Ciena Waveserver Ai Rel 1.3 Security Target

June 14, 2019

v2.6

Prepared By:
Acumen Security
2400 Research Blvd Suite 395
Rockville, MD, 20850
www.acumensecurity.net

Prepared for:
Ciena Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America
www.ciena.com

Table of Contents

Revision History

Version	Date	Description
0.1	8/9/2018	Initial version
0.2	8/10/2018	Updating Section 1.
0.3	8/12/2018	Sections 1-4 complete
0.4	8/13/2018	Began Section 5.
0.5	8/14/2018	Completion of Section 5 and began Section 6.
0.6	8/15/2018	Section 6 Crypto
0.7	8/16/2018	Section 6 Complete, ST Draft complete and submit to vendor for review and address outstanding comments.
0.8	8/26/2018	Updated Sections 1-5 based on vendor comments.
0.9	8/27/2018	Updated Sections 6 based on vendor comments.
1.0	10/1/2018	Minor updates based on dry run testing.
1.1	10/19/2018	Minor updates to Sections based on vendor feedback
1.2	10/29/2018	Minor updates to SFRs and TSS section based on vendor feedback
1.3	10/31/2018	Minor updates to SFRs and TSS section based on vendor feedback
1.4	11/1/2018	Finalized version of the ST – minor updates
1.5	11/21/2018	Updated processor and operating system information
1.6	1/8/2019	Updated TOE labelling from Ver 1.3 to Rel 1.3.
1.7	2/13/2019	Updated TD table 7 with TD260 and TD262 as per validator comments.
1.8	2/26/2019	Updated TD table 7 based on newly released NIAP TDs.
1.9	3/7/2019	Updated Section 1.6
2.0	3/20/2019	Updates to Section 5 based on ASE – ETR work units
2.1	3/26/2019	Updated TD table 7 based on newly released NIAP TDs.
2.2	4/4/2019	Updated ST based on vendor feedback to Section 6.
2.3	4/9/2019	Minor edits to TSS section, TD table and finalization
2.4	4/30/2019	Addressing validator check out comments
2.5	5/13/19	Minor edits to Section 1.6 and 6
2.6	6/14/19	Removed references to TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

1 Security Target Introduction

1.1 Security Target and TOE Reference

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

Category	Identifier
ST Title	Ciena Waveserver Ai Rel 1.3 Security Target
ST Version	2.6
ST Date	June 14, 2019
ST Author	Acumen Security, LLC.
TOE Identifier	Ciena Waveserver Ai Rel 1.3
TOE Software Version	1.3
TOE Developer	Ciena Corporation
Key Words	Network Device, Waveserver Ai

Table 1 TOE/ST Identification

1.2 TOE Overview

The Ciena Waveserver (herein referred to as the TOE) Ai Rel 1.3 is a network device which offers ultra-high capacity connections between data centre locations thus reducing the network costs for both enterprises and content providers. The Wavesever Ai utilizes the Ciena's WaveLogic Ai technology. The Waveserver Ai uses the WCS2 hardware.

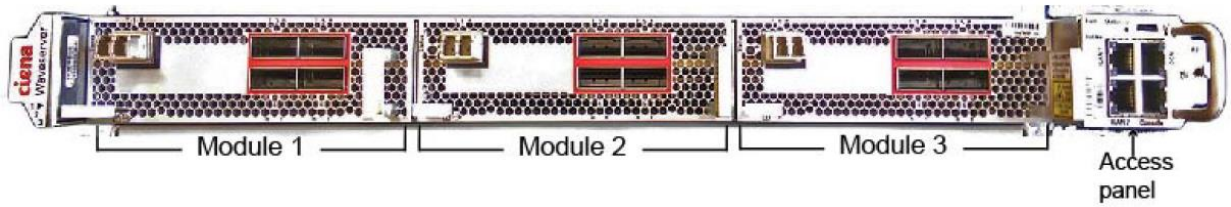
1.2.1 TOE Product Type

The Ciena Waveserver Ai Rel 1.3 is a network device which is composed of hardware and software that offers a scalable solution to the end users. It satisfies all of the criterion to meet the collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e.

