ciena : the network specialist

Ciena Carrier Ethernet Solutions 3900/5100 Series

Security Target

ST Version: 1.0
December 28, 2018

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West St
Laurel, MD 20707

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

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

1.1 ST Reference

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

1.1.1 ST Identification

ST Title: Ciena Carrier Ethernet Solutions 3900/5100 Series Security Target
ST Version: 1.0
ST Publication Date: December 28, 2018
ST Author: Booz Allen Hamilton

1.1.2 Document Organization

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

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

Chapter 3 describes the conformance claims made by this ST.

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

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

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

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

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

1.1.3 Terminology

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

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

Table 1-1: Customer Specific Terminology

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

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

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

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CES	Carrier Ethernet Solutions
CSP	Critical Security Parameter
CTR	Counter (AES mode)
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code
KAS	Key Agreement Scheme
MAC	Media Access Control
NDcPP	Collaborative Protection Profile for Network Devices
POST	Power On Self-Test
NTP	Network Time Protocol
QoS	Quality of Service
RSA	Rivest Shamir Adelman (encryption algorithm)
SAOS	Service Aware Operating System
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SSH	Secure Shell

Table 1-3: Acronym Definition

1.1.5 References

[1] collaborative Protection Profile for Network Devices version 2.0 + Errata 20180314

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model CCMB-2012-09-001, Version 3.1 Revision 4, September 2012
[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012
[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
[6] ISO/IEC 18033-3:2010, Information Technology-Security techniques-Encryption algorithms—Part3: Block ciphers
[7] ISO/IEC 10116:2017, Information Technology-Security techniques-Modes of operation for an n-bit block cipher
[8] ISO/IEC 9796-2:2010, Information Technology -- Security techniques -- Digital signature schemes giving message recovery—Part 2 Integer factorization based mechanisms
[9] ISO/IEC 14888-3:2016, Information Technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
[10] ISO/IEC 10118-3:2004, Information Technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
[11] ISO/IEC 9797-2:2011, Information Technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
[12] ISO/IEC 18031:2011, Information Technology -- Security techniques -- Random bit generation
[13] FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013
[14] FIPS PUB 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation January 2018

1.2 TOE Reference

The TOE is the Ciena Carrier Ethernet Solutions 3900/5100 Series. The TOE is a family of standalone network hardware appliances that run on the Ciena Service Aware Operating System (SAOS) 6.17 with uniform security functionality between each of the hardware appliances. The exception being that the 5170 model which runs SAOS 8.6.1. SAOS is a Linux-based operating system.

1.3 TOE Overview

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

The following diagram shows one instance of the TOE in its operational environment. All models of the TOE have the same environment and interfaces with one exception: some models lack an Ethernet

management port so remote administration and placement of the required environmental objects in this case will use a data hardware interface that is specifically configured to handle management traffic.

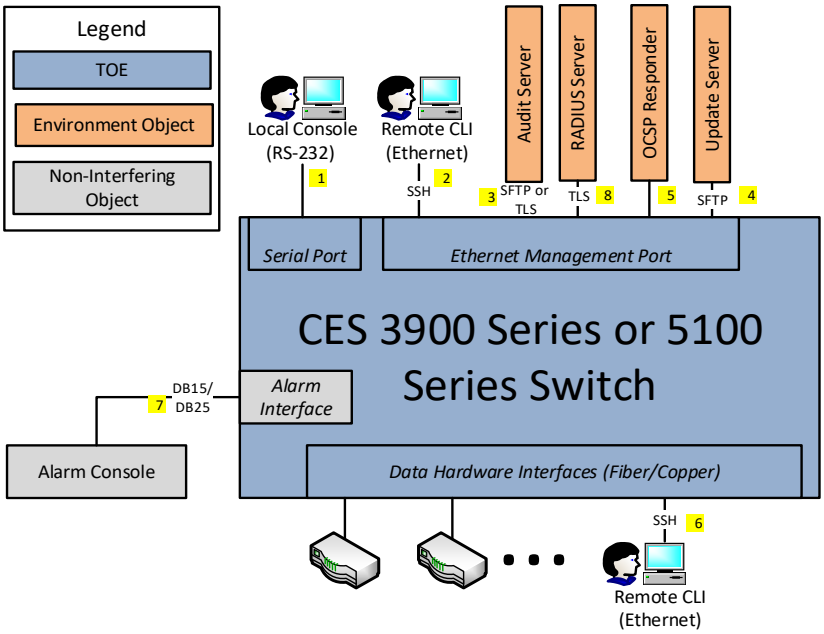

Figure 1 – TOE Boundary

As illustrated in Figure 1, the TOE is one of a family of hardware devices, each of which has an interface for local administration (Ethernet management port and/or local serial port) and data hardware interfaces. The Ethernet management port allows users to connect to the TOE via SSH through a command line interface. In addition, the Ethernet management port serves as a communication channel to external entities such as a RADIUS server, remote audit storage server (syslog server), OCSP responder, and update server. The channels to the remote audit server and updates server are secured by SFTP over SSH. The TOE provides an alternate configuration option that would use a TLS interface to the remote audit server. The RADIUS server is protected using TLS. The data hardware interfaces provide both ingress and egress for switched network traffic. This traffic is not associated with any security functionality and is not within the scope of the TOE. However, these interfaces can also be configured to handle management traffic through a dedicated management VLAN as well. This is how the functionality provided by the Ethernet management port is implemented for models that lack a dedicated management port.

1.4 TOE Type

The TOE type for this product is Network Device. The TOE is a hardware appliance whose primary functionality is related to the handling of network traffic. The 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 3 functionality. The TOE is a switch that has Layer 2 and Layer 3 functionality. The TOE type is justified

because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise.

2 TOE Description

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

2.1 Evaluated Components of the TOE

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

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

Platform	3903 / 3904 / 3905	3906	3916	3926M	3928	3930-900/910	3931-900/910	3932 / 3930-930	3942
10/100/1000M RJ-45	--	2	--	--	--	--	4	--	20
Combo RJ-45/SFP	3903 - 1 3904 - 2 3905 - 2	2	2	--	--	4	--	4	--
100M/1G SFP	2	2	4	2	8	4	4	4	--
1G/10G SFP+	--	--	--	6	4	2	2	2	4
CPU	2x800 MHz ARMv7 Cortex A9	2x800 MHz ARMv7 Cortex A9	2x500 MHz Cavium OCTEON 5220	4x1.5GHz ARM Cortex A53 AARCH64	4x1.5GHz ARM Cortex A53 AARCH64	4x600 MHz Cavium OCTEON 5230	2x600 MHz Cavium OCTEON 5220	4x600 MHz Cavium OCTEON 5230	4x1 GHz Cavium OCTEON II CN6230
Ethernet Management Port	N	Y	N	Y	Y	Y	N	Y	Y
Power Options	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC

Table 2-1: 3900 models

Platform	5142	CN 5150	5160	5170
10/100/1000M RJ-45	--	--	--	--
Combo RJ-45/SFP	--	--	--	--
100M/1G SFP	20	48	--	--
1G/10G SFP+	4	--	24	40
XFP	--	4	--	--
100G	--	--	--	5170U - 4xQSFP28 5170H – 2xQSFP28/2xCFP4
CPU	6x800MHz Cavium OCTEON II CN6335	4x600MHz Cavium OCTEON 5230	6x800MHz Cavium OCTEON II CN6335	Intel Xeon D-1500
Ethernet Management Port	Y	Y	Y	Y

Power Options	AC, DC	AC, DC	AC, DC	AC, DC

Table 2-2: 5100 Models

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

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

2.2 Components and Applications in the Operational Environment

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

Component	Definition
Audit Server (SFTP Server)	A file server running the secure file transfer protocol (SFTP) that is used by the TOE to securely transmit audit data to a remote storage location.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Certification Authority	A server that acts as a trusted issuer of digital certificates and implements an OCSP responder to verify revocation status of a certificate.
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.
Update Server	A server running the secure file transfer protocol (SFTP) that is used as a location for storing product updates that can be transferred to the TOE.
RADIUS Server	A server providing centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service, i.e. external authentication mechanism. Communications are secured using TLS.

Table 2-3: Evaluated Components of the Operational Environment

2.3 Excluded from the TOE

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

2.3.1 Not Installed

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

2.3.2 Installed but Requires a Separate License

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

2.3.3 Installed But Not Part of the TSF

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

- Non-FIPS mode of operation – The TOE includes a FIPS compliant mode of operation which allows the TOE to use only approved cipher suites for SSH communications and to perform cryptographic self-tests on system startup. This mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
- Alarm console – The TOE includes a local alarm console that can provide immediate notification of various security alerts. This is not part of the evaluated configuration because security alerts and automatic response to security alerts is outside the scope of the claimed PP.
- Remote Telnet interface – The TOE includes both Telnet and SSH interfaces for administration. Telnet is acceptable to use locally via serial connection, but in the evaluated configuration this remote service will be disabled.

