ciena : the network specialist

Ciena Carrier Ethernet Solutions 3900/5100 Series

Security Target

ST Version: 1.0
January 7, 2016

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.1.1 ST Identification

ST Title:	Ciena Carrier Ethernet Solutions 3900/5100 Series Security Target
ST Version:	1.0
ST Publication Date:	January 7, 2016
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.1.3 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1-1 and 1-2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
SAOS	Service-Aware Operating System (SAOS) is the Linux-based operating system provided by Ciena as part of the TOE that provides network switch configuration functionality and a method of limited administrator access that prevents the use of an unrestricted shell.

Table 1-1: Customer Specific Terminology

Term	Definition
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. The TOE maintains three administrator roles: Limited, Admin, and Super, each of which has certain authorizations to perform management functions on the TOE. An Authorized Administrator is a user who is attempting to perform a function that is allowed by their assigned administrative role. The use of 'privilege' is synonymous with the use of 'role' when discussing the administrator roles defined by the TOE.
Entropy	A string of quasi-random data that is generated by unpredictable physical and/or logical phenomena in a computer and is used in the generation of random numbers.
Security Administrator	Synonymous with Authorized Administrator.
Trusted Channel	An encrypted connection between the TOE and a trusted remote server.
Trusted Path	An encrypted connection between a remote administrative interface and the TOE.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

The acronyms used throughout this ST are defined in Table 1-3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CES	Carrier Ethernet Solutions
CLI	Command Line Interface
CSP	Critical Security Parameter
CTR	Counter (AES mode)
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code

IDSs	Intrusion Detection Systems
KAS	Key Agreement Scheme
MAC	Media Access Control
NDPP	Network Device Protection Profile
POST	Power On Self-Test
NTP	Network Time Protocol
QoS	Quality of Service
RSA	Rivest Shamir Adelman (encryption algorithm)
SAOS	Service Aware Operating System
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell

Table 1-3: Acronym Definition

1.1.5 References

[1] SAOS 6.14.0 CLI Reference Manual

[2] SAOS 6.14.0 Software Configuration Guide

1.2 TOE Reference

The TOE is the Ciena Carrier Ethernet Solutions 3900/5100 Series. The TOE is a family of standalone network hardware appliances that run the Ciena Service Aware Operating System (SAOS) 6.14, with uniform security functionality between each of the hardware appliances. SAOS is itself an extension of Linux kernel version 3.10.

1.3 TOE Overview

Ciena Carrier Ethernet Solutions 3900/5100 Series is a network switch that receives data from an external source and forwards that data to one or many ports. Carrier Ethernet provides a way to deliver Ethernet services across many networks while providing bandwidth management. CES operates on quality-of-service (QoS) capabilities and virtual switching functions to deliver different amounts of data to various ports. CES also contains next-generation Ethernet features that transport different Ethernet services through fiber or copper connections. The Target of Evaluation (TOE) is the general network device functionality (I&A, auditing, security management, trusted communications, etc.) of the switch, consistent with the claimed Protection Profile.

The following diagram shows one instance of the TOE in its operational environment. All models of the TOE have the same environment and interfaces with one exception: some models lack an Ethernet management port so remote administration and placement of the required environmental objects in this case will use a data hardware interface that is specifically configured to handle management traffic.

