Hewlett-Packard Company Network Switches Security Target

Version 1.02
08/16/2013

Prepared for:

Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

SAIC
From Science to Solutions

Science Applications International Corporation

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 Network Switches provided by Hewlett-Packard Development Company. Each of the Network Switch products is a stand-alone Gigabit Ethernet switch appliance designed to implement a wide range of network layers 2 and 3 switching, service and routing operations.

The Security Target contains the following additional sections:

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

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett-Packard Company Network Switches Security Target

ST Version – Version 1.02

ST Date – 08/16/2013

TOE Identification – Hewlett-Packard Company Network Family with Comware version 5.2

Product Series	Specific Devices
HP 5120 Series Gigabit Ethernet Switches	HP 5120-24G EI 2-slot Switch
	HP 5120-48G EI 2-slot Switch
	HP 5120-24G-PoE EI 2-slot Switch
	HP 5120-48G-PoE EI 2-slot Switch
HP 5500 Series Gigabit Ethernet Switches	HP 5500-24G EI Switch
	HP 5500-24G-PoE EI Switch
	HP 5500-24G-SFP EI Switch
	HP 5500-48G EI Switch
	HP 5500-48G-PoE EI Switch
The HP 5500 HI Series Gigabit Ethernet switches	HP 5500-24G-4SFP HI Switch with 2 Interface Slots
	HP 5500-48G-4SFP HI Switch with 2 Interface Slots
	HP 5500-24G-PoE+-4SFP HI Switch with 2 Interface Slots
	HP 5500-48G-PoE+-4SFP HI Switch with 2 Interface Slots
	HP 5500-24G-SFP HI Switch with 2 Interface Slots
HP 5800 Series Flex Chassis Switches	HP 5800-24G-PoE Switch
	HP 5800-24G Switch
	HP 5800-48G Switch with 2 Slots

Product Series	Specific Devices
	HP 5800-24G-SFP Switch
	HP 5800-48G-PoE Switch
	HP 5800-48G Switch
	HP 5800AF-48G Switch
HP 5820 Series 10-Gigabit Switches	HP 5820-24XG-SFP+ Switch
	HP 5820AF-24G Switch
	HP 5820-14XG-SFP+ 2-slot Switch
HP 7500 Series Modular Core Switches	HP 7510 Switch Chassis
	HP 7506 Switch Chassis
	HP 7506-V Switch Chassis
	HP 7503 Switch Chassis
	HP 7502 Switch Chassis
	HP 7503 1 Fabric Slot Switch Chassis
HP 9500 Series Modular Core Switches	HP 9505 Switch Chassis
	HP 9508-V Switch Chassis
	HP 9512 Switch Chassis
HP 12500 Series Data Center Switches	HP 12518 Switch Chassis
	HP 12508 Switch Chassis
	HP 12518 Switch Chassis with memory upgrade
	HP 12508 Switch Chassis with memory upgrade
	HP 12504 Switch Chassis with memory upgrade

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 3, July 2009*

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- This ST is conformant to the *Security Requirements for Network Devices, Version 1.1, 8 June 2012* (including the optional IPSEC and SSH requirements).
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.
  - Part 3 Conformant
  - Assurance Level: EAL 1

  The effective assurance level is beyond the base CC-defined EAL 1 level since the NDPP defines a number of assurance activities that are out of scope for EAL 1. These assurance activities have been *reproduced in this Security Target to ensure they are within scope of the corresponding evaluation. However, at the present time international recognition of the evaluation results is limited to defined assurance packages, such as EAL1, and does not extend to Scheme-defined assurance extensions or refinements.*

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 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**]). 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 …"). '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.

2. TOE Description

The Target of Evaluation (TOE) is the Hewlett-Packard Network family of switches. The Network switches in the evaluated configuration include the 5120, 5500, 5800, 5820, 7500, 9500 and 12500 series. Each series of this family consists of a set of distinct devices (as identified in section 1.1) which vary primarily according to power delivery, performance, and port density.

While most of the Network switches have fixed ports, they all support plug-in modules (or blades) that provide additional functionality (e.g., various numbers and types of network connection ports). With the exception of pluggable security blades, all of the available plug-in modules are included in the evaluated configuration (see below). The security blades offer additional advanced (e.g., firewall) security functions and are intended to be addressed in an alternate evaluation.

The TOE can be deployed as a single Network device or alternately as a group of Network devices connected using the HP Intelligent Resilient Framework (IRF) technology to effectively form a logical switch device. The IRF technology requires Network device be directly connected to one another using an IRF stack utilizing one or more dedicated Ethernet connections that are used to coordinate the overall logical switch configuration and also to forward applicable network traffic as necessary between attached devices.

2.1 TOE Overview

The HP Network switches are Gigabit Ethernet switch appliances which consist of hardware and software components. While the physical form factor of each distinct series in the Network family is substantially different, the underlying hardware share a similar architecture. The software utilized is a common code base of a modular nature with only the modules applicable for the specific hardware installed.

5120 Series Switches

The HP 5120 series switches are Gigabit Ethernet switches that support static Layer 3 routing, diversified services, and IPv6 forwarding and provide up to four 10-Gigabit Ethernet (10 GbE) extended interfaces. An Intelligent Resilient Framework (IRF) technology creates virtual fabric by virtualizing several switches into one logical device, which increases network resilience, performance, and availability while reducing operational complexity. These switches provide Gigabit Ethernet access and can be used at the edge of a network or to connect server clusters in data centers. High scalability provides investment protection with two expansion slots, each of which can support two-port 10 GbE expansion modules. High availability, simplified management, and comprehensive security control policies are among the key features that distinguish this series. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 5500/5120-EI 2-port 10-GbE XFP Module
- HP 5500/5120-EI 2-port 10-GbE CX4 Module
- HP 5500/5120-EI 1-port 10-GbE XFP Module
- HP 5500/5120-EI 2-port 10-GbE SFP+ Module
- HP 5500/5120-EI 2-Port GbE SFP Module

5500 Series Switches

The HP 5500 series switches deliver security, reliability, and multiservice support capabilities for switching at the edge or aggregation layer of large enterprise and campus networks or in the core layer of SMB networks. The HP 5500 series switches are comprised of Layer 2/3 Gigabit Ethernet switches that can accommodate the most demanding applications and provide resilient and secure connectivity as well as the traffic prioritization technologies to enhance applications on convergent networks. With IPv4/IPv6 dual stack support, the series supports transitions from IPv4 to IPv6 networks. Designed for flexibility, these switches are available with 24 or 48 Gigabit Ethernet ports. Power over Ethernet (PoE) and non-PoE models are available with optional GbE and 10 GbE expansion capabilities. The all-fiber model with dual power supplies is ideal for applications that require the highest availability. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 5500/5120-EI 2-port 10-GbE XFP Module
- HP 5500/5120-EI 2-port 10-GbE CX4 Module
- HP 5500/5120-EI 1-port 10-GbE XFP Module
- HP 5500/5120-EI 2-port 10-GbE SFP+ Module
- HP 5500/5120-EI 2-Port GbE SFP Module

5500HI Series Switches

The HP 5500 HI Series of Gigabit Ethernet switches delivers outstanding resiliency, security, and multiservice support capabilities at the edge layer of data center, large campus, and metro Ethernet networks. The switches can also be used in the core layer of SMB networks. The HP 5500 HI Switch Series supports a dual power supply and an IRF virtual fabric to provide the highest levels of resiliency and manageability. With complete IPv4/IPv6 and MPLS/VPLS features, the series provides investment protection with an easy transition from IPv4 to IPv6 networks. Designed with two fixed 10G ports and extension flexibility, these switches can provide up to six 10-GbE uplink or 70 GbE ports. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 5500 HI 8-port SFP Module
- HP 5500 HI 8-port Gig-T Module
- HP 5500/5120 2-port 10GbE SFP+ Module
- HP 5500/4800 2-port GbE SFP Module
- HP 5500 1-port 10GbE XFP Module
- HP 5500 2-port 10GbE Local Connect Module
- HP 5500 2-port 10GbE XFP Module

