ciena : the network specialist

Ciena 6500 Packet Optical Platform

Security Target

ST Version: 1.0
August 6, 2018

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
Booz Allen Hamilton
1100 West Street
Laurel, MD 20701

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

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

1.1 ST Reference

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

1.1.1 ST Identification

ST Title:	Ciena 6500 Packet Optical Platform Security Target
ST Version:	1.0
ST Publication Date:	August 6, 2018
ST Author:	Booz Allen Hamilton

1.1.2 Document Organization

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

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

Chapter 3 describes the conformance claims made by this ST.

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

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

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

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

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

1.1.3 Terminology

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

Term	Definition
TL1 [Management Interface]	The Transaction Language 1 (TL1) management interface is a TL1-compatible command shell interface that can be used to administer the TOE locally or remotely using SSH. This is used to perform functions that may be modified during ongoing administration of the TOE. The TL1 interface can be used by Site Manager or for direct CLI invocation.
Administrator	A user of the TOE that has an Administrator's User Privilege Code (UPC), which is a value in the range 1 to 5. TOE users with this role will configure and manage the TOE security functions and manages audit records.
User Privilege Code	A User Privilege Code (UPC) is a numerical value that is associated with TOE functions and with administrative accounts. An administrative account is authorized to perform a given function if its UPC is greater than or equal to that of the desired function.

Table 1-1: Customer Specific Terminology

Term	Definition
Security Administrator	The claimed Protection Profile defines a Security Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the Administrator's User Privilege Code (UPC), which is a value in the range 1 to 5.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

Table 1-2: CC Specific Terminology

1.1.4 Acronyms

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

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
COLAN	Central Office Local Area Network
CPU	Central Processing Unit
CSP	Critical Security Parameter
DHE	Diffie-Hellman Ephemeral

DRBG	Deterministic Random Bit Generator
FTP	File Transfer Protocol
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MPLS	Multiprotocol Label Switching
NDcPP	collaborative Network Device Protection Profile
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
OTN	Optical Transport Network
PP	Protection Profile
RSA	Rivest Shamir Adelman (encryption algorithm)
RU	Rack Unit
SAR	Security Assurance Requirement
SDH	Synchronous Digital Hierarchy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SONET	Synchronous Optical Networking
SSH	Secure Shell
ST	Security Target
TFTP	Trivial File Transfer Protocol
TL1	Transaction Language One
TOE	Target of Evaluation
TP	Tool Port
TSF	TOE Security Function
UPC	User Privilege Code
VLAN	Virtual Local Area Network

Table 1-3: Acronym Definition

1.1.5 References

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

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model CCMB-2012-09-001, Version 3.1 Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[6] ISO/IEC 18033-3:2010, Information Technology-Security techniques-Encryption algorithms—Part3: Block ciphers

[7] ISO/IEC 10116:2017, Information Technology-Security techniques-Modes of operation for an n-bit block cipher

[8] ISO/IEC 9796-2:2010, Information Technology -- Security techniques -- Digital signature schemes giving message recovery—Part 2 Integer factorization based mechanisms

[9] ISO/IEC 14888-3:2016, Information Technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms

[10] ISO/IEC 10118-3:2004, Information Technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[11] ISO/IEC 9797-2:2011, Information Technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function

[12] ISO/IEC 18031:2011, Information Technology -- Security techniques -- Random bit generation

[13] FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[14] FIPS PUB 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation January 2018

1.2 TOE Reference

The TOE is the Ciena 6500 Packet Optical Platform, which is a packet-optical switching platform. It is also known as the Ciena 6500. The Ciena 6500 contains 14 models together with the shelf processor (SP2 or SPAP2): NTK503LA (SPAP2), NTK503PA (SP2), NTK503KA (SPAP2), NTK503RA (SP2), NTK503BA (SP2), NTK503CA (SP2), NTK503CC (SP2), NTK503GA (SP2), NTK503AD (SP2), NTK503BD (SP2), NTK503CD (SP2), NTK503SA (SP2), NTK603AA (SP2), NTK603AB (SP2).

