National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

for

Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches

Report Number: CCEVS-VR-VID10567-2014
Dated: December 5, 2014
Version: 1.0

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

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation Hewlett-Packard (HP) Company 5900 Series, and 5920 Series both running Comware V7.1.045 Release 2311 P03, HP 10500 Series running Comware V7.1.045 Release 2111 P05, and HP 12500 Series Switches running Comware 7.1.045, Release 7328 P03. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in December 2014. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE is a hardware and software solution that consists of the Hewlett-Packard (HP) Company 5900 Series, and 5920 Series both running Comware V7.1.045 Release 2311 P03, HP 10500 Series running Comware V7.1.045 Release 2111 P05, and HP 12500 Series Switches running Comware 7.1.045, Release 7328 P03. The network on which it resides is considered part of the operational environment.

Product Series	Specific Devices
HP 5900	HP 5900AF-48XG-4QSFP+ Switch HP 5900AF-48XGT-4QSFP+ Switch HP 5900AF-48G-4XG-2QSFP+ Switch
HP 5920	HP 5920AF-24XG Switch

Product Series	Specific Devices
HP 10500 Series Chassis' with HP 10500 Type A Main Processing Unit with Comware v7 Operating System (JG496A)	HP 10504 Switch Chassis HP 10508 Switch Chassis HP 10508-V Switch Chassis HP 10512 Switch Chassis
HP 12500 Series Chassis' with HP 12500 Type A Main Processing Unit with Comware v7 Operating System (JG497A)	HP 12504 (AC) Switch Chassis HP 12504 (DC) Switch Chassis HP 12508 (AC) Switch Chassis HP 12508 (DC) Switch Chassis HP 12518 (AC) Switch Chassis HP 12518 (DC) Switch Chassis

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Hewlett-Packard (HP) Company 5900 Series and 5920 Series both running Comware V7.1.045 Release 2311 P03, HP 10500 Series running Comware V7.1.045 Release 2111 P05, and HP 12500 Series Switches running Comware 7.1.045, Release 7328 P03.
Sponsor & Developer	Hewlett-Packard Development Company, L.P. 11445 Compaq Center Drive West Houston, Texas 77070
CCTL	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	December 2014
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Network Devices, Version 1.1, 8 June 2012 Security Requirements for Network Devices Errata #2, 13 January 2013
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches by any agency of the U.S. Government and no warranty of Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches is either expressed or implied.
Evaluation Personnel	Katie Sykes Chris Keenan Pascal Patin Greg Beaver
Validation Personnel	Patrick Mallett, PHD Jerome Myers, PHD

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target
ST Version	1.0
Publication Date	October 28, 2014
Vendor	Hewlett-Packard Company
ST Author	Leidos (formerly SAIC)
TOE Reference	Hewlett-Packard (HP) Company 5900 Series and 5920 Series both running Comware V7.1.045 Release 2311 P03, HP 10500 Series running Comware V7.1.045 Release 2111 P05, and HP 12500 Series Switches running Comware 7.1.045, Release 7328 P03.
TOE Hardware Models	HP 5900AF-48XG-4QSFP+ Switch HP 5900AF-48XGT-4QSFP+ Switch HP 5900AF-48G-4XG-2QSFP+ Switch HP 5920AF-24XG Switch HP 10504 Switch Chassis HP 10508 Switch Chassis HP 10508-V Switch Chassis HP 10512 Switch Chassis HP 12504 (AC) Switch Chassis HP 12504 (DC) Switch Chassis HP 12508 (AC) Switch Chassis HP 12508 (DC) Switch Chassis HP 12518 (AC) Switch Chassis HP 12518 (DC) Switch Chassis
TOE Software Version	Comware V7.1.045 Release 2311 P03 (5900 Series and 5920 Series), Comware V7.1.045 Release 2111 P05 (10500 Series) Comware 7.1.045, Release 7328 P03(12500 Series)
Keywords	Switch, Layer 2, Layer 3

2.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

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

2.2 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operational environment are intended to fulfill:

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

3 Architectural Information

The Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches comprising the TOE share a common software code base, called Comware. Comware is special purpose appliance system software that implements various networking technologies, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; VLANs; IRF routing; and Quality of Service (QoS). The evaluated version of Comware is V7.1. It should be noted that although Comware can run on a variety of underlying architectures but the only underlying architecture evaluated is Linux.