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

2.4 Physical Boundary

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

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

2.5 Logical Boundary

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

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

2.5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record contains the user information, time stamp, message briefly describing what actions were performed, outcome of the event, and severity. All audit record information is associated with the user of the TOE that caused the event where applicable. Locally-stored audit data is read-only with the exception of a Security Administrator capable of deleting logs. Audit data can be securely transmitted to a remote storage location using SFTP or to a remote syslog server using TLS.

2.5.2 Cryptographic Support

The TOE provides cryptography in support of TLS and SSH trusted communications. Asymmetric keys that are used by the TSF are generated in accordance with FIPS PUB 186-4 and RFC 3526. Keys are established according to NIST SP 800-56A Revision 2, NIST SP 800-56B Revision 1 and RFC 3526.

The TOE uses software-based cryptography to provide cryptographic services using the OpenSSL FIPS Object Module (FOM) version 2.0.12 with CMVP certificate #1747. Both SAOS 6.17 and SAOS 8.6.1 use OpenSSL module 2.0.12.

The TOE uses FIPS-validated cryptographic algorithms to provide cryptographic services. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications:

SFR	Algorithm Cert	CAVP Cert. #
FCS_COP.1/DataEncryption	AES	5419, 5665
FCS_CKM.2	CVL	1872, 2048
FCS_RBG_EXT.1	DRBG	2114, 2287
FCS_CKM.1, FCS_COP.1/SigGen	ECDSA	1440, 1531
FCS_COP.1/KeyedHash	HMAC	3589, 3770
FCS_CKM.1, FCS_COP.1/SigGen	RSA	2903, 3047
FCS_COP.1/Hash	SHS	4350, 4539

Table 2-4: Cryptographic Algorithm Certificates

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

connecting to the TOE locally using the management workstation, password data will be obfuscated as it is being input. When the configured amount of failed authentication attempts is reached, the user is locked out for configurable amount of time. The Super role can also manually unlock the user.

2.5.4 Security Management

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

The Limited user is a read-only user, so any commands the user performs on the TOE will only allow the user to view different attributes and settings. The next level role is the Admin user who can perform all system configurations, set the time, configure cryptographic functionality, view/edit audit data, and initiate updates. Following the Admin role is the Super role. An administrator with the Super role can perform all system configurations including user management, including creating and deleting users on the TOE, transferring audit data to a remote location. 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 expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE stores passwords in an obfuscated format. The cryptographic module prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-512. The TOE maintains system time via its local hardware clock which is manually set by an administrator. TOE software updates are acquired using SFTP and initiated using the CLI. The TOE software version is administratively verifiable and software updates are signed to provide assurance of their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

2.5.6 TOE Access

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

2.5.7 Trusted Path/Channels

A trusted path is established to the TOE using SSHv2 for remote administration. The TOE establishes trusted channels for sending audit data to remote syslog server, for downloading software updates, and authenticating to the RADIUS server. Audit logs are sent to a remote syslog server using TLS or using SFTP (FTP over SSH) to a remote audit server. An SSH trusted channel is established to download updates using SFTP from an update server. The trusted channel to the RADIUS server is protected by 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 as claimed in the PP.

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 28 December 2018.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant to include all applicable NIAP and International interpretations through 28 December 2018.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profile:

- Collaborative Protection Profile for Network Devices version 2.0 + Errata 20180314 [NDcPP]

The following is the list of NIAP Technical Decisions that are applicable to the ST/TOE and a summary of their impact:

TD #	Title	Changes			Analysis to this evaluation	
		SFR	AA	Notes	NA	Reason
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	X	X		X	AA: TSS, AGD, and Test Not claiming IPSEC
TD0342	NIT Technical Decision for TLS and DTLS Server Tests		X		X	AA: Test Not claiming TLSS
TD0341	NIT Technical Decision for TLS wildcard checking			X		
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	X				
TD0339	NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	X	X	X		AA: TSS and Test
TD0338	NIT Technical Decision for Access Banner Verification		X			AA: TSS
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	X	X	X		AA: Test
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8		X			AA: Test

TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites			X	X	Not claiming DTLS to TLSS
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported		X			AA: Test
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	X	X	X		AA: AGD and Test
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1		X			AA: Test SAR FSP.1-1 and -2 wording Affects AAR
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list		X		X	AA: Test Not claiming DTLS
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list		X		X	AA: Test Not claiming TLSS Supersedes TD0262
TD0321	Protection of NTP communications			X		
TD0291	NIT technical decision for DH14 and FCS_CKM.1	X				
TD0290	NIT technical decision for physical interruption of trusted path/channel.		X			AA: TSS and Test
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e		X			AA: Test
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey		X			AA: Test
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	X		X		
TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4		X		X	AA: Test Not claiming DTLSC Claiming TLSC
TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication		X			AA: Test
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation		X			AA: Test

Table 3-1: Technical Decisions

3.5 Package Claims

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/Rev
- FIA_X509_EXT.2
- FIA_X509_EXT.3
- FMT_MOF.1/Functions

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

- FAU_STG.1
- FMT_MOF.1/Services
- FMT_MTD.1/CryptoKeys

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

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are conformant with the claimed cPP.

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. It provides a minimal set of security requirements expected by all network devices that target the mitigation of a set of defined threats. This baseline set of requirements will be built upon by future cPPs to provide an overall set of security solutions for networks up to carrier and enterprise scale. 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 role within the network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil[sic] the requirements of this cPP.”

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

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the 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_CHANNELS	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. a 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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the 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 4-2: TOE Organization Security Policies

4.3 Assumptions

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

Note: the NDcPP also defines the assumption A.COMPONENTS_RUNNING. However, the NDcPP also states that this applies to distributed TOEs only. Since the Ciena CES is not a distributed TOE, the TOE's Operational Environment does not include this assumption.

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 a 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.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4-3: TOE Assumptions

4.4 Security Objectives

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

4.4.1 TOE Security Objectives

There are no security objectives identified for the TOE.

4.4.2 Security Objectives for the Operational Environment

This section identifies the security objectives of the Operational Environment. These objectives have been taken directly from the NDcPP.

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

Objective	Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.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.TRUSTED_ADMIN	Security 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.

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.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4-4: TOE Operational Environment Objectives

O.E_COMPONENTS_RUNNING is not included in the Objectives because this is not a Distributed TOE.

4.5 Security Problem Definition Rationale

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

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the cPP to which the ST and TOE claim conformance. These extended components are formally defined in the cPP 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 underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR and/or separated by a "/" with a notation that references the function for which the iteration is used, e.g. "/DataEncryption" 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 cPP for a particular operation (such as if the cPP'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 cPP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG_EXT.1	Protected Audit Event Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation
	FCS_COP.1/SigGen	Cryptographic Operation
	FCS_COP.1/Hash	Cryptographic Operation
	FCS_COP.1/KeyedHash	Cryptographic Operation
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.2	TLS Client Protocol with Authentication
Identification and Authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UAU_EXT.2	Password-based Authentication Mechanism

Class Name	Component Identification	Component Name
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
Security Management	FMT_MOF.1/Functions	Management of Security Functions Behavior
	FMT_MOF.1/ManualUpdate	Management of Security Functions Behavior
	FMT_MOF.1/Services	Management of Security Functions Behavior
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
	FPT_TUD_EXT.2	Trusted Updated based on Certificates
TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1/Admin	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class FAU: Security Audit

6.3.1.1 *FAU_GEN.1 Audit Data Generation*

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising;
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
- Changes to TSF data related to 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]];

d) Specifically defined auditable events listed in Table **6-2**.

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

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

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSC_EXT.2	Failure to establish an TLS session.	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g. IP Address)
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure.
FMT_MOF.1/Functions	Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/Services	Starting and stopping of services.	None.
FMT_MTD.1/CoreData	All management activities of TSF data	None.
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.
FPT_TUD_EXT.2	Failure of update.	Reason for failure (including identifier of invalid certificate).
FPT_STM_EXT.1	Discontinuous changes to the time – either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	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.
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/Admin	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted path functions.	None.

Table 6-2: 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_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: *[the oldest file becomes the newest file when the data is overwritten with current log information]*] when the local storage space for audit data is full.

6.3.1.4 *FAU_STG.1 Protected Audit Trail Storage*

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation*

FCS_CKM.1.1[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;
- FFC schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

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 meet the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3].

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/DataEncryption Cryptographic Operation*

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC, CTR, GCM] mode and cryptographic key sizes [128 bits, 256 bits] that

[1] TD0291

meet the following: AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

6.3.2.5 *FCS_COP.1/SigGen Cryptographic Operation*

FCS_COP.1.1/SigGen 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 bits, 512 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/Hash Cryptographic Operation*

FCS_COP.1.1/Hash The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 10118-3:2004.

6.3.2.7 *FCS_COP.1/KeyedHash Cryptographic Operation*

FCS_COP.1.1/KeyedHash 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 *[160 bits, 256 bits, 512 bits]* 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 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 [HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[3]* software-based noise sources] 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 RFC(s) [4251, 4252, 4253, 4254, 5656, 6187, 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 *[262,144]* bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4[2] The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr].

FCS_SSHC_EXT.1.5[3] The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6[4] The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] 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 threshold 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 certification authorities] as described in RFC 4251 section 4.1.

[2] TD0337
[3] TD0259
[4] TD0337

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, 5656, 6187, 6668].

