Hewlett-Packard Company A-Series Switches/w Security Blades Security Target

Version 1.0
3/20/2013

Prepared for:
Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

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 A-Series Switches provided by Hewlett-Packard Development Company. Each of the A-Series 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 A-Series Switches/w Security Blades Security Target

ST Version – Version 1.0

ST Date – 3/20/2013

TOE Identification – Hewlett-Packard Company A-Series Switches with Comware version 5.20 and installed Security Blades (VPN Firewall Module)

Product Series	Specific Devices
HP A7500 Series Modular Core Switches with • HP A7500 VPN Firewall Module	HP A7510 Switch Chassis
	HP A7506 Switch Chassis
	HP A7506-V Switch Chassis
	HP A7503 Switch Chassis
	HP A7502 Switch Chassis
	HP A7503 1 Fabric Slot Switch Chassis
HP A9500 Series Modular Core Switches with • HP A9500 VPN Firewall Module	HP A9508 Switch Chassis
	HP A9508-V Switch Chassis
	HP A9512 Switch Chassis
HP A12500 Series Data Center Switches with • HP A12500 VPN Firewall Module	HP A12518 Switch Chassis
	HP A12508 Switch Chassis

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 conforms to the *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007*
- 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 2 augmented with ALC_FLR.2

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- 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 A-Series family of switches with installed Security Blades (VPN Firewall Module) introducing firewall features. The A-Series switches in the evaluated configuration include the A7500, A9500 and A12500 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 A-Series 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). While pluggable security blades are required in the evaluated configuration, all of the available plug-in modules are included and can optionally be used in the evaluated configuration (see below). The security blades offer additional advanced (e.g., firewall) security functions that are claimed in this Security Target and hence are required.

The TOE can be deployed as a single A-Series device or alternately as a group of A-Series devices connected using the HP Intelligent Resilient Framework (IRF) technology to effectively form a logical switch device. The IRF technology requires that A-Series 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 A-Series switches are Gigabit Ethernet switch appliances which consist of hardware and software components. While the physical form factor of each distinct series in the A-Series 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.

A7500 Series Switches

The HP A7500 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 A7500 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 module is required by this series in the evaluated configuration:

- HP A7500 VPN Firewall Module

The following additional 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 A7510 768Gbps Fabric/Main Processing Unit
- HP A7500 384Gbps Fabric/Main Processing Unit
- HP A7500 384Gbps Fabric/Main Processing Unit with 12 GbE SFP Ports
- HP A7500 384Gbps Fabric/Main Processing Unit with 2 10-GbE XFP Ports
- HP A7500 384Gbps Fabric/Advanced Main Processing Unit
- HP A7500 384Gbps Fabric/Lite Main Processing Unit
- HP A7500 48-port 100Base-FX SA Module
- HP A7500 48-port 10/100Base-TX PoE-upgradable SA Module
- HP A7500 48-port Gig-T PoE-upgradable SA Module
- HP A7500 48-port GbE SFP SC Module
- HP A7500 48-port Gig-T PoE-upgradable SC Module
- HP A7500 40-port Gig-T/8-port GbE SFP PoE-upgradable SC Module
- HP A7500 24-port GbE SFP/2-port 10-GbE XFP SC Module

- HP A7500 24-port Gig-T/2-port 10-GbE XFP SC Module
- HP A7500 24-port GbE SFP SC Module
- HP A7500 24-port Gig-T SC Module
- HP A7500 16-port GbE SFP/8-port GbE Combo SC Module
- HP A7500 12-port GbE SFP SC Module
- HP A7500 8-port 10-GbE SFP+ SC Module
- HP A7500 2-port 10-GbE XFP SC Module
- HP A7500 12-port GbE SFP EA Module
- HP A7500 1-port 10-GbE XFP EA Module
- HP A7500 48-port GbE SFP SD Module
- HP A7500 48-port Gig-T PoE+ SD Module
- HP A7500 24-port GbE SFP/2-port 10-GbE XFP SD Module
- HP A7500 16-port GbE SFP/8-port GbE Combo SD Module
- HP A7500 8-port 10-GbE XFP SD Module
- HP A7500 4-port 10-GbE XFP SD Module
- HP A7500 2-port 10-GbE XFP SD Module
- HP A7500 48-port GbE SFP EB Module
- HP A7500 16-port GbE SFP/8-port GbE Combo EB Module
- HP A7500 4-port 10-GbE XFP EB Module
- HP A7500 2-port 10-GbE XFP EB Module

A9500 Series Switches

The HP A9500 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 A9500 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 module is required by this series in the evaluated configuration:

- HP A9500 VPN Firewall Module

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 A9500 48-port GbE SFP LEB Module
- HP A9500 48-port Gig-T LEB Module
- HP A9500 48-port Gig-T REB Module
- HP A9500 16-port GbE SFP/8-port GbE Combo LEB Module
- HP A9500 16-port Gig-T/8-port GbE Combo LEB Module
- HP A9500 16-port 10-GbE SFP+ REB Module
- HP A9500 4-port 10-GbE XFP LEB Module
- HP A9500 2-port 10-GbE XFP LEB Module
- HP A9500 48-port GbE SFP LEC Module
- HP A9500 48-port Gig-T LEC Module
- HP A9500 16-port GbE SFP/8-port GbE Combo LEC Module
- HP A9500 16-port Gig-T/8-port GbE Combo LEC Module
- HP A9500 4-port 10-GbE XFP LEC Module
- HP A9500 2-port 10-GbE XFP LEC Module

A12500 Series Switches

The HP A12500 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 A12500 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 module is required by this series in the evaluated configuration:

- HP A12500 VPN Firewall Module

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 A12500 Main Processing Unit
- HP A12508 Fabric Module
- HP A12518 Fabric Module
- HP A12500 48-port Gig-T LEB Module
- HP A12500 48-port Gig-T LEC Module
- HP A12500 48-port GbE SFP LEB Module
- HP A12500 48-port GbE SFP LEC Module
- HP A12500 4-port 10-GbE XFP LEB Module
- HP A12500 4-port 10-GbE XFP LEC Module
- HP A12500 8-port 10-GbE XFP LEB Module
- HP A12500 8-port 10-GbE XFP LEC Module
- HP A12500 32-port 10-GbE SFP+ REB Module
- HP A12500 32-port 10-GbE SFP+ REC Module
- HP A12500 Spare Power Monitor Module

2.2 TOE Architecture

The HP A-Series switches all 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, Ethernet switching, Intelligent Resilient Framework (IRF), routing, Quality of Service (QoS), etc.. The evaluated version of Comware is 5.20. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux (i.e., Fedora 14).

The Comware v5.20 architecture can be depicted as follows:

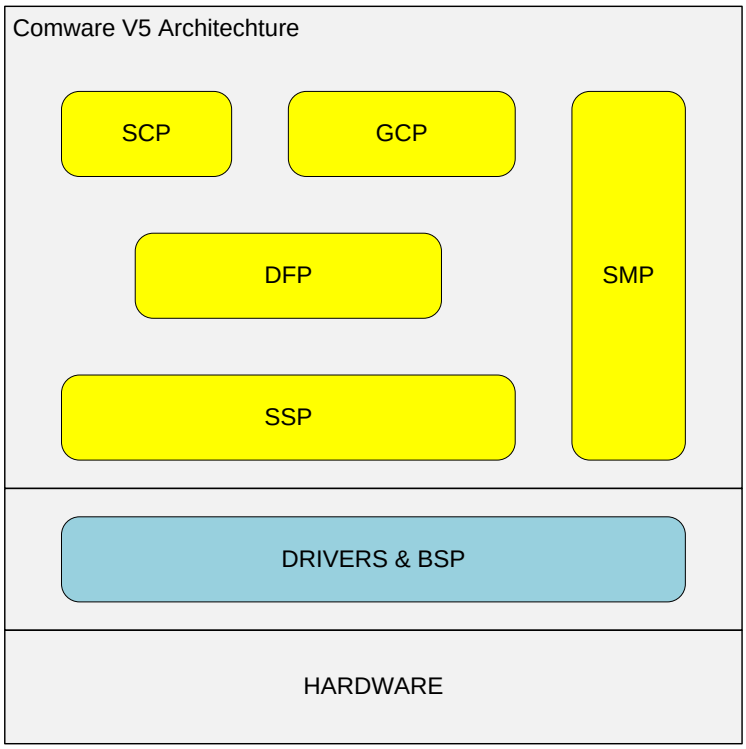

Figure 1 Comware v5.20 Architecture

- ***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), Web (HTTPS), and Management Information Base - MIB (SNMPv3) management options. Note that Web access is not included within the scope of evaluation.

- ***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 MIB, Web, and CLI management. 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 a cryptographic module that supports SSH, SNMPv3, and HTTPS (HTTP over TLSv1) 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.

With security blades (modules) installed in the TOE, more advanced firewall security features are available including stateful packet filtering and IPSec VPN support.

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

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

Note that the IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must 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.

Alternately, the TOE can be deployed as a pair of appliances connected via a dedicated high-availability link so that the pair operates in a redundant manner allowing continued operations should one of the appliances fail.

