Hewlett-Packard Company
6125 Ethernet Blade Switch Series
Security Target

Version 2.3
26 June 2014

Prepared for:

Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

leidos

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

LIST OF TABLES

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 6125 Ethernet Blade Switch Series provided by Hewlett-Packard Development Company. Each of the devices included in the TOE is a Gigabit Ethernet blade switch designed to implement a 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 6125 Ethernet Blade Switch Series Security Target

ST Version – Version 2.3

ST Date – 26 June 2014

TOE Identification – Hewlett-Packard Company 6125 Ethernet Blade Switch Series with Comware version 5.20.99, Release 2108

Product Series	Specific Devices
HP 6125 Ethernet Blade Switches	HP 6125G Blade Switch
	HP 6125G/XG Blade Switch

Table 1 TOE Series and Devices

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 ST and the TOE it describes are conformant to the following CC specifications:

- *Protection Profile for Network Devices, Version 1.1, 8 June 2012*, 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 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
CLI	Command Line Interface
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
IPC	Inter-process communication
IPsec	Internet Protocol Security
IRF	Intelligent Resilient Framework
IT	Information Technology
LACP	Link Aggregation Control Protocol
NDPP	Protection Profile for Network Devices
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

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSF	TOE Security Functions
VLAN	Virtual Local Area Network

2. TOE Description

The Target of Evaluation (TOE) is the Hewlett-Packard 6125 Ethernet Blade Switch Series, comprising the 6125G and 6125G/XG Ethernet blade switches. The HP 6125 Ethernet blade switches are c-class blade-system switches that can be installed in the HP BladeSystem c3000 and c7000 enclosures and provide network connectivity to HP servers.

The TOE can be deployed as a single device or alternately as a group of 6125 Series devices connected using the HP Intelligent Resilient Framework (IRF) technology to effectively form a logical switch device. Using IRF, HP6125G and HP6125G/XG switches can be combined together at the enclosure, rack or datacenter level into a single virtual switch and managed through a single IP address for high bandwidth applications. The IRF technology does not require that switches be co-located, but can be attached using standard Link Aggregation Control Protocol (LACP) for automatic load balancing and high availability.

2.1 TOE Overview

The HP 6125 Ethernet Blade Switch Series devices are Gigabit Ethernet switch appliances consisting of hardware and software components. The underlying hardware shares a similar architecture and has the same form factor. The software is identical for the 6125G and 6125G/XG blade switches.

The HP 6125 Ethernet Blade Switch Series devices are used in network environments that include remote office applications, clustering, and virtual machine applications or wherever IPv6, full layer 3 routing and distributed trunking are required for 1GB applications.

HP 6125G Blade Switch

The basic functionality of the 6125G blade switch includes IRF technology that creates a virtual resilient switching fabric, where two or more switches perform as one logical device—this increases network resilience, performance, and availability while reducing operational complexity. The 6125G blade switch includes sixteen 1GB downlink (server) ports, up to eight 1GB uplink ports, up to two 10 GB IRF stacking ports and one 10GB cross-link port.

HP 6125G/XG Blade Switch

The HP 6125G/XG blade switches are available in a hybrid 1GB/10GB switch format. They include sixteen 1GB downlink server ports, a combination of 1GB and 10GB uplink ports, and a 10GB crosslink port.

The 6125G and the 6125G/XG both provide the following capabilities (note that these capabilities are not covered by the evaluation):

- wire speed switching and IPv4/IPv6 routing on all ports
- ability to combine up to 10 switches into a single virtual switch
- layer-2 switching support, including support for up to 4096 VLANs and jumbo packet support
- layer 3 routing support, including IPv6 tunneling and policy-based routing
- application of Quality of Service (QoS) policies such as priority level, rate limit on a per-port or per-VLAN basis.

2.2 TOE Architecture

The HP 6125 Ethernet Blade Switch Series devices share a common software code base, called Comware. Comware is special purpose appliance system software that implements an array of networking technology, including: IPv4/IPv6 dual-stacks; a data link layer; layer 2 and 3 routing; Ethernet switching; VLANs; IRF; routing; and QoS. The evaluated version of Comware is 5.20.99, Release 2108. It should be noted that although Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows, the only underlying architecture found in the evaluated configuration is Linux kernel 2.6.26.