5800 Series Switches

HP 5800 series switches offer an unmatched combination of Gigabit and 10-Gigabit Ethernet port density, high-availability architecture, and full Layer 2 and Layer 3 dual-stack IPv4 and IPv6 capabilities. In addition to wire-speed line-rate performance on all ports, the switches include patented Intelligent Resilient Framework (IRF) technology and Rapid Ring Protection Protocol (RRPP), which allow local or geographically distributed HP 5800 switches to be interconnected for higher resiliency and performance. Available in PoE and non-PoE models, as well as 1 RU and 2 RU flex chassis configurations, HP 5800 switches are built on open standards and include an open application architecture (OAA) module slot that enables flexible deployment options for new services. These versatile switches are ideal for use in the network core of buildings or departments, or as high-performance switches in the convergence layer or network edge of enterprise campus networks.. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 5820X/5800 4-port 10-GbE SFP+ Module
- HP 5820X/5800 2-port 10-GbE SFP+ Module
- HP 5800 16-port Gig-T Module
- HP 5800 16-port GbE SFP Module

5820 Series Switches

The HP 5820 series switches feature flex-chassis devices that deliver a unique combination of unmatched 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) connectivity, high-availability architecture, full Layer 2/3 dual-stack IPv4/v6, and line-rate, low-latency performance on all ports. The switches can be used in high-performance, high-density building or department cores as part of a consolidated network; for data center top-of-rack server access; or as high-performance Layer 3, 10-GbE aggregation switches in campus and data center networks. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 5820X/5800 4-port 10-GbE SFP+ Module
- HP 5820X/5800 2-port 10-GbE SFP+ Module

7500 Series Switches

The HP 7500 series switches comprise 10 Gigabit modular core devices designed for the requirements of enterprise data center applications. These multilayer switches are designed to meet the evolving needs of integrated services networks, and can be deployed in multiple network environments, including the enterprise LAN core, aggregation layer, and wiring closet edge, as well as in metropolitan area networks (MANs) and data centers. They feature cost-effective wire-speed 10 Gigabit Ethernet ports to provide the throughput and bandwidth necessary for mission-critical data and high-speed communications. A passive backplane, support for load sharing, and redundant management and fabrics help HP 7500 series switches offer high availability. Moreover, these switches deliver wire-speed Layer 2 and Layer 3 routing services for the most demanding applications. The following modules are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 7510 768Gbps Fabric/Main Processing Unit
- HP 7500 384Gbps Fabric/Main Processing Unit
- HP 7500 384Gbps Fabric/Main Processing Unit with 12 GbE SFP Ports
- HP 7500 384Gbps Fabric/Main Processing Unit with 2 10-GbE XFP Ports
- HP 7500 384Gbps Fabric/Advanced Main Processing Unit
- HP 7500 384Gbps Fabric/Lite Main Processing Unit
- HP 7500 48-port 100Base-FX SA Module
- HP 7500 48-port 10/100Base-TX PoE-upgradable SA Module
- HP 7500 48-port Gig-T PoE-upgradable SA Module
- HP 7500 48-port GbE SFP SC Module
- HP 7500 48-port Gig-T PoE-upgradable SC Module
- HP 7500 40-port Gig-T/8-port GbE SFP PoE-upgradable SC Module
- HP 7500 24-port GbE SFP/2-port 10-GbE XFP SC Module
- HP 7500 24-port Gig-T/2-port 10-GbE XFP SC Module
- HP 7500 24-port GbE SFP SC Module
- HP 7500 24-port Gig-T SC Module
- HP 7500 16-port GbE SFP/8-port GbE Combo SC Module
- HP 7500 12-port GbE SFP SC Module
- HP 7500 8-port 10-GbE SFP+ SC Module
- HP 7500 2-port 10-GbE XFP SC Module
- HP 7500 12-port GbE SFP EA Module
- HP 7500 1-port 10-GbE XFP EA Module
- HP 7500 48-port GbE SFP SD Module
- HP 7500 48-port Gig-T PoE+ SD Module
- HP 7500 24-port GbE SFP/2-port 10-GbE XFP SD Module
- HP 7500 16-port GbE SFP/8-port GbE Combo SD Module
- HP 7500 8-port 10-GbE XFP SD Module
- HP 7500 4-port 10-GbE XFP SD Module
- HP 7500 2-port 10-GbE XFP SD Module
- HP 7500 48-port GbE SFP EB Module
- HP 7500 16-port GbE SFP/8-port GbE Combo EB Module
- HP 7500 4-port 10-GbE XFP EB Module
- HP 7500 2-port 10-GbE XFP EB Module

Most of the available modules serve to extend the number of physical ports available and the throughput performance to the base appliance. However, the main processing units serve to add additional processing power to the base appliance. In each case, the processors of the main processing unit execute the same multiprocessor-capable operating system in conjunction with the instance operating on the processor(s) found in the base appliance. The processing units (including lite and advanced varieties) differ in processing speed and available on-unit memory and interface resources.

9500 Series Switches

The HP 9500 series switches are modular switches that can form a data center/large campus core switching platform. With high levels of networking performance, availability, and flexible and efficient deployment options, these switches enable new services while driving down the cost of network operations. The 9500 series switches can provide more than 1.4 TB of high-performance switching capacity, aggregate up to 192 10-GbE or 576 GbE ports, and offer an architecture that enables customers to support emerging enterprise core or data center requirements. The following modules, extending the physically available ports, are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 9500 48-port GbE SFP LEB Module
- HP 9500 48-port Gig-T LEB Module

- HP 9500 48-port Gig-T REB Module
- HP 9500 16-port GbE SFP/8-port GbE Combo LEB Module
- HP 9500 16-port Gig-T/8-port GbE Combo LEB Module
- HP 9500 16-port 10-GbE SFP+ REB Module
- HP 9500 4-port 10-GbE XFP LEB Module
- HP 9500 2-port 10-GbE XFP LEB Module
- HP 9500 48-port GbE SFP LEC Module
- HP 9500 48-port Gig-T LEC Module
- HP 9500 16-port GbE SFP/8-port GbE Combo LEC Module
- HP 9500 16-port Gig-T/8-port GbE Combo LEC Module
- HP 9500 4-port 10-GbE XFP LEC Module
- HP 9500 2-port 10-GbE XFP LEC Module

12500 Series Switches

The HP 12500 series switches comprise a pair of powerful routing switches with capacity for the network core or the data center and include Intelligent Resilient Framework (IRF) technology that provides high levels of performance and high availability. These switches also have energy-efficiency features that can drive down operational expenses. The 12500 series is ideal for organizations contemplating large-scale data center or campus consolidations, business continuity and disaster recovery sites, metropolitan area network deployments, and other applications requiring a robust, high-performance switching platform. The following modules are supported by this series and can optionally be used since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HP 12500 Main Processing Unit
- HP 12508 Fabric Module
- HP 12518 Fabric Module
- HP 12500 48-port Gig-T LEB Module
- HP 12500 48-port Gig-T LEC Module
- HP 12500 48-port GbE SFP LEB Module
- HP 12500 48-port GbE SFP LEC Module
- HP 12500 4-port 10-GbE XFP LEB Module
- HP 12500 4-port 10-GbE XFP LEC Module
- HP 12500 8-port 10-GbE XFP LEB Module
- HP 12500 8-port 10-GbE XFP LEC Module
- HP 12500 32-port 10-GbE SFP+ REB Module
- HP 12500 32-port 10-GbE SFP+ REC Module
- HP 12500 8-port 10GbE SFP+ LEF Module
- HP 12500 48-port GbE SFP LEF Module
- HP 12500 8-port 10GbE SFP+ LEB Module
- HP 12500 8-port 10GbE SFP+ LEC Module
- HP 12500 16-port 10GbE SFP+ LEB Module
- HP 12500 16-port 10GbE SFP+ LEC Module
- HP 12500 Spare Power Monitor Module

Most of the available modules, including the fabric modules, serve to extend the number of physical ports available and the throughput performance to the base appliance. However, the main processing unit serves to add additional processing power to the base appliance by executing the same multiprocessor-capable operating system in conjunction with the instance operating on the processor(s) found in the base appliance.