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 and received SNMP traps. Note that the TOE supports SNMPv3.
- Certificate Authority (CA) server – The TOE can be configured to utilize digital certificates, e.g., for VPN connections.
- VPN Peers – The TOE can establish VPNs with peers via IPSec.
- Management Workstation – The TOE supports CLI access and as such an administrator would need a terminal emulator (supporting SSHv2) to utilize those administrative interfaces.

2.2.3 Logical Boundaries

This section summarizes the security functions provided by HP A-Series Switch:

- Security audit

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

2.2.3.1 Security audit

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

Locally stored audit records can be reviewed and otherwise managed by an administrator.

2.2.3.2 Cryptographic support

The TOE includes a FIPS 140-2 certified cryptographic module (Certificate #1910) that provides 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, SSH, and SNMP.

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 carefully designed to ensure that it doesn't inadvertently reuse data found in network traffic.

With the installed Security Blades, the TOE implements stateful packet filtering and IPSec VPN services. These services can be configured and monitored by an administrator.

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. An SNMPv3 interface, which also requires proper user credentials, is also available non-interactive MIB based management of the TOE.

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 and Management Interface Block (MIB) SNMPv3 interface 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 that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

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). Note that 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 the the IRF communication channels are not protected using mechanisms such as encryption, they need to be as protected as the TOE devices themselves.

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

2.2.3.7 Resource utilisation

The TOE can limit network connections in order to ensure that administrators will be able to connect when they need to perform security management operations on the TOE.

2.2.3.8 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.

2.2.3.9 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Access to the non-interactive MIB interface is protected using SNMPv3. In each case, both integrity and disclosure protection is ensured.

The TOE protects communication with network peers, such as a log server, using an IPSec VPNs.

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of Hewlett-Packard A-Series Switches. The following documents were specifically examined in the context of the evaluation:

- Command Reference for CC Supplement for 5120EI, 5500EI, 5800, 5820, and 7500
- Command Reference for CC Supplement for 12500, 9500, and 8800
- Command Reference for CC Supplement for Firewall Modules
- Configuration Reference for CC Supplement for 5120EI, 5500EI, 5800, 5820, and 7500
- Configuration Reference for CC Supplement for 12500, 9500, and 8800
- Configuration Reference for CC Supplement for Firewall Modules
- H3C S7500E Series Ethernet Switches Fundamentals Configuration Guide (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches Fundamentals Command Reference (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches ACL and QoS Configuration Guide (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches ACL and QoS Command Reference (Document Version 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches Security Configuration Guide (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches Security Command Reference (Document Version: 20100930-C-1.01)
- IPSec Guide (2.IPsec Commands.doc and 2.IPsec Configuration.doc)
- H3C S7500E Series Ethernet Switches Network Management and Monitoring Configuration Guide (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches Network Management and Monitoring Command Reference (Document Version: 20100930-C-1.01)
- H3C S7500E Series Ethernet Switches OAA Configuration Guide (Document Version: 20100722-C-1.01)
- H3C S7500E Series Ethernet Switches OAA Command Reference (Document Version: 20100930-C-1.01)

- H3C S9500E Series Routing Switches Fundamentals Configuration Guide (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches Fundamentals Command Reference (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches ACL and QoS Configuration Guide (Document Version: 5PW114-20101210)
- H3C S9500E Routing Switches ACL and QoS Command Reference (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches Security Configuration Guide (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches Security Command Reference (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches Network Management and Monitoring Configuration Guide (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches Network Management and Monitoring Command Reference (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches OAA Configuration Guide (Document Version: 5PW114-20101210)
- H3C S9500E Series Routing Switches OAA Command Reference (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Fundamentals Configuration Guide (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Fundamentals Command Reference (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches ACL and QoS Configuration Guide (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches ACL and QoS Command Reference (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Security Configuration Guide (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Security Command Reference (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Network Management and Monitoring Configuration Guide (Document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches Network Management and Monitoring Command Reference (document Version: 5PW114-20101210)
- H3C S12500 Series Routing Switches OAA Configuration Guide (Document version: 5W130-20110411)
- H3C S12500 Series Routing Switches OAA Command Reference (Document version: 5W130-20110411)
- H3C SecPath Series High-End Firewalls Getting Started Guide (Document version: 5PW105-20110921)
- H3C SecPath Series High-End Firewalls Access Control Configuration Guide (Document version: 5PW105-20110921)
- H3C SecPath Series High-End Firewalls VPN Configuration Guide (Document version: 5PW105-20110921)
- H3C SecPath Series High-End Firewalls System Management and Maintenance Configuration Guide (Document version: 5PW105-20110921)

Additional, on-line documentation can be found for the applicable TOE models and devices can be found via the following URLs:

- HP A7500 Switch Series overview

  http://h10010.www1.hp.com/wwpc/uk/en/sm/WF05a/12883-12883-4172267-4172283-4172283-4177519.html

  http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S7500E_Series_Switches/

- HP A9500 Switch Series overview

  http://h10010.www1.hp.com/wwpc/uk/en/sm/WF05a/12883-12883-4172267-4172283-4172283-4177590.html

  http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S9500E_Series_Switches/

- HP A12500 Switch Series overview

http://h10010.www1.hp.com/wwpc/us/en/sm/WF05a/12883-12883-4172267-4172305-4172283-4177453.html

http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/

- Firewall VPN Security Blade

  http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/Security_Products/H3C_SecBlade_II_Firewall_Cards/

3. Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from two distinct Protection Profiles (PPs): the *Security Requirements for Network Devices, Version 1.0, 10 December 2010* (NDPP) and the *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007* (TFFWPP). Note that 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. More specifically, the TFFWPP has presented a Security Problem Definition specifically appropriate for firewall devices and is applicable to the HP TOE in its evaluated configuration (i.e., with Security Blades installed).

Note that the Security Problem Definitions from the NDPP and TFFWPP are presented separately below. There has been no attempt to merge or integrate them.

3.1 NDPP Security Problem Definition

3.1.1 NDPP 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.

3.1.2 NDPP Threats

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
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.

3.1.3 NDPP 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.

3.2 TFFWPP Security Problem Definition

3.2.1 TFFWPP Threats

T.ASPOOF	An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons.

3.2.2 TFFWPP Assumptions

A.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
A.PHYSEC	The TOE is physically secure.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
A.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

4. Security Objectives

Like the Security Problem Definition, the Security Objectives have been drawn verbatim from the NDPP and TFFWPP. Note that 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. More specifically, the TFFWPP has presented a Security Objectives specifically directed at firewall devices and is applicable to the HP TOE in its evaluated configuration (i.e., with Security Blades installed).

Note that the Security Objectives from the NDPP and TFFWPP are presented separately below. There has been no attempt to merge or integrate them.

4.1 NDPP Security Objectives

4.1.1 NDPP Security Objectives for the TOE

O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the

	administrator to be unaltered and (optionally) from a trusted source.

4.1.2 NDPP 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.

4.2 TFFWPP Security Objectives

4.2.1 TFFWPP Security Objectives for the TOE

O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.MEDIAT	The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

4.2.2 TFFWPP Security Objectives for the Environment

OE.ADMTRA	Authorized administrators are trained as to establishment and maintenance of security policies and practices.
OE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.LOWEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
OE.NOREMO	Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
OE.PHYSEC	The TOE is physically secure.
OE.PUBLIC	The TOE does not host public data.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.
OE.SINGEN	Information can not flow among the internal and external networks unless it passes through the TOE.

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.

With the exception of the FPT_ITT.1 iterations (drawn directly from the CC to replace NDPP versions), the SFRs have been drawn from the Protection Profiles (PPs): *Security Requirements for Network Devices, Version 1.0, 10 December 2010* (NDPP) and *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007* (TFFWPP). As a result, refinements and operations already performed in those PPs are not identified (e.g., highlighted) here, rather the requirements have been copied from those PPs and any residual operations have been completed herein. Of particular note, those PPs make a number of refinements and complete some of the SFR operations defined in the CC and those PPs should be consulted to identify those changes if necessary. Note that unlike the previous sections, the SFRs from both PPs have been combined to present a common set of SFRs for the TOE.

The SARs are drawn from the Common Criteria (CC) part 3 since this ST is claiming EAL2.

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
- FAU_STG_EXT.3: Action in case of Loss of Audit Server Connectivity
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_COMM_PROT_EXT.1: Communications Protection
- 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.5: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FPT_PTD.1: Management of TSF Data
- 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 A-Series Switches.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
	FAU_STG_EXT.1: External Audit Trail Storage
	FAU_STG_EXT.3: Action in case of Loss of Audit Server Connectivity
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COMM_PROT_EXT.1: Communications Protection
	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_IFC.1: Subset information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_PMG_EXT.1: Password Management
	FIA_UAU.1: Timing of authentication
	FIA_UAU.4: Single-use authentication mechanisms
	FIA_UAU.6: Re-authenticating
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.5: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_ITT.1(1): Basic Internal TSF Data Transfer Protection (Disclosure)
	FPT_ITT.1(2): Basic Internal TSF Data Transfer Protection (Modification)
	FPT_PTD.1(1): Management of TSF Data (for reading of authentication data)
	FPT_PTD.1(2): Management of TSF Data (for reading of all symmetric keys)
	FPT_RPL.1: Replay Detection
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FRU: Resource utilisation	FRU_RSA.1: Maximum Quotas
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (Prevention of Disclosure)
	FTP_ITC.1(2): Inter-TSF Trusted Channel (Detection of Modification)
	FTP_TRP.1(1): Trusted Path
	FTP_TRP.1(2): 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 basic 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**].

