National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

HPE 5400R zl2 Switch Series Version 5.011, KB_15_18_0008p01

Report Number: CCEVS-VR-VID10587-2016
Dated: February 19, 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

Paul A. Bicknell
Jay Vora

The MITRE Corporation

Daniel Faigin

The Aerospace Corporation

Common Criteria Testing Laboratory

Iain Holness
Nithya Rachamadugu

Much of the material in this report was extracted from evaluation material prepared by the CCTL.

Table of Contents

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product *HPE 5400R zl2 Switch Series Version 5.011* as defined in the *HPE 5400r zl2 Security Target.* It presents the evaluation results, their justifications, and the conformance results. The validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either express or implied.

The Target of Evaluation (TOE) is a network device as defined by the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise"*. The TOE claims exact compliance to this protection profile.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL) and was completed in February, 2016. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The TOE has been evaluated using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Network Devices (NDPP) with Errata #3 and all applicable Technical Decisions.

This Validation Report applies only to the specific version of the TOE operating in the specific evaluated configuration. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on the web site www.niap-ccevs.org.

2. Identification

Target of Evaluation: HPE 5400R zl2 Switch Series Version 5.011, KB_15_18_0008p01

Evaluated Platforms:

Platforms	Models
HPE[1] 5400R zl2 Switch Series	HPE 5406R zl2 Switch (J9821A)
	HPE 5412R zl2 Switch (J9822A)
	HPE 5406R-44G-PoE+/2SFP+ (No PSU) v2 zl2 Switch (J9823A)
	HPE 5406R-44G-PoE+/4SFP (No PSU) v2 zl2 Switch (J9824A)
	HPE 5406R-8XGT/8SFP+ (No PSU) v2 zl2 Switch (J9868A)
	HPE 5412R-92G-PoE+/2SFP+ (No PSU) v2 zl2 Switch (J9825A)
	HPE 5412R-92G-PoE+/4SFP (No PSU) v2 zl2 Switch (J9826A)

ST Title: HPE Networking Switches Security Target

Developer: CygnaCom Solutions

CCTL: CygnaCom Solutions
7925 Jones Branch Dr, Suite 5400
McLean, VA 22102-3321

Evaluators: Iain Holness
Nithya Rachamadugu

Validation Scheme: National Information Assurance Partnership CCEVS

Validators: Paul Bicknell, Daniel Faigin and Jay Vora

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, September 2012

[1] Note: 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” or “HPE”. For the purpose of this evaluation, these name variations are used interchangeably and refer to the same product.

CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, September 2012
PP Identification:	US Government Protection Profile for Network Devices, Version 1.1, 8 June 2012 with Errata 3

3. The Scope of Evaluation

3.1. Physical Boundary

The physical boundary of the TOE is the hardware appliance.

3.2. Logical Boundary

The logical scope of the TOE is defined by implemented security functions. These security functions are as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

3.2.1. Security Audit

The TOE generates audit records for all security-relevant events. For each event the TOE records the date and time, the type of event, the subject identity, and the outcome of the event logged. The resulting logs can be stored locally to be viewed by Managers and Operators and can securely be sent to a designated syslog server for archiving. The logs can be viewed by Operators and Managers using the appropriate CLI commands. TOE also implements timestamps to ensure reliable audit information is available using the appropriate CLI commands.

3.2.2. Cryptographic Support

The TOE performs all cryptographic operations using a certified cryptographic module operating in enhanced secure mode.

The TOE implements the following cryptographic protocols: SSHv2 and TLS v1.0.

The TOE implements the SSHv2 protocol and supports public key-based or password-based authentication with following parameters:

- AES-CBC-128, AES-CBC-256 for data encryption
- SSH_RSA for public-key authentication
- hmac-sha1 for data integrity

- diffie-hellman-group14-sha1 for key exchange

The TOE implements the TLSv1.0, and supports the following ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The TOE implements following cryptographic functionality:

- Random bit generation using CTR_DRBG(AES) seeded with 256 bits of entropy
- Zeroization of Critical Security Parameters (CSPs)

The TSF uses the Mocana cryptographic library to manage CSPs, implementing zeroization procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE implements commands to on-demand zeroize CSPs (e.g. private RSA keys) that can be invoked by an authorized administrator with a sufficient permissions based on their role.

3.2.3. User Data Protection

The TOF ensures that network packets sent from the TOE do not include data “left over” from processing the previous network information.

3.2.4. Identification and Authentication Functions

The TOE uses Role-Based Access Control (RBAC) before allowing access to the command line, and menu interfaces. Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with assigned role and specific permissions that determine access to TOE features. The TOE enhances user login security by masking passwords during entry on user login.