FCS_SSHS_EXT.1.2[5] 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 *[262,144]* bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4[6] The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr].

FCS_SSHS_EXT.1.5[7] The TSF shall ensure that the SSH public-key based authentication implementation uses [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6[8] The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, 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)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- [TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268;
- 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;

[5] TD0339
[6] TD0337
[7] TD0259
[8] TD0337

- 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 section 6.

FCS_TLSC_EXT.2.3 The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSC_EXT.2.4 The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves] in the Client Hello.

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_AFL.1 Authentication Failure Management*

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within *[1-5]* unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending remote Administrator from successfully authenticating *until [manual unlock by administrator with Super role]* is taken by a local Administrator; prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed].

6.3.3.2 *FIA_PMG_EXT.1 Password Management*

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"];
b) Minimum password length shall be configurable to *[15 character minimum]* and *[128 character maximum]*.

6.3.3.3 *FIA_UAU_EXT.2 Password-based Authentication Mechanism*

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

6.3.3.4 *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.

6.3.3.5 *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.

6.3.3.6 *FIA_X509_EXT.1/Rev X.509 Certificate Validation*

FIA_X509_EXT.1.1/Rev[9] The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

[9] TD0340

- 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/Rev 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.

6.3.3.7 *FIA_X509_EXT.2 X.509 Certificate Authentication*

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [SSH, TLS], and [code signing for system software updates].

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].

6.3.3.8 *FIA_X509_EXT.3 X.509 Certificate Requests*

FIA_X509_EXT.3.1[10] The TSF shall generate a Certification Request 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/Functions Management of Security Functions Behavior*

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [modify the behaviour of] the functions [transmission of audit data to an external IT entity] to Security Administrators.

6.3.4.2 *FMT_MOF.1/ManualUpdate Management of Security Functions Behavior*

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

[10] TD0333

6.3.4.3 *FMT_MOF.1/Services Management of Security Functions Behavior*

FMT_MOF.1.1/Services The TSF shall restrict the ability to enable and disable functions and services to Security Administrators.

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

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

6.3.4.5 *FMT_MTD.1/CryptoKeys Management of TSF Data*

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

6.3.4.6 *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 the authentication failure parameters for FIA_AFL.1; [
  - Ability to configure audit behaviour;
  - Ability to configure the cryptographic functionality;
  - Ability to configure thresholds for SSH rekeying;
  - Ability to set the time which is used for time-stamps].

6.3.4.7 *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

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*

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_EXT.1 Reliable Time Stamps*

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

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

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

6.3.5.6 *FPT_TUD_EXT.2 Trusted Update based on Certificates*

FPT_TUD_EXT.2.1 The TSF shall not install an update if the code signing certificate is deemed invalid.

FPT_TUD_EXT.2.2 When the certificate is deemed invalid because the certificate has expired, the TSF shall [not accept the certificate].

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 user-initiated termination of the user's own interactive session.

6.3.6.4 *FTA_TAB.1 Default TOE Access Banners*

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

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, *[update server]*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[transmission of audit data, acquisition of software updates, authentication requests]*.

6.3.7.2 *FTP_TRP.1/Admin Trusted Path*

FTP_TRP.1.1/Admin The TSF shall be capable of using [SSH] to provide a trusted communication path between itself and remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

FTP_TRP.1.2/Admin The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

6.4 Statement of Security Functional Requirements Consistency

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

7 Security Assurance Requirements

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

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

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

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

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

ADV_FSP.1.2C

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

ADV_FSP.1.3C

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

ADV_FSP.1.4C

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

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

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

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documents

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

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

AGD_OPE.1.2C

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

AGD_OPE.1.3C

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

AGD_OPE.1.4C

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

AGD_OPE.1.5C

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

AGD_OPE.1.6C

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

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

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

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life-cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

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

7.3.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 ***Evaluator action elements:***

ALC_CMC.1.1E

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

7.3.2 TOE CM coverage (ALC_CMS.1)

7.3.2.1 ***Developer action elements:***

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

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

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 ***Evaluator action elements:***

ALC_CMS.1.1E

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

7.4 Class ATE: Tests

7.4.1 Independent testing -- conformance (ATE_IND.1)

7.4.1.1 ***Developer action elements:***

ATE_IND.1.1D

The developer shall provide the TOE for testing.

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

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 ***Evaluator action elements:***

ATE_IND.1.1E

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

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

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

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

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

8 TOE Summary Specification

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

8.1 Security Audit

8.1.1 FAU_GEN.1:

The TSF generates audit records of the TOE's behavior. Within each of the audited events listed in Table 6-2 above, the TOE records at least the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Date and time is derived from the TOE's system clock provided by the underlying hardware. An administrator with Admin or Super role has the ability to manually set the time using the CLI. Generating/import of, changing or deleting cryptographic keys is audited also as well as what information is logged to identify the relevant key.

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 periodically. The user can enable and disable logs (security log, event log, and command log) that are sent to an SFTP server.

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

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. All events auditable events can be transmitted via syslog depending on how the syslog collectors are configured. The user can enable and disable logs (security log, event log, and command log) that are sent to an SFTP server.

The generation of an audit record for the generation or deletion of the SSH server key pair contains the date and time, id of the device, SOURCE (interface), USERID, and SSH Server key event (generate or delete). There is only ever one SSH key pair associated with the TOE. Therefore, there is no issue identifying the SSH Server Host Key in the audit trail.

Appendix A provides sample audit records of all the actions performed on the TOE that are logged and scoped by FAU_GEN.1: Table 6-2.

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_EXT.1:

The TOE is not an audit server; however, it does store audit data locally. Audit records are stored persistently on the TOE's local file system. 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 of 32MB, the oldest log file is automatically deleted, and the

remaining log files roll over in order to allow the new file to be created. There is no TSF provided means to modify audit records. However, the ability to delete logs from the audit trail is restricted to an administrator with Super role.

The TOE can be configured to transfer the log files to the remote SFTP server on an administratively configured timed interval. When a transfer is initiated by the TSF, the entire contents of the most recent log file are transferred. If the SFTP server connectivity is unavailable, the audit records will continue to be generated and stored within that log file until it reaches its allowed maximum size. The next transfer will again only attempt to send the entire contents of the most recent log file.

The TOE can also be configured to continuously send syslog messages to a syslog server via TLS. To use Syslog TLS, a private key must be created and an X.509 certificate must be signed and installed. An administrator with Super role will also need to configure the Syslog TLS OCSP client for X.509 certificate revocation checking. If Syslog Server connectivity is unavailable, audit records will only be stored locally. Upon re-establishment of communications with the Syslog Server, new audit records will resume being transmitted to it but the audit records that were generated during the time the Syslog Server connection was down remain stored locally and are not sent to the Syslog Server.

8.1.4 FAU_STG.1

The TOE prevents unauthorized deletion of the audit trail by requiring an administrator with Super role in order to delete the logs. The TOE's management interfaces do not provide any direct access to the file system so there is no administrative method of accessing this data to modify the content. See Section 8.1.3 FAU_STG_EXT.1 for full description of local audit behavior and storage.

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 DH Group 14 keys are generated to meet RFC 3526. The DH Group modulus size is 2048 bits. RSA supports 2048 bit key sizes. The ECC curves supported are P-256, P-384, and P-521. The following table lists the key generation algorithms that are supported by the TOE along with the trusted communications protocols that they are used for:

Algorithm/Protocol	TLS	SSHC	SSHS
RSA	**X**		
ECC	**X**	**X**	**X**
FFC (Diffie-Hellman Group 14)		**X**	**X**

Table 8-1: Cryptographic Key Generation

The TOE's key generation functions are validated under the following CAVP certificates:

RSA: #2903 and #3047

ECDSA: #1440 and #1531

The TSF generates asymmetric cryptographic keys using RSA, ECC and FFC algorithms. SSH is implemented for remote administration as well as sending audit data to the external audit server (SFTP server) for storage and retrieving updates from an update server via SFTP. TLS is implemented for

sending syslog data to the external syslog server for storage. TLS is also used for the communication between the TOE and the RADIUS server for remote authentication data.

8.2.2 FCS_CKM.2:

The TOE implements NIST SP 800-56A Revision 2 conformant key establishment mechanisms for Elliptic Curve Diffie-Hellman (ECDH) key establishment schemes. Specifically, the TOE complies with the NIST SP 800-56A Revision 2 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 Revision 1. The TOE complies with sections 5.9, 6, and 8 of NIST SP 800-56B Revision 1 (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. In accordance with RFC 3526, The TOE also implements Diffie-Hellman group 14 in support of SSH key establishment.

The TOE's key establishment function is validated under CAVP CVL certificate #1872 and #2048

The TOE acts as a sender and receiver for NIST SP 800-56A Revision 2 and 800-56B Revision 1 key establishment methods (as a TLS client and SSH client/server when elliptic-curve key establishment methods are used) and Diffie-Hellman group 14 key establishment methods (as an SSH server).

8.2.3 FCS_CKM.4:

The TOE performs key and cryptographic material destruction. There are no known instances where key destruction does not happen as defined below.

