NETSCOUT SYSTEMS, INC.

nGenius® 3900 Series Packet Flow Switch with Software Version 3.3.40

Security Target

Version 1.0

April 28, 2016

Prepared for:

NETSCOUT SYSTEMS, INC.
310 Littleton Road
Westford, MA 01886-4105

Prepared By:

Ward Rosenberry

Rosenberry Associates Inc.
30 Newfield Street
N. Chelmsford, MA 01863

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the nGenius® 3900 Series Packet Flow Switch

This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
0.1	August 12, 2013 Initial Release
0.2	October 25, Address inputs from initial release.
0.3	November 12, Address NETSCOUT PFS 3900_OR_1.0
0.4	November 26, 2013 Address follow up comments.
0.5	August 12, 2014, Prepare for Submission
0.6	October 30, 2014, Respond to OR 383-4-281 OR 0.5v1.
0.6B	Remove 3912 and external authentication.
0.7	July 16, 2015, Realign with TOE modifications.
0.8	August 11, 2015, Exclude use of TLS v1.0.
0.8A	August 12, 2015. Remove Linux client support.
08.B	August 28, 2015, Realign with TOE modifications.
08.C	October 30. Minor adjustments.
0.8D	November 4, 2015 Minor revision.
1.0	April 28, 2016. Final submission.

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

CC ..... **Common Criteria**
CLI ..... **Command Line Interface**
CSP ..... **Critical Security Parameter**
GB ..... **GigaByte**
GUI ..... **Graphical User Interface**
HTTPS ..... **HyperText Transfer Protocol over Secure Socket Layer**
I&A ..... **Identification and Authentication**
IP ..... **Internet Protocol**
IT ..... **Information Technology**
JRE ..... **Java Runtime Environment**
KVM ..... **Keyboard, Video, Mouse**
MAC ..... **Media Access Control**
MB ..... **MegaByte**
PFS ..... **Packet Flow Switch**
PP ..... **Protection Profile**
SFP ..... **Security Function Policy**
ST ..... **Security Target**
TCP ..... **Transmission Control Protocol**
TOE ..... **Target of Evaluation**
TSF ..... **TOE Security Function**
TSFI ..... **TSF Interface**
UDP ..... **User Datagram Protocol**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the NETSCOUT nGenius® 3900 Series Packet Flow Switch network switches.

1.1 Security Target Reference

NETSCOUT Systems, Inc. nGenius® 3900 Series Packet Flow Switch with software version 3.3.40 Security Target, Version 1.0, April 28, 2016.

1.2 TOE Reference

NETSCOUT nGenius® 3900 Series Packet Flow Switch with P-Blade and software version 3.3.40 build #32 and NETSCOUT nGenius® PFS Management Server with software version 3.3.40 build #32.

1.3 TOE type

The TOE type is Network Switch.

1.4 Conformance Claims

This TOE is conformant to the following CC specifications:

- Protection Profile for Network Devices (PP-ND), Version 1.1, June 8, 2012 including the Security Requirements for Network Devices Errata #3.
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

1.5 TOE Overview

1.5.1 TOE Description

The nGenius 3900 series switch features a high-performance processor. Distributed cut-through switching architecture delivers performance at scale and supports full-duplex throughput to address the most demanding, high traffic volume environments. The nGenius 3900 series packet flow switch supports up to 576 ports of 1/10 GbE or 48 ports of 40 GbE in a single chassis with intelligent traffic conditioning features on every port with sustained line rate performance, and ultra-low sustained latency port-to-port and across the switch fabric. These high-scale capacities enable network architects to consolidate the network monitoring fabric into fewer switches with less complexity. This reduces undesirable bandwidth bottlenecks and the unnecessary consumption of ports for inter-switch links, simplifies the monitoring architecture, and eases manageability and provisioning.

Leveraging a common interface module, nGenius 3900 series switches supports 1 GbE, 10 GbE and 40 GbE connectivity to enable flexible deployment from the network edge to core, as well as the attachment of diverse monitoring tools. A highly resilient switch architecture enables reliable operation in face of component failure, and facilitates in-service software upgrades and hot swapping of modules. In addition, the switches are manageable via nGenius PFS Management software which enables streamlined, centralized management of multi-switch deployments as well as the ability to provision multiple teams of users, where each team has unique authorization privileges to access and control PFS resources.

For single-switch deployments a Java client downloads from the switch to a client workstation.

Blade architecture allows easy expansion of capabilities. A single blade provides up to 24 RJ45 ports of 1 GbE and 10 GbE in a single (1U form factor) rack unit. FlexPort interfaces support 1 GbE, 10 GbE and 40 GbE interfaces on a single module.

The nGenius 3900 series switch is available in a one- and three-slot chassis.

- UCS 3901 (hereafter referred to as the 3901): A one-slot, 1U high, 19-inch rack mount unit containing a single blade, supporting up to 48 ports.
- UCS 3903 (hereafter referred to as the 3903): A three-slot, 3U high, 19-inch rack mount unit containing up to three blades, supporting up to 144 ports.

Figure 1 - 3900 Series PFS Deployment Options.

nGenius 3901R nGenius 3903

FlexPorts can be activated as 1 GbE connections using SFP transceivers, or 10 GbE connections using SFP+ transceivers. An additional group of specialized high-speed FlexPorts+ support either 4 Ports of 40 GbE or 16 ports of 10 GbE using a QSFP breakout cable. Medium type and speed of each port can be defined manually or may be auto-configured through detection of the connected transceiver module.

Gigabit Ethernet chassis in a 1U form factor with 20 RJ-45 ports individually configurable to 10/100/1000BaseT, four combo ports configurable to be 10/100/1000BaseT or 1000BaseX, and two dedicated 10G stacking ports. Combo ports support either copper or fiber and can be used on a one for one basis

The nGenius 3900 Series Packet Flow Switch supports any of three blade types (a P-blade, an S-blade, and O-blade), however, the TOE configuration is limited to the P-blade.

1.5.2 Usage and Major Security Features

nGenius® 3900 series packet flow switch is a highly extensible chassis-based, data center class network monitoring switch that enables scalable, high-capacity, highly available access to network traffic across distributed networks for use by any network monitoring, performance management and security system. Network architects are faced with the challenges of providing selective packet-flow access to an increasing number of task-specific management tools, overcoming interface speed mismatch issues, remaining within tool capacity limits, all while avoiding disruption to the monitored links. The nGenius 3900 series switch addresses all these challenges while addressing diverse deployment requirements, optimizing management tool investments, and simplifying end-to-end management and provisioning of the monitoring fabric.

The TOE is a standalone or stackable intelligent, modular, highly scalable network monitoring switch capable of line rate packet-flow aggregation, replication, load-balancing, and filtering.

To protect the integrity of these functions, the TOE provides the following security functionality:

Protected Communications – The TOE protects communications with administrators, between distributed TOE components, and with servers it uses in the environment.

Verifiable Updates – The TOE helps ensure that any updates to the TOE software can be verified by the administrator to be unaltered and (optionally) from a trusted source.

System Monitoring – The TOE generates audit data and sends those data to an external syslog server to avoid loss of audit data.

Secure TOE Administration – The TOE ensures that only administrators are able to log in and configure the TOE, and provides protections for logged-in administrators. The TOE also displays an advisory warning regarding use of the TOE.

Full Residual Information Clearing – The TOE ensures that any data contained in a protected resource (protected memory location) is not available when the resource is reallocated.

TOE Security Function Self-Test – The TOE performs self-tests on cryptographic algorithms and other security functions to ensure it is operating properly.

1.5.3 TOE Component Descriptions

1.5.3.1 nGenius 3900 Series Packet Flow Switch Chassis Deployments

The following diagram shows the 3900 Series Packet Flow Switch deployment. A single chassis (PFS 3901 or PFS 3903) includes an embedded management server for user administration and device configuration for blades in that chassis. The chassis provides power distribution for blades within the chassis.

For administering blades deployed in multiple chassis, a standalone dedicated PFS Management Server must be used for user administration and device configuration.

The switch includes built-in user account management. The figures illustrate secure remote administration channels, a directly connected local console for initial configuration using a KVM (keyboard, video, mouse device) or HyperTerminal, and a secure channel to a syslog server (required for audit event archiving).

Figure 2 - 3900 Series Single Chassis Deployment.

