Ciena 6500 Packet Optical Platform Security Target

Document Version: 1.0

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 0.1	July 2023	Initial Release
Version 0.2	August 2023	Edits based on vendor feedback
Version 0.3	September 2023	Minor edits
Version 0.4	January 2024	Updated Claims
Version 0.5	February 2024	Updated TSS and Technical Decisions
Version 0.6	August 2024	Updated TSS and Minor edits
Version 0.7	October 2024	Peer Review Updates for Check-Out
Version 0.8	November 2024	Peer Review Updates, Round 2
Version 0.9	December 2024	ECR Comments
Version 1.0	January 2025	Minor Updates

Contents

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Ciena 6500 Packet Optical Platform Security Target
ST Version	1.0
ST Date	January 2025
ST Author	Acumen Security
TOE Identifier	Ciena 6500 Packet Optical Platform
TOE Version	15.6
TOE Developer	Ciena Corporation
Key Words	Network Device, Optical, Switch

1.2 TOE Overview

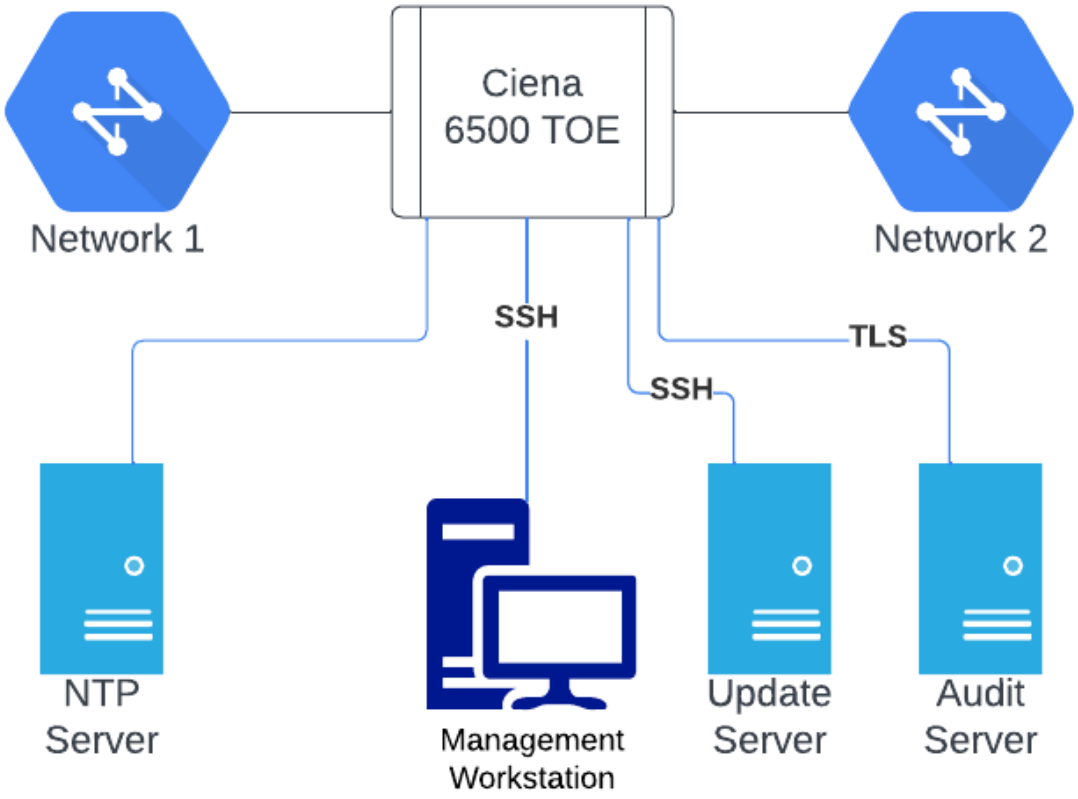
The TOE is the Ciena 6500 Packet Optical Platform running software version 15.6 and is developed by Ciena Corporation. The Ciena 6500 Packet Optical Platform, the Target of Evaluation (TOE), is a family of standalone hardware devices that run VxWorks and provide OSI Layers 1 and 2 network traffic management services. The security functions provided by the TOE include security auditing, cryptographic support, identification and authentication, security management, protection of TSF, TOE access controls, and trusted communications. The appliance provides the TL1 interface to the TOE's security management functionality. The TOE enables users to direct traffic to designated ports, giving them control of network availability for specific services. The system features an agnostic switch fabric that is capable of switching SONET/SDH, OTN, and Ethernet/MPLS networks. The switching behavior is beyond the scope of the claimed Protection Profile.

1.3 TOE Description

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. The Ciena 6500 has five shelf variants which range in size from 2RU (Rack Units) to 22RU (Rack Units). Each variant has the same software image loaded onto it and therefore each has the same security functionality across the family.

The five variants are:
6500-2
6500-4
6500-7
6500-14
6500-32

Figure 1 – Representative TOE Deployment



1.3.1 Physical Boundaries

The Physical boundary of the TOE is the Ciena 6500 Packet Optical Platform hardware appliance and the software which runs on it. The TOE runs VxWorks 6.9 for the SP3 and SPAP3 shelf processors. The TOE is managed using the Transaction Language 1 (TL1) interface, used for local or remote administration.

The TOE has two physical connections for security management: a local console (RJ-45 Craft ethernet port) for direct connections and a Central Office Local Area Network (COLAN) ethernet port for remote connections. An administrator can access the TL1 interface using either a local workstation connected directly to the TOE's Craft ethernet port or a remote workstation that can connect to the TOE over the COLAN ethernet via SSH. The TL1 interface is the command line interface for the TOE. The audit server communicates to the TOE via TLS; the update server communicates with the TOE using SFTP via SSH over the COLAN ethernet port. In practice, the TOE will be deployed to perform network switching functions and will be connected to a number of other pieces of network traffic infrastructure equipment. This has not been depicted in detail because this capability is out of scope of the TOE from a security functional perspective.

