In the evaluated configuration this connection is secured using TLS.

Ciena 8700 Packetwave Platform with SAOS 8.5

Security Target

ST Version: 1.0
May 11, 2017

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
304 Sentinel Drive
Suite 1160
Annapolis Junction, MD 20701

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 8700 Packetwave Platform with SAOS 8.5 Security Target
ST Version:	1.0
ST Publication Date:	May 11, 2017
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 and 2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator	A user who is assigned any of the three administrative roles defined for the TOE: Limited, Admin, and Super. While these are all considered to be administrators, the assigned role determines the specific level of privilege a given administrator has to interact with TOE functions and data.

Table 1: Customer Specific Terminology

Term	Definition
Security Administrator	The claimed Protection Profile defines a single Security Administrator role that is authorized to manage the TOE and its data. Since this particular TOE defines three separate administrator roles, an administrator is considered to be the Security Administrator for only the management functions that are associated with their assigned role.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

Table 2: CC Specific Terminology

1.1.4 Acronyms

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

Acronym	Definition
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
FTP	File Transfer Protocol
IP	Internet Protocol
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generator
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell

ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

Table 3: Acronym Definition

1.1.5 References

[1] Collaborative Protection Profile for Network Devices, version 1.0 (NDcPP)
[2] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[6] NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009
[7] NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, December 2001
[8] FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[9] FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[10] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS) March 2012
[11] FIPS PUB 197 Advanced Encryption Standard November 26 2012
[12] FIPS PUB 198-1 Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

1.2 TOE Reference

The TOE is the Ciena 8700 Packetwave Platform. There are two models of the TOE: one model with a 4-slot chassis and another model with a 10-slot chassis. Both of these models run on the Ciena Service Aware Operating System (SAOS) 8.5 and have uniform security functionality between them.

1.3 TOE Overview

Ciena 8700 Packetwave Platform (also known as the Ciena 8700 or the TOE) is a network device that includes hardware and software and has two separate models. The TOE has one model with a 4-slot chassis and the other with a 10-slot chassis. The basic difference between the two models in Section 2.4 is the number of module slots and number of power supplies. Both models use the same Service Aware Operating System (SAOS) v8.5 management shell with identical security functionality. The software binary images and underlying processor architecture are also identical. The TOE is managed through a command-line interface (CLI) that is available both locally and remotely. Remote administration can be performed either out-of-band (via a dedicated management port) or in-band (via a network traffic port configured to direct traffic inbound to the TOE's management plane).

The following figure depicts the TOE boundary:

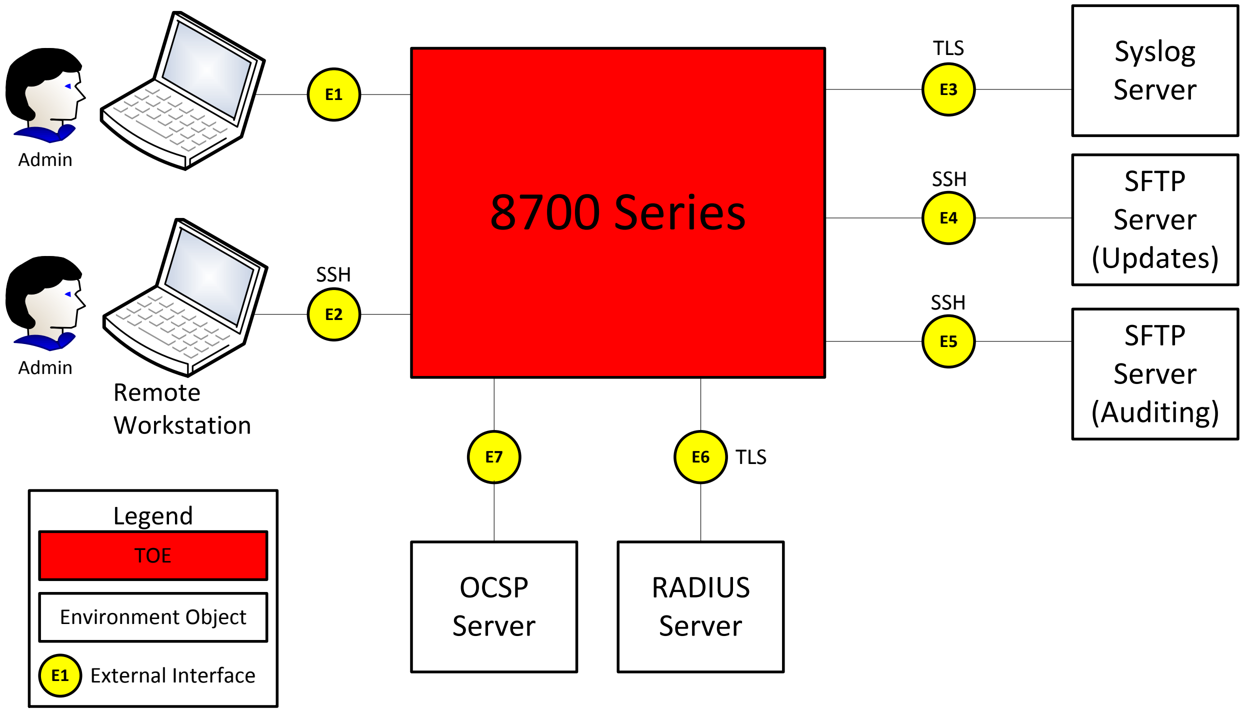

Figure 1: TOE Boundary

There are seven security-relevant external interfaces supported by the Ciena 8700. The intended usage and security of each of these interfaces is described in the TOE Summary Specification below. The audit records produced by the TOE are transmitted to a remote syslog server over TLS (for syslog audit records) and to a remote audit server over SFTP (for security, event, and command log records). Software/firmware updates for the TOE can be transferred from a remote server to the TOE via SFTP. The OCSP server interface is used to verify the revocation status of certificates. The RADIUS server interface can be used for administrator authentication (although administrator credentials can also be defined by the TOE itself). All RADIUS communications are secured using TLS. It should be noted that the primary purpose of this product is to perform packet networking. However, this is outside the scope of the TOE because it is not a security function that is specified in the claimed cPP and therefore excluded from Figure 1.

1.4 TOE Type

The TOE type for this product is Network Device. The product is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDcPP 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 NDcPP says that example devices that fit this definition include routers, firewalls, intrusion detection systems, audit servers, and switches that have Layer 2 functionality. The TOE is a packet networking switch that performs second tier aggregation of network traffic that interfaces with an IP/MPLS domain.