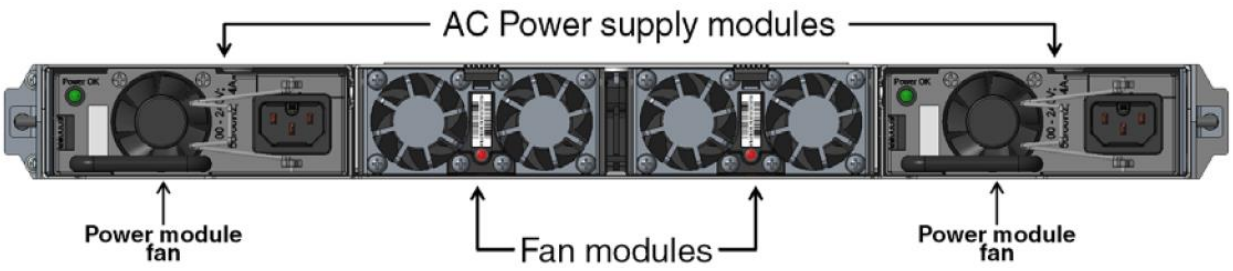
1.3 TOE Description

The TOE is comprised of the following model:

Waveserver Ai front panel:



Waveserver Ai rear panel: AC power and fan modules



Waveserver Ai rear panel: DC power and fan modules

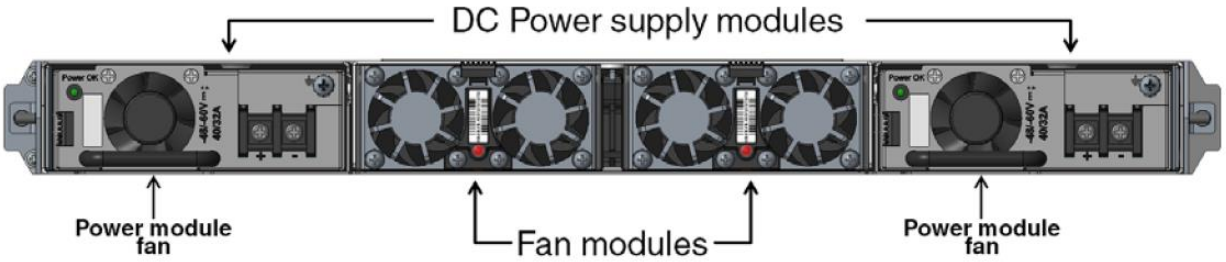


Figure 1: Front and rear panels of the TOE

Waveserver Ai Appliance	
Processor	ARM Cortex-A53
Client ports	Up to 24 x QSFP28 (24 x 100GbE)
Line Ports	Up to 2.4 Tb/s; Line ports support single carrier 100 Gb/s, 200 Gb/s, 300 Gb/s or 400 Gb/s
Enclosure	Single rack unit
Power Supply	AC or DC power AC input voltage range: 100 Vac to 264 Vac DC input voltage range: -40 Vdc to -72 Vdc Power consumption: 0.4 W/Gb
Environment Characteristics	Normal operating temperature: 0 °C to +40 °C (32 °F to 104 °F)

Table 2 Waveserver Ai appliance

1.4 TOE Evaluated Configuration

The TOE in the evaluated configuration consists of the platform as stated in Section 1.3. The TOE supports secure connectivity with other IT environment device as stated in Table 3.

Component	**Required**	**Usage**
NTP server (optional)	No	The TOE supports communication with an NTP server to synchronize date and time.
Syslog server	Yes	The TOE exports audit events to an external syslog server via TLS v1.2 protocol.
Radius server	Yes	The TOE supports secure communication to RADIUS server via TLS v1.2 protocol.
Management workstation with Web Browser/SSH client	Yes	This includes any IT Environment Management workstation with a Web Browser and a SSH client

Component	Required	Usage
		installed that is used by the TOE. *NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.*
Certificate Authority server	Yes	The Certificate Authority is used for creation and management of X509 certificates to be used with the TOE.