2.2 TOE Architecture

The HP Network switches share a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4/IPv6 dual-stacks, a data link layer, layer 2 and 3 routing, Ethernet switching, VLANs, Intelligent Resilient Framework (IRF), routing, Quality of Service (QoS), etc. The evaluated version of Comware is 5.2. Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux.

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

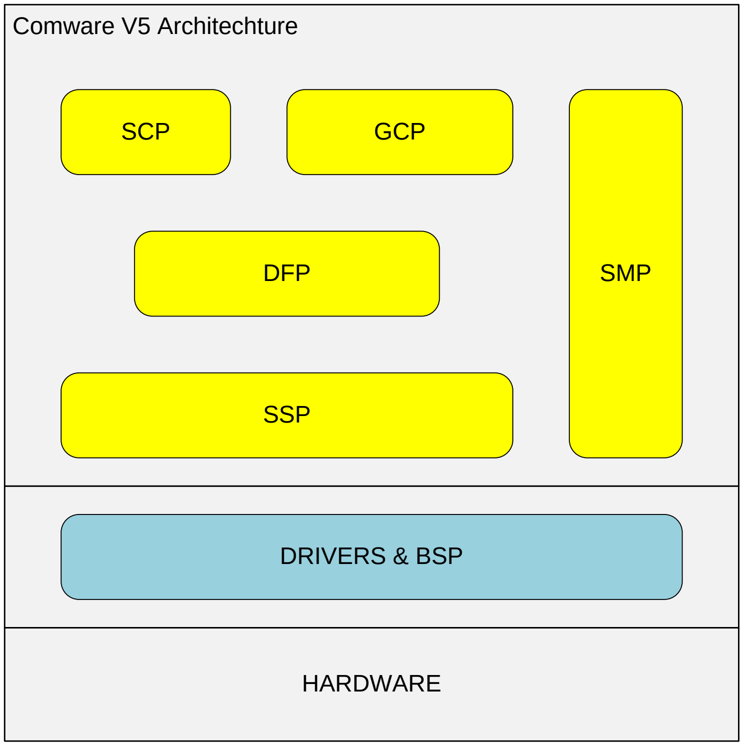

Figure 1 Comware v5.2 Architecture

- ***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 implementations for Command line - CLI (SSHv2) and Management Information Base - management options. The Management Information Base management option is excluded from the TOE.

- ***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 stacks as well as the applicable network protocols and forwarding, routing, etc.

From a security perspective, the TOE includes FIPS certified cryptographic algorithms 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, multiple HP Network switch devices can be deployed as an IRF group. Each device in the IRF group is directly connected to the other IRF group members using an IRF stack utilizing dedicated network connections. One device in the group is designated as master and should that device fail a voting procedure ensues to elect a new master among the remaining IRF group members.

All Network 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 forwarded 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.

The IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must necessarily 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 rack-mountable appliance (or IRF connected group of appliances) that supports 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 list of applicable series and devices is provided in section 1.1 and the applicable modules for each series are identified in section 2.1.

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.
- RADIUS and TACACS servers – The TOE can be configured to utilize external authentication servers.
- SNMP server – The TOE can be configured to issue SNMP traps.
- Certificate Authority (CA) server – The TOE can be configured to utilize digital certificates, e.g., for SSH connections.
- Management Workstation – The TOE supports CLI access and as such an administrator would need a terminal emulator (supporting SSHv2) to utilize this administrative interface.

2.2.3 Logical Boundaries

This section summarizes the security functions provided by HP Network Switch:

- 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 designed to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally to be accessed by an administrator or alternately to send the logs to a designated log server.

2.2.3.2 Cryptographic support

The TOE includes FIPS-certified cryptographic algorithms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec and SSH.

2.2.3.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various physical and logical (e.g., VLAN) network connections. While implementing applicable network protocols associated with network traffic forwarding, the TOE is designed to ensure 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 as well as network accessible interfaces (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 Command Line (CLI) commands to access the wide range of security management functions. Security management commands are limited to administrators 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 design to protect itself to ensure the reliability and integrity of its security features.

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

From a communication perspective, it employs both dedicated communication channels (based on physically separate networks and VLAN technology) and also cryptographic means (e.g., to prevent replays) to protect communication between distributed TOE components as well as between TOE and other components in the operation environment (e.g., administrator workstations). IRF communication is not considered communication between distributed TOE components, but rather is communication among collocated components that logically form an instance of the TOE. As such, since IRF communication channels are not protected using mechanisms such as encryption, they need to be as protected as the TOE devices themselves.

The TOE includes functions to perform self-tests so it might detect when it is failing. It also includes mechanisms so the TOE itself can be updated while ensuring 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 an informative banner when an administrator establishes an interactive session and 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 a log server, using IPsec connections and optionally using a dedicated VLAN 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 Hewlett-Packard Network Switches. In particular, there are three Common Criteria specific guides that reference the security-related guidance material for all products evaluated.

“Command Reference for CC Supplement”, Version 1.0, dated 3/18/2013
“Configuration Guide for CC Supplement”, Version 1.0, dated 3/18/2013
“Comware V5 Platform System Log Messages”, Version 1.1, dated 3/29/2013

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

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

3. Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from the *Security Requirements 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

Like 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 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 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 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 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): *Security Requirements 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 also drawn from the NDPP which includes all the SARs for EAL1 as defined in the CC. Additionally, the SARs are effectively refined since the 'Assurance Activities' defined in the NDPP that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL1 assurance requirements alone. As such, those assurance activities have been reproduced in section 5.4 to ensure they are included in the scope of the evaluation effort.

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_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 describes the SFRs that are satisfied by HP Network Switches.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1: Explicit: IPSEC
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1: Explicit: SSH
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_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 authentication and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.1	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.	Identification of the claimed user

Requirement	Auditable Events	Additional Audit Record Contents
	Termination of the trusted channel. Failures of the trusted path functions.	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 [**ECB and CBC modes**]] and cryptographic key sizes 128-bits, 256-bits, and [***192 bits***] that meets the following:

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

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

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

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

that meets the following:

Case: RSA Digital Signature Algorithm

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

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

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

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

FCS_COP.1(4).1 Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**20 octets**], 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 IPsec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [***no other algorithms***] and using IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109; [***no other method***] to establish the security association.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [**100**] MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [***[DH Group 2 (1024-bit MODP), DH Group 5 (1536-bit MODP)]***].

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [***rDSA***] algorithm.

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”, [“'”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “[”, “\”, “]”, “_”, “`”, “{”, “}”, and “~”]];
2. Pre-shared keys of 22 characters and [***[1-128 characters]***].

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* and *a TSF-hardware-based noise source***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [***128 bits***] of entropy at least equal to the greatest bit length of the keys and authorization factors 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, and 4254.

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 is the only allowed key exchange method 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 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.

5.2.4.3 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.

