National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005

Report Number:	**CCEVS-VR-VID10410-2011**
Dated:	**18 October 2011**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jandria Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Ms. Prajakta Kulkami
CygnaCom Solutions
McLean, Virginia

Table of Contents

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 both 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 any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the HP Networking E-Series Switches. It presents the evaluation results, their justifications, and the conformance results. This Validation Report 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 Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the HP Networking E-Series Switches was performed by the CygnaCom Solutions Inc., the Common Criteria Testing Laboratory, in McLean, Virginia USA and was completed in September 2011.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written on behalf of HP by CygnaCom Solutions. The ETR and test report used in developing this validation report were written by CygnaCom Solutions. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, dated September 2007 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R2, dated September 2007. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the HP Networking E-Series Switches Security Target. The evaluation team determined the product to be both Part 2 and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE provides the following security functionality: generation of audit records for security relevant events and user review of these records; user identification and authentication and user login security; cryptographic support for data operations; information flow control; role-based access controlled security management features; protection of TSF data during transit; TSF self-testing; TOE access banners; and termination of a user session after a period of inactivity.

The HP Networking E-Series Switch's operating image base software Version K.15.02.0005 is embedded in the switch appliances. The appliance hardware, the underlying operating systems, and third-party applications installed on the appliances provide support to security functions of the TOE, and are included in the TOE.

This product was previously known as HP ProCurve Switches. Under an HP re-organization, HP has changed the reference to the TOE to be “HP Networking E-Series Switches”. Titles to Vendor user manuals have not been updated to reflect this change. Therefore, there are still references to ProCurve in tables and examples within the ST.

NOTE: The version of SSL and SSH used in this product has not been FIPS certified. Compliance to any standards is Vendor asserted. The compliance of the encryption modules to any standard is not being certified.

NOTE: It is not the intent of the evaluation to determine compliance to any IP standards mentioned in this ST. Testing will include specific filters identified for particular IP standards (i.e ICMP filter). As a byproduct of the filter testing, certain aspects of the TOE’s ability to parse IP packets and protocol formats will be confirmed. Protocol compliance is strictly by vendor assertion.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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 Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	**Identifier**
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005
Protection Profile	N/A
Security Target	*HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005 Security Target*, version 2.0, August 26, 2011
Dates of evaluation	January 2010 through September 2011
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation Volume 1 : Evaluation of the ST HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005*, 5 September 2011 *Evaluation Technical Report for a Target of Evaluation Volume 2 : Evaluation of the TOE HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005*, 2 September 2011
Conformance Result	Part 2 conformant and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on January 27, 2010
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July 2009and all applicable NIAP and International Interpretations effective on January 27, 2010
Sponsor	Hewlett-Packard

Developer	Hewlett-Packard
Common Criteria Testing Lab	CygnaCom Solutions Inc. McLean, Virginia
Evaluators	Prajakta Kulkami
Validation Team	Jandria Alexander and Mike Allen of The Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None

International Interpretations

None

3 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.
The TOE provides the following security features:

3.1 Security Audit

The TOE records security relevant event data in an Event Log. The audit records in the Event Log serve as a tool to isolate and troubleshoot problems. The audit trail is stored on the switch and is accessible via the protected management functional interfaces. The TOE is able to protect the Event Log from unauthorized deletion or modification. TOE users can view the audit records via the Menu Interface and the CLI.

The Security Audit Functions may optionally depend on an SNTP Server in the operational environment to provide reliable timestamps for the audit records. Event Log records and debugging messages can be optionally sent to an external Syslog Server or sent via SNMP trap as new events are generated. There is the ability to export the entire event log via TFTP and SFTP for off TOE storage and review.

3.2 Cryptographic Support

The TOE provides cryptographic support for SSH communications; SSL data transport; SNMP messaging and authentication support; hashing of passwords; secure communications with an external authentication server. The Vendor is not claiming FIPS compliance for the cryptographic functionality. The version of SSL and SSH used in this product has not been FIPS certified. Compliance to any standards is Vendor asserted. The compliance of the encryption modules to any standard is not being certified.

3.3 User Data Protection

The TOE performs user data protection through information flow control. Only legitimate external IT entities are granted access to pass information through the TOE or to the TOE. Traffic is allowed or blocked through the use of rate limiting, ICMP throttling, protocol-based filtering, source-port filtering and dynamic ARP protection. Traffic can be blocked from unauthorized DHCP servers, configured MAC addresses, configured IP addresses and source-ports and through the use of access control lists.

