP's; both copper and fiber are supported. Hot swappable redundant power supplies and fans are also included.

Table 2-1: 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
RADIUS Server	This component allows for RADIUS authentication instead of internal ACL GigaVUE authentication. The TOE communicates to this component to verify users and user attributes including user-groups. RADIUS authentication is appropriate for TOEs deployed within an enterprise environment.
SNMP Manager	This component allows the TOE to communicate with it by receiving SNMP traps from the SNMP Agent residing in the TOE based on specified events. SNMP traps are sent out based upon security violations or system faults detected by the TOE. The SNMP Manager can poll the TOE and request information by communicated to the SNMP Server inside the TOE. GigaVUE supports SNMP v1 and v2c for sending traps to the configured SNMP Manager. GigaVUE also supports SNMP v1, v2c, and v3 communication when requests are received from an SNMP Manager. However, in the evaluated configuration the TOE will be configured to only support SNMP v2c for sending traps and only support

	receiving requests in SNMP v3 format from the SNMP Manager.
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.
TACACS+ Server	This component allows for TACACS+ authentication instead of normal GigaVUE authentication. The TOE communicates to this component to verify users and user attributes and user-groups. TACACS+ authentication is appropriate for TOEs deployed within an enterprise environment, but can be used in any environment where user authentication is a concern.
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.

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with GigaVUE 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

- GigaSMART – This is an optional module that provides packet modification functionality to data flowing through GigaVUE. GigaSMART is not part of the evaluated configuration because it provides separate enhanced functionality and is a separately purchased product.

2.3.2 Installed but Requires a Separate License

No components are installed that 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.

- Console Management Port – Is only used for initial set up and configuration of the TOE. This port is not part of the evaluated configuration because it does not allow for remote management and is not used in standard practice.

- NTP – NTP is used to synchronize the TOE's system time with external NTP servers. NTP is not part of the evaluated configuration because it synchronizes time in an insecure manner.

- Telnet – Telnet is used to remotely connect to the TOE via the Ethernet management port. Telnet is not part of the evaluated configuration because it is an insecure communication protocol.

- TFTP Server – TFTP is used to transfer files to the TOE during initial configuration. The TOE access banner and main configuration file can be retrieved from a TFTP server during set up and configuration. It is not part of the evaluated configuration because it is an insecure communication protocol, provides no authentication, and is only to be used by administrators of the TOE during initial configuration.

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 or 10G ports.

The model specific hardware is as follows:

GigaVUE-212

- Redundant Power Supplies & Fans
- Serial Console port (excluded)
- Management Ethernet port
- (2) 10 Gbps ports (optical)
- (8) 1 Gbps ports (electrical or optical)
- Expansion slot: 1
    - (4) 1 Gbps ports (electrical or optical)
    - Bypass TAP (GigaTAP-TX-D)
    - GigaTAP-TX-D
- O/S: ECOS v2.0

GigaVUE-420

- Redundant Power Supplies & Fans
- Serial Console port (excluded)
- Management Ethernet port
- (4) 1 Gb ports (electrical or optical)
- Expansion slots: 8
    - (4) 1 Gbps expansion slots
        - 4 GigaPORT (electrical or optical)
        - GigaTAP-TX or GigaTAP-SX/LX/ZX
        - Bypass Tap (GigaTAP-BPC)
    - (4) 10 Gbps expansion slots
        - 4 ports (CX4 or optical)

        - 10G-GigaTAP (requires (2) 10Gb ports)
- O/S: ECOS v2.0

GigaVUE-2404

- Redundant Power Supplies & Fans
- Serial Console port (excluded)
- Management Ethernet port
- (8) 10 Gb ports (optical, with SFP+), each downgradable to 1Gb port (optical, replace SFP+ with SFP)
    - SFP dependant
- (4) 10/100/1000 ports (electrical or optical)
    - SFP dependant
- Expansion slots: 2
    - (8) 10 Gbps ports (optical, with SFP+), each port downgradable to a 1 Gb port (optical, replace SFP+ with SFP)
    - (4) Full Duplex GigaTAP (optical only)
- O/S: ECOS v2.0

2.4.2 Software

TOE software is GigaVUE version 7.2.29.

2.5 Logical Boundary

The logical boundary of the TOE is described in the terms of the security functionalities that the TOE provides to the systems that utilize this product for copied network data aggregation, mapping and filtering.

The logical boundary of the TOE is broken down into the following security classes: Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access, and Trusted Path/Channels. Listed below are the security functions with a listing of the capabilities associated with them:

2.5.1 Security Audit

The TOE contains mechanisms to generate audit data based upon successful and unsuccessful management actions initiated by all authorized users of the TOE. Each audit record contains identifying information of the subject performing the action. The TOE explicitly allows all roles to read audit data within the TOE. In addition, the TOE provides mechanisms to filter viewed audit data based upon start/end date. The TOE contains mechanisms to determine if a potential security violation has occurred by monitoring audit events that are based upon the changing of the TOE's configuration file, updating the firmware, changing modules, a change in port link status, failed authentication attempts, and the existence of a TOE reset. All of these violations are a threshold of a single occurrence as well as being selectable by Super users. In the event of any of these changing or occurring, the TOE sends an SNMP trap. The TOE protects audit records from unauthorized deletion and prevents changes to the stored records. The oldest audit records are overwritten with newer records in the event of data storage exhaustion. Syslog servers can be configured to backup audit logs for more permanent storage.

2.5.2 Cryptographic Support

The TOE provides mechanisms to generate and destroy cryptographic keys to set up the SSH connection. The evaluated configuration requires the generation and use of 2048 bit RSA keys only. Supers users must upload 3rd party 2048 bit RSA key pairs signed by a key authority to use for communication through the GUI (HTTPS). When keys are uploaded or generated the old keys are overwritten. The evaluated configuration of the TOE then uses AES with SHA-1 in CBC mode with 256 bit keys (HTTPS) or 128 bit keys (SSH) to encrypt the data within TOE trusted paths and channels. By default, the GUI interface utilizes port 443 (HTTPS) and the SSH interface utilizes port 22 (SSH) which are the ports to be utilized within the evaluated configuration.

2.5.3 User Data Protection

The TOE's core functionality is to forward, flow map and/or filter copied network data to be delivered to specific tools. This is a one-way data flow. The TOE contains a forwarding policy to determine which copied network data is sent to which tools and denies any return path back to the production network from any user or connected tool. The policy is used to control various subjects (TOE interfaces from which information is received and TOE interfaces to which information is forwarded) and objects (copied network data). The TOE accounts for specific security attributes, such as port identifiers, source identity, destination identity, and protocols used. A forward occurs if the network and tool port identifiers are within the rule set, the copied network data security attributes match attributes within a forward policy rule, and the rule specifies that the forwarding is permitted. There are no additional rules past the defined policy or exceptions to the defined flow policy, either on an explicit allow or explicit deny basis.

2.5.4 Identification and Authentication

The TOE or its configured enterprise authentication server maintains distinct user accounts which contain the following attributes: username, password, role, port ownership, and user group association. All user accounts must contain specific standards for password complexity, which requires passwords to be 8 to 30 characters and contain at least one number, one upper case letter, one lower case letter, and one special character (ASCII 0x21-0x2f inclusive). All TOE users must be identified and authenticated before performing any TSF-relevant actions. Upon authentication, users are granted sessions within the TOE to associate the user with their role and attributes. User sessions are forcibly removed if the corresponding user account is deleted within the TOE. In addition, the TOE reacts to multiple failed authentications based upon UI type used by locking out all login attempts for that interface for 20 seconds. The TOE supports several methods of authentication in addition to native username/password authentication: RADIUS, and TACACS+ integration are supported. When using enterprise authentication, all user data is stored on the enterprise authentication server, and the necessary user data is queried by the TOE to perform user authentication and to create user sessions.

2.5.5 Security Management

The TOE maintains three distinct roles for user accounts: Super, Normal, and Audit. These roles determine the scope of management functions available to the user. The Super role assumes all TOE management functionality. The Normal role can perform read operations and can modify the TOE's forwarding policy. The Audit role can perform read operations only.

Lock-Levels – Specific lock-levels (none, medium, high) exist to further describe what actions are available to Normal users. The "none" lock-level allows all network and tool ports to be assigned by any Super or Normal user. The "medium" lock-level requires tool ports to be owned by the Normal before allowing an action. The "high" lock-level requires both network and tool ports to be owned by Normal user before allowing an action. Note that the lock-level only affects the Normal user, and *does not* change the permissions of Audit or Super users. The lock-level is globally set for the entire TOE. The TOE maintains restrictive default values for security attributes within the TOE and permits Super and Normal users to modify the default values. Super users can revoke any user account within the system and can also change the lock-level. Deleting user accounts and changing the lock-level are reflected immediately upon making access control decisions to the TOE.

2.5.6 Protection of the TSF

The TOE maintains accurate system time to provide accurate timestamps on audit and system records.

2.5.7 Resource Utilization

The TOE provides fault tolerance by ensuring that the flow of network traffic is unaffected when used in a tap configuration in the event of TOE or CPU failure. However, copied network data that has been configured to flow from a network port to a tool port will cease in the event of a TOE or CPU failure.

2.5.8 TOE Access

All users are shown a configurable banner before being allowed to authenticate to the TOE. Only Super users are allowed to configure the banner. The TOE revokes user sessions after a specific user-definable amount of time has passed without an action being performed within an active session. This number varies based upon whether the GUI or CLI was used to access the TOE. The TOE also maintains functionality for all users to terminate their own sessions by logging out.

2.5.9 Trusted Path/Channels

Connections to/from the TOE are protected using the standards defined within the Cryptographic Support section. Trusted paths are used to secure all user sessions to the GUI or CLI. All connections are protected from modification and disclosure by using these cryptographic methods.

3 Conformance Claims

3.1 CC Version

This ST is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2009-07-004, Version 3.1 Revision 3 July 2009.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 conformant for EAL2 to include all applicable NIAP and International interpretations through 6 September 2011.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant plus flaw remediation for EAL2 to include all applicable NIAP and International interpretations through 6 September 2011.

3.4 PP Claims

This ST does not claim conformance to any Protection Profile.

3.5 Package Claims

This TOE has a package claim of EAL2.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are conformant to EAL2 package claims augmented with ALC_FLR.1.

3.7 Conformance Claim Rationale

There is no Conformance Claim rationale for this ST.

4 Security Problem Definition

4.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

4.2 TOE Threats

T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause the records or information to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

T.NETWORK_FLOW A malicious user may attempt to subvert the TOE or defeat the operation of its security mechanisms to cause a disruption in the flow of data on the production network.

T.MASK Users, whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.

T.STEALTH A malicious user or process could perform suspicious activities against objects in the Operational Environment without an Operational Environment user becoming aware of this behavior because the TOE's forwarding policy did not forward the information to the necessary tool per its configuration.

4.3 Organizational Security Policies

The TOE addresses the organizational security policy described below.

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 system.

4.4 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

4.4.1 Personnel Assumptions

A.ADMIN One or more authorized administrators are assigned to install, configure and manage the TOE and the security of the information it contains.

A.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.

A.PATCHES System Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.

A.NO_GENERAL_PURPOSE The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, database servers, or user applications) available on the TOE.

4.4.2 Physical Assumptions

A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

5 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.

