National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches

Report Number: CCEVS-VR-VID10672-2016
Dated: 4 March 2016
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

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
The Aerospace Corporation

Ken Stutterheim
The Aerospace Corporation

Dianne Hale
National Information Assurance Partnership

Common Criteria Testing Laboratory

Leidos Inc. (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report is intended to assist the end-user of this Information Technology (IT) product and any security certification agent for that end-user in determining the suitability of this product in their environment. End-users should review the Security Target (ST) ([6]), 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 of the Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches with Comware 7.1 (the Target of Evaluation, or TOE)[1]. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the 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 the Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches with Comware 7.1 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in February 2016. 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 ([1], [2], [3], [4]) and assurance activities specified in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012, as amended by Errata #3 dated 3 November 2014 ([5]), and including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1. The conduct of 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 TOE is a hardware and software solution that consists of the Comware 7.1 software running on any of the Hewlett Packard Enterprise appliances listed here according to the model series.

The 5900 Series devices in the evaluated configuration are as follows:

- HP 5900AF-48XG-4QSFP+ Switch (JG772A)
- HP 5900AF-48XGT-4QSFP+ Switch (JG336A)
- HP 5900AF-48G-4XG-2QSFP+ Switch (JG510A)
- HP FlexFabric 5900CP-48XG-4QSFP+ Switch (JG838A).

The 5920 Series device in the evaluated configuration is the HP 5920AF-24XG Switch (JG296A).

The 5930 Series devices in the evaluated configuration are as follows:

- HP FlexFabric 5930-32QSFP+ Switch (JG726A)

[1] On November 1, 2015, Hewlett-Packard became two separate companies: Hewlett Packard Enterprise and HP Inc. The network products are part of the new Hewlett Packard Enterprise. The former HP network switches and routers are undergoing product rebranding. The rebranding is not complete in the documentation and on the websites. The TOE maybe referred to with the suffix “HP”, “HP FlexFabric”, “HPE” or “HPE FlexFabric”. For the purpose of this evaluation, these name variations are used interchangeably and refer to the same product.

- HP FlexFabric 5930-4Slot Switch (JH179A)
- HP FlexFabric 5930 2QSFP+ 2-slot Switch (JH178A).

The 10500 Series devices in the evaluated configuration are as follows:

- HP 10504 Switch Chassis (JC613A)
- HP 10508 Switch Chassis (JC612A)
- HP 10508-V Switch Chassis (JC611A)
- HP 10512 Switch Chassis (JC748A)

Note: Each chassis requires a compatible Main Processing Unit. The following are included in the evaluated configuration:

- HP 10500 Type A Main Processing Unit with Comware v7 Operating System (JG496A)
- HP 10500 Type D Main Processing Unit with Comware v7 Operating System (JH198A)
- HP 10500 Type D TAA-compliant Main Processing Unit with Comware v7 Operating System (JH206A)

The 12500 Series devices in the evaluated configuration are as follows, each with the HP 12500 Type A Main Processing Unit with Comware v7 Operating System (JG497A):

- HP 12504 (AC) Switch Chassis (JC654A)
- HP 12504 (DC) Switch Chassis (JC655A)
- HP 12508 (AC) Switch Chassis (JF421C)
- HP 12508E (AC) Switch Chassis (JG782A)
- HP 12508 (DC) Switch Chassis (JC652A)
- HP 12508E (DC) Switch Chassis (JG783A)
- HP 12518 (AC) Switch Chassis (JF430C)
- HP 12518E (AC) Switch Chassis (JG784A)
- HP 12518 (DC) Switch Chassis (JC653A)
- HP 12518E (DC) Switch Chassis (JG785A).

Note: Each 12500 Series chassis requires one of the following:

- HP 12500 Type A Main Processing Unit with Comware v7 Operating System (JG497A)
- HP 12500, LSTM5MRPNC, Management and Route Unit with OAM Module, Overseas Version (JC072B)
- HP FlexFabric 12500E, LSTM5MRPNE1, Management and Route Process Unit, Overseas Version (JG802A)

The 12900 Series devices in the evaluated configuration are as follows:

- HP FlexFabric 12910 Switch AC Chassis with 12910 Main Processing Unit (JG621A)
- HP FlexFabric 12916 Switch AC Chassis with 12916 Main Processing Unit (JG634A).