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 following table describes the TOE components in the evaluated configuration:

Component	Hardware Components	Software Version
Ciena 8700 Packetwave Platform	4-slot or 10-slot chassis	SAOS Version 8.5

Table 4: Evaluated Components of the TOE

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
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.
OCSP Server	The OCSP server is used by the TOE to validate certificate revocation status.
SFTP Server	The SFTP server is used for storage of TOE software/firmware updates that can be retrieved remotely by the TSF. The Administrator can also transfer the security, event, and command logs to another or the same SFTP server over this interface. Communications over this interface are secured using SFTP via SSH where the TOE is acting as an SSH client.
Syslog Server	A remote server that is used to store syslog audit records that the TOE transmits to it. The TOE communicates with the syslog server using TLS.
RADIUS Server	The RADIUS server enables user authentication and is secured using TLS. Note that while RADIUS authentication is supported by the TOE, the use of it is not mandatory.

Table 5: 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

There are no optional components that are omitted from the installation process.

2.3.2 Installed but Requires a Separate License

There are no excluded components that are installed and require a separate license.

2.3.3 Installed but Not Part of the TSF

- **Non-FIPS mode of operation -** The product includes a FIPS compliant mode of operation which allows the TOE to use only approved ciphersuites 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.
- **Remote Telnet interface -** The product 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.
- **DHCP Server interface -** The product includes this interface that supports communications between the TOE and a DHCP Server in the Operational Environment; however, it will be disabled in the evaluated configuration.
- **SNMP interface -** The product includes this interface which may be used by external entities to communicate with it using the SNMP protocol in order to configure or read the device state. It also provides the ability to generate SNMP traps that are sent to external SNMP tools. In the evaluated configuration, this will be disabled.
- **TACACS+ Interface -** The product supports this interface which is used to provide authentication services, but will be disabled in this evaluated configuration.
- **Network Configuration Protocol (NETCONF) –** the installation, deletion, and manipulation of network configuration over SSH will not be included.
- **Diagnostic (Diag) role -** The product supports a Diagnostic role; however, this role is only used for non-security-relevant service functionality and will be excluded from the evaluated configuration when the TOE is in an operational state.

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 Ciena 8700 has two separate models that are pictured below. They have no differences in processor type, software/firmware, or security-related functions. However, they do differ in hardware because of their chassis size, number of ports, and network capacity for switched traffic. The Ciena 8700 has two processors: CTX - P4080NSE7PNC and LM-200 series - NXP/Freescale P2020. Hardware cryptologic acceleration is not being used for either processor.

Figure 2: 10-Slot Chassis

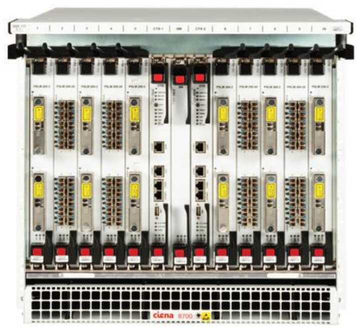

Figure 3: 4-Slot Chassis

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. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted Path/Channels

2.5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The TOE transmits syslog audit data securely to a remote syslog server using TLS. The TOE also maintains security, event, and command logs internally. The contents of these logs can be configured to be transferred automatically to a remote SFTP server. Each audit record contains the subject 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 can be deleted by a user with the Super role but it is read-only for all other roles. Local audit data is overwritten when the local storage space is full.

2.5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS trusted communications. Asymmetric keys that are used by the TSF are generated in accordance with FIPS PUB 186-4 and are established in accordance with NIST SP 800-56A and NIST SP 800-56B. The TOE uses NIST-validated cryptographic algorithms (certificates DSA #1198, RSA #2445, ECDSA #1092, KAS ECC #120, AES #4470, SHS #3682, HMAC #2967, DRBG #1454) to provide cryptographic services. Ciena's implementation of these has been validated to ensure that the algorithms are appropriately strong and correctly implemented for use in trusted communications. The TOE collects entropy from software-based sources contained within the device to ensure sufficient randomness for secure key generation. Cryptographic keys are destroyed when no longer needed.

2.5.3 Identification and Authentication

Users authenticate to the TOE 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 other than viewing the pre-authentication warning banner. Users can be authenticated using RADIUS by connecting to a RADIUS server in the Operational Environment over TLS. Depending on the configuration of the TSF and the method used to access the TOE, the user can also authenticate using a locally-defined username/password combination (as opposed to credentials being defined in RADIUS) or through SSH public key-based authentication. 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. The TSF connects to an OCSP server to verify certificate revocation status and includes a mechanism internally to determine the validity of certificates. The TOE also provides support for X.509v3 certificates for authentication.

2.5.4 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. A Limited user has read-only privileges for certain TOE functions and data whereas a user with the Admin role has read/write permission over most TOE functionality. The Super role is the highest role and can perform read/write operations on all TOE functions and data, including those functions that the Admin role is not authorized to perform. 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.

2.5.5 Protection of the TSF

The TOE is able to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE provides no interface for the disclosure of secret cryptographic data, and administrative passwords themselves are hashed using SHA-512. The TOE maintains system time locally based on an administratively-defined time. 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 validates its own correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

2.5.6 TOE Access

The TSF 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 its administrative use.

2.5.7 Trusted Path/Channels

The TOE establishes a trusted path to the TOE using SSH for remote administration. The TOE establishes trusted channels using TLS for sending syslog audit data to a remote syslog server and SSH for sending stored security, command, and event log data to a remote SFTP server. In addition, the TOE uses the SFTP interface to download updates and store log files. The TOE may also connect to the RADIUS server for user authentication using TLS.

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 May 11, 2017.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through May 11, 2017.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- collaborative Protection Profile for Network Devices, version 1.0 [NDcPP]

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE:

- TD0090
- TD0095
- TD0112
- TD0117
- TD0130
- TD0143
- TD0150
- TD0152
- TD0154
- TD0155
- TD0164
- TD0168
- TD0182
- TD0183
- TD0185
- TD0186
- TD0187
- TD0199
- TD0200

Note that Technical Decisions were not considered to be applicable if any of the following conditions were true:

- The Technical Decision does not apply to the NDcPP
- The Technical Decision applies to an SFR that was not claimed by the TOE
- The Technical Decision applies to an SFR selection or assignment that was not chosen for the TOE
- The Technical Decision only applies to one or more Application Notes in the NDcPP and does not affect the SFRs or how the evaluation of the TOE is conducted
- The Technical Decision was superseded by a more recent Technical Decision
- The Technical Decision is issued as guidance for future versions of the NDcPP

3.5 Package Claims

The TOE claims exact conformance to the NDcPP, which is conformant with CC Part 3.

The TOE claims following Selection-Based SFRs that are defined in the appendices of the claimed PP:

- FCS_SSHC_EXT.1
- FCS_SSHS_EXT.1
- FCS_TLSC_EXT.2
- FIA_X509_EXT.1
- FIA_X509_EXT.2
- FIA_X509_EXT.3

The TOE claims the following Optional SFRs that are defined in the appendices of the claimed cPP:

- FAU_STG.1
- FMT_MOF.1(1)/Audit
- FMT_MTD.1(1)/AdminAct

This does not violate the notion of exact conformance because the cPP specifically indicates these as allowable selections and options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the NDcPP.