5.1 TOE Security Objectives

The following are the TOE security objectives:

O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.

O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded.

O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.

O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.

O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.

O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.

O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.

O.MAP The TOE will provide mechanisms to set and control the forwarding of information to a tool based upon its configuration.

O.NETWORK_FLOW_PROTECTION The TOE will preserve the information flow of the production network traffic through the TOE in the presence of adversarial activity when a component of the TOE fails.

O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.

O.SYSTIME The TOE will provide reliable system time.

5.2 Security Objectives for the operational environment of the TOE

The TOE's operating environment must satisfy the following objectives.

OE.ADMIN One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.

OE.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

OE.NO_GENERAL_PURPOSE The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.

OE.NOEVIL All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization’s guidance documentation.

6 Extended Security Functional and Assurance Requirements

6.1 Extended Security Functional Requirements for the TOE

There are no extended Security Functional Requirements in this ST.

6.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

7 Security Functional Requirements

7.1 Security Functional Requirements for the TOE

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

Security Function	Security Functional Components
Security Audit (FAU)	FAU_ARP.1 Security alarms
	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAA.1 Potential violation analysis
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.2 Guarantees of audit data availability
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1 Subset information control
	FDP_IFF.1 Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1(1) Authentication failure handling
	FIA_AFL.1(2) Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_SOS.1 Verification of secrets
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_REV.1(1) Revocation
	FMT_REV.1(2) Revocation
	FMT_SMF.1 Specification of Management Functions
	FMT_MSA.1 Management of security attributes
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamp
Resource Utilization (FRU)	FRU_FLT.1 Fault tolerance
TOE Access (FTA)	FTA_SSL.3(1) TSF-initiated termination
	FTA_SSL.3(2) TSF-initiated termination
	FTA_SSL.4 User initiated termination
	FTA_TAB.1 Default TOE access banners
Trusted Path/Channels(FTP)	FTP_TRP.1 Trusted path

Table 7-1: Security Functional Requirements for the TOE

7.1.1 Class FAU: Security Audit

7.1.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall take [***the following action based upon the configuration by an authorized user***

1. Sending an SNMP trap] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

7.1.1.2 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [***auditable events in Table 7-2 below***].

Component	**Event**
FAU_ARP.1	Actions taken due to potential security violations
FAU_GEN.1	None
FAU_GEN.2	None
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms; Automated responses performed by the tool
FAU_SAR.1	Searching audit data
FAU_SAR.2	Searching audit data
FAU_SAR.3	Searching audit data
FAU_STG.2	Actions taken due to exceeding the audit data threshold
FCS_CKM.1	None
FCS_CKM.4	None
FCS_COP.1	None
FDP_IFC.1	None
FDP_IFF.1	None
FIA_AFL.1(1)	The reaching of the threshold for the unsuccessful authentication attempts and the action taken
FIA_AFL.1(2)	The reaching of the threshold for the unsuccessful authentication attempts and the

	action taken
FIA_ATD.1	None
FIA_SOS.1	Rejection by the TSF of any tested secret
FIA_UAU.2	Successful and unsuccessful use of authentication mechanisms
FIA_UAU.5	Successful and unsuccessful use of authentication mechanisms
FIA_UID.2	Successful and unsuccessful use of authentication mechanisms
FIA_USB.1	Success and failure of binding of user security attributes to a subject
FMT_MOF.1	All modifications in the behavior of the functions in the TSF (See Table 7-3)
FMT_MSA.1	All manipulation of the security attributes (See Table 7-3)
FMT_MSA.3	None
FMT_MTD.1	All modifications of the values of TSF data by the administrator (See Table 7-3)
FMT_REV.1(1)	All attempts to revoke security attributes (See Table 7-3)
FMT_REV.1(2)	All attempts to revoke security attributes (See Table 7-3)
FMT_SMF.1	All use of the management functions (See Table 7-3)
FMT_SMR.1	Modifications of users assigned to a role
FPT_STM.1	Changes to the time
FRU_FLT.1	None
FTA_SSL.3(1)	Termination of an interactive session by the session locking mechanism
FTA_SSL.3(2)	Termination of an interactive session by the session locking mechanism
FTA_SSL.4	Termination of an interactive session by the user
FTA_TAB.1	None
FTP_TRP.1	All attempted uses of the trusted path functions, Identification of the user associated with all trusted path invocations, if available

Table 7-2: Auditable Events

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, [***none***].

Application Note: *The text command processed by the TOE for each user event is recorded within each audit record. Additionally, an authorized user can determine the role associated with the user at the time of the command being processed. Thus, an authorized user will be able to* *determine the outcome (success or failure) of the event based upon the subject identity and the text command processed. Although the outcome is not specifically stated in the audit record, the other information within the audit record can be utilized to determine the success or failure of all user actions.*

Dependencies: FPT_STM.1 Reliable time stamps

7.1.1.3 FAU_GEN.2 User identity association

Hierarchical to: No other components.

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.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

7.1.1.4 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [***a single event, when configured by an authorized user, for the following events:***

1. Change to the TOE's configuration file via the config save command

2. Change to the TOE's firmware

3. Change to the TOE's modules

4. Change to a port’s link status for Network, Tool, and Stacking ports

5. Resetting the TOE

6. Failed authentication attempt] known to indicate a potential security violation;

b) [***none***].

Dependencies: FAU_GEN.1 Audit data generation

7.1.1.5 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [***all users***] with the capability to read [***all local audit data generated by FAU_GEN.1***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

7.1.1.6 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

7.1.1.7 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to apply [***filtering***] of audit data based on [***start date and/or end date***].

Dependencies: FAU_SAR.1 Audit review

7.1.1.8 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1 Protected audit trail storage

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [***all but the audit records stored in the oldest audit log***] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion].

Application Note: *The TOE provides 8 audit log files of a maximum of 1 MB each, and the oldest log file is overwritten upon all 8 log files filling up. See Section 9.1.1.1 for more discussion on this.*

Dependencies: FAU_GEN.1 Audit data generation

7.1.2 Class FCS: Cryptographic Support

7.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA***] and specified cryptographic key sizes [***2048 bit***] that meet the following: [***RFC 2313***].

Application Note: *This key generation scheme is used to generate keys for both SSH and SSL. Although both keys are using the same scheme, they generate separate keys.*

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

7.1.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***overwrite***] that meets the following: [***no standard***].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

7.1.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***AES with SHA-1 in CBC mode***] and cryptographic key sizes [***256 bit (HTTPS) or 128 bit (SSH)***] that meet the following: [***RFC 3268***].

Application Note:This encryption scheme is used for both SSH and SSL.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

7.1.3 Class FDP: User Data Protection

7.1.3.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [***Gigamon Forwarding Policy SFP***] on

[***copied network data: attributes contained with the information copied from the production network;***

network subject: TOE interface(s) from which information is received;

tool subject: TOE interface(s) to which information is forwarded;

information: copied network data;

operations: forward information].

Dependencies: FDP_IFF.1 Simple security attributes

7.1.3.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the [***Gigamon Forwarding Policy SFP***] based on the following types of subject and information security attributes: [

a) Network subject security attributes: Set of port identifiers

b) Tool subject security attributes: Set of port identifiers

c) Copied network data security attributes: set of security attributes defined within copied network data:

identity of source subject;

identity of destination subject;

transport layer protocol;

network layer protocol;

Ethertype;

VLAN;

time-to-live/hop limit;

DSCP/IPv4 fragments;

Type of Service (TOS);

16-byte pattern matches;

source service identifier (e.g., TCP or UDP destination port number);

destination service identifier (e.g., TCP or UDP destination port number); and

Flags for Connection-oriented protocols:

a. SYN;

b. ACK;

c. RST;

d. FIN;

e. PSH;

f. URG;

g. Congestion Window Reduced; and

h. ECN echo].

FDP_IFF.1.2 Refinement: The TSF shall permit an information flow between a controlled ~~subject~~ ***network subject*** and controlled ~~information~~ ***tool subject*** via a controlled operation if the following rules hold: [

the identity (port identifier) of the network subject is within the forward policy rule set;

	the identity (port identifier) of the tool subject is within the forward policy rule set;
	the copied network data security attributes match the attributes in a forward policy rule (contained in the forward policy rule set defined by an authorized user) according to the following algorithm [Gigamon Forwarding Policy SFP]; and
	the selected forward policy rule specifies that information flow (forwarding) is to be permitted].
FDP_IFF.1.3	The TSF shall enforce the [***no additional information flow (forwarding) rules***].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [***none***].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [***none***].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

7.1.4 Class FIA: Identification and Authentication

7.1.4.1 FIA_AFL.1(1) Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1(1)	The TSF shall detect when [***5***] unsuccessful authentication attempts occur related to [***a single user name authentication request via the GUI***].
FIA_AFL.1.2(1)	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [***lock the GUI from accepting all authentication requests for 20 seconds***].
Dependencies:	FIA_UAU.1 Timing of authentication

7.1.4.2 FIA_AFL.1(2) Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1(2)	The TSF shall detect when [***6***] unsuccessful authentication attempts occur related to [***a single user name authentication request via the CLI***].
FIA_AFL.1.2(2)	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [***lock the CLI from accepting all authentication requests for 20 seconds***].
Dependencies:	FIA_UAU.1 Timing of authentication

7.1.4.3 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***user name, password, role, port ownership, user group association***].

Dependencies: No dependencies.

7.1.4.4 FIA_SOS.1 Specification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

1. 8-30 characters

2. at least one of the characters must be a numeral

3. at least one of the characters must be an upper case letter

4. at least one of the characters must be a lower case letter

5. at least one of the characters must be a special character (ASCII 0x21-0x2F inclusive)

***6. at least 4 characters have changed from the previous password]*.**

Dependencies: No dependencies.

7.1.4.5 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

7.1.4.6 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide [***User name/password, TACACS+, or RADIUS***] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***global configuration defined by authorized users***].

Dependencies: No dependencies.

7.1.4.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

7.1.4.8 FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***all user attributes as specified in FIA_ATD.1***].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***association of a user's attributes to a session object***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***Revocation of the user-subject binding and termination of the user's session under the following condition: deleting of the user based upon their user name, user logging out, user being logged out due to inactivity***].