The TOE consists of any of the following models:

MODEL TYPE	MODEL PART #	SP3 Shelf Processor Card	SPAP3 Shelf Processor Card
2-slot Type 2	NTK503LA	NO	YES

4-slot Type	NTK503HA	YES	NO
7-slot	NTK503PA	YES	NO
7-slot type 2	NTK503KA	NO	YES
6500-7	NTK503RA	YES	NO
14-slot	NTK503BA NTK503CA NTK503CC NTK503GA NTK503AD NTK503BD NTK503CD NTK503SA	YES	NO
32-slot	NTK603AA NTK603AB	YES	NO

Models using the SP3 service card are running on QorIQ T1042 Quad Core processor, with VxWorks 6.9; models using SPAP3 Service Cards are runniong on QorIQ T1022 Dual Core processors with VxWorks 6.9.

The TOE software version is 15.6.

The TOE also includes the guidance documentation.

1.3.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

1.3.2.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE creates audit records for events related to security relevant events including authentication (success and failure, remote and local), cryptographic key management, session establishment (success and failure) and session termination, including for SSH communications. In addition, all actions corresponding to management functions are audited.
The TOE records, for each audited event, 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. Depending on the specific type of event, additional data may be included in the audit record.
Audit data is stored locally transmitted in real-time to the remote audit server via TLS-protected trusted channel. The local audit data keeps the most recent records by overwriting the oldest records when the maximum size threshold of the file is met. No filesystem access is allowed to ensure protection of local audit data from deletion or modification.

1.3.2.2 Cryptographic Support

The TOE provides cryptography in support of SSH for remote administration, and secure download of TOE updates. The TOE provides a TLS protected channel for remote storage of audit data. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications. Cryptographic keys are overwritten by zeroes by the TOE when they are no longer needed for their purpose.

The TOE collects entropy from a local hardware entropy source contained within the device to ensure sufficient randomness for secure key generation.

1.3.2.3 Identification and Authentication

All users must be identified and authenticated by the TOE before being allowed to perform any actions on the TOE, except viewing a banner. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum-security strength through the set of supported characters and configurable minimum password length. As part of connecting to the TOE locally, using the management workstation, password data is obfuscated as it is inputted.
The TOE detects when a configurable number of failed authentication attempts are made by a remote user. Once this configurable threshold of between 2 and 20 attempts has been met the TSF will automatically lock a user's account. The user's account can be unlocked after a configurable time period of between 0 and 300 seconds or can be unlocked by a Security Administrator with sufficient User Privilege Code (UPC) level.

1.3.2.4 Security Management

The TSF provides the TL1 interface for performing management functions remotely or locally. Also, the Security Administrator can use the Site Manager to pass commands to the TL1 interface. The functions that a Security Administrator can perform on the TL1 interface are determined by the Security Administrator's UPC value. The Security Administrator is the only administrative role that has the ability to manage the TSF, so it is the only role that is within the scope of the TOE. Apart from the Security Administrator, other roles that perform network management related functionality are not considered part of the TSF.

1.3.2.5 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 TSF prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-256. The TOE maintains system time with its local hardware clock, and can synchronize with up to 3 NTPv4 time sources. TOE software updates are acquired using SFTP and initiated using the TL1 interface. Software updates are digitally signed to ensure their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

1.3.2.6 TOE Access

The TOE can terminate inactive sessions after a Security 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 can also display a configurable banner on the TL1 interface that is displayed prior to use of any other security-relevant functionality.

1.3.2.7 Trusted Path/Channels

The Security Administrator establishes a trusted path to the TOE for remote administration using SSH. The TOE initiates a TLS-protected trusted channel to the remote audit data server. The TOE establishes a trusted channel (SSH) for downloading software updates from the update server using SSH.

1.3.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- Ciena 6500 Packet Optical Platform Security Target, v1.0 [ST]
- Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria, version 1.8 [AGD]

    - Externally Referenced Documents in the AGD
        - Ciena 6500 Packet-Optical Platform Administration and Security Release 15.6
        - Ciena 6500 Packet-Optical Platform TL1 Command Definition Release 15.6
        - Ciena 6500 Packet-Optical Platform User Interface Overview and Site Manager Fundamentals Release 15.6
        - Suite of Hardware Installation Manuals Release 15.6:
            - General Information
            - 2, 4, 7, 14, & 32 Slot Shelves (individual documents)

1.4 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 2 – Required Environmental Components

Component	Function
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. Alternatively, the workstation can physically be connected to the TOE using the craft port, which is an Ethernet port through which the TOE can be managed locally using a SSH Client
Audit Server	A properly configured audit data storage server implementing the Syslog over TLS protocol.
Update Server	A server that supports SSH/SFTP and that is used as a location for storing product updates that can be transferred to the TOE.
Site Manager Software (Optional)	The Site Manager software provides a graphical interface to the TL1 interface for managing the TOE. The Site Manager software is installed on the Management workstation and uses an SSH channel to connect to the TOE.

1.5 Product Functionality Not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:
HTTP server, FTP service, Telnet and SNMP services – these must be disabled in the evaluated configuration. The TOE also includes a number of strictly unevaluated features and functions, which are outside the scope of the evaluation.

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant)

2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [PP-ND]

2.3 Conformance Rationale

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table 3 identifies all applicable TDs.

Table 3 – Relevant Technical Decisions

Technical Decision	Applicable PP	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0527: Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	cpp_nd_v2.2e	Y	
TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	cpp_nd_v2.2e	Y	
TD0536: NIT Technical Decision for Update Verification Inconsistency	cpp_nd_v2.2e	Y	
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	cpp_nd_v2.2e	Y	
TD0546: NIT Technical Decision for DTLS -	cpp_nd_v2.2e	N	TOE does not claim DTLS

Technical Decision	Applicable PP	Applicable (Y/N)	Exclusion Rationale (if applicable)
clarification of Application Note 63			
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	cpp_nd_v2.2e	Y	
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	cpp_nd_v2.2e	N	The TOE does not support TLSS
TD0556: NIT Technical Decision for RFC 5077 question	cpp_nd_v2.2e	N	The TOE does not support TLSS
TD0563: NiT Technical Decision for Clarification of audit date information	cpp_nd_v2.2e	Y	
TD0564: NiT Technical Decision for Vulnerability Analysis Search Criteria	cpp_nd_v2.2e	Y	
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	cpp_nd_v2.2e	N	TOE does not claim DTLS nor TLSS
TD0570: NiT Technical Decision for Clarification about FIA_AFL.1	cpp_nd_v2.2e	Y	
TD0571: NiT Technical Decision for Guidance on how to handle FIA_AFL.1	cpp_nd_v2.2e	Y	
TD0572: NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	cpp_nd_v2.2e	Y	
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	cpp_nd_v2.2e	Y	
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	cpp_nd_v2.2e	Y	