5.2.4.4 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1

The TSF shall allow responses to 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 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, [***no other capabilities***] 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**].

5.2.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 Refinement: The TSF shall use [***SSH***] to provide a 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 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 Refinement: 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 the EAL 1 components as specified in Part 3 of the Common Criteria (with the exception of some name changes in accordance with the NDPP). The SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

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 Labeling 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 categorization 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 fulfill 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 Labeling 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 labeled 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.

5.4 Explicit Assurance Activities

The following tables (Table 5 NDPP Security Functional Requirement Assurance Activities and Table 6 NDPP Assurance Family Assurance Activities) define the explicit assurance activities presented in the NDPP for applicable SFR elements and SAR families.

The table for the SFRs has divided the assurance activities based on whether they apply to TOE design, operational guidance, or testing. The NDPP doesn't include any SFR-specific life-cycle or vulnerability analysis assurance activities. All SFR elements are represented in the table. The first column identifies the applicable SFR element, but when there are no associated assurance activities the row is modified to identify only the applicable element.

The assurance activities in the following tables serve to *refine* the SARs above with specific activities to be performed by the evaluators during the course of their evaluation.

	Assurance Activity – Design	**Assurance Activity - Guidance**	**Assurance Activity - Testing**
FAU_GEN.1.1		The evaluator shall check the administrative guide and ensure it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure every audit event type mandated by the NDPP is described and the description of the fields contains the information required in FAU_GEN1.2, and the additional information specified in Table 3. The evaluator shall also make a determination of the administrative actions that are relevant in the context of the NDPP. The evaluator shall examine the administrative guide and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the NDPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to the NDPP. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in table 1 and administrative actions. This should include all instances of an event--for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. For administrative actions, the evaluator shall test that each action determined by the evaluator above to be security relevant in the context of the NDPP is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and the fields in each audit record have the proper entries. Testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.
FAU_GEN.1.2		**This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.**	

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FAU_STG_EXT.1.1	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.	The evaluator shall also examine the operational guidance to determine it describes the relationship between the local audit data and the audit data that are sent to the audit log server (for TOEs that are not acting as an audit log server). For example, when an audit event is generated, it is simultaneously sent to the external server and the local store, or the local store is used as a buffer and "cleared" periodically by sending the data to the audit server. The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.	Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following test for this requirement: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.
FCS_CKM.1.1	In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information: The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies. For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE; For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described; Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.		The evaluator shall use the key pair generation portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require the evaluator have a trusted reference implementation of the algorithms can produce test vectors that are verifiable during the test.

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FCS_CKM_EXT.4.1	The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").		
FCS_COP.1.1(1)			The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require the evaluator have a reference implementation of the algorithms known to be good can produce test vectors that are verifiable during the test.
FCS_COP.1.1(2)			The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSAVS or DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSAVS or ECDSA2VS), and "The RSA Validation System" (RSAVS) as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-2 or FIPS PUB 186-3). This will require the evaluator have a reference implementation of the algorithms known to be good can produce test vectors that are verifiable during the test.
FCS_COP.1.1(3)			The evaluator shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require the evaluator have a reference implementation of the algorithms known to be good can produce test vectors that are verifiable during the test.
FCS_COP.1.1(4)			The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require the evaluator have a reference implementation of the algorithms known to be good can produce test vectors that are verifiable during the test.
FCS_IPSEC_EXT.1.1			

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FCS_IPSEC_EXT.1.2	The evaluator shall examine the TSS to verify that it describes how "confidentiality only" ESP mode is disabled. The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used.	The evaluator shall also examine the operational guidance to determine that it describes any configuration necessary to ensure "confidentiality only" mode is disabled, and that an advisory is present indicating that tunnel mode is the preferred ESP mode since it protects the entire packet. If this requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure instructions for this configuration are contained within that guidance.	The evaluator shall also perform the following tests: Test 1: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. Test 2: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using ESP in "confidentiality only" mode. This attempt should fail. The evaluator shall then establish a connection using ESP in confidentiality and integrity mode.
FCS_IPSEC_EXT.1.3	The evaluator checks to ensure that the TSS describes how lifetimes for IKEv1 SAs (both Phase 1 and Phase 2) are established.	If they are configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance.	The evaluator also performs the following test: Test 1: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe this SA is closed or renegotiated in 24 hours or less. If such an action requires the TOE be configured in a specific way, the evaluator shall implement tests demonstrating the configuration capability of the TOE works as documented in the operational guidance. Test 2: The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.
FCS_IPSEC_EXT.1.4	The evaluator checks to ensure that the TSS describes how lifetimes for IKEv1 Phase 2 SAs--with respect to the amount of traffic that is allowed to flow using a given SA--are established.	If the value is configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance.	The evaluator also performs the following test: Test 1: The evaluator shall construct a test where a Phase 2 SA is established and attempted to be maintained while more data than is specified in the above assignment flows over the connection. The evaluator shall observe this SA is closed or renegotiated before the amount of data specified is exceeded. If such an action requires the TOE be configured in a specific way, the evaluator shall implement tests demonstrating the configuration capability of the TOE works as documented in the operational guidance.
FCS_IPSEC_EXT.1.5	The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.		The evaluator shall also perform the following test: Test 1: For each supported DH group, the evaluator shall test to ensure all IKE protocols can be successfully completed using that particular DH group.
FCS_IPSEC_EXT.1.6	The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.		The evaluator shall also perform the following test: Test 1: For each supported signature algorithm, the evaluator shall test that peer authentication using the algorithm can be successfully achieved.

	Assurance Activity – Design	**Assurance Activity - Guidance**	**Assurance Activity - Testing**
FCS_IPSEC_EXT.1.7	The evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.	The evaluator shall check that the operational guidance describes how pre-shared keys are to be generated and established for a TOE. The description in the operational guidance shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.	The evaluator shall also perform the following test: Test 1: The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection between two peers. If the TOE supports generation of the pre-shared key, the evaluator shall ensure establishment of the key is carried out for an instance of the TOE generating the key as well as an instance of the TOE merely taking in and using the key.
FCS_IPSEC_EXT.1.8		The evaluator shall check the operational guidance to ensure it describes the generation of pre-shared keys, including guidance on generating strong keys and the allowed character set. The evaluator shall check that this guidance does not limit the pre-shared key in a way that would not satisfy the requirement. While the administrator (in contravention to the operational guidance) can choose a key that does not conform to the requirement, there is no requirement that the TOE check the key to ensure it meets the rules specified in this component. However, should the administrator choose to create a password that conforms to the rules above (and the operational guidance); the TOE should not prohibit such a choice.	The evaluator shall also perform the following test; this may be combined with Test 1 for FCS_IPSEC_EXT.1.7: Test 1: The evaluator shall generate a pre-shared 22 characters long key that meets the composition requirements above. The evaluator shall then use this key to successfully establish an IPsec connection. While the evaluator is not required to test that all of the special characters or lengths listed in the requirement are supported, it is required they justify the subset of those characters chosen for testing, if a subset is indeed used.
FCS_RBG_(EXT).1.1			
FCS_RBG_(EXT).1.2	Documentation shall be produced—and the evaluator shall perform the activities—in accordance with Annex D [see NDPP], Entropy Documentation and Assessment.		The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms. Implementations Conforming to FIPS 140-2, Annex C *…[see NDPP]…* Implementations Conforming to NIST Special Publication 800-90 *…[see NDPP]…* The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator. Entropy input: the length of the entropy input value must equal the seed length. Nonce: If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length. Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied. Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.
FCS_SSH_EXT.1.1			