3.7 Conformance Claim Rationale

The NDcPP states the following: “This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure within the network… Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches.”

The TOE is a network device composed of hardware and software that is designed to perform packet switching for large quantities of packet traffic. 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 NDcPP.

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNEL	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines

	the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

Table 6: 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 NDcPP.

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 7: Organizational 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 NDcPP.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized

	entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_ PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_ SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

Table 8: 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

The NDcPP does not define any security objectives for the TOE.

4.4.2 Security Objectives for the Operational Environment

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

Objective	Objective Definition
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
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.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

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 guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Table 9: 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.

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** text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with <u>underlined</u> 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 and/or separated by a "/" with a notation that references the function for which the iteration is used, e.g. "/TrustedUpdate" for an SFR that relates to update functionality

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 (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)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG_EXT.1	Protected Audit Event Storage
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(4)	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_TLSC_EXT.2	TLS Client Protocol with Authentication

Class Name	Component Identification	Component Name
Identification and Authentication (FIA)	FIA_PMG_EXT.1	Password Management
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_X509_EXT.1	X509 Certificate Validation
	FIA_X509_EXT.2	X509 Certificate Authentication
	FIA_X509_EXT.3	X509 Certificate Requests
Security Management (FMT)	FMT_MOF.1(1)/Audit	Management of Security Functions
	FMT_MOF.1(1)/Trusted Update	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_MTD.1/AdminAct	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF (FPT)	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)	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
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 10: 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 comprising:
    - Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
    - Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).

- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- Starting and stopping services (if applicable)
- [no other actions]*;*

d) Specifically defined auditable events listed in Table **11**;

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 **11**

Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure. Non-TOE endpoint of connection (IP Address).
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure. Non-TOE endpoint of connection (IP Address).
FCS_TLSC_EXT.2	Failure to establish a TLS session.	Reason for failure.
FIA_PMG_EXT.1	None.	None.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP Address).
FIA_UAU.7	None.	None.
FIA_UIA_EXT.1	All use of identification mechanism.	Provided user identity, origin of the attempt (e.g., IP Address).
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate.	Reason for failure.
FIA_X509_EXT.2	All use of identification and authentication mechanism.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1(1)/ Audit	Modification of behavior of the transmission of audit data to an external IT entity.	None.
FMT_MOF.1(1)/TrustedUpdate	Any attempt to initiate a manual update	None.

FMT_MTD.1	All management activities of TSF data.	None.
FMT_MTD.1/Admin Act	Modification, deletion, generation/import of cryptographic keys.	None
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	No additional information.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	Identification of the claimed user identity.

Table 11: Auditable Events

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.1 Security Audit Trail Storage*

FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3.1.4 *FAU_STG_EXT.1 Protected Audit Event 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 according to FTP_ITC.1.

FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3

The TSF shall [overwrite previous audit records according to the following rule: [*overwrite oldest log file of that audit record type*]] when the local storage space for audit data is full.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation*

FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4].

6.3.2.2 *FCS_CKM.2 Cryptographic Key Establishment*

FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]

6.3.2.3 *FCS_CKM.4 Cryptographic Key Destruction*

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
    - instructs a part of the TSF to destroy the abstraction that represents the key]]

that meets the following: No Standard.

6.3.2.4 *FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)*

FCS_COP.1.1(1)

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC, GCM] mode and cryptographic key sizes [128 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].

6.3.2.5 *FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)*

FCS_COP.1.1(2)

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits*]]
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256, 384, 521 bits*]]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4].

6.3.2.6 *FCS_COP.1(3) Cryptographic Operation (Hash Algorithm)*

FCS_COP.1.1(3)

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] that meet the following: ISO/IEC 10118-3:2004.

6.3.2.7 *FCS_COP.1(4) Cryptographic Operation (Keyed Hash Algorithm)*

FCS_COP.1.1(4)

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] and cryptographic key sizes [*greater than block size, less than block size, equal to block size*], and message digest sizes [160, 256, 512] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.3.2.8 *FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)*

FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[2] software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.3.2.9 *FCS_SSHC_EXT.1 SSH Client Protocol*

FCS_SSHC_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [5647, 5656, 6668].

FCS_SSHC_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_SSHC_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [*32,768*] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHC_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [ssh-rsa, ecdsa-sha2-nistp256] and [ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] and [no other MAC algorithms] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7

The TSF shall ensure that [ecdh-sha2-nistp256] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8

The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

FCS_SSHC_EXT.1.9

The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [*a list of trusted certificate authorities*] as described in RFC 4251 section 4.1.

6.3.2.10 *FCS_SSHS_EXT.1 SSH Server Protocol*

FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFCs, 4251, 4252, 4253, 4254, and [5647, 5656, 6668].

FCS_SSHS_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_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [*32,768*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH transport implementation uses [ssh-rsa, ecdsa-sha2-nistp256] and [ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] and [no other MAC algorithms] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

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

FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

6.3.2.11 *FCS_TLSC_EXT.2 TLS Client Protocol with Authentication*

FCS_TLSC_EXT.2.1

The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1,1(RFC 4346)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

Optional Ciphersuites:

- [TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289]

FCS_TLSC_EXT.2.2

The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.2.3

The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.2.4

The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves.

FCS_TLSC_EXT.2.5

The TSF shall support mutual authentication using x.509v3 certificates.

6.3.3 Class FIA: Identification and Authentication

6.3.3.1 *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.

6.3.3.2 *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, remote password-based authentication*]] to perform administrative user authentication.

6.3.3.3 *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.

6.3.3.4 *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.

6.3.3.5 *FIA_X509_EXT.1 X509 Certificate Validation*

FIA_X509_EXT.1.1

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.3.3.6 *FIA_X509_EXT.2 X509 Certificate Authentication*

FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS, SSH], and [no additional uses].

FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

6.3.3.7 *FIA_X509_EXT.3 X509 Certificate Requests*

FIA_X509_EXT.3.1

The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.3.4 Class FMT: Security Management

6.3.4.1 *FMT_MOF.1(1)/Audit Management of Security Functions Behavior*

FMT_MOF.1.1(1)/Audit

The TSF shall restrict the ability to determine the behavior of, modify the behavior of the functions transmission of audit data to an external IT entity to Security Administrators.

6.3.4.2 *FMT_MOF.1(1)/TrustedUpdate Management of Security Functions Behavior*

FMT_MOF.1.1(1)/TrustedUpdate

The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

6.3.4.3 *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.

6.3.4.4 *FMT_MTD.1/AdminAct Management of TSF Data*

FMT_MTD.1.1/AdminAct

The TSF shall restrict the ability to modify, delete, generate/import the cryptographic keys to Security Administrators.

6.3.4.5 *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 configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- [Ability to configure audit behavior;
- Ability to configure the cryptographic functionality;
- Ability to configure thresholds for SSH rekeying]

6.3.4.6 *FMT_SMR.2 Restrictions on Security Roles*

FMT_SMR.2.1

The TSF shall maintain the roles:

- Security 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

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

are satisfied.