Technical Decision	Applicable PP	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	cpp_nd_v2.2e	N	This TD is not applicable since the TOE is a hardware appliance.
TD0592: NIT Technical Decision for Local Storage of Audit Records	cpp_nd_v2.2e	Y	
TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server	cpp_nd_v2.2e	Y	
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	cpp_nd_v2.2e	N	The TOE is not a virtual device
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	cpp_nd_v2.2e	N	TOE does not support TLSS
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	cpp_nd_v2.2e	Y	
TD0638: NIT Technical Decision for Key Pair Generation for Authentication	cpp_nd_v2.2e	Y	
TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	cpp_nd_v2.2e	Y	
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	cpp_nd_v2.2e	Y	
TD0738: NIT Technical Decision for Link to Allowed-With List	cpp_nd_v2.2e	Y	
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	cpp_nd_v2.2e	Y	
TD0792: NIT Technical Decision:	cpp_nd_v2.2e	Y	

Technical Decision	Applicable PP	Applicable (Y/N)	Exclusion Rationale (if applicable)
FIA_PMG_EXT.1 - TSS EA not in line with SFR			
TD0800: Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	cpp_nd_v2.2e	N	The TOE does not support IPsec

3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 4 are drawn directly from the PP and any EPs/Modules/Packages specified in Section 2.2.

Table 4 – Threats

ID	Threat
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 tunnelling 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

ID	Threat
	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.

3.2 Assumptions

The assumptions included in Table 5 are drawn directly from PP and any relevant EPs/Modules/Packages.

Table 5 – Assumptions

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules 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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification)

ID	Assumption
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.

3.3 Organizational Security Policies

The OSPs included in Table 6 are drawn directly from the PP and any relevant EPs/Modules/Packages.

Table 6 – OSPs

ID	OSP
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.

4 Security Objectives

The security objectives have been taken directly from the claimed PP and any relevant EPs/Modules/Packages and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

There are no Security Objectives for the TOE.

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 7 – Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
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_ADMN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.

ID	Objectives for the Operational Environment
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

5 Extended Components Definition

5.1 Extended Security Functional Components

All extended components are sourced directly from [PP].

5.2 Extended Security Functional Requirements Rationale

All extended security functional components are sourced directly from [PP]. Exact conformance required by the PP also mandates inclusion of all applicable extended components defined in the PP.

6 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 8 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_NTP_EXT.1	NTP Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHC_EXT.1	SSH Client Protocol
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/Services	Management of Security Functions Behaviour
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
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing

Requirement	Description
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TUD_EXT.1	Trusted Update
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

6.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

6.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;
b) 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 9 – Security Functional Requirements and Auditable Events.

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 9*.*

Table 9 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_RBG_EXT.1	None	None
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity of new/removed time server.
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.1	Failure to establish a 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_PMG_EXT.1	None	None
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None	None
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.2	None	None
FMT_MOF.1/Functions	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None
FMT_MOF.1/Services	None	None
FMT_MTD.1/CoreData	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	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).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None
FTA_SSL.4	The termination of an interactive session	None
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism	None
FTA_TAB.1	None	None
FTP_ITC.1	• Initiation of the trusted channel • Termination of the trusted channel • Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt

Requirement	Auditable Events	Additional Audit Record Contents
FTP_TRP.1/Admin	• Initiation of the trusted path • Termination of the trusted path. • Failure of the trusted path functions.	None

Application note: Even though the FAU_GEN.1 entry in table above states auditable events as "none", the PP does include audit events as part of FAU_GEN.1.1.

6.2.1.2 FAU_GEN.2 User Identity Association

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

6.2.1.3 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. In addition [

- *The TOE shall consist of a single standalone component that stores audit data locally,*

].

FAU_STG_EXT.1.3
The TSF shall [*overwrite previous audit records according to the following rule: [overwrite oldest audit records]*] when the local storage space for audit data is full.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1
The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

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

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

6.2.2.2 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: [

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*

].

Application Note: This SFR has been updated as per TD0580 and TD0581

6.2.2.3 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 [:*
  - *logically addresses the storage location of the key and performs a* [*single] overwrite consisting of* [*zeroes*];

that meets the following: *No Standard*

6.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption
The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [*CBC, GCM, CTR*] *mode* and cryptographic key sizes [*128 bits, 256 bits*] that meet the following: *AES as specified in ISO 18033-3,* [*CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772*].

6.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

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, 384 bits, 521 bits]*

]
that meet the following: [

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

].

6.2.2.6 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

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

6.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-256, HMAC-SHA-384*] and cryptographic key sizes *[256 bits, 384 bits]* **and message digest sizes [*256 and 384*] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

6.2.2.8 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [*NTP v4 (RFC 5905)*].

FCS_NTP_EXT.1.2
The TSF shall update its system time using [

- Authentication using [*SHA256*] as the message digest algorithm(s);

].

FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

6.2.2.9 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 [*CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[1] platform-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.2.2.10 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254, [4344, 5656, 6668, 8308 section 3.1, 8332].*

FCS_SSHC_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user 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 *[32768]* bytes in an SSH transport connection are dropped.

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

FCS_SSHC_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [*rsa-sha2-256, rsa-sha2-512*] as its public key algorithm(s) and rejects all other public key algorithms.

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

FCS_SSHC_EXT.1.7
The TSF shall ensure that [*ecdh-sha2-nistp256*] and [*ecdh-sha2-nistp384*] 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 each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9
The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [*no other methods*] as described in RFC 4251 section 4.1.

6.2.2.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254 [*4344*, *5656, 6668, 8308 Section 3.1, 8332*].

FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [*no other method*].

FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than *[32768]* bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [*rsa-sha2-256, rsa-sha2-512*] as its public key algorithm(s) and rejects all other public key algorithms.

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

FCS_SSHS_EXT.1.7
The TSF shall ensure that [*ecdh-sha2-nistp256*] and [*ecdh-sha2-nistp384*] 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 each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

6.2.2.12 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1
The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *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*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [*the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN*]

FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- *Not implement any administrator override mechanism*

]

FCS_TLSC_EXT.1.4
The TSF shall [*present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups:* [*secp256r1, secp384r1, secp521r1*] *and no other curves/groups*] in the Client Hello.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[2 to 20]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [unlocking the account] is taken by an Administrator; prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].*

6.2.3.2 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 between [*8*] and [*128*] characters.