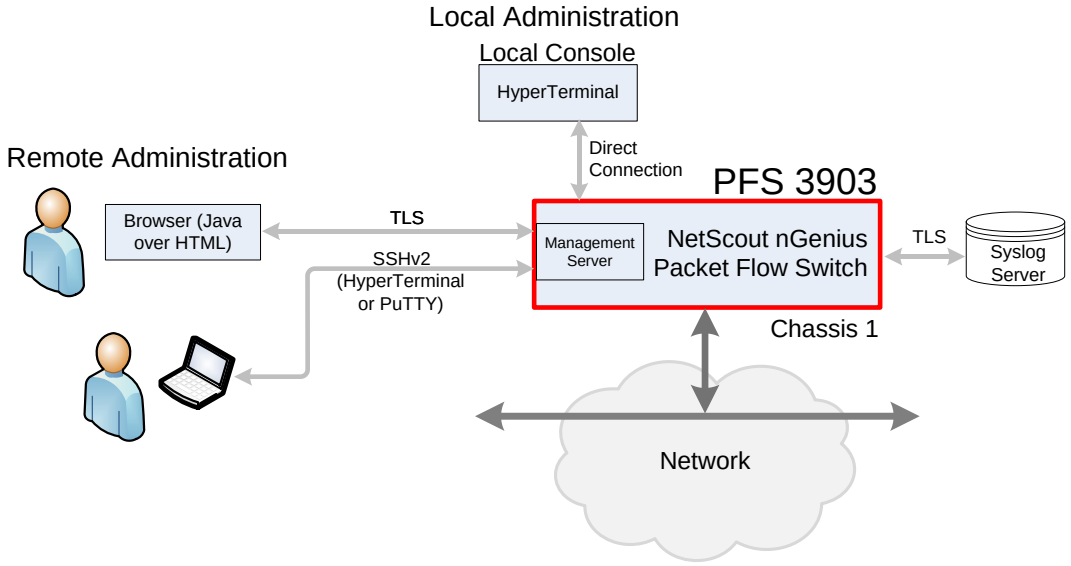
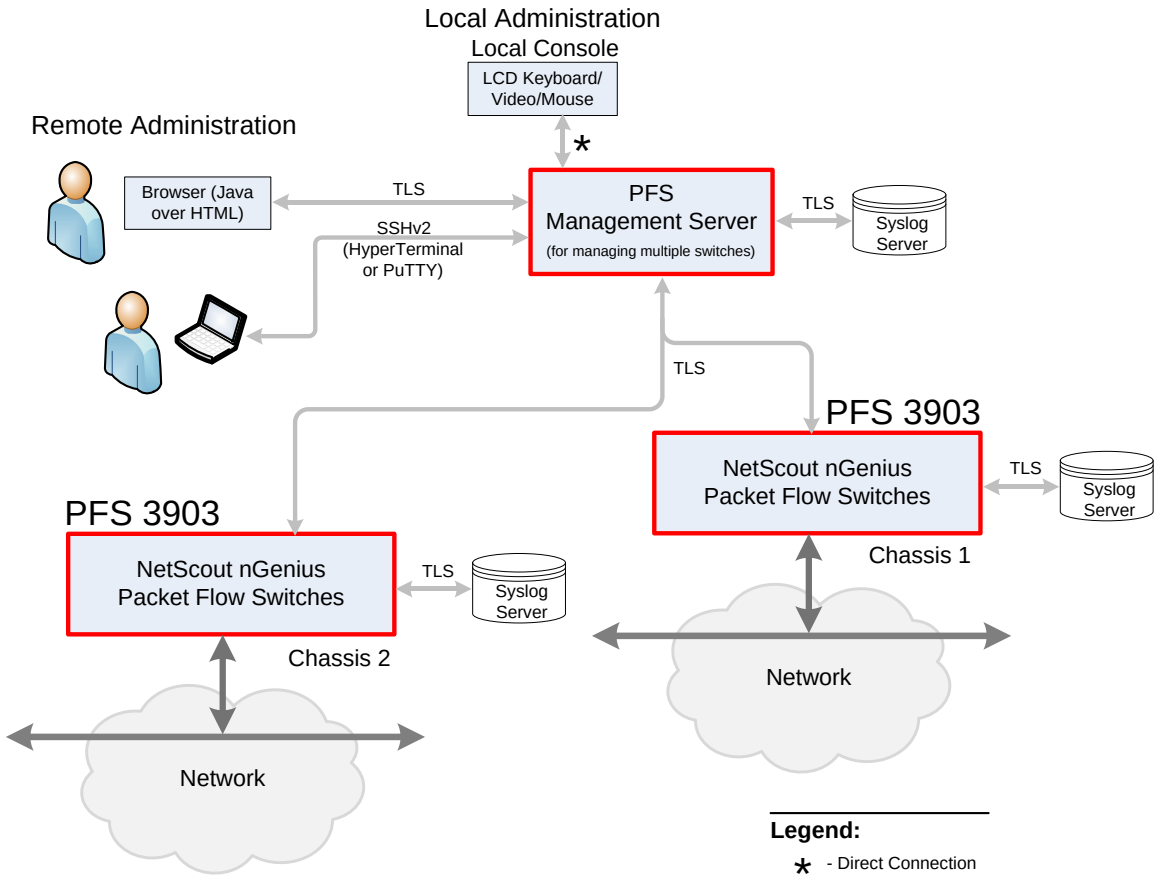


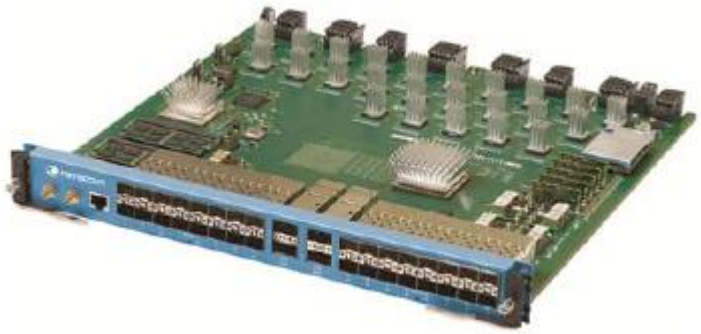
Figure 3 - 3900 Series Multi-Chassis Deployment.



1.5.4 nGenius PFS 3900 Packet-Blade Hardware and Software

The PFS 3900 Packet-Blade (also referred to as P-Blade) appliance is the basic packet flow switch used in the nGenius PFS 3901 and 3903 systems. The appliance hardware is custom built and contains nGenius PFS Management software running on a custom Linux distribution. One or more PFS 3900 P-Blade appliances are contained in one of the custom built chassis shown in Figure 1.

Figure 4 - PFS 3900 Packet (P)-Blade



1.5.5 nGenius PFS Management Server Hardware and Software

An nGenius PFS Management Server appliance (required to manage more than one chassis), is purchased as a rack-mountable appliance consisting of a Dell R-720 server platform with a Red Hat Enterprise Linux 6.2 operating system running nGenius PFS Management software version 3.3.40.

A KVM is supplied for initial configuration of the nGenius PFS Management Server.

1.6 Required Non-TOE Hardware/Software/Firmware

The TOE hardware includes a local console management interface and a remote management interface.

Use of the local console for initial configuration requires a KVM or standard PC with a serial port and a terminal program such as Hyper Terminal or PuTTY.

Use of the remote management interface (provided by the switch) requires a management client system that satisfies the following requirements:

Operating systems currently supported for use with the nGenius PFS management (java) client include:

- Microsoft Windows 7 SP2 (32 bit)
- Microsoft Windows 7 Professional (64 bit)
- Microsoft Windows XP SP3 (32 bit)
- Microsoft Windows XP SP2 (64 bit)

Web browsers supported for use with nGenius PFS Management client include:

- Microsoft Internet Explorer, versions 7, 8, and 9
- Mozilla Firefox version 38
- Google Chrome version 25

Java JRE versions currently supported for use with nGenius PFS Management client include:

- jre-8u45-windows-i586.exe (on Windows environments)

A KVM or a PC running HyperTerminal or PuTTY is required for local console access that is required for initial configuration.

The minimum requirements for the nGenius PFS Management client workstation are listed in the following table. It is assumed that a mouse and internal speaker are standard equipment.