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 *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.

6.3.5.2 *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.

6.3.5.3 *FPT_STM.1 Reliable Time Stamps*

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.3.5.4 *FPT_TST_EXT.1 TSF Testing*

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*software integrity, cryptographic module integrity, hardware integrity*].

6.3.5.5 *FPT_TUD_EXT.1 Trusted Update*

FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [the most recently installed version of the TOE firmware/software].

FPT_TUD_EXT.1.2

The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

6.3.6 Class FTA: TOE Access

6.3.6.1 *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.

6.3.6.2 *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.

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

FTA_SSL.4.1

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

6.3.6.4 ***FTA_TAB.1 TOE Access Banner***

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.

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 ***FTP_ITC.1 Inter-TSF Trusted Channel***

FTP_ITC.1.1

The TSF shall be capable of using [SSH, TLS] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [authentication server, [*SFTP 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 transfer, authentication requests, software updates*].

6.3.7.2 ***FTP_TRP.1 Trusted Path***

FTP_TRP.1.1

The TSF shall be capable of using [SSH] to provide a communication path between itself and authorized 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 provides detection of modification of the channel 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, a subset of the optional requirements, and all applicable selection-based requirements that have been included as specified for 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 in exact conformance with the NDcPP.

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 Documentation

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 Supports

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, 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 TOE has the ability to generate audit records of behavior that occurs within the TSF. The audit records are sent to a remote syslog server and can also be sent to an SFTP server. The user can enable and disable logs (security log, event log, and command log) that are sent to an SFTP server.

The TOE contains mechanisms which generate audit data based upon successful and unsuccessful management actions by all authorized users of the TOE. The startup and shutdown of the TOE's audit functionality is synonymous with the startup and shutdown of the TOE, which is recorded in the TOE's audit records.

All actions performed on the TOE are logged and the table below represents what is being logged and where the event is being stored.

The following table lists the auditable events defined by this component, the location(s) where the TSF generates audit records for the events, and examples of audit records for that particular event and type.

Auditable Event	Location	Sample Data
Failure to establish an SSH session	Security Log	799: Wed Mar 29 17:07:45.497 2017 [local] P Sev:8 chassis(1): :sshd[8787]: fatal: Unable to negotiate with 10.41.71.103: no matching cipher found. Their offer: 3des-cbc [preauth] 858: Wed Mar 29 18:36:03.400 2017 [local] P Sev:8 chassis(1): :sshd[5734]: fatal: Unable to negotiate with 10.41.71.103: no matching host key type found. Their offer: ssh-dss [preauth] 1383: Thu Mar 30 15:16:48.349 2017 [local] P Sev:8 chassis(1): :sshd[2506]: fatal: Unable to negotiate with 10.41.71.103: no matching MAC found. Their offer: [preauth] 1167: Wed Mar 29 20:50:16.922 2017 [local] P Sev:8 chassis(1): :sshd[5764]: fatal: Unable to negotiate with 10.41.71.103: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth]
	Syslog	Apr 11 13:48:05 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-6-SSHD_LOG: chassis(1): :sshd[5253]: fatal: Unable to negotiate with 10.41.71.103: no matching cipher found. Their offer: 3des-cbc [preauth] Apr 11 13:53:56 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-6-SSHD_LOG: chassis(1): :sshd[6935]: fatal: Unable to negotiate with 10.41.71.103: no matching MAC found. Their offer: [preauth]

		Apr 11 13:51:03 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-6-SSHD_LOG: chassis(1): :sshd[6083]: fatal: Unable to negotiate with 10.41.71.103: no matching host key type found. Their offer: ssh-dss [preauth] Apr 11 13:45:44 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-6-SSHD_LOG: chassis(1): :sshd[4584]: fatal: Unable to negotiate with 10.41.71.103: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth]
Failure to establish a TLS session	Security Log	18580: Mon Apr 17 14:55:02.386 2017 [local] P Sev:8 radsec: RadSec Error: Error during TLS connect : Connection refused. Server: 10.41.71.110:2083
	Syslog	Apr 17 14:55:02 localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 RADSEC-6-T_L_S_ERROR: radsec: RadSec Error: Error during TLS connect : Connection refused. Server: 10.41.71.110:2083 285: Wed Apr 5 14:10:59.512 2017 [local] P Sev:8 chassis(1): :SyslogTLS Error: Error during TLS connect : Connection refused Dest: 10.41.71.100:6514
All uses of the authentication mechanism	Security Log	118: Tue Dec 22 20:21:06.798 2015 [local] P Sev:8 chassis(1): :sshd[3085]: Incoming connection from 10.41.71.103 port 64898 on 10.41.71.101 port 22 119: Tue Dec 22 20:21:11.116 2015 [local] P Sev:8 chassis(1): :User successfully logged in from IP 10.41.71.103 user name 'su' 126: Tue Dec 22 20:24:08.260 2015 [local] P Sev:8 chassis(1): :sshd[3946]: Incoming connection from 10.41.71.103 port 64933 on 10.41.71.101 port 22 127: Tue Dec 22 20:24:08.582 2015 [local] P Sev:6 chassis(1): :User authentication failed from IP shell user name 'su' 128: Tue Dec 22 20:24:11.516 2015 [local] P Sev:8 chassis(1): :sshd[3947]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive"
	Syslog	Apr 11 14:17:11 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-6-LOGIN_ACCEPTED: chassis(1): :User successfully logged in from IP 10.41.71.103 user name 'su' Apr 11 14:23:05 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-4-INTRUSION_DETECTION: chassis(1): :User authentication failed from IP shell user name 'su' Apr 11 14:25:43 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-6-LOGIN_ACCEPTED: chassis(1): :User successfully logged in from IP Console user name 'su'

		Apr 11 14:26:35 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-4-INTRUSION_DETECTION: chassis(1): :User authentication failed from IP ttyS0 user name 'su'
Unsuccessful attempt to validate a certificate	Security Log	18547: Mon Apr 17 14:01:51.339 2017 [local] P Sev:6 chassis(1): SSH IP 10.41.71.106 User su:CA certificate install fail: Not a CA certificate
	Syslog	Apr 17 14:01:51 localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-4-INVALID_C_A: chassis(1): SSH IP 10.41.71.106 User su:CA certificate install fail: Not a CA certificate
Modification of behavior of the transmission of audit data to an external IT entity	Security Log	17903: Thu Apr 13 18:15:14.343 2017 [local] P Sev:7 syslogTLS: Local RS-232 User su: SyslogTLS admin state set to disabled 17904: Thu Apr 13 18:15:18.212 2017 [local] P Sev:7 syslogTLS: Local RS-232 User su: SyslogTLS admin state set to enabled
	Event Log	April 13, 2017 18:15:14.343 [local] Sev:7 syslogTLS: Local RS-232 User su: SyslogTLS admin state set to disabled April 13, 2017 18:15:18.212 [local] Sev:7 syslogTLS: Local RS-232 User su: SyslogTLS admin state set to enabled
	Command Log	6545: system security log transfer enable 6546: command-log transfer enable 6547: logging transfer enable 6555: syslog tls disable 6556: syslog tls enable
	Syslog	Apr 11 16:55:58 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-COMMAND_LOG_SET: chassis(1): Local RS-232 Console User su:Command log enabled Apr 11 16:55:53 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-COMMAND_LOG_SET: chassis(1): Local RS-232 Console User su:Command log disabled
Initiation of Update	Command Log	44: software install package-path rel_saos8700_8.5.0_ga215.tgz default-sftp-server start now
	Syslog	Apr 11 16:35:28 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SWXGRADE-5-SOFTWARE_INSTALL: swXGrade: Local RS-232 User su: Software install request, package-path: SFTP:10.41.71.100/saos-08-05-223/rel_saos8700_8.5.0_ga223.tgz source: 10.41.71.100