Dependencies: FIA_ATD.1 User attribute definition

7.1.5 Class FMT: Security Management

7.1.5.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behaviour of, modify the behaviour of] the functions [***operations on objects as defined in the Object and Operation columns of Table 7-3 Management of TSF Data***] to [***see Lock-Level column of Table 7-3 Management of TSF Data***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
Session	Login	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Own 1 or more ports.	Yes
Connect	Show	Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Owned NP/TP only	Yes
Diag		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
File		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Filter		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
gigastream		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hostkeys		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
Lock		Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
Log		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
map-rule		Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Owned NP/TP only	Yes
port-filter		Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Owned NP/TP only	Yes
port-params		Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Owned NP/TP only	Yes
port-stats		Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Owned NP/TP only	Yes
port-owner		Yes	Yes	Yes	Yes	Owned TP & all NP	Yes	Yes	Shows all normal users sharing NP/TP owned by issuer	Yes
rad_server		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
Snmp		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
sntp_server		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
System		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Symbols		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
tac_server		Yes	No	Yes	Yes	No	Yes	Yes	No	Yes
Uda		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
user-group		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
whoison		Yes	Yes	Yes	Yes	Shows all logged in normal users	Yes	Yes	Shows all logged in normal users	Yes

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
						only			only	
Xbsync		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
All	Delete	No	No	Yes	No	No	Yes	No	No	Yes
Connect		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned TP & all NP	Yes
File		No	No	Yes	No	No	Yes	No	No	Yes
Filter		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
gigastream		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Lock		No	Owned locks	Yes	No	N/A	N/A	No	N/A	N/A
Log		No	No	Yes	No	No	Yes	No	No	Yes
ntp_server		No	No	Yes	No	No	Yes	No	No	Yes
pass-all		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-pair		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-alias		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-filter		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Flow Map		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Mapping		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
map-rule		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
rad_server		No	No	Yes	No	No	Yes	No	No	Yes
snmp_trap		No	No	Yes	No	No	Yes	No	No	Yes
sntp_server		No	No	Yes	No	No	Yes	No	No	Yes
stack_info		No	No	Yes	No	No	Yes	No	No	Yes
tac_server		No	No	Yes	No	No	Yes	No	No	Yes
User		No	No	Yes	No	No	Yes	No	No	Yes
user-group		No	No	Yes	No	No	Yes	No	No	Yes
xbconnect		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Xbmap		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
xbmapping		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
xbport-filter		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Connect	Config	No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
File		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Filter		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
gigastream		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Lock		No	No	Yes	N/A	N/A	N/A	N/A	N/A	N/A
sntp_server		No	Yes	Yes	No	No	Yes	No	No	Yes
Flow Map		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
map_rule		No	Yes	Yes	No	Owned TP & all	Yes	No	Owned NP/TP	Yes

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
						NP			only	
Mapping		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
ntp_server		No	No	Yes	No	No	Yes	No	No	Yes
pass_all		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
password		No	Yes, own account only	Yes	No	Yes, own account only	Yes	No	Yes, own account only	Yes
port-alias		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-filter		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-owner		No	No	None at this lock-level	No	No	Yes	No	No	Yes
port-pair		No	Yes	Yes	No	All NP	Yes	No	Owned NP/TP only	Yes
port-params		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-type		No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
rad_server		No	No	Yes	No	No	Yes	No	No	Yes
Restore		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Save		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
snmp_server		No	No	Yes	No	No	Yes	No	No	Yes
snmp_trap		No	No	Yes	No	No	Yes	No	No	Yes

Object	Operation	Lock-Level								
		None			Medium			High		
		Audit	Normal	Super	Audit	Normal	Super	Audit	Normal	Super
sntp_server		No	No	Yes	No	No	Yes	No	No	Yes
System		No	No	Yes	No	No	Yes	No	No	Yes
tac_server		No	No	Yes	No	No	Yes	No	No	Yes
Uda		No	No	Yes	No	No	Yes	No	No	Yes
User		No	No	Yes	No	No	Yes	No	No	Yes
user-group		No	No	Yes	No	No	Yes	No	No	Yes
xbconnect		No	Yes*	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
Xbmap		No	Yes*	Yes	No	Owned cross-box TP	Yes	No	Owned cross-box TP	Yes
xbmapping		No	Yes	Yes	No	Owned cross-box TP	Yes	No	Owned cross-box TP	Yes
xbport-filter		No	Yes	Yes	No	Owned cross-box TP	Yes	No	Owned cross-box TP	Yes
Xbsync		No	No	Yes	No	No	Yes	No	No	Yes
Image	Install	No	No	Yes	No	No	Yes	No	No	Yes
port-stats	Reset	No	Yes	Yes	No	Owned TP & all NP	Yes	No	Owned NP/TP only	Yes
port-stats all		No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
system/factory default		No	No	Yes	No	Yes	Yes	No	Yes	Yes

Table 7-3: Management of TSF Data

*See Connection Locking Policy in Table 7-4 for permissions on these commands on objects that are part of a connection lock.

Object after locking	Deny Policy	Allow Policy
connect	Not allow to add/delete port-filter Not allow to share tool port with other	Allow to create "port-pair" on network ports of a "connect"

	logical connections	Allow to be used as a source port for a "pass-all" configuration Allow to branch out a new "connect" from this locked "connect"
map	Not allow to add/delete/modify map-rule Not allow to add/remove network-port and tool-port Not allow to share tool port with other logical connections	Allow to create "port-pair" Allow to be used as a source port of a new "pass-all"
pass-all	Not allow to share pass-all tool port with other connections Not allow to apply tool-port filter on a pass-all tool port	Allow to create "connect" and "xbconnect" Allow to apply network-port filter on a pass-all network port Allow to create "map" and "xbmap" Allow to configure "port-pair" if any
port-pair	No limitation	Allow to create "connect" and "xbconnect" Allow to apply network-port filters Allow to create "map" and "xbmap" Allow to configure "pass-all"
xbconnect	Not allow to add/delete xbport-filter Not allow to share tool port with other logical connections	Allow to create "port-pair" on network ports of a "xbconnect" Allow to be used as a source port for a "pass-all" configuration
xbmap	Not allow to add/delete/modify map-rule Not allow to add/remove network-port and tool-port Not allow to share tool port with other logical connections	Allow to create "port-pair" Allow to be used as a source port of a new "pass-all"

Table 7-4: Connection Locking Policy

7.1.5.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [***Gigamon Forwarding Policy SFP***] to restrict the ability to [change default, query, modify] the security attributes [***referenced in the indicated forward policies***] to [***see Lock-Level column of Table 7-3 Management of TSF Data***].

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

7.1.5.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [***Gigamon Forwarding Policy SFP***] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***users with the Super or Normal roles***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

7.1.5.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [***see Operation column of Table 7-3 Management of TSF Data***] the [***see Object column of Table 7-3 Management Functions of the TOE***] to [***see Lock-Level column of Table 7-3 Management of TSF Data***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

7.1.5.5 FMT_REV.1(1) Revocation

Hierarchical to: No other components.

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke [***lock-level***] associated with the [objects] under the control of the TSF to [***users with the Super role***].

FMT_REV.1.2(1) The TSF shall enforce the rules [***changing the lock-level will immediately enforce the authorization policies associated with that lock-level***].

Dependencies: FMT_SMR.1 Security roles

7.1.5.6 FMT_REV.1(2) Revocation

Hierarchical to: No other components.

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke [***username***] associated with the [users] under the control of the TSF to [***users with the Super role***].

FMT_REV.1.2(2) The TSF shall enforce the rules [***deleting a user based upon their user name will terminate the user's session***].

Application Note: *When roles are changed within the TOE, the module in charge of authorization will update the user to role binding.*

Dependencies: FMT_SMR.1 Security roles

7.1.5.7 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***operations on objects as defined in the Object and Operation columns of Table 7-3 Management Functions of the TOE***].

Dependencies: No dependencies.

7.1.5.8 FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [***Super, Normal, Audit***].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

7.1.6 Class FPT: Protection of the TOE Security Functions

7.1.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Dependencies: No dependencies.

7.1.7 Class FRU: Resource Utilization

7.1.7.1 FRU_FLT.1 Fault Tolerance

Hierarchical to: No other components.

FRU_FLT.1.1 The TSF shall ensure the operation of [***throughput of the production network traffic***] when the following failures occur: [***failure of the CPU, failure of a tap, failure of the TOE, failure of a link within a GigaStream, failure of external in-line device***].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

7.1.8 Class FTA: TOE Access

7.1.8.1 FTA_SSL.3(1) TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1(1) The TSF shall terminate an interactive session after a [***Super user definable set of time between 1-60 minutes for an inactive GUI session***].

Dependencies: No dependencies.

7.1.8.2 FTA_SSL.3(2) TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1(2) The TSF shall terminate an interactive session after a [***Super user definable set of time between 10-86400 seconds for an inactive CLI session***].

Dependencies: No dependencies.

7.1.8.3 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

Dependencies: No dependencies.

7.1.8.4 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies.

7.1.9 Class FTP: Trusted Paths/Channels

7.1.9.1 FTP_TRP.1 Trusted Paths

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, management functions].

Dependencies: No dependencies.

7.2 Operations Defined

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were modified from existing Security Audit (FAU) requirements, are designed to address the requirements for the TOE’s primary function, which is collection and indexing of IT data and the ability to search said data.

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

- Assignment: allows the specification of an identified parameter. Indicated with ***bold text and italics*** if further operations are necessary by the Security Target author.
- Refinement: allows the addition of details. Indicated with <u>***underlined bold text and italics***</u> if further operations are necessary by the Security Target author.
- Selection: allows the specification of one or more elements from a list. Indicated with <u>underlined text</u>.
- Iteration: allows a component to be used more than once with varying operations. Indicated with the iteration number within parentheses after the short family name, e.g. FAU_GEN.1 (1), FAU_GEN.1 (2).

8 Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2 augmented with ALC_FLR.1.

8.1 Security Architecture

8.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D: The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D: The developer shall design and implement the TSF so that it is able to protect itself from tampering by un-trusted active entities.

ADV_ARC.1.3D: The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C: The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C: The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C: The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C: The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1D: The developer shall provide a functional specification.

ADV_FSP.2.2D: The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C: The functional specification shall completely represent the TSF.

ADV_FSP.2.2C: The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C: The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C: For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C: For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C: The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E: The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

8.1.3 Basic Design (ADV_TDS.1)

ADV_TDS.1.1D: The developer shall provide the design of the TOE.

ADV_TDS.1.2D: The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C: The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C: The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C: The design shall describe the behavior of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C: The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C: The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C: The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

ADV_TDS.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E: The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

8.2 Guidance Documents

8.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

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.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

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.

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.

8.3 Lifecycle Support

8.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1D: The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D: The developer shall provide the CM documentation.

ALC_CMC.2.3D: The developer shall use a CM system. ALC_CMC.2.1C: The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C: The CM system shall uniquely identify all configuration items.

ALC_CMC.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1D: The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C: The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.3.3 Delivery Procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.3.4 Flaw reporting procedures (ALC_FLR.1)

ALC_FLR.1.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4 Security Target Evaluation

8.4.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

8.4.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

8.4.3 ST Introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

8.4.4 Security objectives (ASE_OBJ.2)

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide security objectives rationale.

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4.5 Derived security requirements (ASE_REQ.2)

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirement’s rationale.

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4.6 Security Problem Definition (ASE_SPD.1)

ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.4.7 TOE Summary Specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

8.5 Tests

8.5.1 Evidence of Coverage (ATE_COV.1)

ATE_COV.1.1D: The developer shall provide evidence of the test coverage.

ATE_COV.1.1C: The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.5.2 Functional Testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

8.5.3 Independent Testing - Sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

8.6 Vulnerability Assessment

8.6.1 Vulnerability Analysis (AVA_VAN.2)

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.1C The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E 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.

9 TOE Summary Specification

9.1 TOE Security Functions

The following sections identify the security functions of the TOE. They include Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access, and Trusted Path/Channels.

9.1.1 Security Audit

The TOE supports audit generation in the form of syslogs. All actions performed on the TOE are logged. Table 7-2 contains a list of all audited actions within the system.