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 (Cortex)	Clearing of Key Material (Cavium 52XX and 6XXX)	Clearing of Key Material (Xeon D-500)
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	Overwrite logical erase blocks with 0xAB to clear cache, confirm with read-verify; then remap affected logical erase to new physical blocks while overwriting old physical blocks with 0xFF, confirmed with read-verify.	Overwrite with 0 to clear cache and read verify, then erase file
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	Overwrite logical erase blocks with 0xAB to clear cache, confirm with read-verify; then remap affected logical erase to new physical blocks while overwriting old physical blocks with 0xFF, confirmed with read-verify.	Overwrite with 0 to clear cache and read verify, then erase file

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

Table 8-2: Cryptographic Materials, Storage, and Destruction Methods

8.2.4 FCS_COP.1/DataEncryption:

The TOE performs encryption and decryption using the AES algorithm in CBC, CTR, and GCM mode with key sizes of 128 and 256 bits. This algorithm implementation is validated under CAVP AES certificate #5419 and #5665. The AES algorithm meets ISO 18033-3. Also, CBC meets ISO 10116 and GCM meets ISO 19772.

8.2.5 FCS_COP.1/SigGen:

In accordance with FIPS PUB 186-4 and ISO/IEC 9796-2, the TOE provides cryptographic digital signature verification using RSA Digital Signature Algorithm (rDSA). In accordance with FIPS PUB 186-4 and ISO/IEC 14888-3, the TOE also provides Elliptic Curve Digital Signature Algorithm (ECDSA). The TOE supports rDSA with a key size of 2048 bits. The TOE supports ECDSA with 256 and 512 bit key sizes for NIST curves P256, P-384, and P-521. These implementations are validated under CAVP RSA certificate #2903 and #3047, and CAVP ECDSA certificate #1440 and #1531.

8.2.6 FCS_COP.1/Hash:

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 and ISO/IEC 10118-3:2004. The TSF uses hashing services the following functions:

- SHA-1, SHA-256, and SHA-512 for SSH HMAC message authentication
- SHA-256 for RSA
- SHA-1, SHA-256, and SHA-384 for ECDSA
- SHA-512 for password hashing

The SHA algorithm implementation meets ISO/IEC 10118-3:2004 and is validated under CAVP SHS certificate #4350 and #4539.

8.2.7 FCS_COP.1/KeyedHash:

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 PUB 198-1, FIPS PUB 180-3, and ISO/IEC 9797-2:2011, Section 7 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 Section 7 and is validated under CAVP HMAC certificate #3589 and #3770.

8.2.8 FCS_RBG_EXT.1:

The TOE implements a NIST-approved deterministic random bit generators (DRBG). The DRBGs used by the TOE are CTR_DRBG and HMAC_DRBG. The TOE models uniformly provide a software-based entropy source as described in the proprietary entropy specification. The DRBG is seeded with a minimum of 256 bits of entropy so that it is sufficient to ensure full entropy for 256-bit keys, which are the largest keys generated by the TSF. The TOE's DRBG implementation meets ISO/IEC 18031:2011 and is validated under CAVP DRBG certificate #2114 and #2287.

8.2.9 FCS_SSHC_EXT.1/FCS_SSHS_EXT.1:

The TOE's SSHv2 implementation for remote CLI sessions complies with RFCs 4251, 4252, 4253, 4254, 5656, 6187, and 6668. There is no SSHv1 implementation on the TOE. The TOE implementation of SSHv2 supports public key authentication for authentication in addition to password-based authentication. SSH is used for remote administrators to connect securely to the TOE for use of the CLI, 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 262,144 bytes and drop in accordance with RFC 4253.

The TOE implementation of SSHv2 supports AES-CBC and AES-CTR for its encryption algorithm with 128 or 256 bit key sizes. The SSH server and client implementation can use only Diffie-Hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521 for key exchange methods. 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.

The TOE's SSH implementation uses ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, and x509v3-ecdsa-sha2-nistp521 as its public key algorithms. In addition, the SSH Client implementation supports the ssh-rsa public key algorithm. As for data integrity, the TOE supports hmac-sha-1, hmac-sha2-256, and hmac-sha2-512. The SSH connection will be rekeyed when either the rekey time threshold is reached or if the transfer size threshold is reached, whichever threshold is hit first.

The actual rekey thresholds are administratively configurable by a user with the Super role. The transfer size limit can be set to 1GB or 500MB in the evaluated configuration. The rekey time threshold must be set to 1 hour or less for the evaluated configuration and must not be turned off (setting to 0).

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. 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) as the reference identifiers. 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. The TOE will validate the server's certificate according to FIA_X509_EXT.1/Rev. If the server certificate is invalid, the connection will not

be established. Client-side certificates are presented when configured for TLS mutual authentication. Certificate pinning is not supported.

The following ciphersuites are supported:

- TLS_RSA_WITH_AES_128_CBC_SHA
- 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_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

8.3 Identification and Authentication

8.3.1 FIA_AFL.1:

The TOE detects how many unsuccessful logon attempts for users defined on the TOE itself. The threshold number of failed attempts can be configured by an administrator with the Super role starting at 1 and up to 5. Once the TOE's unsuccessful logon counter equals the threshold number of failed attempts, the account is locked and prevented from login until an administrator with the Super role manually unlocks the account or when the automatic unlocking countdown timer has expired. An administrator with the Super role can also configure the automatic unlocking timer. There is no default account that is exempt from lockout, however lockout of the local serial port connection is not supported to prevent a situation where no administration access is available.

8.3.2 FIA_PMG_EXT.1:

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

8.3.3 FIA_UAU_EXT.2:

Users can authenticate to the TOE using locally defined username/password credentials or using RADIUS. By default, the TOE queries its local database for user authentication. Users can be authenticated either by username and password, or by username and SSH public key if authenticating

remotely using SSH. The TSF displays an administratively configurable warning banner as part of the login screen. This is the only actions allowed prior to user identification and authentication.

At initial login, locally or through SSH, the administrative user is prompted to provide a username. The user provides either their username and password or their username and SSH key, depending on the method of authentication the TOE is configured to use. The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. 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_UAU.7:

While authenticating to the TOE with an incorrect login (specifically an invalid username and/or an invalid credential 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. Password entry is not echoed back to the screen.

8.3.5 FIA_UIA_EXT.1:

See FIA_UAU_EXT.2 above.

8.3.6 FIA_X509_EXT.1/FIA_X509_EXT.2/FIA_X509_EXT.3:

The TOE performs certificate validity checking for signed software updates, for TLS mutual authentication with the remote syslog server and RADIUS server, and potentially for SSH public key authentication if configured to do so. 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/ManualUpdate, FMT_MOF.1/Services, FMT_MOF.1/Functions:

The term "Security Administrator" is used to refer to any administrative user with the appropriate role with sufficient privilege to perform all relevant functions as scoped by the evaluation. Specifically, the TOE restricts the ability to perform manual updates, enabling and disabling services, and transmitting audit data to the Security Administrator. Section 8.3.9 below specifies the minimum privilege level needed to serve as a Security Administrator for each TOE function.

8.4.2 FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys:

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

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

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

The cryptographic keys that can be managed are the SSH and X.509 authentication keys and can only be managed by the Super role.

The TSF displays an administratively configurable warning banner as part of the login screen. This is the only actions allowed prior to user identification and authentication.

8.4.3 FMT_SMF.1:

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

Management Function	Minimum Role
Creation of user accounts and assignment to administrative roles	Super
Configuration of session inactivity time before session termination or locking	Admin
Administer the TOE locally and remotely	Admin
Configure the access banner	Super

Start and Stop services	Super
Update the TOE, and to verify the updates using digital signature capability prior to installing those updates;	Admin
Configuration of the authentication failure parameters	Super
Configuration of minimum password length	Super
Configuration and manual transfer of audit data to remote storage location	Super
Ability to set the time which is used for time stamps	Admin
Configure cryptographic functionality	Admin
Initiation and verification of system software/firmware update	Admin
Configure thresholds for SSH rekeying	Super
Configure the interaction between TOE components	Admin
Re-enable an Administrator account	Super
Configure the reference identifier for the peer	Super

Table 8-3: TSF Management Functions

8.4.4 FMT_SMR.2:

The TOE maintains three administrative roles: Limited, Admin, and Super. Each of these roles has a different set of authorizations associated with them. Users with any of these roles have the capability to manage the TSF locally or remotely and are considered to be administrators of the TSF for the functions that are assigned to their respective roles. An administrator may only have one role assigned to their account. The Security Administrator user is synonymous with an administrator with any of the three roles.

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 are hashed using SHA-512 and the hash is what is stored by the TOE. There is no function provided by the TOE to display a password value in plaintext.