All management activities of the TSF	Security Log	14983: Mon Apr 10 19:26:19.499 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:System Global Inactivity Timer Enable 14984: Mon Apr 10 19:26:37.507 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:System Global Inactivity Timeout Set 60 18705: Mon Apr 17 16:32:00.590 2017 [local] P Sev:6 chassis(1): SSH IP 10.41.71.103 User su:Shell banner has been modified: Login banner file line was modified 4374: Mon Apr 3 19:06:29.801 2017 [local] P Sev:7 chassis(1): SSH IP 10.41.71.103 User su:Ssh client user generate key, user: su Apr 5 16:22:30 localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-5-X509_CERT_INSTALLED: chassis(1): :Ssh X509 certificate installed for ciena1
	Command Log	431: system shell set global-inactivity-timer on 432: system shell set global-inactivity-timeout 5
	Syslog	Apr 11 16:21:25 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 CHASSIS-5-SYSTEM_GLOBAL_INACTIVITY_TIMER_ENABLE: chassis(1): SSH IP 10.41.71.103 User user1:System Global Inactivity Timer Enable
Modification, deletion, generation/import of cryptographic keys	Security Log	267: Tue Mar 28 14:48:39.531 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:Ssh server key delete 268: Tue Mar 28 14:48:43.509 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:Ssh Generate Key
	Command Log	5303: ssh server key delete 5304: ssh server key generate key-type ecdsa256
	Syslog	Apr 11 15:26:15 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-5-SSH_KEY_DELETE: chassis(1): Local RS-232 Console User su:Ssh server key delete Apr 11 15:26:32 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SSH-5-GENERATE_KEY: chassis(1): Local RS-232 Console User su:Ssh Generate Key
Changes to the time	Security Log	259: Tue Mar 28 14:35:00.073 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:System TimeDate Set From Tue Mar 28 14:33:33 2017 To Tue Mar 28 14:35:00 2017
	Event Log	259: Tue Mar 28 14:35:00.073 2017 [local] P Sev:7 chassis(1): Local RS-232 Console User test1:System TimeDate Set From Tue Mar 28 14:33:33 2017 To Tue Mar 28 14:35:00 2017
	Command Log	5241: system set time 15:33:30

	Syslog	Apr 11 15:33:30 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 CHASSIS-5-SYSTEM_TIME_DATE_SET: chassis(1): Local RS-232 Console User su:System TimeDate Set From Tue Apr 11 14:34:25 2017 To Tue Apr 11 15:33:30 2017 Apr 11 15:33:37 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 CHASSIS-4-TIME_CHANGED_FORWARD: chassis(1): :System time changed forward by more than 5secs
Any attempts at unlocking of an interactive session	Same as "the termination of a remote session by the session locking mechanism" below – the TSF will terminate idle interactive sessions, not lock them.	
The termination of a remote session by the session locking mechanism	Security Log	430: Tue Mar 28 21:01:01.277 2017 [local] P Sev:8 chassis(1): :User logged out from IP 10.41.71.103 user name 'su' due to inactivity
	Syslog	Apr 11 16:24:57 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-6-KILL_LOGIN: chassis(1): :Login/Shell Process 3371 Terminated
The termination of an interactive session	Security Log	1175: Thu Mar 30 13:06:16.401 2017 [local] P Sev:8 chassis(1): :User logged out from IP Console user name 'su' 1179: Thu Mar 30 13:11:43.941 2017 [local] P Sev:8 chassis(1): :User logged out from IP 10.41.71.103 user name 'su'
	Syslog	Apr 11 15:02:34 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-6-LOGOUT: chassis(1): :User logged out from IP Console user name 'su' Apr 11 15:08:15 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-6-LOGOUT: chassis(1): :User logged out from IP 10.41.71.103 user name 'user1'
Initiation of the trusted channel	Security Log	3228: Fri Mar 31 20:43:29.510 2017 [local] P Sev:7 chassis(1): :Software download request, server: 10.41.71.100, package-path: rel_saos8700_8.5.0_ga215.tgz, destination: rel_saos8700_8.5.0_ga215.tgz
	Syslog	Apr 11 16:35:28 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SWXGRADE-5-SOFTWARE_INSTALL: swXGrade: Local RS-232 User su: Software install request, package-path: SFTP:10.41.71.100/saos-08-05-223/rel_saos8700_8.5.0_ga223.tgz source: 10.41.71.100
Termination of the trusted channel	Syslog	Apr 11 20:05:52 localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SYSLOGTLS-6-T_L_S_CONNECTION_CLOSED: chassis(1): :SyslogTLS connection closed normally. Collector: 10.41.71.100:6514
Failure of the trusted channel functions	Same as "failure to establish an SSH session" and "failure to establish a TLS session" above, depending on the specific protocol experiencing failure.	

Initiation of the trusted path	Security Log	118: Tue Dec 22 20:21:06.798 2015 [local] P Sev:8 chassis(1): :sshd[3085]: Incoming connection from 10.41.71.103 port 64898 on 10.41.71.101 port 22 119: Tue Dec 22 20:21:11.116 2015 [local] P Sev:8 chassis(1): :User successfully logged in from IP 10.41.71.103 user name 'su'
Termination of the trusted path	Security Log	1179: Thu Mar 30 13:11:43.941 2017 [local] P Sev:8 chassis(1): :User logged out from IP 10.41.71.103 user name 'su'
	Syslog	DAEMON.INFO: Feb 22 06:11:06 [Local] 192.168.122.27 02:a8:7a:1b:00:00 8700 SSH-6-SSH_CLIENT_LOG: chassis(1): :ssh[]: Connection to 10.32.8.65 as 'su' completed, exit status 0
Failure of the trusted path functions	Same as “failure to establish an SSH session” above.	
Modification of the behavior of the TSF	Same as “all management activities of the TSF” above.	
Resetting passwords	Security Log	4416: Mon Apr 3 19:55:32.882 2017 [local] P Sev:7 chassis(1): SSH IP 10.41.71.103 User su:User Password Set test10
	Command Log	5254: user set user test1 echoless-password
	Syslog	Apr 11 14:53:16 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SEC-5-USER_PASSWORD_SET: chassis(1): Local RS-232 Console User su:User Password Set test1
Start-up and shutdown of the audit functions	Security Log	15742: Tue Apr 11 17:00:23.083 2017 [local] P Sev:7 logging: Local RS-232 User su: Security Log event number 0x1B000A disabled 15743: Tue Apr 11 17:00:32.439 2017 [local] P Sev:7 logging: Local RS-232 User su: Security Log event number 0x1B000A enabled
	Command Log	5347: logging disable destination flash 5348: logging enable destination flash 5351: command-log disable 5352: command-log enable 1398: syslog tls disable collector cc-server-2.ciena.com 1400: syslog tls enable collector cc-server-2.ciena.com 5359: system security log disable event-id 0x1B000A 5360: system security log enable event-id 0x1B000A

