Hewlett-Packard Company
6125XLG Ethernet Blade Switch
Security Target

Version 2.0
19 February 2015

Prepared for:

Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

Leidos Inc. (formerly Science Applications International Corporation)

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

1. SECURITY TARGET INTRODUCTION 4
1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 4
1.2 CONFORMANCE CLAIMS 4
1.3 CONVENTIONS 4
1.3.1 Terminology 5
1.3.2 Acronyms 5
2. TOE DESCRIPTION 6
2.1 TOE OVERVIEW 7
2.2 TOE ARCHITECTURE 8
2.2.1 Intelligent Resilient Framework 9
2.2.2 Multitenant device context 9
2.2.3 Physical Boundaries 9
2.2.4 Logical Boundaries 9
2.3 TOE DOCUMENTATION 11
3. SECURITY PROBLEM DEFINITION 12
4. SECURITY OBJECTIVES 13
4.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 13
5. IT SECURITY REQUIREMENTS 14
5.1 EXTENDED REQUIREMENTS 14
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 15
5.2.1 Security audit (FAU) 15
5.2.2 Cryptographic support (FCS) 17
5.2.3 User data protection (FDP) 19
5.2.4 Identification and authentication (FIA) 19
5.2.5 Security management (FMT) 20
5.2.6 Protection of the TSF (FPT) 20
5.2.7 TOE access (FTA) 21
5.2.8 Trusted path/channels (FTP) 21
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 22
6. TOE SUMMARY SPECIFICATION 22
6.1 SECURITY AUDIT 22
6.2 CRYPTOGRAPHIC SUPPORT 23
6.3 USER DATA PROTECTION 31
6.4 IDENTIFICATION AND AUTHENTICATION 32
6.5 SECURITY MANAGEMENT 32
6.6 PROTECTION OF THE TSF 33
6.7 TOE ACCESS 34
6.8 TRUSTED PATH/CHANNELS 35
7. PROTECTION PROFILE CLAIMS 36
8. RATIONALE 37
8.1 TOE SUMMARY SPECIFICATION RATIONALE 37
APPENDIX A: DOCUMENTATION FOR HP 6125XLG ETHERNET BLADE SWITCH 39

LIST OF TABLES

Table 1 TOE Security Functional Components 15
Table 2 Auditable Events 17
Table 3 Assurance Components 22
Table 4 Cryptographic Functions 24
Table 5 NIST SP800-56B Conformance 25
Table 6 Key/CSP Zeroization Summary 30
Table 7 SFR Protection Profile Sources 36
Table 8 Security Functions vs. Requirements Mapping....38

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Hewlett-Packard Company 6125XLG Ethernet Blade Switch with Comware V7.1 provided by Hewlett-Packard Development Company. The Switch product is a Gigabit Ethernet Blade Switch blade designed to implement a wide range of network layers 2 and 3 switching, service and routing operations.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett-Packard Company 6125XLG Ethernet Blade Switch Security Target

ST Version – Version 2.0

ST Date – 19 February 2015

TOE Identification – Hewlett-Packard Company 6125XLG Ethernet Blade Switch with Comware Version 7.1.045, Release 2406 P01

TOE Developer – Hewlett-Packard Company

Evaluation Sponsor – Hewlett-Packard Company

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012*

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- This ST is conformant to the *Protection Profile for Network Devices*, Version 1.1, 8 June 2012 (NDPP) as amended by Errata #2 dated 13 January 2013 [*sic*], and including the following optional SFRs: FCS_IPSEC_EXT.1; FCS_SSH_EXT.1; and FIA_PSK_EXT.1.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Terminology

BladeSystem	An HP term which refers to their all-in-one design architecture that includes the essentials needed for an HP infrastructure
c-class blade-system	c-class blade-system is a flexible general-purpose architecture specific to HP that makes the HP computing, network, and storage resources easier to install and arrange.

1.3.2 Acronyms

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AUT	Authentication
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CLI	Command Line Interface
DH	Diffie-Hellman
EVB	Edge Virtual Bridging
EVI	Ethernet Virtualization Interconnection
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FIPS	Federal Information Processing Standard
FMT	Security Management CC Class
FSP	Functional Specification
GR	Graceful Restart
HMAC	Hashed Message Authentication Code
IP	Internet Protocol

IPC	Inter-process communication
IPSEC	Internet Protocol Security
IRF	Intelligent Resilient Framework
ISSU	In Service Software Upgrades
IT	Information Technology
LACP	Link Aggregation Control Protocol
MDC	Multitenant device context
MOF	Management of Functions
MPLS	Multiprotocol Label Switching
MTD	Management of TSF Data
NDPP	Protection Profile for Network Devices
OAA	Open Application Architecture
OSP	Organization Security Policy
OSPF	Open Shortest Path First
PP	Protection Profile
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RPC	Remote procedure call
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TACACS	Terminal Access Controller Access Control System
TOE	Target of Evaluation
TRILL	Transparent Interconnection of Lots of Links
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection
VLAN	Virtual Local Area Network

2. TOE Description

The Target of Evaluation (TOE) is the Hewlett-Packard 6125XLG Ethernet Blade Switch with Comware V7.1. The HP 6125XLG Ethernet Blade Switch is a standalone c-class blade-system switch appliance that provides network connectivity for the following: Cloud computing, service providers, Web2.0, health care, Universities, Government agencies and for use in HP c7000 chassis blade-system enclosures. The 6125XLG is built with the enterprise data center in mind and architected to deliver 880G of switching performance. The HP 6125XLG Ethernet Blade Switch includes the HP Comware V7.1 network operating system, which delivers enterprise grade resiliency and is designed for data center convergence with full support for IEEE Data Center Bridging (DCB) for lossless Ethernet, and Fibre Channel over Ethernet (FCoE) protocols. The switch supports IETF industry standard TRILL (Transparent Interconnection of Lots of Links) that enables loop free large Layer 2 networks with multi-path support. The switch provides Intelligent Resilient Framework (IRF) which enables multiple switches to be virtualized and managed as a single entity with HP's Intelligent Management Center (IMC). The IMC is not within the scope of the evaluation. Management of the IRF group can and should occur via any of the IRF group members by an authorized administrator using the CLI.