The Comware v5.2 architecture can be depicted as follows:

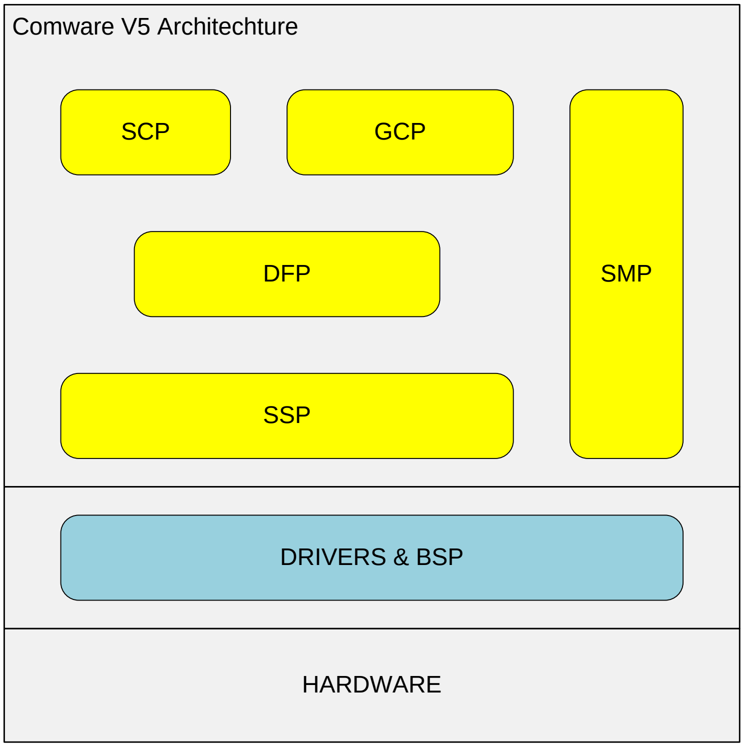

Figure 1 Comware v5.2 Architecture

- ***General Control Plane (GCP)* –** The GCP fully supports the IPv4 and IPv6 protocol stacks and provides support to a variety of IPv4/IPv6 applications including routing protocols, voice, WAN link features, and QoS features.

- ***Service Control Plane (SCP)* –** The SCP supports value-added services such as connection control, user policy management AAA, RADIUS, and TACACS+.
- ***Data Forwarding Plane (DFP)* –** The DFP underpins all network data processing. The forwarding engine is the core of the DFP.
- ***System Management Plane (SMP)* –** The SMP provides user interfaces for device management. This includes implementation of a Command Line Interface (CLI) accessible remotely via SSHv2.
- ***System Service Plane (SSP)* –** The SSP provides a foundation layer that implements primitives on which the other planes rely, for example, memory management, task management, timer management, message queue management, semaphore management, time management, IPC, RPC, module loading management and component management.

Underlying the main Comware components are the hardware-specific Board Support Package (BSP) and device drivers to provide necessary abstractions of the hardware components for the higher-level software components.

The Comware software components are composed of 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 stack, as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE includes NIST-validated cryptographic mechanisms that support IPsec, SSH and also digital signatures used to protect the available remote management and to enable secure update capabilities of the TOE. Otherwise, the TOE implements a wide range of network switching protocols and functions.

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

2.2.1 Intelligent Resilient Framework

As indicated above, the HP 6125 Ethernet Blade Switch Series devices can be deployed as an IRF group. Each device in the IRF group is directly connected to the other IRF group members by physically connecting to the physical IRF ports of member switches. 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.

All devices in the group share the same configuration, which is shared across the IRF connections when the group is formed and later when configuration changes occur. Management of the IRF group can occur via any of the IRF group members by an authorized administrator.

Once configured, the IRF group acts as a single, logical switch with a common configuration and will act to receive and forward network traffic in accordance with that common configuration. When necessary, network traffic is forward through the IRF connection in order to get the network traffic to and from the applicable physical network connections used to attach other network peers or clients.

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.

2.2.2 Physical Boundaries

The TOE is a physical network blade switch appliance (or IRF connected group of appliances) specifically designed to fit in the c-Class Blade-System HP c3000 and HP c7000 enclosures[1] that support modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber), and performance (1 – 10 Gb).

The TOE can be configured to rely on and utilize 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.

[1] A c-Class Blade-System enclosure is not a required component of the TOE environment.

- RADIUS and TACACS servers – The TOE can be configured to utilize external authentication servers.
- Management Workstation – The TOE supports remote CLI access and as such a remote administrator would need a terminal emulator supporting SSHv2 to utilize the administrative interface.

2.2.3 Logical Boundaries

This section summarizes the security functions provided by HP 6125 Ethernet Blade Switch Series:

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

2.2.3.1 Security Audit

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

2.2.3.2 Cryptographic Support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, symmetric encryption/decryption, digital signature services, secure hashing and keyed-hash message authentication capabilities in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that in order to be in the evaluated configuration, the TOE must be configured in FIPS mode, to ensure that the TOE is consistent with the FIPS 140-2 standard.

2.2.3.3 User Data Protection

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

2.2.3.4 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 (CLI via 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 utilize the services of trusted RADIUS and TACACS servers in the operational environment to support, for example, centralized user administration.

2.2.3.5 Security Management

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

2.2.3.6 Protection of the TSF

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

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

When deployed as an IRF group, all devices that are part of the IRF group are co-located and directly connected to form one instance of the TOE. IRF communication is not considered communication between distributed TOE components; rather, it is communication among co-located components that logically form an instance of the TOE. Since the IRF communication channels are not protected using mechanisms such as encryption, they need to be as protected as the TOE devices themselves.