	Syslog	Apr 11 16:52:04 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-LOG_DESTINATION_ADMIN_STATE_SET: chassis(1): Local RS-232 Console User su:Log Destination Admin State Set destination flash admin state disabled Apr 11 16:52:13 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-LOG_DESTINATION_ADMIN_STATE_SET: chassis(1): Local RS-232 Console User su:Log Destination Admin State Set destination flash admin state enabled Apr 11 16:55:53 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-COMMAND_LOG_SET: chassis(1): Local RS-232 Console User su:Command log disabled Apr 11 16:55:58 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-COMMAND_LOG_SET: chassis(1): Local RS-232 Console User su:Command log enabled Apr 11 16:57:55 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SYSLOG-5-GLOBAL_ADMIN_STATE_SET: chassis(1): Local RS-232 Console User su:Syslog global admin state set disabled Apr 11 16:57:58 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 SYSLOG-5-GLOBAL_ADMIN_STATE_SET: chassis(1): Local RS-232 Console User su:Syslog global admin state set enabled Apr 11 17:00:23 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-SEC_LOG_EVENT_STATE: logging: Local RS-232 User su: Security Log event number 0x1B000A disabled Apr 11 17:00:32 ip6-localhost [Local] 10.41.71.101 2c:39:c1:b9:c8:00 8700 LOGGING-5-SEC_LOG_EVENT_STATE: logging: Local RS-232 User su: Security Log event number 0x1B000A enabled
Administrative login and logout	Same as “all use of the authentication mechanism” and “termination of an interactive session” above.	
Security related configuration	Same as “all management activities of the TSF” above.	

Table 12: Sample Audit Records

Audit records are created when the administrator performs each of the management functions listed above via the CLI (local and remote). As shown in the table above, each audit record provides a timestamp, username and a description of the action performed including a success/failure indication.

8.1.2 **FAU_GEN.2:**

The TOE records the identity of the user associated with each audited event that occurred due to a user action in the audit record.

8.1.3 FAU_STG.1:

The TSF protects stored audit records in the security, event, and command logs by only allowing a user with the Super role to delete records from the trail. The Super role is also the only role that is authorized to view the security log, whereas the Admin role is the minimum privilege required to view event and command log data. The log can only be cleared in its entirety so any deleting of any individual records is not allowed. The TSF does not retain syslog data beyond a small temporary cache that the TLS secure syslog implementation uses to ensure that audit data is not lost during brief network outages. This data cannot be manually interacted with by any administrator.

8.1.4 FAU_STG_EXT.1:

The TSF provides the ability to securely transmit audit data to the Operational Environment without administrator intervention. When syslog audit events are generated they are immediately transmitted to the environmental syslog server over TLS. Any audit data that is stored locally in the security, event, and command logs will be transmitted over SSH to a remote SFTP server at an administratively configurable period interval. Security and events logs only differ in date format and command logs are only capturing the CLI syntax for configurations. Syslogs can be identified by a syslog header and can also contain any event, but can be configured to filter specific logs based on importance.

The SSH and TLS implementations used for this process conform to FCS_SSHC_EXT.1 and FCS_TLSC_EXT.2, respectively. Only a user with the Super role has permissions to configure the remote audit storage behavior.

The TOE is not an audit server; however, it can store audit data locally. Syslog data is only stored in a temporary buffer as part of the secure syslog implementation so this is not considered to be local storage. However, the security, event, and command logs are stored persistently on the TOE's local file system. When these log files are transferred to the remote SFTP server, the entire contents of the most recent log file are transferred.

When a log file reaches its allowed maximum size it is closed and renamed sequentially. A new log file is then opened as the current log. Once the number of log files reaches its configured maximum amount, the oldest log file is automatically deleted and the remaining log files roll over in order to allow the new file to be created. A user with the Super role also has the ability to manually delete log files. The maximum quantity and size for each log file is as follows:

- Security Log: up to 4 historical files with up to 5,000 entries per file
- Event Log: up to 4 historical files with up to 10,000 entries per file
- Command Log: up to 5 historical files with up to 2,500 entries per file

8.2 Cryptographic Support

8.2.1 FCS_CKM.1:

The TOE generates RSA and Elliptic Curve Diffie-Hellman (ECC) keys in accordance with FIPS PUB 186-4. The TOE generates cryptographic keys according to table 14 below. RSA supports 2048 bit key sizes. The ECC curves supported are P-256, P-384, and P-521. For SSH, the TOE only supports the generation of RSA with 2048 bits. The TOE uses OpenSSL version 1.0.2j to support cryptographic algorithm certificates which has been tested on Ciena's hardware and software.

Algorithm/Protocol	TLS	SSHC	SSHS
Elliptic Curve Diffie-Hellman (ECC)	X	X	X
RSA Key Establishment	X		
RSA Digital Signatures	X	X	X
Elliptic Curve Digital Signature Algorithm (ECDSA)	X	X	X

Table 13: Cryptographic Key Generation

The TOE's key generation functions have the following CAVP certificates:

DSA: #1198

RSA: #2445

ECDSA: #1092

8.2.2 FCS_CKM.2:

The TOE implements NIST SP 800-56A conformant key establishment mechanisms for Elliptic Curve Diffie-Hellman (ECDH) 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. In addition, the TOE implements RSA key establishment, conformant to NIST SP 800-56B. The TOE complies with sections 5.9, 6, and 8 of NIST SP 800-56B (including all subsections) for RSA key pair generation and key establishment. The TOE is able to generate RSA key pairs with a modulus of 2048 bits which has an equivalent key strength of 112 bits.

The TOE's key establishment function has KAS ECC certificate #120.

8.2.3 FCS_CKM.4:

The TOE destroys cryptographic keys in accordance with the specified destruction method based on the memory it is stored on. All keys stored in volatile memory (RAM) are destroyed by a single direct overwrite consisting of zeroes .After overwriting, the TSF reads the memory to verify the key has been destroyed. If the read-verify fails, the process is repeated. For non-volatile keys, the TSF destroys the abstraction of the key to the portion of the flash memory where the key resides using the secure erase command.