The HP 6125XLG Ethernet Blade Switch has a fixed number of ports: four (4) 40 GbE (QSFP+) ports; and Eight (8) 10 GbE (SFP+) ports. In the evaluated configuration, the switch can be deployed as a single switch device or alternately as a group of up to four devices connected using the HP Intelligent Resilient Framework (IRF) technology to effectively form a logical switch device. The IRF technology requires that devices be directly connected to one another using an IRF stack using one or more dedicated Ethernet connections that are used to coordinate the overall logical switch configuration and also to forward applicable network traffic as necessary between attached devices. The IRF technology does not require that switches be co-located, but can be attached using standard LACP for automatic load balancing and high availability. Note that the IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must be collocated and the IRF connections need to be as protected as the IRF group devices themselves.

The HP 6125XLG Ethernet Blade Switch supports plug-in modules, which provide additional functionality (e.g., various numbers and types of network connection ports). All of the available plug-in modules are included in the evaluated configuration (see below).

2.1 TOE Overview

The HP 6125XLG Ethernet Blade Switch is a Gigabit Ethernet switch appliance that consists of hardware and software components. The software used is Comware V7.1 and is common code base of a modular nature with only the modules applicable for the specific hardware installed.

The HP 6125XLG Ethernet Blade Switch features 240Gb uplink bandwidth; 160Gb available server side bandwidth; 4x10Gb QSFP+ ports; and either 1Gb or 10Gb SFP+ ports depending on the module inserted. Additionally, the switch provides dedicated 4x10GB internal cross-connect ports between adjacent switches; as well as wire speed switching and IPv6 support with full Layer 2 and Layer 3 features.

The HP Intelligent Resilient Framework (IRF) is also supported for virtualization, such that up to four devices can be grouped together and managed as a single switch with a single IP address, which simplifies the deployment and management of top-of-rack switches, as well as reduces data center deployment and operating expenses. The IRF technology simplifies the architecture of server access networks, such that the switches can deliver unmatched scalability of virtualized access layer switches and flatter, two-tier FlexFabric networks using IRF.

The following modules, extending the physically available ports, are supported by the HP 6125XLG Ethernet Blade Switch and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP X120 1G SFP LC SX 850nm Transceiver JD118B
- HP X120 1G SFP LC LX 1310nm Transceiver JD119B
- HP X125 1G SFP LC LH40 1310nm Transceiver JD061A
- HP X120 1G SFP LC LH40 1550nm Transceiver JD062A
- HP X125 1G SFP LC LH70 1550nm Transceiver JD063B
- HP X120 1G SFP LC RJ45 T Transceiver JD089B
- HP BLc 1Gb SFP LC SX 850nm Transceiver
  NOTE: Using these transceivers/cables will display a console warning on the switch. It is recommended that the warnings be disregarded when using these transceivers/cables. 453151-B21
- HP BLc 1Gb SFP LC RJ45 T Transceiver
  NOTE: Using these transceivers/cables will display a console warning on the switch. It is recommended that the warnings be disregarded when using these transceivers/cables.453154-B21
- HP X130 10G SFP+ LC SR 850nm Transceiver JD092B
- HP X130 10G SFP+ LC LRM 1310nm Transceiver JD093B
- HP X130 10G SFP+ LC LR 1310nm Transceiver JD094B
- HP X130 10G SFP+ LC ER 1550nm Transceiver JG234A
- HP BladeSystem c-Class 10G SFP+ LC SR 850nm Transceiver
  NOTE: Using these transceivers/cables will display a console warning on the switch. It is recommended that the warnings be disregarded when using these transceivers/cables. 455883-B21
- HP BladeSystem c-Class 10G SFP+ LC LR 1310nm Transceiver

NOTE: Using these transceivers/cables will display a console warning on the switch. It is recommended that the warnings be disregarded when using these transceivers/cables. 455886-B21

- HP X140 40G QSFP+ MPO SR4 850nm Transceiver JG325A

2.2 TOE Architecture

The HP 6125XLG Ethernet Blade Switch comprising the TOE includes a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks, a data link layer, layer 2 and 3 routing, Ethernet switching, VLANs, Intelligent Resilient Framework (IRF) routing, Quality of Service (QoS), etc. The evaluated version of Comware is V7.1. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux.

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

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

Comware V7.1 optimizes the following functions:

- Virtualization—Supports N:1 virtualization.
- ISSU—Supports ISSU for line cards.
- Auxiliary CPU and OAA—Improve scalability for devices.

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

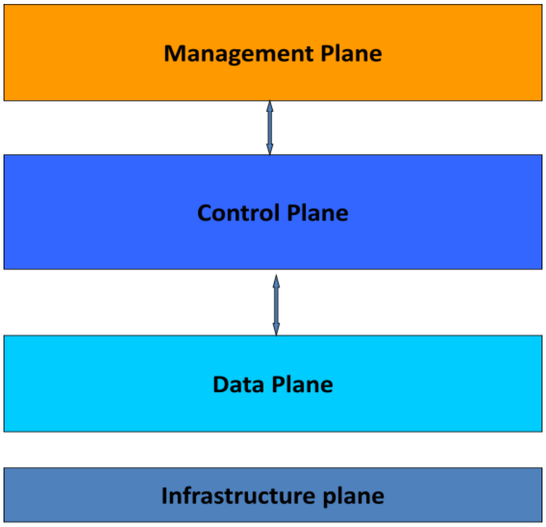

Figure 1 Comware V7.1 Architecture

- ***Infrastructure plane*** – 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.
- ***Data plane*** – The data plane provides data forwarding for local packets and received IPv4 and IPv6 packets at different layers.

- ***Control plane*** – The control plane comprises all routing, signaling, and control protocols, such as MPLS, OSPF, and security control protocols. It generates forwarding tables for the data plane.
- ***Management plane*** – The management plane provides a management interface for administrators and operators to configure, monitor, and manage Comware V7.1. The management interface comprises a CLI accessed using SSH.

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

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

2.2.1 Intelligent Resilient Framework

As indicated above, multiple devices in the evaluated configuration can be deployed as an IRF group. Each device in the IRF group is directly connected to the other IRF group members using an IRF stack using dedicated network connections. One device in the group is designated as master and should that device fail a voting procedure ensues to elect a new master among the remaining IRF group members.

Note that the IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must be collocated and the IRF connections need to be as protected as the IRF group devices themselves. The IRF is excluded from the evaluation.

2.2.2 Multitenant device context

Multitenant device context (MDC) is a 1:N virtualization technology. It virtualizes the data plane, control plane, and management plane of a physical device to create multiple logical devices called MDCs. MDCs use the same kernel, but their data is separated. Each MDC has its own interfaces and CPU resources. Rebooting an MDC does not affect the configuration or service of any other MDC.