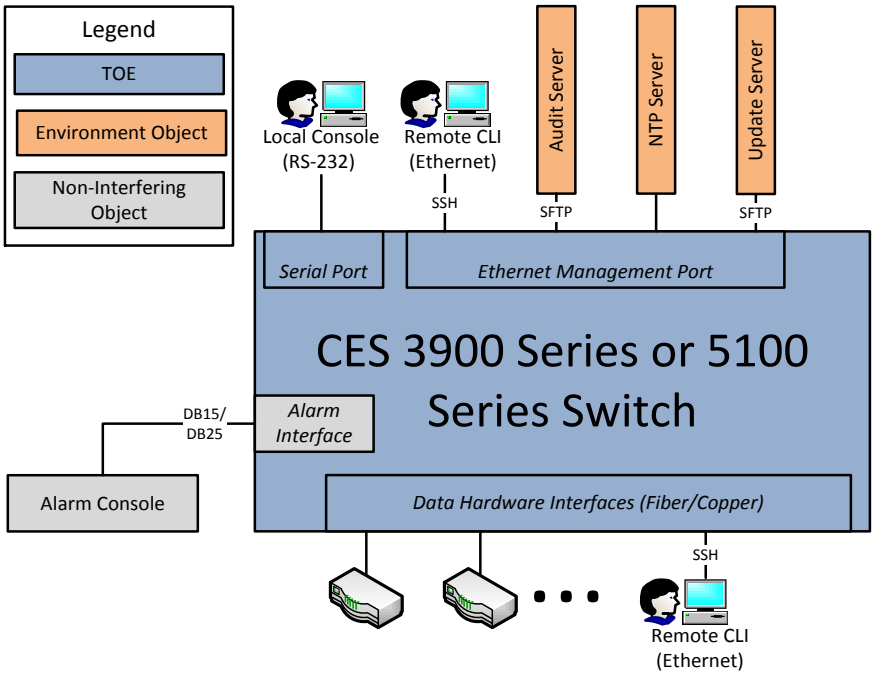

Figure 1 – TOE Boundary

As illustrated in Figure 1, the TOE is one of a family of hardware devices that has an Ethernet management port, a local serial port, and data hardware interfaces. The Ethernet management port allows users to connect to the TOE via SSH through a command line interface. In addition, the Ethernet management port serves as a communication channel to external entities such as remote audit storage, NTP and update servers. The data hardware interfaces provide both ingress and egress for switched network traffic. This traffic is not associated with any security functionality and is not within the scope of the TOE. However, these interfaces can also be configured to handle management traffic through a dedicated management VLAN as well.

1.4 TOE Type

The TOE type for this product is Network Device. The TOE is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDPP defines a network device as "a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise." Additionally, the NDPP says that example devices that fit this definition include routers, firewalls, intrusion detection systems, audit servers, and switches that have Layer 3 functionality. The TOE is a switch that has Layer 2 and Layer 3 functionality. The TOE type is justified because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE.

2.1 Evaluated Components of the TOE

The TOE is the Ciena Carrier Ethernet Solutions (CES) 3900/5100 Series family of network switches. The family provides uniform logical security functions throughout all models. Physically, the only security-relevant difference between the models is that some have a dedicated Ethernet management port.

For those models that have a dedicated Ethernet management port, an administrator can access the CLI remotely through the management network, also known as out-of-band management. For models that lack the Ethernet management port, remote administration is performed by configuring a data hardware interface to direct traffic to the management plane of the TSF rather than to a remote network. This is known as in-band management. The following table lists the models that are within the scope of the TOE as well as whether or not they have an Ethernet management port:

Platform	**3903 / 3904 / 3905**	**3916**	**3930-900/910**	**3931-900/910**	**3932 / 3930-930**	**3938 (Smart NID)**	**3942**	**5142**	**CN 5150**	**5160**
1G/10G RJ-45	0	0	0	0	0	2	0	0	0	0
1G/10G SFP+	0	0	2	2	2	2	4	4	0	24
10/100/1000M RJ-45	0	0	0	4	0	8	0	0	0	0
100M/1G SFP	2	4	4	4	4	8	0	20	48	0
XFP	0	0	0	0	0	0	0	0	4	0
Combo RJ-45/SFP	3903 - 1 3904 - 2 3905 - 2	2	4	0	4	0	20	0	0	0
CPU	2x800 MHz ARM Cortex A9	2x500 MHz Cavium 5220	4x600 MHz Cavium 5230	2x600 MHz Cavium 5220	4x600 MHz Cavium 5230	6x1 GHz Cavium 6335	4x1 GHz Cavium 6230	6x1 GHz Cavium 6335	4x600 MHz Cavium 5230	6x1 GHz Cavium 6335
Ethernet Management Port	N	N	Y	N	Y	Y	Y	Y	Y	Y
Power Options	AC, DC	AC, DC	AC, DC (modular)	AC, DC (modular)	AC, DC (modular)	AC	AC, DC	AC, DC (modular)	AC, DC (modular)	AC, DC (modular)

Table 2-1: TOE Models

The remaining differences between the product models concern physical properties such as data plane ports, processing power, size, and power consumption, none of which are relevant to the TSF.

The TOE also includes the ‘advanced security’ license in its evaluated configuration, which allows the TOE to operate as an SSH server for secure remote administration.

2.2 Components and Applications in the Operational Environment

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
Audit Server	A file server running the secure file transfer protocol (SFTP) that is used by the TOE to securely transmit audit data to a remote storage location.
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
NTP Server	A system that provides an authoritative and reliable source of time using network time protocol (NTP).
Update Server	A server running the secure file transfer protocol (SFTP) that is used as a location for storing product updates that can be transferred to the TOE.