6.2.3.3 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;
- [*[respond to ICMP echo request with ICMP echo response]*].

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.

6.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

6.2.3.5 FIA_UAU.7.1 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**.

6.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates** .
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- 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:

- *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.

6.2.3.7 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 [*TLS*] and [*no additional uses*].

FIA_X509_EXT.2.2
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*not accept the certificate*].

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour.

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

6.2.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

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

6.2.4.3 FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services
The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators*.

6.2.4.4 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 Security Administrators.*

6.2.4.5 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*.

6.2.4.6 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 start and stop services;
    - Ability to manage the trusted public keys database;
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to manage the cryptographic keys;
    - Ability to configure the cryptographic functionality;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to configure the reference identifier for the peer;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to import X.509v3 certificates to the TOE's trust store;

].

6.2.4.7 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

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

are satisfied.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FTP_APW_EXT.1 Protection of Administrator Passwords

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

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

6.2.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)

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

6.2.5.3 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, synchronise time with an NTP server]*.

6.2.5.4 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), at the conditions [whenever keys are generated, continuously]*] to demonstrate the correct operation of the TSF: [*Cryptographic algorithm known answer tests, pair-wise consistency tests, continuous random number generator tests, SP 800-90B health tests, software integrity check*].

6.2.5.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1
The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [*the most recently installed version of the TOE firmware/software*].

FPT_TUD_EXT.1.2
The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [*digital signature*] prior to installing those updates.

6.2.6 TOE Access (FTA)

6.2.6.1 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

6.2.6.2 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.*

6.2.6.3 FTA_SSL.4 User-initiated Termination

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

6.2.6.4 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.

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 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, [*[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 *[audit, updates]*.

6.2.7.2 FTP_TRP.1/Admin Trusted Path

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

FTP_TRP.1.2/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*.

6.3 TOE SFR Dependencies Rationale for SFRs

The PP contains all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

6.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP, which is derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 10.

Table 10 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

6.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Ciena Corporation to satisfy the assurance requirements. The following table lists the details.

Table 11 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.

SAR Component	How the SAR will be met
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

7 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 12 – TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1	The TSF generates audit records of the TOE's behavior. Auditing is always functional and thus cannot be disabled or enabled. As a result, the startup and shutdown of audit functions is synonymous with the startup and shutdown of the TOE. Within each of the audited events listed above, the TOE records at least the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Additional attributes that the TOE records for specific events have been listed in the 'Additional Audit Record Contents' Column of Table 9 – Security Functional Requirements and Auditable Events. The date and time are derived from the TOE's hardware clock. This is shown in the following sample audit record example for the creation of a SSH certificate: "SHELF-1:<134>1 2018-05-21T17-42-15.000345Z 192.168.2.101 DBCHG OME-2C39C1A48438:SHELF-1 000973 DBCHGSEQ=719,DATE=18-05-21,TIME=17-42-15,USERID=ADMIN,SOURCE=CTAG, PRIORITY=GEN_TL1_CMD,STATUS=COMPLD:CRTE-SSH-KEYS:::KEYSIZE=2048,KEYTYPE=RSA" The generation of an audit record for the creation, importing and deletion of the SSH key pair contains the id of the device, date and time, USERID, SOURCE, PRIORITY, STATUS, KEYSIZE, and KEYTYPE. There is only ever one SSH key pair associated with the TOE. Therefore, there is no issue identifying the one key in the audit trail. However, the key is characterized by its KEYSIZE and KEYTYPE and the particular machine the key is on such as: 192.168.2.101. A similar audit record is generated for TLS keys when importing or deleting X509 certificates. The audit record contains the DN, SERIALNUMBER, ISSUER and Validity date of the certificate. The TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The audit records will display in different formats depending on where the audit record originated from. Each audit record generated contains all the required information (date and time of the event, type of event, subject identity, and the outcome of the event). See the Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria for a complete set of sample audit events.
FAU_GEN.2	The TOE ensures that each auditable event that is user-initiated includes the identity of the user that performed the function. This is shown in the following sample audit record: "SHELF-1:<133>1 2018-05-25T14:11:55.000786Z 192.168.2.101 SECU OME-2C39C1A48438:SHELF-1 000185 SHELF-1:18-05-25,14-11-55:YEAR=2018,LOGNAME=SECU400,LOGEVENT=ACT-USER,UID=\"SURVEIL\",UPC=1,PORTTYPE=SSH,PORTADDR=\"192.168.2.126:52124\",STATUS=DENY,EVTDESCR=\"Invalid login\""

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td>FAU_STG_EXT.1</td><td>The TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The security log is the record of events such as login/authentication, authorized commands, changes made in the network configuration. The AO contains the detailed information about the event such as what parameters were used. The TOE aggregates both the security log and the AO files into the local audit records file. The local audit record file contains all the information required to satisfy the PP requirements and is therefore the file that is subject to export to the external audit server.

The maximum audit size is approximate as the TSF limits the audit logs based on the number of records per log file or a combined file size of approximately 7MB of data. The security log holds a maximum of 1000 records or 800KB. The AO log holds a maximum of 9000 records or 4MB. For SP3, the local audit record holds a maximum of 1000 records or 800KB. For SPAP3, the local audit record holds a maximum of 3000 records or 2.5MB.

When a locally stored audit file has reached its defined maximum number of records allowed, or has reached the maximum file size, the oldest record is overwritten with new audit data. The TOE does not provide a user mechanism to delete or modify the locally-stored audit data and the filesystem is not accessible by any user of the TOE.