Application Note: The table below is based on the audit events required in the NDPP. The material identified using underlined blue text is drawn from the TFFWPP, so all together the required auditable events and audit record content from both PPs is fully represented.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FAU_SAR.3	None.	
FAU_STG.1	None.	
FAU_STG.4	None.	
FAU_STG_EXT.1	None.	
FAU_STG_EXT.3	Loss of connectivity.	No additional information.
FCS_CKM.1	Failure on invoking functionality.	No additional information.
FCS_CKM_EXT.4	Failure on invoking functionality.	No additional information.
FCS_COMM_PROT_EXT.1	None.	
FCS_COP.1(1)	Failure on invoking functionality. Success and failure, and the type of cryptographic operation.	The identity of the external IT entity attempting to perform the cryptographic operation.
FCS_COP.1(2)	Failure on invoking functionality.	No additional information.
FCS_COP.1(3)	Failure on invoking functionality.	No additional information.
FCS_COP.1(4)	Failure on invoking functionality.	No additional information.
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	Failure of the randomization process.	No additional information.
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_IFC.1	None.	
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.

Requirement	Auditable Events	Additional Audit Record Contents
FDP_RIP.2	None.	
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts and the subsequent restoration by an administrator of the user's capability to authenticate.	The identity of the offending user and the administrator.
FIA_ATD.1	None.	
FIA_PMG_EXT.1	None.	
FIA_UAU_EXT.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE.
FIA_UAU.4	None.	
FIA_UAU.6	Attempt to re-authenticate.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_UID.2	All use of the user identification Mechanism.	The user identities provided to the TOE.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the administrator performing the operation.
FMT_MSA.3	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.1	Modifications to the group of users that are part of an administrator role per FMT_SMR.1.	The identity of the administrator performing the modification and the user identity being associated with the administrator role.
FPT_ITT.1(1)	None.	
FPT_ITT.1(2)	None.	
FPT_PTD.1(1)	None.	
FPT_PTD.1(2)	None.	
FPT_RPL.1	Detected replay attacks.	Origin of the attempt (e.g., IP address).
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address). The identity of the administrator performing the operation.
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond "success" or "failure".
FRU_RSA.1	Maximum quota being exceeded.	Resource identifier.
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_TAB.1	None.	
FTP_ITC.1(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_ITC.1(2)	Initiation of the trusted channel. Termination of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment

Requirement	Auditable Events	Additional Audit Record Contents
	Failure of the trusted channel functions.	attempt.
FTP_TRP.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FTP_TRP.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 3 Auditable Events

5.2.1.2 User identity association (FAU_GEN.2)

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

5.2.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on:

a) [presumed subject address;
b) ranges of dates;
c) ranges of times;
d) ranges of addresses].

5.2.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.

5.2.1.6 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized administrator and [shall limit the number of audit records lost] if the audit trail is full.

5.2.1.7 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 over a trusted channel defined in FTP_ITC.1***].

5.2.1.8 Action in case of Loss of Audit Server Connectivity (FAU_STG_EXT.3)

FAU_STG_EXT.3.1 The TSF shall [**generate an SNMP trap**] if the link to the external IT entity collecting the audit data generated by the TOE is not available.

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 in accordance with a domain parameter generator and [***a random number generator***] that meet the following:

a) All cases: (i.e., any of the above)

- ANSI X9.80 (3 January 2000), “Prime Number Generation, Primality Testing, and Primality Certificates” using random integers with deterministic tests, or constructive generation methods
- Generated key strength shall be equivalent to, or greater than, a symmetric key strength of 112 bits using conservative estimates.

b) Case: For domain parameters used in finite field-based key establishment schemes
- NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'

c) Case: For domain parameters used in RSA-based key establishment schemes
- NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography'.

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 Communications Protection (FCS_COMM_PROT_EXT.1)

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [***IPSec, SSH***] and [***no other protocol***].

5.2.2.4 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***].

5.2.2.5 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) Digital Signature Algorithm (DSA) with a key size (modulus) of 1024 bits[1],
(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]
that meets the following:
Case: Digital Signature Algorithm
- [***FIPS PUB 186-2, 'Digital Signature Standard'***]

Case: RSA Digital Signature Algorithm
- [***FIPS PUB 186-2, 'Digital Signature Standard'***].

5.2.2.6 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.'

5.2.2.7 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.'

[1] The NDPP indicates 2048 bits or greater, but FIPS 186-2 supports only 1024 bits for DSA. It has been determined the NDPP is in error and will be corrected in the future – this ST includes the corrected SFR.

5.2.2.8 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 1 (768-bit MODP), 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 (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")");
2. Pre-shared keys of 22 characters and [***8 ~ 128 characters***].

5.2.2.9 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 at least one independent 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.

5.2.2.10 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 connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [**90 seconds**], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [**3**] attempts.

FCS_SSH_EXT.1.4 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.1.5 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.1.6 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.1.7 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.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***hmac-sha1, hmac-sha1-96***].

FCS_SSH_EXT.1.9 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 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] on:

a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
b) information: traffic sent through the TOE from one subject to another;
c) operation: pass information].

5.2.3.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [UNAUTHENTICATED SFP] based on at least the following types of subject and information security attributes:

a) [subject security attributes: • presumed address;
b) information security attributes:
   - presumed address of source subject;
   - presumed address of destination subject;
   - transport layer protocol;
   - TOE interface on which traffic arrives and departs;
   - service;].

~~FDP_IF~~F.1.2 The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
   - the presumed address of the source subject, in the information, translates to an internal network address;
   - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.
b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
   - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
   - the presumed address of the source subject, in the information, translates to an external network address;
   - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall provide the following [none].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:

a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.]

5.2.3.3 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 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [a settable, non-zero number, **that is a positive integer**] of unsuccessful authentication attempts occur related to [external IT entities attempting to authenticate from an internal or external network.]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending external IT entity from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT entity in question.]

5.2.4.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: a) [identity; b) association of a human user with the authorized administrator role; c) **Authentication data (e.g. password)** ~~**any other user security attributes {to be determined by the Security Target writer(s)}**~~].

5.2.4.3 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 special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')');
2. Minimum password length shall settable by the Security Administrator, and support passwords of 8 characters or greater;
3. Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Security Administrator.
4. Passwords shall have a maximum lifetime, configurable by the Security Administrator.
5. New passwords must contain a minimum of 4 character changes from the previous password.

5.2.4.4 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [identification as stated in FIA_UID.2] on behalf of the authorized administrator or authorized external IT entity accessing the TOE to be performed before the authorized administrator or authorized external IT entity is authenticated.

FIA_UAU.1.2 The TSF shall require each authorized administrator or authorized external IT entity to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that authorized administrator or authorized IT entity.

5.2.4.5 Single-use authentication mechanisms (FIA_UAU.4)

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

a) authorized administrators;

b) authorized external IT entities].

5.2.4.6 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions: when the user changes their password, [***following TSF-initiated locking (FTA_SSL)***].

5.2.4.7 Protected Authentication Feedback (FIA_UAU.7)

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

5.2.4.8 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.5)

FIA_UAU_EXT.5.1 The TSF shall provide a local password-based authentication mechanism, [***[and/or access to external RADIUS and TACACS]***] to perform user authentication.

FIA_UAU_EXT.5.2 The TSF shall ensure that users with expired passwords are [***required to create a new password after correctly entering the expired password***].

Application Note: For the purpose of changing an expired password, there is no limit as to when that must occur.

5.2.4.9 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1 The TSF shall allow [***no services***] on behalf of the user to be performed before the user is identified and authenticated.

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

5.2.4.10 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Security management (FMT)

5.2.5.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to perform the functions:

a) [start-up and shutdown;
b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
c) create, delete, modify, and view user attribute values defined in FIA_ATD.1;
d) enable and disable single-use authentication mechanisms in FIA_UAU.4 (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
e) modify and set the threshold for the number of permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures (if the TOE supports authorized IT entities and/or remote administration from either an internal or external network);
g) enable and disable external IT entities from communicating to the TOE (if the TOE supports authorized external IT entities);
h) modify and set the time and date;
i) archive, create, delete, empty, and review the audit trail;
j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
k) recover to the state following the last backup;

l) additionally, if the TSF supports remote administration from either an internal or external network:
   - o enable and disable remote administration from internal and external networks;
   - o restrict addresses from which remote administration can be performed].

to [an authorized administrator].

5.2.5.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [UNAUTHENTICATED SFP] to provide restrictive default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.3 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.