Each of these devices runs software release 12.3 and provides identical security functionality to one another.

1.3 TOE Overview

The Ciena 6500 S-Series and D-Series Packet Optical Platform, the Target of Evaluation (TOE), is a family of standalone hardware devices that run VxWorks and provide OSI Layer 0/1/2 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.

The Ciena 6500 has four shelf variants which range in size from 2RU to 22RU. Each variant has the same software image loaded onto it and therefore each has the same security functionality across the family. The four variants are:

- 6500-2
- 6500-7
- 6500-14
- 6500-32

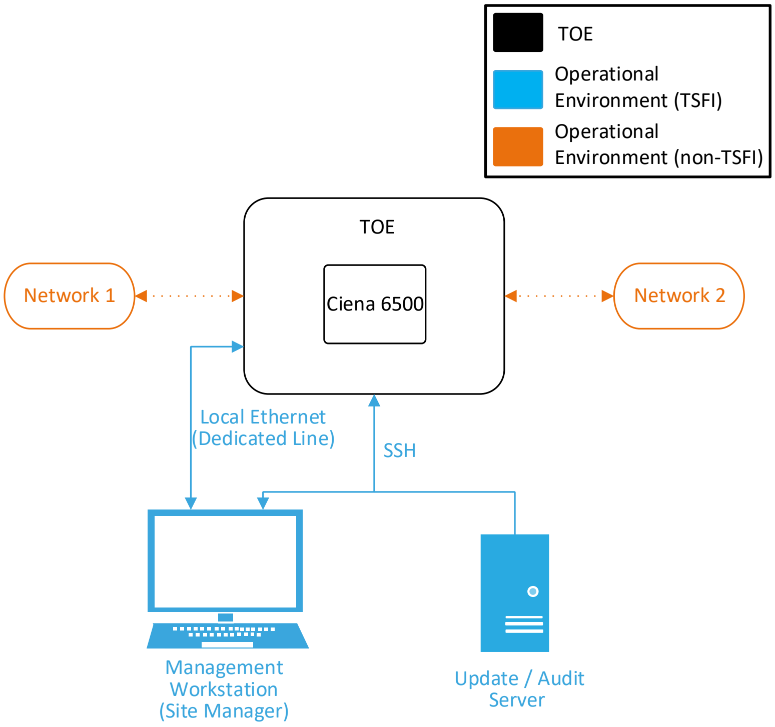
TOE
Operational Environment (TSFI)
Operational Environment (non-TSFI)
TOE
Ciena 6500
Network 1
Network 2
Local Ethernet (Dedicated Line)
SSH
Management Workstation (Site Manager)
Update / Audit Server

Figure 1-1: TOE Boundary

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 and update server communicate 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.

1.4 TOE Type

The TOE type for the Ciena 6500 is Network Device. The TOE is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDcPP defines a network device as “a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.” In addition, the NDcPP states “Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches.” The TOE is a family of standalone hardware devices that run VxWorks and provide OSI Layer 0/1/2 network traffic management services. The TOE type is justified because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise.

2 TOE Description

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

2.1 Evaluated Components of the TOE

The TOE is the Ciena 6500 Packet Optical Platform. This is a family of products that contains the following hardware models:

Model Type	Model Part #	SP2 Service Card PowerQUICC II Processor with VxWorks 6.3 NTK555CA NTK555EA NTK555FA	SPAP2 Service Card PowerQUICC II Processor with VxWorks 6.1 NTK555NA NTK555NB
2-slot Type 2	NTK503LA	No	Yes
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

Table 2-1: Hardware Model Information

The TOE software version is Release 12.3.

Each of these hardware models is a standalone network appliance.

2.2 Components and Applications in the Operational Environment

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

Component	Definition
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications. 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 general-purpose computer that runs a script to pull audit records from the TOE automatically, using the TL1 interface over SSH/secure file transfer protocol (SFTP).

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	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.