3.4 Identification and Authentication

The TOE enforces password based authentication before allowing access to the command line, menu and web-based management interfaces. The TOE also allows the use of an optional external authentication server (RADIUS or TACACS+) for TOE user identification and authentication.

The TOE enhances user login security by masking passwords during entry on user login.

3.5 Security Management

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, a Web-Based interface, and a physical interface available on the front panel of the switch appliance, and a SNMP interface.

The TOE supports management of the security attributes that are used for information flow control.

The Security Management functionality depends on the remote management console using SSH for accessing the console interfaces (CLI or Menu Interface) or a SSL enabled web browser for use of the Web interface.

Functionality is provided for the disabling/locking the Front Panel Interface and the USB interface to prevent unauthorized physical tampering.

In order to use the SNMP interface, the TOE requires the use of an operational environmentally supplied Network Management Station, which is not in scope, with SNMPv3 enabled.

3.6 TOE Access

The TOE displays a customizable banner regarding unauthorized use of the TOE before establishing a user session. The TOE will also terminate a user’s session after an administrator configured period of inactivity.

3.7 Protection of the TSF

The TOE, in conjunction with the operational environment, protects TSF data from unauthorized disclosure when transmitted between itself and trusted external IT entities.

The TOE is also capable of self-testing during initial start-up and reboot to detect security failures.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraphs were made during the evaluation of HP Networking E-Series Switches.

4.1 Assumptions

The ST provides additional information on the assumptions made and the threats countered. It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains. They are trained for the secure operation of the TOE. They can be trusted not to deliberately abuse their privileges so as to undermine security.

It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.

It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.

It is assumed that the TOE hardware and software critical to the security policy enforcement will be protected from unauthorized physical modification.

It is assumed that users will protect their authentication data.

4.2 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 (EAL 2 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The following are not included in the Evaluation Scope:
    a. *ProCurve Manager (PCM) and ProCurve Manager Plus (PCM+). These are network management applications that can optionally be used to manage and monitor HP Networking E-Series Switches via SNMP from an MS Windows-based workstation/server. A copy of PCM and PCM+ (trial-version) is included on the CD-*

ROM that comes with the TOE. However, these are separate HP products that have not been evaluated.

   b. *Testmode interface (accessed via CLI) which is only used for maintenance and troubleshooting.*

5. The IT environment needs to provide the following capabilities:

   a. *External authentication server(s) (RADIUS, TACACS+)*

   b. *External SNTP Server (Time Sync Server)*

   c. *External Syslog Server*

   d. *External SNMP Server*

   e. *External client software to support 802.1X*

   f. *DNS Server*

   g. *SSL compatible Web Browser for use of web-based management interface (Web Interface support)*

   h. *SSH Client on host used to support remote management of console interfaces (CLI and Menu Interface)*

   i. *External Network Management Station and software used for remote management of MIB attributes over SNMPv3*

   j. *Connected networks and assets*

6. The version of SSL and SSH used in this product has not been FIPS certified. Compliance to any standards is Vendor asserted. The compliance of the encryption modules to any standard is not being certified.

7. Compliance to any IP standards mentioned in the ST was not specifically tested. Testing will include specific filters identified for particular IP standards (i.e ICMP filter). As a byproduct of the filter testing, certain aspects of the TOE's ability to parse IP packets and protocol formats will be confirmed. Complete protocol compliance is strictly by vendor assertion.

5 Architectural Information

The TOE consists of the entire HP Networking Switch, Software Version K.15.02.0005 as available commercially from the Vendor. The TOE consists of all hardware, firmware, HP developed software and third party software installed upon the switch appliance. In addition, the evaluated TOE includes:

- Intelligent Edge Software Features. These features are automatically included on all switches.
- Premium License Software Features. For models E3500yl, E5400zl, E6600, and E8200zl the Premium License features can be acquired by purchasing the optional Premium License and installing it on the Intelligent Edge version of these switches. (These features are automatically included on the E6200yl switches.)