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.

2.2.3.7 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 banners will be displayed 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.

2.2.3.8 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 an audit server, 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, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

- *Preparative Procedures for CC NDPP Evaluated Hewlett-Packard 6125G & 6125G/XG Network Switches based on Comware V5*, Version 1.04, 24 June 2014
- *Command Reference for CC Supplement*, Version 1.03, 24 June 2014
- *Configuration Guide for CC Supplement*, Version 1.03, 25 June 2014
- *Comware V5 Platform System Log Messages*, Version 1.21, 4 June 2014

The links in Appendix A for the HP 6125 Ethernet Blade Switch Series can be used to find the full set of documentation for the evaluated switch series. The following documents were specifically examined during the evaluation:

- *ACL and QoS Command Reference*
- *ACL and QoS Configuration Guide*
- *Fundamentals Command Reference*
- *Fundamentals Configuration Guide*
- *High Availability Command Reference*
- *High Availability Configuration Guide*

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

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

- HP 6125G Blade Switch specifications

  http://h17007.www1.hp.com/us/en/networking/products/switches/HP_6125G_Blade_Switch/index.aspx#.UZ_Bbpx8qCg

- HP 6125G/XG Blade Switch specifications

  http://h17007.www1.hp.com/us/en/networking/products/switches/HP_6125GXG_Blade_Switch/index.aspx#.UZ_CCJx8qCg

3. Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from the *Protection Profile for Network Devices, Version 1.1, 8 June 2012* (NDPP). The NDPP offers additional information about the identified threats, but that has not been reproduced here and the NDPP should be consulted if there is interest in that material.

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.

3.1 Organizational Policies

P.ACCESS_BANNER

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

3.2 Threats

T.ADMIN_ERROR

An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

T.TSF_FAILURE

Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

T.UNAUTHORIZED_ACCESS

A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

T.UNAUTHORIZED_UPDATE

A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

T.UNDETECTED_ACTIONS

Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

T.USER_DATA_REUSE

User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Assumptions

A.NO_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4. Security Objectives

As with the Security Problem Definition, the Security Objectives have been drawn verbatim from the NDPP. The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP should be consulted if there is interest in that material.

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

4.1 Security Objectives for the TOE

O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

O.PROTECTED_COMMUNICATIONS

The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

O.RESIDUAL_INFORMATION_CLEARING

The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

O.SESSION_LOCK

The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

O.SYSTEM_MONITORING

The TOE will provide the capability to generate audit data and send those data to an external IT entity.

O.TOE_ADMINISTRATION

The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

O.TSF_SELF_TEST

The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

O.VERIFIABLE_UPDATES

The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

4.2 Security Objectives for the 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 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 TOE.

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 2 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 3**.

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 3**.

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. Establishment/Termination of an IPsec SA.	Reason for failure. 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. Establishment/Termination of an SSH session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	
FIA_PMG_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 identification 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. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and 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 3 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’.[2]

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.'

[2] The TOE’s implementation of RSA has been validated against FIPS PUB 186-4, the testing requirements of which are identical to FIPS PUB 186-3.

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***], key size [**160 bits**], and message digest sizes [***160***] 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 [*no other RFCs 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*]; *length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]]**.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and **[*5 (1536-bit MODP)), [2 (1024-bit MODP)]*]**.

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 [***FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using 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 [***no other RFCs***].

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 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;

5.2.4.2 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 8 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*]**.

5.2.4.3 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 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 reproduced verbatim 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 4 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.

AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

5.3.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d The developer shall provide the TOE for testing.

ATE_IND.1.1c The TOE shall be suitable for testing

ATE_IND.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d The developer shall provide the TOE for testing..

AVA_VAN.1.1c The TOE shall be suitable for testing.

AVA_VAN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

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 able to generate audit records of security relevant 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, as well as all of the events identified in **Table 3**. Note that the only protocol (i.e., IPsec, SSH) failures auditable by the TOE are authentication failures for user-level connections.

Generated audit records include the date and time of the event, 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 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 3**.

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 storage is full, the TOE will overwrite the oldest records between 1 and 10MB. Access to the local audit trail requires ‘manage’ level access privileges. Alternately, the TOE can be configured to send generated audit records to an external syslog server using IPsec.

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

- FAU_GEN.1: The TOE can generate audit records for events including starting and stopping the audit function, administrator commands, and all other events identified in **Table 3**. Furthermore, each audit record includes the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 3**.