Each series of switches included in the TOE consists of a set of distinct devices that vary primarily according to power delivery, performance, and port density. Each device in the TOE is a stand-alone gigabit Ethernet switch that implements network layers 2 and 3 switching, service and routing operations.

The Leidos evaluation team determined that the TOE is conformant to *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014. The TOE, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches Security Target, Version 1.0, 16 February 2016. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([9]) and associated proprietary test report ([10]) produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation results showed that the TOE satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014, and that the assurance activities specified in the Protection Profile have been performed appropriately. 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 (ETR) ([8]) are consistent with the evidence produced.

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).

Table 1 provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Summary

Evaluated Product:	Hewlett Packard Enterprise Switches as follows: • 5900 Series, 5920 Series, and 5930 Series running Comware V7.1.045 Release 2423 • 10500 Series running Comware V7.1.045 Release 7170 • 12500 Series Switches running Comware 7.1.045 Release 7376 • 12900 Series running Comware 7.1.045 Release 1138 P02
Sponsor & Developer:	Hewlett Packard Enterprise 11445 Compaq Center Drive West Houston, Texas 77070 United States
CCTL:	Leidos (formerly SAIC) Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	February 2016
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.
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, as amended by Errata #3 dated 3 November 2014
Evaluation Personnel:	Katie Sykes Kevin Steiner Cody Cummins Robert Russ Tony Apted
Validation Body:	National Information Assurance Partnership CCEVS

2.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0004: FCS_TLS_EXT Man-in-the-Middle Test - This Technical Decision removes the FCS_TLS_EXT man-in-the-middle tests for the NDPP (FCS_TLS_EXT.1.1, Test 2), pending development of new TLS requirements and assurance activities and identification of suitable test tools.
- TD0005: FPT_ITT Test 3 Resolution - This Technical Decision removes the need to perform Test 3 associated with FPT_ITT.1 in NDPP, consistent with the test requirements for FTP_ITC.1 and FTP_TRP.1.
- TD0011: FCS_SSH_EXT.1.4 Clarification - The SFR requires that the SSH transport implementation use specific encryption algorithms. Can the restriction to those algorithms be reliant upon configuration of the SSH client? No. The restrictions must be implemented by the TOE.
- TD0012: FCS_SSH_EXT.1.4 - Algorithms not identified in FCS_SSH_EXT.1.4 must not be allowed; other cipher suites (such as 3DES-CBC) must be disabled in evaluated configurations. The Assurance Activities associated with this requirement must verify that connection attempts with algorithms not listed in FCS_SSH_EXT.1.4 are denied. The NDPP will be updated to reflect this decision.
- TD0017: NDPP Audit Shutdown - This Technical Decision allows for the use of a startup audit record to indicate audit shutdown in the event of an uncontrolled shutdown.
- TD0026: FPT_TUD_EXT.1 - This Technical Decision allows for the administrator following TOE guidance to reject an illegitimate update detected by the TOE, in addition to the TOE rejecting the update automatically.
- TD0032: FCS_SSH_EXT.1.2 – SFR will be rewritten to conditionally require password-based authentication

2.2 Threats

The ST references the Protection Profile for Network Devices to identify 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.

2.3 Organizational Security Policies

The ST references the Protection Profile for Network Devices to identify 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 various routers comprising the TOE share a common software code base, called Comware. Comware is special purpose appliance system software that implements networking technology.