Table 2-2: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

- Ethernet Services Manager – This is an optional module that serves as an automated service activation, creation, and management platform for the CES devices. This is used as a primary viewer of appliance and endpoint status within a deployment of Carrier Ethernet devices. The Ethernet Services Manager is not part of the evaluated configuration because it is not security relevant and is a separately purchased product.

2.3.2 Installed but Requires a Separate License

The product contains several capabilities that are not included with the purchase of the product and must be purchased separately and activated via a license key. Other than the Advanced Security license, none of the licensed components are security relevant and are therefore excluded from the TOE.

2.3.3 Installed But Not Part of the TSF

This section contains functionality or components that are part of the purchased product but are not part of the TSF relevant functionality that is being evaluated as the TOE.

- Non-FIPS mode of operation – The TOE includes a FIPS compliant mode of operation which allows the TOE to use only approved cipher suites for SSH communications and to perform cryptographic self-tests on system startup. This mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.

- Alarm console – The TOE includes a local alarm console that can provide immediate notification of various security alerts. This is not part of the evaluated configuration because security alerts and automatic response to security alerts is outside the scope of the claimed PP.
- Remote Telnet interface – The TOE includes both Telnet and SSH interfaces for administration. Telnet is acceptable to use locally via serial connection, but in the evaluated configuration this remote service will be disabled.

Additionally, the TOE includes a number of functions that are outside the scope of the claimed Protection Profile. These functions are not part of the TSF because there are no SFRs that apply to them.

2.4 Physical Boundary

The physical boundary of the TOE includes the Ciena CES 3900/5100 series appliances and the software that runs on them, which is Ciena's Linux-based Service Aware Operating System (SAOS).

The TOE guidance documentation that is considered to be part of the TOE can be found in the Common Criteria-specific guidance for the Ciena 3900/5100 series appliances, which is delivered on physical media to customers purchasing the equipment and is also made available on the Ciena website.

2.5 Logical Boundary

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

2.5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record contains the user information, time stamp, message briefly describing what actions were performed, outcome of the event, and severity. All audit record information is associated with the user of the TOE that caused the event where applicable. Locally-stored audit data is read-only for authorized administrators. Authorized administrators can securely transmit stored audit data to a remote storage location using SFTP.

2.5.2 Cryptographic Support

The TOE provides cryptography in support of SSH trusted communications. Asymmetric keys that used by the TSF are generated in accordance with NIST SP 800-56A. The TOE uses FIPS-validated cryptographic algorithms (certificates AES #3522, RSA #1808, SHS #2904, HMAC #2250, DRBG #881) to provide cryptographic services. Ciena's implementation of these has been validated to ensure that the

algorithms are appropriately strong for use in trusted communications. The TOE collects entropy from a source contained within the device to ensure sufficient randomness for secure key generation.

2.5.3 User Data Protection

The TOE ensures that administrative traffic is isolated from data plane traffic through the use of VLANs. The TOE also ensures that packets transmitted from the TOE do not contain residual information from previous packets. Any data that terminates before the minimum packet size is reached is padded with zeroes.

2.5.4 Identification and Authentication

Users authenticate to the TOE as administrators either via the local console or remotely using SSH for management of the TSF. All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE. Users are authenticated either through a locally-defined username/password combination or through SSH public key-based authentication, depending on the configuration of the TSF and the method used to access the TOE. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum security strength. As part of connecting to the TOE locally using the management workstation, password data will be obfuscated as it is being input.

2.5.5 Security Management

The TOE maintains distinct roles for user accounts: Limited, Admin, and Super. These roles define the management functions for each user on the TOE. A user who is assigned one of these roles is considered to be an administrator of the TOE, but the functions they are authorized to perform will differ based on the assigned role. The three roles are hierarchical, so each role has all of the privileges of the role(s) below it.

The Limited user is a read-only user, so any commands the user performs on the TOE will only allow the user to view different attributes and settings. The next level role is the Admin user who can perform all system configurations with the exception of managing users. Following the Admin role is the Super role. An administrator with the Super role can perform all system configurations including user management, including creating and deleting users on the TOE. All administration of the TOE can be performed locally using a management workstation with a terminal client, or remotely using an SSH remote terminal application.

2.5.6 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE stores passwords in an obfuscated format. The cryptographic module prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-512. The TOE maintains system time with either its local hardware clock or optionally with an NTP server synchronization. TOE software updates are acquired using SFTP and initiated using the CLI. The TOE software version is administratively verifiable and software updates are signed to provide assurance of their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

2.5.7 TOE Access

The TOE can terminate inactive sessions after an administrator-configurable time period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE displays a configurable warning banner prior to use of the TSF.