- 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	RSA #1495
Encryption/Decryption		
• AES CBC and CTR modes (128, 256 bits)	FIPS PUB 197 NIST SP 800-38A	AES #2854
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-4	RSA #1495

Functions	Standards	Certificates
Cryptographic hashing		
- SHA-1, SHA-256, SHA-512 (digest sizes 160, 256, and 512 bits)	FIPS Pub 180-3	SHS #2397
Keyed-hash message authentication		
- HMAC-SHA-1 (key size 160 bits and digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	HMAC #1794
Random bit generation		
- DRBG with software -based noise source of 256 bits of non-determinism	FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES	RNG #1280

Table 5 Cryptographic Functions

While the TOE generally fulfills all of the NIST SP 800-56B requirements without extensions, the following table specifically identifies 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.

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	
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

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
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 6 NIST SP800-56B Conformance

The TOE uses a software-based random bit generator that complies with ANSI x9.31 Random Number Generation (RNG) when operating in the CC/FIPS mode. The entropy source is a 128-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.

Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. The following table identifies the applicable secret and private keys and summarizes how and when they are deleted. 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. When a CLI command is used to zeroize a key, the key is zeroized immediately on execution of the command. Keys that are resident in RAM when the device is rebooted are zeroized during the course of the reboot.

Identifier	Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
CSP1	RSA public/private keys	ANSI X9.31/RSA	Identity certificates for the security appliance itself and also used in IPsec and SSH negotiations. The security appliance supports 2048 bit key sizes. Note that in order to be in the evaluated configuration, RSA keys smaller than 2048 bits must NOT be used, since they correspond to strengths less than 112 bits (112 bit strength, which is required by FCS_CKM.1.1 above, is associated with 2048 bit RSA keys by SP 800-56B).	Private Key - FLASH (cipher text/AES-CTR 256 bits) and RAM (plain text) Public Key – FLASH (cipher text/AES-CTR 256 bits) and RAM (plain text)	Private Key – The 'public-key local destroy' CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM. Public Key – The 'undo public-key peer' CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM.

Identifier	Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
CSP2	DSA public/private keys *(note that DSA is not included in the evaluated configuration)*	ANSI X9.31/DSA	Identity certificates for the security appliance itself and also used in SSH negotiations.	Private Key - FLASH (cipher text/AES-CTR 256 bits) and RAM (plain text) Public Key – FLASH cipher text/AES-CTR 256 bits) and RAM (plain text)	Private Key – The 'public-key local destroy' CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM. Public Key – The 'undo public-key peer' CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM.
CSP3	Diffie-Hellman Key Pairs	ANSI X9.31 / DH	Key agreement for IKE and SSH sessions.	RAM (plain text)	Keys in RAM will be zeroized upon resetting (i.e., terminating all sessions) or rebooting the security appliance.
CSP4	Public keys	DSA / RSA	Public keys of peers	FLASH(plain text)/RAM (plain text)	Peer public keys exist in a FLASH start-up configuration file and are added, deleted, or changed when that file is edited by an authorized administrator and the security appliance is rebooted.
CSP5	TLS Traffic Keys *(note that TLS is not included in the evaluated configuration)*	Generated using the TLS protocol (X9.31PRNG + SHA1 + either DH or RSA) Algorithm: Also AES, HMAC-SHA1	Used in HTTPS connections	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP6	SSH Session Keys	Generated using the SSH protocol(ANSI X9.31(AES) /SHA1/DH) Algorithms: AES, HMAC-SHA1 or HMAC-SHA1-96	SSH keys	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP7	IPsec authentication Keys	Generation: ANSI X9.31(AES) / SHA1/DH Algorithm: HMAC-SHA1-96	Exchanged using the IKE protocol and the public/private key pairs. Used to authenticate the IPsec traffic	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.

Identifier	Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
CSP8	IPsec traffic Keys	Generation: ANSI X9.31(AES) / SHA1/DH Algorithm: AES	Exchanged using the IKE protocol and the public/private key pairs. Used to encrypt the IPsec traffic.	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP9	IPsec authentication Keys	HMAC-SHA1-96	HMAC-SHA1-96 Key is manually configured for IPsec security associations.	FLASH (cipher text) and RAM (plain text)	IPsec keys exist in a FLASH start-up configuration file and are added, deleted, or changed when that file is edited by an authorized administrator. Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP10	IPsec traffic Keys	AES	AES Key is manually configured for IPsec security associations.	FLASH (cipher text) and RAM (plain text)	IPsec keys exist in a FLASH start-up configuration file and are added, deleted, or changed when that file is edited by an authorized administrator. Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP11	IKE pre-shared Keys	Shared Secret	Entered by the Crypto-Officer in plain text form and used for authentication during IKE	FLASH (cipher text) and RAM (plain text)	IKE keys exist in a FLASH start-up configuration file and are added, deleted, or changed when that file is edited by an authorized administrator. Alternately, the keys will be overwritten once with zeroes when a ‘format’ CLI command is issued against the FLASH. Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP12	IKE Authentication Key	Generated using IKE (X9.31+SHA1+DH). Algorithms: HMAC-SHA-1-96	Used to authenticate IKE negotiations	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.