8.5.2 FPT_SKP_EXT.1:

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

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

8.5.3 FPT_STM_EXT.1:

The TOE provides a source of date and time information, used in audit timestamps, in determining whether an administrative session has gone inactive, and also when determining if a certificate is valid. The clock function is reliant on the system clock provided by the underlying hardware. An administrator with Admin or Super role has the ability to manually set the time by entering the command:

```
system set date <yy-mm-dd> time <hh:mm:ss>
```

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

In the event that a self-test fails, the TOE will automatically reboot. If the TSF has been corrupted or the hardware has failed such that rebooting will not resolve the issue, an administrator with Admin or Super role will need to factory reset the TOE and/or replace the failed hardware component. These tests and their response to failures is sufficient to ensure that the TSF behaves as described in the ST because it would detect any unauthorized modifications to the TOE, failures or tampering of the hardware (which could be an attempt to compromise its storage or take the TOE out of the range of operating conditions specified for its entropy source), and any cryptographic failures that could result in the establishment of insecure trusted channels.

8.5.5 FPT_TUD_EXT.1:

The TOE provides the ability for an administrator with the Admin or Super role to update its software. The TOE has an SFTP client that is used to retrieve software updates from an SFTP server. This can be a server maintained by Ciena or one maintained by the organization operating the TOE, in which case updates are shipped on read-only physical media when made available by Ciena. The most current and most recently installed versions of the TOE's software or firmware can be queried via the "`software show`" command on the CLI.

In the evaluated configuration, the TOE is configured by an administrator with Admin or Super role to only accept signed updates. Updates provided by Ciena are signed using 2048-bit RSA certificate that is traceable back to an Entrust root CA. Certificate validation and revocation checking occurs every time an update is attempted.

A signed software load includes a signed hash of the rest of the software. In the evaluated configuration the signature is expected to be created with an X.509 certificate authority (CA) and a private key. Software signing is verified against the public key in the certificate. During the software installation process, the software release and signature file is prechecked against a locally stored copy of the CA certificate used to sign the software. SAOS looks for a .sig file that corresponds to a .gz file with a fingerprint matching the installed load signing certificate. Both files are used to verify the .gz file. Certificate expiration and revocation checking are also part of the validation checks. If the code signing certificate is deemed expired or invalid in any way, the TSF will reject the update, meaning the update process stops, and the invalid software image is deleted from the TOE's storage. The TOE generates an audit record of the failed attempt including the reason for failure along with the identifier of the invalid certificate. This process does not require administrative action and there is no administrative override

capability provided by the TSF. If the certificate is valid then the TSF will continue with the installation based on the parameters set forth in the software management command issued.

Software management comprises the following CLI options:

- `software install` — Software can be installed without becoming activated. A running package is software that is currently active. The administrator with Admin or Super role can specify if they want the installed software to be loaded on the next reboot.
- `software upgrade` — Upgrades software from one release to another. Once the software package is downloaded, the software is activated to become the running package.
- `software activate` — The software activate command validates previously installed software and uses that software version for the next boot. This command allows the administrator with Admin or Super role to choose whether it is service disrupting. This command fails if the administrator attempts to activate an invalid bank or the package does not exist on the device. A software activate can be used to cancel a previously executed install or activate by specifying the currently running bank.
- `software validate` — The software validate command validates the status of the standby bank and checks for its integrity.

8.5.6 FPT_TUD_EXT.2:

The certificate validation, including revocation checking, occurs every time an update is attempted. The certificate is validated according to FIA_X509v3_EXT.1/Rev. If the code signing certificate is deemed expired or invalid, the TSF will reject the update meaning, the update process stops, and the invalid software image is deleted from the TOE's storage The TOE generates an audit record of the failed attempt including the reason for failure along with the identifier of the invalid certificate.

8.6 TOE Access

8.6.1 FTA_SSL_EXT.1:

An 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 after an administrator-defined period of inactivity. As stated above, the Admin and Super role have the ability to define the inactivity period.

8.6.3 FTA_SSL.4:

The TOE provides the ability for administrators (Limited, Admin, or Super) to manually terminate their own sessions by issuing as many "quit" commands as is necessary to navigate to the highest level of the CLI, followed by an "exit" command. Additionally, when managing the TOE remotely, the terminal

application used on the management workstation will typically terminate the SSH session if the application itself is closed.

8.6.4 FTA_TAB.1:

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

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1:

The TOE provides the ability to secure sensitive data in transit to and from assured endpoints in the TOE's Operational Environment. In the evaluated configuration, the TOE is configured to transmit audit data to a remote audit server using SFTP, which uses SSH to secure communications. The TOE also uses TLS for syslog audit data transfer and for RADIUS authentication. The TOE uses OpenSSH to support SSH communications to the image update server.

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

8.7.2 FTP_TRP.1:

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

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

9 Appendix A: Audit Event Samples

SFR	Auditable Event	Sample Data
FAU_GEN.1.1a	Startup and Shutdown of function	**Startup of audit function (equivalent to system startup)** 1916: Sat Jan 1 00:01:32.680 2000 [local] Sev:7 chassis(1): :Ssh server x509-host-key set to enabled 1917: Sat Jan 1 00:01:37.000 2000 [local] Sev:7 chassis(1): :System Global Inactivity Timeout Set 7 1918: Sat Jan 1 00:01:37.000 2000 [local] Sev:7 chassis(1): :System Global Inactivity Timer Disable

		1919: Sat Jan 1 00:01:38.193 2000 [local] Sev:8 chassis(1): : Firewall closed for port 23 (Telnet Server) 1920: Sat Jan 1 00:01:38.810 2000 [local] Sev:7 chassis(1): :User Create ciena super 1921: Sat Jan 1 00:01:39.307 2000 [local] Sev:7 chassis(1): :User Create limiteduser limited 1922: Sat Jan 1 00:01:39.440 2000 [local] Sev:8 chassis(1): :Firewall opened for port 22 (SSH Server) 1923: Sat Jan 1 00:01:39.000 2000 [local] Sev:8 1 Active, MAC 00:23:8A:0B:D1:5E, Chassis MAC 00:23:8A:0B:D1:40 1924: Sat Jan 1 00:01:49.291 2000 [local] Sev:7 chassis(1): :Dot1x port state changed to authorized port 1 1 **Shutdown of audit function (equivalent to system shutdown)** 51819: Mon Jul 2 13:54:09.304 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' logged out from 192.168.2.51 due to shutdown 51820: Mon Jul 2 13:54:10.000 2018 [local] Sev:8 1 Shutdown
FAU_GEN.1.1.c	Administrative login and logout.	**Admin Login** 760: Mon Jun 11 15:26:55.243 2018 [local] Sev:8 chassis(1): Local RS-232 User ciena:User 'ciena' successfully logged in from ttyS0 **Admin Logout** 789: Mon Jun 11 16:25:13.577 2018 [local] Sev:8 chassis(1): Local RS-232 User ciena:User 'ciena' logged out from ttyS0
FAU_GEN.1.1.c	Changes to TSF data related to configuration changes.	**Configuration of Warning Banner** 2018-06-20T15:56:41-04:00 localhost [local] 192.168.2.111 00:23:8a:0b:d1:40 3905 CHASSIS-5-SYSTEM_LOGIN_BANNER_FILE_SET: chassis(1): :System Login Banner File Set /tmp/etc/loginBanner 2018-06-20T15:56:41-04:00 localhost [local] 192.168.2.111 00:23:8a:0b:d1:40 3905 CONFIG-5-CONFIG_CHANGED: chassis(1): Configuration Has Changed **Minimum Length Password Configuration** 2207: Wed Jun 13 09:59:37.288 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Minimum Password Length Set to 15
FAU_GEN.1.1.c	Generating/import of, changing, or deleting of cryptographic keys.	**Generate SSH Server Host Key** 55825: Fri Jul 13 10:42:44.307 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:SSH Generate Server Host Key **Delete SSH Server Host Key** 55824: Fri Jul 13 10:42:30.063 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:SSH Delete Server Host Key

		Traffic-Based SSH Rekey 1213: Tue Jun 12 11:54:35.946 2018 [local] Sev:8 chassis(1): :ssh[16317]: [16058]ssh_set_newkeys: rekeying after 16206 output blocks (259856 bytes total) 1214: Tue Jun 12 11:54:35.946 2018 [local] Sev:8 chassis(1): :ssh[16317]: [16058]ssh_set_newkeys: rekeying after 32813048 input blocks (525010504 bytes total) **Time-Based SSH Rekey** 1238: Tue Jun 12 12:00:59.988 2018 [local] Sev:8 chassis(1): :ssh[16431]: [16058]ssh_set_newkeys: rekeying after 4365 output blocks (196064 bytes total) 1239: Tue Jun 12 12:00:59.989 2018 [local] Sev:8 chassis(1): :ssh[16431]: [16058]ssh_set_newkeys: rekeying after 2638580 input blocks (117860888 bytes total)
FAU_GEN.1.1.c	Resetting passwords.	**limiteduser Password Change: abcdefghijklmnopqrstuvwxyzA12!** 2208: Wed Jun 13 10:07:47.678 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:User Password Set limiteduser
FAU_GEN.1.1.c	Starting and stopping services	**Enabling SSH** June 15, 2018 13:00:28.524 [local] Sev:8 chassis(1): :SSH Oper State Enabled June 15, 2018 13:00:28.524 [local] Sev:7 chassis(1): Local RS-232 User ttyS0: Configuration Has Changed June 15, 2018 13:00:28.526 [local] Sev:7 chassis(1): Local RS-232 User ciena:Ssh Enabled **Disabling SSH** June 15, 2018 13:00:18.048 [local] Sev:8 chassis(1): :SSH Oper State Disabled June 15, 2018 13:00:18.064 [local] Sev:7 chassis(1): Local RS-232 User ttyS0: Configuration Has Changed June 15, 2018 13:00:18.064 [local] Sev:7 chassis(1): Local RS-232 User ciena:Ssh Disabled
FCS_SSHC_EXT.1	Failure to establish an SSH session (SSH Client).	1117: Tue Jun 12 10:13:31.662 2018 [local] Sev:8 chassis(1): :ssh[15397]: [15304]Authenticating to 192.168.2.100:8022 as 'ciena' 1118: Tue Jun 12 10:13:31.662 2018 [local] Sev:8 chassis(1): :ssh[15397]: [15304]Unable to negotiate with 192.168.2.100 port 8022: no matching host key type found. Their offer: ssh-ed25519,ssh-ed25519
FCS_SSHS_EXT.1	Failure to establish an SSH session (SSH Server).	1559: Wed Jun 6 15:04:32.852 2018 [local] Sev:8 chassis(1): :sshd[12519]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive" 1560: Wed Jun 6 15:04:32.541 2018 [local] Sev:6 chassis(1): :User authentication failed from IP 192.168.2.51:63749 user name 'ciena'