The modular design of Comware V7.1 enables each MDC to run its own control protocol processes on a separate control plane. A process failure of an MDC does not affect other MDCs.

Note that since this technology is not covered in the NDPP, the Multitenant device context (MDC) was not subject to evaluation.

2.2.3 Physical Boundaries

A TOE device (HP 6125XLG Ethernet Blade Switch) is a physical network rack-mountable appliance with a fixed number of ports. The switch has four (4) 40 GbE (QSFP+) ports, eight (8) 10 GbE (SFP+) ports, and 1 Console port to front panel, 16 10 GbE internal ports to backplane, and 4 10GbE cross-connect ports.

The TOE can be configured to rely on and use a number of other components in its operational environment.

- Syslog server – to receive audit records when the TOE is configured to deliver them to an external log server.
- RADIUS and TACACS servers – The TOE can be configured to use external authentication servers.
- Management Workstation – The TOE supports CLI access and as such an administrator would need an SSHv2 client to use the administrative interface.

2.2.4 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Cryptographic support
- User data protection

- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

2.2.4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events including the events specified in NDPP. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to a designated external log server.

2.2.4.2 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's configuration is consistent with the FIPS 140-2 standard.

2.2.4.3 User data protection

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

2.2.4.4 Identification and authentication

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

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

2.2.4.5 Security management

The TOE provides Command Line (CLI) commands to access the wide range of 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.

2.2.4.6 Protection of the TSF

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

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE uses a clock managed by the OS for reliable time clock information that the TOE uses (e.g., for log accountability).

The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of a Syslog server or authentication servers in the operational environment, the communication between the TOE and the operational environment component is protected using encryption.

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

2.2.4.7 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.

2.2.4.8 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 a log server, and authentication servers (RADIUS and TACACS) using IPsec connections to prevent unintended disclosure or modification of logs.

2.3 TOE Documentation

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

- “Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125XLG Network Switch based on Comware V7”, v1.02, dated 02/19/2015
- “Command Reference for CC Supplement”, Revision # v1.04, dated 02/19/2015
- “Configuration Guide for CC Supplement”, Revision # v1.5 dated 02/19/2015
- “Comware V7.1 Platform System Log Messages”, Revision # v0.25, dated 4/21/2014.

These documents are distributed by the HP Federal sales and support team as part of the sales delivery process.

The links in Appendix A for each series can be used to find the remaining documentation for each of the evaluated switch series. The following documents (available for each series) were specifically examined during the evaluation.

- *Security Configuration Guide*
- *Security Command Reference*
- *Fundamentals Configuration Guide*
- *Fundamentals Command Reference*
- *Network Management and Monitoring Configuration Guide*
- *Network Management and Monitoring Command Reference*
- *ACL and QoS Configuration Guide*
- *ACL and QoS Command Reference*
- *Layer-3 IP Services Configuration Guide*
- *Layer-3 IP Services Command Reference*
- *Installation Guide*

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumption) from the NDPP.

In general, the NDPP has presented a Security Problem Definition appropriate for network infrastructure devices, such as switches, and as such is applicable to the HP TOE.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the NDPP. The NDPP security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the NDPP has presented a Security Objectives appropriate for network infrastructure devices, such as switches, and as such are applicable to the HP TOE.

4.1 Security Objectives for the Operational Environment

OE.NO_GENERAL_PURPOSE	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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Protection Profile for Network Devices, Version 1.1, 8 June 2012* (NDPP), as amended by Errata #2. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the NDPP made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in NDPP.

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the NDPP. The NDPP defines the following extended SFRs and since they are not redefined in this ST, the NDPP should be consulted for more information in regard to those CC extensions.

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_IPSEC_EXT.1: Explicit: IPSEC
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_SSH_EXT.1: Explicit: SSH
- FIA_PMG_EXT.1: Password Management
- FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the HP Switches.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1: Explicit: IPSEC
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1: Explicit: SSH
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) Specifically defined auditable events listed in **Table 2**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of **Table 2**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	
FCS_SSH_EXT.1	Failure to establish an SSH session.	Reason for failure
	Establishment/Termination of an SSH session.	Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	
FIA_PSK_EXT.1	None.	
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of the authentication and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT_APW_EXT.1	None.	
FPT_SKP_EXT.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel.	Identification of the initiator and

Requirement	Auditable Events	Additional Audit Record Contents
	Termination of the trusted channel. Failure of the trusted channel functions.	target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 2 Auditable Events

5.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1 The TSF shall be able to [***transmit the generated audit data to an external IT entity***] using a trusted channel implementing the [***IPsec***] protocol.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

FCS_CKM.1.1 Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- ***NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes***]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.2.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.2.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1(1).1 Refinement: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES operating in [**CBC, /CTR/**] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- [***NIST SP 800-38A***].

5.2.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1(2).1 Refinement: The TSF shall perform cryptographic signature services in accordance with a [

(1) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater,

that meets the following:

Case: RSA Digital Signature Algorithm

- FIPS PUB 186-2 or FIPS PUB 186-3, 'Digital Signature Standard'.

5.2.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1(3).1 Refinement: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-512***] and message digest sizes [***160, 256, 512***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

FCS_COP.1(4).1 Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1, SHA-256***], key size [**160 bits, 256 bits**], and message digest sizes [***160, 256***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.7 Explicit: IPSEC (FCS_IPSEC_EXT.1)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement **[*tunnel mode, transport mode*]**.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using **[*the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, [no other algorithms]*]**.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: **[*IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109*, [*no other RFCs for extended sequence numbers*], and [*RFC 4868 for hash functions*]]**.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the **[*IKEv1*]** protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and **[*no other algorithm*]**.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that **[*IKEv1 SA lifetimes can be established based on* [*number of packets/number of bytes*]]**.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and **[*no other DH groups*]**.

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [***RSA***] algorithm and Pre-shared Keys.

5.2.2.8 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using [CTR_DRBG (AES)]***] seeded by an entropy source that accumulated entropy from [***a software-based noise source***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.2.2.9 Explicit: SSH (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [***5656***].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [**256K**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [***no other algorithms***].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [***SSH_RSA***] and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***hmac-sha1, hmac-sha1-96***].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

5.2.3 User data protection (FDP)

5.2.3.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.2.4 Identification and authentication (FIA)

5.2.4.1 Extended: Pre-Shared Key Composition (FIA_PSK_EXT.1)

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [***[lengths from 15 to 128 characters]***];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using **[*[the bit representation of the ASCII coding of the entered characters as the key]*]** and be able to **[*accept bit-based pre-shared keys*]**.