Comware V7.1 implements full modularization and multi-process applications, and provides the following benefits:

- Full modularization—Brings improvements in system availability, virtualization, multi-core multi-CPU applications, distributed computing, and dynamic loading and upgrading.
- Openness—Comware V7.1 is a generic, open system based on Linux.
- Improved operations—Comware V7.1 improves some detailed operations. For example, it uses preemptive scheduling to improve real-time performance.

Comware V7.1 optimizes the following functions:

- Virtualization—Supports N:1 virtualization.
- In Service Support Updates (ISSU)—Supports ISSU for line cards.
- Auxiliary CPU and OAA—Improves scalability for devices.

In addition, Comware V7.1 supports new technologies for data centers, including TRILL and EVB.

Comware V7.1 comprises four planes: management; control; data; and infrastructure.

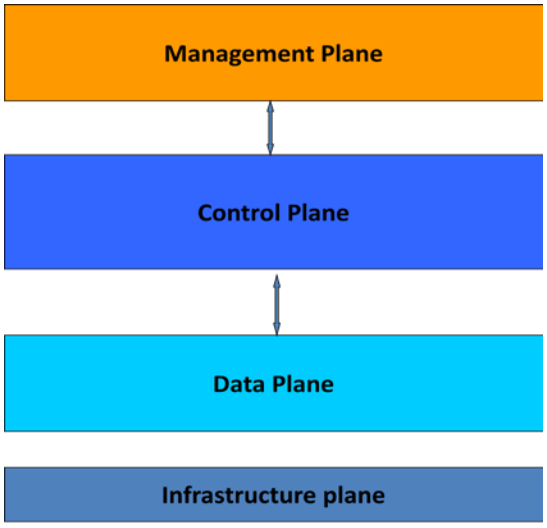

Figure 1: Comware V7.1 Architecture

- **Infrastructure**—the infrastructure plane provides basic Linux services and Comware support functions. Basic Linux services comprise basic Linux functions, C language library functions,

data structure operations, and standard algorithms. Comware support functions provide software and service infrastructure for Comware processes, including all basic functions.

- **Data**—the data plane provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.
- **Control**—the control plane comprises all routing, signaling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- **Management**—the management plane provides a management interface for operators to configure, monitor, and manage Comware V7.1. The management interface comprises a Command Line Interface (CLI) accessed using SSH.

The Comware V7.1 software is further decomposed into subsystems designed to implement applicable functions. For example, there are subsystems dedicated to the security management interface. There are also subsystems dedicated to the IPv4 and IPv6 network stacks as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE implements NIST-validated cryptographic algorithms that support the IPsec and SSH protocols as well as digital signature services that support the secure update capabilities of the TOE. Otherwise, the TOE implements various network switching protocols and functions.

The various TOE devices include the same security functions. The salient differences between the devices are the available ports and port adapters, primarily representing differences in numbers, types, and speeds of available network connections.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

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

4.1 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. The TOE can be configured to rely on and utilize a number of other components in its operational environment:
    a. Syslog server—to receive audit records when the TOE is configured to deliver them to an external log server.
    b. RADIUS and TACACS servers—the TOE can be configured to use external authentication servers.
    c. Management Workstation—the TOE supports remote access to the CLI over SSHv2. As such, an administrator requires an SSHv2 client to access the CLI remotely.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

5.1 Security Audit

The TOE is able to generate audit records of security relevant events. The TOE can be configured to store the audit records locally so they can be accessed by an administrator or alternately to send the audit records to a designated log server.

5.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that to be in the evaluated configuration, the TOE must be configured in FIPS mode, which ensures the TOE's configuration is consistent with the FIPS 140-2 standard.