2.5.8 Trusted Path/Channels

The TOE establishes a trusted path to the TOE using SSH for remote administration. The TOE also establishes trusted channels for sending audit data to a remote server and for downloading software updates using SFTP (FTP over SSH).

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 September 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through 7 January 2016.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant to include all applicable NIAP and International interpretations through 7 January 2016.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profile:

- Protection Profile for Network Devices, version 1.1 [NDPP]

This PP claim also includes the NDPP Errata #3 that provides updates and clarifications to the NDPP.

3.5 Package Claims

The TOE claims exact conformance to the NDPP, version 1.1.

The TOE claims following optional SFRs that are defined in the appendices of the claimed PP:

- FCS_SSH_EXT.1

This does not violate the notion of exact conformance because the PP specifically indicates this as an allowable option and provides both the ST author and evaluation laboratory with instructions on how the SFR is to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are conformant with the claimed PP.

3.7 Conformance Claim Rationale

The NDPP states the following: “This is a Protection Profile (PP) for a network device. A network device in the context of this PP is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise. Examples of a ‘network device’ that should claim compliance to this PP include routers, firewalls, IDSs, audit servers, and switches that have Layer 3 functionality.”

The TOE is a family of hardware appliances that is designed to perform Ethernet switching for carrier networks. As such, it can be understood as a network switch. Therefore, the conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the NDPP.

Threat	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.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the NDPP.

Policy	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.

Table 4-2: TOE Organization Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the NDPP.

Assumption	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Table 4-3: TOE Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

This section identifies the security objectives of the TOE. These objectives have been taken directly from the NDPP.

Objective	Objective Definition
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.

Table 4-4: TOE Objectives

4.4.2 Security Objectives for the Operational Environment

The TOE's operating environment must satisfy the following objectives:

Objective	Objective Definition
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.

Table 4-5: TOE Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE

objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with italicized text.
- **Refinement:** allows the addition of details. Indicated with bold and italicized text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP for a particular operation (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
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_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1	SSH
User Data Protection	FDP_RIP.2	Full Residual Information Protection
Identification and Authentication	FIA_PMG_EXT.1	Password Management
	FIA_UAU_EXT.2	Password-based Authentication Mechanism

Class Name	Component Identification	Component Name
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UIA_EXT.1	User Identification and Authentication
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
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	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	Trusted Update
TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class FAU: Security Audit

6.3.1.1 *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 and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) [Specifically defined auditable events listed in ***Table 6-2***].

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of ***Table 6-2***].

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
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).
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.
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.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 6-2: Auditable Events

Application Note: *The severity is defined as log-level as well as a numerical representation of log-level. Please refer to Section 8.1.1 for the full list.*

6.3.1.2 *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.

6.3.1.3 *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 [SSH] protocol.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *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 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-3, "Digital Signature Standard");]

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

6.3.2.2 *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.

6.3.2.3 *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, [*no other modes*]] and cryptographic key sizes 128-bits and 256-bits that meets the following:

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

6.3.2.4 *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 [(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]

that meets the following:

Case: RSA Digital Signature Algorithm

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

6.3.2.5 *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, SHA-512] and message digest sizes [160, 256, 512] bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

6.3.2.6 *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, SHA-512], key size [*greater than block size, less than block size, equal to block size*], and message digest sizes [160, 256, 512] bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

6.3.2.7 *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 [NIST Special Publication 800-90 using [Hash_DRBG (any)]] seeded by an entropy source that accumulated entropy from [a software-based noise source].

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

6.3.2.8 *FCS_SSH_EXT.1 SSH*

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [5656, 6668].

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 [*32768*] bytes in an SSH transport connection are dropped.

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

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

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha2-256].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

6.3.3 Class FDP: User Data Protection

6.3.3.1 *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, deallocation of the resource from] all objects.

6.3.4 Class FIA: Identification and Authentication

6.3.4.1 *FIA_PMG_EXT.1 Password Management*

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;

6.3.4.2 *FIA_UAU_EXT.2 Password-based Authentication Mechanism*

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [SSH *public key-based authentication mechanism*] to perform administrative user authentication.

6.3.4.3 *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.

6.3.4.4 *FIA_UIA_EXT.1 User Identification and Authentication*

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;
- [no other actions]

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.

6.3.5 Class FMT: Security Management

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

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

Application Note: *The TSF provides three administrative roles, each with differing levels of privilege.*

6.3.5.2 ***FMT_SMF.1 Specification of Management Functions***

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

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

6.3.5.3 ***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.