The physical boundary of the TOE is depicted in Figure 1 below:

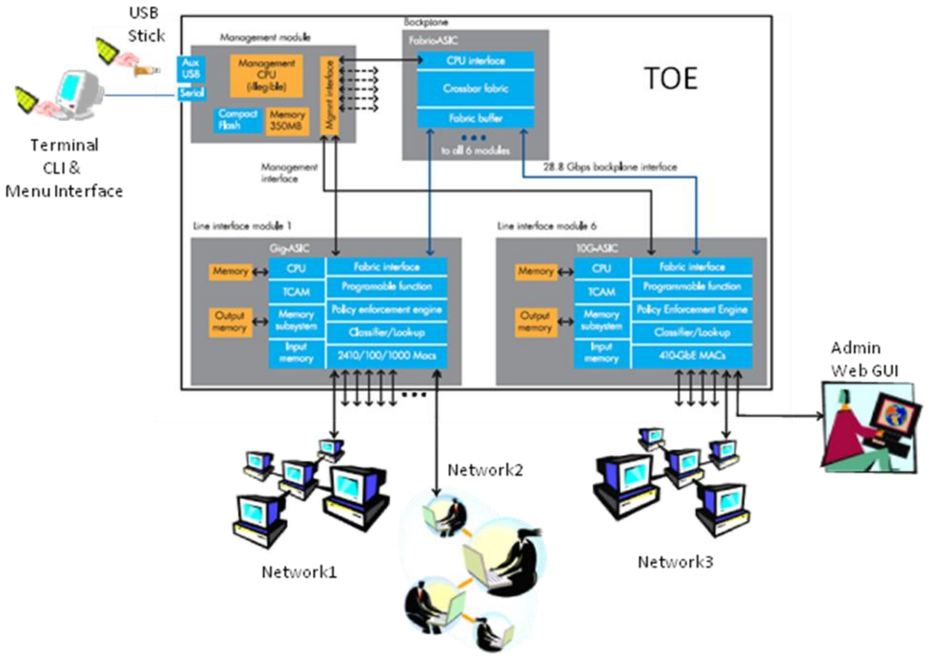


Figure 1: TOE Boundary

The HP Networking's ProVision™ ASIC is the fourth generation of HP Networking network chipsets. A key component of the HP Networking Switches, the highly integrated ProVision ASIC has built-in wirespeed intelligence, a unified set of configuration management tools and is scalable across a number of products. The ProVision ASIC is designed to operate continuously and withstand error conditions and malicious network attacks. The HP Networking Switches use a combination of software and ProVision ASIC functionality to verify which data packets need to be sent to the CPU. Excessive packets from malicious attacks or network mis-configuration can be identified and demoted to lower-priority queues before they overwhelm and shut down the CPU and the switch. In addition, the ProVision ASIC contains processes such as end-to-end data checking, embedded RAM error correction, and ECC on an external DRAM. These processes ensure the integrity of the traffic as it passes through the switch, protecting the traffic from environmental elements.

TOE Operational Conditions:

To be in the evaluated configuration the TOE must be configured with the following requirements:

- TELNET for CLI and Menu Interfaces must be disabled and SSH must be used.
- HTTP Web access for management using a standard web browser connection must be disabled.
- HTTPS must be enabled for Web access management
- TFTP client and server must be disabled.
- Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP) should be enabled.
- SNMP v2 and v1 must be disabled.
- SNMP v3 with encryption should be enabled if remote SNMP Management is used.
- Replace the default community name ("*public*") with a non-default community name.
- Manager and Operator access levels must have a password assigned.

- Full individual user identification and authentication can only be achieved if the switch is configured so that identification and authentication are handled via an external authentication server (RADIUS or TACACS+) or certificates.
- The console inactivity timer must be configured to a nonzero value.
- There are two recessed buttons on the front-panel of the switch: "password clear" and "factory reset." Both must be disabled to fully secure the device.
- The switch includes a USB port to receive a flash drive for deploying, troubleshooting, backing up configurations, or updating switches. This port should be disabled when not in use and temporarily enabled when needed.
- DO NOT disable Password-Recovery option

The following are optional operational environment components that are not included in the TOE:

- External authentication server(s) (RADIUS, TACACS+)
- External SNTP Server (Time Sync Server)
- External Syslog Server
- External SNMP Server
- External client software to support 802.1X
- DNS Server

- SSL compatible Web Browser for use of web-based management interface (Web Interface support)
- SSH Client on host used to support remote management of console interfaces (CLI and Menu Interface)
- External Network Management Station and software used for remote management of MIB attributes over SNMPv3
- Connected networks and assets

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005. The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered in printed form and as PDFs on the installation media.