Comware V7.1 comprises four planes, as depicted in Figure 1 below: management plane; control plane; data plane; and infrastructure plane:

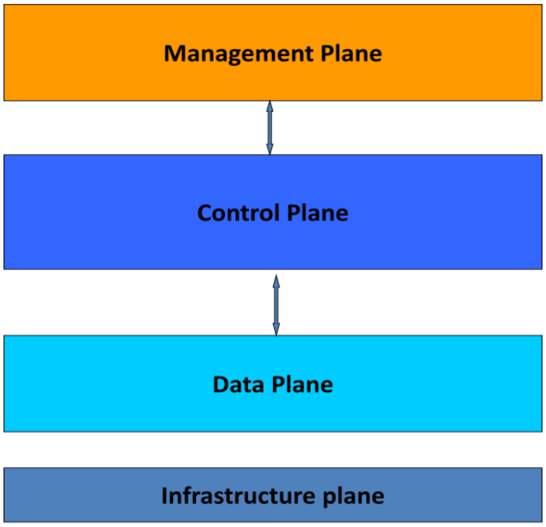

Figure 1: Comware V7.1 Architecture

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 infrastructures for Comware processes, including all basic functions.

The **Data Plane** provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.

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.

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 locally via the console port and remotely via Secure Shell (SSH).

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 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 references the Protection Profile for Network Devices to identify 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 PP and performed by the evaluation team).
2. This evaluation covers only the specific device models and software versions 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 PP. 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 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 proprietary Final ETR documents.

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 in the evaluated configuration, the TOE must be configured in FIPS mode, which ensures the TOE uses only FIPS-approved and NIST-recommended cryptographic algorithms.

5.3 User Data Protection

The TOE performs network switching and routing functions, passing network traffic among its various physical and logical network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE ensures that it does not inadvertently reuse data found in network traffic.

5.4 Identification and Authentication

The TOE requires 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 local definition of administrators with usernames and passwords. Additionally, the TOE can be configured to utilize the services of trusted RADIUS and TACACS+ servers in the operational environment to support, for example, centralized user administration. The TOE supports the use of text-based pre-shared keys for IKE peer authentication.

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 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 (for example, 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 network peers, such as audit and authentication servers, using IPsec connections to prevent unintended disclosure or modification of data.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. Only those documents that were used to place the TOE into its evaluated configuration are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration

In particular, the following Common Criteria specific guides provide the security-related guidance documentation for all devices in the evaluated configuration:

- *Preparative Procedures for CC NDPP Evaluated HPE 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switch Modules based on Comware V7.1*, Version 1.01, 16 Feb 2016
- *Command Reference for CC Supplement*, Revision 1.05, 22 Jan 2016
- *Configuration Guide for CC Supplement*, Revision 1.6, 22 Jan 2016
- *Comware V7 Platform System Log Messages*, Revision 1.00, 21 Apr 2014.

The links in Table 2 below for each series can be used to find the full set of documentation for each of the evaluated router series. Note that only the documents listed above were examined during the course of the evaluation, and are the approved documents for configuring and using the TOE in its evaluated configuration.

Table 2: Product Documentation Links

Product Family	Link to Series Documentation
HPE 5900 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5221896#manuals
HPE 5920 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5221896#manuals
HPE 5930 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=6604154#manuals
HPE 10500 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5117468#manuals
HPE 12500 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=4177453#manuals
HPE 12900 series	http://h20566.www2.hpe.com/portal/site/hpsc/public/psi/home/?sp4ts.oid=5443167#manuals

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Evaluation Team Test Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches*, Version 1.0, 16 February 2016 and as summarized in the document *Assurance Activities Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches*, Version 1.0, 16 February 2016

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 the Protection Profile for Network Devices, Version 1.1, 8 June 2012, as amended by Errata #3 dated 3 November 2014. As such, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the PP.

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, documented the results in the proprietary Team Test Report identified above and provided the report to the validation team and NIAP.

Due to the size of the devices, which precluded shipping to the Leidos CCTL, testing of the 12500 and 12900 Series Switch Chassis was conducted independently by Leidos personnel under controlled conditions at the vendor's facility in Littleton, MA, from 14 – 18 December, 2015. Testing of the other devices in the evaluated configuration took place at the Leidos facility in Columbia, Maryland from 22 December 2015 – January 21, 2016.

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.

The configuration depicted in Figure 2 was used for testing.