5.2.4.2 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, [“'”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “[”, “\”, “]”, “_”, “`”, “{”, “}”, and “~”]];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.2.4.3 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.2.4.4 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [***[and access to external RADIUS and TACACS]***] to perform administrative user authentication.

5.2.4.5 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [[network switching services]].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.2.5 Security management (FMT)

5.2.5.1 Management of TSF Data (for general TSF data) (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

5.2.5.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using the [digital signature] capability prior to installing those updates; [
- ***Ability to configure the cryptographic functionality***].

5.2.5.3 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.2.6.2 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.6.3 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2.6.4 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2.6.5 Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [***digital signature mechanism***] prior to installing those updates.

5.2.7 TOE access (FTA)

5.2.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 Refinement: The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.2.7.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.2.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.2.7.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1 Refinement: Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.2.8 Trusted path/channels (FTP)

5.2.8.1 Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 Refinement: The TSF shall use [***IPsec***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***[authentication server]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server, and external authentication functions**].

5.2.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 Refinement: The TSF shall use [***SSH***] **to** provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administrative actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the NDPP.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 3 Assurance Components

Consequently, the assurance activities specified in NDPP apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in **Table 2** (which corresponds to the audit events specified in NDPP). Note that the only protocol (i.e., IPsec, SSH) failures auditable by the TOE are authentication failures for user-level connections.

The logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user) responsible for the event (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in **Table 2**.

The TOE includes an internal log implementation that can be used to store and review audit records locally. The maximum storage space reserved for the local log file can be configured to a range between 1 and 10MB. When the local log storage is full, the TOE will overwrite the oldest records with new records. Only users with the role network-admin, network-operator, or level-15 can access the local audit trail. Alternately, the TOE can be configured to send generated audit records to an external Syslog server using IPsec.

Note that audit records are not buffered for transmission to the syslog server. If the connection to the syslog server goes down, generated audit records are not queued and will not be transmitted to the syslog server when the connection is re-established. However, audit records will still be delivered to any other configured audit destinations, such as the log buffer and local log file. Additionally, the TOE generates audit records when connection to the syslog server is lost and when it is restored, and these audit records are sent to any other configured audit destinations. Therefore, the administrator is advised to ensure additional audit destinations are configured so that generated audit records will still be available for review in the event of loss of connectivity to the syslog server. In addition, multiple log servers can be configured to provide redundancy.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in **Table 2**. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 2**.
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external Syslog server and can be configured to use IPsec for communication with the Syslog server.

6.2 Cryptographic support

The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions. The following functions have been certified in accordance with the identified standards.

Functions	Standards	Certificates
Asymmetric key generation		
• Domain parameter generation (key size 2048 bits)	NIST Special Publication 800-56B	Component Test #341
Encryption/Decryption		
● AES CBC and CTR(128-256 bits)	FIPS PUB 197 NIST SP 800-38A	#2943
Cryptographic signature services		
● RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2 FIPS PUB 186-3	#1546
Cryptographic hashing		
● SHA-1, SHA-256 and SHA-512 (digest sizes 160 , 256 and 512 bits)	FIPS Pub 180-3	#2479
Keyed-hash message authentication		
● HMAC-SHA-1 (key size 160 bits and digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	#1866
● HMAC-SHA-256 (key size 256 bits and digest size 256 bits)	FIPS Pub 198-1 FIPS Pub 180-3	#1866
Random bit generation		
● CTR-DRBG(AES) with one independent software-based noise source of 256 bits of non-determinism	NIST Special Publication 800-90A	#546

Table 4 Cryptographic Functions

The following table demonstrates that the TSF complies with 800-56B. The table identifies the sections in 800-56B that are implemented by the TSF; and the “should”, “should not”, and “shall not” conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized. Key establishment is among the identified sections.

NIST SP800-56B Section Reference	“should”, “should not”, or “shall not”	Implemented accordingly?	Rationale for deviation
5.6	should	yes	
5.8	shall not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
5.9	shall not (first occurrence)	yes	
5.9	shall not (second occurrence)	yes	
6.1	should not	yes	
6.1	should (first occurrence)	yes	
6.1	should (second occurrence)	yes	
6.1	should (third occurrence)	yes	
6.1	should (fourth occurrence)	yes	
6.1	shall not (first occurrence)	yes	
6.1	shall not (second occurrence)	yes	
6.2.3	should	yes	
6.5.1	should	yes	
6.5.2	should	yes	
6.5.2.1	should	yes	

NIST SP800-56B Section Reference	“should”, “should not”, or “shall not”	Implemented accordingly?	Rationale for deviation
6.6	shall not	yes	
7.1.2	should	yes	
7.2.1.3	should	yes	
7.2.1.3	should not	yes	
7.2.2.3	should (first occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (second occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (third occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should (fourth occurrence)	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	should not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.2.3	shall not	no	RSA-OAEP is not supported. The device supports RSA-PKCS1 Padding
7.2.3.3	should (first occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (second occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (third occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (fourth occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should (fifth occurrence)	no	RSA-KEM-KWS is not supported
7.2.3.3	should not	no	RSA-KEM-KWS is not supported
8	Should	yes	
8.3.2	should not	yes	

Table 5 NIST SP800-56B Conformance

The TOE uses a software-based deterministic random bit generator that complies with NIST SP 800-90, using CTR_DRBG (AES). The entropy source is a 256-bit value derived from Comware entropy pool. The design architecture of the Comware entropy source is the same as the architecture of the Linux kernel entropy pool. The noise sources for the Comware entropy pool include interrupt, process scheduling and memory allocation.

The TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. **Table 6** identifies the applicable secret and private keys and summarizes, how and when they are deleted. Note that only some of the keys and CSPs are applicable to the evaluation. Also note that where identified zeroization occurs as follows: 1) when deleted from FLASH, the previous value is overwritten once with zeroes; 2) when added or changed in FLASH, any old value is overwritten completely with the new value; and, 3) the zeroization of values in RAM is achieved by overwriting once with zeroes.