Vendor User Documentation

Reference Title	Part #	Software Version	Publication Date
Switch Software Manuals			
HP ProCurve Switch Software Access Security Guide	5992-3061	K.15.01	June 2010
HP ProCurve Switch Software Advanced Traffic Management Guide	5992-3060	K.15.01	June 2010
HP ProCurve Switch Software IPv6 Configuration Guide	5992-3067	K.15.01	June 2010
HP ProCurve Switch Software Management and Configuration Guide	5992-3059	K.15.01	June 2010
HP ProCurve Switch Software Multicast and Routing Guide	5992-3062	K.15.01	June 2010
HP ProCurve Switch Software Command Line Interface Reference Guide	5992-3063	K.14.09	April 2009
HP ProCurve Switch Software Event Log Message Reference Guide	5992-5486	K.15.01	June 2010
Release Notes: Version K.15.01.0031 Software for the HP ProCurve Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches	5998-0595	K.15.01.0031	May 2010
Release Notes: Version K.15.01.0033 Software for the HP ProCurve Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches	5998-0595	K.15.01.0033	September 2010
Release Notes: Version K.15.02.0005 Software for the HP ProCurve Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches	5998-1186	K.15.02.0005	Nov. 2010
Common Criteria for HP Networking Switches Read Me First	5998-2311 Rev. B	K.15.02.005	Aug. 2011
3500, 3500yl, and 6200yl Switches			
HP ProCurve Switch Quick Setup Guide	5992-4964	N/A	February 2010
HP ProCurve 3500, 3500yl and 6200yl Switches Installation and Getting Started Guide	5900-0230	N/A	Aug. 2010
ProCurve Switch yl Module Installation Guide	5991-3783	N/A	December 2005
HP ProCurve 3500-24 and 3500-48 Switches Safety and Regulatory Information	5992-6001	N/A	May 2009

HP ProCurve 3500-24-PoE and 3500-48-PoE Switches Safety and Regulatory Information	5992-6002	N/A	May 2009
Series 3500yl-PoE+ Switch Safety and Regulatory Information	5900-0288	N/A	November 2009
Series 3500yl-PWR Switch Safety and Regulatory Information	5900-0232	N/A	November 2009
5400zl Switches			
HP E5400 zl Switches Installation and Getting Started Guide	5900-0281	N/A	May 2011
Quick Setup Guide for HP E5400 zl Switches	5998-1170	N/A	November 2010
HP E5400 zl Switches Safety and Regulatory Information	5998-1171	N/A	November 2010
6600 Switches			
HP ProCurve 6600 Switch: Quick Setup Guide	5992-5508	N/A	June 2009
HP ProCurve 6600 Switches Installation and Getting Started Guide	5992-4962	N/A	June 2009
HP ProCurve 6600 Switches Safety and Regulatory Information	5992-5997	N/A	June 2009

Common Criteria Evidence

Reference Title		**ID**
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 Security Target	Aug 26 2011 HP Networking E-Series EAL2 Security Target v2 0.doc	[ST]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 TOE Design	Mar 22 2011 HP Networking E-Series EAL2_ADV_TDS.2 v1.2.doc	[TDS]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 Functional Specification	Mar 24 2011 HP Networking E-Series EAL2_ADV_FSP.4 v1.0.doc	[FSP]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 Security Architecture	Mar 25 2011 HP Networking E-Series EAL2_ADV_ARC.1 v0.2.doc	[ARC]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 CM System Usage	Mar 25 2011 HP Networking E-Series EAL2_ALC_CMC.2 v0.2.doc	[CMC]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 Configuration Item List	Aug 24 2011 HP Networking E-Series EAL2_ALC_CMS.2 v0.1.doc	[CMS]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl with Software Version K.15.02.0005 Delivery Procedures	May 23 2011 HP Networking E-Series EAL2_ALC_DEL.1 v1.0.doc	[DEL]