In the evaluated configuration, the TOE simultaneously transmits all audit events to the audit server over a TLS trusted channel.</td></tr>
<tr><td>FCS_CKM.1</td><td>The TOE generates 2048-bit asymmetric key for RSA providing support for SSHv2 and TLS according to FIPS PUB 186-4.
The TOE generates ECC keys over NIST curves P-256, P-384, and P-521 in accordance with FIPS PUB 186-4 Appendix B.4. ECC keys are used in support of SSH and TLS.
<table>
<tr><th>Key Generation</th><th>SFR</th><th>Usage</th></tr>
<tr><td>RSA</td><td>FCS_SSHC_EXT.1,
FCS_SSHS_EXT.1,
FCS_TLSC_EXT.1</td><td>SSH Server for administration and SSH Client for connections to an update server.
TLS client connections to a syslog server</td></tr>
<tr><td>Elliptic curve</td><td>FCS_SSHC_EXT.1,
FCS_SSHS_EXT.1,
FCS_TLSC_EXT.1</td><td>SSH Server for administration and SSH Client for connections to an update server
TLS Client for connections to an update server.</td></tr>
</table></td></tr>
<tr><td>FCS_CKM.2</td><td>The TOE implements ECC key establishment in accordance with SP 800-56Ar3. This key establishment scheme are used in support of SSH and TLS trusted channels.
<table>
<tr><th>Key Generation</th><th>SFR</th><th>Usage</th></tr>
<tr><td>Elliptic curve</td><td>FCS_SSHC_EXT.1,
FCS_SSHS_EXT.1,
FCS_TLSC_EXT.1</td><td>SSH Server for administration and SSH Client for connections to an update server</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td><table><tr><td></td><td></td><td>TLS Client for connections to an update server.</td></tr></table></td></tr>
<tr><td>FCS_CKM.4</td><td>The Diffie-Hellman Shared Secret, Diffie Hellman private exponent, and SSH session key are generated by the TOE and stored in volatile memory (RAM). These keys are destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization prior to releasing the memory free(). These keys are zeroized immediately after they are no longer needed (i.e. connection terminated or re-key) and when the TOE is shut down as well as when power is lost. Since zeroization occurs this is considered a consistent value and the use of zero’s is a non-CSP containing value.
The X.509v3 private keys and SSH private key are encrypted with a 256 bit AES key before being stored in non-volatile storage. This 256-bit AES symmetric key is stored as two halves. One half is stored in flash on the shelf-processor, the other half is stored in another device on the backplane, separate from the shelf processor. If the INIT-ZEROIZE TL1 command is invoked by the Security Administrator, the AES encryption key is destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization. This effectively destroys the SSH keys as the encrypted SSH private key is not recoverable. There are no known instances where key destruction does not happen as defined.
X.509v3 private keys are destroyed by logically addressing the storage location with zeroization using a single overwrite of zero’s.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using AES in CBC and CTR modes with 128 and 256-bit keys in support of SSH functionality. The TOE implements AES with 128-bit or 256-bit keys in GCM or CBC modes in support of TLS functionality.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE provides SHA2-256 and SHA2-384 hashing services in support of TLS. The TOE provides SHA2-256, SHA2-384, and SHA2-512 hashing services, offering 256 or 512 bit output MAC sizes, in support of SSH services. These are also used to compute the software integrity checksum.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE provides keyed hashing using HMAC-SHA2-256 and HMAC-SHA-384 used for TLS and SSH. The HMAC-SHA-256 key size is 256 bits, the block size is 512 bits, and the output MAC is 256 bits. The HMAC-SHA-384 key size is 384 bits, the block size is 1024 bits, and the output MAC is 384 bits.
<table>
<tr><th>Algorithm</th><th>Block Size</th><th>Key Size</th><th>Digest Size</th></tr>
<tr><td>HMAC-SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
</table></td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides RSA and ECDSA signature generation and verification. RSA keys are 2048 bits, while ECDSA keys are 256, 384, or 521 bits. These keys are used in support of SSH and TLS.
<table>
<tr><th>Protocol</th><th>ECDSA Key Size</th><th>RSA Key Size</th></tr>
<tr><td>TLS</td><td>P-256 and P-384</td><td>2048 bits</td></tr>
</table></td></tr>
</table>

Requirement	TSS Description
	SSH | P-256 and P-521 | 2048 bits
FCS_NTP_EXT.1	The TOE implements NTP version 4, in accordance with RFC 5905. The TOE verifies that the received timestamp is from an authenticated time server by using SHA2-256 as the authentication algorithm.
FCS_RBG_EXT.1	The TOE implements a NIST-approved deterministic random bit generator (DRBG) as specified in ISO/IEC 18031:2011. The DRBG used by the TOE is the CTR_DRBG (AES). The TOE models provide an FPGA hardware-based entropy source as described in the proprietary Entropy Analysis Report (EAR). 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.
FCS_SSHC_EXT.1 FCS_SSHS_EXT.1	The TOE (SSH client) downloads updates from the update server using SFTP over an SSH trusted channel. When acting as an SSH client, the TOE supports using either public key or password-based authentication. The TOE SSH server functionality is for remote administrative connections over SSHv2. When the TOE acts as an SSH server, only public key authentication is supported. Once the public key is verified the admin can login. The TOE implements SSHv2 that complies with the following RFCs: 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1, and 8332. The TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms (and has an associated identity), and ECDH-SHA2-NISTp256 or ECDH-SHA2-NISTp384 as the key exchange algorithms. The TOE drops packets larger than 32,768 bytes meeting the requirements of RFC 4253. The TOE implementation of SSHv2 supports AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR for its encryption algorithms. Data integrity is assured using HMAC-SHA2-256. The SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first. The TOE authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key as specified in RFC 4251 Section 4.1. No additional optional characteristics are claimed.

FCS_TLSC_EXT.1	The TOE acts as a TLS client for transmission of audit data to an external audit service. It supports the following ciphersuites: • *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* • *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256* • *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384* The TOE uses administrator-configured reference identifiers according to RFC 6125 section 6, as well as IPv4 Address in CN or SAN, IPv6 Address in the CN or SAN. Wildcards are supported. IP addresses are converted to binary in network byte order using standard decimal-to-binary encoding, which is then encoded in hex according to the canonical format defined in RFC 3986 and RFC 5952. The TOE presents the Supported Elliptic Curves extension with the following curves: secp256r1, secp384r1, and secp521r1. These are supported by default on the TOE and don't require configuration.