Identifier	Name	Generation/ Algorithm	Purpose	Storage Location	Zeroization Summary
CSP13	IKE Encryption Key	Generated using IKE (X9.31+SHA1+ DH). Algorithms: AES	Used to encrypt IKE negotiations	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP14	RADIUS /TACACS+ shared secret Keys	Shared Secret	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) and RAM (plain text)	Keys exist in a FLASH start-up configuration file and are replaced when that file is edited by an authorized administrator. Alternately, the keys will be overwritten once with zeroes when a 'format' CLI command is issued against the FLASH. Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP15	Usernames/ Passwords/ super password	Secret	Critical security parameters used to authenticate the administrator login or privilege promoting.	FLASH (cipher text) and RAM (plain text)	Passwords exist in a FLASH start-up configuration file and are replaced when that file is edited by an authorized administrator. Passwords in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP16	Certificates of Certificate Authorities (CAs)	ANSI X9.31	Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates.	FLASH (plain text) and RAM (plain text)	CA certificates are removed when FLASH is cleared, the PKI domain is removed from the FLASH configuration file, if the 'pki delete certificate' CLI command is used. CA certificates in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP17	PRNG Seed Key	Entropy	Seed key for X9.31 PRNG	RAM (plain text)	Seed keys are zeroized and overwritten with the generation of new seed

Table 7 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 authentication timeout period is 90 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 supports connections using both transport mode and tunnel mode. The TOE implements the Encapsulating Security Payload (ESP) as specified in RFC 4303 and supports AES-CBC-128 and AES-CBC-256 (as specified by RFC 3602) for data confidentiality, along with HMAC-SHA-1 for data integrity. The TOE implements IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109, supporting AES-CBC-128 and AES-CBC-256 for data confidentiality. 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.

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.

IKEv1 SA lifetime and volume limits can be configured by an authorized administrator and can be limited to 24 hours (actually any value between 60 and 604,800 seconds) for phase 1 and 8 hours (actually any value from 180 to 604,800 seconds) for phase 2 and also 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 include DH Groups 2 (1024-bit MODP), 5 (1536-bit MODP), and 14 (2048-bit MODP) and utilize RSA (aka rDSA) peer authentication. 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 8 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 the use of pre-shared keys for IPsec.

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 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 an identity and also authentication data (e.g., password or RSA public key used in conjunction with an SSH session) that matches the provided identity. Users can be defined locally within the TOE with a user identity, password, and privilege level. Alternately, users can be defined within an external RADIUS or TACACS server configured to be used by the TOE, each of which also define the user’s privilege level 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 privilege level (see Section 6.5) assigned to the user.

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 gain access to a new session.

When changing passwords, they 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 (15 characters) minimum password length.

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

- FIA_PMG_EXT.1: The TOE implements 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 utilize 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 supports four privilege levels (i.e., roles): Visit; Monitor; System; and Manage. Manage is the highest privilege level, followed closely by the System privilege level. While there are some differences between the System and Manage roles, as seen below, for the purpose of this Security Target both are considered instances of the ‘Security Administrator’ as defined in the NDPP, since they allow for security relevant configuration management capabilities. The other two privilege levels represent logical subsets of those security management roles, but do not offer any security relevant configuration management capabilities.

Visit: Involves commands for network diagnosis and accessing an external device. Configuration of commands at this level cannot survive a device restart. Upon device restart, the commands at this level will be restored to the default settings. Commands at this level include ping, tracert, telnet and ssh2.

Monitor: Involves commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the switch is restarted, the commands at this level will be restored to the default settings. Commands at this level include debugging, terminal, refresh, reset, and send.

System: Involves service configuration commands, such as routing configuration commands and commands for configuring services at different network levels. By default, commands at this level include all configuration commands except for those at the manage level.

Manage: Involves commands that influence the basic operation of the system and commands for configuring system support modules. By default, commands at this level involve the configuration commands of file system, SFTP, STELNET, user management, level setting, and parameter settings within a system (which are not defined by any protocols or RFCs).

The System and Manage roles, and hence the Security Administrator, are the only roles capable of managing the security functions of the TOE. The other roles are limited to non-security relevant functions and review of information.

The TOE offers a command line interface providing 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 (i.e., System and Manage roles).
- 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 four defined roles, two of which correspond to the require 'Authorized Administrator'.

6.6 Protection of the TSF

The TOE is a c-Class blade-system blade switch, designed to work within the HP c3000 and c7000 enclosures which can consolidate storage, networking and power management into a single solution. Secure communication with third-party peers is addressed in Section 6.8. Secure communication among multiple instances of the TOE is considered communication among co-located components that logically form an instance of the TOE and 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 blade 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 co-located 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 forbid access to locally-stored cryptographically protected (and not plain text) 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 that existed before FIPS mode was enabled) or by encrypting the password using AES in CTR mode (for user accounts created after FIPS mode was enabled). See Table 7 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 is a hardware appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The clock is used for audit record time stamps, measuring session activity for termination, and for cryptographic operations based on time/date.

