National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Gigamon LLC GigaVUE version 7.2.29

Report Number: CCEVS-VR-VID10451-2011
Version 1.0
November 14, 2011

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

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

ACKNOWLEDGEMENTS

Validation Team

John Nilles, Senior Validator
Aerospace

Ralph Broom, Lead Validator
Noblis

Ken Stutterheim, Validator Observer
Aerospace

Common Criteria Testing Laboratory

Chris Gugel, Lead Evaluator
Booz Allen Hamilton (BAH)
Linthicum, Maryland

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is Gigamon LLC GigaVUE version 7.2.29. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in September 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.1 (Flaw reporting procedures). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

GigaVUE version 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 GigaVUE appliance, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The Gigamon LLC GigaVUE version 7.2.29 Security Target version 3.0, dated 26 August 2011 identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the Gigamon appliance by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	Gigamon LLC GigaVUE version 7.2.29
Sponsor & Developer	Gigamon LLC, Milpitas, CA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	4 October 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2 Augmented ALC_FLR.1
Description	The TOE is the GigaVUE appliance, which is a security software product developed by Gigamon LLC as a Security Management system.
Disclaimer	The information contained in this Validation Report is not an endorsement of the GigaVUE product by any agency of the U.S. Government, and no warranty of the Security Management product is either expressed or implied.
PP	None
Evaluation Personnel	Seyithan Ayhan Justin Fisher Christopher Gugel Kevin Micciche John Schroeder Amit Sharma Andrea Wright
Validation Body	NIAP CCEVS

3 Identification

The product being evaluated is Gigamon LLC GigaVUE version 7.2.29.

4 Security Policy

4.1 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. The TOE explicitly allows all roles to read audit data within the TOE. 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. In the event of any of these changing or occurring, the TOE sends an SNMP trap.

4.2 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.

4.3 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 and is protected by the separation of the data and control planes. 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. Attached tools are also denied a return path back into the TOE. 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.

4.4 Identification and Authentication

All TOE users must be identified and authenticated before performing any TSF-relevant actions. 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. All native 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).

4.5 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 all 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.

4.6 Protection of the TSF

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

4.7 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.

4.8 TOE Access

All users are shown a configurable banner before being allowed to authenticate to the TOE. 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.

4.9 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 Clonal connections are protected from modification and disclosure by using these cryptographic methods.

5 Threats, OSPs, and Assumptions

5.1 Threats to Security

Table 1 summarizes the threats that the evaluated product addresses.

Table 1 – Threats

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.
An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
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.
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
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.
Users, whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.
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.

5.2 Organizational Security Policies

Table 2 – Organizational Security Policies

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.

5.3 Personnel Assumptions

Table 3 – Personnel Assumptions

One or more authorized administrators are assigned to install, configure and manage the TOE and the security of the information it contains.
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.
System Administrators exercise due diligence to patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks.
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.

5.4 Physical Assumptions

Table 4 – Physical Assumptions

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

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 extended in this case).
- As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the Gigamon LLC GigaVUE version 7.2.29 product that is comprised of one or more of the following:

- GigaVUE-212 model
- GigaVUE-420 model
- GigaVUE-2404 model

6.1 System Requirements

The following components are required on the appliances for the TOE:

GigaVUE-212 model

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

GigaVUE-420 model

Standard	Modular
Redundant Power Supplies & Fans	Expansion slots: 8

Serial Console port (excluded)
Management Ethernet port
(4) 1 Gb ports (electrical or optical)
O/S: ECOS v2.0
	• (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)

GigaVUE-2404 model

Standard	Modular
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 O/S: ECOS v2.0	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)

6.2 Cryptographic Assurance

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to FIPS 140-2 cryptographic standards as part of this evaluation. The vendor has asserted that all cryptography used by the product has been tested.