Requirement	TSS Description
FIA_AFL.1	The TOE uses a counter to keep track of the number of unsuccessful authentication attempts that occur per user. The authentication failure threshold is configurable by a Security Administrator with UPC >=4 and can be set between 2 and 20. Once the authentication failure threshold is reached, the TOE prevents further authentication attempts by locking that users account. The TOE will prevent the user from successfully authenticating until a Security Administrator with a UPC >=4 unlocks the accounts or the account is automatically unlocked after a configurable period of between 0 and 300 seconds, with 0 meaning no automatic locking, i.e. user account is not locked out. The counter is reset to zero upon a successful authentication provided it is accomplished prior to the authentication failure threshold being met and the account being locked. Security Administrators with a UPC>=4 are exempt from being locked out over the local connection to ensures that remote authentication failures cannot cause a denial of service.
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 special characters. The supported special characters include “!”, “@”, “#”, “$”, “%”, “^”, “*”, “(”, “)”, “””, “’”, “+”, “-”, “_”, “/”, “<”, “=”, “>”, “{“, “}”, “\” and “~”. A Security Administrator has the ability to set the minimum length that is permitted to any value between 8 and 128. In the evaluated configuration passwords must be set to 8 characters or greater. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the 6500.
FIA_UIA_EXT.1	The TOE requires the use of locally-defined authentication credentials. Users are not allowed to perform any security-relevant functions on the TOE without first being successfully identified and authenticated by the TOE’s authentication method, with the exception of viewing the warning banner. At initial login, via the TL1 ACT-USER command, the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and credential are correct) or indicates that the login was unsuccessful. The TOE stores username and password hash data in the local storage for the TL1 interfaces. The TOE will respond to ICMP echo requests with an ICMP echo response. The TOE supports remote authentication using SSH public keys. Local authentication is handled with username/password.
FIA_UAU.7	When a user enters their password at the local console, the password characters entered by the user are not echoed back to the console.
FIA_X509_EXT.1/ Rev	Because the TOE is only a TLS client, the TOE performs certificate validation when RootCA and IntermediateCA certificates are first installed on the TOE for its own use in validating trust chains, and when peer certificates are presented to the TOE during authentication steps. The TOE does not have or present a certificate of its own. Certificates are validated to ensure that they have the correct basicConstraints for the certificate type, and that all presented certificates terminate in a root of

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>Trust. The peer certificate gets checked for SAN and CN while the validating CA certificate uses basicConstraint checking.
Validation includes:
That the presented certificates terminate in a root of trust. If the peer does not present its entire trust chain, the TOE will use its installed CA certificates to validate the peer. If the peer's identity does not match the configured reference identifier set by the administrator, the connection is refused.
That the current date and time lies between the validity dates for all certificates in the trust chain.
That the basicConstraints extension is included, with the CA flag set to "TRUE", for all CA certificates in the chain of trust
That the extendedKeyUsage field in the peer's certificate has the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1)
That the digital signatures are correct for all certificates, and there has been no loss in transit
That none of the certificates in the trust chain are revoked.
Certificate revocation checking is performed using the OCSP as specified in RFC 6960. The certificate is checked on each TLS Client connection and if the TOE cannot reach the revocation server then the TOE will reject the certificate and deny the connection.</td></tr>
<tr><td>FIA_X509_EXT.2</td><td>X.509v3 certificates are only used for TLS, in which the TOE acts as a client. The TOE has no certificates of its own, except certificates installed to validate peers.

When a connection to the OCSP server cannot be established, the TOE will reject the presented certificate and deny the connection.</td></tr>
<tr><td>FMT_MOF.1/Functions</td><td>The TOE restricts the management of audit data functionality to Security Administrators. This includes the transmission of audit data to the audit server. Security administrators are defined by their UPC levels, which are shown below:
<table>
<tr><th>Level</th><th>Functions Permitted</th></tr>
<tr><td>1</td><td>(monitoring only – no provisioning, maintenance or administration) – Retrieve allows retrieve and report related commands to be executed.</td></tr>
<tr><td>2</td><td>(maintenance but no provisioning) – Control allows access to control and retrieve commands but not to provisioning. Maintenance access provides the ability to reset performance monitoring counts.</td></tr>
<tr><td>3</td><td>(provisioning but no administration) – Provisioning allows access to provision, test, edit and retrieve commands.</td></tr>
<tr><td>4</td><td>(provisioning and administration) – Administration allows complete access to all commands.</td></tr>
<tr><td>5</td><td>(provisional and administration) – Surveillance allows complete access to all commands.</td></tr>
</table></td></tr>
</table>

Requirement	TSS Description
	The ability to determine the behavior of and modify the behavior of the transmission of audit data to an external IT entity is restricted to administrators with a UPC level of >=4. The administrator is able to configure the IP, reference identifiers and trusted certificate authorities for remote syslog connections by using the TL1 command interface or Site Manager via SSH or local craft ethernet port.
FMT_MOF.1/ManualUpdate	The TOE restricts the ability to perform manual software updates via the update server to Security Administrators.
FMT_MOF.1/Services	The TOE restricts the ability to enable and disable the remote syslog service and SSH service to Security Administrators with (UPC>=4). The enabling and disabling of the remote syslog service affects the audit behavior and is covered under the FMT_SMF.1 selection of "ability to configure audit behavior". The enabling and disabling of the SSH service affects remote administrative access and obtaining update files from the remote repository. Disabling SSH services can be accomplished with the following command: • ED-SH:6500SP3::CTAG:::,,SERVER=DISABLED,,,,,,,,; Enabling SSH services can be accomplished with the following command: • ED-SH:6500SP3::CTAG:::,,SERVER=ENABLED,,,,,,,,; Disabling remote syslog service can be accomplished with the following command: • SET-SYSLOG-SERVER:6500-SP3::CTAG::SERVER1:STATE=DISABLED,,,TLSSTATE=ENABLED,,,,; Enabling remote syslog service can be accomplished with the following command: • SET-SYSLOG-SERVER:6500-SP3::CTAG::SERVER1:STATE=ENABLED,,,TLSSTATE=ENABLED,,,,; Note: "TLS State" is required to be enabled on the TOE to ensure that syslog traffic is sent securely via a TLS channel from the TOE.
FMT_MTD.1/CoreData	The TOE restricts access to the management functions to Security Administrators. No management function of TSF data is available prior to login. The product provides five administrator roles on its TL1 interface. Each of the five Security Administrator roles, has a fixed set of allowed operations based on the UPC value (1 through 5) assigned to the Security Administrator. A larger UPC value provides more capabilities for the Security Administrator. Non-administrative users are not allowed to manipulate the TSF data at any time. The TOE restricts access to the x.509v3 certificate trust store to security administrators and no other users. Non-administrative users are not allowed the ability to manipulate the TSF data at any time.
FMT_MTD.1/CryptoKeys	Only the Security Administrator can manage cryptographic keys. This includes key generation for symmetric and asymmetric keys and key