Application Note: *The Authorized Administrator can be a user with the 'Limited', 'Admin', or 'Super' administrative role assigned to their account. Each of these roles has a different set of authorizations associated with them.*

6.3.6 Class FPT: Protection of the TSF

6.3.6.1 ***FPT_APW_EXT.1 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.

6.3.6.2 ***FPT_SKP_EXT.1 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.

6.3.6.3 ***FPT_STM.1 Reliable Time Stamps***

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

6.3.6.4 ***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.

6.3.6.5 ***FPT_TUD_EXT.1 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 [digital signature mechanism] prior to installing those updates.

6.3.7 Class FTA: TOE Access

6.3.7.1 ***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.

Application Note: *'Security Administrator' in this case is considered to be synonymous with Authorized Administrator as defined in FMT_SMR.2.*

6.3.7.2 ***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.

Application Note: *'Security Administrator' in this case is considered to be synonymous with Authorized Administrator as defined in FMT_SMR.2.*

6.3.7.3 ***FTA_SSL.4 User-initiated Termination***

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

6.3.7.4 ***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.

Application Note: *'Security Administrator' in this case is considered to be synonymous with Authorized Administrator as defined in FMT_SMR.2.*

6.3.8 Class FTP: Trusted Path/Channels

6.3.8.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

FTP_ITC.1.1 The TSF shall use [SSH] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [[*update 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 [*remote transmission of audit data, acquisition of software updates*].

6.3.8.2 *FTP_TRP.1 Trusted Path*

FTP_TRP.1.1 The TSF shall use [SSH] 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 administration actions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the claimed PP as well as a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PP.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are consistent with the claimed PP.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

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.

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

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

ADV_FSP.1.2C

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

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

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

7.1.1.3 *Evaluator action elements:*

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.

7.2 Class AGD: Guidance Documents

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 ***Developer action elements:***

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 ***Content and presentation elements:***

AGD_OPE.1.1C

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

AGD_OPE.1.2C

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

AGD_OPE.1.3C

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

AGD_OPE.1.4C

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

AGD_OPE.1.5C

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

AGD_OPE.1.6C

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

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 ***Evaluator action elements:***

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 ***Developer action elements:***

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 ***Content and presentation elements:***

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.

7.2.2.3 ***Evaluator action elements:***

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.

7.3 Class ALC: Life-cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 ***Developer action elements:***

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 ***Content and presentation elements:***

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 ***Evaluator action elements:***

ALC_CMC.1.1E

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

7.3.2 TOE CM coverage (ALC_CMS.1)

7.3.2.1 ***Developer action elements:***

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 ***Content and presentation elements:***

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.

7.3.2.3 ***Evaluator action elements:***

ALC_CMS.1.1E

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

7.4 Class ATE: Tests

7.4.1 Independent testing -- conformance (ATE_IND.1)

7.4.1.1 ***Developer action elements:***

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 ***Content and presentation elements:***

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 ***Evaluator action elements:***

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.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

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.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. They include Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, TOE Access and Trusted Path / Channels

8.1 Security Audit

8.1.1 FAU_GEN.1:

The TSF generates audit records of the TOE's behavior. Specifically, the following security-relevant events are audited:

Requirement	Auditable Events
FAU_GEN.1	Start-up and shut-down of the audit functions.
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment/Termination of an SSH session.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.
FIA_UAU_EXT.2	All use of the authentication mechanism.
FPT_STM.1	Changes to the time.
FPT_TUD_EXT.1	Initiation of update.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.
FTA_SSL.4	The termination of an interactive session.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.

Table 8-1: Audit Events

Auditing is always functional and thus cannot be disabled or enabled. As a result, the starting up and shutting down of audit functions is synonymous with the startup and shutdown of the TOE. Within each of the audited events listed above, the TOE records at least the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Additional attributes that the TOE records for specific events have been listed in the Additional Details Column of Table 6-2. Date and time is derived from the TOE's hardware clock or optionally from system time that is synchronized to an NTP server.

The TOE logs all events related to startup/shutdown, external communications, user authentication, and user management (user creation/deletion, password changes, role changes) in the security log. All administrative commands not related to user management are recorded in the command log.

8.1.2 FAU_GEN.2:

Each audit record contains the date and time, severity, user, and message about the event. The TOE provides the audit record in the following format: <day> <year> <date-time>: <severity> <id string> <message string>. The "id string" field displays the IP address where the administrative action originated,

while the "message string" field displays a short summary of the user actions, which includes the identity of the user performing the action.