9.1.1.1 Syslog

The TOE logs all user actions and saves a local copy of the events as syslog messages to its local cache memory. The TOE saves a maximum of 8 syslog files to the local memory with the filenames syslog.log and syslog1.log through syslog7.log. When the current syslog.log file reaches its maximum of 1 MB, syslog6.log is renamed to syslog7.log, syslog5.log is renamed to syslog6.log, and so on, until syslog.log is named syslog1.log and a new syslog.log is created. When syslog6.log is renamed to syslog7.log, the previous syslog7.log is overwritten. This ensures that only the oldest log containing the oldest events are overwritten when the new log is created when the audit trail is full. The TOE does not allow for the modification of local syslogs by lacking the functionality to perform such actions. Super users have the ability to delete log files, but this operation is also captured within the syslog. The TOE provides a timestamp in the format **YY-MM-DD hh:mm:ss** and includes the type of event ("userif," as shown in the example below), the subject identity ("gigamonster," below), and the commands used ("config port-filter 1 2," below). GigaVUE creates an event of all action performed on the TOE, including all commands issued and the start-up and shut-down of the system, which is synonymous with the start/stop of the audit system. The following is an example of a logged event:

```
11-12-07 10:34:40 info userif gigamonster config port-filter 1 2
```

The audit logs within the TOE do not specifically specify success or failure. However, the user can determine the success or failure nature of each audit record from the rest of the information within the log, including the subject identity and text command processed.

GigaVUE provides the capability to view the local log files from the command line with the **show log** command. The **logfile** argument specifies the log file to be viewed. The TOE also provides the **start** argument to sort and filter the data in the log files by start date and end date. The TOE will only allow a single sort command per log file, as the authorized user would enter the start command as follows "**show log <logfile> start <value(s)>**."

All of these arguments are required as part of the **show log** command structure but are not all security relevant. The only security relevant argument is **start**.

All user roles have explicit access to view the local syslog files with the **show log** command but only the Super user can delete the log files. Deletion of log files by Super users is also captured in the syslog.

In addition, the TOE can communicate to a syslog server through the management port. The syslogs sent to the server are identical to the local syslog files on the TOE. Super users are able to configure a single syslog server to which it can send syslogs.

9.1.1.2 Alerting

The TOE monitors for potential security violations in the events that get audited. Specific events can be configured to trigger an alert. The events are as follows: change to TOE configuration, change to TOE firmware, change to TOE modules, change to a port's link status, resetting the TOE, and a failed authentication attempt. The threshold for each of these events is one, meaning that a single occurrence, if configured, triggers an alert condition. The TOE sends alerts to an SNMP Manager in the form of an SNMP trap.

GigaVUE can send alerts via SNMP traps to up to 5 different destinations based on the following configurable events:

- **configsave**: A trap is sent to each configured destination each time the config save *filename*.cfg command is used.
- **firmwarechange**: A trap is sent to each configured destination each time it boots and detects that the firmware has been updated from the previous boot.
- **modulechange**: A trap is sent to each configured destination each time it detects a module is removed or added to a slot.
- **portlinkchange**: A trap is sent to each configured destination each time a port changes state from up to down or from down to up.
- **systemreset**: A trap is sent to each configured destination each time the unit starts up.
- **userauthfail**: A trap is sent to each configured destination each time a user login fails.

GigaVUE has the capability to send SNMP v1 and v2c traps, however, in the evaluated configuration the TOE will only be configured to use SNMP v2c traps.

9.1.1.3 Log-level

The TOE tracks auditable events through syslog. The evaluated configuration has the Log-level set to **Info** Log-level. This is not statically defined within the TOE, but the **config system log-level** command can be used to set the log-level. This Log-level logs all the events defined in the SFRs.

9.1.2 Cryptographic Support

To ensure secure communication through the GUI interface the TOE utilizes OpenSSL version 1.0.0c. The TOE generates 2048 bit RSA key pairs and uses AES with SHA-1 in CBC mode using 256 bit keys (HTTPS) or 128 bit keys (SSH) to encrypt and decrypt the communication. The TOE will generate the RSA key pairs for SSH during installation and provides Super users the ability to regenerate key pairs at any time. The TOE conforms to standards in RFC 2313 and RFC 3268. The key size that is utilized by AES in the evaluated configuration is 256 bit keys for HTTPS and 128 bit keys for SSH. In addition, the TOE must use 3rd party certificates to be used for SSL encryption. The TOE cannot generate RSA keys for the SSL encryption; a Super user must upload to the TOE the 2048 bit RSA certificates obtained by a certificate authority. When a new key is generated or uploaded to the TOE the old key is overwritten.

The TOE utilizes SSH to provide secure communication through the management port. The evaluated configuration utilizes 2048 bit RSA keys for key exchange and uses 256 bit AES keys (HTTPS) or 128 bit AES keys (SSH) for encrypting communication. The TOE follows the same encryption scheme as OpenSSL but utilizes a different internal mechanism and a different set of keys. A new key can be generated for SSH at any time by Super users with the **config system hostkey** command. The TOE uses the RSA keys and AES with SHA-1 in CBC mode to encrypt and decrypt the communication.

When connecting to the TOE with local authentication the TOE uses the Blowfish algorithm with a 128 bit key size to encrypt the passwords. When authenticating to the TOE via RADIUS and TACACS+ the TOE uses a shared secret key to encrypt communication the RADIUS or TACACS+ server. RADIUS supports the use of MS-CHAP v2 for authentication. SNMP traps are sent in the clear for all models.

9.1.3 User Data Protection

The TOE provides a forwarding policy called the Gigamon Forwarding Policy. The TOE takes the data that is received from one or more network ports and drops the data or forwards it to one or more tool ports.

The TOE provides mechanisms for the authorized users to manage where the data is sent and filter which data is sent through the TOE by setting attributes in the Gigamon Forwarding Policy. Only Normal users and Super users can manage where data is sent. The forwarding policy enforces data flow through the use of flow maps, filters, connections, Pass-Alls, collectors, and GigaStreams. There are no additional rules past the defined policy or exceptions to the defined flow policy, either on an explicit allow or explicit deny basis.

9.1.3.1 Gigamon Forwarding Policy

The TOE either receives copied network data or duplicates the network traffic into copied network data depending on configuration. The TOE then forwards the unmodified copied network data based on the attributes set in the Gigamon Forwarding Policy. The forwarding policy attributes include information based upon the network port, tool port, and information in the copied network data. The forwarding policy is enforced by the following types of subject and information security attributes:

Type	Attributes	Definition
Network Subject	Network Port #	Physical ingress port number where the copied network data or network traffic enters the TOE
Tool Subject	Tool Port #	Physical egress port number for tools connected to the TOE
Copied Network Data Attributes	Congestion Window Reduced	Determination on whether the congestion window is reduced or not; determines the outstanding bytes maximum within a connection
	ECN Echo	Determination on whether ECN Echo is used; allows end-to-end notification of network connection without dropping packets
	identity of source subject	Source IP address
	identity of destination subject	Destination IP address
	transport layer protocol	TCP, UDP, etc.
	network layer protocol	IPv4, IPv6, ICMP, etc.
	Ethertype	Describes which protocols are encapsulated within the packet
	VLAN	Virtual LAN to be filtered upon
	time-to-live/hop limit	Life cycle of a packet
	IPv4 fragment	Stream of data fragmented into multiple packets
	DSCP	Data priority classification
	Type of Service (TOS)	Data priority classification
	16-byte pattern matches	User-defined patterns to be

		filtered upon
	source service identifier	Source port number
	destination service identifier	Destination port number
	TCP flags	SYN (Synchronize flag)
		ACK (Acknowledge flag)
		RST (Reset flag)
		FIN (Finish flag)
		PSH (Push flag)
		URG (Urgent flag)

Table 5-1: Gigamon Forwarding Policy Attributes

The TOE uses the attributes listed above to allow or deny information flow from a network port to a tool port. The TOE also uses the attributes to determine how to filter the data being sent. So when data is sent to a tool, the policy may dictate, based upon filters, that only certain types of data (e.g. data with SYN flag) be transmitted to the tool. In addition, the identity of the network subject and tool subject must be in the policy rule set. The TOE prohibits any other information flow unless it is specified.

9.1.3.2 Forwarding Rules

The core functionality of the TOE is its ability to forward data based on specified criteria. The TOE receives data from a network through an internal or external tap. The TOE then filters the received data from a network port and forwards it to a tool port based on flow maps, filters, connections, pass-alls, collectors, and GigaStreams commands. The TOE has multiple ports that can be assigned to be either a tool port or a network port. There are no explicit allow or explicit deny rules within the TOE in terms of the forwarding policy. Any physical port on the TOE can be designated as a Network or Tool port, but cannot be simultaneously designated as both, this prohibited for security purposes.

9.1.3.2.1 Receiving Data

A network port receives copied network traffic or production network traffic in many ways. The TOE can be attached to a SPAN port coming from a network device, attached to a 3rd party tap, or it can be configured to use an internal tap. If data is received by the TOE from a 3rd party tap or SPAN, then the data is not considered secure, as it has already been copied from the main network stream. Internal taps are considered secure as they are controlled by the TOE management authentication process. The internal taps can be optical or electrical.

The TOE can also utilize internal optical tap(s) to receive network traffic. The optical tap is physically connected in-line with the production network cable and only splits the light. The split light is an exact copy of the production network traffic. As with the electrical tap, no data is added to or removed from the network traffic when using the optical tap. The nature of the physical optical tap protects the flow of network traffic from power failure, tool failure or TOE failure. Even though the production network traffic continues to flow, the ability of the TOE to forward copied data from a network port to a tool port is affected by power or TOE failure.

The TOE can also use an electrical tap to sit in-line with the network traffic and make an exact copy of the data coming in, allowing the network traffic to flow through the tap. No data is added or removed from the production network traffic as it passes through the TOE. In addition, the TOE has provided mechanical failover protection to ensure network traffic flow even if the TOE is in an error state, the tap module is removed, or the TOE is shut down. The electrical tap has a mechanical relay that automatically closes if there is a power failure or other failure of the TOE allowing the network traffic to continue to flow. However, the TOE will not be able forward copied network data from a network port to a tool port when in an error state. The TOE utilizes an internal watchdog which checks to ensure the CPU is functioning. If the watchdog finds the CPU in an error state, it shunts (closes) the relay, allowing the network traffic to flow unimpeded by the TOE's error, while the watchdog resets the CPU.

The TOE can also act as a bypass tap. In this configuration, the TOE connects to both sides of an IPS or other in-line device and monitors both itself and the in-line device. Specifically, the TOE copies network traffic creating copied network data, filters it, and sends it to tools. The TOE 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 TOE 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 TOE bypass tap will send the network traffic out to the production network. Monitoring the IPS or other in-line device connections ensures connectivity only; if the in-line device does not respond to the bypass tap heartbeat, the bypass tap will close and take the in-line device offline (bypass). The TOE monitoring itself is the same as already described where if the TOE fails it will bypass the TOE's functionality and thus also bypasses the in-line device.

If the power fails or the TOE fails it shunts the relay and allows production network traffic flow to continue, but the forwarding of copied network data from a network port to a tool port is stopped when this occurs. In addition, if the TOE detects that the device has stopped the flow of traffic, the TOE can bypass the in-line device and allow all traffic to pass through to the network un-interrupted.

The TOE can also configure two network ports as a port pair to allow the TOE to sit in-line with the network flow when no tap modules or external taps are available. The port pair is configured and the in-line port is used to receive network traffic, copy it internally, and sent the traffic back out to the network. The copied network data is then forwarded based on the Gigamon Forwarding Policy. However, it should be noted that this configuration does not provide the fault tolerance of the tap modules. A power failure or failure of the TOE will stop network traffic from flowing.