5.2.5.4 Specification of Management Functions (FMT_SMF.1)

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

- Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1, respectively.
- Ability to configure the cryptographic functionality.
- Ability to update the TOE, and to verify the updates using the digital signature capability (FCS_COP.1(2)) and [***[other functions identified in FMT_MOF.1]***].

5.2.5.5 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: [Security Administrator[2], [***no other roles***]].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Basic Internal TSF Data Transfer Protection (Disclosure) (FPT_ITT.1(1))

FPT_ITT.1(1).1 The TSF shall protect TSF data from [***disclosure***] when it is transmitted between separate parts of the TOE.

Application Note: While the NDPP includes a version of this requirement to require the use of a cryptographic service to protect communication between distributed TOE components, the base CC requirement has been substituted since when applicable (e.g., redundancy supporting high-availability) protection is afforded by virtue of a dedicated link between TOE components in the evaluated configuration.

5.2.6.2 Basic Internal TSF Data Transfer Protection (Modification) (FPT_ITT.1(2))

FPT_ITT.1(2).1 The TSF shall protect TSF data from [***modification***] when it is transmitted between separate parts of the TOE.

Application Note: While the NDPP includes a version of this requirement to require the use of a cryptographic service to protect communication between distributed TOE components, the base CC requirement has been substituted since when applicable (e.g., redundancy supporting high-availability) protection is afforded by virtue of a dedicated link between TOE components in the evaluated configuration.

[2] While the TOE implements four distinct roles: visit, monitor, system, and manage, only two of them (system and manage) can perform security management functions and are logically mapped to the required 'Security Administrator' role.

5.2.6.3 Management of TSF Data (for reading of authentication data) (FPT_PTD.1(1))

FPT_PTD.1(1).1 Refinement: The TSF shall prevent reading of the plaintext passwords.

5.2.6.4 Management of TSF Data (for reading of all symmetric keys) (FPT_PTD.1(2))

FPT_PTD.1(2).1 Refinement: The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.6.5 Replay Detection (FPT_RPL.1)

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [network packets terminated at the TOE].

FPT_RPL.1.2 The TSF shall perform: [reject the data] when replay is detected.

5.2.6.6 Reliable Time Stamps (FPT_STM.1)

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

5.2.6.7 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.

5.2.6.8 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 Resource utilisation (FRU)

5.2.7.1 Maximum Quotas (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [**user sessions supporting the administrative interface**], [***[memory, CPU]***] that [***subjects***] can use [***simultaneously***].

5.2.8 TOE access (FTA)

5.2.8.1 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].

5.2.8.2 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- ***lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session***]

after a Security Administrator-specified time period of inactivity.

5.2.8.3 Default TOE Access Banners (FTA_TAB.1)

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

5.2.9 Trusted path/channels (FTP)

5.2.9.1 Inter-TSF Trusted Channel (Prevention of Disclosure) (FTP_ITC.1(1))

FTP_ITC.1(1).1 Refinement: The TSF shall use [**IPSEC**] to provide a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

FTP_ITC.1(1).2 Refinement: The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1(1).3 The TSF shall initiate communication via the trusted channel for [all authentication functions, [**audit data, and VPN peer communication**]].

5.2.9.2 Inter-TSF Trusted Channel (Detection of Modification) (FTP_ITC.1(2))

FTP_ITC.1(2).1 Refinement: The TSF shall use [**IPSEC**] in providing a trusted communication channel between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and detection of the modification of data.

FTP_ITC.1(2).2 Refinement: The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1(2).3 The TSF shall initiate communication via the trusted channel for [all authentication functions, [**audit data, and VPN peer communication**]].

5.2.9.3 Trusted Path (FTP_TRP.1(1))

FTP_TRP.1(1).1 Refinement: The TSF shall provide a communication path between itself and remote administrators using [**SSH**] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

FTP_TRP.1(1).2 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1(1).3 Refinement: The TSF shall require the use of the trusted path for all remote administrative actions.

5.2.9.4 Trusted Path (FTP_TRP.1(2))

FTP_TRP.1(2).1 Refinement: The TSF shall provide a communication path between itself and remote administrators using [**SSH**] that is logically distinct from other communication paths and provides assured identification of its end points and detection of modification of the communicated data.

FTP_TRP.1(2).2 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1(2).3 Refinement: The TSF shall require the use of the trusted path for all remote administrative actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4 EAL 2 augmented with ALC_FLR.2 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1c The functional specification shall completely represent the TSF.

ADV_FSP.2.2c The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1d The developer shall provide the design of the TOE.
ADV_TDS.1.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1c The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2c The design shall identify all subsystems of the TSF.
ADV_TDS.1.3c The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4c The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5c The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6c The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

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

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2d The developer shall provide the CM documentation.
ALC_CMC.2.3d The developer shall use a CM system.
ALC_CMC.2.1c The TOE shall be labelled with its unique reference.
ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.
ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e 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 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e 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 analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.
AVA_VAN.2.1c The TOE shall be suitable for testing.
AVA_VAN.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

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

6.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in Table 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. The TOE can be configured to use an IPSEC VPN to communicate with the external SYSLOG server, ensuring that audit records are protected from disclosure and modification. The TOE can be further configured so that that SYSLOG server is on a dedicated VLAN to help protect exported audit records for disclosure or modification. This necessarily requires that the dedicated VLAN be used for this dedicated purpose in the operational environment.

When configured to export audit records, when the TOE finds that 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 that an administrator can become aware of, and remedy, the situation.

When configured to store audit records locally, the TOE can be configured to basically suspend operations should the internal log run out of space allowing only a Security Administrator to log in and remedy the situation (e.g., clear the log) so that the TOE can resume normal operations. When that occurs, the TOE could potentially lose any audit records not committed to the log (i.e., those buffered in internal memory) but it would not lose records already in the log.

The internal log can be accessed only by a Security Administrator, who can review, delete (but not modify), or archive stored audit records using available CLI commands specifically designed for the management of the internal LOG. The functions available to review audit records allow the audit records to be sorted in forward or reverse order according to date/time and to be searched using regular expressions.

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_SAR.1: The internal log can be fully reviewed by a Security Administrator.
- FAU_SAR.3: The available log review tools support sorting and searching. Sorting is based on time/date and searching is based on any attributes or ranges thereof using regular expressions.
- FAU_STG.1: Audit records in the internal log can be deleted only by a Security Administrator and are not otherwise subject to modification.
- FAU_STG.4: The TOE can be configured so that it will stop performing auditable actions once the internal log has exhausted its available storage space and the only audit records subject to loss are those that happen to be buffered in memory when the space becomes exhausted.. This can be remedied by a Security Administrator.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server and can be configured to use an IPSEC VPN for communication with the SYSLOG server.
- FAU_STG_EXT.3: The TOE will issue an SNMP trap to a configured SNMP server when it discovers the configured external SYSLOG server is not responding.

6.2 Cryptographic support

The TOE includes a FIPS 140-2 certified cryptomodule (Certificate #1910) 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 800-56A NIST Special Publication 800-56B	NA
• Random number generation	ANSI X9.80	NA
Encryption/Decryption		
• AES ECB and CBC (128-256 bits)	FIPS PUB 197 NIST SP 800-38A	AES Cert #1927
Cryptographic signature services		
• Digital Signature Algorithm (DSA) (modulus 1024)	FIPS PUB 186-2	DSA Cert #611
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-2	RSA Cert #993
Cryptographic hashing		
• SHA-1 and SHA-256 (digest sizes 160 and 256 bits)	FIPS Pub 180-3	SHS Cert #1692
Keyed-hash message authentication		
• HMAC-SHA-1 (digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	HMAC Cert #1161
Random bit generation		
• RBG 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 #1014

The TOE is able to generate asymmetric key pairs with modulus 2048 bits which is equivalent to a symmetric key strength of 112 bits. The RSA asymmetric key generation ability has not been covered by FIPS testing; however, it is allowed for use in FIPS mode provided it is used with 80 or 112 bits of encryption strength. In the evaluated configuration it must be used with 112 bits.

Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. This function has also been subject to FIPS 140 certification.

These supporting cryptographic functions are included to support the IPSEC (RFC 4304), IKEv1 (RFCs 2407, 2408, 2409, and 4109), SSHv2 (RFCs 4251, 4252, 4253, and 4254), and SNMPv3 (based on AES-128) secure communication protocols.

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). SSHv2 connections are rekeyed prior to reaching 228 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 supports IPSec to form VPN connections with peer network devices using the ESP protocol and AES-CBC-128 or AES-CBC-256 and using IKEv1 (including DH Group 14 with a modulus of 2048 and peer authentication using rDSA). IKEv1 Phase 1 exchanges use only main mode and SA lifetimes are limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs. Phase 2 SAs can also be limited to no more than 100MB of network traffic. The TOE supports the configuration of pre-shared keys for the purpose of authenticating IPSec connections. Pre-shared keys can be between 8 and 128 characters in length and can be composed of any combination of upper and lower case letters, numbers and special characters including blank space and ~`!@#$%^&*()_+-={}|[]\:";'<>,./.