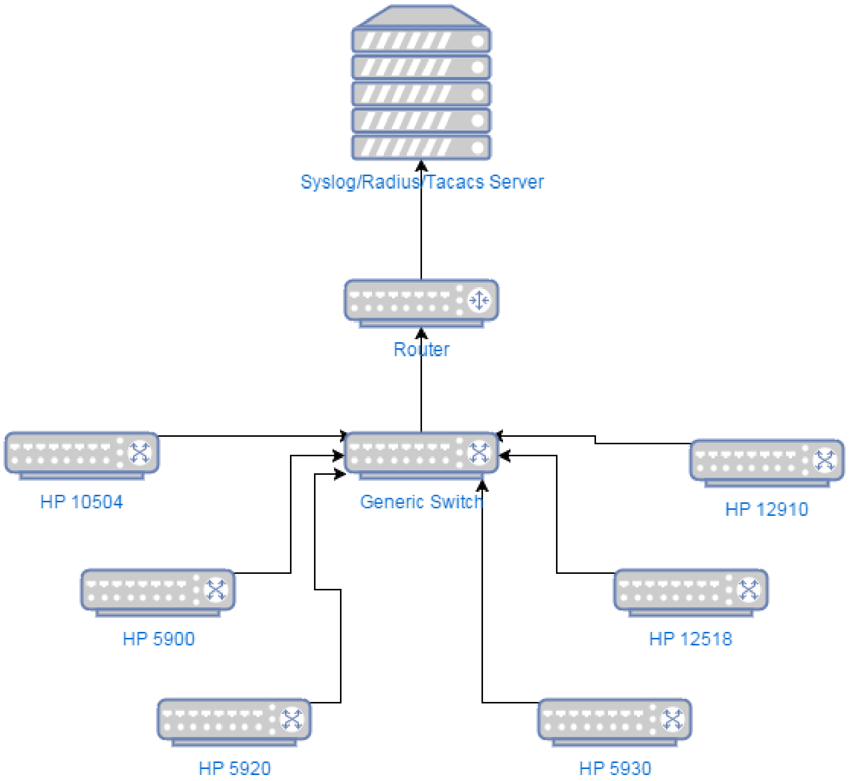

Figure 2: Test Configuration

The following hardware and software components were included in the evaluated configuration during testing:

- Hardware
    - HP 5900AF-48G-4XG-2QSFP+ Switch
    - HP 5920AF-24XG Switch
    - HP 5930-4Slot Switch
    - HP 10504 Switch Chassis with HP 10500 Type A Main Processing Unit with Comware v7 Operating System (JG496A)
    - HP 12518 Switch Chassis with HP 12500 Type A Main Processing Unit
    - HP FlexFabric 12910 Switch AC Chassis with 12910 Main Processing Unit
- Software
    - HP Comware 7.1.045.

The following components are not part of the TOE but were included in the testing environment:

- Router
- Syslog - 3CDaemon Version 2.0 Revision 10 running on Windows Server 2008
- FreeRadius
- Tacacs.NET

7.1 Penetration Testing

The evaluation team conducted a limited open source search for vulnerabilities in the product(s) using simple product related search terms via several known vulnerability tracking websites. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

The vulnerability search results are summarized in the document: *Assurance Activities Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches*, Version 1.0, 16 February 2016

8 Evaluated Configuration

The TOE is the Hewlett Packard Enterprise 5900, 5920, 5930, 10500, 12500, and 12900 Series Switches, which are installed and configured according to the product installation guidance identified in Section 6. The TOE appliances are configured to operate in FIPS mode. The specific devices and software included in the evaluated configuration are identified in the following table.