		1561: Wed Jun 6 15:04:38.852 2018 [local] Sev:8 chassis(1): :sshd[12519]: error: PAM: Authentication failure for ciena from 192.168.2.51 1562: Wed Jun 6 15:04:38.852 2018 [local] Sev:8 chassis(1): :sshd[12519]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive"
FCS_TLSC_EXT.2	Failure to establish a TLS session (TLS Client).	**RADUIS** 51486: Thu Jun 28 16:26:39.805 2018 [local] Sev:8 chassis(1): RadSec beginning connection. Server: 192.168.2.100:2083 51487: Thu Jun 28 16:26:40.825 2018 [local] Sev:8 chassis(1): RadSec X.509 certificate verification failed. Subject: /C=US/ST=Maryland/L=Hanover/O=Ciena/OU=SNE/CN=CC-RADSEC-Server.ciena.local/emailAddress=CC-RADSEC-Server@no.where Server: 192.168.2.100:2083 51488: Thu Jun 28 16:26:40.826 2018 [local] Sev:8 chassis(1): RadSec Error: X509 verification error : unsupported certificate purpose. Server: 192.168.2.100:2083 **Syslog** 51446: Sat Jan 1 05:56:51.094 2000 [local] Sev:8 chassis(1): :SyslogTLS beginning connection. Collector: 192.168.2.102:60514 51447: Sat Jan 1 05:56:51.136 2000 [local] Sev:8 chassis(1): :SyslogTLS X.509 certificate verification fail. Subject: /C=US/ST=Maryland/L=Hanover/O=Ciena/OU=SNE/CN=CC-SFTP-Syslog-Server.ciena.local/emailAddress=CC-SFTP-Syslog-Server@no.where Collector: 192.168.2.102:60514 51448: Sat Jan 1 05:56:51.137 2000 [local] Sev:8 chassis(1): :SyslogTLS Error: X509 verification error : unsupported certificate purpose Dest: 192.168.2.102:60514
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	**Lockout Policy Set to 3 Attempts** 58195: Fri Jul 20 22:15:04.078 2018 [local] Sev:7 chassis(1): :User lockout settings changed: fail-limit: 3 -- time: 300 **User Failed Authentication 3 Times** 58268: Fri Jul 20 22:35:07.872 2018 [local] Sev:8 chassis(1): :sshd[12451]: Incoming connection from 192.168.2.51 port 60531 on 192.168.2.111 port 22 58269: Fri Jul 20 22:35:11.845 2018 [local] Sev:6 chassis(1): :User authentication failed from IP 192.168.2.51:60531 user name 'admin' 58270: Fri Jul 20 22:35:11.873 2018 [local] Sev:8 chassis(1): :sshd[12451]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive" 58271: Fri Jul 20 22:35:11.873 2018 [local] Sev:8 chassis(1): :sshd[12451]: Postponed keyboard-interactive for admin from 192.168.2.51 port 60531 ssh2 58272: Fri Jul 20 22:35:11.873 2018 [local] Sev:8 chassis(1): :sshd[12453]: pam_radsec_auth: Radsec not operationally enabled

		58273: Fri Jul 20 22:35:17.874 2018 [local] Sev:8 chassis(1): :sshd[12451]: error: PAM: Authentication failure for admin from 192.168.2.51 58274: Fri Jul 20 22:35:17.874 2018 [local] Sev:8 chassis(1): :sshd[12451]: Failed keyboard-interactive/pam for admin from 192.168.2.51 port 60531 ssh2 **4th Attempt with Valid Password** 58306: Fri Jul 20 22:35:52.834 2018 [local] Sev:6 chassis(1): :User authentication failed with a locked account from 192.168.2.51:60538 user name 'admin'
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	**Local Console – Username and Password Success** 2196: Wed Jun 13 09:48:56.326 2018 [local] Sev:8 chassis(1): Local RS-232 User ciena:User 'ciena' successfully logged in from ttyS0 **Local Console – Username and Password Failure** 2192: Wed Jun 13 09:47:56.300 2018 [local] Sev:6 chassis(1): :User authentication failed from IP ttyS0 user name 'ciena' **Local Console RADUIS – Username and Password Success** 263: Sat Jan 1 16:52:27.905 2000 [local] Sev:8 chassis(1): RadSec connection established. Server: 192.168.2.100:2083 265: Sat Jan 1 16:52:28.705 2000 [local] Sev:8 chassis(1): Local RS-232 User cdl:User successfully logged in from IP cdl user name 'ttyS0' **Local Console RADIUS – Username and Password Failure** 258: Sat Jan 1 16:52:14.651 2000 [local] Sev:8 chassis(1): RadSec connection established. Server: 192.168.2.100:2083 259: Sat Jan 1 16:52:15.708 2000 [local] Sev:6 chassis(1): :User authentication failed from IP ttyS0 user name 'baduser' **Remote SSH – Username and Password Success** 2139: Tue Jun 12 16:54:08.871 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User successfully logged in from IP ciena user name '192.168.2.51' **Remote SSH – Username and Password Failure** 2112: Tue Jun 12 16:53:28.799 2018 [local] Sev:8 chassis(1): :sshd[3235]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive" **Remote SSH Public Key – Username and Password Success** 55436: Wed Jul 11 11:27:55.321 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' successfully logged in from 192.168.2.51

		55437: Wed Jul 11 11:27:56.148 2018 [local] Sev:8 chassis(1): :sshd[1784]: Accepted publickey for ciena from 192.168.2.51 port 59414 ssh2: ECDSA SHA256:ce:ba:b1:ed:ed:cf:31:1d:94:f4:fe:cb:92:7f:c8:df:c7:cf:81:23:18:f2:ca:07:4a:5c:52:a9:73:51:61:1d 55438: Wed Jul 11 11:27:56.148 2018 [local] Sev:8 chassis(1): :sftp-server[1787]: session opened for local user ciena from [192.168.2.51] **Remote SSH Public Key – Username and Password Failure** 55455: Wed Jul 11 11:31:34.158 2018 [local] Sev:8 chassis(1): :sshd[1819]: Failed publickey for baduser from 192.168.2.51 port 59446 ssh2: ECDSA SHA256:ce:ba:b1:ed:ed:cf:31:1d:94:f4:fe:cb:92:7f:c8:df:c7:cf:81:23:18:f2:ca:07:4a:5c:52:a9:73:51:61:1d **Remote SSH RADIUS – Username and Password Success** 2181: Tue Jun 12 17:05:57.971 2018 [local] Sev:8 chassis(1): RadSec connection established. Server: 192.168.2.100:2083 2182: Tue Jun 12 17:05:58.666 2018 [local] Sev:8 chassis(1): RadSec connection closed normally. Server: 192.168.2.100:2083 2183: Tue Jun 12 17:05:58.005 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User cdl:User successfully logged in from IP cdl user name '192.168.2.51' **Remote SSH RADIUS – Username and Password Failure** 2148: Tue Jun 12 17:04:51.878 2018 [local] Sev:8 chassis(1): RadSec connection established. Server: 192.168.2.100:2083 2149: Tue Jun 12 17:04:52.933 2018 [local] Sev:6 chassis(1): :User authentication failed from IP 192.168.2.51:64090 user name 'cdl' 2151: Tue Jun 12 17:04:54.827 2018 [local] Sev:8 chassis(1): :sshd[3358]: error: PAM: Authentication failure for cdl from 192.168.2.51 2152: Tue Jun 12 17:04:54.827 2018 [local] Sev:8 chassis(1): :sshd[3358]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive"
FIA_UAU_EXT.2	All use of the authentication mechanism.	See “All use of the identification and authentication mechanism.”
FIA_X509_EXT.1/ Rev	Unsuccessful attempt to validate a certificate	2591: Wed Jun 20 16:59:30.462 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Beginning download of file /home/ciena/ca/int2CAFalse/int2CAFalse.cert.pem from SFTP server 192.168.2.101 2592: Wed Jun 20 16:59:31.289 2018 [local] Sev:6 chassis(1): SSH IP 192.168.2.51 User ciena:X.509 CA certificate install fail: Not a CA certificate