3.2.5. Security Management Functions

The TOE supports role-based access to the administrative interfaces and management functions. The TOE provides the following management interfaces: a Command Line Interface (CLI), a Menu Interface, and a physical console available on the front panel of the switch appliance. The TOE supports the following roles: Manager, Operator. Remote and local administration are accomplished over the CLI that provides access to all management functions used to administer the TOE, which are restricted to the manager role.

3.2.6. Protection of Security Functions

The TOE implements a number of measures to protect the integrity of its security features.

- The TOE protects CSPs such as stored passwords and cryptographic keys so they are not directly accessible in plaintext.

- The TOE ensures that reliable time information is available for both log accountability and synchronization with the operating environment.
- The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operation environment.
- The TOE performs self-tests to detect failure and protect itself from malicious updates.

3.2.7. TOE Access

The TOE displays a banner regarding unauthorized use of the TOE before establishing a user session. The banners are customer-configurable. The TOE will also terminate a user's session after an administrator-configured period of inactivity. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

3.2.8. Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path between itself and the administrator. The TOE prevents disclosure or modification of logs by establishing a trusted channel between itself and the Syslog using the TLS protocol. To implement a trusted path/secure channel the TOE uses the SSHv2 protocol.

3.3. Excluded Functionality

The TOE supports a number of features that are not part of the core functionality. These features are *not* included in the scope of the evaluation:

- Any integration and/or communication with authentication servers such as Terminal Access Controller Access-Control Systems (TACACS) is excluded from the evaluated configuration.
- Routing protocols that integrate authentication or encryption such as Routing Information Protocol (RIPv2), Open Shortest Path First (OSPFv2), and Border Gateway Protocol (BGP). RFC-compliant implementations are unable to satisfy NDPP cryptographic requirements.
- Use of telnet is excluded and it is disabled by default.
- Use of the SFTP server is excluded.
- Use of the SNMP functionality is excluded and it is disabled by default. The use of SNMPv3 is not restricted; however, it is an excluded functionality in NDPP evaluations.
- Although the product supports use of IPv6, IPv6 was not covered as part of evaluation testing.

3.4. Secure Usage Assumptions

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

1. 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. The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
2. Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
3. TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Architectural Information

4.1. TOE Components

The TOE is the HPE 5400R zl2 Switch Series Version 5.011, KB_15_18_0008p01. While the physical form factor of each appliance in the HPE Networking family may vary, the underlying hardware and software share similar architecture. The software utilizes a common code base of a modular nature with only the modules applicable for the specific hardware loaded

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the software Greenhills Integrity OS version 5.011 is shared across all platforms. Greenhills Integrity OS version 5.011 is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. Dedicated cryptographic module provides functionality that implements secure channel and protects critical security parameters. Control plane subsystem that includes an IP host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. System management subsystem, that includes AAA module, implements administrative interface and maintains configuration information.

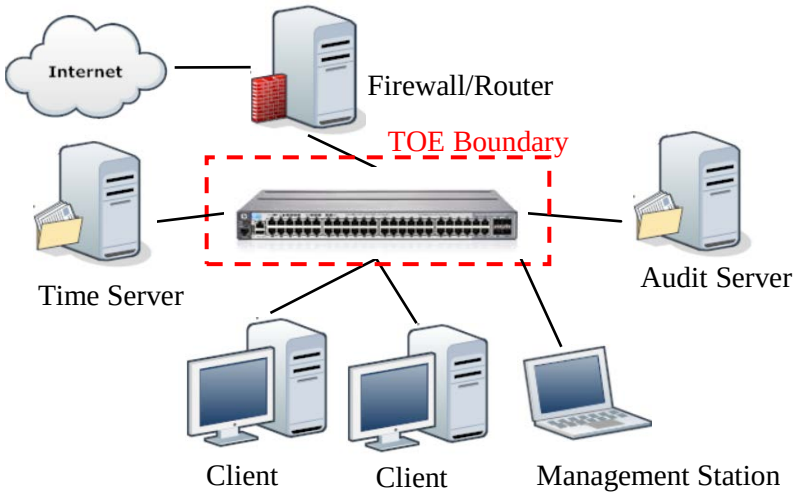
There is no direct user-space access to the underlying OS, and the TOE does not provide any general-purpose computing capabilities other than the limited subset necessary for its operation. A determined administrator with physical access to the hardware device can always gain access to the OS, but such mode of operation is outside the scope of the evaluation.

The physical boundary of the TOE is the hardware appliance itself running Greenhills Integrity OS version 5.011.