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. Furthermore, the TOE is designed to query each pluggable module which in turn includes its own diagnostics that will serve to help identify any failing modules. When operating in CC/FIPS mode, the power-on self-tests comply with 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, so as 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 includes its own hardware clock.
- 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 an administrator-configured login banner to display welcome information or a security warning in conjunction with login prompts. The banner will be displayed when accessing the TOE via the console and 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. 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) the 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. In order to protect exported audit records from disclosure or modification, the TOE can be configured to utilize IPsec connections for this purpose.

Additionally, an IPsec tunnel is used by the TOE to protect the communication with the RADIUS and TACACS servers, which are used for external authentication with the TOE. This ensures that the credentials passed through the tunnel to authenticate using the external servers are not disclosed.

Additionally, note that IRF communication is not considered communication between distributed TOE components, but rather is communication among co-located components that logically form an instance of the TOE. As such, since the IRF communication channels are not protected using mechanisms such as encryption, they need to be protected as the TOE devices themselves.

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's implementation of SSHv2 supports both public key-based and password-based administrator authentication. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (i.e., user id and password, or RSA credentials), 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 authentication information communicated with an external authentication server and audit records exported to a configured syslog server are protected from disclosure and undetected modification.
- FTP_TRP.1: The TOE implements SSHv2 to support secure remote administration. Administrators can initiate a remote session that is secured (disclosure and modification) using NIST-validated cryptographic operations and all remote security management functions require the use of a secure channel.

7. Protection Profile Claims

This ST is conformant to the *Protection Profile for Network Devices*, *Version 1.1, 8 June 2012*, 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.

The TOE includes Ethernet switch devices. 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 copied verbatim into this ST.

As explained in Section 4, Security Objectives, the Security Objectives of the NDPP have been copied verbatim into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the NDPP. The only operations performed on the SFRs drawn from the NDPP are assignment and selection operations.

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	FTP_ITC.1: Trusted Channel	NDPP

Requirement Class	Requirement Component	Source
path/channels	FTP_TRP.1: Trusted Path	NDPP

Table 8 SFR Protection Profile Sources

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives. Note that the NDPP does not explicitly or clearly correspond or rationale correspondence between its Security Problem Definition and Security Objectives, so the mapping had to be inferred and correspondence rationale has been devised to complete this ST appropriately.

	P.ACCESS_BANNER	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN
O.DISPLAY_BANNER	X									
O.PROTECTED_COMMUNICATIONS				X						
O.RESIDUAL_INFORMATION_CLEARING							X			
O.SESSION_LOCK				X						
O.SYSTEM_MONITORING		X		X		X				
O.TOE_ADMINISTRATION				X						
O.TSF_SELF_TEST			X							
O.VERIFIABLE_UPDATES					X					
OE.NO_GENERAL_PURPOSE								X		
OE.PHYSICAL									X	

	P.ACCESS_BANNER	T.ADMIN_ERROR	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN
OE.TRUSTED_ADMIN	■	■	■	■	■	■	■			X

Table 9 Environment to Objective Correspondence

8.1.1.1 P.ACCESS_BANNER

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

This Organizational Policy is satisfied by ensuring that:

- O.DISPLAY_BANNER: To fulfill the policy to display advisory information to users prior to their use of the TOE, the TOE is expected to display a configured banner when users login to establish an interactive session.

8.1.1.2 T.ADMIN_ERROR

An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential of an administrative error that might be unnoticed or untraceable, the TOE is expected to log security relevant events and export those logs to an external log server.

8.1.1.3 T.TSF_FAILURE

Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

This Threat is satisfied by ensuring that:

- O.TSF_SELF_TEST: To reduce the potential for undetected TOE failures and to help ensure that the TOE security functions are operating properly, the TOE is expected to perform self-tests.

8.1.1.4 T.UNAUTHORIZED_ACCESS

A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

This Threat is satisfied by ensuring that:

- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its communication channels.
- O.SESSION_LOCK: To reduce the potential for unauthorized access to TOE security functions and data, the TOE is expected to lock or terminate unattended or inactive sessions.

- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events and export those logs to an external log server.
- O.TOE_ADMINISTRATION: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only presumably authorized administrators can log in and access security management functions.

8.1.1.5 T.UNAUTHORIZED_UPDATE

A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

This Threat is satisfied by ensuring that:

- O.VERIFIABLE_UPDATES: To reduce the potential that an update might contain malicious or unintended features, the TOE is expected to provide mechanisms that serve to ensure the integrity of updates prior to their use.
-

8.1.1.6 T.UNDETECTED_ACTIONS

Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential of security relevant actions occurring without notice, the TOE is expected to log security relevant events and export those logs to an external log server.

8.1.1.7 T.USER_DATA_REUSE

User data may be inadvertently sent to a destination not intended by the original sender.