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FCS_SSH_EXT.1.2	The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.5, and ensure that password-based authentication methods are also allowed.		The evaluator shall also perform the following tests: Test 1: The evaluator shall, for each public key algorithm supported, show the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance. Test 2: Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.
FCS_SSH_EXT.1.3	The evaluator shall check that the TSS describes how 'large packets' in terms of RFC 4253 are detected and handled.		The evaluator shall also perform the following test: Test 1: The evaluator shall demonstrate that if the TOE receives a packet larger than specified in this component, that packet is dropped.
FCS_SSH_EXT.1.4	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.	The evaluator shall also check the operational guidance to ensure it contains instructions on configuring the TOE so SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).	The evaluator shall also perform the following test: Test 1: The evaluator shall establish a SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of a protocol to satisfy the intent of the test.
FCS_SSH_EXT.1.5		The assurance activity associated with FCS_SSH_EXT.1.4 verifies this requirement.	
FCS_SSH_EXT.1.6	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.	The evaluator shall also check the operational guidance to ensure it contains instructions to the administrator on how to ensure only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the 'none' MAC algorithm is not allowed).	
FCS_SSH_EXT.1.7	If this capability is 'hard-coded' into the TOE, the evaluator shall check the TSS to ensure that this is stated in the discussion of the SSH protocol.	The evaluator shall ensure operational guidance contains configuration information that will allow the security administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14.	The evaluator shall also perform the following test: Test 1: The evaluator shall attempt to perform a diffie-hellman-group1-sha1 key exchange, and observe the attempt fails. The evaluator shall then attempt to perform a diffie-hellman-group14-sha1 key exchange, and observe the attempt succeeds.

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FDP_RIP.2.1	"Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.		
FIA_PMG_EXT.1.1		The evaluator shall examine the operational guidance to determine it provides guidance to security administrators on the composition of strong passwords, and it provides instructions on setting the minimum password length.	The evaluator shall also perform the following tests. One or more of these tests can be performed with a single test case. Test 1: The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.
FIA_UIA_EXT.1	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".	The evaluator shall examine the operational guidance to determine any necessary preparatory steps (e.g., establishing credential material such as pre-shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the operational guidance provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine the operational guidance provides sufficient instruction on limiting the allowed services.	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the operational guidance to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access. Test 2: The evaluator shall configure the services allowed (if any) according to the operational guidance, and then determine the services available to an external remote entity. The evaluator shall determine the list of services available is limited to those specified in the requirement. Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
FIA_UAU_EXT.2.1		Assurance activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1.	

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FIA_UAU_EXT.7.1			The evaluator shall perform the following test for each method of local login allowed: Test 1: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
FMT_MTD.1.1	The evaluator shall examine the TSS to determine that, for each administrative function identified in the operational guidance; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.	The evaluator shall review the operational guidance to determine each of the TSF-data-manipulating functions implemented in response to the requirements of the NDPP is identified, and configuration information is provided to ensure only administrators have access to the functions.	
FMT_SMF.1.1		The security management functions for FMT_SMF.1 are distributed throughout the NDPP and are included as part of the requirements in FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.	
FMT_SMR.2		The evaluator shall review the operational guidance to ensure it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, each supported method of administering the TOE that conforms to the requirements of the NDPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
FPT_STM.1.1	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time. The TSS provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.	The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.	Test 1: The evaluator uses the operational guide to set the time. The evaluator shall then use an available interface to observe the time was set correctly. Test2: [conditional] If the TOE supports the use of an NTP server; the evaluator shall use the operational guidance to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe the NTP server has set the time to what is expected. If the TOE supports multiple cryptographic protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol.
FPT_APW_EXT.1	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.		
FPT_SKP_EXT.1	The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.		

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FPT_TUD_(EXT).1.1			
FPT_TUD_(EXT).1.2			
FPT_TUD_(EXT).1.3	Updates to the TOE either have a hash associated with them, or are signed by an authorized source. If digital signatures are used, the definition of an authorized source is contained in the TSS, along with a description of how the certificates used by the update verification mechanism are contained on the device. The evaluator ensures this information is contained in the TSS. The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate updates are obtained; the processing associated with verifying the digital signature or calculating the hash of the updates; and the actions that take place for successful (hash or signature was verified) and unsuccessful (hash or signature could not be verified) cases.		The evaluator shall perform the following tests: Test 1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies it is successfully installed on the TOE. Then, the evaluator performs a subset of other assurance activity tests to demonstrate the update functions as expected. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to the update. Test 2: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces an illegitimate update, and attempts to install it on the TOE. The evaluator verifies the TOE rejects the update.
FPT_TST_EXT.1.1	The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.	The evaluator shall also ensure the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.	
FTA_SSL.3.1			The evaluator shall perform the following test: Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes the session is terminated after the configured time period.
FTA_SSL.4.1			The evaluator shall perform the following test: Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes the session has been terminated. Test 2: The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes the session has been terminated.
FTA_SSL_EXT.1.1			The evaluator shall perform the following test: Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures re-authentication is needed when trying to unlock the session.

	Assurance Activity – Design	Assurance Activity - Guidance	Assurance Activity - Testing
FTA_TAB.1.1	The evaluator shall check the TSS to ensure that it details each method of access (local and remote) available to the administrator (e.g., serial port, SSH, HTTPS).		The evaluator shall also perform the following test: Test 1: The evaluator follows the operational guidance to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify the notice and consent warning message is displayed in each instance.
FTP_ITC.1.1	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.	The evaluator shall confirm the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and it contains recovery instructions should a connection be unintentionally broken.	The evaluator shall also perform the following tests: Test 1: The evaluators shall ensure communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring communication is successful. Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure the communication channel can be initiated from the TOE. Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. Test 4: The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE. Test 5: The evaluators shall, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure when physical connectivity is restored, communications are appropriately protected.
FTP_TRP.1.1	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.	The evaluator shall confirm the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.	The evaluator shall also perform the following tests: Test 1: The evaluators shall ensure communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring communication is successful. Test 2: For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure there is no available interface that can be used by a remote user to establish remote administrative sessions without invoking the trusted path. Test 3: The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext. Test 4: The evaluator shall ensure, for each method of remote administration, modification of the channel data is detected by the TOE.

Table 5 NDPP Security Functional Requirement Assurance Activities

	Assurance Activity
ADV_FSP	There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.2 (of the NDPP), and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.
AGD_OPE	Some of the contents of the operational guidance will be verified by the assurance activities above and evaluation of the TOE according to the CEM. The following additional information is also required. The operational guidance shall at a minimum list the processes running (or that could run) on the TOE in its evaluated configuration during its operation that are capable of processing data received on the network interfaces (there are likely more than one of these, and this is not limited to the process that 'listens' on the network interface). It is acceptable to list all processes running (or that could run) on the TOE in its evaluated configuration instead of attempting to determine just those process the network data. For each process listed, the administrative guidance will contain a short (e.g., one- or two-line) description of the process' function, and the privilege with which the service runs. 'Privilege' includes the hardware privilege level (e.g., ring 0, ring 1), any software privileges specifically associated with the process, and the privileges associated with the user role the process runs as or under. The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. The documentation must describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify this process includes the following steps: 1. For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1(2) mechanism to ensure a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means. 2. Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). 3. Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.
AGD_PRE	As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.
ALC_CMC	The evaluator shall check the ST to ensure it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure the information in the ST is sufficient to distinguish the product.
ALC_CMS	The 'evaluation evidence required by the SARs' in the NDPP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring the TOE is specifically identified and this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

	Assurance Activity
ATE_IND	The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of the NDPP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluator must document in the test plan each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument the differences do not affect the testing to be performed. It is not sufficient to merely assert the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. The evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by the NDPP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a 'fail' and 'pass' result (and the supporting details), and not just the 'pass' result.
AVA_VAN	As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in network infrastructure devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, a test would be suitable at the assurance level of the NDPP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Table 6 NDPP Assurance Family Assurance Activities

6. TOE Summary Specification

This chapter describes the security functions:

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

6.1 Security audit

The TOE is designed to generate log records for a wide range of security relevant and other events as they occur. The events that can cause a logged audit record include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in **Table 3**.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user) responsible for the event (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in **Table 3**.