Key Material	Origin	Storage Location	Clearing of Key Material
SSH keys	SSH server/ client application	Non-volatile storage/file system	Overwrite with 0 to clear cache and read verify, then call eMMC secure erase feature on the file blocks
Authentication keys	X.509 certificates	Non-volatile storage/ file system	Overwrite with 0 to clear cache and read verify, then call eMMC secure erase feature on the file blocks

TLS session keys	syslogtls, radsec applications	Non-volatile storage/ RAM	Overwrite with 0 and read verify

Table 14: Cryptographic Materials, Storage, and Destruction Methods

8.2.4 FCS_COP.1(1):

The TOE performs encryption and decryption using the AES algorithm in CBC and GCM mode with key sizes of 128 and 256 bits. This algorithm implementation has CAVP AES certificate #4470. The AES algorithm meets ISO 18033-3. Also, CBC meets ISO 10116 and GCM meets ISO 19772.

8.2.5 FCS_COP.1(2):

In accordance with FIPS 186-4, the TOE provides cryptographic digital signature verification using RSA Digital Signature Algorithm (rDSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). The TOE supports rDSA with a key size of 2048 bits. The TOE supports ECDSA with a key size of 256, 384, 521 bits. These implementations have CAVP RSA certificate #2445 and ECDSA certificate #1092.

8.2.6 FCS_COP.1(3):

The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 with message digest sizes of 160, 256, 384, and 512 bits respectively, as specified in FIPS PUB 180-4. The TSF uses hashing services the following functions:

- SHA-1, SHA-256, and SHA-512 for SSH data integrity
- SHA-256 for software integrity
- SHA-1, SHA-256, and SHA-384 for TLS
- SHA-512 for password hashing

The SHA algorithm meets ISO/IEC 10118-3:2004 and has CAVP SHS certificate #3682.

8.2.7 FCS_COP.1(4):

The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512. All key sizes relative to block size are supported by HMAC implementation as specified in FIPS 198-1 and FIPS 180-3, and the following MAC sizes are supported:

- HMAC-SHA-1: 10, 12, 16, 20 bytes.
- HMAC-SHA-256: 16, 24, 32 bytes.
- HMAC-SHA-512: 32, 40, 48, 56, 64 bytes.

The algorithm meets ISO/IEC 9797-2:2011 and has CAVP HMAC certificate #2967.

8.2.8 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 CTR_DRBG with AES. The TOE models uniformly provide two software-based and noise-based entropy sources 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 #1454.

8.2.9 FCS_SSHC_EXT.1/ FCS_SSHS_EXT.1:

The TOE acts as an SSHv2 for remote CLI sessions that complies with RFCs 4251, 4252, 4253, 4254, 5656, 5647, and 6668. There is no SSHv1 implementation on the TOE. The TOE implementation of SSHv2 supports RSA and ECDSA signature verification for authentication in addition to password-based authentication. SSH is used for remote administrators to connect securely to the TOE for CLI connections, transferring audit logs to a remote SFTP server, and for the transmitting updates to the TOE. The SSH implementation will detect all large packets greater than 32,768 bytes and drop accordingly.

The TOE implementation of SSHv2 supports AES-CBC for its encryption algorithm with 128 or 256 bit key sizes. The SSH client differs from the SSH server by its use of key exchange methods. The SSH client implementation only uses ecdh-sha2-nistp256 whereas the SSH server implementation can use any of ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521. Additionally, the TOE's SSH client implementation will authenticate an environmental SSH server using a local database that associates each host name with its public key. This is not applicable to the SSH server. These two differences are the only are the only security-relevant differences between the client and the server implementations.

The TOE's SSH implementation uses ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp256, and x509v3-ecdsa-sha2-nistp384 as its public key algorithms. As for data integrity, the TOE supports hmac-sha-1, hmac-sha2-256, and hmac-sha2-512. The SSH connection will be rekeyed after no more than 2^28 packets or more than one hour. The actual rekey data threshold is administratively configurable by a user with the Super role and can be set to 4GB, 2GB, 1GB, or 500MB. The time threshold can be set to an administrator-defined number of minutes and/or seconds.

8.2.10 FCS_TLSC_EXT.2:

The TOE uses TLS to secure communications with the remote syslog server and optional RADIUS server in the Operational Environment. Both TLS 1.1 and 1.2 are supported. Each of these connections supports mutual authentication using valid X.509v3 certificates.

The presented identifier has to match the reference identifier in order to establish the connection. The TSF uses the Common Name (CN) as the Subject Name and either DNS name or IP address as the Subject Alternative Name (SAN). Wildcards are supported for all fields that use them. In the evaluated configuration, the TOE's TLS implementation is configured to present the Supported Elliptic Curves Extension in the Client Hello using NIST curves secp256r1, secp384r1, and secp521r1. Certificate pinning is not supported.

The mandatory ciphersuite of TLS_RSA_WITH_AES_128_CBC_SHA is supported. The following optional ciphersuites are also used if configured by the user with the Super role:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

8.3 Identification and Authentication

8.3.1 **FIA_PMG_EXT.1:**

The TOE supports user passwords with a minimum length of 1 and a maximum length of 128 characters. In the evaluated configuration, a minimum of 15 characters should be set. The accepted characters include upper and lower case letters, numbers, and the special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")".

8.3.2 **FIA_UAU.7:**

While authenticating to the TOE with an incorrect login (specifically an invalid username and/or an invalid password) on any interface the TOE does not indicate to the user whether the username or password was incorrect so the nature of the authentication failure is obfuscated.

8.3.3 **FIA_UAU_EXT.2:**

Users can authenticate to the TOE using locally defined username/password credentials or using RADIUS. If attempting to authenticate to the TOE using SSH, public key authentication can also be used. A user with the Super role can specify the authentication method(s) allowed for the TOE. The methods of authentication used for the local CLI versus the remote CLI can be configured separately even though they provide identical management functionality.

8.3.4 **FIA_UIA_EXT.1:**

The TOE provides authorized administrators with a local CLI that is accessible via serial port and a remote CLI that is accessible via SSH. These interfaces both support username and password authentication, where the credentials are defined either internally to the TOE or in an environmental RADIUS server. Remote SSH connectivity can also be configured to authenticate administrators using public key.

In the evaluated configuration, the TOE displays a warning banner before authentication regardless of whether the TOE is being accessed locally or remotely. The warning banner text is configurable and display of this banner is the only TOE functionality that is available to an unauthenticated user.

8.3.5 **FIA_X509_EXT.1/ FIA_X509_EXT.2/ FIA_X509_EXT.3:**

The TOE performs certificate validity checking for TLS mutual authentication with the remote syslog server and RADIUS server. Depending on configuration, the TOE may also perform certificate validity checking when establishing SSH communications. In addition to the validity checking that is performed by the TOE, the TSF will validate certificate revocation status using an OCSP server in the Operational Environment. In the event that the revocation status cannot be verified, the certificate will be rejected.