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_COMM_PROT_EXT.1: The TOE provides IPSEC and SSH in support of secure administrator session protection.
- 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/IKEv1 VPN connections as indicated above.
- 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. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

The TOE includes firewall functions that allow the definition of firewall rules, collectively known as access control lists (ACLs), that are applied to applicable network traffic as it is received and would pass through the TOE between connected networks. The ACLs can be *basic*, with matching criteria based only on source IP address, or *advanced*, with matching criteria based on source and destination addresses, protocols, and other header information. ACLs can also be defined independently for both IPv4 and IPv6 network traffic.

Basic ACLs define matching criteria in terms of source IPv4 or IPv6 addresses and a time range and support permit and deny operations.

Advanced ACLs define matching criteria in terms of source and destination IPv4 or IPv6 addresses, source and destination ports, protocol/transport layer, other header fields (ack, fin, psh, rst, syn, urg), whether the traffic is a fragment, ICMP type, time range, and VPN instance information and also support permit and deny operations.

In each case, ACL ordering can be selected by the Security Administrator to be either as configured (i.e., rules are processed in the order they are defined by the administrator) or automatic, in which case the rules are automatically sorted in a depth-first order so that the most specific matching criteria is applied first with some tie-breaking heuristics to resolve equal specificity.

Once ACLs are defined, the TOE will process all network traffic against the configured ACLs. The rules in the applicable ACLs are processed in the specified order until a match is encountered and the operation associated with that matching rule (permit or deny) will be enforced. If there is no match, the traffic will be denied by default.

In addition to the administrator-configured rules, there are a number of implicit rules that are always applied to ensure the validity of network traffic being processed:

- If the source address of the network traffic does not translate to an address on the network interface on which it was received it will be rejected.
- If the destination address of the network traffic does not translate to a network associated with an available network interface it will be rejected.
- If the source address of the network traffic is on a broadcast network it will be rejected.
- If the source address of the network traffic is on a loopback network it will be rejected.

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

- FDP_IFC.1: The TOE implements an unauthenticated security functional policy (i.e., firewall policy) that applies to all network traffic that would flow through the TOE between connected networks.
- FDP_IFF.1: The TOE provides a flexible set of firewall rules that can be employed to permit or deny network traffic that would flow through the TOE based on source and destination addresses, source and destination ports, transport layer, TOE interface (where networks are defined), and service (e.g., ports and other header information). These rules also serve to address network traffic validity issues ensuring that received traffic is defined on the interface that it arrives and also that broadcast and loopback networks are not valid source networks for passing traffic through the TOE.
- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects.

6.4 Identification and authentication

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

In the evaluated configuration, users can connect to the TOE via a local console or remotely using SSHv2 or SNMPv3. In each case, the user is required to log in prior to successfully establishing a session through which TOE functions can be exercised.

The only other form of authentication associated with the TOE is that required to establish IPSEC/IKEv1 VPNs. In all cases, authentication functions occur within cryptographically protected network traffic and as such are inherently protected from potential replay or reuse of the authentication data.

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. Once a locally defined user logs in, they can optionally provide RSA credentials (i.e., their public key) that the TOE will store for use with subsequent SSH credential based authentication. 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, if a user's password has been expired by the TOE, the user will be required to both provide their current expire password and also provide a new password that is acceptable to the TOE. This results in a password

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

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

If a user fails to log in an administrator configured number of times in a row, the user (unless the user identity is not defined) is added to a blacklist and is subject to the following configurable results:

- The user is prohibited from logging in until removed from a black list.
- The user can continue to try to log in and is removed from the blacklist if successful or the blacklist entry times out (after one minute).
- The user is prohibited from logging in for a configurable period of time, allowing the user to log in again after that time has lapsed or the user has been removed from the black list (i.e., by an administrator).

In order to ensure that passwords are changed periodically, an administrator can configure a maximum password lifetime for locally defined users. Additionally, an administrator can define a value which identifies the number of times a user can log in with an expired password before the password has to be changed. The password lifetime is checked each time a user logs in and if the configured lifetime is expired, the user is notified that the password has expired. The configured value allowing the use of expired passwords is also checked and if that value has been exceeded the user is required to change their password immediately. Note that the TOE can also be configured with a minimum password update interval to similarly ensure that passwords are not changed too frequently.

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 configured minimum password length and, if configured, the new password cannot match any of the passwords retained within the scope of the configured history.

Administrators have even more control over password composition using configurable complexity checking. First, the number (1 through 4) of categories (upper case letters, lower case letters, numbers, and special characters) can be configured. Next, the minimum number of characters in each of the required categories can also be configured. Finally, a password complexity feature can be enabled which ensures a password cannot contain the username or the reverse of the username and also that no character of the password is repeated three or more times consecutively.

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

- FIA_AFL.1: The administrator can configure a non-zero threshold for authentication failures that can occur before the TOE takes action to prevent subsequent authentication attempts. The TOE can be configured to disable the user until an administrator takes an explicit action to change that. However, the TOE offers other options (summarized above) for operational environments where that may not be necessary.
- FIA_ATD.1: Locally defined users are assigned identities, passwords, and privilege levels (i.e., roles).
- FIA_PMG_EXT.1: The TOE implements a rich set of password composition and aging constraints as described above.
- FIA_UAU.1: The TOE doesn't offer any services or access to its functions without requiring a user to be identified and authenticated.
- FIA_UAU.4: The TOE prevents reuse of authentication data by virtue of the cryptographic mechanism employed for administrator sessions and IPSec VPNs.
- FIA_UAU.6: The TOE requires re-authentication when changing passwords and unlocking locked sessions.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.5: 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.
- FIA_UID.2: 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: 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 command-line, web-based graphical user, and MIB interfaces each 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 TOE also offers the following functions, limited to the Security Administrator (i.e., System and Manage roles):

- Start-up and shutdown the TOE,
- Manage the firewall rules,
- Manage user account definitions,
- Manage the secure administration mechanisms (SSHv2, HTTPS, SNMPv3) and associated authentication,
- Manage password and logon constraints (e.g., failed logon threshold),
- Restoration of disabled users,
- Manage configuration of peer components (e.g., SYSLOG, RADIUS, and TACACS servers),
- Manage the internal clock,
- Manage the internal audit log,
- Backup and restore the TOE data and configuration,
- Enable/disable secure remote administration, and
- Manage locations (e.g., specify allowed IP addresses) from which external administration can occur.

The TOE imposes a restrictive default behavior in regard to its firewall policy by virtue of the fact that if there are no matching rules, the traffic is dropped. This default behavior can in effect be modified by a Security Administrator by defining one or more firewall rules that would serve to match all network traffic that might be received by the TOE.

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

- FMT_MOF.1: The TOE restricts the access to manage the TOE security functions to Security Administrators (i.e., System and Manage roles).
- FMT_MSA.3: The TOE implements a restrictive default firewall policy by dropping network traffic when there are no matching rules. Only a Security Administrator (i.e., System and Manage roles) can change that by defining rules that are capable of matching and taking specifically configured actions for all network traffic the TOE might receive.
- 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 6.9, 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. Note that peer switches can be con figured to utilize IPSec connections to cryptographically protect communications between them.

Note that IRF groups are not considered peer switches in the IPSec (or VPN) sense. Rather IRF groups effectively form a logical instance of the TOE comprised of up to nine distinct A-Series 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 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 SHA512.

The TOE utilizes SSHv2 and SNMPv3 for secure communications. Each of these protocols 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 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, flash read, software checksum tests, and device detection tests. Furthermore, the TOE is designed to query each pluggable module which in turn includes its own diagnostics that will serve to help identify any failing modules. When operating in CC/FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self testing.

The TOE is designed to support upgrades to the boot ROM program and system boot file as well as to support software hotfixes. The TOE provides interfaces so that an administrator can query the current boot ROM program or system boot file versions as well as to identify any installed patches. Both the boot ROM program and system boot file can be upgraded via the Boot ROM menu or the command line interface, but a reboot is required in each case.

Hotfixes, which can affect only the system boot file, can be installed via the command line interface and do not require a reboot to become effective.

The TOE includes a validity checking function that can be enabled when upgrading the boot ROM program, while system boot files and software patches are always validated prior to installation. In each case, the upgrade version will be checked to ensure it is appropriate and the upgrade file will be verified using an embedded (HP authorized) digital signature verified against a configured pair of hard-coded keys embedded in the TOE. If the version is incorrect or the signature cannot be verified, the upgrade will not proceed to protect the integrity of the TOE.