Table 1 - Minimum Client System Hardware Requirements

PC Feature	nGenius PFS Management Client Workstation
Processor	866MHz Intel P3 or better
RAM	1GB or better
Hard drive free space required	40 GB or better
Ethernet Adapter	10/100 Gigabit
Screen Resolution (minimum)	1024 x 768, 256 color

Other required non-TOE hardware includes an external syslog server accessed by the TOE for long term archiving of audit event logs using a secure channel protected by TLS.

1.7 Physical Boundary

The physical boundary of the TOE includes either of the following:

A) One chassis containing from one to three instances of the 3900 Series Packet Flow Switch appliance with built-in online help.

Or

B) A single instance of the PFS Management Server with built-in online help is required when managing multiple chassis, each of which contains from one to three instances of a 3900 Series Packet Flow Switch.

Product operating manuals include:

- *nGenius® 3900 Series Packet Flow Switch Hardware Installation Guide* (Part Number 733-0596 Rev. A)
- *nGenius® 3901R Packet Flow Switch Quick Connection Guide Guide* (Part Number 293-2567 Rev. A)
- *nGenius® 3903 Packet Flow Switch Quick Connection Guide* (Part Number 293-2568 Rev. A)
- *nGenius® PFS Management Software Administrator Guide* (Part Number 733-0595 Rev. B)

- *nGenius® PFS Management Server Hardware Installation Guide* (Part Number 293-2566 Rev. B)
- *nGenius® 3900 Series Packet Flow Switch v3.3 Release Notes* (Part Number 733-0672 Rev. A)
- *Common Criteria Supplemental Guidance for nGenius PFS Management Server and PFS Switch Software Version 3.3.40* (Part Number 733-0504 Rev. A)

1.8 Logical Scope of the TOE

The TOE logical scope is defined by the following security functionality:

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

1.8.1 Security Audit (FAU)

During operation, the TOE generates audit records for critical system and management events. The audit records are stored on locally on the TOE where they can be viewed by all authorized users with appropriate privileges. A syslog server is required in operational environment for long term event storage.

1.8.2 Cryptographic Support (FCS)

The TOE includes a FIPs 140-2 validated cryptographic module and provides FIPS approved cryptography supporting key generation and destruction and the use of FIPS validated algorithms for protecting connections between TOE components, between the TOE and its users, and between the TOE and external services where required.

1.8.3 User Data Protection (FDP)

Full Residual Information Protection is provided as the TOE programmatically ensures that network packet payloads exiting the TOE contain only the intended data.

1.8.4 Identification and Authentication (FIA)

All users accessing the TOE are identified and authorized before they are granted access to any TOE security and management functions. User interfaces include a java applet (GUI) for routine operations. The applet download is triggered using an HTTPS web interface. Access to the Java applet and to the PFS operating system CLI requires a unique user name and password before access is granted. The operating system CLI is accessible remotely using SSH. The CLI is accessible locally by using a serial console port on the PFS Switch and a KVM (keyboard, video, mouse) device on the PFS Management Server. The SSH connection to the operating system CLI is protected by password authentication and alternatively, certificate authentication may be configured. The serial console port and KVM are protected by password authentication.

1.8.5 Security Management (FMT)

The TOE provides local access using a KVM or PC terminal via a direct connection to the console (serial) port available both on the PFS 3900 switch and on the nGenius PFS Management Server appliance. This access supports initial configuration and maintenance operations. Remote access is provided by the java applet interface which is used for performing day-to-day operations.

1.8.6 Protection of the TSF (FPT)

The TOE provides a number of features to protect its functions from unauthorized use.

A suite of self tests executes during initial start-up to ensure the correct operation of TOE functions. Cryptography and other proven techniques protect passwords, cryptographic keys and other critical security parameters from access during entry, use and storage.

The TOE prevents reading of passwords, cryptographic keys and other critical security parameters using encrypted storage and other techniques. Time protocols synchronize time across all TOE components to prevent time based errors and exploits.

The TOE protects TSF data from disclosure and detects its modification when it is transmitted between PFS Switch and a PFS Management Server when a PFS Management Server is included in the TOE configuration.

The TOE includes a utility that validates software updates before they are installed by recalculating their SHA1 hash value and matching that to the published hash value. The TOE rejects updates with un-matching hash values.

1.8.7 TOE Access (FTA)

Before users may access the TOE functions, they must acknowledge an administrator-specified advisory notice and consent warning message regarding use of the TOE. The TOE also monitors user sessions, enforcing session locking and logout on idle sessions.

1.8.8 Trusted Path/Channels (FTP)

The TOE uses FIPS validated cryptography for establishing trusted communication channels between the TOE and external entities.

- HTTPS over TLS protects user communications with the web user interface.
- TLS protects user communications with the Java applet.
- SSHv2 protects user communications with the operating system CLI interface.
- TLS protects TOE communication with an external audit server.

1.9 Evaluated Configuration

1. Identification and authentication are performed locally by the TOE.
2. HTTPS/SSL(TLS) is activated on the TOE remote management web interface (whether the interface is provided by the PFS Switch or the PFS Management Server) and all connections from remote users to the TOE remote management interface use HTTPS. (HTTP is not allowed for use.)

3. SSHv2 is activated on the TOE PFS operating system CLI access (whether the interface is provided by the PFS Switch or the PFS Management Server) and all connections from remote administrators to the TOE remote management interface use SSHv2 (telnet is not allowed for use and is disabled by default.)
4. TLS functionality is configured on the TOE to provide a trusted channel between distributed TOE components, and between the TOE and an external audit server.

2. Security Problem Definition

2.1 Introduction

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) with Errata 3. The NDPP offers additional information about the identified threats, but that has not been reproduced here and the NDPP should be consulted for those details.

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets, and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

2.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 - Assumptions

Assumption Name	Description
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	Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

2.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 3 - Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.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.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.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

2.4 Organisational Security Policies

This section describes the Organizational Security Policy (OSP) that applies to the TOE. An OSP is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 4 - Organizational Security Policy

Policy Name	Policy Definition
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. Security Objectives

The Security objectives have been drawn verbatim from the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) with Errata 3. The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP should be consulted for those details.

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as O.objective. Objectives that apply to the operational environment are designated as OE.objective.

3.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 5 - Security Objectives for the TOE

Objective Name	Description
O.PROTECTED _COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
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.RESIDUAL_INFORMATION _CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

3.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 6 - Security Objectives of the Operational Environment

IT Environment Security Objective Name	Description
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. Extended Components Definition

The Security Target includes extended components listed below because the Protection Profile for Network Devices on which the TOE is based prescribes security objectives for the TOE that cannot be translated to Part 2 SFRs, or can be translated, but only with great difficulty based on components in CC Part 2. The extended components included in this security target are replicated directly from Protection Profile for Network Devices (NDPP), Version 1.1, June 8, 2012 with Errata 3.

Consult the NDPP for details regarding these extensions as they are not redefined here.

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

5. IT Security Requirements

This section defines the TOE Security Function Requirements (SFRs) and TOE Security Assurance Requirements (SARs) representing the security claims for the Target of Evaluation and to scope the evaluation effort.

The SFRs are drawn from the Protection Profile (PP): Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) with Errata 3. Assignments and operations made within the PP are not identified (highlighted) here. Only the requirements and residual assignments and operations from the PP are completed here. The PP makes a number of refinements and completes operations made in the CC. Consult the CC and the PP for more information.

The SARs are also drawn from the NDPP version 1.1.

5.1 Conventions

The PP defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the PP:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

5.2 TOE Security Function Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from the Protection Profile for Network Devices which is based on Part 2 of the CC.

Table 7 - TOE Security Function Requirements

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)

	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1 Explicit: HTTPS
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1: Explicit: SSH
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection [1]
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted Path

The security functional requirements are stated in the following subsections.

[1] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

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

a) Start-up of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions

d) Specifically defined audit events listed in Table ~~1~~**8**.

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, the additional information specified in column 3 of table ~~1~~**8**.