FMT_MOF.1/Functions	Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full.	1944: Tue Jun 12 14:48:54.926 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' successfully logged in from 192.168.2.51 1945: Tue Jun 12 14:50:11.589 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: SyslogTLS admin state set to disabled 1946: Tue Jun 12 14:50:27.508 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: SyslogTLS admin state set to enabled 1947: Tue Jun 12 14:50:49.922 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: SyslogTLS minimum TLS version set to TLSv1.0 1948: Tue Jun 12 14:51:08.561 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: SyslogTLS collector CC-SFTP-SYSLOG-SERVER.CIENA.LOCAL had port changed to 1234 **Command Log** | ID | Date & Time (Local) | User(privilege) on Terminal / Exit Status | +-------+-------------------------+--+ | 863 | Tue Jun 12 14:50:11 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | syslog tls disable | | Tue Jun 12 14:50:11 2018 | Status: 0 | +-------+-------------------------+--+ | 864 | Tue Jun 12 14:50:21 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | configuration save | | Tue Jun 12 14:50:22 2018 | Status: 0 | +-------+-------------------------+--+ | 865 | Tue Jun 12 14:50:27 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | syslog tls enable | | Tue Jun 12 14:50:27 2018 | Status: 0 | +-------+-------------------------+--+ | 866 | Tue Jun 12 14:50:30 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | configuration save | | Tue Jun 12 14:50:31 2018 | Status: 0 | +-------+-------------------------+--+

		| 867 | Tue Jun 12 14:50:49 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | syslog tls set minimum-tls-version TLSv1.0 | | Tue Jun 12 14:50:49 2018 | Status: 0 | +-------+-------------------------+----------+ | 868 | Tue Jun 12 14:51:07 2018 | ciena(super) /ssh_shell_192.168.2.51:62423 | | syslog tls set collector 192.168.2.102 port 1234 | | Tue Jun 12 14:51:08 2018 | Status: 0
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	55683: Sat Jan 1 00:29:01.687 2000 [local] Sev:8 chassis(1): :ssh[1824]: Authenticating to 192.168.2.102:22 as 'ciena' 55684: Sat Jan 1 00:29:01.687 2000 [local] Sev:8 chassis(1): :ssh[1824]: Authentication succeeded to 192.168.2.102 as 'ciena' (password) 55685: Sat Jan 1 00:29:01.688 2000 [local] Sev:8 chassis(1): :ssh[1824]: Connection to 192.168.2.102 as 'ciena' completed, exit status 0 55686: Sat Jan 1 00:29:01.789 2000 [local] Sev:7 chassis(1): :Commencing with software signature checking 55687: Sat Jan 1 00:29:01.850 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/ssct/saos-06-17-00-6664/le-6664.dernhelm.tar.xz.1E4277AE3D10A9C505368227381BB8A620A57C9B.sig from SFTP server 192.168.2.102 55688: Sat Jan 1 00:29:02.787 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/ssct/saos-06-17-00-6664/Certs/software-signing-cert.pem from SFTP server 192.168.2.102
FMT_MOF.1/Services	Starting and stopping of services.	**Enabling SSH** June 15, 2018 13:00:28.524 [local] Sev:8 chassis(1): :SSH Oper State Enabled June 15, 2018 13:00:28.524 [local] Sev:7 chassis(1): Local RS-232 User ttyS0: Configuration Has Changed June 15, 2018 13:00:28.526 [local] Sev:7 chassis(1): Local RS-232 User ciena:Ssh Enabled **Disabling SSH** June 15, 2018 13:00:18.048 [local] Sev:8 chassis(1): :SSH Oper State Disabled June 15, 2018 13:00:18.064 [local] Sev:7 chassis(1): Local RS-232 User ttyS0: Configuration Has Changed June 15, 2018 13:00:18.064 [local] Sev:7 chassis(1): Local RS-232 User ciena:Ssh Disabled
FMT_MTD.1/CoreData	All management activities of TSF data	**Local Console** 757: Mon Jun 11 15:26:27.055 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:System Global Inactivity Timer Enable

		758: Mon Jun 11 15:26:36.166 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:System Global Inactivity Timeout Set 3 **SSH Server** 1920: Sat Jan 1 00:01:38.810 2000 [local] Sev:7 chassis(1): :User Create ciena super 1921: Sat Jan 1 00:01:39.307 2000 [local] Sev:7 chassis(1): :User Create limiteduser limited **Remote SSH** June 11, 2018 17:09:49.601 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System TimeDate Set From Mon Jun 11 17:09:49 2018 To Mon Jun 11 17:09:49 2018 June 11, 2018 13:11:00.603 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System TimeDate Set From Mon Jun 11 17:09:49 2018 To Mon Jun 11 13:11:00 2018 June 11, 2018 13:11:03.360 [local] Sev:6 chassis(1): :System time changed backward by 3h58m49s
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	55824: Fri Jul 13 10:42:30.063 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:SSH Delete Server Host Key 55825: Fri Jul 13 10:42:44.307 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:Ssh Generate Server Host Key
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	**Success** 43694: Fri Jun 29 01:59:48.707 2018 [local] P Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: :Software install request, package-path: SFTP:192.168.2.102//home/ciena/packages/saos-08-06-01-198/rel_saos5170_8.6.1_ga198.tgz source: 192.168.2.102 43698: Fri Jun 29 02:00:10.056 2018 [local] P Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Commencing with software signature checking 43702: Fri Jun 29 02:00:12.102 2018 [local] P Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Software signature checking passed 43703: Fri Jun 29 02:00:48.604 2018 [local] P Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Software install success 43704: Fri Jun 29 02:03:35.526 2018 [local] P Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena: :Software activate request, revert timeout: 0 43732: Fri Jun 29 02:08:03.443 2018 [local] P Sev:7 chassis(1): Software activate success **Failure** 1699: Sat Jan 1 00:06:02.448 2000 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Software manager package upgrade request slot: 1, from pkg: saos-06-17-00-0195 to pkg: saos-06-17-00-0219 1700: Sat Jan 1 00:06:02.532 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-

		00-0219_3905_modified_sig/pmf-saos-06-17-00-0219.xml from SFTP server 192.168.2.102 1701: Sat Jan 1 00:06:03.487 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0219_3905_modified_sig/le-16536.chk from SFTP server 192.168.2.102 1702: Sat Jan 1 00:06:04.646 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0219_3905_modified_sig/le-16536.dernhelm.ins from SFTP server 192.168.2.102 1710: Sat Jan 1 00:06:05.750 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0219_3905_modified_sig/le-16536.dernhelm.tar.xz.0CC076298E53180BE829C78F6B6B7E1C9CE2DE3C.sig from SFTP server 192.168.2.102 1711: Sat Jan 1 00:06:06.671 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0219_3905_modified_sig/le-16536.dernhelm.tar.xz from SFTP server 192.168.2.102 1721: Sat Jan 1 00:06:13.765 2000 [local] Sev:7 chassis(1): :Software signature checking failed 1722: Sat Jan 1 00:06:13.810 2000 [local] Sev:7 chassis(1): :Sw Xgrade Complete operation: xgrade result: Invalid Signature
FPT_TUD_EXT.2	Failure of update.	55673: Sat Jan 1 00:28:58.357 2000 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Software manager package upgrade request slot: 1, from pkg: saos-06-17-00-6660 to pkg: saos-06-17-00-6664 55683: Sat Jan 1 00:29:01.687 2000 [local] Sev:8 chassis(1): :ssh[1824]: Authenticating to 192.168.2.102:22 as 'ciena' 55684: Sat Jan 1 00:29:01.687 2000 [local] Sev:8 chassis(1): :ssh[1824]: Authentication succeeded to 192.168.2.102 as 'ciena' (password) 55685: Sat Jan 1 00:29:01.688 2000 [local] Sev:8 chassis(1): :ssh[1824]: Connection to 192.168.2.102 as 'ciena' completed, exit status 0 55686: Sat Jan 1 00:29:01.789 2000 [local] Sev:7 chassis(1): :Commencing with software signature checking 55687: Sat Jan 1 00:29:01.850 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/ssct/saos-06-17-00-6664/le-6664.dernhelm.tar.xz.1E4277AE3D10A9C505368227381BB8A620A57C9B.sig from SFTP server 192.168.2.102 55688: Sat Jan 1 00:29:02.787 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/ssct/saos-06-17-00-6664/Certs/software-signing-cert.pem from SFTP server 192.168.2.102 55689: Sat Jan 1 00:29:03.649 2000 [local] Sev:7 chassis(1): :Software signature checking failed 55690: Sat Jan 1 00:29:03.672 2000 [local] Sev:7 chassis(1): :Sw Xgrade Complete operation: xgrade result: Unknown error