9.1.3.2.2 Filtering and Forwarding Data

After receiving the data through a network port the TOE allows the authorized users to select the desired data needed by the collection devices. Filters provide filtering capabilities and are attached to a network port or a tool port. A filter is a single rule that denies or allows data based on the attributes in the forwarding policy as described in section 9.1.3.1. A pre-filter is attached to a network port and filters the data before it is forwarded to one or more tool ports. Post-filters are attached to a tool port and filter data after it has been forwarded to a tool port. Pre-filters are used to send the same filtered data to all configured tool ports. Post-filters are used to filter data for each individual tool port that has one configured for it, so the connected tool will receive only the data that it needs to analyze, collect, or capture. Filters are used in conjunction with connections to forward only the desired data from a network port to a tool port. There is a 100 filter limit on tool filters defined, and filters cannot be set up on a network port before there is a connection set up. Flow maps and map rules provide similar functionality to connections and filters, but do not count against the filter limit.

The TOE allows connections to be made from a network port to a tool port. A 'connection' has a one to one relationship between the ports and is used for simple packet distribution. Multiple connections can be made on a single network port, but can only forward to a single tool port. The connections do nothing more than take the copied network data from one network port and forward it to a tool port. Filters may be added to the network port or the tool port to increase functionality by filtering the copied network data entering or leaving the TOE.

The TOE provides a more advanced and sophisticated way to forward copied network data through the use of flow maps. Flow maps are a collection of rules and filters that allow the authorized user to specify rules in a many to one, one to many, or many to many relationship between the respective network ports and the tool ports. Whereas the connections are limited to one network port and one tool port, the flow map can be assigned to one or multiple network ports and can forward copied network data to one or multiple tool ports. Flow maps allow the authorized user to define rules that allow or deny copied network data based on the attributes within the data (see Table 10). Many rules can be defined in a single flow map to allow the tools to get a copy of the exact data that they require to analyze, collect or capture. Flow maps also allow the authorized user to configure the TOE to forward copied network data to a virtual drop port, where copied network data that the tool does not require is discarded.

The TOE allows the authorized user to configure a Pass-all. A Pass-all rule collects all copied network data from a network or tool port and sends it to another tool port regardless of the filters, connections, or flow maps that are associated with those ports. This functionality is useful for troubleshooting or to send all copied network data to an IDS monitor, packet capture device, sniffer, performance monitor, or other IT product.

9.1.3.2.3 Moving the Data

After the TOE has received and filtered the copied network data, it sends the copied data to a tool port based on the connections and flow maps associated with the network port. Once the tool port receives the copied network data it will be transferred to a tool via a physical connection. Tools can be any type of analysis tool such as an IDS, forensic data recorder, protocol analyzer, packet capture device, or performance monitor.

The TOE also provides the ability to connect one GigaVUE to another through stacking (GigaStream port trunking). This allows authorized users to have more sources of input, greater flexibility when forwarding copied network data, higher throughput, and the ability to attach more tools to a multi-TOE deployment. The TOE allows one or multiple ports to be designated as stacking ports and pass copied network data through the configured stacking port to the other TOE. The two TOEs must be physically connected together and be configured to forward copied network data to each other. When stacked, the connection is a two way connection meaning that the TOEs can forward copied network data to another TOE. Flow maps, filters, and connections are compatible with stacking and are used in conjunction with stacking. Copied network data coming in on a network port on one TOE can be sent to a tool port on another TOE. This means that the TOE sending the copied data to the other TOE is receiving the copied data from the network and performing all of the filtering and forwarding decisions.

Stacking can be configured in a master-slave or classic configuration. The master-slave configuration allows authorized users to update all slave TOEs connected to the master TOE by updating the configuration on the master TOE. In this configuration the master TOE sends the management commands through the stacking port to the physically connected slave TOEs. Note that the slave TOEs can be physically connected to the master TOE or physically connected to another slave TOE in a daisy chain topology. This distributed management functionality allows the authorized user to identify and authenticate to only the master TOE, and then have the TOEs pass the updated configuration information to all slave TOEs. The classic configuration requires authorized users to log into each TOE separately to use the management functions. For the classic configuration to operate the same configuration must be defined on both sides. In classic configuration, the TOEs must also be physically connected to each other. In either configuration, the GigaVUEs verify that they are communicating with another GigaVUE once the stacking functionality has been configured on all TOEs, and the TOEs send alive packets to maintain that trusted connection. GigaVUE 2404 and GigaVUE 420 are the only models that can be used as a master in the master-slave configuration. The GigaVUE 212, GigaVUE 420, and GigaVUE 2404 can be a slave in the master-slave configuration as long as the master is a GigaVUE 2404.

The TOE is able to utilize a proprietary variant of the Ethernet trunking standard 802.1 called GigaStream. This capability allows the TOE to logically combine the functionality of multiple ports to increase throughput. There are three GigaStream deployment options which are described as follows:

1. Tool GigaStream – combining up to 8 ports to create a single trunk to a tool. This trunk supports single tools with up to 8 ports or multiple tools with individual network ports. Tool GigaStream supports both 1G and 10G network physical speeds.

2. Stacking GigaStream – combining up to 8 ports per chassis to create a single interconnecting bi-directional bus between TOE devices. Each TOE must allocate the same number of equal speed

physical connections and must be running the same version of TOE operating system. Stacking GigaStream supports both 1G and 10G network physical ports.

3. Crossbox GigaStream – a logical configuration which sends data from a network port(s) to a tool physically connected on another TOE. Crossbox stacks are dependent on the Stacking GigaStream physical connections.

9.1.4 Identification and Authentication

The TOE provides two interfaces to log on to the system in the evaluated configuration, a command line interface (CLI) via an SSH connection and a graphical user interface (GUI) via an HTTPS connection. Both interfaces connect to the TOE via the Ethernet Management port. All users must identify and authenticate before any other actions can occur on the TOE.

9.1.4.1 User attributes

Each user has the following security attributes associated with them:

- User name
- password
- role
- port ownership
- user group association

These user attributes are contained within whatever authentication mechanism is configured for the TOE. This means that the TOE will store user data if local authentication is used, and the enterprise server configured will store the user data in the event of enterprise authentication being used. The user name and password are for authenticating to the TOE. The role can be Audit, Normal, or Super, depending on the role assigned by an authorized user. Port ownership assigns network and tool ports to Normal users only. Port ownership is a concept that applies to Normal role users and defines their ability to configure the forwarding policy. This is further restricted based on lock-level, which is discussed in Section 9.1.5.2. Audit users are not assigned ports as they never have rights to ports, and Super users always have rights to all ports. User group association describes which group the user is associated with. The Normal user inherits the assigned ports of the user group. If a Normal user is assigned ports in the port ownership attribute as well as assigned a user group, the user group takes precedence.

9.1.4.2 Authentication Methods

The TOE provides multiple authentication methods. The TOE can support local authentication with user name and password, RADIUS, and TACACS+. Only a single authentication method can be configured for the TOE, so if an enterprise authentication server is used, local authentication or any other enterprise server is not used. The authentication method is configured by Super users and is a global configuration of the TOE. Regardless of the authentication method used, when an authorized user accesses the GUI or CLI they have their username and password requested by the respective interface. These credentials, in the case of local authentication, are checked against locally stored user data. The TOE uses Blowfish to generate hashes for storing user passwords, and all other user data is stored in plain text.

In the event of enterprise authentication, the TOE generates an MD5 hash of the password entered and communicates the entered username and password hash to the configured authentication server. The authentication server used then checks the username and password within its own internal user tables. If enterprise authentication is used, then no local user information is stored upon the TOE and thus the TOE will receive the user data from the enterprise server when an authorized user successfully authenticates. This is so a session can be created and authorizations can be performed.

For RADIUS, the TOE issues an access-request RADIUS packet, including the username and password hash. For TACACS+, the TOE sends a TACACS+ Start packet with the username and password hash. For all enterprise authentication methods, the user password is protected using MD5 hashes to share the secret.

The hash is checked with the hashes within the user tables of the authentication server. If the TOE receives a positive determination from the configured authentication server, a session is established on the TOE for the user based upon the username and password passed in.

The TOE does not allow any TSF-mediated actions before the user is identified and authenticated through the administrator-configured authentication method. After authentication, the user's security attributes are associated with all subject actions on session objects. This includes changes to security attributes associated with the user subjects, such that the updates are reflected appropriately. Therefore, if a user logs out, times out, or is removed as an authorized user of the TOE, the session is immediately revoked to account for the action taken. This differs depending on the user interface used. If the GUI is used, then the TOE generates a random number and places it into a session cookie, which associates that user with an active session. If the CLI is used, the TOE establishes an SSH session, which associates that user with an active session. In addition, the TOE starts an internal process to maintain that user's active session and will associate all requests with a cookie or SSH session identifier with the associated user. Both cookies and SSH sessions are considered internal processes and operate similarly for I&A purposes.

9.1.4.3 Failed Authentication Attempts

The TOE keeps track of failed consecutive authentication attempts from users within each distinctive user interface. After five consecutive unsuccessful authentication attempts from a single user via the GUI the TOE locks the GUI from accepting authentication requests from all users for 20 seconds. This only affects new authentication requests; all other simultaneous HTTPS connections to the GUI are unaffected. After six unsuccessful authentication attempts from a single user via the CLI the TOE locks the CLI from accepting authentication requests for 20 seconds. This only affects new authentication requests, all other simultaneous SSH connections to the CLI are unaffected.

9.1.4.4 Password Policy

The TOE enforces a password policy for all users. The password policy requires that the password is between 8-30 characters and that at least one character is a numeral, at least one character is an upper case letter, at least one character is a lower case letter, and at least one character is a special character (ASCII 0x21-0x2F). Super users can set expiration dates on user's passwords that will force them to reset their password after the configured amount of time has been met. Passwords can be set to never expire, or to expire between 1 and 90 days. Additionally, new passwords must have at least 4 characters change from the previous password. Normal users can change their own passwords as long as they have not changed it in the last 24 hour period. Super users can change all users' passwords and is the only role authorized to change the password of Audit users. Note that all users, including Super users, must adhere to the password policy when creating or modifying passwords. This involves both modifying the user's own password, or the Super user's ability to create new users with new passwords and the ability to modify an existing user's password.

9.1.5 Security Management

The TOE enforces security management through many mechanisms. All security management functions available to authorized users of the TOE are mediated by an RBAC system. There are three roles defined within the TOE; each has different levels of authorization in terms of the functions that can be performed by them. The TOE contains multiple lock-levels which determine the requirement of owning a network or tool port before creating, modifying, or deleting rules within the Gigamon Forwarding Policy, assuming the user is of the Normal role. When put into a Medium or High lock-level, the TOE requires Normal users to have port ownership, which allows them to create, modify, and delete rules that utilize that physical port. These ports are separated into network (ingress traffic) and tool (egress traffic) ports. When the lock-level is set to None, Normal users can create, modify, and delete rules without owning ports. The use of user-groups, roles, and lock-levels provide the administrator the ability to restrict the management functions, commands, and the administrative data accessible by Normal users. The default values for the TOE do not include any forwarding rules, so the TOE will not forward any potentially sensitive data without explicit configuration by authorized users. Additionally, only authorized users are allowed to change the values from their default values based upon the permissions in Table 7-3. No authorized users have the ability to manage or have visibility of production network traffic flowing through the TOE. For an explicit list of the roles and all functions that are allowed to said role at each lock-level, refer to Table 7-3 Management of TSF Data.