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

- FPT_ITT.1(1): The only inter-TOE secure communications involve a dedicated link used for high-availability redundant or IRF configurations. The link is dedicated to this purpose and does not extend beyond the physical environment hosting the redundant components and hence serves to ensure data is not subject to disclosure or modification.
- FPT_ITT.1(2): The only inter-TOE secure communications involve a dedicated link used for high-availability redundant or IRF configurations. The link is dedicated to this purpose and does not extend beyond the physical environment hosting the redundant components and hence serves to ensure data is not subject to disclosure or modification.
- FPT_PTD.1(1): The TOE does not offer any functions that will disclose to any user a plain text password.
- FPT_PTD.1(2): The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_RPL.1: The TOE rejects network traffic replays automatically in the context of SSHv2, HTTPS, and SNMPv3 secure communication channels.
- FPT_STM.1: The TOE includes its own hardware clock.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.
- FPT_TUD_EXT.1: The TOE provides functions to query and upgrade the versions of the boot ROM program and system boot file (including installing hotfixes). Digital signatures are used to ensure the integrity of each upgrade prior to performing the upgrade; this checking is optional for the boot ROM program since special circumstances might require those checks to be disabled.

6.7 Resource utilisation

The TOE is designed so that sessions available via the SSH interface, as well as the memory and CPU resources available to those sessions can be limited. Normally, each user is limited to a single administrative session and all sessions have a predefined memory and CPU usage threshold.

When memory usage reaches the defined threshold, the Comware memory manager will notify the offending task to free memory to ensure administrator always can get memory resources.

Similarly, Comware is a non-preemptive system and each task has its own limited and scheduled CPU time slice. This ensures the administrator tasks can always get CPU resources.

The Resource utilisation function is designed to satisfy the following security functional requirements:

- FRU_RSA.1: The TOE limits the number of interactive user sessions and administrator can have at any given time and also the memory and CPU resources available to each of those sessions.

6.8 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 displayed 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.

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 locked. Once locked, the TOE will not interact with the console display or accept console inputs except to re-authenticate the user that was locked. The user will be required to re-enter their user id and their password so they can be reauthenticated. 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_EXT.1: The TOE locks local sessions that have been inactive for an administrator-configured period of time. Locked sessions are disconnected from the local console input/output functions and can be reconnected only if the locked user correctly reenters their user id and password in order to be reauthenticated.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE.

6.9 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 an IPSEC VPN for this purpose. Of course, the SYSLOG server would need to be similarly configured to use the IPSEC VPN in the operational environment.

Note that other remote peers, such as SNMP, RADIUS, and TACACS servers, could also be configured to use IPSEC VPNs if deemed necessary in a given operational environment.

To support secure remote administration, the TOE includes implementations of SSHv2 and SNMPv3. 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. Note that 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 SNMPv3, the TOE acts as an SNMP server accepting non-interactive Management Information Base (MIB) options from an authenticated source. SNMPv3 requires the client to be authenticated against a locally configured user base and utilizes AES-128 in order to protect this security management channel.

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 cryptomodule included in the TOE implementation.

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

- FTP_ITC.1(1): The TOE can be configured to use a IPSEC VPNs to ensure that exported audit records are not subject to inappropriate disclosure or modification. Note that there are no applicable TOE-to-peer authentication functions, other than those addressed by the FTP_TRP.1 requirements, but IPSEC VPNs can be configured for essentially any network peers.
- FTP_ITC.1(2): The TOE can be configured to use a IPSEC VPNs to ensure that exported audit records are not subject to inappropriate disclosure or modification. Note that there are no applicable TOE-to-peer authentication functions, other than those addressed by the FTP_TRP.1 requirements, but IPSEC VPNs can be configured for essentially any network peers.
- FTP_TRP.1(1): The TOE provides SSH, based on its embedded cryptomodule, to support secure remote administration. Furthermore, the TOE supports SNMPv3 for secure remote non-interactive remote administration functions. In each case, the administrator can initiate the remote session, the remote session 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.
- FTP_TRP.1(2): The TOE provides SSH, based on its embedded cryptomodule, to support secure remote administration. Furthermore, the TOE supports SNMPv3 for secure remote non-interactive remote administration functions. In each case, the administrator can initiate the remote session, the remote session 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 *U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007* (TFFWPP).

The TOE includes Ethernet switch devices that include security blades (modules) that introduce firewall security functions. As such, the TOE is both a network device and a traffic filter firewall.

As explained in section 3, Security Problem Definition, the Security Problem Definitions of both the TFFWPP and NDPP have been copied verbatim into distinct subsections in this ST. The statements are generally complimentary and are not contradictory.

As explained in section 4, Security Objectives, the Security Objectives of both the TFFWPP and NDPP have been copied verbatim into distinct subsections in this ST. Again, the statements are generally complimentary and are not contradictory.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the NDPP, TFFWPP, or both. The SFRs from both PPs have been copied verbatim from those PPs, except as follows.

There are only 5 requirements that intersect and they have been combined appropriately.

- FAU_GEN.1 – The auditable events from both PPS have been combined to form a superset of auditable events satisfying both PPs.
- FCS_COP.1(1) – FCS_COP.1(1) from the NDPP maps directly to FCS_COP.1 from the TFFWPP, both serving to define requirements for AES encryption and the single instance in this ST satisfies both PPs.
- FDP_RIP.2 – While the TFFWPP requires only FDP_RIP.1, the NDPP requires FDP_RIP.2 which is hierarchical to and hence satisfies both PPs.
- FMT_SMR.1 – The TFFWPP requires a single ‘authorized administrator’ role while the NDPP requires a single ‘security administrator’ role. This ST is using ‘security administrator’ to represent both and hence satisfies both PPs.
- FPT_STM.1 – This SFR is identical in both PPs and hence both PPs are satisfied by a single instance in this ST.

Note that this ST does not conform to the NDPP since it does not always use cryptographic mechanisms to protect communication between its distributed parts (e.g., in a high-availability configuration) and it does not include the explicit assurance activities defined in the NDPP.

Requirement Class	Requirement Component	PP Source - Notes
FAU: Security audit	FAU_GEN.1: Audit Data Generation	Both – Combined
	FAU_GEN.2: User identity association	NDPP
	FAU_SAR.1: Audit review	TFFWPP
	FAU_SAR.3: Selectable audit review	TFFWPP
	FAU_STG.1: Protected audit trail storage	TFFWPP
	FAU_STG.4: Prevention of audit data loss	TFFWPP
	FAU_STG_EXT.1: External Audit Trail Storage	NDPP
	FAU_STG_EXT.3: Action in case of Loss of Audit Server Connectivity	NDPP
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)	NDPP
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	NDPP
	FCS_COMM_PROT_EXT.1: Communications Protection	NDPP
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)	Both – FCS_COP.1 in the TFFWPP maps directly to

Requirement Class	Requirement Component	PP Source - Notes
		FCS_COP.1(1) in the 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_IFC.1: Subset information flow control	TFFWPP
	FDP_IFF.1: Simple security attributes	TFFWPP
	FDP_RIP.2: Full Residual Information Protection	Both – FDP_RIP.1 in the TFFWPP has been augmented to FDP_RIP.2 in the NDPP
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling	TFFWPP
	FIA_ATD.1: User attribute definition	TFFWPP
	FIA_PMG_EXT.1: Password Management	NDPP
	FIA_UAU.1: Timing of authentication	TFFWPP
	FIA_UAU.4: Single-use authentication mechanisms	TFFWPP
	FIA_UAU.6: Re-authenticating	NDPP
	FIA_UAU.7: Protected Authentication Feedback	NDPP
	FIA_UAU_EXT.5: Extended: Password-based Authentication Mechanism	NDPP
	FIA_UIA_EXT.1: User Identification and Authentication	NDPP
	FIA_UID.2: User identification before any action	TFFWPP
FMT: Security management	FMT_MOF.1: Management of security functions behavior	TFFWPP
	FMT_MSA.3: Static attribute initialization	TFFWPP
	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	Both – Consolidated the TFFWPP and NDPP role terminology
FPT: Protection of the TSF	FPT_ITT.1(1): Basic Internal TSF Data Transfer Protection (Disclosure)	CC – see above
	FPT_ITT.1(2): Basic Internal TSF Data Transfer Protection (Modification)	CC – see above
	FPT_PTD.1(1): Management of TSF Data (for reading of authentication data)	NDPP
	FPT_PTD.1(2): Management of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_RPL.1: Replay Detection	NDPP
	FPT_STM.1: Reliable Time Stamps	Both
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FRU: Resource utilisation	FRU_RSA.1: Maximum Quotas	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP

Requirement Class	Requirement Component	PP Source - Notes
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (Prevention of Disclosure)	NDPP
	FTP_ITC.1(2): Inter-TSF Trusted Channel (Detection of Modification)	NDPP
	FTP_TRP.1(1): Trusted Path	NDPP
	FTP_TRP.1(2): Trusted Path	NDPP

Table 5 SFR Protection Profile Sources and Notes

8. Rationale

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

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

8.1 Security Objectives Rationale

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

Note that the rationale for the objectives from the NDPP and TFFWPP have been presented separately since the Security Problem Definitions and Security Objectives have also been presented separately earlier in this ST.

8.1.1 NDPP Security Objectives Rationale for the TOE and Environment

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

	P.ACCESS_BANNER	T.ADMIN_ERROR	T.RESOURCE_EXHAUSTION	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.RESOURCE_AVAILABILITY			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 6 NDPP Environment to Objective Correspondence

8.1.1.1 P.ACCESS_BANNER

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

This Organizational Policy is satisfied by ensuring that:

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

8.1.1.2 T.ADMIN_ERROR

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

This Threat is satisfied by ensuring that:

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

8.1.1.3 T.RESOURCE_EXHAUSTION

A process or user may deny access to TOE services by exhausting critical resources on the TOE.