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>destruction/zeroization. Secret and private keys cannot be seen by Security Administrators.
SSH Public keys are also managed by Security Administrators for users authenticating to the TOE.
TLS and X509 keys are managed by the security administrator for the purpose of syslog functions.
All keys and their options are shown below:
<table>
<tr><th>Option Available</th><th>Key Type</th></tr>
<tr><td>Generate</td><td>TLS, X509, SSH</td></tr>
<tr><td>Import</td><td>TLS, X509, SSH</td></tr>
<tr><td>Modify</td><td>TLS, X509, SSH</td></tr>
<tr><td>Delete</td><td>TLS, X509, SSH</td></tr>
</table>
All supported keys and their purposes can be found in Table 14 – Cryptographic Key Destruction Table.</td></tr>
<tr><td>FMT_SMF.1</td><td>The TOE provides all the capabilities necessary to securely manage the TSF. The TOE includes an SSH and TL1 interface to administer the functions associated with day-to-day operations of the TOE. The TL1 interface can be accessed locally or via the Site Manager graphical front-end that resides on a remote PC and connects to the TOE via SSH. The Site Manager translates user activity into equivalent TL1 commands. The management functionality via TL1 or Site Manager is identical.
The following management functions are supported by the TOE:
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 start and stop services;
Ability to manage the trusted public keys database;
Ability to modify the behaviour of the transmission of audit data to an external IT entity;
Ability to manage the cryptographic keys;
Ability to configure the cryptographic functionality;
Ability to re-enable an Administrator account;
Ability to set the time which is used for time-stamps;
Ability to configure NTP;
Ability to configure the reference identifier for the peer;</td></tr>
</table>

Requirement	TSS Description
	○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; ○ Ability to import X.509v3 certificates to the TOE's trust store;].
FMT_SMR.2	The Security Administrator role as defined by the NDcPP is met through the Security Administrator role with a UPC between 1 and 5 that is defined for the TL1 interface and remote administration over SSH. Each of the five Security Administrator roles, has a fixed set of allowed operations based on the UPC value assigned to the Security Administrator. A larger UPC value provides more capabilities for the Security Administrator. These Security Administrators manage the TOE locally and remotely using SSH via the TL1 interface of the TSF.
FPT_APW_EXT.1	Administrator passwords are not stored in plaintext on the TOE. All administrative passwords are hashed using SHA-256 and the hash is what is stored on the TOE. There is no function provided by the TOE to display a password value in plaintext.
FPT_SKP_EXT.1	The TOE does not provide a mechanism to view secret keys and key material. The fingerprint of the public key data that is stored on the TOE can be viewed by a Security Administrator depending on their UPC level: node SSH public key (UPC>=1), SSH server host keys (UPC>=2), and SSH client authorized keys or the X.509v3 certificates used for TLS authentication (UPC>=4). In the case of the public key with known hosts, only the fingerprint of the key is observable. 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 therefore, there is no administrative method of accessing this data. The X.509v3 private keys and SSH private key are encrypted with a 256 bit AES key before being stored in non-volatile storage (filesystem).
FPT_STM_EXT.1	The TOE provides source date and time information for use in audit timestamps, tracking administrator session inactivity for session termination, automatically unlocking an account after the administrator defined period of time, X.509 certificate expiry, and for determining when SSH rekeying should occur. The clock function is reliant on the system clock provided by the underlying hardware. A Security Administrator with UPC >=4 has the ability to manually set the time using the following TL1 command: ED-DAT:::CTAG::[yy-mm-dd],[hh-mm-ss] Additionally, the administrator (UPC>=3)can configure the TOE to accept time from as many as three NTP servers, authenticated using SHA2-256. The TOE does not rely on any underlying virtual system for time updates as the TOE is a standalone hardware product.
FPT_TST_EXT.1	The TOE runs a series of self-tests during initial start-up to verify its correct operation. As part of the startup of the TOE, the TOE will perform a series of known answer tests, pair-wise consistency tests, continuous random number

Requirement	TSS Description

	generator tests, SP 800-90B health tests to verify the correct functionality of the cryptographic functions.
	• Known answer tests - A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the KAT test fails.
	• Pair-wise consistency tests - The test is run when a RSA or ECDSA asymmetrical key pair is generated. The system uses the private key to sign the specific data, and then uses the public key to authenticate the signed data. If the authentication is successful, the test succeeds.
	• Continuous random number generator tests - Runs when a random number is generated. The system compares the generated random number with the previously generated random number. If the two numbers are the same, the test fails.
	• SP800-90B health tests
	  ○ Repetition Count Test (RCT) – the goal of the Repetition Count Test is to quickly detect catastrophic failures that cause the noise source to become “stuck” on a single output value for a long period of time.
	  ○ Adaptive Proportion Test (APT) – the Adaptive Proportion Test is designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source.
	Additionally, the TOE performs a software integrity check using SHA2-256. The TOE calculates a SHA2-256 hash of the installed firmware and compares it with the known value to verify the software integrity during power-up.
	In the event that a cryptographic self-test or the software integrity check fails, the TOE will create a log to indicate which self-test failed. These tests and the responses to failures are sufficient to ensure that the TSF is functioning in the manner that is described in the ST because they will detect unauthorized modified of the TOE software image and detect improperly functioning cryptography which could lead to insecure trusted channels.

FPT_TUD_EXT.1	The TOE provides the ability for a Security Administrator with UPC >=4 to update its software from the TL1 interface. The TOE, acting as the SSH client, will use SFTP via SSH to retrieve software updates from an update 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 and then loaded onto the update server, which must support SFTP via SSH, in the Operational Environment. Updates are digitally signed and verified using ECDSA using the P-521 elliptic curve with SHA-384. Once the update has been loaded on the TOE, the digital signature of the software upgrade is verified. The upgrade process will stop if the digital signature verification fails and the downloaded software release will be flushed from the device’s temporary memory. After successful digital signature validation, the Security Administrator must load the update into flash memory, by executing the LOAD-UPGRD command, where it remains until invoked. Invoking the update requires the Security Administrator to execute the INVK-UPGRD command to install the upgrade onto the shelf processor and then forces the TOE to reboot.