9.1.5.1 Roles

There are three different roles that users can be assigned to; Super user, Normal user, and Audit user. Each user must be assigned to a role. The role is one of the mechanisms that determine which commands can be executed by a user.

- **Super user**: Have access to all ports on the TOE regardless of the lock-level and can perform all configuration commands.
- **Normal user**: Have access to different ports depending on the lock-level and port assignment and cannot perform most of the system configuration commands.
- **Audit user**: Do not have access to any ports. Audit user's primary ability is to use the **show** command to see what basic settings are in place on the TOE.

Note that only Super users have the ability to delete other users by username, which goes into effect immediately by terminating the user's session and removing the user information from the TOE.

9.1.5.2 Lock-level

The Lock-level is used to restrict the rights of Normal users. As the Lock-level increases, Normal users have fewer rights over ports on the TOE. A description of the three lock-levels is below.

- **None**: Normal users have access to all network ports and tool ports on the TOE.
- **Medium**: Normal users have access to all network ports but can only set up connections/filters/flow maps for tool ports they own.
- **High**: Normal users can only configure connections/filters/flow maps for network ports and tool ports that they own.

Note that the Lock-level can only be changed by Super users and that it only affects Normal users. When the Lock-level is changed by a Super user the restrictions are enforced immediately. Super users always have access to all ports on the TOE, and Audit users never have write access to any ports on the TOE. However, regardless of the lock-level, Audit users are able to review all policy information.

9.1.5.3 Connection Locking

All connections created by Super or Normal users associate that user account as the "owner" of the connection. The owner of a connection can lock the connection. Locking a connection means that all Normal users are prevented from modifying or deleting the connection except for the "owner" of the connection. Super users are unaffected by locking, as Super users have access to all TOE functionality at all times (even in different lock-levels). Connection locking is separate from lock-levels and only applies at the "None" lock-level.

9.1.5.4 User-group

User-groups allow the administrator to set the same port ownership privileges to multiple Normal users. This is helpful when there are multiple people using the same information with similar needs. The administrator sets the port ownership to the user-group and can then assign multiple Normal users to that user-group. Assigning a Normal user to a user-group gives that user the port ownership permissions that have been assigned to that user-group. Normal users do not have to be assigned to a user-group, however, and can simply be assigned port ownership. In addition, if a Normal user within a user-group locks his or her own connection, then other Normal users within the same user-group will have access to the connection as if it weren't locked. Note that port ownership is only enforced at a lock-level of Medium or High. When the lock-level is set to None, all Normal users have access to all network ports and tool ports. Also note that user-groups are only assignable to Normal users. Super users always have access to all ports and Audit users never have write access to any ports. If a Normal user is assigned certain ports and the user is also assigned to a user-group with different ports, the user-group takes precedence.

9.1.6 Protection of the TSF

The TOE enforces reliable timestamps of syslog captured events through the use of a reliable clock.

The TOE uses a watchdog component to ensure the CPU is working correctly. If the CPU fails, the watchdog closes the mechanical relay if an electrical tap is included in the model to ensure that the network traffic continues to flow. The watchdog then reboots the CPU. While the CPU is rebooting, the production network traffic continues to flow, but the TOE does not filter and forward copied network data until the TOE is finished rebooting. When the TOE is deployed as an in-line device using an electrical or optical tap, any TOE failure such as complete shutdown never affects production network traffic passing through the TOE for production purposes. However, the TOE will not be able to copy and forward the copied network data from network ports to tool ports. This is achieved because the TOE operates as a fiber splitter or mechanical relay when these taps are used. Optical taps only split light and are unaffected by power loss, while the mechanical relays of an electrical tap will shunt due to power failure.

If the TOE detects that a link goes down on a GigaStream, it fails over to the next configured port. Since a GigaStream is a logical connection of more than one port, when one link goes down, the traffic that was going through that port is redirected to one of the remaining ports in the GigaStream. GigaStream can also be configured to redirect the failed ports' allocated traffic to the remaining ports within the GigaStream. Either scenario is automatic and based on the pre-configured attributes of the GigaStream.

9.1.7 Resource Utilization

The TOE can act as an electrical tap allowing the network traffic to flow through it while the TOE creates a copy of the network traffic to forward and filter to the tools connected to it. In this configuration the TOE ensures that the throughput of network traffic continues to flow when the CPU fails or if there is a power failure. There is a watchdog timer that checks on the CPU in specified intervals to ensure it is running correctly. If the CPU fails for any reason the watchdog closes the mechanical gate on the electrical tap to ensure network traffic flow. In the case of a power failure there is a mechanical relay that closes as soon as power is lost to ensure the network traffic continues to pass through. In this state the TOE cannot copy the network traffic so no copied network data will be forwarded from network ports to tool ports. If the TOE detects that a link goes down on a GigaStream port, it fails over to the next configured port or is redirected to the remaining ports. In the event of a previously-failed port in a GigaStream coming back online, the TOE will automatically redetect the link to the network device and will restore the GigaStream traffic across the link.

9.1.8 TOE Access

The TOE allows a Super user to set up a definable banner that is displayed on user facing interfaces before they can log in. When logging in via an SSH session the banner is displayed at the top after the user enters their user name but before the user can input their password. When logging in via the GUI, the user receives a pop up window that displays the banner and must click "OK" before they can continue. The banner should contain information specific to the organization that defines it, such as restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. Upon accepting the banner text, the user is then allowed to log in with their username and password.

After logging in the TOE provides means to logout when the user is finished. The authorized user can issue the **logout** command when connected via the CLI, and the user can click on the **logout** button when connected via the GUI. In addition, the Super user can specify the amount of time session can be inactive before it is logged out. The Super user can set the time-out session to be between 10-86400 seconds for the

CLI, and between 1-60 minutes for the GUI. When a session has been inactive for the specified amount of time, the user is logged out.

9.1.9 Trusted Path/Channels

The TOE provides two user facing communication paths in the evaluated configuration including a CLI and a GUI. The CLI uses SSH encryption to protect the communication between the remote user and the TOE. Remote users can also communicate with the TOE through a GUI over HTTPS which uses OpenSSL version 1.0.0c. The trusted communication path for either interface is initiated by the user: by navigating to the web address for the GUI or by initiating an SSH connection for the CLI. Sessions are encrypted using AES and RSA keys to ensure a secure communication and validation of the end points. The users must authenticate through the CLI or the GUI to be able to perform any functions on the TOE. This trusted path connection is used throughout the entire user session, which means that it is used from the initial authentication to all management functions that an authorized user attempts to perform through the interface.

9.1.10 Security Architecture

GigaVUE has multiple architecture features that enhance the security functions of the TOE. GigaVUE uses roles, connection locking, and lock-levels to limit Normal user access to functions of the TOE. In addition, the TOE includes domain separation techniques in its architecture to separate users' actions. The TOE also utilizes fault tolerance, and a watchdog to ensure the TOE installs and runs securely.

9.1.10.1 Separation of Roles

The TOE utilizes three distinct roles that have differing levels of access to management functions. Roles provide a mechanism for the administrators to protect important functions of the TOE by restricting access to functions that are not required for all users. Audit users, for example, only have read access to all major functions of the TOE, allowing them to see settings and configuration, but not allowing them to make any changes. Roles can be changed for all user accounts, including the default user account with the Super role assigned to it. However, there must always be a Super user. In addition, the TOE provides the ability to lock connections that are set up by authorized users. This protects the data that is received by a tool from tampering by other users. The other users are not permitted to add to or remove data flows on locked connections. The lock-level provides additional separation of roles by limiting Normal user's access to network ports and tool ports.

9.1.10.2 Domain Separation

The TOE has been developed to have access to the operating system disabled for all users of the TOE. There is a separation between the operating system, the data the operating system uses, and the copied network data that the TOE forwards. There is no method for users to view, modify, or interact with the actual production network traffic traversing through the TOE when the TOE performs its functionality both when in-line with the network traffic and when it receives copied network data out-of-band. The TOE does not add any data to network traffic in when using a tap in in-line mode or any other mode. There is no return path of TOE data to be included in the production network traffic. The TOE does not include functionality in its code base to allow copied traffic to be read by users of the TOE, nor to allow the TOE to send back or inject any data onto the production network, other than the network traffic traversing through a tap that was received from the production network.

The TOE also provides mechanisms that isolate information being used by a user from access or modification by other users.

9.1.10.3 Secure Operation

All users of the TOE must authenticate before performing any action on the TOE. This prevents users from accessing functions outside the scope of their role. There is encryption between authorized users and the TOE to protect the confidentiality and integrity of the information and commands. There is proprietary encryption between the TOE and 3rd party authentication mechanisms (e.g. RADIUS, TACACS+), although it does not conform to any cryptographic standard. This encryption between these components and the TOE consists of a pre-shared key.

A watchdog continuously watches the CPU to ensure it is running correctly, as soon as it notices a fault in the CPU it will close the relay of all the internal electrical taps and restart the CPU. The watchdog is an internal OS process that is constantly running in the background and cannot be disabled by TOE users. Closing the relay will allow all data to continue to flow through the tap and ensure connectivity of the network traffic, even though the TOE cannot forward copied network data. If for any reason the TOE errors or faults, there will be no connectivity loss with the production network traffic when the TOE is used in-line with network flow. When the TOE is not used in-line no production network traffic flows through the TOE, it is on received out-of-band by the TOE. The TOE also has the capability to monitor a device through a bypass tap. If the TOE finds that the device is not working correctly, it will bypass the device and allow production network traffic to continue to flow unimpeded as well as send an SNMP alert identifying the issue and create a Syslog event.

9.2 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

Security Function	Security Functional Components
Security Audit (FAU)	FAU_ARP.1 Security alarms
	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_SAA.1 Potential violation analysis
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.2 Guarantees of audit data availability
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic key generation
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1 Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1 Subset information control
	FDP_IFF.1 Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1(1) Authentication failure handling
	FIA_AFL.1(2) Authentication failure handling
	FIA_ATD.1 User attribute definition
	FIA_SOS.1 Verification of secrets
	FIA_UAU.2 User authentication before any action
	FIA_UAU.5 Multiple authentication mechanisms
	FIA_UID.2 User identification before any action
	FIA_USB.1 User-subject binding
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior
	FMT_MSA.1 Management of security attributes
	FMT_MSA.3 Static attribute initialization
	FMT_MTD.1 Management of TSF data
	FMT_REV.1(1) Revocation
	FMT_REV.1(2) Revocation
	FMT_SMF.1 Specification of Management Functions

Security Function	Security Functional Components
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_STM.1 Reliable time stamp
Resource Utilization (FRU)	FRU_FLT.1 Fault tolerance
TOE Access (FTA)	FTA_SSL.3(1) TSF-initiated termination
	FTA_SSL.3(2) TSF-initiated termination
	FTA_SSL.4 User initiated termination
	FTA_TAB.1 Default TOE access banners
Trusted Path/Channels(FTP)	FTP_TRP.1 Trusted path

Table 9-6: Security Functional Components for the TOE

9.2.1 Security Audit

This section maps directly to the information found in Section 9.1.1. This security classification addresses the following requirements: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.2.