This Threat is satisfied by ensuring that:

- O.RESOURCE_AVAILABILITY: To reduce the potential that critical resources might be unavailable, the TOE is expected to implement mechanisms that serve to mitigate the potential for exhaustion of critical resources.

8.1.1.4 T.TSF_FAILURE

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

This Threat is satisfied by ensuring that:

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

8.1.1.5 T.UNAUTHORIZED_ACCESS

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

This Threat is satisfied by ensuring that:

- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its communication channels.
- O.SESSION_LOCK: To reduce the potential for unauthorized access to TOE security functions and data, the TOE is expected to lock or terminate unattended or inactive sessions.
- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events and export those logs to an external log server.
- O.TOE_ADMINISTRATION: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only presumably authorized administrators can log in and access security management functions.

8.1.1.6 T.UNAUTHORIZED_UPDATE

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

This Threat is satisfied by ensuring that:

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

8.1.1.7 T.UNDETECTED_ACTIONS

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

This Threat is satisfied by ensuring that:

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

8.1.1.8 T.USER_DATA_REUSE

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

This Threat is satisfied by ensuring that:

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

8.1.1.9 A.NO_GENERAL_PURPOSE

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

This Assumption is satisfied by ensuring that:

- OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

8.1.1.10 A.PHYSICAL

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

This Assumption is satisfied by ensuring that:

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

8.1.1.11 A.TRUSTED_ADMIN

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

This Assumption is satisfied by ensuring that:

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

8.1.2 TFFWPP 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. Since the Security Problem Definition and Security Objectives have been adopted verbatim from the TFFWPP, the correspondence and rationale below have likewise been adopted from the TFFWPP.

	T.ASPOOF	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAUTH	T.OLDINF	T.PROCOM	T.REPEAT	T.REPLAY	T.SELPRO	T.TUSAGE	A.DIRECT	A.GENPUR	A.LOWEXP	A.NOEVIL	A.NOREMO	A.PHYSEC	A.PUBLIC	A.REMACC	A.SINGEN
O.ACCOUN		X																		
O.AUDREC		X																		
O.ENCRYP					X		X													
O.IDAUTH					X															
O.LIMEXT					X															
O.MEDIAT	X			X		X														
O.SECFUN			X		X				X											
O.SECSTA					X					X										
O.SELPRO			X							X										
O.SINUSE								X	X											
OE.ADMTRA											X									
OE.DIRECT												X								
OE.GENPUR													X							
OE.GUIDAN											X									
OE.LOWEXP														X						
OE.NOEVIL															X					
OE.NOREMO																X				
OE.PHYSEC																	X			
OE.PUBLIC																		X		
OE.REMACC																			X	
OE.SINGEN																				X

Table 7 TFFWPP Environment to Objective Correspondence

8.1.2.1 T.ASPOOF

An unauthorized person may carry out spoofing in which information flow through the TOE into a connected network by using a spoofed source address.

This Threat is satisfied by ensuring that:

- O.MEDIAT: This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

8.1.2.2 T.AUDACC

Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

This Threat is satisfied by ensuring that:

- O.ACCOUN: This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and that authorized administrators are accountable for the use of security functions related to audit.

- O.AUDREC: This security objective is necessary to counter the threat: T.AUDACC by requiring a readable audit trail and a means to search and sort the information contained in the audit trail.

8.1.2.3 T.AUDFUL

An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

This Threat is satisfied by ensuring that:

- O.SECFUN: This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.
- O.SELPRO: This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

8.1.2.4 T.MEDIAT

An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

This Threat is satisfied by ensuring that:

- O.MEDIAT: This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

8.1.2.5 T.NOAUTH

An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

This Threat is satisfied by ensuring that:

- O.ENCRYP: This security objective is necessary to counter the threats: T.NOAUTH and T.PROCOM by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.
- O.IDAUTH: This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
- O.LIMEXT: This security objective is necessary to counter the threat: T.NOAUTH because it requires that the TOE provide the means for an authorized administrator to control and limit access to TOE security functions.
- O.SECFUN: This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.
- O.SECSTA: This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.

8.1.2.6 T.OLDINF

Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

This Threat is satisfied by ensuring that:

- O.MEDIAT: This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF which have to do with getting impermissible information to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted.

8.1.2.7 T.PROCOM

An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

This Threat is satisfied by ensuring that:

- O.ENCRYP: This security objective is necessary to counter the threats: T.NOAUTH and T.PROCOM by requiring that an authorized administrator use encryption when performing administrative functions on the TOE remotely.

8.1.2.8 T.REPEAT

An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.

This Threat is satisfied by ensuring that:

- O.SINUSE: This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

8.1.2.9 T.REPLAY

An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.

This Threat is satisfied by ensuring that:

- O.SECFUN: This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL by requiring that the TOE provide functionality that ensures that only the authorized administrator has access to the TOE security functions.
- O.SINUSE: This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.

8.1.2.10 T.SELPRO

An unauthorized person may read, modify, or destroy security critical TOE configuration data.

This Threat is satisfied by ensuring that:

- O.SECSTA: This security objective ensures that no information is comprised by the TOE upon start-up or recovery and thus counters the threats: T.NOAUTH and T.SELPRO.
- O.SELPRO: This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.

8.1.2.11 T.TUSAGE

The TOE may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons.

This Threat is satisfied by ensuring that:

- OE.ADMTRA: This non-IT security objective is necessary to counter the threat: T.TUSAGE because it ensures that authorized administrators receive the proper training.
- OE.GUIDAN: This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.

8.1.2.12 A.DIRECT

Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

This Assumption is satisfied by ensuring that:

- OE.DIRECT: Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

8.1.2.13 A.GENPUR

There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

This Assumption is satisfied by ensuring that:

- OE.GENPUR: There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

8.1.2.14 A.LOWEXP

The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

This Assumption is satisfied by ensuring that:

- OE.LOWEXP: The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

8.1.2.15 A.NOEVIL

Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

8.1.2.16 A.NOREMO

Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

This Assumption is satisfied by ensuring that:

- OE.NOREMO: Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.

8.1.2.17 A.PHYSEC

The TOE is physically secure.

This Assumption is satisfied by ensuring that:

- OE.PHYSEC: The TOE is physically secure.

8.1.2.18 A.PUBLIC

The TOE does not host public data.

This Assumption is satisfied by ensuring that:

- OE.PUBLIC: The TOE does not host public data.

8.1.2.19 A.REMACC

Authorized administrators may access the TOE remotely from the internal and external networks.

This Assumption is satisfied by ensuring that:

- OE.REMACC: Authorized administrators may access the TOE remotely from the internal and external networks.

8.1.2.20 A.SINGEN

Information can not flow among the internal and external networks unless it passes through the TOE.

This Assumption is satisfied by ensuring that:

- OE.SINGEN: Information can not flow among the internal and external networks unless it passes through the TOE.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that the subsequent tables in this section identify the requirements that effectively satisfy the individual objectives.

Note that the rationale for the requirements from the NDPP and TFFWPP have been presented separately since the Security Objectives have also been presented separately earlier in this ST. The requirements in each case have been adjusted based on the final SFRS in this ST.

8.2.1 NDPP Security Functional Requirements Rationale

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

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	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			
FAU_STG_EXT.3		X				X			
FCS_CKM.1		X							
FCS_CKM_EXT.4		X							
FCS_COMM_PROT_EXT.1		X							

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.RESOURCE_AVAILABILITY	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
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.6							X		
FIA_UAU.7							X		
FIA_UAU_EXT.5							X		
FIA_UIA_EXT.1							X		
FMT_MTD.1							X		
FMT_SMF.1							X		
FMT_SMR.1							X		
FPT_ITT.1(1)		X							
FPT_ITT.1(2)		X							
FPT_PTD.1(1)							X		
FPT_PTD.1(2)		X							
FPT_RPL.1		X							
FPT_STM.1						X			
FPT_TST_EXT.1								X	
FPT_TUD_EXT.1									X
FRU_RSA.1				X					
FTA_SSL.3					X		X		
FTA_SSL_EXT.1					X		X		
FTA_TAB.1	X								
FTP_ITC.1(1)		X							
FTP_ITC.1(2)		X							
FTP_TRP.1(1)		X							
FTP_TRP.1(2)		X							

Table 8 NDPP Objective to Requirement Correspondence

8.2.1.1 O.DISPLAY_BANNER

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

This TOE Security Objective is satisfied by ensuring that:

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

8.2.1.2 O.PROTECTED_COMMUNICATIONS

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG_EXT.3: The TOE is required to be able to detect when its audit server is not available and take an appropriate action.
- 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_COMM_PROT_EXT.1: The TOE is required to implement SSH or IPSEC and optionally TLS to protect its network communication channels.
- 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 network communication channels.
- 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_ITT.1(1): The TOE is required to protect communication between its distributed parts from disclosure and modification.
- FPT_ITT.1(2): The TOE is required to protect communication between its distributed parts from disclosure and modification.
- FPT_PTD.1(2): The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as cryptographic keys.
- FPT_RPL.1: The TOE is required to prevent the replay of data to ensure that data cannot be collected and reused at some later time to benefit an attacker.
- FTP_ITC.1(1): The TOE is required to protect communication between itself and its external peers from disclosure and modification.
- FTP_ITC.1(2): The TOE is required to protect communication between itself and its external peers from disclosure and modification.
- FTP_TRP.1(1): The TOE is required to protect communication between itself and its administrators from disclosure and modification.
- FTP_TRP.1(2): The TOE is required to protect communication between itself and its administrators from disclosure and modification.