Requirement	TSS Description
	The Security Administrator will then need to reauthenticate to the TOE and commit the upgrade using the CMMT-UPGRD command. The Security Administrator can query the currently executing version and most recently installed version using the following commands after authenticating to the TOE: RTRV-RELEASE:::CTAG; RTRV-SW-VER:::CTAG; Note: The update will not be completed if the digital verification fails. The TOE supports delayed activation for trusted updates only when a valid update file is downloaded from the update server. The TOE performs a check on the image when it is fetched from the update server via SFTP. If the update file is an illegitimate image, the TOE will not load the image into flash memory and it will generate an error log. If the update file is legitimate, the administrator will have to commit the upgrade manually after a successful fetch of the image.
FTA_SSL.3	The Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface. By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. The TOE will terminate a remote TL1 session after a Security Administrator-defined period of inactivity. Additionally, there is an inactivity timer for SSH with a default of 30 minutes.
FTA_SSL.4	The TOE provides the ability for administrators to manually terminate their own sessions. Both the TL1 interface and Site Manager use the CANC-USER command. These commands apply to both local and remote usage. Additionally, when managing the TOE remotely, the terminal application used on the management workstation will terminate the SSH session if the application itself is closed.
FTA_SSL_EXT.1	The Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface. By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. When a local session is inactive for the configured period of time the TOE will terminate the session, requiring the Security Administrator to establish a new session, including authenticating to the TOE.
FTA_TAB.1	The TOE displays a configurable warning banner on the local and remote interface prior to a user supplying their authentication credentials. Remote authentication requires the use of SSH. Local authentication requires the use of the RJ-45 craft ethernet port. The warning banner is configured by a Security Administrator with a UPC >=4.
FTP_ITC.1	The TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. In the evaluated configuration, the TOE, acting as the TLS client, pushes audit data periodically to a remote audit server. The identity of the audit server is verified by checking the administrator-configured reference

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>identifier. Additionally, the TOE, acting as an SSH client, retrieves software updates via the update server using SFTP protected by SSH. The table below shows the usage of these protocols and which SFR they map to:

<table><tr><th>Protocol</th><th>Usage</th></tr><tr><td>SSH</td><td>FCS_SSHC_EXT.1</td></tr><tr><td>TLS</td><td>FCS_TLSC_EXT.1
FIA_X509_EXT.1</td></tr></table>
The TOE relies on the CAVP-validated cryptographic algorithm implementation used to establish these trusted channels.</td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>All remote administrative communications, regardless of which logical interface they originate from, take place over a secure encrypted SSHv2 session. For these secure connections the TOE acts as a SSH server and is compliant with FCS_SSHS_EXT.1. The TOE relies on the CAVP-validated cryptographic algorithm implementation used to establish these trusted channels.</td></tr>
</table>

7.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in the table below.

Table 13 – CAVP Algorithm Certificate References

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #	TOE OE
FCS_CKM.1	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	Ciena 6500 Packet-Optical Family Version 15.6	RSA KeyGen FIPS PUB 186-4	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
	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	Ciena 6500 Packet-Optical Family Version 15.6	ECDSA KeyGen FIPS PUB 186-4 ECDSA KeyVer FIPS PUB 186-4	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core

FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	Ciena 6500 Packet-Optical Family Version 15.6	KAS-ECC-SSC sp800-56Ar3	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
FCS_COP.1/ DataEncryption	AES used in [CBC, GCM, and CTR] mode and cryptographic key sizes [128 bits, 256 bits]	Ciena 6500 Packet-Optical Family Version 15.6	AES-CBC AES-CTR AES-GCM	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
FCS_COP.1/ SigGen	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	Ciena 6500 Packet-Optical Family Version 15.6	RSA-SigGen FIPS PUB 186-4 RSA-SigVer FIPS Pub 186-4	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
	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	Ciena 6500 Packet-Optical Family Version 15.6	ECDSA-SigGen FIPS PUB 186-4 ECDSA-SigVer FIPS PUB 186-4	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
FCS_COP.1/ Hash	[SHA-256, SHA-384, SHA-512] and message digest sizes [256, 384, 512] bits	Ciena 6500 Packet-Optical Family	SHA-256 SHA-384 SHA-512	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core

		Version 15.6			VxWorks 6.9 on QorIQ T1042 Dual Core
FCS_COP.1/ KeyedHash	[HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [256 bits, 384 bits] and message digest sizes [256] bits	Ciena 6500 Packet-Optical Family Version 15.6	HMAC-SHA-256 HMAC-SHA-384	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core
FCS_RBG_EXT.1	CTR_DRBG (AES)	Ciena 6500 Packet-Optical Family Version 15.6	Counter DRBG	A5421	VxWorks 6.9 on QorIQ T1022 Dual Core VxWorks 6.9 on QorIQ T1042 Dual Core

7.2 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 14 – Cryptographic Key Destruction Table

Keys/CSPs	Purpose	Generation	Storage Location	Method of Zeroization
SSH Server RSA Private Key	SSH host authentication for remote administrative session	Generated internally when the SSH service on the TOE is first started, or when a new keypair is requested by the administrator	Underlying file system	Logical address storage location; single overwrite with zeroes
SSH Client RSA private key	SSH host authentication for talking to other servers	Generated internally when the SSH service on the TOE is first started, or when a new keypair is requested by the administrator	Underlying file system	Logical address storage location; single overwrite with zeroes
SSH Session Encryption Key	Provides bulk encryption and authentication for SSH sessions	Generated during SSH session establishment	RAM	Single overwrite with zeroes

Keys/CSPs	Purpose	Generation	Storage Location	Method of Zeroization
SSH Session ECDH key	Key exchange during SSH sessions	Generated during SSH session establishment	RAM	Single overwrite with zeroes
TLS Client session keys	Message authentication and encryption in TLS sessions	Generated during TLS session establishment	RAM	Single overwrite with zeroes
X.509v3 Private Key	TLS session key agreement	Imported to the TOE when the TOE's certificate is first installed	Underlying file system	Logically addressing the storage location; single overwrite with zeroes

8 Acronym Table

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CRL	Certificate Revocation List
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EP	Extended Package
GUI	Graphical User Interface
IP	Internet Protocol
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RSA	Rivest, Shamir & Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification
UPC	User Privilege Code