This Threat is satisfied by ensuring that:

- O.RESIDUAL_INFORMATION_CLEARING: To reduce the potential of data being erroneously sent to an unintended recipient, the TOE is expected to ensure that residual data is appropriately managed.

8.1.1.8 A.NO_GENERAL_PURPOSE

It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

This Assumption is satisfied by ensuring that:

- 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.

8.1.1.9 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

8.1.1.10 A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

This Assumption is satisfied by ensuring that:

- OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 10** indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy. Note that the NDPP identifies the correspondence between Security Objectives and SFRs, but fails to provide any rationale for the correspondence. As such, correspondence rationale has been devised to complete this ST appropriately.

	O.DISPLAY_BANNER	**O.PROTECTED_COMMUNICATIONS**	**O.RESIDUAL_INFORMATION_CLEARING**	**O.SESSION_LOCK**	**O.SYSTEM_MONITORING**	**O.TOE_ADMINISTRATION**	**O.TSF_SELF_TEST**	**O.VERIFIABLE_UPDATES**
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						X
FCS_COP.1(3)		X						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_PSK_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						

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FPT_STM.1					X			
FPT_TST_EXT.1							X	
FPT_TUD_EXT.1								X
FTA_SSL.3				X		X		
FTA_SSL.4						X		
FTA_SSL_EXT.1				X		X		
FTA_TAB.1	X							
FTP_ITC.1		X						
FTP_TRP.1		X						

Table 10 Objective to Requirement Correspondence

8.2.1.1 O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FTA_TAB.1: The TOE is required to display the configured advisory banner whenever a user/administrator connects to the TOE.

8.2.1.2 O.PROTECTED_COMMUNICATIONS

The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

This TOE Security Objective is satisfied by ensuring that:

- FCS_CKM.1: The TOE is required to be able to generate encryption keys to support other cryptographic operations.
- FCS_CKM_EXT.4: The TOE is required to zeroize keys when no longer need to prevent subsequent disclosure.
- FCS_COP.1(1): The TOE is required to implement FIPS-conformant AES in support of cryptographic protocols.
- FCS_COP.1(2): The TOE is required to implement FIPS-conformant DSA, rDSA, and/or ECDSA in support of cryptographic protocols.
- FCS_COP.1(3): The TOE is required to implement FIPS-conformant SHA-1, SHA-256, SHA-384, and/or SHA-512 in support of cryptographic protocols.
- FCS_COP.1(4): The TOE is required to implement FIPS-conformant HMAC SHA-1, SHA-256, SHA-384, and/or SHA-512 in support of cryptographic protocols.
- FCS_IPSEC_EXT.1: The TOE is required to implement IPSEC properly to protect applicable communications channels with supporting products accessible via network connections.

- FCS_RBG_EXT.1: The TOE is required to implement NIST- or FIPS-conformant Random Bit Generation in support of cryptographic protocols.
- FCS_SSH_EXT.1: The TOE is required to implement SSH properly to protect applicable network communication channels.
- FIA_PSK_EXT.1: The TOE is required to support the use of pre-shared keys for authentication of IPsec connections.
- FPT_SKP_EXT.1: The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as cryptographic keys.
- FTP_ITC.1: The TOE is required to protect communication between itself and its external peers from disclosure and modification.
- FTP_TRP.1: The TOE is required to protect communication between itself and its administrators from disclosure and modification.

8.2.1.3 O.RESIDUAL_INFORMATION_CLEARING

The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

This TOE Security Objective is satisfied by ensuring that:

- FDP_RIP.2: The TOE is required to clear all information when allocating storage resources for subsequent activities.

8.2.1.4 O.SESSION_LOCK

The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

This TOE Security Objective is satisfied by ensuring that:

- FTA_SSL.3: The TOE is required to terminate remote sessions after an administrator defined period of inactivity indicating the user may not be in attendance.
- FTA_SSL_EXT.1: The TOE is required to lock or terminate local sessions after an administrator defined period of inactivity indicating the user may not be in attendance.

8.2.1.5 O.SYSTEM_MONITORING

The TOE will provide the capability to generate audit data and send those data to an external IT entity.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to be able to generate audit events for security relevant activities on the TOE.
- FAU_GEN.2: The TOE is required to associate audit events to users to ensure proper accountability.
- FAU_STG_EXT.1: The TOE is required to be able to export audit records to an external audit server via a secure channel to protect the integrity and security of those records.
- FPT_STM.1: The TOE is required to generate reliable time stamps to be used in its audit records for proper accounting.

8.2.1.6 O.TOE_ADMINISTRATION

The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

This TOE Security Objective is satisfied by ensuring that:

- FIA_PMG_EXT.1: The TOE is required to implement mechanisms allowing an administrator to constrain the construction of passwords to encourage more secure (or harder to guess) passwords.
- FIA_UAU.7: The TOE is required to not echo passwords when being entered to mitigate the chance of an accidental password disclosure.
- FIA_UAU_EXT.2: The TOE is required to implement a local authentication mechanism and can support additional authentication mechanisms.