HP Networking Secure Product Development - EVPG.ppt	*HP Networking Secure Product Development - EVPG.ppt*	[FLR]
Common Criteria for HP Networking Switches Read Me First	Aug 2011. 5998-2311 Rev. B	[CC SUPP]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl *with Software Version K.15.02.0005 Developer Test Plan*	May 15 2011 HP Networking E-Series EAL2_ATE_FUN 1 v0 2.doc	[DTP]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl *with Software Version K.15.02.0005 Test Procedures*	Common Criteria Test Procedures and Coverage 110517.htm	[DTS]
HP Networking E-Series Switch Models: 3500yl, 5400zl, 6200yl, 6600, 8200zl *with Software Version K.15.02.0005 Test Matrix*	Common Criteria Test Procedures and Coverage 110517.htm	[COV]

7 IT Product Testing

This section describes the testing efforts of the vendor and the evaluation team.
The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests."

7.1 Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations described in Section **Error! Reference source not found.**: **Error! Reference source not found.**.

7.1.1 Overall Test Approach and Results:

Developer testing consisted of the following types of tests:

Manual Tests:

All the developer tests were performed manually. All expected results are mentioned as part of the Developer's test procedure description and all actual results are observations to ensure that expected results match actual results.

7.1.2 Depth and Coverage

All developer test cases test TOE security functions by stimulating an external interface. Although the developer tests are performed using the WebUI, the evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces. TOE testing directly tests external TSF interfaces. The behavior of the TSF is realized at its interfaces. Hostile intent will be expressed at the Network Asset Interface.

The evaluator ensured that the test sample included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised
- All Security Functional Requirements are tested.
- More emphasis is laid on the Network Interface being tested.
- All relevant security relevant features mentioned in the Administration/User Guides are covered in testing.

The evaluators worked with HP to determine the adequate extent of coverage required at EAL 2.

7.1.3 Results

The evaluator checked the test procedures and the Test Evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the Test Evidence and found that the actual results were consistent with the expected results.

The evaluator used a sampling technique to check the test procedures. The evaluator checked one or more test cases per SFR.

Given the Evaluation Assurance level (EAL 2), the evaluator determined that HP's TOE testing was adequate. All the external TSF interfaces were tested. TOE testing exercised all security functions identified in the Functional Specification.

7.2 Evaluator Independent Testing

The evaluator performed the following activities during independent testing:

- Execution the Developer's Functional Tests (ATE_IND.2)
- Team-Defined Functional Testing (ATE_IND.2)
- Vulnerability/Penetration Testing (AVA_VAN.2)

7.2.1 Execution the Developer's Functional Tests

The evaluator selected to rerun 80% of the developer's tests:

- as a means of ensuring the coverage of the security features,
- as a means to gain confidence in the developer's test results, and
- a quick means of ensuring TOE is in a properly configured state

The developer's test cases were executed only after the TOE was installed in the evaluated configuration that is consistent with the Security Target (Section 1) and the HP Common Criteria Supplement Document. The evaluator confirmed that the test configuration was consistent with the evaluated configuration in the Security Target and the HP CC Supplement. The test configurations used by the evaluator were the same as that used by the developer. The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results. Anomalies were documented along with suggested / required solutions.
All of the Developer's Functional Tests reran by the Evaluator received a 'Pass' verdict.

7.2.2 Team-Defined Functional Testing

The Evaluator selected individual test procedures from the set of Developer Functional Tests, and modified the input parameters to ensure fuller coverage of security functions and correctness of developer reported results (ensuring that the results were not canned). Additional tests were developed for the purpose of verifying that the product operates in accordance with Vendor claims, i.e. that a bug is fixed or a capability operates as described in the product documentation. The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the tests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

The Evaluator developed the following additional tests:

1. Test that verifies the password recovery feature for the front panel interface of the switch and confirm that the Switch is protected from malicious users while resetting passwords
2. Test that verifies the access control functions of the switch when a combination of Access Control Lists is run on the Switch. The evaluator verified this feature on both V1 and V2 Modules to demonstrate similar behavior without change in functionality.
3. Test that verifies the RADIUS Access Control feature to gain broader coverage as this was not covered as a part of the Developer testing.
4. Test that verifies that appropriate warnings are displayed in the log records when a bad cable is connected or bad packets are sent across.
5. Test that verifies the Management Cross-over functionality of the 8200 series.

All of the Team-Defined Tests received a 'Pass' verdict.