The TOE includes an internal log implementation that can be used to store and review audit records locally. Alternately, the TOE can be configured to send generated audit records to an external SYSLOG server using IPsec. The TOE can be further configured so the SYSLOG server is on a dedicated VLAN to help protect exported audit records for disclosure or modification. This necessarily requires the dedicated VLAN be used for this dedicated purpose in the operational environment.

When configured to export audit records, when the TOE finds the external SYSLOG server is not responding (e.g., due to a network discontinuity), it will send an SNMP trap to a configure SNMP server so an administrator can become aware of, and remedy, the situation.

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

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in **Table 3**. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 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 a dedicated VLAN and IPSEC for communication with the SYSLOG server.

6.2 Cryptographic support

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

Functions	Standards	Certificates
Asymmetric key generation		
• Domain parameter generation	NIST Special Publication 800-56B	RSA Cert #1327
Encryption/Decryption		
• AES ECB and CBC (128-256 bits)	FIPS PUB 197 NIST SP 800-38A	AES Cert #2413
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2	RSA Cert #1247
Cryptographic hashing		
• SHA-1 and SHA-256 (digest sizes 160 and 256 bits)	FIPS Pub 180-3	SHS Cert #2070
Keyed-hash message authentication		
• HMAC-SHA-1 (digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	HMAC Cert #1499
Random bit generation		
• RGB with one independent hardware based noise source of 128 bits of non-determinism	FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES	RNG Cert #1191

Table 7 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	
5.9	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	
8	Should	yes	
8.3.2	should not	yes	

Table 8 NIST SP800-56B Conformance

The TOE uses a software-based random bit generator that complies with FIPS 140-2 ANSI x9.31 Random Number Generation (RNG) when operating in the FIPS mode. The entropy source is a 128-bit value extracted 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. Where identified zeroization occurs as follows: 1) when deleted from FLASH, the previous value is overwritten once with zeroes; 2) when added to 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.

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 1024 ~ 2048 bit key sizes.	Private Key - FLASH (cipher text/3DES) and RAM (plain text) Public Key – FLASH (cipher text/3DES) and RAM (plain text)	Private Key - A CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM. Public Key - A CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM.
CSP2	DSA public/private keys *(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/3DES) and RAM (plain text) Public Key – FLASH cipher text/3DES) and RAM (plain text)	Private Key - A CLI command is used to zeroize keys in FLASH and reboot results in the zeroization of keys in RAM. Public Key - A 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 *(TLS is not included in the evaluated configuration)*	Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + either DH or RSA) Algorithm: Also 3DES & AES	Used in HTTPS connections	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
CSP6	SSH Session Keys	ANSI X9.31 / 3DES-AES	SSH keys	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP7	IPsec authentication Keys	ANSI X9.31 / 3DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are 3DES or AES keys.	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP8	IPsec traffic Keys	ANSI X9.31 / 3DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are 3DES or AES keys.	RAM (plain text)	Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP9	IPsec authentication Keys	3DES-AES	3DES or AES Keys are 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	3DES-AES	3DES or AES Keys are 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 clear FLASH command is issued. Keys in RAM will be zeroized upon resetting or rebooting the security appliance.
CSP12	IKE Authentication Key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: 3DES, AES, SHA-1	Used to encrypt and 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+HMAC-SHA1+DH). Algorithms: 3DES, AES, SHA-1	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 clear FLASH command is issued. 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, when 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 9 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 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. The TOE manages a packet counter for each SSH session so 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 4303 for security. The primary cryptographic algorithms used by the TOE include AES-CBC-128 and AES-CBC-256 (both specified by RFC 3602 along with IKEv1 as defined in RFCs 2407, 2408, 2409, and RFC 4109. The TOE supports both main and aggressive modes, though aggressive mode is disabled in FIPS mode as indicated above. Furthermore, "confidentiality only" ESP mode is disabled by default.

IKEv1 SA lifetime and volume limits can be configured via a CLI function 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 implements 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 the peer also has the pre-shared key. 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 1 to 128 characters in length (e.g., 22 characters). The TOE requires suitable keys to be entered by an authorized administrator using a CLI function.

The following sections summarize how keys are established and used for IPsec and SSH. Each feature using a key pair must generate its own new key pair.

If the key pair is used for IPsec, the operational procedure to establish and use the key pair is as follows:

1. The administrator configures the device with standard IPsec configuration and must specify the "rsa-signature" authentication method for the IKE proposal.
2. The administrator generates the RSA key pair via the command line "public-key local create rsa". This key pair is used for IKE negotiation.
3. The administrator configures the PKI entity and PKI domain to retrieve and request the CA certificate and local certificate with RSA key pairs. The local certificate has public RSA key.
4. IKE negotiation will be triggered to set up SAs when there is protected subnet traffic in the device.
5. In the IKE phase 1 main mode negotiation, the 5th IKE packet has signature payload signed by RSA private key and certificate payload with RSA public key. When receiving this IKE packet, the device verifies the signature payload using the public key in the certificate payload.

If the key pair used for SSH, and the device is an SSH server, the operational procedure to establish and use the key pair is as follows:

1. The administrator generates the RSA key pair via the command line "public-key local create rsa". This command will replace the key pair for the IPsec and generate a new one for SSH.
2. The administrator configures the other SSH server configuration and the device as SSH server.
3. When an SSH client accesses the device, during the key exchange stage, the rsa public key of the device is sent to the client.
4. RSA key pairs are required for generating the session key and session ID in the key exchange stage, and can also be used by a client to authenticate the server. When a client tries to communicate with a server, it compares the public key it receives from the server with the server public key it saved locally. If the keys are consistent, the client uses the public key to authenticate the digital signature it receives from the server. If the digital signatures are consistent, the authentication succeeds.

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

- FCS_CKM.1: See table above.
- FCS_CKM_EXT.4: Keys are zeroized when they are no longer needed by the TOE.
- 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.

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. 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, and 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. 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.

In order to log in, the user must provide an identity and also authentication data (e.g., password or RSA credentials 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 defined 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 passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

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 regain 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 (from 8 to 32 characters) minimum password length and, if configured, the new password cannot match any of the passwords retained within the scope of the configured history.

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

- FIA_PMG_EXT.1: The TOE implements a configurable minimum password length and allows passwords to be composed of any combination of upper and lower case letters, numbers and special characters, 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 doesn't offer any services or access to its functions without requiring a user to be 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 and, given limited differences, for the purpose of this Security Target both are considered instances of the 'Security Administrator' as defined in the NDPP. 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 a range of security management functions for use by an authorized administrator. Among these functions are those necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

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

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Security Administrators (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.1: The TOE includes four defined roles, two of which correspond to the require 'Security Administrator'.

6.6 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components to a large extent. Secure communication with third-party peers as addressed in section 6.8, Trusted path/channels, and secure communication among multiple instances of the TOE is limited to a direct link between redundant switch appliances deployed in a high-availability configuration. 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.

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

While the administrative interface is function rich, the TOE is designed specifically to provide access only to locally-stored hashed (and not plain text) passwords and also, while cryptographic keys can be entered, the TOE does not disclose any keys stored in the TOE. Stored passwords are hashed using SHA-256. See Table 9 Key/CSP Zeroization Summary for more information about stored keys and passwords; 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 utilizes SSHv2 for secure communications. This protocol includes built-in capabilities to detect and appropriately handle (e.g., reject) replayed network traffic.