Table 8 - TOE Security Functional Requirements and Auditable Security Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU Security Audit		
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_ Cryptographic Support		
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session	Reason for failure.
	Establishment/Termination of a HTTPS session.	Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure.
	Establishment/Termination of an SSH session	Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
	Establishment/Termination of a TLS	Non-TOE endpoint of connection (IP

Requirement	Auditable Events	Additional Audit Record Contents
	session	address) for both successes and failures.
FDP User Data Protection		
FDP_RIP.2	None.	
FIA Identification and Authentication		
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT Security Management		
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT Protection of the TSF		
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_ITT.1	None	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	
FTA TOE Access		
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP Trusted Path/Channels		
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

5.2.1.2 FAU_GEN.2 User Identity Association

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 FAU_STG_EXT.1 External Audit Trail Storage

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

5.2.2 Cryptographic Support (FCS)

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

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

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

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

5.2.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

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

FCS_COP.1.1(1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in *CBC* and cryptographic key sizes 128-bits, 256-bits, and no other key sizes that meets the following:

- FIPS PUB 197, "Advanced Encryption Standard (AES)"
- NIST SP 800-38A

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

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services in accordance with a

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

that meets the following:

- FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"

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

FCS_COP.1.1(3) The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256 and message digest sizes 160, 256 bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

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

FCS_COP.1.1(4) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, SHA-256 key size *160, 256 bits*, and message digest sizes 160, 256 bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

5.2.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.2.8 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of 256 bits of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.2.2.9 FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246) supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

5.2.2.10 FCS_SSH_EXT.1 Explicit: SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and no other RFCs.

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

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

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

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

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

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

5.2.3 User Data Protection (FDP)

5.2.3.1 FDP_RIP.2 Full Residual Information Protection

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)

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

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

5.2.4.1 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, to perform administrative user authentication.

5.2.4.2 FIA_UAU.7 Protected Authentication Feedback

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

5.2.4.3 User Identification and Authentication (FIA_UIA) FIA_UIA_EXT.1

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

- Display the warning banner in accordance with FTA_TAB.1;

- *Respond to ICMP ping operations.*

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

5.2.5 Security Management (FMT)

5.2.5.1 FMT_MTD.1 Management of TSF Data

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

5.2.5.2 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using published hash capability prior to installing those updates;
- No other capabilities.

5.2.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

5.2.6.2 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use TLS. [2]

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

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

5.2.6.4 FPT_STM.1 Reliable Time Stamps

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

5.2.6.5 FPT_TST_EXT.1: TSF Testing

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.

5.2.6.6 FPT_TUD_EXT.1 Extended: Trusted Update

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 published hash prior to installing those updates.

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL.3 TSF-initiated Termination

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

5.2.7.2 FTA_SSL.4 User-initiated Termination

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

5.2.7.3 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

5.2.7.4 FTA_TAB.1 Default TOE Access Banners

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

[2] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1	The TSF shall use TLS to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
FTP_ITC.1.2	The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.
FTP_ ITC.1.3	The TSF shall initiate communication via the trusted channel for *audit service*.

5.2.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1	The TSF shall use SSH, TLS/HTTPS provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.
FTP_TRP.1.2	The TSF shall permit remote administrators to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for initial administrator authentication and all remote administrative actions.

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements specified by Protection Profile for Network Devices (PP-ND), Version 1.1, June 8, 2012 with Errata 3. These requirements are summarized in the following table.

Table 9 - Security Assurance Requirements

Assurance Class	Component ID
Development	ADV_FSP.1 Basic Functional Specification
Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative User guidance
Life-Cycle Support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM coverage
Tests	ATE_IND.1 Independent testing - conformance
Vulnerability Assessment	AVA_VAN.1 Vulnerability analysis

5.3.1 Development (ADV)

5.3.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d	The developer shall provide a functional specification.
ADV_FSP.1.2d	The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.1.1c	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2c	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3c	The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
ADV_FSP.1.4c	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

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

5.3.2.2 Preparative procedures (AGD_PRE.1)

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

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

5.3.3 Life-Cycle Support (ALC)

5.3.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.1.1c	The TOE shall be labelled with its unique reference.
ALC_CMC.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d	The developer shall provide a configuration list for the TOE.
ALC_CMS.1.1c	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2c	The configuration list shall uniquely identify the configuration items.
ALC_CMS.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d	The developer shall provide the TOE for testing.
ATE_IND.1.1c	The TOE shall be suitable for testing
ATE_IND.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2e	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d	The developer shall provide the TOE for testing..
AVA_VAN.1.1c	The TOE shall be suitable for testing.
AVA_VAN.1.1e	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2e	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3e	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section explains how the TOE provides the required security functions.

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

Note – The TOE has two configurations. A standalone nGenius PFS switch consists of one to three blades in a single chassis. This configuration provides a management interface from one of the blades in the chassis. When multiple chassis are required such as deployments with more than three blades, a separate nGenius PFS Management Server is required to manage the system. For clarity and simplicity, descriptions in the TOE Summary Specification do not repeat this distinction for each mention of a PFS Management Server.

6.1 Security Audit (FAU)

The security capabilities described in this section satisfy the following security function requirements:

FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1,

The TOE logs start-up of the audit functions, TOE administrative operations, and the events listed in Table 8.

All TOE log messages include the following parameters: the time the message was generated, the user that triggered the audit event (if applicable), the user's IP address (if applicable) and the message description.

The audit trail (GUI audit log) is stored on disk in the nGenius PFS Management Server appliance database and in the Micro SD memory device on the PFS 3900 switch. The GUI audit log on a standalone switch configuration is also stored in the database. The log stores up to two days of events, after which time the oldest events are overwritten with new events. If the local audit trail becomes full, the oldest events are overwritten with new events.

The operating system log files are stored on disk in the nGenius PFS Management Server and on the PFS 3900 switch. The logs store up to two days of events, after which time the oldest events are overwritten with new events. If a log file becomes full, the oldest events are overwritten with new events.

To avoid losing log events, an external syslog audit server is configured as required by FAU_STG_EXT.1 to store logs over the long term. Whenever messages are written to the local log, the messages are copied to the syslog server over a TLS channel. The Common Criteria

supplemental guidance directs users to configure a secure TLS channel to protect data transferred to syslog on that channel.

Audit records stored on the TOE are protected from unauthorized access as only identified and authenticated administrators may log in and view the records. Audit records transferred to syslog server are protected in transit by the use of FIPS validated cryptography.

6.2 Cryptographic Support (FCS)

The security capabilities described in this section satisfy the following security function requirements:

> FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1

The TOE uses FIPS-validated cryptography provided by OpenSSL FIPS 2.0.2 object module with OpenSSL 1.0.1 wrappers to communicate with users and other entities in the IT environment. OpenSSL 1.0.1p is built into the PFS 3900 switch and OpenSSL 1.0.1e is built into the nGenius PFS Management Server appliance for use within cryptographic services.

6.2.1 Key Generation

The following table describes the cryptographic keys that are used by the TOE to protect communication channels to external entities and between distributed TOE components.

Table 10 - TOE Critical Security Parameter Usage Storage, and Destruction

Critical Security Parameter	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
PFS 3900 Appliance CSPs				
Web server RSA key pair [Note 1]	[SP 800-90] DRBG RSA	Authenticate to incoming web connections and provide RSA key exchange (SP-800-56B)	Maintained in key store while valid (plaintext). Copied into memory for session establishment.	Both keys zeroized in key store when expired. Zeroized from memory after key exchange.
Web Server Session key [Note 1]	TLS key agreement	Encrypt or decrypt web session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination.

Critical Security Parameter	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
Software/Firmware load test RSA public key	Generated by manufacturing	Authenticate software/ firmware updates	Embedded in the TOE firmware (obscured)	Never Expire
[SP 800-90] DRBG Seed Key	Entropy	Seed key for [SP 800-90] DRBG	RAM (plain text)	Zeroized and overwritten with the generation of new seed
SSH session key [Note 1]	DH Key establishment	Encrypt or decrypt SSH session traffic	Ephemeral, maintained in memory during use	Zeroized at rekey and at session termination.
SSH RSA key pair[Note 1]	[SP 800-90] DRBG RSA	Authenticate to incoming web connections and provide RSA key exchange (SP-800-56B)	Maintained in web server key store (plaintext) and private key only in memory for key transfer	Private key zeroized from memory after key exchange. Key store is zeroized when updated keys replace expired key pair
SSH DH public and private parameters[Note 1]	Diffie-Hellman	Key Establishment	Ephemeral, maintained in memory during session establishment	Zeroized after session establishment
Syslog TLS channel session key. [Note 1]	SP 800-90 DRBG	Encrypt or decrypt session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination.