Table 3: Evaluated Configuration Identification

Series	Software Identification	Hardware Identification
HP 5900	Comware V7.1.045 Release 2423	HP 5900AF-48XG-4QSFP+ Switch (JG772A) HP 5900AF-48XGT-4QSFP+ Switch (JG336A) HP 5900AF-48G-4XG-2QSFP+ Switch (JG510A) HP FlexFabric 5900CP-48XG-4QSFP + Switch (JG838A)
HP 5920	Comware V7.1.045 Release 2423	HP 5920AF-24XG Switch (JG296A)
HP 5930	Comware V7.1.045 Release 2423	HP FlexFabric 5930-32QSFP+Switch (JG726A) HP FlexFabric 5930-4Slot Switch (JH179A) HP FlexFabric 5930 2QSFP+ 2-slot Switch (JH178A)
HP 10500	Comware V7.1.045 Release 7170	HP 10504 Switch Chassis (JC613A) HP 10508 Switch Chassis (JC612A) HP 10508-V Switch Chassis (JC611A) HP 10512 Switch Chassis (JC748A) Each chassis requires a compatible Main Processing Unit. The following are included in the evaluated configuration: • HP 10500 Type A Main Processing Unit with Comware v7 Operating System (JG496A) • HP 10500 Type D Main Processing Unit with Comware v7 Operating System (JH198A) • HP 10500 Type D TAA-compliant Main Processing Unit with Comware v7 Operating System (JH206A)
HP 12500	Comware V7.1.045 Release 7376	HP 12504 (AC) Switch Chassis (JC654A) HP 12504 (DC) Switch Chassis (JC655A) HP 12508 (AC) Switch Chassis (JF421C) HP 12508E (AC) Switch Chassis (JG782A) HP 12508 (DC) Switch Chassis (JC652A) HP 12508E (DC) Switch Chassis (JG783A) HP 12518 (AC) Switch Chassis (JF430C) HP 12518E (AC) Switch Chassis (JG784A) HP 12518 (DC) Switch Chassis (JC653A) HP 12518E (DC) Switch Chassis (JG785A)

Series	Software Identification	Hardware Identification
		Each 12500 Series chassis requires one of the following: • HP 12500 Type A Main Processing Unit with Comware v7 Operating System (JG497A) • HP 12500, LSTM5MRPNC, Management and Route Unit with OAM Module, Overseas Version (JC072B) • HP FlexFabric 12500E, LSTM5MRPNE1, Management and Route Process Unit, Overseas Version (JG802A)
HP 12900	Comware V7.1.045 Release 1138 P02	HP FlexFabric 12910 Switch AC Chassis with 12910 Main Processing Unit (JG621A) HP FlexFabric 12916 Switch AC Chassis with 12916 Main Processing Unit (JG634A)

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, as amended by Errata #3 dated 3 November 2014 (including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1), 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 PP, 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

The evaluated configuration may include non-security relevant product features and hardware modules that were not assessed, such as IRF, MDC, ISSU, TRILL, OAA, VLAN support and QoS which may have been addressed in the Security Target and elsewhere. The consumer should be aware that no further conclusions can be drawn about their effectiveness as any claimed capabilities of those items were not exercised as part of the security testing.

The TOE supports both IPv4 and IPv6 networks; however, however, IPv6 was not exercised during any of the assurance activities.

Note that audit records are not buffered for transmission to the syslog server, therefore the administrator is advised to ensure additional audit destinations are configured so that audit logs are not lost in the event of loss of connectivity to a single syslog server.

11 Annexes

Not applicable.

12 Security Target

- Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches Security Target, Version 1.0, 16 February 2016

13 Abbreviations and Acronyms

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CM	Configuration Management
CLI	Command Line Interface
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISSU	In Service Software Upgrades
IT	Information Technology
MPLS	Multiprotocol Label Switching
NDPP	Protection Profile for Network Devices
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OAA	Open Application Architecture
OSPF	Open Shortest Path First
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TRILL	Transparent Interconnection of Lots of Links
TSF	TOE Security Functions
VLAN	Virtual Local Area Network
VR	Validation Report

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] Protection Profile for Network Devices, Version 1.1, 8 June 2012, as amended by Errata #3 dated 3 November 2014.

[6] Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches Security Target, Version 1.0, 16 February 2016

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

[8] Evaluation Technical Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches, Version 1.0, 16 February 2016.

[9] Assurance Activities Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches, Version 1.0, 16 February 2016.

[10] Evaluation Team Test Report for Hewlett Packard Enterprise 5900 Series, 5920 Series, 5930 Series, 10500 Series, 12500 Series, and 12900 Series Switches, Version 1.0, 16 February 2016