Table 2-2: Components of the Operational Environment

2.3 Excluded from the TOE

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

2.3.1 Not Installed

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

2.3.2 Installed but Requires a Separate License

No components are installed that require a separate license.

2.3.3 Installed but Not Part of the TSF

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

- FTP, HTTP(S), TELNET, SNMP – these protocols must be locked (disabled) in the evaluated configuration.

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

2.4 Physical Boundary

The physical boundary of the TOE includes the Ciena 6500 Packet Optical Platform hardware appliance and the software that runs on it.

The TOE guidance documentation that is considered to be part of the TOE can be found in the Common Criteria-specific guidance for the Ciena 6500 Packet Optical Platform, which is delivered on physical media to customers purchasing the equipment and is also made available on the Ciena website.

2.4.1 Software

The operating system used by the TOE is VxWorks 6.3 for the SP2 shelf processor and VxWorks 6.1 for the SPAP2 shelf processor. The TOE is managed using the Transaction Language 1 (TL1) interface. This interface can be used for either local administration or secure remote administration using SSH.

2.5 Logical Boundary

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

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

2.5.1 Security Audit

The TOE 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 and is pulled by a remote audit server via an automated script, using SFTP over an SSH 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.

2.5.2 Cryptographic Support

The TOE provides cryptography in support of SSH for remote administration, remote storage of audit data, and secure download of TOE updates. The TOE provides cryptography in support of SSH for remote administration, remote storage of audit data, and secure download of TOE updates. Diffie-Hellman group 14 asymmetric key generation and key establishment used by the TSF conforms to RFC 3526, Section 3. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications:

SFR	Algorithm	CAVP Cert. #
FCS_COP.1/DataEncryption	AES	4855
FCS_RBG_EXT.1	DRBG	1706
FCS_COP.1/SigGen	ECDSA	1244
FCS_COP.1/KeyedHash	HMAC	3250
FCS_CKM.1 and FCS_COP.1/SigGen	RSA	2666
FCS_COP.1/Hash	SHS	3992

Table 2-3: Cryptographic Algorithm Certificates

Cryptographic keys are overwritten by zeroes by the TOE when they are no longer needed for their purpose.

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

2.5.3 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 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 7200 seconds or can be unlocked by a Security Administrator with sufficient UPC level (privilege).

2.5.4 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.

2.5.5 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The 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. 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.

2.5.6 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.

2.5.7 Trusted Path/Channels

The Security Administrator establishes a trusted path to the TOE for remote administration using SSH. An audit server establishes a trusted channel (SSH) to the TOE to pull audit data from the TOE using SFTP. The TOE establishes a trusted channel (SSH) for downloading software updates from the update server using SFTP.

3 Conformance Claims

3.1 CC Version

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

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through 6 August 2018.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 3 conformant to include all applicable NIAP and International interpretations through 6 August 2018.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profile:

- *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* [NDcPP]

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

		Changes			**Analysis to this evaluation**	
TD #	**Title**	**SF R**	**A A**	**Notes**	**NA**	**Reason**
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	X	X		X	AA: TSS, AGD, and Test Not claiming IPSEC
TD0342	NIT Technical Decision for TLS and DTLS Server Tests		X		X	AA: Test Not claiming TLSS
TD0341	NIT Technical Decision for TLS wildcard checking			X	X	Not claiming TLSX
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	X			X	Not claiming FIA_X509
TD0339	NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	X	X	X		AA: TSS and Test
TD0338	NIT Technical Decision for Access Banner Verification		X			AA: TSS
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	X	X	X		AA: Test
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8		X			AA: Test

TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites			X	X	Not claiming DTLS or TLSS
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported		X			AA: Test
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	X	X	X	X	AA: AGD and Test Not claiming FIA_X509
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1		X			AA: Test SAR FSP.1-1 and -2 wording Affects AAR
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list		X		X	AA: Test Not claiming DTLS
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list		X		X	AA: Test Not claiming TLSS Supersedes TD0262
TD0321	Protection of NTP communications			X		
TD0291	NIT technical decision for DH14 and FCS_CKM.1	X				
TD0290	NIT technical decision for physical interruption of trusted path/channel.		X			AA: TSS and Test
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e		X		X	AA: Test Not claiming TLSC
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey		X			AA: Test
TD0260	NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4	X				
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	X		X		
TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4		X		X	AA: Test Not claiming DTLSC or TLSC
TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication		X		X	AA: Test Not claiming TLSC
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation		X		X	AA: Test Not claiming X509