5.3 User Data Protection

The TOE performs network switching and routing functions, passing network traffic among its various physical and logical (e.g., VLAN) network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE is designed to ensure that it does not inadvertently reuse data found in network traffic.

5.4 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface (SSHv2) for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of trusted RADIUS and TACACS servers in the operational environment to support, for example, centralized user administration.

5.5 Security Management

The TOE provides a CLI to access its security management functions. Security management commands are limited to administrators and are available only after they have provided acceptable user identification and authentication data to the TOE.

5.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of a Syslog server or authentication servers in the operational

environment, the communication between the TOE and the operational environment component is protected using encryption.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

5.7 TOE Access

The TOE can be configured to display an informative banner that will appear prior to authentication when accessing the TOE via the console or SSH interfaces. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

5.8 Trusted Path/Channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured.

The TOE protects communication with external IT entities, including audit and authentication servers, using IPsec connections, which prevent unintended disclosure or modification of data.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target, Version 1.0, 28 October 2014

Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches on Comware V7, V1.06, dated 12/2/2014

Command Reference for CC Supplement, Revision 1.2, dated 10/14/2014

Configuration Guide for CC Supplement, Revision 1.3, dated 10/14/2014

Comware V7.1 Platform System Log Messages, Revision .25, dated 4/21/2014.

The links in Appendix A for the Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target can be used to find the full set of documentation for the evaluated switch series. The following documents were specifically examined during the evaluation:

- *ACL and QoS Command Reference*
- *ACL and QoS Configuration Guide*
- *Fundamentals Command Reference*
- *Fundamentals Configuration Guide*
- *High Availability Command Reference*
- *High Availability Configuration Guide*
- *Installation Guide*
- *IP Multicast Command Reference*
- *IP Multicast Configuration Guide*
- *IRF Command Reference*
- *IRF Configuration Guide*
- *Layer-2 LAN Switching Command Reference*
- *Layer-2 LAN Switching Configuration Guide*
- *Layer-3 IP Routing Command Reference*
- *Layer-3 IP Routing Configuration Guide*
- *Layer-3 IP Services Command Reference*
- *Layer-3 IP Services Configuration Guide*
- *Network Management and Monitoring Command Reference*
- *Network Management and Monitoring Configuration Guide*
- *Security Command Reference*
- *Security Configuration Guide*

On-line documentation for the TOE devices can be found via the following URLs:

5900/5920 Switch Series

The following documents for the 5900/5920 Switch series can be found under the *General Reference* section of the 5900 Switch Series documentation page on the HP Web site. The link is provided below.

- R2307-HP 5900 Security Command Reference, 17 Jan 2014
- R2307-HP 5900 Fundamentals Command Reference 17 Jan 2014
- R2307-HP 5900 ACL and QoS Command Reference, 17 Jan 2014
- R2307-HP 5900 Layer-3 IP Services Command Reference, 17 Jan 2014

The following documents for the 5900/5920 Switch series can be found under the *Setup and Install* section of the 5900 Switch Series documentation page on the HP Web site. The link is provided below.

- R2307-HP 5900 Security Configuration Guide, 17 Jan 2014
- R2307-HP 5900 Fundamentals Configuration Guide, 17 Jan 2014
- R2307-HP 5900 Network Management and Monitoring Configuration Guide, 17 Jan 2014
- HP 5900/5920 Switch Series Installation Guide, 12 Feb 2014

http://h20566.www2.hp.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5221896#manuals

10500 Switch Series

The following documents for the 10500 Switch series can be found under the *General Reference* section of the 10500 Switch Series documentation page on the HP Web site. The link is provided below.

- R211x-HP 10500 Switch Series Security Command Reference, 17 Aug 2014
- R211x-HP 10500 Switch Series Fundamentals Command Reference, 17 Aug 2014
- R211x-HP 10500 Switch Series ACL and QoS Command Reference, 17 Aug 2014
- R211x-HP 10500 Switch Series Layer-3 IP Services Command Reference, 17 Aug 2014

The following documents for the 10500 Switch series can be found under the *Setup and Install* section of the 10500 Switch Series documentation page on the HP Web site. The link is provided below.