FPT_STM_EXT.1	Discontinuous changes to the time – either Administrator actuated or changed via an automated process.	June 11, 2018 17:09:49.601 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System TimeDate Set From Mon Jun 11 17:09:49 2018 To Mon Jun 11 17:09:49 2018 June 11, 2018 13:11:00.603 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System TimeDate Set From Mon Jun 11 17:09:49 2018 To Mon Jun 11 13:11:00 2018 June 11, 2018 13:11:03.360 [local] Sev:6 chassis(1): :System time changed backward by 3h58m49s
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	**Configuration of Timeout - 3 minutes** 757: Mon Jun 11 15:26:27.055 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:System Global Inactivity Timer Enable 758: Mon Jun 11 15:26:36.166 2018 [local] Sev:7 chassis(1): Local RS-232 User ciena:System Global Inactivity Timeout Set 3 **Admin Authenticated** 760: Mon Jun 11 15:26:55.243 2018 [local] Sev:8 chassis(1): Local RS-232 User ciena:User 'ciena' successfully logged in from ttyS0 **Session Ended Due to Inactivity** 761: Mon Jun 11 15:29:34.446 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' logged out from 192.168.2.51 due to inactivity
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	**Configuration of the Timeout - 3 minutes** 568: Fri Jun 8 20:52:10.391 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System Global Inactivity Timer Enable 569: Fri Jun 8 20:52:21.880 2018 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:System Global Inactivity Timeout Set 3 **Admin Authenticated** 573: Fri Jun 8 20:52:43.061 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' successfully logged in from 192.168.2.51 574: Fri Jun 8 20:52:43.367 2018 [local] Sev:8 chassis(1): :sshd[5957]: error: Could not load host key: /flash0/ssh/ssh_host_x509_key 575: Fri Jun 8 20:52:43.367 2018 [local] Sev:8 chassis(1): :sshd[5957]: Incoming connection from 192.168.2.51 port 49254 on 192. 168.2.111 port 22 **Session Ended Due to Inactivity** 576: Fri Jun 8 20:55:43.085 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' logged out from 192.168.2.51 due to inactivity

		577: Fri Jun 8 20:55:45.374 2018 [local] Sev:8 chassis(1): :sshd[5959]: Received disconnect from 192.168.2.51 port 49254:11: FlowSshClientSession: disconnected on user's request 578: Fri Jun 8 20:55:45.374 2018 [local] Sev:8 chassis(1): :sshd[5959]: Disconnected from user ciena 192.168.2.51 port 49254
FTA_SSL.4	The termination of an interactive session.	**User Logged Out of Local Session** 789: Mon Jun 11 16:25:13.577 2018 [local] Sev:8 chassis(1): Local RS-232 User ciena:User 'ciena' logged out from ttyS0 **User Logged Out of Remote Session** 2575: Wed Jun 20 16:25:10.719 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.51 User ciena:User 'ciena' logged out from 192.168.2.51
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**Initiation of Trusted Channel for Syslog** 44921: Sat Jan 1 00:16:16.384 2000 [local] Sev:8 chassis(1): :SyslogTLS beginning connection. Collector: 192.168.2.102:60514 44922: Sat Jan 1 00:16:16.582 2000 [local] Sev:8 chassis(1): :SyslogTLS X.509 certificate verified. Subject: /C=US/ST=Maryland/L=Hanover/O=Ciena/OU=SNE/CN=CC-SFTP-Syslog-Server.ciena.local/emailAddress=CC-SFTP-Syslog-Server@no.where Collector: 192.168.2.102:60514 44923: Sat Jan 1 00:16:16.583 2000 [local] Sev:8 chassis(1): :SyslogTLS connection established. Collector: 192.168.2.102:60514 **Termination of Trusted Channel for Syslog** 44918: Sat Jan 1 00:16:03.931 2000 [local] Sev:7 chassis(1): SSH IP ciena User 192.168.2.51: SyslogTLS collector CC-SFTP-SYSLOG-SERVER.ciena.local admin state set to disabled 44919: Sat Jan 1 00:16:03.931 2000 [local] Sev:8 chassis(1): :SyslogTLS connection closed normally. Collector: 192.168.2.102:60514 **Failure to Establish Trusted Channel for Syslog** 44947: Tue Jun 26 12:39:36.438 2018 [local] Sev:8 chassis(1): :SyslogTLS beginning connection. Collector: 192.168.2.102:60514 44948: Tue Jun 26 12:39:36.450 2018 [local] Sev:8 chassis(1): :SyslogTLS Error: TLS error during connect : sslv3 alert handshake failure Dest: 192.168.2.102:60514 **Initiation of Trusted Channel for RADIUS** 44965: Tue Jun 26 13:03:00.286 2018 [local] Sev:8 chassis(1): RadSec beginning connection. Server: 192.168.2.100:2083 44966: Tue Jun 26 13:03:00.460 2018 [local] Sev:8 chassis(1): RadSec X.509 certificate verified. Subject: /C=US/ST=Maryland/L=Hanover/O=Ciena/OU=SNE/CN=CC-

		RADSEC-Server.ciena.local/emailAddress=CC-RADSEC-Server@no.where Server: 192.168.2.100:2083 44967: Tue Jun 26 13:03:00.460 2018 [local] Sev:8 chassis(1): RadSec connection established. Server: 192.168.2.100:2083 **Termination of Trusted Channel for RADIUS** 44968: Tue Jun 26 13:03:01.162 2018 [local] Sev:8 chassis(1): RadSec connection closed normally. Server: 192.168.2.100:2083 **Failure of the Trusted Channel for RADIUS** 44992: Tue Jun 26 13:09:45.686 2018 [local] Sev:8 chassis(1): RadSec beginning connection. Server: 192.168.2.100:2083 44993: Tue Jun 26 13:09:45.699 2018 [local] Sev:8 chassis(1): RadSec Error: TLS error during connect : sslv3 alert handshake failure. Server: 192.168.2.100:2083 **Initiation of Trusted Channel for SFTP** 44830: Sat Jan 1 00:10:31.009 2000 [local] Sev:7 chassis(1): SSH IP 192.168.2.51 User ciena:Software manager package upgrade request slot: 1, from pkg: saos-06-17-00-0219 to pkg: saos-06-17-00-0226 44831: Sat Jan 1 00:10:32.088 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0226/pmf-saos-06-17-00-0226.xml from SFTP server 192.168.2.102 44832: Sat Jan 1 00:10:33.069 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0226/le-16614.chk from SFTP server 192.168.2.102 44833: Sat Jan 1 00:10:33.799 2000 [local] Sev:8 chassis(1): :ssh[1720]: Authenticating to 192.168.2.102:22 as 'ciena' 44834: Sat Jan 1 00:10:33.799 2000 [local] Sev:8 chassis(1): :ssh[1720]: Authentication succeeded to 192.168.2.102 as 'ciena' (password) **Termination of Trusted Channel for SFTP** 44835: Sat Jan 1 00:10:33.799 2000 [local] Sev:8 chassis(1): :ssh[1720]: Connection to 192.168.2.102 as 'ciena' completed, exit status 0 **Failure to Establish Trusted Channel for SFTP** 44819: Sat Jan 1 00:05:07.071 2000 [local] Sev:7 chassis(1): :Beginning download of file /home/ciena/packages/saos-06-17-00-0226/pmf-saos-06-17-00-0226.xml from SFTP server 192.168.2.102 44820: Sat Jan 1 00:05:07.641 2000 [local] Sev:7 chassis(1): :Sw Xgrade Complete operation: install result: An SFTP error was encountered during the file transfer 44821: Sat Jan 1 00:05:07.786 2000 [local] Sev:8 chassis(1): :ssh[1648]: Authenticating to 192.168.2.102:22 as 'ciena'

		44822: Sat Jan 1 00:05:07.787 2000 [local] Sev:8 chassis(1): :ssh[1648]: Unable to negotiate with 192.168.2.102 port 22: no matching MAC found. Their offer: hmac-md5
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	**Initiation of Trusted Path** 2530: Wed Jun 20 15:21:01.265 2018 [local] Sev:8 chassis(1): :sshd[21323]: Incoming connection from 192.168.2.52 port 33616 on 192.168.2.111 port 22 2531: Wed Jun 20 15:21:03.265 2018 [local] Sev:8 chassis(1): :sshd[21323]: Failed user authentication method, partial=0 next methods="publickey,password,keyboard-interactive" 2534: Wed Jun 20 15:21:06.392 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.52 User ciena:User 'ciena' successfully logged in from 192.168.2.52 **Termination of Trusted Path** 2536: Wed Jun 20 15:21:15.691 2018 [local] Sev:8 chassis(1): SSH IP 192.168.2.52 User ciena:User 'ciena' logged out from 192.168.2.52 2537: Wed Jun 20 15:21:17.266 2018 [local] Sev:8 chassis(1): :sshd[21326]: Received disconnect from 192.168.2.52 port 33616:11: disconnected by user 2538: Wed Jun 20 15:21:17.266 2018 [local] Sev:8 chassis(1): :sshd[21326]: Disconnected from user ciena 192.168.2.52 port 33616 **Failure of Trusted Path** 2540: Wed Jun 20 15:24:13.273 2018 [local] Sev:8 chassis(1): :sshd[21355]: Unable to negotiate with 192.168.2.52 port 33618: no matching cipher found. Their offer: 3des-cbc

Table 9-1: Sample Audit Records