Table 3-1: Technical Decisions

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

- The Technical Decision does not apply to the NDcPP
- The Technical Decision applies to an SFR that was not claimed by the TOE

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

3.5 Package Claims

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

- FCS_SSHC_EXT.1
- FCS_SSHS_EXT.1
- FMT_MOF.1/Functions

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

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

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

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are only claiming exact conformance to the claimed NDcPP.

3.7 Conformance Claim Rationale

The NDcPP states the following: “This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device. It provides a minimal set of security requirements expected by all network devices that target the mitigation of a set of defined threats. This baseline set of requirements will be built upon by future cPPs to provide an overall set of security solutions for networks up to carrier and enterprise scale. A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of this cPP (a more extensive description of distributed network device TOEs is given in section 3).” In addition, the NDcPP states “Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches”.

The TOE is a family of hardware appliances that is designed to perform low-level network traffic switching between SONET/SDH, OTN, and Ethernet/MPLS switches. As such, it can be understood as a network switch. Therefore, the conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

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

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

	confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 4-1: TOE Threats

4.2 Organizational Security Policies

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

Policy	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Table 4-2: TOE Organization Security Policies

4.3 Assumptions

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

Note: the NDcPP also defines the assumption A.COMPONENTS_RUNNING. However, the NDcPP also states that this applies to distributed TOEs only. Since the Ciena 6500 is not a distributed TOE, the TOE's Operational Environment does not include this assumption.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4-3: TOE Assumptions

4.4 Security Objectives

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

Note: This section only discusses environmental objectives because the NDcPP does not contain TOE objectives.

4.4.1 Security Objectives for the Operational Environment

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

Objective	Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4-4: TOE Operational Environment Objectives

Note: the NDcPP also defines OE.COMPONENTS_RUNNING. However, the NDcPP also states that this applies to distributed TOEs only. Since the Ciena 6500 is not a distributed TOE, the TOE’s Operational Environment does not include this assumption.

4.5 Security Problem Definition Rationale

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

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required. Therefore the “Extended” used in SFR component name will be dropped.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

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

- **Assignment:** allows the specification of an identified parameter. Indicated with *italicized* text.
- **Refinement:** allows the addition of details. Indicated with **bold** text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with <u>underlined</u> text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR and/or separated by a "/" with a notation that references the function for which the iteration is used, e.g. "/TrustedUpdate" for an SFR that relates to update functionality.

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

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

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
	FAU_STG.1	Protected Audit Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	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_RBG_EXT.1	Random Bit Generation
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol

Class Name	Component Identification	Component Name
Identification and Authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UIA_EXT.1	User Identification and Authentication
Security Management	FMT_MOF.1/ManualUpdate	Management of Security Functions Behavior
	FMT_MOF.1/Functions	Management of Security Functions Behavior
	FMT_MOF.1/Services	Management of Security Functions Behavior
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
Trusted Path /Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1/Admin	Trusted Path

Table 6-1: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class FAU: Security Audit

6.3.1.1 *FAU_GEN.1 Audit Data Generation*

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
   - Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
   - Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
   - Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
   - Resetting passwords (name of related user account shall be logged).
   - [[Starting and stopping services]];
d) Specifically defined auditable events listed in Table **6-2**.