- R211x-HP 10500 Switch Series Security Configuration Guide, 18 Aug 2014
- R211x-HP 10500 Switch Series Fundamentals Configuration Guide, 18 Aug 2014
- R211x-HP 10500 Switch Series Network Management and Monitoring Configuration Guide, 18 Aug 2014
- HP 10500 Switch Series Installation Guide, 20 Aug 2014

http://h20566.www2.hp.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5117468#manuals

12500 Switch Series

The following documents for the 12500 Switch series can be found under the *General Reference* section of the 12500 Switch Series documentation page on the HP Web site. The link is provided below.

- R1825P01-HP 12500 Switch Series Security Command Reference, 2 Apr 2013

- R1825P01-HP 12500 Switch Series Fundamentals Command Reference 2 Apr 2013
- R1825P01-HP 12500 Switch Series ACL and QoS Command Reference, 2 Apr 2013
- R1825P01-HP 12500 Switch Series Layer-3 IP Services Command Reference, 2 Apr 2013

The following documents for the 12500 Switch series can be found under the *Setup and Install* section of the 12500 Switch Series documentation page on the HP Web site. The link is provided below.

- R1825P01-HP 12500 Switch Series Security Configuration Guide, 2 Apr 2013
- R1825P01-HP 12500 Switch Series Fundamentals Configuration Guide, 2 Apr 2013
- R7128-HP 12500 Switch Series Network Management and Monitoring Configuration Guide, 30 Nov 2012
- HP FlexFabric 12500E Switch Series Installation Guide, 25 Sep 2014

http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?sp4ts.oid=4177453&ac.admitted=1413205932488.876444892.199480143

Supporting TOE Guidance Documentation

Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target, Version 1.0, 28 October 2014

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Evaluation Team Test Report for Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches, Version 2.0, December 11, 2014

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2.

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDPPv1.1 and Security Requirements for Network Devices Errata #2. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the developer facility and via Virtual Rooms in four separate sessions.

Testing took place in four sessions:

- Session 1: August 18-22, 2014 at the Hewlett Packard facility in Boston, MA.

  August 2014 at Leidos facility in Columbia MD
- Session 2: September 29 – October 3, 2014 at the Hewlett Packard facility in Boston, MA
- Session 3: October 2014 at the Leidos facility in Columbia, MD
- Session 4: October 2014 –Virtual Rooms

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for NDPPv1.1 and Security Requirements for Network Devices Errata #2 are fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE is Hewlett-Packard Company 5900 Series, and 5920 Series both running Comware V7.1.045 Release 2311 P03, 10500 Series running Comware V7.1.045 Release 2111 P05, and 12500 Series Switches running Comware 7.1.045, Release 7328 P03, as installed and configured according to the Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches on Comware V7 as well as the supporting guidance documentation identified in Section 6.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Network Devices, Version 1.1, 8 June 2012 and Security Requirements for Network Devices Errata #2, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 4: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

Administrators are cautioned to pay particular attention to the Common Criteria preparative procedures when configuring the devices. Administrators should plan for the fact that log records are not buffered for transmission to the syslog server. Therefore, if the connection to the syslog server goes down, generated log records are not queued and will not be transmitted to the syslog server when the connection is re-established. The document, Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches on Comware V7, v1.06, December 2, 2014, provides several configuration options that help reduce the risk that audit records will be lost.

11 Annexes

Not applicable.

12 Security Target

Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target, Version 1.0, October 28, 2014

13 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
AAR	Assurance Activities Report
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CC Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CLI	Command Line Interface
EP	Extended Package
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IPsec	Internet Protocol security
IT	Information Technology
LAN	Local Area Network
NDPP	Network Device Protection Profile
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell version 2
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VPN	Virtual Private Network
VR	Validation Report
WAN	Wide Area Network

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches Security Target, v1.0, October 28, 2014

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Hewlett-Packard Company 5900 Series, 5920 Series, 10500 Series, and 12500 Series Switches, parts 1 and 2 (and associated AAR and test report), version 2.0, December 11, 2014.