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

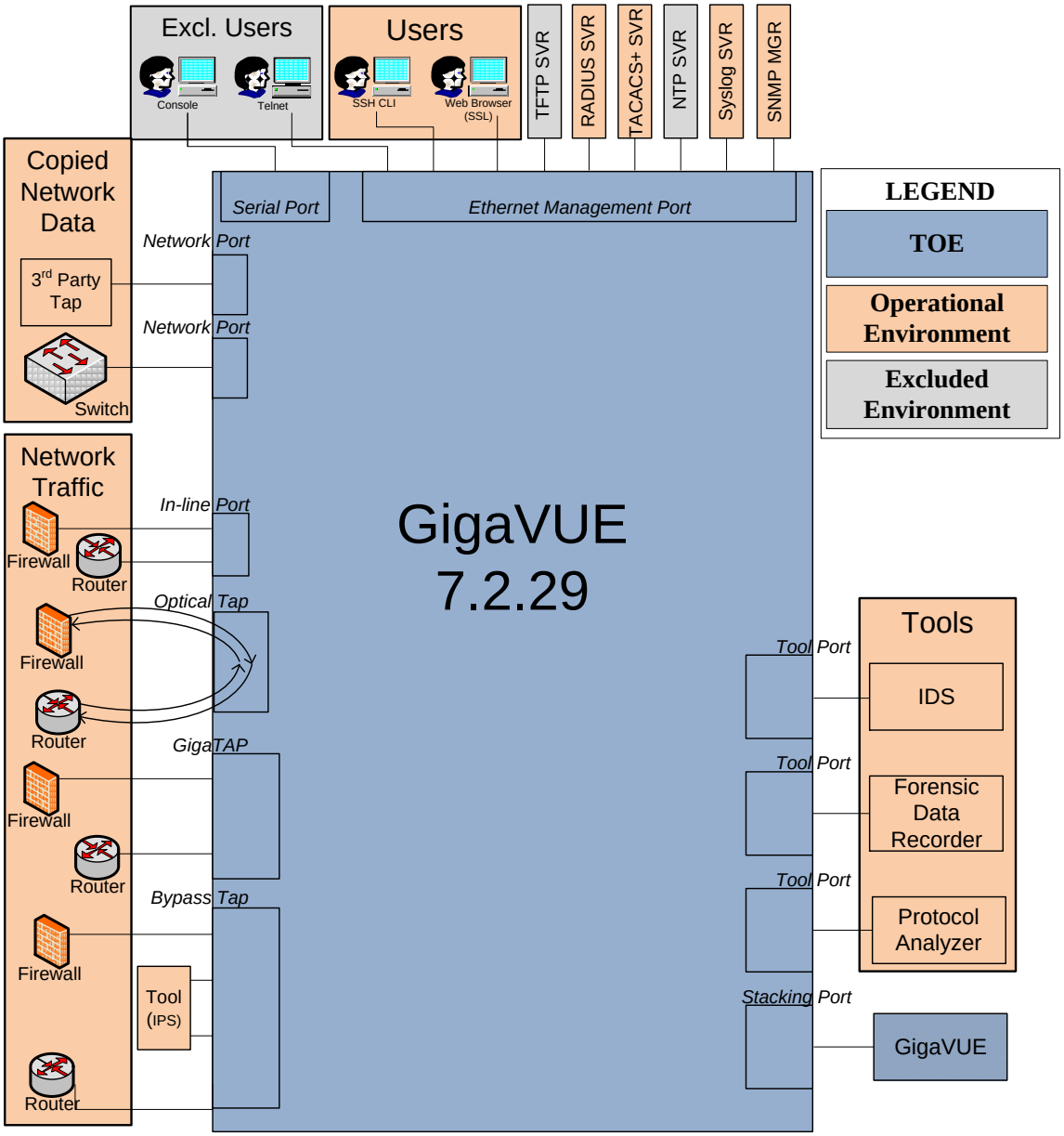

Figure 1 – TOE Boundary for Gigamon LLC GigaVUE version 7.2.29

7.1 TOE Components

The TOE is a hardware appliance and software based product which can stand alone or be placed in a stacking configuration. Thus, each GigaVUE model described in Section 6 is the TOE and the only component of the TOE. When there are multiple GigaVUEs in a stacked configuration, each GigaVUE represents a single TOE component in the stacked configuration.

8 Documentation and Delivery

The NIAP-certified Gigamon GigaVUE product is acquired via normal sales channels, and physical delivery of the TOE is coordinated with the end customer by Gigamon LLC The product is provided to normal customers as an appliance. The vendor provides documentation on their support website, http://www.gigamon.com/customer-portal. Not included within this documentation is the 'Evaluated Configuration for Gigamon LLC GigaVUE version 7.2.29' which can be requested from Gigamon by contacting customer support via phone (408) 263-2024 or email support@Gigamon.com and opening a support ticket. This guidance must be referenced to place the product within the CC evaluated configuration.

The following documents were included within the scope of the evaluation:

- 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

9 IT Product Testing

9.1 Functional Testing

9.1.1 Functional Test Methodology

The test team's test approach is to test the security mechanisms of Gigamon by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

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

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team executed a subset of the vendor functional testing. It has been determined that a sampling of the tests can be taken such that each SFR is tested to an appropriate level. The evaluation team also supplemented the vendor test cases with their own independent test plan to address any gaps in the coverage of SFRs.

The evaluators have determined that the vendor functional testing is a majority representation of the SFR and TSS claims made in the ST regarding the security functional requirements. However, the evaluators felt that additional testing was needed in order to verify the validity of the developer test environment and to provide additional assurance of the functionality of the TOE.