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
Public key management						

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
CSP1-1	RSA private key	CTR_DRBG (AES)/RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPsec and SSH negotiations.	FLASH (cipher text / AES-CTR 256)	Using CLI command “**public-key local destroy rsa** …” to zeroize.
CSP1-2	DSA private key	CTR_DRBG (AES)/DSA	2048 bits	Identity certificates for the security appliance itself and also used in SSH negotiations.	FLASH (cipher text /AES-CTR 256)	Using CLI command “**public-key local destroy dsa** …” to zeroize
CSP1-3	Public keys	DSA / RSA	RSA:1024 ~ 2048 bits DSA: 1024 ~ 2048 bits	Public keys of peers to validate the digital signature	FLASH(plain text)	Peer public keys exist in a FLASH start-up configuration file. Using CLI commands “**undo public-key peer** “ and “**save**” to zeroize the public keys.
IPsec						
CSP2-1	IPsec authentication keys	Generated using IKE protocol (CTR_DRBG (AES)+HMAC-SHA1/HMAC-SHA256+DH). Algorithms: HMAC-SHA1-96	160 bits	Used for authenticating the IPsec traffic	RAM (plain text)	Zeroized upon deleting the IPsec session.
CSP2-2	IPsec encryption keys	Generated using IKE protocol (CTR_DRBG (AES)+HMAC-SHA1/HMAC-SHA256+DH). Algorithms: AES	128 bits 192 bits 256 bits Note: 192 – bit keys are not used in the evaluated configuration	Used for encrypting the IPsec traffic	RAM (plain text)	Zeroized upon deleting the IPsec session.
CSP2-3	IPsec authentication keys	HMAC-SHA1-96	160 bits	Manually configured key used for authenticating the IPsec traffic.	FLASH (cipher text / AES-CTR 256) and RAM (plain text)	Keys will be zeroized using CLI commands “**undo sa hex-key authentication …**” and “ **save**”,
CSP2-4	IPsec encryption keys	AES	128 bits 192 bits 256 bits Note: 192 – bit keys are not used in the evaluated configuration	Manually configured key used for encrypting the IPsec traffic.	FLASH (cipher text / AES-CTR 256) and RAM (plain text)	Keys will be zeroized using CLI commands “**undo sa hex-key encryption …**” and “ **save**”,
IKE						

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
CSP3-1	IKE pre-shared keys	Shared Secret	15 ~ 128 bytes	Entered by the Crypto-Officer in plain text form and used for authentication during IKE	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Keys will be zeroized using CLI commands “**undo pre-shared-key …**” and “ **save**”,
CSP3-2	IKE RSA Authentication private Key	RSA	2048 bits	private key used for IKE protocol during the handshake	RAM(plain text)	Automatically zeroized upon handshake finishing
CSP3-3	IKE DSA Authentication private Key	DSA	2048 bits	private key used for IKE protocol during the handshake	RAM(plain text)	Automatically zeroized upon handshake finishing
CSP3-4	IKE Diffie-Hellman Key Pairs	CTR_DRBG (AES) / DH	2048 bits	Key agreement for IKE	RAM (plain text)	Automatically zeroized upon handshake finishing
CSP3-5	IKE Authentication key	Generated using IKE (CTR_DRBG (AES)+HMAC-SHA1/HMAC-SHA256+DH). Algorithms: HMAC-SHA1, HMAC-SHA256	160 bits 256 bits	Used for authenticating IKE negotiations	RAM (plain text)	Zeroized upon deleting the IKE session.
CSP3-6	IKE Encryption Key	Generated using IKE (CTR_DRBG (AES)+HMAC-SHA1/HMAC-SHA256+DH). Algorithms: AES	128 bits, 192 bits, 256 bits Note: 192 –bit keys are not used in the evaluated configuration	Used for encrypting IKE negotiations	RAM (plain text)	Zeroized upon deleting the IKE session.
SSH						
CSP4-1	SSH RSA Private key	RSA	2048 bits	private key used for SSH protocol during handshake	RAM(plain text)	Automatically zeroized upon finishing handshake.
CSP4-2	SSH Diffie-Hellman Key Pairs	CTR_DRBG (AES) / DH	2048 bits	Key agreement for SSH sessions.	RAM (plain text)	Automatically zeroized upon finishing handshake.
CSP4-3	SSH Session encryption key	Generated using the SSH protocol(CTR_DRBG(AES)+SHA1+DH) Algorithms: AES	128 bits, 256 bits	Key used for encrypting SSH session.	RAM (plain text)	Automatically zeroized when SSH session terminated.

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
CSP4-4	SSH Session authentication key	Generated using the SSH protocol(CTR_DRBG(AES)+SHA1+DH) Algorithms: HMAC-SHA1, HMAC-SHA1-96	160 bits	Key used for authenticating SSH session.	RAM (plain text)	Automatically zeroized when SSH session terminated.
AAA						
CSP5-1	User Passwords	Secret	15 ~ 63 bytes	Critical security parameters used to authenticate the administrator login.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Use CLI command "**password**" to set new password, or use CLI command "**undo local-user** …" to zeroize the password and delete user account.
CSP5-2	Super password	Secret	15 ~ 63 bytes	Critical security parameters used to authenticate privilege promoting.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Use CLI command "**undo super password**" to zeroize the super password.
CSP5-3	RADIUS shared secret keys	Shared Secret	15 ~ 64 bytes	Used for authenticating the RADIUS server to the security appliance and vice versa. Entered by the Security administrator in plain text form and stored in cipher text form.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Keys will be zeroized using following commands: "**undo primary authentication**", ""**undo primary accounting",** "**undo secondary authentication**", ""**undo secondary accounting".**
CSP5-4	TACACS+ shared secret keys	Shared Secret	15~255 bytes	Used for authenticating the TACACS+ server to the security appliance and vice versa. Entered by the Security administrator in plain text form and stored in cipher text form.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Keys will be zeroized using following commands: "**undo primary authentication**", ""**undo primary accounting",** ""**undo primary authorization",** "**undo secondary authentication**", ""**undo secondary accounting",** ""**undo secondary authorization".**
Random Bits Generation						

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
CSP6-1	DRBG seed	Entropy / SP 800‐90 CTR_DRBG	256 bits	Input to the DRBG that determines the internal state of the DRBG	RAM (plaintext)	Automatically zeroized when DRBG initialized
CSP6-2	DRBG V	SP 800‐90 CTR_DRBG	128 bits	Generated by entropy source via the CTR_DRBG derivation function	RAM (plaintext)	Resetting or rebooting the security appliance
CSP6-3	DRBG Key	SP 800‐90 CTR_DRBG	256 bits	Generated by entropy source via the CTR_DRBG derivation function	RAM (plaintext)	Resetting or rebooting the security appliance
SNMPv3						
CSP7-1	SNMPv3 Authentication Key	SHA1	160 bits	Used to verify SNMPv3 packet.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Using CLI command "**undo snmp-agent usm-user v3 ...**" to zeroize
CSP7-2	SNMPv3 Encryption Key	AES	128 bits	Used to encrypt SNMPv3 packet.	FLASH(cipher text/ AES-CTR 256) and RAM (plain)	Using CLI command "**undo snmp-agent usm-user v3 ...**" to zeroize
TLS (*note that TLS is not included in the evaluated configuration***)**						
CSP8-1	TLS Server RSA private key	RSA	2048 bits	private key used for TLS negotiations.	RAM (plain text)	Automatically zeroized when handshake finishing
CSP8-2	TLS Master secret	Generated using the TLS protocol (CTR_DRBG (AES) + SHA1+MD5 + RSA)	384 bits	Shared secret used for creating TLS traffic keys.	RAM (plain text)	Automatically zeroized when session terminated.