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

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

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

Requirements	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Services	Starting and stopping of services	None.
FMT_MTD.1/CoreData	All management activities of the TSF	None
FMT_MTD.1/CryptoKeys	Management of cryptographic keys	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process.	For discontinuous changes to time: the old and new values for the time. Origin of the attempt to change time for success and failure (e.g. IP address)
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted channel. Termination of the trusted path. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 6-2: Auditable Events

6.3.1.2 *FAU_GEN.2 User Identity Association*

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

6.3.1.3 *FAU_STG_EXT.1 Protected Audit Event Storage*

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

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

6.3.1.4 *FAU_STG.1 Protected Audit Trail Storage*

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

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

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation*

FCS_CKM.1.1[1] The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

6.3.2.2 *FCS_CKM.2 Cryptographic Key Establishment*

FCS_CKM.2.1 The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3].

6.3.2.3 *FCS_CKM.4 Cryptographic Key Destruction*

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method:

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
    - logically addresses the storage location of the key and performs a [single]-pass overwrite consisting of [zeroes]]

that meets the following: No Standard.

[1] TD0291

6.3.2.4 *FCS_COP.1/DataEncryption Cryptographic Operation (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, 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].

6.3.2.5 *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, 3072 bits*]
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*512 bits*]]

that meet the following: [

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

].

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

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

6.3.2.7 *FCS_COP.1/KeyedHash Cryptographic Operation (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-1, HMAC-SHA-256] and cryptographic key sizes [*160 bits, 256 bits*], and message digest sizes [160, 256] bits that meet the following: ISO/IEC 9797-2:2011, Section 7, “MAC Algorithm 2”.

6.3.2.8 *FCS_RBG_EXT.1 Random Bit Generation*

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [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*] hardware based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.3.2.9 *FCS_SSHC_EXT.1 SSH Client Protocol*

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

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

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

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

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

FCS_SSHC_EXT.1.6[4] The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha1-96, 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 [diffie-hellman-group14-sha1] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

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

[2] TD0337

[3] TD0259

[4] TD0337

6.3.2.10 *FCS_SSHS_EXT.1 SSH Server Protocol*

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

FCS_SSHS_EXT.1.2[5] The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [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[6] The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr].

FCS_SSHS_EXT.1.5[7] The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6[8] The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha1-96, 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 [diffie-hellman-group14-sha1] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

6.3.3 Class FIA: Identification and Authentication

6.3.3.1 *FIA_AFL.1 Authentication Failure Management*

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

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

[5] TD0339
[6] TD0260 & TD0337
[7] TD0259
[8] TD0337

6.3.3.2 *FIA_PMG_EXT.1 Password Management*

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “,^”, “*”, “(”, “)” [“””, “’”, “+”, “-”, “_”, “/”, “<”, “=”, “>”, “{“, “}”, “\”, “~”]]

b) Minimum password length shall be configurable **from** [*8*] **to** [*128 characters*].

6.3.3.3 *FIA_UAU_EXT.2 Password-based Authentication Mechanism*

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, and [no other authentication mechanism(s)] to perform local administrative user authentication.

6.3.3.4 *FIA_UAU.7 Protected Authentication Feedback*

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

6.3.3.5 *FIA_UIA_EXT.1 User Identification and Authentication*

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

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions]

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

6.3.4 Class FMT: Security Management

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

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

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

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.

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

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

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

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

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

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

6.3.4.6 *FMT_SMF.1 Specification of Management Functions*

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [
  - Ability to configure audit behaviour;
  - Ability to configure the cryptographic functionality;
  - Ability to re-enable an Administrator account;
  - Ability to set the time which is used for time-stamps]

6.3.4.7 *FMT_SMR.2* *Restrictions on Security Roles*

FMT_SMR.2.1 The TSF shall maintain the roles:

- Security Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions**:**

- 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.

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 *FPT_APW_EXT.1 Protection of Administrator Passwords*

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

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

6.3.5.2 *FPT_SKP_EXT.1 Protection of TSF Data (for reading of all 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.