Critical Security Parameter	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
PFS Management Server to PFS Blade TLS Channel RSA key (when a PFS Management Server Appliance is used)	[SP 800-90] DRBG RSA	RSA key exchange	Maintained in keystore while valid (plaintext). Copied into memory for session establishment.	Zeroized in keystore when expired. Zeroized from memory after key exchange.
PFS Management Server to PFS Blade TLS Channel session key (when a PFS Management Server Appliance is used)	RSA key exchange	Encrypt or decrypt session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination
User passwords	Manual	User Authentication to the switch	Stored in hash (SHA) format.	Not zeroized.
PFS Management Server Appliance CSPs				
Web server RSA key pair	[SP 800-90] DRBG RSA	Authenticate to incoming web connections and provide RSA key exchange (SP-800-56B)	Maintained in keystore while valid (plaintext). Copied into memory for session establishment.	Zeroized in keystore when expired. Zeroized from memory after key exchange.
Web Server Session key	TLS key agreement	Encrypt or decrypt web session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination.

Critical Security Parameter	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
Software/Firmware load test RSA public key	Generated by manufacturing	Authenticate software/ firmware updates	Embedded in the TOE firmware (obscured).	Never Expire
[SP 800-90] DRBG Seed Key	Entropy	Seed key for [SP 800-90] DRBG	RAM (plain text)	Zeroized and overwritten with the generation of new seed
SSH session key	DH Key establishment	Encrypt or decrypt SSH session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination
SSH RSA key	[SP 800-90] DRBG RSA	Server Authentication	Maintained in keystore while valid (plaintext). Copied into memory for session establishment.	Zeroized in keystore when expired. Zeroized from memory after key exchange.
SSH DH key	Diffie-Hellman	Key Establishment	Ephemeral, maintained in memory during session establishment	Zeroized after session establishment
Syslog TLS channel session key.	[SP 800-90] DRBG	Encrypt or decrypt session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination.

Critical Security Parameter	Key Generation / Establishment Method	Purpose or use	Storage	Zeroization
PFS Management Server to PFS Blade TLS Channel session key	RSA key exchange	Encrypt or decrypt session traffic	Ephemeral, maintained in memory during use	Zeroized at session termination
User passwords	Manual	User Authentication to the PFS Management Server	Stored in hash (SHA) format.	Not zeroized.

[Note 1] CSP not used when the PFS 3900 is managed by a PFS Management Server Appliance.

CSPs including user passwords, symmetric keys, and private keys are protected from viewing as the TOE does not provide an interface designed specifically for that purpose.

The SSHv2 protocol uses RSA keys for client authentication and the Diffie-Hellman protocol for symmetric session key establishment. For use within HTTPS and TLS, the TOE generates RSA keys for server authentication and for use with RSA key establishment.

RSA keys are generated in accordance with NIST Special Publication 800-56B. When these key pairs are used for key establishment, they are used in accordance with NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes.

The TOE satisfies the NIST SP 800-56B requirements without extensions. The following table specifically identifies the "should," "should not," and "shall not" statements from the publication indicating whether the TOE conforms to those statements and rationalizing any deviations.

Table 11 - NIST SP800-56B Conformance

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.6	Should	Yes	
5.9	shall not (first occurrence)	Yes	
5.9	shall not (second occurrence)	Yes	
6.1	should not	Yes	
6.1	should (first occurrence)	Yes	
6.1	should (second occurrence)	Yes	

6.1	should (third occurrence)	Yes	
6.1	should (fourth occurrence)	Yes	
6.1	shall not (first occurrence)	Yes	
6.1	shall not (second occurrence)	Yes	
6.2.3	should	Yes	
6.5.1	should	Yes	
6.5.2	should	Yes	
6.5.2.1	should	Yes	
6.6	shall not	Yes	
7.1.2	should	Yes	
7.2.1.3	should	Yes	
7.2.1.3	should not	Yes	
8	should	Yes	
8.3.2	should not	Yes	

6.2.2 Key Zeroization

When keys are zeroized after use as described in Table 12, the zeroization function overwrites the key memory buffers with zeros. For key material maintained in key stores on disk, the disk location is overwritten 25 times with a final overwrite of zeros.

Passwords are not stored in human readable format. These CSPs are not zeroized**.**

6.2.3 Cryptographic Operations

Cryptographic Operations (algorithms) are provided by the OpenSSL cryptographic module. The following table describes the cryptographic operations and their use within the SSHv2 protocol.

Table 12 - SSHv2 Cryptography

Cryptographic Method	Purpose in SSHv2
RSA Digital Signatures	Server authentication.
Key Exchange (Diffie-Hellman)	Session establishment.
HMAC-SHA	Traffic integrity verification.
[SP 800-90] DRBG	Key material provisioning.
AES	Session traffic encryption.

The following table describes the cryptographic operations and their use within the TLS protocol. Note the TLS protocol may be used alone or within the HTTPS protocol.

Table 13 - TLS Cryptography

Cryptographic Method	Purpose in TLS
RSA Digital Signatures	Server authentication.
RSA Key Exchange	Session establishment.
SHA	Traffic integrity verification.
[SP 800-90] DRBG	Key material provisioning.
AES	Session traffic encryption.

The following table lists the FIPS-validated algorithms implemented within the TOE. These algorithms are provided by the OpenSSL cryptographic module (CMVP certificate 1747) included in the TOE.

Table 14 - TOE Cryptographic Algorithms

Function	Standard	Algorithm
Random Bit Generation	[SP 800-90] DRBG	DRBG CTR DRBG (AES) (Certificate 264)
Encryption / Decryption	[FIPS Pub 197]	AES 128/256 CBC (Certificate 2234)
Message Digests	[FIPS Pub 180-3]	SHA-1, SHA-2 (256) (Certificate 1923)
Keyed Hash	[FIPS Pub 198]	HMAC SHA-1, SHA-2 (256) (Certificate 1363)
Digital Signature	RSA	RSA SigGen9.31, SigGenPKCS1.5, SigVer9.31, SigVerPKCS1.5 (Certificate 1145)

6.2.4 SSH Conformance to RFCs 4251, 4252, 4253, and 4254

TOE SSH implementations conform to RFCs 4251, 4252, 4253, and 4254.

The SSH protocol supports SSH_RSA public key authentication and Linux password-based client authentication. The default configuration does not enable public key authentication. Diffie-Hellman support is limited to using group 14 keying material.

For compliance with RFC 4253, the TOE drops packets greater than 256k bytes. Independent implementations for client-to-server and server-to-client channel algorithms use AES-CBC-128 or AES-CBC-256 encryption and hmac-sha1 or hmac-sha1-96 for packet integrity as negotiated during the handshake. Rekey is triggered after one hour or after 2^{28} packets have been transferred (whichever event occurs first).

6.2.5 TLS Conformance

Up to four TLS server channels exist on the TOE:

- The channel between the nGenius PFS Management Server appliance and the PFS 3900 switch (if an external management server is used).
- The channel between the management interface and users (clients) accessing the TOE GUI (the Java applet).
- The channel between the TOE and external audit (syslog) server.

In all cases, the TOE implements the mandatory cipher suite specified by NDPP and the following optional cipher suite:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

The TOE supports TLS v1.1 and v1.2 and does not use md5 for integrity. The TLS Record Protocol and TLS Handshake Protocol are used for authentication and key negotiation. Client authentication is not used for any TLS channels.

The TOE does not implement any TLS extensions defined in RFC 3546.

Vendor assured adherence to the FIPS-140-2 standard is provided by linking the openssl-fips module at the TOE platform layer. In addition, the TOE limits the list of encryption protocols to only those specified by the standard.

TOE Channel TLS Support

The TOE GUI channel supports simultaneous connections using TLS versions 1.1 and 1.2.

The channel between the PFS Management Server and a managed PFS switch used TLS version 1.1 or 1.2 as configured during setup of the evaluated configuration.

The channel between the TOE and external audit (syslog) server use TLS versions 1.1 or 1.2, defaulting to the highest version.

Users that need TLS version 1.1, for example, when an external syslog server does not support TLS version 1.2, can disable TLS version 1.2 using a procedure in the syslog troubleshooting section of the *Common Criteria Supplemental Guidance for nGenius PFS Management Server and PFS Switch Software Version 3.3.40*.

6.2.6 HTTPS Conformance to RFC 2818

The TOE provides up to two HTTPS servers for establishing TLS communication channels:

- The appliance HTTP server establishes a TLS communication channel between the appliance and users (clients) accessing the web Java client UI.
- When a PFS Management Server us used, the PFS Switch provides an HTTPS server to establish a secure remote management connection with the PFS Management Server .