#	Key/ CSP Name	Generation/ Algorithm	Key Size	Description	Storage	Zeroization
CSP8-3	TLS Traffic encryption key	Generated using the TLS protocol (SHA1+MD5) Algorithms: AES	128 bits 256 bits	Used for encrypting TLS data.	RAM (plain text)	Automatically zeroized when session terminated.
CSP8-4	TLS traffic authentication key	Generated using the TLS protocol (SHA1+MD5) Algorithms: HMAC-SHA1	160 bits	Used for authenticating HTTPS data.	RAM (plain text)	Automatically zeroized when session terminated.

Table 6 Key/CSP Zeroization Summary

These supporting cryptographic functions are included to support the SSHv2 (RFCs 4251, 4252, 4253, and 4254) secure communication protocol.

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1 or HMAC-SHA-1-96, and RSA (with diffie-hellman-group14-sha1 for the key exchange method). While DES and 3DES (CBC), HMAC-MD5 and HMAC-MD5-96, as well as diffie-hellman-group-1 and diffie-hellman-exchange are all implemented, they are disabled while the TOE is operating in CC/FIPS mode.

SSHv2 connections are rekeyed prior to reaching 2^{28} packets; the default authentication timeout period is 60 seconds allowing clients to retry only 3 times; both public-key and password based authentication can be configured; and packets are limited to 256K bytes. Note that the TOE manages a packet counter for each SSH session so that it can initiate a new key exchange when the 2^{28} packet limit is reached. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256K bytes) the packet will be dropped.

The TOE includes an implementation of IPsec in accordance with RFC 4301. The TOE’s implementation of IPsec supports both tunnel mode and transport mode. The primary cryptographic algorithms used by the TOE include AES-CBC-128 and AES-CBC-256 (both specified by RFC 3602) along with IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109. Note that the TOE supports both main and aggressive modes, though aggressive mode is disabled in CC/FIPS mode as indicated above. Furthermore, “confidentiality only” ESP mode is disabled by default. HMAC SHA-1 (key size 160 bits) and HMAC SHA-256 (key size 256 bits) are used in support of the IPsec protocol ESP (FCS_IPSEC_EXT.1.4). IKE authentication keys are generated using the HMAC algorithms. The keys are used for authenticating IKE negotiations and IPsec traffic authentications and subsequent traffic encryption. HMAC SHA for IPsec key authentication and encryption can be generated by using IKE commands.

The TOE provides mechanisms to implement an IPsec Security Policy Database (SPD) and to process packets to satisfy the behavior of DISCARD, BYPASS and PROTECT packet processing as described in RFC 4301. This is achieved through the administrator configuring appropriately specified access control lists (ACLs). The administrator first establishes an IPsec Policy containing a Security ACL to match traffic to be encrypted (PROTECTed) and applies it to the outbound interface. The Security ACL contains one or more rules, which are ordered based on a numeric index from lowest to highest. The TOE compares packets in turn against each rule in the Security ACL to determine if the packet matches the rule. Packets can be matched based on protocol (e.g., TCP, UDP), source IP address and destination IP address. As soon as a match is found, the packet is handled based on the action specified in the rule—either **permit**, which equates to PROTECT, or **deny**, which equates to BYPASS. Traffic matching a **deny** rule or not matching any rule in the Security ACL is passed on to the next stage of processing. Note that multiple IPsec Policies can be assigned to an interface as a policy group. In this case, each policy in the group has its own priority number that is unique within the policy group. Each policy is considered in turn, starting at the lowest number policy (which has highest priority) and proceeding in turn with increasing policy numbers until a match is found or until all policies have been examined. To cater for packets that match a **deny** rule or do not match any of the IPsec Policies, the administrator needs to configure further ACLs and bind them to the outbound interface using the "`packet-filter`" command. These ACLs specify permit/deny rules to implement BYPASS/DISCARD behavior. As with the Security ACL, the TOE compares packets against rules in the Firewall ACL based on protocol, source IP address and destination IP address. The rules in the Firewall ACL can be ordered in the same fashion as in a Security ACL. In the Firewall ACL, a **permit** rule equates to BYPASS, and a **deny** rule equates to DISCARD. By default, the packet filter permits packets that do not match any ACL rule to pass.

IKEv1 SA lifetime volume limits can be configured by an authorized administrator and can be limited to as little as 2.5 MB (actually any value between 2,560 and 4,294,967,295 KB) of traffic for phase 2. The IKEv1 protocols implemented by the TOE includes DH Groups 2 (1024-bit MODP), 5 (1536-bit MODP), and 14 (2048-bit MODP) and use RSA (aka rDSA) peer authentication. However, when the TOE is operating in FIPS mode only DH Group 14 is supported. In the IKEv1 phase 1 and phase 2 exchanges, the TOE and peer will agree on the best DH group both can support. When the TOE initiates IKE negotiation, the DH group is sent in order according to the peer's configuration. When the TOE receives an IKE proposal, it will select the first match and the negotiation will fail if there is no match. During IKEv1 phase 1 authentication is based on a verifiable signature as described in RFC2409.