8.2.1.3 O.RESIDUAL_INFORMATION_CLEARING

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

This TOE Security Objective is satisfied by ensuring that:

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

8.2.1.4 O.RESOURCE_AVAILABILITY

The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).

This TOE Security Objective is satisfied by ensuring that:

- FRU_RSA.1: The TOE is required to enforce resource quotas for defined resources to reduce the potential for critical resource exhaustion.

8.2.1.5 O.SESSION_LOCK

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

This TOE Security Objective is satisfied by ensuring that:

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

8.2.1.6 O.SYSTEM_MONITORING

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to be able to generate audit events for security relevant activities on the TOE.
- FAU_GEN.2: The TOE is required to associate audit events to users to ensure proper accountability.
- FAU_STG_EXT.1: The TOE is required to be able to export audit records to an external audit server via a secure channel to protect the integrity and security of those records.
- FAU_STG_EXT.3: The TOE is required to detect when the external audit server is not available and take an appropriate action.
- FPT_STM.1: The TOE is required to generate reliable time stamps to be used in its audit records for proper accounting.

8.2.1.7 O.TOE_ADMINISTRATION

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

This TOE Security Objective is satisfied by ensuring that:

- FIA_PMG_EXT.1: The TOE is required to implement mechanisms allowing an administrator to constrain the construction of passwords to encourage more secure (or harder to guess) passwords.
- FIA_UAU.6: The TOE is required to ensure that users must be re-authenticated in order to change their password to further ensure the user changing the password is authentic.
- 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.5: The TOE is required to implement a local authentication mechanism and can support additional authentication mechanisms.
- FIA_UIA_EXT.1: The TOE is required to ensure that users must be identified and authenticated in order to access functions, other than those specifically intended to be accessed without identification and authentication.
- FMT_MTD.1: The TOE is required to restrict access to security relevant data to administrators.
- FMT_SMF.1: The TOE is required to provide a minimum set of security functions to ensure the TOE security features can be properly managed.

- FMT_SMR.1: The TOE is required to implement a minimum of a Security Administrator role and can implement additional roles where necessary.
- FPT_PTD.1(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_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.

8.2.1.8 O.TSF_SELF_TEST

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

This TOE Security Objective is satisfied by ensuring that:

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

8.2.1.9 O.VERIFIABLE_UPDATES

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

This TOE Security Objective is satisfied by ensuring that:

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

8.2.2 TFFWPP 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. Since the Security Objectives have been adopted verbatim and the SFRs with only minor changes from the TFFWPP, the correspondence and rationale below have been adopted from the TFFWPP.

	O.ACCOUN	O.AUDREC	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE
FAU_GEN.1	X	X								
FAU_SAR.1		X								
FAU_SAR.3		X								
FAU_STG.1							X		X	
FAU_STG.4							X		X	
FCS_COP.1 (1)			X							
FDP_IFC.1						X				
FDP_IFF.1						X				
FDP_RIP.1						X				
FIA_AFL.1									X	
FIA_ATD.1				X						X

	O.ACCOUN	O.AUDREC	O.ENCRYP	O.IDAUTH	O.LIMEXT	O.MEDIAT	O.SECFUN	O.SECSTA	O.SELPRO	O.SINUSE
FIA_UAU.1				X						X
FIA_UAU.4										X
FIA_UID.2	X			X						
FMT_MOF.1					X		X	X		
FMT_MSA.3						X	X	X		
FMT_SMR.1							X			
FPT_STM.1		X								
ADV_ARC.1									X	

Table 9 TFFWPP Objective to Requirement Correspondence

8.2.2.1 O.ACCOUN

The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
- FIA_UID.2: This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

8.2.2.2 O.AUDREC

The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
- FAU_SAR.1: This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.
- FAU_SAR.3: This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
- FPT_STM.1: FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

8.2.2.3 O.ENCRYP

The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

This TOE Security Objective is satisfied by ensuring that:

- FCS_COP.1(1): This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.

8.2.2.4 O.IDAUTH

The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
- FIA_UAU.1: This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
- FIA_UID.2: This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

8.2.2.5 O.LIMEXT

The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.

8.2.2.6 O.MEDIAT

The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.1: This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FDP_IFF.1: This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FDP_RIP.2: This component ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.
- FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

8.2.2.7 O.SECFUN

The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.1: This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

- FAU_STG.4: This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
- FMT_MOF.1: This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.
- FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.
- FMT_SMR.1: Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

8.2.2.8 O.SECSTA

Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN, O.LIMEXT, and O.SECSTA.
- FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA, and O.SECFUN.

8.2.2.9 O.SELPRO

The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.1: This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
- FAU_STG.4: This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
- FIA_AFL.1: This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some administrator-configured number of failures, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

8.2.2.10 O.SINUSE

The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

- FIA_UAU.1: This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
- FIA_UAU.4: This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: O.SINUSE.

8.3 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs), which correspond to EAL2 augmented with ALF_FLR.2, in this ST have been adopted from the TFFWPP. They represent a superset of the SARs identified in the NDPP.

Note that 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 with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. As explained in the TFFWPP, FMT_MOF.1 addresses that dependency by restricting the ability to manage the information flow policies settings.

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_UID.2 and FIA_UIA_EXT.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FAU_STG_EXT.3	FAU_STG_EXT.1	FAU_STG_EXT.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_COMM_PROT_EXT.1	(FCS_IPSEC_EXT.1 or FCS_SSH_EXT.1 or FCS_TLS_EXT.1)	FCS_IPSEC_EXT.1 and FCS_SSH_EXT.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_IFC.1	FDP_IFF.1	FDP_IFF.1

ST Requirement	CC Dependencies	ST Dependencies
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 and FMT_MSA.3
FDP_RIP.2	none	none
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	none	none
FIA_PMG_EXT.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.4	none	none
FIA_UAU.6	none	none
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.5	none	none
FIA_UIA_EXT.1	none	none
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	FMT_SMR.1 and FMT_MSA.1	FMT_SMR.1 and FMT_MOF.1 (see above)
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2 and FIA_UIA_EXT.1
FPT_ITT.1(1)	none	none
FPT_ITT.1(2)	none	none
FPT_PTD.1(1)	none	none
FPT_PTD.1(2)	none	none
FPT_RPL.1	none	none
FPT_STM.1	none	none
FPT_TST_EXT.1	none	none
FPT_TUD_EXT.1	none	none
FRU_RSA.1	none	none
FTA_SSL.3	none	none
FTA_SSL_EXT.1	none	none
FTA_TAB.1	none	none
FTP_ITC.1(1)	none	none
FTP_ITC.1(2)	none	none
FTP_TRP.1(1)	none	none
FTP_TRP.1(2)	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 10 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 11 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	Resource utilisation	TOE access	Trusted path/channels
FAU_GEN.1	X								
FAU_GEN.2	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FAU_STG.1	X								
FAU_STG.4	X								
FAU_STG_EXT.1	X								
FAU_STG_EXT.3	X								
FCS_CKM.1		X							
FCS_CKM_EXT.4		X							
FCS_COMM_PROT_EXT.1		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_IFC.1			X						
FDP_IFF.1			X						
FDP_RIP.2			X						
FIA_AFL.1				X					
FIA_ATD.1				X					
FIA_PMG_EXT.1				X					
FIA_UAU.1				X					
FIA_UAU.4				X					
FIA_UAU.6				X					
FIA_UAU.7				X					
FIA_UAU_EXT.5				X					

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	Resource utilisation	TOE access	Trusted path/channels
FIA_UIA_EXT.1				X					
FIA_UID.2				X					
FMT_MOF.1					X				
FMT_MSA.3					X				
FMT_MTD.1					X				
FMT_SMF.1					X				
FMT_SMR.1					X				
FPT_ITT.1(1)						X			
FPT_ITT.1(2)						X			
FPT_PTD.1(1)						X			
FPT_PTD.1(2)						X			
FPT_RPL.1						X			
FPT_STM.1						X			
FPT_TST_EXT.1						X			
FPT_TUD_EXT.1						X			
FRU_RSA.1							X		
FTA_SSL.3								X	
FTA_SSL_EXT.1								X	
FTA_TAB.1								X	
FTP_ITC.1(1)									X
FTP_ITC.1(2)									X
FTP_TRP.1(1)									X
FTP_TRP.1(2)									X

Table 11 Security Functions vs. Requirements Mapping