7.2.3 Vulnerability/Penetration Testing

The Vulnerability / Penetration tests covered hypothesized vulnerabilities and potential misuse of guidance. The evaluator ran the following tests on the 8206 chassis connected to the IXIA Traffic Generator:

1. Test to check for Buffer Overflow conditions by overflowing character strings in password policy settings
2. Test to check for input errors by using invalid characters in password policy settings
3. Ran a Nessus Scan with all plugins turned on against one of the Management Ports.
4. Evaluator performed several Negative tests to check the functionality of the Switch:
    - 4.1. Disabling FTP
    - 4.2. Disabling Telnet
    - 4.3. Accessing the web through an Invalid Certificate

The test results and screenshots for the test cases were recorded during the evaluator testing. Overall success of this testing was measured by 100% of the tests being consistent with expected results. The Evaluator went through the Nessus Scan Reports and found that no security holes were listed. However, the evaluator found Warnings listed. The evaluator found that HP was using an older version of SSL. As a result, HP has added this shortcoming to its future process of upgrades.

All identified vulnerabilities were ruled out in the evaluated configurations.

.

8 Evaluated Configuration

The HP Networking E-Series evaluated configuration may consist of 3 platforms:

The TOE was tested with the following test bed components:

- 3500yl with K.15.02.0005
- 5406zl with K.15.02.0005
- 8206zl K.15.02.0005

The Operational Environment includes the following test bed components:

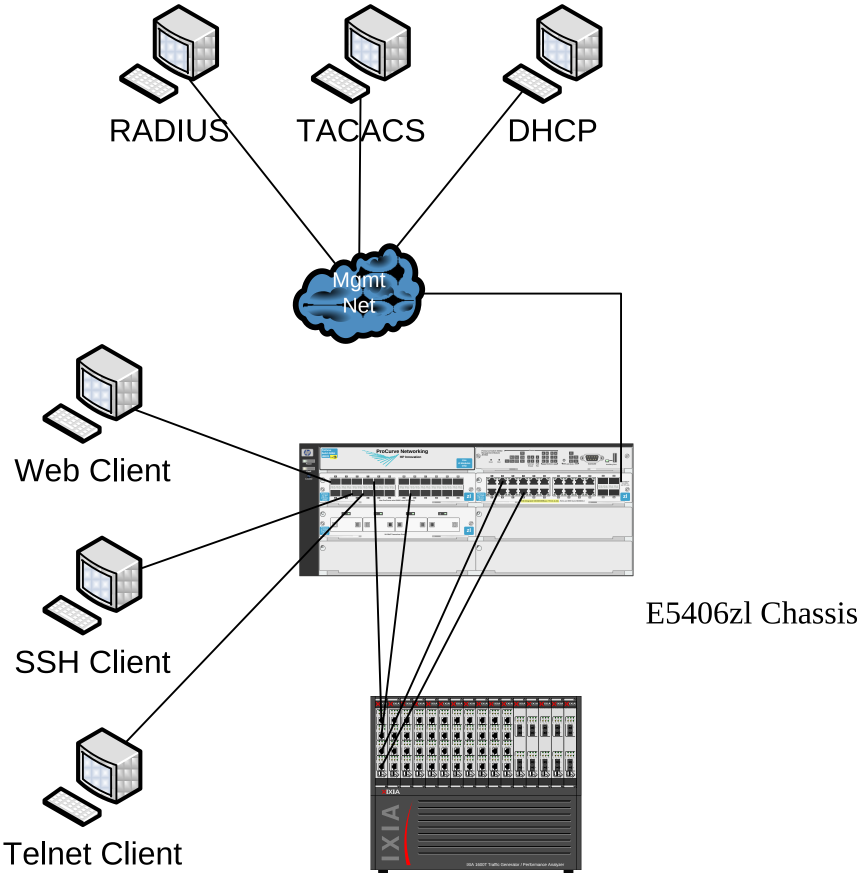
- E5406zl Chassis – J8697A
- RADIUS Server- FreeRADIUS Version 2.1.10
- TACACS Server- Tac_Plus F4.0.4.19
- Web Client- IE 7.0.5730.13, Firefox 3.6.16
- SSH Client- SecureCRT 5.5.0 OpenSSH 5.8p1-4.1
- Telnet Client- Windows XP
- DHCP Server- Internet Consortiums DHCP Server 4.2.1

The following figures illustrate the main components required for running all test cases. They describe all the different test configurations described in the ST.