8.1.3 FAU_STG_EXT.1:

The TOE is not an audit server. In the evaluated configuration, the TOE is configured to transmit its collected audit data to an SFTP server in the Operational Environment, which protects FTP traffic using an SSH trusted channel. The security log can be transferred automatically on a periodic basis but command log data is transferred manually. Each of these operations can be done by an authorized administrator with Super level privileges. The command logs are contained in the directory /flash1/log and are called cmdLog.0 etc. These files can be sent individually to the SFTP server by running the command file xput cmdLog.0 cmdLog.0

Locally, the TOE allocates four files each for the command and security logs. When one file reaches the maximum size, the next file is used to store the logs. When all four log files have reached the maximum capacity of 32 MB, the oldest file becomes the newest file to be overwritten with current log information. An authorized administrator with Super level privileges is able to delete the logs.

8.2 Cryptographic Support

8.2.1 FCS_CKM.1:

The TOE implements a NIST SP 800-56A conformant key generation mechanism for Diffie-Hellman key establishment schemes. Specifically, the TOE complies with the NIST SP 800-56A key agreement scheme (KAS) primitives that are defined in section 5.6 of the SP. This is used to generate the keys for diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.

8.2.2 FCS_CKM_EXT.4:

The TOE performs key and cryptographic material destruction. The OpenSSL cryptographic module automatically zeroizes sensitive data via API function calls for any data that resides in temporary memory. This includes SSH host and session key data that is needed to establish SSH communications. In each case, the cryptographic data is overwritten in memory with all zeroes when no longer in use before the memory is freed. Similarly, plaintext password data that is entered by a user as part of the authentication process will be zeroized from temporary memory once the password has been hashed. Any SSH keys that are stored persistently on the TOE can be deleted by an administrator with Admin or Super privilege level using the "ssh server key delete" command which overwrites the stored key data with pseudo-random bits.

8.2.3 FCS_COP.1(1):

The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128 and 256 bits) as described NIST SP 800-38A. The TOE provides AES-CBC encryption and decryption in support of SSH communications. The TOE's AES implementation is validated under CAVP, certificate #3522.

8.2.4 FCS_COP.1(2):

The TOE provides cryptographic digital signature services using RSA in support of SSH communications. All RSA modulus sizes are 2048 its or larger. The TOE supports elliptic curve cryptography to support ECDH key exchange for SSH; however, it does not support ECDSA digital signatures. The TOE's RSA implementation is validated under CAVP, certificate #1808.

8.2.5 FCS_COP.1(3):

The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard". The TOE uses cryptographic hashing services in support of SSH key establishment as well as session establishment for SSH communications. The TOE's SHS implementation is validated under CAVP, certificate #2904.

8.2.6 FCS_COP.1(4):

The TOE provides keyed-hash message authentication services using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 as specified in FIPS Pub 198-1,"The Keyed-Hash Message Authentication Code," and FIPS 180-3, "Secure Hash Standard". All key sizes relative to block sizes are supported by the HMAC implementation. The TOE's HMAC implementation is validated under CAVP, certificate #2250.

8.2.7 FCS_RBG_EXT.1:

The TOE implements a NIST-approved deterministic random bit generator (DRBG). The DRBG used by the TOE is a NIST Special Publication 800-90 Hash_DRBG. The TOE models uniformly provide a software-based entropy source as described in the proprietary entropy specification. The DRBG is seeded with a minimum of 256 bits of entropy so that it is sufficient to ensure full entropy for 256-bit keys, which are the largest keys generated by the TSF. The TOE's DRBG implementation is validated under CAVP, certificate #881.

8.2.8 FCS_SSH_EXT.1:

The TOE implements SSHv2 for remote CLI sessions that complies with RFCs 4251, 4252, 4253, 4254, 5656, and 6668. There is no SSHv1 implementation on the TOE. SSH is used both for remote administrators to connect securely to the TOE and for the TOE to connect to a remote SFTP server for transmission of audit data and receipt of system updates.

Large packets, defined here as being greater than 32,768 bytes, are detected by the SSH implementation and dropped by the SSH process.

The TOE implementation of SSHv2 supports RSA signature verification for authentication in addition to password-based authentication.

The TOE implementation of SSHv2 supports AES-CBC-128 and AES-CBC-256 for its transport algorithms, SSH_RSA for its public key algorithm, and either of hmac-sha1 or hmac-sha2-256 for its data integrity algorithms. The allowed key exchange methods are diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.