In both cases when the HTTPS server receives a connection request, it waits for the TLS ClientHello message to begin the TLS handshake. When the TLS handshake has finished, the server waits for the client to initiate the first HTTP request. All HTTP data is sent and treated as TLS "application data". Normal HTTP behavior is followed.

6.3 User Data Protection (FDP)

The following description of network packet processing explains how the TOE satisfies FDP_RIP.2, Residual Information Processing.

After a packet is transmitted from the server, the server de-allocates the packet buffer, returning it to the buffer pool. When a new packet is to be sent, the server allocates a new buffer from the buffer pool. As soon as the buffer is allocated, the TSF zeroizes the entire allocated buffer. The TSF then constructs the packet and writes it into the clean buffer. This ensures that no residual data is included in the new packet.

6.4 Identification and Authentication (FIA)

The security capabilities described in this section satisfy the following security function requirements:

FIA_PMG_EXT.1, FIA_UIA_EXT.1.1, FIA_UIA_EXT.1.2, FIA_UAU_EXT.2.1, FIA_UAU.7.1

The TOE offers the following user interfaces interacting with the TOE features.

- A Java applet that provides a graphical user interface. The applet is launched from a browser over HTTPS.
- SSHv2 connections to TOE port 22 access operating system functions and are reserved for initial TOE configuration and for TOE maintenance operations only.
- A console (serial) port that accesses operating system functions is provided for initial TOE configuration and maintenance operations.

6.4.1 Local Administrator TOE Access

Local Administration of the TOE (for initial configuration and maintenance) is provided using a direct connection to the console (serial) port via a null-modem cable from a KVM or a PC running a terminal client such as Hyper Terminal or PuTTY.

- For a TOE deployment consisting of a single PFS 3900 Series Switch chassis (that does not include a PFS Management Server), the managing switch has a local console (serial) port that is used for local administration including initial configuration and maintenance.
- When a PFS Management Server is required for managing more than one PFS 3900 Series Switch chassis, the PFS Management Server supports KVM connection used for local administration including initial configuration and maintenance.

Both access methods require users to authenticate before they are granted access to TOE functions.

6.4.2 Remote Administrator GUI Access

Remote administrators access the TOE web interface directly over HTTPS (TLS) to download a JNLP (Java Network Launch Protocol) file which launches the TOE Java applet GUI. The JNLP file loads a java authentication applet that takes the identification and authentication data and passes it to the TOE for authentication. The TOE displays the consent box in accordance with FTA_TAB.1. The user must check the checkbox to indicate they have read the consent statement and to enable the Accept button. The user must click **Accept** to access the TOE functions. If the user clicks **Decline**, the authentication applet terminates and the user is denied access to TOE security functions.

This behavior is identical whether accessing the PFS 3900 appliance or the PFS Management Server appliance.

6.4.3 Remote Administrator Operating System CLI Access

Remote administrators access the operating system CLI using port 22 over SSHv2 for configuration and maintenance operations. The TOE displays a warning banner for remote users

in accordance with FTA_TAB.1. The banner appears after users identify and but before the TOE provides access to TOE security functions.

This behavior is identical whether accessing the PFS 3900 appliance or the PFS Management Server appliance.

6.4.4 TOE Authentication

The TOE looks up the user-provided username in the internal database and then compares a SHA hash of the user-provided password to a hash of the password that is stored in the database. If the hashed passwords match, an authentication success message is generated and logged, and the user is allowed to access the TOE resources. If the hashed passwords do not match, an authentication failure message is generated and (if authenticating to the java client), the login screen is returned to the user. If authenticating to the operating system CLI, the password prompt is returned to the user.

> **Note:** SHA operations on passwords are invoked from internal cryptographic methods that are not FIPS-validated. The use of other cryptographic engines was not evaluated or tested during the CC evaluation of the TOE.

If ICMP is enabled on the TOE, users may initiate an ICMP ping to the IP address of the TOE and receive an ICMP response indicating the device is running on the network. Any other TSF-mediated action other than handling user authentication requests from unauthenticated users requires the user to be successfully identified and authenticated.

For all TOE access methods, password feedback is obscured as follows:

When Java client users enter passwords into the UI, feedback consists of dot characters. When administrators enter passwords into the operating system CLI terminal interface the first time, password characters are not echoed to the terminal. On subsequent attempts, asterisks (*) are returned.

By default minimum password length is one character. The Common Criteria supplemental guidance directs users to set the minimum password length to 8 characters and to enforce complex passwords. Complex passwords must use at least the following:

- one lower case character [a-z]
- one upper case character [A-Z]
- one digit [0-9]
- one special character [@ # $ ^ & * : ; < > , . ? / | { } [ ] + - _ ~ !]

6.5 Security Management (FMT)

The security management capabilities described in this section satisfy the following security function requirements:

> FMT_MTD.1, FMT_SMF.1, FMT_SMR.2.

The TOE supports the following security levels (roles), all of which are administrative in nature.

Administrator – access to all nGenius PFS Management functions and limited diagnostics (The use of diagnostic functions takes the TOE out of its evaluated configuration.) This is the

default account that cannot be deleted from the system. The Common Criteria supplemental guidance directs users to limit use of the Administrator account to a single individual so that audit events can be correctly associated with a single identity.

Operator – access to all nGenius PFS Management functions and limited diagnostics. No access to Switch and user management operations.

Viewer – access to monitor and very limited diagnostics functions only. No access to nGenius PFS Management control functions or user management functions.

Diagnostics - full access to all nGenius PFS Management and diagnostic functions except user management.

TSF data is accessed by the Administrator, Operator, Diagnostic, and Viewer security levels. The combined set of these security levels is the TOE authorized administrator.

The authorized administrator is responsible for managing all TSF data elements including managing TLS certificates and similar protocol settings, configuring communication with external IT services such as syslog, and NTP and managing firmware updates. The TOE provides all functions to enable/disable available network services, to manage cryptography and associated functions, and to manage and verify TOE firmware updates.

6.6 Protection of the TSF (FPT)

The security capabilities described in this section satisfy the following security function requirements:

FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_ITT.1, FPT_STM.1, FPT_TUD_EXT.1, FPT_TST_EXT.1

All passwords used to access the TOE are stored in non-plaintext form such that users are prevented from reading them. Locally stored web user passwords are stored in SHA1 format. Operating system CLI passwords are stored in MD5 hash format.

Locally stored user passwords are stored in SHA-1 hash format. The TOE does not provide methods intended to read cryptographic keys stored within the TOE. See table 10 for information about cryptographic keys and critical security parameters stored within the TOE.

For TOE configurations that require a PFS Management Server, communications between a PFS switch and a PFS Management Server are encrypted using TLS.

The TOE relies on an external NTP server for setting its time clock. For a PFS switch using embedded management, the controlling blade receives the NTP time from the NTP server, sets its clock and synchronizes the time on other managed blades using the NTP protocol. For TOEs containing a PFS Management Server appliance, the active PFS Management Server appliance receives the NTP time from the NTP server, sets its clock and synchronizes the time on other managed blades using the NTP protocol. The TOE online help provides the relevant instructions.

Changes to the system time trigger generation of audit messages indicating the old and new values for the time and the origin (IP address) of the attempt. Security functions that make use of time are: cryptographic operations that use time and date information, audit record timestamps, and session inactivity timing for session locking and termination.

Manual TOE software updates are supported. A valid account on the NETSCOUT Master Care Portal is required to use this service. The Common Criteria supplemental guidance directs users to ensure a valid Master Care Portal account exists for this purpose.

To prevent unauthorized or invalid software updates from being applied, TOE users are instructed to validate software updates before they are installed by calculating their SHA1 hash value and matching that to a corresponding published hash value. Users reject updates with un-matching hash values.

The **Help > About** operation in the nGenius PFS Management Server Appliance GUI displays the TOE current firmware version for the nGenius PFS Management Server Appliance. To see the current firmware version installed on individual blades, in the system View pane, right-click a blade and then click **Diagnostics Status** to view the firmware versions installed. Use these same steps to view the firmware version after updating the firmware.

The following self-tests run on both the nGenius PFS Management Server appliance and ON individual blades during system startup.

On power up or reset, the TOE conducts a series of internal tests (called a POST or power on self-test). The POST confirms that critical functions work before making the system available for use by applications. The ROM based POST program first tests the processor by conducting some operations for which the results are known and maintained in the program. The POST compares the calculated results to the stored results, passing on a match and failing on a mismatch.