The TOE can be configured to use pre-shared keys with a given peer. When a pre-shared key is configured, the IPsec tunnel will be established using the configured pre-shared key, provided that the peer also has the pre-shared key. Text-based pre-shared keys used for IPsec can be constructed of essentially any alphabetic character (upper and lower case), numerals, and special characters (e.g., "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")") and can be anywhere from 15 to 128 characters in length (e.g., 22 characters). In this case, the TOE uses the bit representation of the underlying ASCII characters of the text-based pre-shared key as the key for IPsec peer authentication. The TOE can also accept bit-based pre-shared keys, which are entered as characters using hexadecimal notation—in this case, the TOE uses the bit value represented by the hexadecimal string, rather than the bit representation of the underlying ASCII characters, as the key for IPsec per authentication. The TOE requires suitable keys to be entered by an authorized administrator.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: See table above.
- FCS_CKM_EXT.4: See table above.
- FCS_COP.1(1): See table above.
- FCS_COP.1(2): See table above.
- FCS_COP.1(3): See table above.
- FCS_COP.1(4): See table above.
- FCS_IPSEC_EXT.1: The TOE supports IPsec cryptographic network communication protection.
- FCS_RBG_EXT.1: See table above.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FIA_PSK_EXT.1: The TOE supports pre-shared keys for IPsec peer authentication.

6.3 User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the TOE operations. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

When a network packet is sent, the buffer used by the packet is recalled and managed by the buffer pool. After that, if a new packet acquires a buffer from the buffer pool, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, the additional space will be overwritten (padded) with zeros.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects.

6.4 Identification and authentication

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions. Note that the normal switching of network traffic is not considered accessing TOE functions in this regard.

In the evaluated configuration, users can connect to the TOE CLI via a local console or remotely using SSHv2. For each session, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. Note that the only capabilities allowed prior to users authenticating are the display of the warning banner before authentication, and network switching services.

In order to log in, the user must provide acceptable user credentials (e.g., user id, password), after which they will be able to issue commands within their assigned authorizations. Users can be defined locally within the TOE with a user identity, password, and user role. Alternately, users can be defined within an external RADIUS or TACACS server configured to be used by the TOE each of which also defined the user’s role in the TOE. Locally defined users are authenticated directly by the TOE, while remotely defined users are authenticated by the external server and the result is enforced by the TOE. In either case, any resulting session is dependent upon successful authentication and established sessions are associated with the role(s) (see section 6.5) assigned to the user.

The TOE supports both public key-based and password-based client authentication for the SSH trusted path. To successfully establish an interactive administrative session, the authorized remote administrator must provide either the correct public key or both a password and the correct public key for successful authentication.

When logging in the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

Note also that should a console user have their session terminated (e.g., due to inactivity), they are required to successfully authenticate, by reentering their identity and authentication data, in order to establish a new session.

Passwords can be composed of upper and lower case letters, numbers and special characters, including blank space and ~`!@#$%^&*()_+-={}|[]\:”;’<>,./. Also, new passwords have to satisfy a configurable minimum password length. The administrator can specify a minimum password length of 15 to 32 characters.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_PMG_EXT.1: The TOE implements set of password composition constraints as described above.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.2: The TOE can be configured to use external RADIUS and TACACS authentication servers.
- FIA_UIA_EXT.1: The TOE only displays the warning banner and allows for network switching services prior to a user being identified and authenticated.

6.5 Security management

The TOE controls user access to commands and resources based on user role. Users are given permission to access a set of commands and resources based on their user role.
The TOE includes pre-defined user roles, of which only the user roles: network-admin and level-15, are considered instances of the ‘Security Administrator’ as defined in the NDPP. These Security Administrator roles are capable of managing the security functions of the TOE since they allow for security relevant configuration. These capabilities

include changing the user permission settings including user-role, authentication-mode, protocol, and setting the authentication password in user interface view.

The other roles represent logical subsets of those security management roles, but do not offer any security relevant configuration management capabilities. The other roles are limited to the ability to change a user's own password, non-security relevant functions and review of information. For example, the roles: network-operator, level-1 and level-9 can display the configuration and status of the TOE. The local audit log can only be accessed by those with the network-admin, network-operator, or level-15 role.

The TOE offers a CLI providing a range of security management functions for use by an authorized administrator. Among these functions are those necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Security Administrators.
- FMT_SMF.1: The TOE includes the functions necessary to enable/disable available network services, to manage the cryptomodule and associated functions, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes 19 predefined roles. As described above only the network-admin, and level-15 roles, that have been configured to access all security management functions of the TOE correspond to the required 'Security Administrator'.

6.6 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components to a large extent. Secure communication with third-party peers is addressed in section 6.8. Secure communication among multiple instances of the TOE, which is considered communication among collocated components that logically form an instance of the TOE, is limited to a direct link between redundant switch appliances deployed in a high-availability configuration to physically protect the IRF communication channels as the TOE devices themselves. Normally redundant components are co-located and connected via a link that would not be exposed outside of the same physical environment. As such, no additional protection (e.g., encryption) should be necessary in most operational environments.

Note that IRF groups are not considered peer switches in the IPsec (or VPN) sense. Rather IRF groups effectively form a logical instance of the TOE comprised of up to nine distinct devices. All those devices must be collocated and the IRF connections among them must be protected to the same degree as the devices themselves.

While the administrative interface is function rich, the TOE is designed specifically to prevent access to locally-stored cryptographically protected passwords and also, while cryptographic keys can be entered, the TOE does not disclose any keys stored in the TOE. In the evaluated configuration (i.e., with FIPS mode enabled), the TOE protects user passwords either by saving a SHA-512 hash of the password (for user accounts password that existed before FIPS mode was enabled) or by encrypting the password using AES in CTR mode (for user accounts password entered after FIPS mode was enabled). See Table 6 Key/CSP Zeroization Summary for more information about stored keys and passwords; note that while some keys and passwords occur in plain text in RAM, that is only while they are in use and are not accessible by any user from RAM.

The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The clock is used for audit record time stamps and measuring session activity for termination.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. The built-in self tests include basic read-write memory (i.e., each memory location is written with a non-zero value and read to ensure it is stored as expected), flash read, software checksum tests, and device detection tests. When operating in CC/FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing.

The TOE is designed to support upgrades to the boot ROM program and system boot file as well as to support software hotfixes. The TOE provides interfaces so that an administrator can query the current boot ROM program or system boot file versions as well as to identify any installed patches. Both the boot ROM program and system boot file can be upgraded via the Boot ROM menu or the command line interface, but a reboot is required in each case. Hotfixes, which can affect only the system boot file, can be installed via the command line interface and do not require a reboot to become effective.