FAU_ARP.1 and FAU_SAA.1 are addressed by creating the alerts that are sent via SNMP traps and listing the events that cause the alerts. FAU_GEN.1 and FAU_GEN.2 are demonstrated by showing which actions are audited (all user actions) and providing all the data that is collected in the audit logs. FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 are addressed by discussing the audit logs, and showing what makes up a log, showing who can view audit logs, and showing how it can be filtered. FAU_STG.2 is satisfied by discussing how logs are stored and that only authorized users can delete them.

9.2.2 Cryptographic Support

This section maps directly to the information found in Section 9.1.2. This security classification addresses the following requirements: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

FCS_CKM.1 and FCS_CKM.4 are satisfied by discussing that the TOE creates and destroys cryptographic keys. The TOE will generate 2048 bit RSA keys for use with SSH and will use uploaded 2048 bit RSA certificates for used with HTTPS. The TOE will overwrite cryptographic keys when generated or uploaded. FCS_COP.1 is addressed through the discussion of the TOE utilizing OpenSSL with 2048 bit RSA keys and the AES algorithm with SHA-1 in CBC mode.

9.2.3 User Data Protection

This section maps directly to the information found in Section 9.1.3. This security classification addresses the following requirements: FDP_IFC.1, FDP_IFF.1.

FDP_IFC.1 is addressed by discussing the enforcement of the Gigamon Forwarding Policy. FDP_IFF.1 is satisfied by listing the attributes used to enforce the Gigamon Forwarding Policy. These attributes are used to allow or deny data flow, these attributes are listed in Table 10.

9.2.4 Identification and Authentication

This section maps directly to the information found in Section 9.1.4. This security classification addresses the following requirements: FIA_AFL.1(1), FIA_AFL.1(2), FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FIA_USB.1.

FIA_AFL.1(1) and FIA_AFL.1(2) are addressed by discussing the two user interfaces, which are the GUI and the CLI, and the result of multiple failed authentication attempts. FIA_ATD.1 is satisfied through the discussion of attributes that are associated with each user account. FIA_SOS.1 is addressed by listing the requirements for the password policy, which require the password to be between 8 and 30 characters where at least one character is a numeral, at least one character is an upper case letter, at least one character is a lower case letter, and at least one character is a special character. FIA_UAU.2 is explained through ensuring the TOE will not allow any user to perform actions on the TOE before they are authenticated. FIA_UAU.5 is addressed through the discussion of the authentication mechanisms that the TOE supports. Local Authentication, TACACS+, and RADIUS are all supported authentication mechanisms. FIA_UID.2 is addressed by discussing how all users must be identified before being allowed to perform any action on the TOE. FIA_USB.1 is satisfied by discussing the security attributes that are associated with each user and are revoked when a user is deleted.

9.2.5 Security Management

This section maps directly to the information found in Section 9.1.5. This security classification addresses the following requirements: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1(1), FMT_REV.1(2), FMT_SMF.1, FMT_SMR.1.

FMT_MOF.1 is addressed by discussing the lock-level, what it can be set at, and the how this will limit the permission of Normal users. Table 7-3 includes the lock-level and the permissions restricted for each Normal user. FMT_MSA.1 and FMT_MSA.3 are satisfied by discussing management functions that are available to each role. Table 7-3 includes all management functions and shows which roles are allowed to perform those functions. FMT_MTD.1 is satisfied through Table 7-3 listing which subjects can perform operations on which objects. FMT_REV.1(1) is addressed by discussing the Super user's ability to change the lock-level and how that action restricts the Normal user's ability to perform operations on objects of the TOE. FMT_REV.1(2) is addressed by discussing the Super user's ability to delete users and have the user's session terminated. FMT_SMF.1 is addressed by discussing the management functions and listing them in Table 7-3. FMT_SMR.1 is satisfied by listing the three roles supported by the TOE. Users can be assigned to be a Super user, Normal user, and Audit user.

9.2.6 Protection of the TSF

This section maps directly to the information found in Section 9.1.6. This security classification addresses the following requirements: FPT_ STM.1.

FPT_STM.1 is addressed by discussing how the TOE has an internal clock that is used for time stamps.

9.2.7 Resource Utilization

This section maps directly to the information found in Section 9.1.7. This security classification addresses the following requirements: FRU_FLT.1.

FRU_FLT.1 is satisfied by showing how the TOE maintains throughput of network traffic when the CPU or the TOE fails. The watchdog watches the CPU for failure and closes the relay allowing flow through. The TOE also provides mechanical relays that detect TOE and power failure which also closes the relay allowing flow through of network traffic regardless of the state of the TOE.

9.2.8 TOE Access

This section maps directly to the information found in Section 9.1.8. This security classification addresses the following requirements: FTA_SSL.3(1), FTA_SSL.3(2), FTA_SSL.4, FTA_TAB.1.

FTA_SSL.3(1) and FTA_SSL.3(2) are addressed by discussing the length of time a user session is allowed to be inactive before it is logged out within both the GUI and CLI. The discussion includes the ability to configure the maximum inactivity time to be between 1 and 60 minutes for the GUI and between 10 and 86400 seconds for the CLI. FTA_SSL.4 is addressed by discussing how the users can log out themselves to terminate their session. FTA_TAB.1 is satisfied by allowing the Super users to set a banner that will be displayed before any user is allowed to log in.

9.2.9 Trusted Path/Channels

This section maps directly to the information found in Section 9.1.9. This security classification addresses the following requirements: FTP_TRP.1.

FTP_TRP.1 is addressed by discussing how users remotely connect to the TOE through encrypted channels.

10 Security Problem Definition Rationale

10.1 Security Objectives Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

Assumption	Objective	Rationale
A.ADMIN One or more users authorized by the Operational Environment will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. ADMIN in order to ensure that only the users authorized by the TOE will install and configure the TOE to bring it into the evaluated configuration. During operation only the users authorized by the TOE will be able to manage the TOE in a manner that maintains its ADMIN objectives.
A.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL All users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.	OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
A.PATCHES System Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.	OE.ADMIN One or more authorized users will be assigned to configure the Operational Environment, and install, configure, and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A. PATCHES in order to ensure that the users authorized by the Operational Environment will patch the Operational Environment in a manner that maintains their security objectives.
A.NO_GENERAL_PURPOSE The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, database servers, or user applications) available on the TOE.	OE.NO_GENERAL_PURPOSE The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.	OE.NO_GENERAL_PURPOSE maps to A.NO_GENERAL_PURPOSE to ensure that the TOE is only used for its intended purpose and that there are no general purpose computing or storage repository capabilities available on the TOE.
A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.	OE.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.	OE.LOCATE maps to A.LOCATE in order to ensure that physical security is provided in the environment where the TOE operates.

Table 10-1: Assumption to Objective Mapping

Threat	Objective	Rationale
T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	O.ACCESS (FIA_USB.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1) helps mitigate this threat by providing authorized users the ability to determine the access levels of authenticated users through the assignment and enforcement of roles.
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	O.MANAGE (FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1) helps mitigate this threat by providing authorized users the ability to configure the TOE within a secure state or return the TOE to a secure state.
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause the records or information to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.	O.AUDIT (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.2) helps mitigate this threat by assuring that all security-relevant actions are audited such that all misuse of the TOE can be tracked to the malicious user.
	O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded.	O.ALERT (FAU_ARP.1, FAU_SAA.1) helps mitigate this threat by providing functionality to generate and send alerts based upon definable criteria such that if an alert condition is triggered, an authorized user will be notified within a suitable timeframe.

	O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE	O.ACCESS (FIA_USB.1, FIA_ATD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1) helps mitigate this threat by providing authorized users the ability to determine the access levels of authenticated users through the assignment and enforcement of roles, such that only users explicitly authorized to perform an action can perform one.
	O.SYSTIME The TOE will provide reliable system time.	O.SYSTIME (FPT_STM.1) helps mitigate this threat by assuring that all audit logs will have appropriate timestamps applied to them to pinpoint the exact time a malicious action occurred.
T.EAVESDROPPING A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.	O.EAVESDROPPING (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FTP_TRP.1) helps mitigate this threat by ensuring that all external communication to and from the TOE is encrypted with cryptographic keys of appropriate strength.
T.NETWORK_FLOW A malicious user may attempt to subvert the TOE or defeat the operation of its security mechanisms to cause a disruption in the flow of data on the production network.	O.NETWORK_FLOW_PROTECTION The TOE will preserve the information flow of the production network traffic through the TOE in the presence of adversarial activity when a component of the TOE fails.	O.NETWORK_FLOW_PROTECTION (FRU_FLT.1) helps mitigate this threat by ensuring that the TOE has means to protect network throughput in the event of the system being unexpectedly brought down.
T.MASK Users whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.	O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	O.AUTH (FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FIA_USB.1) helps mitigate this threat by requiring users to have appropriate user accounts on the TOE with appropriate secrets such that a malicious user could not easily gain access to another user’s account.

	O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	O.ROBUST_TOE_ACCESS (FTA_SSL.3(1), FTA_SSL.3(2), FTA_SSL.4, FIA_AFL.1(1), FIA_AFL.1(2)) helps mitigate this threat by providing mechanisms to prevent malicious users from brute forcing passwords, ensuring that inactive sessions are appropriately closed, and providing a secure logout functionality for legitimate users.
T.STEALTH A malicious user or process could perform suspicious activities against objects in the Operational Environment without an Operational Environment user becoming aware of this behavior because the TOE's forwarding policy did not forward the information to the necessary tool per its configuration.	O.MAP The TOE will provide mechanisms to set and control the forwarding of information to a tool based upon its configuration.	O.MAP (FDP_IFC.1, FDP_IFF.1) helps mitigate this threat by creating and enforcing flow control policies to send cloned network traffic to appropriate devices for future analysis.

Table 10-2: Threat to Objective Mapping

10.2 Operational Security Policy Rationale

The following table provides a mapping with rationale to identify the security objectives that address the stated organizational security policy.

OSP	Objective	Rationale
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 system.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays a Security Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE.

10.3 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the security functional requirement components that address the stated TOE objectives.

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the authorized users of the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 shows all of the user attributes that are utilized to authorize users, including user role.
	FIA_USB.1 User-subject binding	FIA_USB.1 shows how users and their roles are associated in a session. It also details how a user loses his or her session based upon administrative changes.
	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 defines the functions that can be performed by specific roles within the TOE.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 defines functions that can be performed by authorized users to configure the forwarding policy.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 requires all security-relevant attributes have restrictive default values, and that an authorized user has the ability to override default values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 defines the specific actions that specific roles can perform on specific data sets within the TOE.
	FMT_REV.1(1) Revocation	FMT_REV.1(1) details how a users' permissions are restricted based upon administrative changes.
	FMT_REV.1(2) Revocation	FMT_REV.1(2) details how a user loses his or her session object based upon administrative changes.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 defines the functions that can be performed by specific types of users of the TOE.
	FMT_SMR.1 Security roles	FMT_SMR.1 defines that there are roles in the system and that users are associated with their role for making authorization decisions.