The memory and disk drive configuration are read from the boot ROM. The POST memory test writes various data patterns into memory locations and reads them back to confirm that each memory location is functional. The test then interacts with every device in the machine looking for any failures.

For failures at this level, the system outputs an error message to the console, and dumps an image of kernel memory to disk for debug purposes. Standard Linux maintenance operations are needed to recover from these catastrophic failures. When the POST ends successfully, the BIOS searches the various boot mechanisms (using the boot ordering maintained in ROM) for the operating system.

The operating system loads and then uses its configuration files to load the TOE software and any other utilities needed by the TOE.

During the TOE software startup, the OpenSSL program is also started and it executes its own POST that contains a software integrity test, KATs (known answer tests) for cryptographic algorithms, PCTs (pairwise consistency tests) for asymmetric key pairs.

The software integrity test is an HMAC-SHA1 verification of the binary code comprising the OpenSSL executable. This test must pass or the OpenSSL cryptographic module exits before being loaded into memory.

A KAT functions by encrypting a predetermined string with a symmetric encryption algorithm and an associated encryption key. The result must match the known answer or the test fails. Then a decryption is performed and that result must match the original string or the test fails.

A PCT functions by using the private key of a key pair to transform a predetermined string. The result is compared to a known answer. The result must match the known answer or the test fails.

Then the answer is transformed with the public key and that result must match the original string or the test fails. .

If any cryptographic module start-up tests fail, the POST writes the failure indicator to the console and (for PFS 3900 switch blades, activates the status LEDs on the front panel. The cryptographic module enters an error state where it does not provide any cryptographic services.

During operation, the cryptographic module continuously monitors the output of the RBG (Random Bit Generator) to determine that random number and bit generators are operating properly.

POST and operational errors that may occur during startup and associated remedial actions are described in the Common Criteria supplemental guidance.

If any tests fail, the module writes the failure indicator to a log file and all data output is halted from that module. As the self-tests completely exercise the cryptographic and other functionality underlying TOE security functions, all tests passing assures the TOE operator that the TOE security functions are operating correctly.

6.7 TOE Access (FTA)

The security capabilities described in this section satisfy the following security function requirements:

FTA_TAB.1.1, FTA_SSL_EXT.1.1, FTA_SSL.3.1, FTA_SSL.4.1.

TOE access is protected by using session management controls and procedures.

The TOE asserts a warning banner called a consent box that must be actively addressed by interactive users accessing the TOE java client interface on both the PFS 3900 switch and the nGenius PFS Management Server appliance. Users must agree to the stated policy before being granted access to TOE functions. The serial port and SSH operating system CLI port assert a warning banner prior to completing authentication. Users indicate acceptance of the stated policy by completing authentication.

TOE banners are disabled by default. The Common Criteria supplemental guidance directs the persons installing and configuring the TOE to enable these protections and provides relevant procedures.

Administrators logged into the local (serial) console, the Java client interface or into the operating system CLI over SSHv2 are automatically logged out when idle sessions meet an administrator –specified period of inactivity. The auto logout also triggers an audit event message indicating the termination of the user's remote session by the session termination mechanism. The Common Criteria supplemental guidance directs administrators to enable and specify the period of inactivity for Java client and operating system CLI users on both the PFS 3900 switch and the nGenius PFS Management Server appliance and provides relevant procedures.

Administrators logged into the Java client can use the GUI exit operation or press Escape to terminate their own interactive session at any time while they are authenticated. Operating system CLI users can terminate their sessions by entering the exit command. User session

termination is identical on both the PFS 3900 switch and the nGenius PFS Management Server appliance.

6.8 Trusted Path/Channels (FTP)

The Trusted path/channels function satisfies the following security functional requirements on both the PFS3900 switch and on the nGenius PFS Management Server appliance:

- FTP_ITC.1: The TOE can be configured to use TLS to ensure that exported audit records, are sent to and readable by only the configured SYSLOG servers so they are not subject to unauthorized disclosure or modification.
- FTP_TRP.1: The TOE provides TLS within HTTPS using an embedded FIPS validated cryptographic module to support secure web access for remote administration. TLS protects remote sessions from unauthorized disclosure and modification using FIPS validated cryptographic algorithms.

The TOE provides SSHv2 using an embedded FIPS validated cryptographic module to support secure access to the operating system CLI for remote maintenance operations. SSHv2 protects remote sessions from unauthorized disclosure and modification using FIPS validated cryptographic algorithms.

No unprotected remote administration channels exist.

TLS and SSH protocols provide the trusted communication channels between the TOE and external entities.

Both of these protocols provide the following protections:

- Protection of the channel data from disclosure is provided by using AES encryption.
- Detection of modification of the channel data is provided by using SHA (in TLS) or HMAC-SHA (in SSHv2) integrity protection mechanisms.

The path between the TOE and external audit server (syslog) is protected by TLS. The syslog server must support TLS connections. In this case, communication channels are initiated by the TOE security function.

The communication channel for remote administrators accessing the Java client interface is protected by TLS. The communication channel is initiated by the client side remote administrator.

Note the cryptography for Java Applets running on the client uses the client cryptographic service provider. No claims for FIPS validated cryptography are placed on the Java applet that is outside the physical scope of the TOE.

For both java client access and operating system CLI access remote administrators must provide valid identification (a registered username) and authentication (a valid password) to access TOE services over the trusted communication channel.

7. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are complete between the threats, policies, and assumptions, and TOE security function requirements.

7.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 15 - Threats and Assumptions to Security Objectives Mapping

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

7.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 16 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ADMIN_ERROR	**O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity. This mitigates the threat that an incorrect configuration would be undetected as the TOE audits TOE configuration actions for review.

T.TYPE	Security Objectives Rationale
T.TSF_FAILURE	**O.TSF_SELF_TEST.** The TOE tests a subset of its security functionality to ensure it is operating properly. This mitigates the threat that security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	**O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity. This mitigates the threat that malicious remote users or external IT entities may take actions that adversely affect the security of the TOE.
T.UNAUTHORIZED_ACCESS	This threat is mitigated by the following objectives: **O.PROTECTED_COMMUNICATIONS**. The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities, preventing attackers from gaining access to the TOE or to TSF data using data transmitted across the network. **O.SYSTEM_MONITORING.** The TOE will provide the capability to generate audit data and send those data to an external IT entity assuring that unauthorized accesses will be detected. **O.TOE_ADMINISTRATION.** The TOE will provide mechanisms to ensure that only authorized administrators are able to log in and configure the TOE, and access security management functions assuring that unauthorized entities cannot access the TOE and reconfigure the TOE security functions. **O.SESSION_LOCK**. The TOE shall provide session locking mechanisms that mitigate the risk of unattended sessions being hijacked.
T.UNAUTHORIZED_UPDATE	**O.VERIFIABLE_UPDATES.** The TOE will ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source. This mitigates the threat of malicious updates intended to compromise TOE security features .
T.USER_DATA_REUSE	**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 mitigates the threat that data would be erroneously sent to an unintended recipient.

7.1.2 Rationale Mapping Assumptions to Environment Security Objectives

The following rationales ensure assumptions are satisfied using tracings to show that security objective *X* directly upholds assumption *Y* by restating the assumption.

7.1.2.1 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.

7.1.2.2 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.

7.1.2.3 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.