6.3.5.3 *FPT_STM_EXT.1 Reliable Time Stamps*

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

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

6.3.5.4 *FPT_TST_EXT.1 TSF Testing*

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on), 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, and software integrity check*]

6.3.5.5 *FPT_TUD_EXT.1 Trusted Update*

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

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

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

6.3.6 Class FTA: TOE Access

6.3.6.1 *FTA_SSL_EXT.1 TSF-initiated Session Locking*

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

6.3.6.2 *FTA_SSL.3 TSF-initiated Termination*

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

6.3.6.3 *FTA_SSL.4 User-initiated Termination*

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

6.3.6.4 *FTA_TAB.1 Default TOE Access Banners*

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

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

FTP_ITC.1.1 The TSF shall be capable of using [SSH] 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 [*acquisition of TOE updates and audit transfer*].

6.3.7.2 *FTP_TRP.1/Admin Trusted Path*

FTP_TRP.1.1/Admin The TSF shall be capable of using [SSH] 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 detection of modification of the channel data**.**

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

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

6.4 Statement of Security Functional Requirements Consistency

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

7 Security Assurance Requirements

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

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

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

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

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

ADV_FSP.1.2C

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

ADV_FSP.1.3C

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

ADV_FSP.1.4C

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

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

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

ADV_ FSP.1.2E

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

7.2 Class AGD: Guidance Documents

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

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

AGD_OPE.1.2C

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

AGD_OPE.1.3C

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

AGD_OPE.1.4C

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

AGD_OPE.1.5C

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

AGD_OPE.1.6C

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

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

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

7.2.2 Preparative Procedures (AGD_PRE.1)

7.2.2.1 *Developer action elements:*

AGD_PRE.1.1D

The developer shall provide the TOE, including its preparative procedures.

7.2.2.2 *Content and presentation elements:*

AGD_ PRE.1.1C

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

AGD_ PRE.1.2C

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

7.2.2.3 *Evaluator action elements:*

AGD_ PRE.1.1E

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

AGD_ PRE.1.2E

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

7.3 Class ALC: Life-cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

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

7.3.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 *Evaluator action elements:*

ALC_CMC.1.1E

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

7.3.2 TOE CM coverage (ALC_CMS.1)

7.3.2.1 *Developer action elements:*

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 *Content and presentation elements:*

ALC_CMS.1.1C

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

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 *Evaluator action elements:*

ALC_CMS.1.1E

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

7.4 Class ATE: Tests

7.4.1 Independent testing - conformance (ATE_IND.1)

7.4.1.1 *Developer action elements:*

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 *Content and presentation elements:*

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 *Evaluator action elements:*

ATE_IND.1.1E

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

ATE_IND.1.2E

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

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

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

AVA_VAN.1.2E

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

AVA_VAN.1.3E

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

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. 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.

8.1 Security Audit

8.1.1 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 Details' Column of Table 6-2. Date and time is 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 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.

See the *Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria* for a complete set of sample audit events.