Product Configuration 1:

- E5406zl Chassis – J8697A
- RADIUS Server- FreeRADIUS Version 2.1.10
- TACACS Server- Tac_Plus F4.0.4.19
- Web Client- IE 7.0.5730.13, Firefox 3.6.16
- SSH Client- SecureCRT 5.5.0 OpenSSH 5.8p1-4.1
- Telnet Client- Windows XP
- DHCP Server- Internet Consortiums DHCP Server 4.2.1

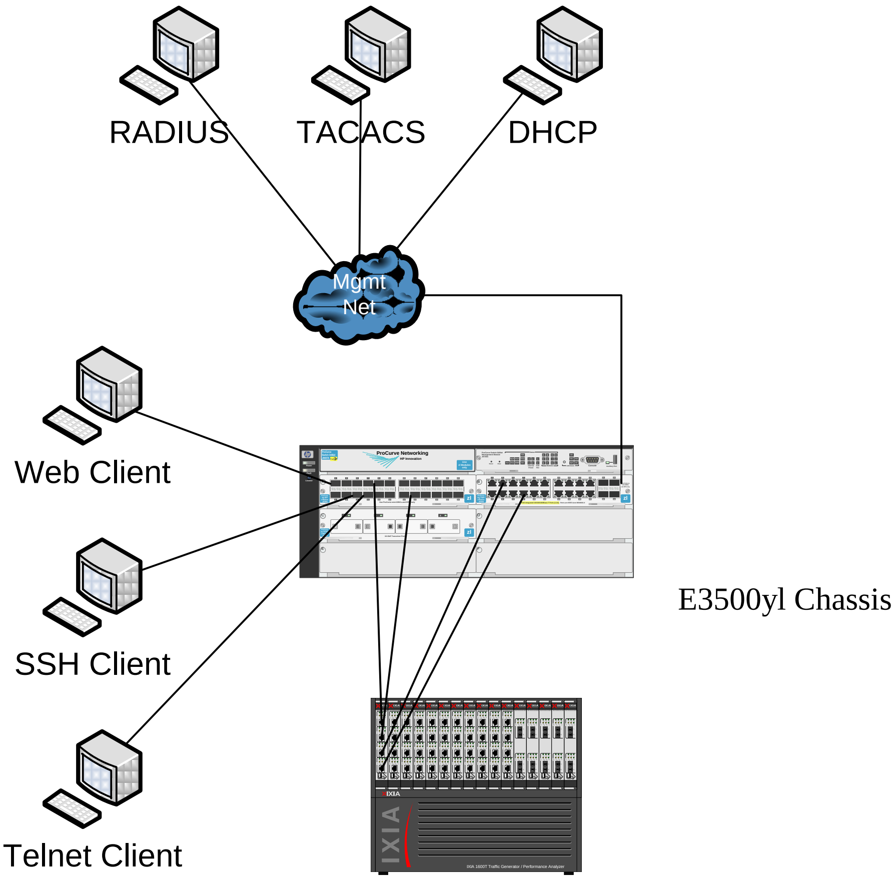
The test set up is as shown in the figure below:



Product Configuration 2:

- E3500-48G-PoE yl Switch – J8693A
- RADIUS Server- FreeRADIUS Version 2.1.10
- TACACS Server- Tac_Plus F4.0.4.19
- Web Client- IE 7.0.5730.13, Firefox 3.6.16
- SSH Client- SecureCRT 5.5.0 OpenSSH 5.8p1-4.1
- Telnet Client- Windows XP