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 FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing.

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

The TOE includes a validity checking function that can be enabled when upgrading the boot ROM program, while system boot files and software patches are always validated prior to installation. In each case, the upgrade version will be checked to ensure it is appropriate and the upgrade file will be verified using an embedded (HP authorized) digital signature verified against a configured pair of hard-coded keys embedded in the TOE. If the version is incorrect or the signature cannot be verified, the upgrade will not proceed to protect the integrity of the TOE. More specifically, each update includes a header and data. The header includes a SHA-256 secure hash of the data that is signed (using rDSA/RSA 2048) by HP. In order to verify the data, the TOE generates its own SHA-256 secure has 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. Passwords are stored in hashed from 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 software checksums are correct, and also to test the presence and function of plugged devices.
- FPT_TUD_EXT.1: The TOE provides functions to query and upgrade the versions of the boot ROM program and system boot file (including installing hotfixes). Digital signatures are used to ensure the integrity of each upgrade prior to performing the upgrade; this checking is optional for the boot ROM program since special circumstances might require those checks to be disabled.

6.7 TOE access

The TOE can be configured to display administrator-configured advisory banners that will appear under a variety of circumstances. A session banner can be configured to be displayed when a session is established. A login banner can be configured to display welcome information in conjunction with login prompts. A message of the day can also be configured to be displayed before authentication is completed. A legal banner can be configured to present legal advisories prior to a user logging in and this banner waits, requiring the user to confirm whether they want to continue with the authentication process. In each case, the banners will be displayed when accessing the TOE via the console or SSH interfaces.

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout) – the default timeout is 10 minutes. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. 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 when administrators successfully establish interactive sessions with the TOE.

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 and can also be configured to utilize dedicated VLANs for this purpose. Of course, the SYSLOG server would need to be configured to also use IPsec and to be on the dedicated VLAN in the operational environment. If the SYSLOG server is adjacent to the TOE, the VLAN configuration would directly ensure audit records are sent only to the SYSLOG server. If the SYSLOG server is not adjacent to the TOE, it is assumed other trusted switches similarly configured to recognize the dedicated VLAN would ensure audit records sent on the dedicated VLAN remain only on that VLAN and will be sent to the configured SYSLOG server appropriately. Regardless, IPsec would ensure SYSLOG records are not disclosed even if they are not restricted to only protected network segments.

Other remote peers, such as SNMP, NTP, RADIUS, and TACACS servers, could also be configured to utilize IPsec or to be on dedicated VLANs if deemed necessary in a given operational environment.

To support secure remote administration, the TOE includes an implementation of SSHv2. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Only the local console is available by default and each of these remote administration services can be independently enabled by an administrator.

In the case of SSHv2, the TOE offers a secure command line interface (CLI) interactive administrator session. An administrator with an appropriate SSHv2-capable client can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

All of the secure protocols are supported by the cryptographic operations provided by the FIPS certified cryptographic algorithms 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 and can also utilize a dedicated VLAN to ensure any authentication operations, exported audit records, and time information are sent only to the configured SYSLOG server so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSH, based on its embedded cryptomodule, to support secure remote administration.. Administrators can initiate a remote session that is secured (disclosure and modification) using FIPS certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.

7. Protection Profile Claims

This ST is conformant to the *Security Requirements for Network Devices, Version 1.1, 8 June 2012* (NDPP) – with the optional SSH and IPsec requirements.

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 sections 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 verbatim from the NDPP.

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_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.1: Security Roles	NDPP
FPT: Protection of the TSF	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	NDPP
	FPT_STM.1: Reliable Time Stamps	NDPP
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL.4: User-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	NDPP
	FTP_TRP.1: Trusted Path	NDPP

Table 10 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 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. The NDPP does not explicitly or clearly correspond or rationalize 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	
OE.TRUSTED_ADMIN										X

Table 11 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:

- 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:

- 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:

- O.TSF_SELF_TEST: To reduce the potential for undetected TOE failures and to help ensure 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:

- 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 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:

- 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:

- 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:

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

8.1.1.8 A.NO_GENERAL_PURPOSE

It is assumed 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:

- 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:

- 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:

- 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. **Table 12** indicates the requirements 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. The NDPP does not explicitly or clearly correspond or rationalize 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.

	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_UAU.7						X		
FIA_UAU_EXT.2						X		
FIA_UIA_EXT.1						X		
FMT_MTD.1						X		
FMT_SMF.1						X		
FMT_SMR.1						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		X		
FTA_SSL.4						X		
FTA_SSL_EXT.1				X		X		
FTA_TAB.1	X							
FTP_ITC.1		X						
FTP_TRP.1		X						

Table 12 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:

- 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:

- 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.
- 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 any data contained in a protected resource is not available when the resource is reallocated.

This TOE Security Objective is satisfied by ensuring:

- 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:

- 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:

- 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 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:

- 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 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.1: 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:

- FPT_TST_EXT.1: The TOE is required to exercise self-tests during start-up to periodically ensure 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 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:

- 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), which correspond to EAL1, in this ST represents the SARs identified in the NDPP.

The NDPP includes a number of 'Assurance Activities' which are in effect refinements of the underlying SARs. As such, those assurance activities have been reproduced in this ST since they need be addressed in the context of the evaluation.

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
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_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.2 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	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

ST Requirement	CC Dependencies	ST Dependencies
FTP_ITC.1	none	none
FTP_TRP.1	none	none
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
AGD_PRE.1	none	none
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1

Table 13 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 14 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_STG_EXT.1	X							
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_IPSEC_EXT.1		X						
FCS_RBG_EXT.1		X						
FCS_SSH_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UAU.7				X				
FIA_UAU_EXT.2				X				
FIA_UIA_EXT.1				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.1					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 14 Security Functions vs. Requirements Mapping

Appendix A: Documentation for A Series Switches

This Appendix provides a list of the product documentation used during the evaluation of each Network switch product family.

5120 EI Switch Series
The following documents for the 5120 EI Switch series can be found under the *General Reference* section of the 5120 EI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5120-EI Series Ethernet Switches 51200-EI Security Command Reference, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches Fundamentals Command Reference, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches Network Management and Monitoring Command Reference, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches ACL and QoS Command Reference, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches Layer-3 IP Services Command Reference, 23 Sep 2011

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4174705#0

The following documents for the 5120 EI Switch series can be found under the *Setup and Install* section of the 5120 EI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5120-EI Series Ethernet Switches Security Configuration Guide, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches Fundamentals Configuration Guide, 23 Sep 2011
- HP 5120 EI Network Management and Monitoring Configuration Guide, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches ACL and QoS Configuration Guide, 23 Sep 2011
- HP 5120-EI Series Ethernet Switches Layer-3 IP Services Configuration Guide, 23 Sep 2011
- HP 5120 EI Switch Series Installation Manual, 24 Sep 2011

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4174705#2

5500 EI Switch Series
The following documents for the 5500 EI Switch series can be found under the *General Reference* section of the 5500 EI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5500-EI & 5500-SI Series Ethernet Switches Security Command Reference, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Fundamentals Command Reference, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Network Management and Monitoring Command Reference, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches ACL and QoS Command Reference, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Layer-3 IP Services Command Reference, 22 Sep 2011

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4174795#0

The following documents for the 5500 EI Switch series can be found under the *Setup and Install* section of the 5500 EI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5500-EI & 5500-SI Series Ethernet Switches Security Configuration Guide, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Fundamentals Configuration Guide, 22 Sep 2011
- HP 5500 EI Network Management and Monitoring Configuration Guide, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches ACL and QoS Configuration Guide, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Layer-3 IP Services Configuration Guide, 22 Sep 2011
- HP 5500-EI & 5500-SI Series Ethernet Switches Installation Manual, 22 Sep 2011

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4174795#2

5500 HI Switch Series

The following documents for the 5500 HI Switch series can be found under the *General Reference* section of the 5500 HI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5500HI Series Ethernet Switches Security Command Reference, 1 Feb 2012
- HP 5500HI Series Ethernet Switches Fundamentals Command Reference, 1 Feb 2012
- HP 5500HI Series Ethernet Switches Network Management and Monitoring Command Reference, 1 Feb 2012
- HP 5500HI Series Ethernet Switches ACL and QoS Command Reference, 1 Feb 2012
- HP 5500-HI Series Ethernet Switches Layer-3 IP Services Command Reference, 1 Feb 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=5195279#0

The following documents for the 5500 HI Switch series can be found under the *Setup and Install* section of the 5500 HI Switch Series documentation page on the HP Web site. The link is provided below.