9.1.2 Functional Results

During the course of the evaluation, the Booz Allen evaluation team reviewed the vendor’s functional testing and determined that all *security relevant* TOE external interfaces were tested and a majority of the claimed functionality was tested by the vendor. The evaluation team then created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing developed by the evaluators. The evaluators test suite emphasized on the product’s primary functionality and any areas that required testing for claimed functionality. Based upon the results of the vendor and evaluator testing; it has been determined that the product functionally operates as described.

9.2 Vulnerability Testing

9.2.1 Vulnerability Test Methodology

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  This test attempted to intercept any TOE involved network traffic. The attack machine executed an arp poisoning attack so that all network traffic between two nodes on a switched LAN were tunneled through the attack machine before it reaches its destination. A sniffer will then be used to analyze the network traffic and attempt to view any confidential information that may be passing over the network.
- Port Scanning
  This test attempted to identify any way to subvert the security of the TOE by executing a side channel attack. A port scanner was run against all TOE systems in an attempt to identify any open ports. Any port on a system that accepts external connections could potentially represent an attack vector. This test attempted to identify any such ports and attempted to enumerate them to determine their original purpose.
- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
- Vulnerability Scanner (Retina)
  This test used the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
- Denial of Service – TCP Malformed Packet Flooding
  This attack attempted to exercise the stability of the IP stack and its components by sending a large amount of TCP packets and malformed TCP packets in an attempt to overload the TOE. If successful, the TOE would crash and not allow any connections until the TOE is rebooted.
- Unauthenticated Access / Directory Traversal Attack
  This test used “URL hacking” to attempt to access protected TOE resources by injecting unexpected input into requests that are being sent to the TOE. This was done using two different approaches to URL exploitation.
- Web Server Vulnerability Scanner (Nikto)

This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interface.
This test executed automated SQL Injection, Cross Site Scripting and Cross Site Request Forgery attacks against the TOE web server using the Webscarab program. This program runs as a proxy and intercepts all traffic between a web client and a server. It used this information to determine any fields or variables that could be prone to attack.

9.2.2 Vulnerability Results

During the vulnerability testing, the evaluation team determined that there were no issues discovered that could affect the security posture of a deployed system.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the Gigamon LLC GigaVUE version 7.2.29 TOE meets the security requirements contained in the Security Target.

The criteria against which the GigaVUE TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the Gigamon LLC GigaVUE version 7.2.29 TOE is EAL2 augmented with ALC_FLR.1. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed on 4 October 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

11 Validator Comments/Recommendations

11.1 RADIUS Server Residual Vulnerability

During the evaluation team's vulnerability analysis, they discovered a potential vulnerability when the TOE is used in conjunction with a RADIUS Server. It is important to note that the following potential vulnerability is not a product of the TOE but of the MD5 technology that has been incorporated into RADIUS.

"The Response Authenticator is essentially an ad hoc MD5 based keyed hash. This primitive facilitates an attack on the shared secret. If an attacker observes a valid Access-Request packet and the associated Access-Accept or Access-Reject packet, they can launch an off-line exhaustive attack on the shared secret. The attacker can pre-compute the MD5 state for (Code+ID+Length+RequestAuth+Attributes) and then resume the hash once for each shared secret guess. The ability to pre-compute the leading sections of this keyed hash primitive reduces the computational requirements for a successful attack." – Joshua Hill (http://www.untruth.org/~josh/security/radius/radius-auth.html)

As RADIUS authentication uses MD5 to protect a shared secret password, the TOE user should establish policy to select non-dictionary RADIUS passwords, and protect the authentication exchange either by conducting it on a trusted administrative network or protecting the channel via IPSec, VPN, etc.

This is considered to be an acceptable residual vulnerability by the Common Criteria process. Even though the computational requirements of this attack are reduced, it still requires an exhaustive search in order to reveal the shared secret. In addition, there do not appear to be any automated tools to facilitate such an attack requiring an increased level of sophistication on the part of the attacker. Also, the RADIUS server communicates through the TOE via its management interface (control plane) which is separated and non-accessible from the data plane. Therefore, an attacker would have to have access to the management network in order to sniff the required packets. Because of the time to exploit, the expertise required, and the window of opportunity, this issue is considered to be above the Basic attack potential evaluated in accordance with a Common Criteria EAL 2 evaluation.

11.2 Secure Installation and Configuration Documentation

The "Evaluated Configuration for Gigamon LLC GigaVUE version 7.2.29" defines the recommendations and secure usage directions for the TOE as derived from testing.

12 Security Target

The security target for this product's evaluation is Gigamon LLC GigaVUE version 7.2.29 Security Target, Version 3.0, 26 August 2011.

13 List of Acronyms

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

14 Terminology

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.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. Gigamon LLC GigaVUE version 7.2.29 Security Target, Version 3.0, August 26, 2011
6. Evaluation Technical Report for a Target of Evaluation "Gigamon LLC GigaVUE 7.2.29" Evaluation Technical Report v3.0 dated September 6 2011.