The TOE includes a validity checking function that can be enabled when upgrading the boot ROM program, while system boot files and software patches are always validated prior to installation. In each case, the upgrade version will be checked to ensure it is appropriate and the upgrade file will be verified using an embedded (HP authorized) digital signature verified against a configured pair of hard-coded keys embedded in the TOE. If the version is incorrect or the signature cannot be verified, the upgrade will not proceed to protect the integrity of the TOE. More specifically, each update includes a header and data. The header includes a SHA-256 secure hash of the data that is signed (using rDSA/RSA 2048) by HP. In order to verify the data, the TOE generates its own SHA-256 secure hash of the update data, compares it with the signed hash in the update header to ensure they match, and verifies the hash signature using its configured public key.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Note that passwords are stored in cryptographically protected form within the TOE FLASH.
- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM.1: The TOE uses a clock managed by the OS for audit record time stamps, measuring session activity for termination, and for cryptographic operations.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.
- FPT_TUD_EXT.1: The TOE provides functions to query and upgrade the versions of the boot ROM program and system boot file (including installing hotfixes). Digital signatures are used to ensure the integrity of each upgrade prior to performing the upgrade; this checking is optional for the boot ROM program since special circumstances might require those checks to be disabled.

6.7 TOE access

The TOE can be configured to display administrator-configured advisory banners. A login banner can be configured to display warning information along with login prompts. The banner will be displayed when accessing the TOE via the console or SSH interfaces.

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout) – the default timeout is 10 minutes. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Note that the timer will stop when a command is issued (starts), and the timer will restart after completing the command. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to re-enter their user id and their password so they can establish a new session once a session is terminated. If the user id and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE provides the function to logout (or terminate) both local and remote user sessions as directed by the user.
- FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners in a variety of circumstances, including before establishing an administrative user session.

6.8 Trusted path/channels

The TOE can be configured to export audit records to an external Syslog server. The TOE uses IPsec to protect communications between itself and components in the operational environment including Syslog and authentication servers (RADIUS and TACACS).

To support secure remote administration, the TOE includes an implementation of SSHv2. An administrator with an appropriate SSHv2-capable client can establish secure remote connections with the TOE. The TOE supports both public key-based and password-based client authentication for the SSH trusted path. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

All of the secure protocols are supported by NIST-validated cryptographic mechanisms included in the TOE implementation.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TOE can be configured to use IPsec to ensure that sensitive data (exported audit records, time information, and authentication data) is not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSH to support secure remote administration. Administrators can initiate a remote session that is secured (from disclosure and modification) using NIST-validated cryptographic operations, and all remote security management functions require the use of this secure channel.

7. Protection Profile Claims

This ST is conformant to the *Protection Profile for Network Devices, Version 1.1, 8 June 2012* (NDPP), as amended by Errata #2 – with the optional SSH, IPsec and pre-shared key requirements.

The TOE is an Ethernet switch device. As such, the TOE is a network device making the NDPP claim valid and applicable.

As explained in section 3, Security Problem Definition, the Security Problem Definition of the NDPP has been included by reference into this ST.

As explained in section 4, Security Objectives, the Security Objectives of the NDPP have been included by reference into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is reproduced from the NDPP and operations completed as appropriate.

Requirement Class	Requirement Component	Source
FAU: Security audit	FAU_GEN.1: Audit Data Generation	NDPP
	FAU_GEN.2: User identity association	NDPP
	FAU_STG_EXT.1: External Audit Trail Storage	NDPP
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)	NDPP
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	NDPP
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)	NDPP
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)	NDPP
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)	NDPP
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)	NDPP
	FCS_IPSEC_EXT.1: Explicit: IPSEC	NDPP
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)	NDPP
	FCS_SSH_EXT.1: Explicit: SSH	NDPP
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection	NDPP
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management	NDPP
	FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition	NDPP
	FIA_UAU.7: Protected Authentication Feedback	NDPP
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism	NDPP
	FIA_UIA_EXT.1: User Identification and Authentication	NDPP
	FMT_MTD.1: Management of TSF Data (for general TSF data)	NDPP
	FMT_SMF.1: Specification of Management Functions	NDPP
	FMT_SMR.2: Restrictions on Security Roles	NDPP
FPT: Protection of the TSF	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	NDPP
	FPT_STM.1: Reliable Time Stamps	NDPP
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL.4: User-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	NDPP
	FTP_TRP.1: Trusted Path	NDPP

Table 7 SFR Protection Profile Sources

8. Rationale

This security target includes by reference the NDPP Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the NDPP assumptions. NDPP security functional requirements have been reproduced with the protection profile operations completed. Operations on the security requirements follow NDPP application notes and assurance activities. Consequently, NDPP rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_STG_EXT.1	X							
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_IPSEC_EXT.1		X						
FCS_RBG_EXT.1		X						
FCS_SSH_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UAU.7				X				
FIA_UAU_EXT.2				X				
FIA_UIA_EXT.1				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_APW_EXT.1						X		
FPT_SKP_EXT.1						X		
FPT_STM.1						X		
FPT_TST_EXT.1						X		
FPT_TUD_EXT.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_SSL_EXT.1							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

Table 8 Security Functions vs. Requirements Mapping

Appendix A: Documentation for HP 6125XLG Ethernet Blade Switch

This Appendix provides a list of the product documentation used during the evaluation of the HP 6125XLG Ethernet Blade Switch.

HP 6125XLG Ethernet Blade Switch

The following documents for the HP 6125XLG Switch can be found under the *General Reference* section of the HP 6125XLG Ethernet Blade Switch documentation page on the HP Web site. The link is provided below.

- R240x-HP 6125XLG Blade Switch ACL and QoS Command Reference
- R240x-HP 6125XLG Blade Switch Layer 3 - IP Services Command Reference
- R240x-HP 6125XLG Blade Switch Fundamentals Command Reference
- R240x-HP 6125XLG Blade Switch Security Command Reference
- R240x-HP 6125XLG Blade Switch Network Management and Monitoring Command Reference

http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr_r1002_usen_link3&lang=en&sp4ts.oid=5404487

The following documents for the HP 6125XLG Switch can be found under the *Setup and Install* section of the HP 6125XLG Ethernet Blade Switch documentation page on the HP Web site. The link is provided below.

- R2306-HP 6125XLG Blade Switch ACL and QoS Configuration Guide
- R2306-HP 6125XLG Blade Switch Layer 3 - IP Services Configuration Guide
- R2306-HP 6125XLG Blade Switch Fundamentals Configuration Guide
- R240x-HP 6125XLG Blade Switch Security Configuration Guide
- R240x-HP 6125XLG Blade Switch Network Management and Monitoring Configuration Guide

http://h20566.www2.hp.com/portal/site/hpsc/public/psi/manualsResults/?cc=us&jumpid=hpr_r1002_usen_link3&lang=en&sp4ts.oid=5404487