Objective	Security Functional Components	Rationale
O.ALERT The TOE will provide measures for determining security alerts when audit data that represent any of these alerts is recorded.	FAU_ARP.1 Security alarms	FAU_ARP.1 requires the TOE to provide mechanisms to alert authorized users in the event of a security violation.
	FAU_SAA.1 Potential violation analysis	FAU_SAA.1 requires the TOE to provide mechanisms to determine if a security violation has taken place. With both this and FAU_ARP.1, the TOE will detect violations and alert authorized users appropriately.
O.AUDIT The TOE will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.	FAU_GEN.1 Audit data generation	FAU_GEN.1 defines the behavior of the TSF which causes security relevant events to be generated and enumerates the data which is contained within these events.
	FAU_GEN.2 User identity association	FAU_GEN.2 confirms that all relevant auditable events include subject identity for the purposes of accountability.
	FAU_SAR.1 Audit review	FAU_SAR.1 provides the ability for all authorized users to read audit data using the UIs.
	FAU_SAR.2 Restricted audit review	FAU_SAR.2 states that all users can read audit data via the UIs.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 requires the TOE to provide mechanisms for users to filter returned audit results within the audit view in the UIs.
	FAU_STG.2 Guarantees of audit data availability	FAU_STG.2 states that only authorized users can use the TOE functionality that exists to modify or delete audit records and that the oldest logs will be deleted once storage is exhausted.
O.AUTH The TOE will provide measures to uniquely identify all users and will authenticate the claimed identity prior to granting a user access to the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 defines the security-relevant attributes of all users. This includes attributes related to authentication.
	FIA_SOS.1 Verification of secrets	FIA_SOS.1 defines the password policy that sufficiently protects generated secrets from brute force attacks.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires users to authenticate to the TOE before any

Objective	Security Functional Components	Rationale
		TSF-mediated actions are allowed.
	FIA_UAU.5 Multiple authentication mechanisms	FIA_UAU.5 defines the various authentication mechanisms in the TOE: native username/password, RADIUS, TACACS+.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires users to identify themselves to the TOE before any TSF-mediated actions are allowed.
	FIA_USB.1 User-subject binding	FIA_USB.1 defines the mapping between users and roles and the creation of a session.
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1 Default TOE access banners	FTA_TAB.1 requires the TOE to provide a warning banner to users prior to authentication.
O.EAVESDROPPING The TOE will encrypt TSF data that traverses the network to prevent malicious users from gaining unauthorized access to TOE data.	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 requires the TOE to generate proper cryptographic keys for use in encrypting sensitive data.
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 requires the TOE to destroy cryptographic keys used in encrypting sensitive data. Keys are destroyed when new keys are generated.
	FCS_COP.1 Cryptographic operation	FCS_COP.1 requires the TOE to utilize the generated cryptographic keys in protecting all data transferred to and from users, other TOE components, and external IT products.
	FTP_TRP.1 Trusted path	FTP_TRP.1 requires the TOE to make all security-relevant data sent to and from users protected against modification. This is done by creating a trusted path with the encryption mechanisms described in FCS_COP.1.

Objective	Security Functional Components	Rationale
O.MANAGE The TOE will provide authorized administrators with the resources to manage and monitor user accounts, resources, and security information relative to the TOE.	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 defines the functions that can be performed by specific roles within the TOE.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 defines functions that can be performed by authorized users to configure the forwarding policy.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 requires all security-relevant attributes have restrictive default values, and that an authorized user has the ability to override default values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 defines the specific actions that specific roles can perform on specific data sets within the TOE.
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 defines the functions that can be performed by specific types of users of the TOE.
O.MAP The TOE will provide mechanisms to set and control the forwarding of information to a tool based upon its configuration.	FDP_IFC.1 Subset information control	FDP_IFC.1 details the subjects and objects defined and controlled within the forwarding policy.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 details the security attributes and rules that are taken into account when enforcing the forwarding policy.
O.NETWORK_FLOW_PROTECTION The TOE will preserve the information flow of the production network traffic through the TOE in the presence of adversarial activity when a component of the TOE fails.	FRU_FLT.1 Fault tolerance	FRU_FLT.1 requires that the TOE protects the network's traffic throughput when the TOE or its CPU goes down.
O.ROBUST_TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	FIA_AFL.1(1) Authentication failure handling	FIA_AFL.1(1) helps authorize and explicitly deny user access by providing a mechanism to protect against brute force password attacks.
	FIA_AFL.1(2) Authentication failure handling	FIA_AFL.1(2) helps authorize and explicitly deny user access by providing a mechanism to protect against brute force password attacks.
	FTA_SSL.3(1) TSF-initiated termination	FTA_SSL.3(1) helps the TOE offer granular controls to provide access to TOE resources by providing functionality to automatically

Objective	Security Functional Components	Rationale
		terminate a user's session if they are idle or away from their terminal.
	FTA_SSL.3(2) TSF-initiated termination	FTA_SSL.3(2) helps the TOE offer granular controls to provide access to TOE resources by providing functionality to automatically terminate a user's session if they are idle or away from their terminal.
	FTA_SSL.4 User-initiated termination	FTA_SSL.4 helps the TOE offer protection of TOE access by presenting users the ability to securely log out of the UI.
O.SYSTIME The TOE will provide reliable system time.	FPT_STM.1 Reliable time stamp	FPT_STM.1 requires the TOE to maintain accurate system time to provide for time stamping purposes.

Table 10-3: Security Functional Requirements Rationale

10.4 EAL2 Justification

The threats that were chosen are consistent with an attacker of basic attack potential, therefore EAL2 augmented with ALC_FLR.1 was chosen for this ST. ALC_FLR.1 is not required, but provides additional quality assurance to the product.

10.5 Requirement Dependency Rationale

The table below lists each requirement from claimed Security Functional Requirements with a dependency and indicates whether the dependent requirement is included. If a dependency has not been met, a short rationale is provided to show why the dependency is not included.

Functional Component	Dependency	Included
FAU_ARP.1	FAU_SAA.1	YES
FAU_GEN.1	FPT_STM.1	YES
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_STG.2	FAU_GEN.1	YES
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	YES (FCS_COP.1)
	FCS_CKM.4	YES
FCS_CKM.4	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1	YES (FCS_CKM.1)

FCS_COP.1	FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1	YES (FCS_CKM.1)
	FCS_CKM.4	YES
FDP_IFC.1	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1	YES
	FMT_MSA.3	YES
FIA_AFL.1(1)	FIA_UAU.1	YES (Hierarchy: FIA_UAU.2)
FIA_AFL.1(2)	FIA_UAU.1	YES (Hierarchy: FIA_UAU.2)
FIA_UAU.2	FIA_UID.1	YES (Hierarchy: FIA_UID.2)
FIA_USB.1	FIA_ATD.1	YES
FMT_MOF.1	FMT_SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	YES (FDP_IFC.1)
	FMT_SMR.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1	YES
	FMT_SMF.1	YES
FMT_REV.1(1)	FMT_SMR.1	YES
FMT_REV.1(2)	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES (Hierarchy: FIA_UID.2)
FRU_FLT.1	FPT_FLS.1	NO, This SFR dependency has not been included because while the TOE does provide fault tolerance for the Operational Environment's production network traffic, this functionality is unrelated to preserving the TOE's secure state

Table 10-4: Requirement Dependencies

10.6 Assurance Measures

The SARs for this evaluation have been chosen because they are consistent with the package claim of EAL2. Augmentations to this claim include ALC_FLR.1. ALC_FLR.1 provides assurance that the TOE is updated in a well-defined manner that is consistent with the development security procedures outlined in ALC_DVS.1.

The following table identifies the SARs for this ST.

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Description	TOE Design Specification Document for Gigamon GigaVUE version 7.2.29 Version 2.0	This document describes the security architecture of the TOE.
ADV_FSP.2 Security-enforcing functional specification	Functional Specification Document for Gigamon GigaVUE version 7.2.29 Version 2.0	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.1 Basic Design	TOE Design Specification Document for Gigamon GigaVUE version 7.2.29 Version 2.0	This document describes the architectural design of the TOE.
AGD_OPE.1 Operational User Guidance	• GigaVUE 7.2 User Guide • GigaVUE 7.2 CLI Summary • Citrus v2.2 QuickStart • Citrus™ 2.2 User's Guide • Evaluated Configuration for Gigamon LLC GigaVUE version 7.2.29	These documents describe the operational user guidance for the TOE.
AGD_PRE.1 Preparative Procedures	• GigaVUE 7.2 User Guide • GigaVUE 7.2 CLI Summary • Citrus v2.2 QuickStart • Citrus™ 2.2 User's Guide • Evaluated Configuration for Gigamon LLC GigaVUE version 7.2.29	This document describes the preparative procedures that need to be done prior to installing the TOE.
ALC_CMC.2 Use of a CM system	• GigaVUE Configuration Management Systems (dated June 17, 2011) • Audit Examples for Source Code Files at Gigamon.docx • Gigamon BOM Tree - Rev 8 for Common Criteria.pdf • GLK-320 132-0014 GigaLINK-Fo product change form Revision D1.pdf • gv212_7.2.24_file_list.txt • gv420_7.2.24_file_list.txt	This document describes the authorization controls for the TOE.

Component	Document(s)	Rationale
	- gv2404_7.2.24_file_list.txt - gvgui_7.2.24_file_list.txt	
ALC_CMS.2 Parts of the TOE CM coverage	- GigaVUE Configuration Management Systems (dated June 17, 2011) - Audit Examples for Source Code Files at Gigamon.docx - Gigamon BOM Tree - Rev 8 for Common Criteria.pdf - GLK-320 132-0014 GigaLINK-Fo product change form Revision D1.pdf - gv212_7.2.24_file_list.txt - gv420_7.2.24_file_list.txt - gv2404_7.2.24_file_list.txt - gvgui_7.2.24_file_list.txt	These documents describe the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	GigaVUE Delivery Process v1.4	This document describes product delivery for the TOE and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ALC_FLR.1 Basic flaw remediation	Flaw Remediation Document v1.3	This document describes the processes taken for flaw remediation for the TOE.
ASE_CCL.1 Conformance Claims	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes all of the security objectives for the TOE.

Component	Document(s)	Rationale
ASE_REQ.2 Derived Security Requirements	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes the security problem definition of the Security Target.
ASE_TSS.1 TOE Summary Specification	Gigamon LLC GigaVUE version 7.2.29 Security Target Version 3.0	This document describes the TSS section of the Security Target.
ATE_COV.1 Evidence of Coverage	• Gigamon Common Criteria Test Plan for GigaVUE-420, GigaVUE-2404 and GigaVUE-212 Release 7.2 v.1.6 • Test Cases for Table 7-3 of Security Target (directory)	This document provides an analysis of coverage for the TOE.
ATE_FUN.1 Functional Testing	• Gigamon Common Criteria Test Plan for GigaVUE-420, GigaVUE-2404 and GigaVUE-212 Release 7.2 v.1.6 • Test Cases for Table 7-3 of Security Target (directory)	This document describes the functional tests for the TOE.
ATE_IND.2 Independent Testing - sample	Independent Test Plan GIGAMON LLC GIGAVUE VERSION 7.2.29 v.2.0	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Vulnerability Analysis GIGAMON LLC GIGAVUE VERSION 7.2.29 v.2.0	This document describes the vulnerability analysis of the TOE.

Table 10-5: Assurance Requirements Evidence