- HP 5500HI Series Ethernet Switches Security Configuration Guide, 1 Feb 2012
- HP 5500HI Series Ethernet Switches Fundamentals Configuration Guide, 1 Feb 2012
- HP 5500 HI Network Management and Monitoring Configuration Guide, 1 Feb 2012
- HP 5500HI Series Ethernet Switches ACL and QoS Configuration Guide, 1 Feb 2012
- HP 5500HI Series Ethernet Switches Layer-3 IP Services Configuration Guide, 1 Feb 2012
- HP 5500HI Series Ethernet Switches Installation Manual, 1 Feb 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=5195279#2

5800 Switch Series

The following documents for the 5800 Switch series can be found under the *General Reference* section of the 5800 Switch Series documentation page on the HP Web site. The link is provided below.

- R1211-HP 5820X & 5800 Switch Series Security Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Fundamentals Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Network Management and Monitoring Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series ACL and QoS Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Layer-3 IP Services Command Reference, 8 Jan 2013

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177501#0

The following documents for the 5800 Switch series can be found under the *Setup and Install* section of the 5800 Switch Series documentation page on the HP Web site. The link is provided below.

- R1211-HP 5820X & 5800 Switch Series Security Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Fundamentals Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Network Management and Monitoring Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series ACL and QoS Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Layer-3 IP Services Configuration Guide, 8 Jan 2013
- HP 5800 Series Ethernet Switches Installation Manual, 30 May 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177501#2

5820 Switch Series

The following documents for the 5820 Switch series can be found under the *General Reference* section of the 5820 Switch Series documentation page on the HP Web site. The link is provided below.

- R1211-HP 5820X & 5800 Switch Series Security Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Fundamentals Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Network Management and Monitoring Command Reference, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series ACL and QoS Command Reference, 8 Jan 2013

- R1211-HP 5820X & 5800 Switch Series Layer-3 IP Services Command Reference, 8 Jan 2013

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4218345#0

The following documents for the 5820 Switch series can be found under the *Setup and Install* section of the 5820 Switch Series documentation page on the HP Web site. The link is provided below.

- R1211-HP 5820X & 5800 Switch Series Security Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Fundamentals Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Network Management and Monitoring Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series ACL and QoS Configuration Guide, 8 Jan 2013
- R1211-HP 5820X & 5800 Switch Series Layer-3 IP Services Configuration Guide, 8 Jan 2013
- HP 5800 Series Ethernet Switches Installation Manual, 30 May 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4218345#2

7500 Switch Series

The following documents for the 7500 Switch series can be found under the *General Reference* section of the 7500 Switch Series documentation page on the HP Web site. The link is provided below.

- R6626 - HP 7500 Switch Series Security Command Reference, 18 Jan 2012
- R6626 - HP 7500 Switch Series Fundamentals Command Reference, 18 Jan 2012
- R6626 - HP 7500 Switch Series Network Management and Monitoring Command Reference, 18 Jan 2012
- R6626 - HP 7500 Switch Series ACL and QoS Command Reference, 18 Jan 2012
- R6626 - HP 7500 Switch Series Layer-3 IP Services Command Reference, 18 Jan 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177519#0

The following documents for the 7500 Switch series can be found under the *Setup and Install* section of the 7500 Switch Series documentation page on the HP Web site. The link is provided below.

- R6626 - HP 7500 Switch Series Security Configuration Guide, 18 Jan 2012
- R6626 - HP 7500 Switch Series Fundamentals Configuration Guide, 18 Jan 2012
- R6626 - HP 7500 Switch Series Network Management and Monitoring Configuration Guide, 18 Jan 2012
- R6626 - HP 7500 Switch Series ACL and QoS Configuration Guide, 18 Jan 2012
- R6626 - HP 7500 Switch Series Layer-3 IP Services Configuration Guide, 18 Jan 2012
- HP 7500 Switch Series Installation Manual, 28 Feb 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177519#2

9500 Switch Series

The following documents for the 9500 Switch series can be found under the *General Reference* section of the 9500 Switch Series documentation page on the HP Web site. The link is provided below.

- H3C S9500E Series Routing Switches Security Command Reference, 1 Dec 2010
- H3C S9500E Series Routing Switches Fundamentals Command Reference, 1 Dec 2010
- H3C S9500E Series Routing Switches Network Management and Monitoring Command Reference, 1 Dec 2010
- H3C S9500E Series Routing Switches ACL and QoS Command Reference, 1 Dec 2010
- H3C S9500E Series Routing Switches Layer-3 IP Services Command Reference, 1 Dec 2010

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177590#0

The following documents for the 9500 Switch series can be found under the *Setup and Install* section of the 9500 Switch Series documentation page on the HP Web site. The link is provided below.

- H3C S9500E Series Routing Switches Security Configuration Guide, 1 Dec 2010
- H3C S9500E Series Routing Switches Fundamentals Configuration Guide, 1 Dec 2010

- H3C S9500E Series Routing Switches Network Management and Monitoring Configuration Guide, 1 Dec 2010
- H3C S9500E Series Routing Switches ACL and QoS Configuration Guide, 3 Feb 2011
- H3C S9500E Series Routing Switches Layer-3 IP Services Configuration Guide, 1 Dec 2010
- H3C S9500E Series Routing Switches Installation Manual, 1 Dec 2010

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177590#2

12500 Switch Series

The following documents for the 12500 Switch series can be found under the *General Reference* section of the 12500 Switch Series documentation page on the HP Web site. The link is provided below.

- R7128-HP 12500 Security Command Reference, 30 Nov 2012
- R7128-HP 12500 Fundamentals Command Reference, 30 Nov 2012
- R7128-HP 12500 Network Management and Monitoring Command Reference, 30 Nov 2012
- R7128-HP 12500 ACL and QoS Command Reference, 30 Nov 2012
- R7128-HP 12500 Layer-3 IP Services Command Reference, 30 Nov 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177453#0

The following documents for the 12500 Switch series can be found under the *Setup and Install* section of the 12500 Switch Series documentation page on the HP Web site. The link is provided below.

- R7128-HP 12500 Security Configuration Guide, 30 Nov 2012
- R7128-HP 12500 Fundamentals Configuration Guide, 20 Dec 2012
- R7128-HP 12500 Network Management and Monitoring Configuration Guide, 30 Nov 2012
- R7128-HP 12500 ACL and QoS Configuration Guide, 30 Nov 2012
- R7128-HP 12500 Layer-3 IP Services Configuration Guide, 30 Nov 2012
- R1726 and R7128-HP 12500 Routing Switch Series Installation Manual, 6 Dec 2012

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=101&prodTypeId=12883&prodSeriesId=4177453#2