8.3 User Data Protection

8.3.1 FDP_RIP.2:

The TOE internally processes ingress frames and forwards the traffic to specific egress ports based on the services associated with the traffic frames. The TOE does not explicitly authorize or deny other than the internal processing of the service attributes, ACLs, and MAC learning tables used to determine the egress ports to which the ingress ports will be forwarded. The management plane (traffic to the TOE) is treated as a network in the same manner as any data plane (traffic through the TOE) networks and traffic for each VLAN is handled in independent threads. This ensures that traffic does not "bleed over" from one network to another. Additionally, any data that terminates before the minimum packet size is reached is padded with zeroes

The TOE also ensures that packets transmitted from the product over all networks do not contain any residual information by zeroizing the data upon allocation of memory. This ensures that if a new packet reuses the same memory location as a previous packet, the location is zeroized first before the new packet is constructed. In certain instances the TOE may also zeroize data immediately after the memory is deallocated; which would occur in addition to the zeroization function that occurs when memory is allocated for a packet.

8.4 Identification and Authentication

8.4.1 FIA_PMG_EXT.1:

The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and the special characters of "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Passwords can be up to 128 characters long and an authorized administrator with the Super privileges can set the minimum length to any positive value up to 128. In the evaluated configuration, minimum password length must be set to 15 characters or greater.

8.4.2 FIA_UAU_EXT.2:

By default, the TOE queries its local database for user authentication. Users can be authenticated either by username and password, or by username and SSH public key if authenticating remotely using SSH. Users are not allowed to perform any functions on the TOE without first being successfully identified and authenticated by the TOE's authentication method. At initial login, locally or through SSH, the administrative user is prompted to provide a username. The user provides either their username and password or their username and SSH key, depending on the method of authentication the TOE is configured to use. The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful.

8.4.3 FIA_UAU.7:

When a user enters their password into the CLI at the local console, the password characters entered by the user are obscured by the TSF not echoing them back to the console as they are being typed. If an administrator authentication attempt fails, a generic "invalid login" message is returned so that specific information about the nature of the failure is not disclosed.

8.4.4 FIA_UIA_EXT.1:

See FIA_UAU_EXT.2 above.

8.5 Security Management

8.5.1 FMT_MTD.1:

The TOE restricts access to the management functions to an authorized administrator. Administrative authorities are separated into pre-defined administrative roles, each of which have a fixed set of hierarchical privileges. These roles are as follows:

- Limited: Read-only access to system configuration information.
- Admin: All access given to Limited users plus the ability to configure all TSF data and functions except for user and authentication data.
- Super: All access given to Admin users plus the ability to modify TOE users and the authentication mechanism used by the TOE.

For the purposes of the TSF, an 'authorized administrator' is any administrator on the TOE with sufficient privilege to perform the desired TOE function. For example, a Limited user is acting as an 'authorized administrator' in the context of FPT_TUD_EXT.1.1 if they are querying the TOE's software version because this is within the scope of their assigned privileges. However, only an Admin or Super user would be able to act as an 'authorized administrator' when actually initiating a TOE software update as per FPT_TUD_EXT.1 because a Limited user does not have this privilege.

8.5.2 FMT_SMF.1:

The TOE provides all the capabilities necessary to securely manage the TSF. The TOE is managed through a CLI which provides different levels of administrative control for each administrative role. The following table describes the management functions provided by the TOE along with the minimum role level required for an administrator to be considered an 'authorized administrator' for this function as defined by the NDPP:

Management Function	Minimum Role
Creation of user accounts and assignment to administrative roles	Super
Specification of maximum idle time for an administrative session before it is terminated	Admin
Configuration of minimum password length	Super
Configuration and manual transfer of audit data to remote storage location	Super
Manual setting of system time	Admin
Configuration of NTP server connection	Admin
Management of cryptographic functions	Admin
Configuration of banner text	Super
Initiation of system software/firmware update	Admin

Table 8-2: TSF Management Functions

8.5.3 FMT_SMR.2:

The TOE maintains three administrative roles: Limited, Admin, and Super. Users with any of these roles have the capability to manage the TSF locally or remotely and are considered to be administrators of the TSF for the functions that are assigned to their respective roles. An administrator may only have one role assigned to their account.

8.6 Protection of the TSF

8.6.1 FPT_APW_EXT.1:

Administrator passwords are not stored by the TOE in plaintext. All administrative passwords are hashed using SHA-512 and the hash is what is stored by the TOE. There is no function provided by the TOE to display a password value in plaintext.

8.6.2 FPT_SKP_EXT.1:

The TOE does not provide a mechanism to view secret keys and key material. Public key data that is stored on the TOE can be viewed by an authorized administrator (Admin or Super). Key data that is resident in volatile memory cannot be accessed by an administrative command. Any persistent key data is stored in the underlying filesystem of the OS on internal flash memory. The TOE's management interfaces do not provide any direct access to the file system so there is no administrative method of accessing this data.