8.1.2 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,LOGNA  ME=SECU400,LOGEVENT=ACT-
USER,UID=\"SURVEIL\",UPC=1,PORTTYPE=SSH,PORTADDR=\"192.168.2.126:52124\",STATUS=DENY,EV
TDESCR=\"Invalid login\""
```

8.1.3 FAU_STG_EXT.1

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 syslog records file. The syslog 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 hold a maximum of 9000 records or 4MB. Syslog records hold a maximum of 1000 records or 2MB. 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 syslog file is periodically pulled to a remote audit server, via an automated script, using SFTP over an SSH trusted channel. Depending on the usage of the TOE depends on how fast the audit logs will fill and start overwriting the old records. Therefore, it is recommended that the script be scheduled to execute every 1-6 hours, even though the frequency could be scheduled for as little as every minute or long as once every 24 hours, to mitigate any potential of audit records not being remotely stored.

8.1.4 FAU_STG.1

The TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The TOE does not provide a mechanism to delete or modify the locally-stored audit data and the filesystem is not accessible by any user of the TOE. See Section 8.1.3 FAU_STG_EXT.1 for full description of local audit behavior and storage.

8.2 Cryptographic Support

8.2.1 FCS_CKM.1

The TOE generates asymmetric keys for Diffie-Hellman group 14 with a key size of 2048 bits that meet the following: RFC 3526, Section 3. Diffie-Hellman group 14 is used for SSHv2 communications. The TOE generates 2048 and 3072-bit asymmetric keys for RSA providing support for SSHv2 according to FIPS PUB 186-4. The TOE's RSA key generation function is validated under CAVP RSA certificate #2666.

8.2.2 FCS_CKM.2

The TOE implements key establishment scheme using Diffie-Hellman group 14 with a key size of 2048 conformant to RFC 3526, Section 3. This key establishment scheme is used in all SSH communications used by the TOE: remote login, sending audit data to a remote audit server and downloading of software images from the update server.

8.2.3 FCS_CKM.4

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.

The SSH private key is encrypted with a 256 bit AES key before being stored in non-volatile storage. This 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.

8.2.4 FCS_COP.1/DataEncryption

The TOE provides symmetric encryption and decryption capabilities using AES in CBC and CTR modes with 128 and 256-bit keys as described in ISO 10116. The TOE provides encryption and decryption in support of SSH communications. The TOE's AES implementation is validated under CAVP AES certificate #4855.

8.2.5 FCS_COP.1/SigGen

The TOE will provide cryptographic signature services using RSA and ECDSA. RSA is the public-key algorithm used in support of SSH communications and ECDSA for software integrity verification.

RSA uses key sizes of 2048 and 3072 bits as specified in FIPS PUB 186-4 and ISO/IEC 9796-2. The RSA implementation is validated under CAVP RSA certificate #2666 as specified.

ECDSA uses a key size of 512 bit and implements the P-521 elliptic curve as specified in FIPS PUB 186-4 and ISO/IEC 14888-3, Section 6.4. The ECDSA implementation is validated under CAVP EDSA certificate #1244.

8.2.6 FCS_COP.1/Hash

The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512 as specified in ISO 10118-3:2004. The TOE uses cryptographic hashing services in support of SSH key establishment (SHA-1), HMAC for SSH (SHA-1, SHA-256), software integrity check (SHA-384) and digital signatures for ECDSA (SHA-512). The TOE's SHS implementation is validated under CAVP SHS certificate #3992.

8.2.7 FCS_COP.1/KeyedHash

The TOE provides keyed-hash message authentication services using HMAC-SHA1 and HMAC-SHA-256 and cryptographic key sizes of 160 and 256 bits, and message digest sizes of 160 and 256 bits as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". HMAC-SHA1 and HMAC-SHA-256 are used to support SSH communications.

The TOE's HMAC implementation is validated under CAVP HMAC certificate #3250.

Note: The TOE supports HMAC-SHA1-96 which is just a 96-bit truncation of the output of HMAC-SHA1. The algorithm certificate for HMAC-SHA1 covers HMAC-SHA1-96.

8.2.8 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, which are the largest keys generated by the TSF. The TOE's DRBG implementation is validated under CAVP DRBG certificate #1706.

8.2.9 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. Additionally, an external script running on the audit server (SSH client) will periodically retrieve audit data from the TOE (SSH server) using SFTP over an SSH trusted channel. When the TOE acts as an SSH server, only public key authentication is supported.

The TOE implements SSHv2 that complies with the following RFCs: 4251, 4252, 4253, 4254, 5656, 6668. The TOE implementation of SSHv2 only supports RSA signature verification for authentication. 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 transport algorithms and ssh-rsa as its only supported public key algorithm. Data integrity is assured using HMAC-SHA1-96 (a 96-bit truncation of HMAC-SHA1), HMAC-SHA-1 and HMAC-SHA2-256. The only allowed key exchange method is diffie-hellman-group14-sha1.

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.

8.3 Identification and Authentication

8.3.1 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 7200 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.

8.3.2 FIA_PMG_EXT.1

The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower-case letters, numbers, and 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 15 characters or greater. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the 6500.

8.3.3 FIA_UAU_EXT.2