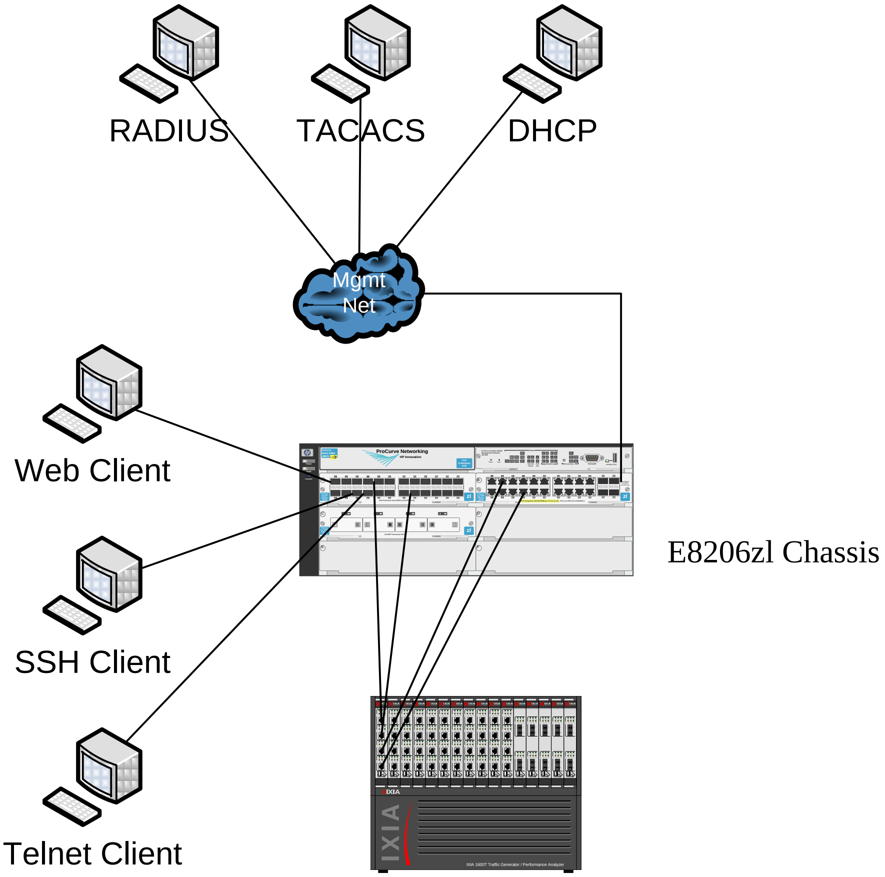
DHCP Server- Internet Consortiums DHCP Server 4.2.1The test set up is as shown in the figure below:



Product Configuration 3:

- E8206zl Chassis – J9638A
- RADIUS Server- FreeRADIUS Version 2.1.10
- TACACS Server- Tac_Plus F4.0.4.19
- Web Client- IE 7.0.5730.13, Firefox 3.6.16
- SSH Client- SecureCRT 5.5.0 OpenSSH 5.8p1-4.1
- Telnet Client- Windows XP
- DHCP Server- Internet Consortiums DHCP Server 4.2.1

The test set up is as shown in the figure below:



Model coverage is achieved by using equivalency arguments for models and LIM cards, running a complete test suite on one model, and running a sampling of the entire test suite on different models (fixed and modular).

9 Results of the Evaluation

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 R3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached PASS verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- 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.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the HP Networking E-Series Switches meet the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The version of SSL and SSH used in this product has not been FIPS certified. Compliance to any standards is Vendor asserted. The compliance of the encryption modules to any standard is not being certified.
- Compliance to any IP standards mentioned in the ST were not specifically tested. Testing included specific filters identified for particular IP standards (i.e., ICMP filter). As a byproduct of the filter testing, certain aspects of the TOE's ability to parse IP packets and protocol formats were confirmed. Complete protocol compliance is strictly by vendor assertion.
- The TOE is intended for use in computing environments where there is a low level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

11 Security Target

The Security Target is identified as the HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005 Security Target. The ST is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

12 Glossary

12.1 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]
CM	Configuration Management
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
HP	Hewlett-Packard
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
RPC	Remote Procedure Call
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
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol
UI	User Interface
URI	Uniform Resource Identifier

12.2 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 Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

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.

13 Bibliography

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

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R3, July 2009.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2009.

Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R3, July 2009.

Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R3, July 2009.

Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

- HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005 Developer Test Plan, May 15, 2011.
- Evaluation Technical Report for a Target of Evaluation Volume 1 : Evaluation of the ST HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005, 5 September 2011
- Evaluation Technical Report for a Target of Evaluation Volume 2 : Evaluation of the TOE HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005, 2 September 2011.

HP Networking E-Series Switch Models: E3500yl, E5400zl, E6200yl, E6600, E8200zl with Software Version K.15.02.0005 Security Target, version 2.0, August 26 2011.