An authorized administrator (Admin or Super) has the ability to delete SSH keys using the "ssh server key delete" command which overwrites key data with pseudo-random bits.

8.6.3 FPT_STM.1:

The TOE provides a source of date and time information, used in audit timestamps and in determining whether an administrative session has gone in-active. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive time from one or more NTP servers. If using the local clock, an authorized administrator (Admin or Super) has the ability to manually set the time using the CLI.

8.6.4 FPT_TST_EXT.1:

Upon the startup of the TOE, multiple Power-On Self Tests (POSTs) are run. The POSTs provide environmental monitoring of the TOE's components, in which early warnings can prevent whole component failure. The following self-tests are performed:

- Software integrity: hashed and validated against a known SHA-256 value which in storage that can only be modified when a software update is performed.
- Cryptographic module integrity: the cryptographic algorithm implementation is run through known answer tests to ensure they are operating properly.
- Hardware integrity: the field-programmable gate arrays (FPGAs) and data plane hardware are tested for correct operation.

In the event that a self-test fails, the TOE will automatically reboot. If the TSF has been corrupted or the hardware has failed such that rebooting will not resolve the issue, an administrator (Admin or Super) will need to factory reset the TOE and/or replace the failed hardware component. These tests are sufficient to validate the correct operation of the TSF because they verify that the SAOS software has not been tampered with and that the underlying hardware does not have any anomalies that would cause the software to be executed in an unpredictable or inconsistent manner.

8.6.5 FPT_TUD_EXT.1:

The TOE provides the ability for an authorized administrator with the Admin or Super role to update its software. The TOE has an SFTP client that is used to retrieve software updates from an SFTP server. This can be a server maintained by Ciena or one maintained by the organization operating the TOE, in which case updates are shipped on read-only physical media when made available by Ciena. In the evaluated configuration, the TOE is configured by an authorized administrator with Admin or Super privileges to only accept signed updates. Updates provided by Ciena are signed using a 2048-bit RSA certificate that is traceable back to an Entrust root CA. Prior to installation of the software image, the certificate is checked to ensure it is valid. If the digital signature is deemed invalid, the update process stops and the invalid software image will be deleted from the TOE's storage. This process does not require administrative action and there is no administrative override capability.

8.7 TOE Access

8.7.1 FTA_SSL_EXT.1:

An authorized administrator with the Admin or Super role can configure maximum inactivity times for both local and remote administrative sessions using the "system shell set global-inactivity-timeout" command. When a session is inactive for the configured period of time the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed. The default value for the inactivity timer is 10 minutes, but it can be set to as little as 1 minute.

8.7.2 FTA_SSL.3:

The TOE will terminate a session after an administrator-defined period of inactivity. As stated above, the Admin and Super level administrators have the ability to define the inactivity period.

8.7.3 FTA_SSL.4:

The TOE provides the ability for administrators (Limited, Admin, or Super) to manually terminate their own sessions by issuing as many "quit" commands as is necessary to navigate to the highest level of the CLI, followed by an "exit" command. Additionally, when managing the TOE remotely, the terminal application used on the management workstation will typically terminate the SSH session if the application itself is closed.

8.7.4 FTA_TAB.1:

The TOE allows administrators with Super level privileges to specify a login banner that will display when any administrator opens either a local or remote connection to the TOE. This is configured by uploading a text file with the desired banner text to the TOE's filesystem storage and then configuring the TOE to display the contents of that file as the login banner.

8.8 Trusted Path/Channels

8.8.1 FTP_ITC.1:

The TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. In the evaluated configuration, the TOE is configured to transmit audit data to a remote FTP server using

SFTP, which uses SSH to secure FTP communications. Updates to the TOE software can also be securely delivered to the TOE using SFTP. The TOE uses OpenSSH 6.6P1 to support SSH communications.

Note that in order to enable a FIPS-compliant mode of operation (which restricts the supported cryptographic algorithms to those specified in this Security Target), it is necessary to enter the command 'system security set security-mode normal encryption-mode fips-140-2 software-signing-mode on' as part of the initial configuration of the TOE.

8.8.2 FTP_TRP.1:

All remote administrative communications take place over a secure encrypted SSHv2 session. The TOE uses OpenSSH to perform SSH functions.

Note that in order to enable a FIPS-compliant mode of operation (which restricts the supported cryptographic algorithms to those specified in this Security Target), it is necessary to enter the command 'system security set security-mode normal encryption-mode fips-140-2 software-signing-mode on' as part of the initial configuration of the TOE.