The Operational Environment of the TOE includes:

- The client software that used to access management interface
- The workstation that hosts the client software
- External IT servers:
    - Syslog for external storage of audit logs
    - SNTP Server and Timep Server for synchronizing system time
    - DNS server

- The TOE Boundary depicted in the following figure:



5. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by Hewlett-Packard Enterprise, and delivered to the end user of the TOE:

5.1. User Documentation

Reference Title	**ID**
HP Switch Software Management and Configuration Guide WB.15.18, HP Part No. 5998-8162, August 2015, Edition 1[2]	[ADMIN]
HPE 5400R Switch Series Version 5.011 Common Criteria Configuration Guide, February 17, 2016. Document Version 1.0	[CC Addendum]
HP Switch Software Basic Operation Guide, HP Part No. 5998-6820d, July 2015, Edition 5.	[BOP]

[2] Although this document indicates it is applicable to the HP Switch 2920-series (J9726A–J9729A), the TOE (HPE 5400R series) covers different model lines of the same device. Only the 5400R is evaluated, but non-CC specific guidance is broader.

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for HPE Network Switches* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

6.1. Developer Testing

NDPP evaluations do not require developer testing evidence for assurance activities.

6.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDPPv1.1

Testing was conducted January 23 to 26, 2016 at the 1000 Innovation Drive, Kanata, Ontario, CANADA facility in a dedicated testing space.

The Evaluator successfully performed the following activities during independent testing:

- Placed the TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the PP Assurance-defined tests, including the optional TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators, that the testing requirements for NDPP v1.1 are fulfilled.

7. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. 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 4.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile U.S. Government Standard Protection Profile for Network Devices, 08 June 2012, Version 1.1 with Errata 3.

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL (proprietary) and Assurance Activity Report (AAR) (public).

The following are the assurance requirements the TOE as specified by the PP. All assurance activities and work units received a passing verdict.

7.1. Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Hewlett Packard Enterprise 5400R zl2 Switch Series Version 5.011, KB_15_18_0008p01 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.2. Evaluation of the Development (ADV)

The evaluation team applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.3. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.4. Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC_OPE.1 and ALC_CMS.1 CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.5. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA_VAN.1 CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

7.7. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

7.8. Clarifications 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 NDPP. 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.

8. Validators Comments/Recommendations

The Validators recommend that the vendor keeps track of vulnerabilities for **GreenHills Integrity OS**, the custom operating system that the vendor chose to use, and apply updates to the TOE as required via their patching process.

9. Glossary

9.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

CC	Common Criteria [for IT Security Evaluation]
CIDR	Classless Inter Domain Routing
CM	Configuration Management
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
ICMP	Internet Control Message Protocol
ID	Identifier
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UI	User Interface
URI	Uniform Resource Identifier

9.2. Terminology

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.

Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) to a package.
Authentication data	Information used to verify the claimed identity of a user.
Authorised user	A user who may, in accordance with the SFR, perform an operation.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.
Connectivity	The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package..
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST, or a TOE against defined criteria.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Inter-TSF transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Iteration	The use of the same component to express two or more distinct requirements.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Organizational security policies	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Prove	This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigor.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP)	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
Transfers outside TSF	TSF mediated communication of data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted path	a means by which a user and a TSF can communicate with necessary confidence.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
TSF interface (TSFI)	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
User	See **external entity**
User data	Data created by and for the user that does not affect the operation of the TSF.

10. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (https://www.niap-ccevs.org/).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com/cc).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012 Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004.

Evaluation Documentation

[1] *HPE Networking Switches Security Target*, Version 1.9, February 19, 2016

[2] *Evaluation Technical Report for HP Networking Switches, Volume 1: Evaluation of the ST*. Version 0.4. January 21, 2016 (proprietary)

[3] *Evaluation Technical Report for HP Networking Switches, Volume 2: Evaluation of the TOE*. Version 0.4. February 17, 2016. (proprietary)

[4] *Assurance Activity Report for HPE 5400R zl2 Switch Series*. Version 1.0. February 19, 2016

[5] *Test Report: HPE 5400r Networking Switches*. Document Version 0.5. February 19, 2016 (proprietary)

[6] *HPE 5400R zl2 Switch Series Version 5.011 Functional Specification*. Version 0.9. January 7th, 2016 (proprietary)

[7] *HP Switch Software Management and Configuration Guide WB.15.18*, HP Part No. 5998-8162, August 2015, Edition 1

[8] *HPE 5400R Switch Series Version 5.011 Common Criteria Configuration Guide*, February 17, 2016. Document Version 1.0

[9] *HP Switch Software Basic Operation Guide*, HP Part No. 5998-6820d, July 2015, Edition 5.

[10] *HP 5400R zl2 Switch Series Version 5.011: Identification of the TOE*. Version 0.3. January 26, 2016 (proprietary)