The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. In addition, the certificate path is terminated in a trusted CA certificate, the basicConstraints extension is present, and the CA flag is set to TRUE for all CA certificates. Finally, the TOE ensures the extendedKeyUsage field includes the code signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) for certificates used for trusted updates and executable code, the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) for server certificates used in TLS, the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2), or the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) for OCSP certificates used for OCSP.

The TOE uses X.509v3 certificates to support authentication for TLS connections in accordance with RFC 5280. Client-side certificates are used for TLS mutual authentication. A Certificate Request Message can be generated as specified in RFC 2986 containing the following information "Common Name, Organization, Organizational Unit, Country" and the chain of certificates is validated from the root CA when the CA Certificate Response is received.

8.4 Security Management

8.4.1 FMT_MOF.1(1)/Audit:

Auditable events generated by the TSF are transferred to the Operational Environment in two ways. Syslog data is transferred in real-time to a remote syslog server using TLS. Data in the persistent file logs (security, event, and command logs) are transferred to a remote SFTP server using SSH. A user with the Super role is responsible for configuring the locations to which audit data is transmitted over these interfaces, and in the case of the SSH interface, the frequency of transmission.

8.4.2 FMT_MOF.1(1)/TrustedUpdate:

Once software updates have been acquired from Ciena and placed onto an SFTP server, a user with the Admin or Super role has the ability to download the updates from the SFTP server onto the TOE.

8.4.3 FMT_MTD.1:

The TOE has three roles: Super, Admin, and Limited. A user with a Limited role is a read-only user without any configuration privileges of their own. A user with the Super role functions as a super user for the entire TOE and can manage all aspects of the TSF. A user with the Admin role can perform most of the same security functions authorized to the Super role. However, the Admin role is not privileged to modify audit configurations, delete audit data, configure cryptographic keys, or manage user accounts.

The only security-relevant TOE functionality that is available to a user prior to authentication is the display of the warning banner.

8.4.4 FMT_MTD.1/AdminAct:

The ability to modify, delete, and generate/import cryptographic keys and importing SSH keys is limited to a user with the Super or Admin role.

8.4.5 FMT_SMF.1:

The TOE defines three administrative roles each of which have differing levels of permission to perform TSF management functions and interact with TSF data. A user functions as the Security Administrator for all management activities that are authorized by their assigned role. The management functions provided by the TOE include the ability to configure the access banner and session lockout functionality, the ability to acquire, verify, and install TOE software/firmware updates, the ability to configure audit behavior, and the ability to configure cryptographic functionality. All administration is performed using the CLI which can be used either locally via serial console or remotely via SSH.

8.4.6 FMT_SMR.2:

The TOE maintains three administrative roles: Limited, Admin, and Super. All three roles have the capability to manage the TSF locally or remotely to varying degrees. Therefore, each role functions as a Security Administrator for different subsets of the TSF, with the Super role providing the ability to manage the entire TSF. All roles can be accessed both locally and remotely using the CLI.

8.5 Protection of the TSF

8.5.1 FPT_APW_EXT.1:

Administrator passwords are not stored by the TOE in plaintext. All administrative passwords themselves are hashed using SHA-512. There is no function provided by the TOE to display a password value in plaintext nor is the password data recoverable. When creating a new user, the password value can either be entered in plaintext or the ‘secret’ parameter can be used in which case a pre-encrypted password string is provided. The password data is encrypted using RSA. This is used for cases where duplicate configuration of multiple systems is desired without exposing vulnerable password hashes in plaintext configuration files.

8.5.2 FPT_SKP_EXT.1:

The TOE does not have a mechanism to view pre-shared keys, symmetric keys and private keys. Volatile memory used to store secret keys, private keys, and secret key data is not accessible by administrators and neither is the file system of the OS. A user with the Admin role or higher is permitted to view public key data only.

8.5.3 FPT_STM.1:

The TOE is able to provide its own time via its internal clock through manual administrator configuration. The TOE uses the clock for several security-relevant purposes, including:

- Audit records
- X.509 certificate validation
- Inactivity of administrator sessions
- Determining RADIUS timeout

8.5.4 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 resides in local storage that can only be modified when a software update is performed.

- Cryptographic 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, a user with Super role will need to factory reset the TOE and/or have it replaced by authorized personnel in accordance with the OE.PHYSICAL and OE.TRUSTED_ADMIN objectives. 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.

8.5.5 FPT_TUD_EXT.1:

The TOE provides the ability for an authorized administrator to view the current software/firmware version of the TOE and to initiate software/firmware updates. 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 to the customer on read-only physical media when made available by Ciena. In the evaluated configuration, the TOE is configured by a user with the Admin or Super role to accept signed updates. Updates provided by Ciena are signed using a 2048-bit RSA digital signature. Prior to installation of the software image, the digital signature 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. When an update is installed, the previously-installed version continues to run until the TOE is rebooted. The TOE provides the ability to query both the running and installed versions of the TOE software/firmware.

8.6 TOE Access

8.6.1 FTA_SSL_EXT.1:

The TSF has the ability to terminate inactive local sessions. 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.

8.6.2 FTA_SSL.3:

The TOE will terminate a remote session due to inactivity according to the configuration set by the Security Administrator, which in this case is a user with the Admin or Super role. This is a global command and will impact all users and interfaces (console and remote CLI). The system timeout is 10 minutes by default, but can be configured from 1-1500 minutes.

This configuration is able to be set by a user with an Admin or Super role using the command:

system shell set global-inactivity-timer on - This enables the timer
system shell set global-inactivity-timeout <minutes>

8.6.3 FTA_SSL.4:

Any user accessing the TOE is capable of terminating their own session by entering the exit command. If in a tiered command, the user will need to type "quit" to leave the tier structure entirely before typing "exit" to terminate their session. Otherwise, typing "exit" in a tiered command will only result in closing the current command tier and going to the previous command tier.

8.6.4 FTA_TAB.1:

There are two possible ways to log in to the TOE: local CLI and remote CLI. When logging in locally or remotely through the CLI, the pre-authentication banner is displayed and can be viewed prior to authentication. There is also a configurable post-authentication banner known as the “Welcome Banner.” A user with the Super or Admin role can configure either banner.

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1:

The TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. Updates to the TOE software are securely delivered to the TOE using SFTP. Security, command, and event log files are transmitted to a remote server using SFTP as well. The TOE uses OpenSSH 6.6P1 to support SSH communications. The TOE also uses TLS for syslog server and RADIUS server communications. When there is a network outage or connection is lost, the secure syslog implementation will maintain a small buffer of data temporarily but this data is not preserved in the event of a persistent outage due to the streaming nature of syslog.

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 manually enable FIPS 140-2 encryption mode as part of the initial configuration of the TOE.

8.7.2 FTP_TRP.1:

Remote administration is secured using SSH. The security administrator of the TOE can authenticate using either username/password or SSH public key authentication. The TOE’s SSH server implementation is conformant to FCS_SSHS_EXT.1.