- FIA_UIA_EXT.1: The TOE is required to ensure that users must be identified and authenticated in order to access functions, other than those specifically intended to be accessed without identification and authentication.
- FMT_MTD.1: The TOE is required to restrict access to security relevant data to administrators.
- FMT_SMF.1: The TOE is required to provide a minimum set of security functions to ensure the TOE security features can be properly managed.
- FMT_SMR.2: The TOE is required to implement a minimum of an Authorized Administrator role and can implement additional roles where necessary.
- FPT_APW_EXT.1: The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as passwords.
- FTA_SSL.3: The TOE is required to terminate remote sessions after an administrator defined period of inactivity indicating the administrator may not be in attendance.
- FTA_SSL.4: The TOE allows users to terminate their sessions at any time to help them ensure their credentials are not inappropriately used.
- FTA_SSL_EXT.1: The TOE is required to lock or terminate local sessions after an administrator defined period of inactivity indicating the administrator may not be in attendance.

8.2.1.7 O.TSF_SELF_TEST

The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

This TOE Security Objective is satisfied by ensuring that:

- FPT_TST_EXT.1: The TOE is required to exercise self-tests during start-up to periodically ensure that the TOE security functions appear to be operating correctly.

8.2.1.8 O.VERIFIABLE_UPDATES

The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1(2): The TOE is required to either use digital signatures or cryptographic hashes to ensure the integrity of updates.
- FCS_COP.1(3): The TOE is required to either use digital signatures or cryptographic hashes to ensure the integrity of updates.
- FPT_TUD_EXT.1: The TOE is required to provide update functions and also the means for an administrator to initiate and verify updates before they are applied.

8.3 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this ST are precisely the SARs identified in the NDPP.

8.4 Requirement Dependency Rationale

As can be seen in the following table all of the SFR and SAR dependencies are satisfied in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(*) and FCS_CKM_EXT.4
FCS_CKM_EXT.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1

ST Requirement	CC Dependencies	ST Dependencies
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_IPSEC_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_RBG_EXT.1	none	none
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FDP_RIP.2	none	none
FIA_PMG_EXT.1	none	none
FIA_PSK_EXT.1	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	none	none
FIA_UIA_EXT.1	none	none
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.2 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_APW_EXT.1	none	none
FPT_SKP_EXT.1	none	none
FPT_STM.1	none	none
FPT_TST_EXT.1	none	none
FPT_TUD_EXT.1	none	none
FTA_SSL.3	none	none
FTA_SSL.4	none	none
FTA_SSL_EXT.1	none	none
FTA_TAB.1	none	none
FTP_ITC.1	none	none
FTP_TRP.1	none	none
ADV_FSP.1	none	none
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	none	none
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1
ALC_CMS.1	none	none
ATE_IND.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1
AVA_VAN.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.1 and AGD_PRE.1

Table 11 Requirement Dependencies

8.5 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 12 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_PSK_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 12 Security Functions vs. Requirements Mapping

Appendix A: Documentation for HP 6125 Ethernet Blade Switch Series

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

The following documents for the HP 6125 Ethernet Blade Switch Series can be found under the *General Reference* section of both the 6125G Ethernet Blade Switch and the 6125G/XG Ethernet Blade Switch documentation pages on the HP Web site. The links are provided below.

- *HP Networking guide to hardening Comware-based devices*, Oct 23, 2012
- *HP 6125G & 6125G/XG Blade Switches Layer 3 - IP Services Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches Layer 3 - IP Routing Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches IP Multicast Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches Layer 2 - LAN Switching Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches IRF Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches High Availability Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches Fundamentals Command Reference*, R2103, Sep 19, 2012
- *About the HP 6125G & 6125G/XG Blade Switches Configuration Guides*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches Security Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches Network Management and Monitoring Command Reference*, R2103, Sep 19, 2012
- *HP 6125G & 6125G/XG Blade Switches ACL and QoS Command Reference*, R2103, Sep 19, 2012
- *About the HP 6125G & 6125G/XG Blade Switches Command References*, R2103, Sep 17, 2012

http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/psi/manualsResults/?sp4ts.oid=5295188&spf_p.tpst=psiContentResults&spf_p.prp_psiContentResults=wsrp-navigationalState%3Daction%253Dmanualslist%257Ccontentid%253DGeneral-Reference%257Clang%253Den&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken

http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/psi/manualsResults/?sp4ts.oid=5295192&spf_p.tpst=psiContentResults&spf_p.prp_psiContentResults=wsrp-navigationalState%3Daction%253Dmanualslist%257Ccontentid%253DGeneral-Reference%257Clang%253Den&javax.portlet.begCacheTok=com.vignette.cachetoken&javax.portlet.endCacheTok=com.vignette.cachetoken