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.

8.3.4 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.

8.3.5 FIA_UIA_EXT.1

See FIA_UAU_EXT.2 above.

8.4 Security Management

8.4.1 FMT_MOF.1/ManualUpdate

The TOE restricts the ability to perform manual software updates via the update server to Security Administrators. See Table 8-1 for the definition of the UPC levels required to perform each claimed function.

8.4.2 FMT_MOF.1/Functions

The TOE restricts the management of audit data functionality to Security Administrators. This includes the transmission of audit data to the audit server. Refer to Section 8.4.6 for the definition of the different Security Administrators defined according to their UPC level. See Table 8-1 for the definition of the UPC levels required to perform each claimed function.

8.4.3 FMT_MOF.1/Services

The TOE restricts the ability to enable and disable the SSH service to Security Administrators with (UPC>=4). The enabling and disabling of the SSH services affects the audit behavior and is covered under the FMT_SMF.1 selection of “ability to configure audit behavior”.

8.4.4 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. These five roles are described in further detail in section 8.4.6 under FMT_SMF.1.

8.4.5 FMT_MTD.1/CryptoKeys

Only the Security Administrator can manage cryptographic keys. This includes key generation for symmetric and asymmetric keys and key destruction/zeroization. Secret and private keys cannot be seen by Security Administrators.

8.4.6 FMT_SMF.1

The TOE provides all the capabilities necessary to securely manage the TSF. The TOE includes a TL1 interface to administer the functions associated with day-to-day operations of the TOE. The TL1 interface can be accessed directly 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.

Security Administrators have a UPC level between 1 and 5 which defines their ability to administer the TOE as follows:

> Level 1: (monitoring only – no provisioning, maintenance or administration) – Retrieve allows retrieve and report related commands to be executed.
>
> Level 2: (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.
>
> Level 3: (provisioning but no administration) – Provisioning allows access to provision, test, edit and retrieve commands.
>
> Level 4: (provisioning and administration) – Administration allows complete access to all commands.
>
> Level 5: (provisional and administration) – Surveillance allows complete access to all commands.

The following table describes the management functions provided by the TOE, along with which type of Security Administrator can perform the function in terms of their UPC level. Security administrators can perform these activities from both the local craft port interface or remote interface.

Management Function	Administrative Level
Ability to administer the TOE locally and remotely	UPC>=1
Ability to configure the access banner	UPC>=4
Ability to configure the session inactivity time before session termination or locking	UPC>=4
Ability to update the TOE and to verify the updates using digital signature capability prior to installing those updates	UPC>=3
Ability to configure the authentication failure parameters for FIA_AFL.1	UPC>=4
Ability to configure audit behavior	UPC>=4
Ability to configure the cryptographic functionality	UPC>=3
Ability to re-enable an Administrator account	UPC>=4
Ability to set the time which is used for time-stamps	UPC>=4

Table 8-1: TSF Management Functions

If administering the TOE remotely via TL1 is desired, the management workstation should be placed on the same dedicated local network as the TOE.

8.4.7 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.

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 the TL1 interface of the TSF. See Table 8-2 for details.

8.5 Protection of the TSF

8.5.1 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.

8.5.2 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 (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.

8.5.3 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, 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]
```

8.5.4 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 generator tests, SP 800-90B health tests to verify the correct functionality of the cryptographic functions. Additionally, the TOE performs a software integrity check (SHA-384). 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.

8.5.5 FPT_TUD_EXT.1

The TOE provides the ability for a Security Administrator with UPC >=3 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-512. 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. 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;
```

8.6 TOE Access

8.6.1 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.

8.6.2 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.

8.6.3 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 typically terminate the SSH session if the application itself is closed.

8.6.4 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. The warning banner is configured by a Security Administrator with a UPC >=4.

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1

The TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. In the evaluated configuration, the TOE, acting as the SSH server, has audit data periodically pulled by a script operating on a remote audit server using SFTP protected by SSH. The identity of the audit server is verified by checking the SSH known hosts public-key. Additionally, the TOE, acting as an SSH client, retrieves software updates via the update server using SFTP protected by SSH.

The TOE relies on the CAVP-validated cryptographic algorithm implementation used to establish these trusted channels.

8.7.2 FTP_TRP.1/Admin

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.