7.2 Security Function Requirements Rationale

7.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 17 - SFRs to Security Objectives Mapping

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FAU_GEN.1				X				
FAU_GEN.2				X				
FAU_STG_EXT.1				X				
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						X
FCS_COP.1(3)		X						X
FCS_COP.1(4)		X						
FCS_HTTPS_EXT.1		X						
FCS_RBG_EXT.1		X						

	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST	O.VERIFIABLE_UPDATES
FCS_SSH_EXT.1		X						
FCS_TLS_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1						X		
FIA_UIA_EXT.1						X		
FIA_UAU_EXT.2						X		
FIA_UAU.7						X		
FMT_MTD.1						X		
FMT_SMF.1						X		
FMT_SMR.2						X		
FPT_APW_EXT.1						X		
FPT_ITT.1 [3]		X						
FPT_SKP_EXT.1		X						
FPT_STM.1					X			
FPT_TST_EXT.1							X	
FPT_TUD_EXT.1								X
FTA_SSL.3				X		X		
FTA_SSL.4						X		
FTA_SSL_EXT.1				X		X		
FTA_TAB.1	X							
FTP_ITC.1		X						
FTP_TRP.1		X						

[3] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.DISPLAY_BANNER	FTA_TAB.1 requires the TOE to display a consent banner to any user attempting to access the TOE user interfaces.
O.PROTECTED_COMMUNICATIONS	FCS_CKM.1: The TOE generates encryption keys to encrypt channels between the TOE and external entities. FCS_CKM_EXT.4: The TOE zeroizes secret cryptographic keys when they are no longer needed. FCS_COP.1(1): The TOE uses FIPS-validated AES for cryptographic operations. FCS_COP.1(2): The TOE uses FIPS-validated rDSA for cryptographic operations. FCS_COP.1(3): The TOE uses FIPS-validated SHA-1 and SHA-256 for cryptographic operations. FCS_COP.1(4): The TOE uses FIPS-validated HMAC SHA-1, for cryptographic operations. FCS_HTTPS_EXT.1.1 The TOE uses HTTPS with TLS to protect communications with remote administrators and users. FCS_RBG_EXT.1: The TOE is required to implement NIST- or FIPS-conformant Random Bit Generation in support of cryptographic protocols. FCS_TLS_EXT.1: The TOE uses mandatory cipher suites AES 128 or 256 to protect communications with remote administrators and users. FCS_SSH_EXT.1: The TOE uses SSHv2 to protect TOE communication with local administrators. FPT_ITT.1: The TOE uses TLS to communicate between distributed TOE components. [4] FPT_SKP_EXT.1: The TOE maintains stored cryptographic keys and CSPs in non-human readable format. FTP_ITC.1: The TOE protects communication between itself and its external authentication and audit services from disclosure and modification. FTP_TRP.1: The TOE protects communication between itself and its administrators from disclosure and modification.
O.RESIDUAL_INFORMATION_CLEARING	FDP_RIP.2: The TOE zeroizes new buffers to ensure network packets do not contain stale data.
O.SESSION_LOCK	FTA_SSL.3: The TOE terminates remote sessions after an administrator defined period of inactivity to help prevent unauthorized access. FTA_SSL_EXT.1: The TOE terminates local sessions after an administrator defined period of inactivity to help prevent unauthorized access.
O.SYSTEM_MONITORING	FAU_GEN.1: The TOE generates audit events for security relevant activities on the TOE. FAU_GEN.2: The TOE associates audit events with users to ensure proper

[4] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

Security Objective	SFR and Rationale
	accountability. FAU_STG_EXT.1: The exports audit records to an external syslog server using a trusted channel to protect the data from disclosure and modification. FPT_STM.1: The TOE generates reliable time stamps for use in audit records for proper accounting.
O.TOE_ADMINISTRATION	FIA_PMG_EXT.1: TOE administrators can configure password length and composition for increased strength of authentication. FIA_UAU.7: The TOE does not echo passwords being entered to prevent password disclosure. FIA_UAU_EXT.2: The TOE implements a local authentication mechanism and an optional external authentication mechanism. FIA_UIA_EXT.1: The TOE identifies and authenticates users before allowing them to access protected TOE security functions. FMT_MTD.1: The TOE restricts management of TSF data to TOE administrators. FMT_SMF.1: The TOE provides management functions to ensure the TOE administrators can properly manage the TOE. FMT_SMR.1: The TOE maintains the role of Authorized Administrator role and provides additional roles as needed. FPT_APW_EXT.1: The TOE stores passwords in non-human readable form to prevent administrators and others from reading them. FTA_SSL.3: The TOE terminates remote sessions after an administrator defined period of inactivity to prevent unauthorized TOE access. FTA_SSL.4: The TOE has a log out interface for users to terminate their sessions as needed to protect an open session from misuse by other users. FTA_SSL_EXT.1: The TOE terminates local sessions after an administrator defined period of inactivity to prevent unauthorized TOE access.
O.TSF_SELF_TEST	FPT_TST_EXT.1: The TOE executes self-tests during start-up to ensure that the TOE security functions are operating correctly.
O.VERIFIABLE_UPDATES	FCS_COP.1(2): The TOE uses digital signatures to ensure the integrity of updates. FPT_TUD_EXT.1: The TOE provides software/firmware update functions and enables an administrator to initiate and verify updates before they are applied.

7.3 Requirements Dependency Rationale

The following table shows the security function requirement dependencies and the security assurance requirement dependencies are satisfied.

Table 19 - Requirement Dependencies

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(*) and FCS_CKM_EXT.4
FCS_CKM_EXT.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_HTTPS_EXT.1	None	None
FCS_RBG_EXT.1	None	None
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(*)
FDP_RIP.2	None	None
FIA_PMG_EXT.1	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	None	None
FIA_UIA_EXT.1	None	None
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_APW_EXT.1	None	None
FPT_ITT.1 [5]	None	None
FPT_SKP_EXT.1	None	None
FPT_STM.1	None	None

[5] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

ST Requirement	CC Dependencies	ST Dependencies
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	None	None
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_SSL_EXT.1	None	None
FTA_TAB.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1
AVA_VAN.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1	ADV_FSP.1 and AGD_OPE.and AGD_PRE.1

7.4 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 20 - SFRs to TOE Security Functions Mapping

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_GEN.1	X							
FAU_GEN.2	X							

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels
FAU_STG_EXT.1	X							
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_HTTPS_EXT.1		X						
FCS_RBG_EXT.1		X						
FCS_SSH_EXT.1		X						
FCS_TLS_EXT.1		X						
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UAU.7				X				
FIA_UAU_EXT.2				X				
FIA_UIA_EXT.1				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_APW_EXT.1						X		
FPT_ITT.1 [6]						X		
FPT_SKP_EXT.1						X		
FPT_STM.1						X		
FPT_TST_EXT.1						X		
FPT_TUD_EXT.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_SSL_EXT.1							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

[6] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.

8. Protection Profile Claims

This ST is conformant to the Security Requirements for Network Devices, Version 1.1, 8 June 2012 (NDPP) – with Errata 3 and the optional SSH, TLS, HTTP, and FPT_ITT requirements.

The TOE includes packet flow switch devices. As such, the TOE is a network device making the NDPP claim valid and applicable.

As explained in section 2, Security Problem Definition, the Security Problem Definition of the NDPP has been copied verbatim into this ST.

As explained in section 3, Security Objectives, the Security Objectives of the NDPP have been copied verbatim into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from verbatim from the NDPP.

Table 21 - SFR Protection Profile Sources

Requirement Class	Requirement Component	Source
FAU: Security audit	FAU_GEN.1: Audit Data Generation	NDPP
	FAU_GEN.2: User identity association	NDPP
	FAU_STG_EXT.1: External Audit Trail Storage	NDPP
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)	NDPP
	FCS_CKM_EXT.4: Cryptographic Key Zeroization	NDPP
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)	NDPP
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)	NDPP
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)	NDPP
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)	NDPP
	FCS_HTTPS_EXT.1 Explicit: HTTPS	NDPP
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)	NDPP
	FCS_SSH_EXT.1: Explicit: SSH	NDPP
	FCS_TLS_EXT.1: Explicit: TLS	NDPP
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection	NDPP
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management	NDPP
	FIA_UAU.7: Protected Authentication Feedback	NDPP
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism	NDPP

	FIA_UIA_EXT.1: User Identification and Authentication	NDPP
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)	NDPP
	FMT_SMF.1: Specification of Management Functions	NDPP
	FMT_SMR.2: Restrictions on Security Roles	NDPP
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	NDPP
	FPT_ITT.1: Basic Internal TSF Data Transfer Protection [7]	NDPP
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	NDPP
	FPT_STM.1: Reliable Time Stamps	NDPP
	FPT_TST_EXT.1: TSF Testing	NDPP
	FPT_TUD_EXT.1: Extended: Trusted Update	NDPP
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination	NDPP
	FTA_SSL.4: User-initiated Termination	NDPP
	FTA_SSL_EXT.1: TSF-initiated Session Locking	NDPP
	FTA_TAB.1: Default TOE Access Banners	NDPP
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	NDPP
	FTP_TRP.1: Trusted Path	NDPP

[7] FPT_ITT.1 applies only to multi-chassis TOEs requiring a separate PFS Management Server.