Table 3 IT Components

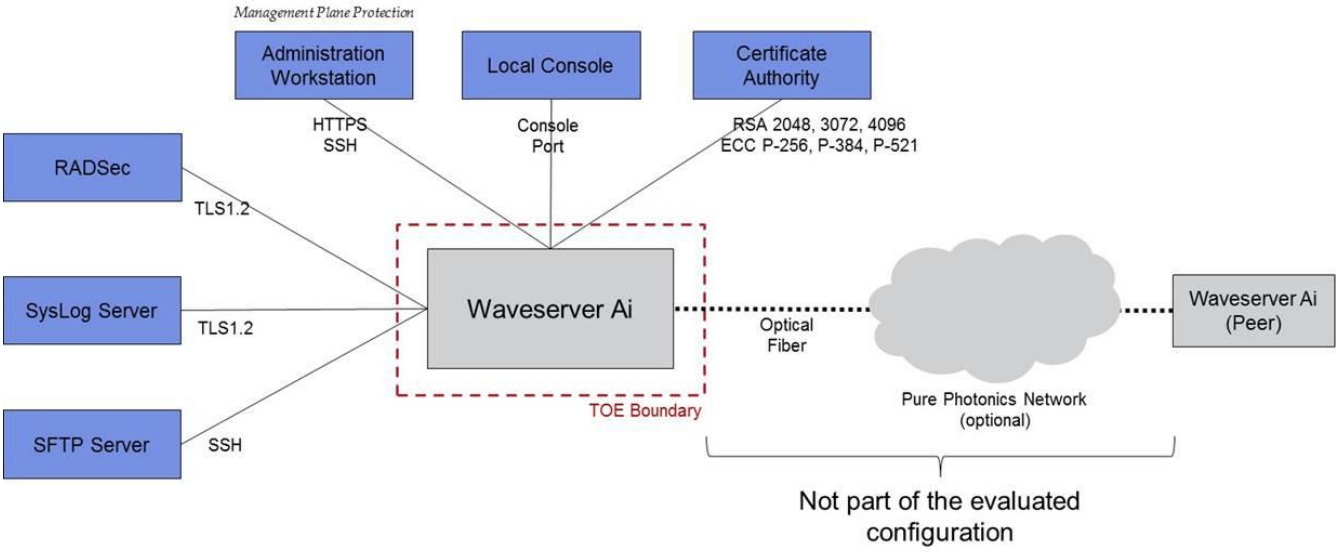


Figure 2 TOE Deployment

1.5 Physical Scope of the TOE

The TOE boundary is the hardware appliance which is comprised of hardware and software components. It is deployed in an environment which contains the various IT components as depicted in Figure 2. The TOE guidance documentation can be found on the Ciena website: https://www.ciena.com. An account is required to access the guidance documents and any software updates.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from the Ciena website.

1.6 Logical Scope of the TOE

The TOE implements the following security functional requirements:

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

Each of these security functionalities are listed in more detail below:

1.6.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in Table 5. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external syslog server using TLS v1.2 protocol. Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event. The syslog server supports the following severity levels: emergency, alert, error, warning, notice, info and debug. In order to enable the logging to syslog server, a user must be logged in with an administrative access privilege.

1.6.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 4. The related CAVP validation details are provided in Table 5. The operating system is Linux Kernel v4.9. The TOE leverages the Waveserver Ai WCS-2 FW Crypto Library 2 for its cryptographic functionality .

Cryptographic Method	Usage
FCS_CKM.1 Cryptographic Key Generation	• Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. • RSA Key sizes supported are 3072 and 4096 bits. 4096 bits support was not tested/evaluated. • RSA key size of 2048 bits must be enabled in the evaluated configuration • Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4 • Elliptic NIST curves supported are: P-256, P-384 and P-521.
FCS_CKM.2 Cryptographic Key Establishment	• RSA-based key establishment conforming to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards

	(PKCS) #1: RSA Cryptography Specifications Version 2.1 • Elliptical curve based establishment conforming to NIST Special Publication 800-56A Revision 2. • Key establishment using Diffie-Hellman group 14 conforming to RFC 3526, Section 3.
FCS_CKM.4 Cryptographic Key Destruction	• Refer to Table 12 for Key Zeroization details.
FCS_COP.1/DataEncryption	• AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772. • AES key size supported is 256 bits • AES modes supported are: CBC, CTR and GCM.
FCS_COP.1/SigGen	• RSA digital signature algorithm conforming to 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. • RSA key size of 2048 bits must be enabled in the evaluated configuration • RSA key sizes supported are: 3072 and 4096 bits. 4096 bits support was not tested/evaluated. • Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" ISO/IEC 14888-3, Section 6.4. • Elliptical curve key size supported is 256 bits.
FCS_COP.1/Hash	• Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. • Hashing algorithms supported are: SHA-256, SHA-384 and SHA-512. • Message digest sizes supported are: 256, 384 and 512 bits.
FCS_COP.1/KeyedHash	• Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm. • Keyed hash algorithm supported are: HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512. • Key sizes supported are: 256, 384, and 512 bits. • Message digest sizes supported are: 256, 384 and 512 bits.
FCS_DRBG_EXT.1 Random Bit Generation	• Random number generation conforming to ISO/IEC 18031:2011. • The TOE leverages CTR_DRBG(AES) • CTR_DRBG seeded with HW_TRNG with a minimum of 256 bits of entropy.

FCS_HTTPS_EXT.1 HTTPS Protocol	• The TOE supports HTTPS protocol that complies with RFC2818. • The TOE implements HTTPS protocol using TLS v1.2 in support of Web UI.
FCS_TLSC_EXT.2 TLS Client Protocol with authentication	• The TOE supports TLS v1.2 protocol for use with X.509v3 based authentication. • Supports the following ciphersuites in the evaluated configuration: • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
FCS_TLSS_EXT.2 TLS Server Protocol with mutual authentication	• The TOE supports TLS v1.2 protocol and supports mutual authentication for use with X.509v3 certificates. • Supports the following ciphersuites in the evaluated configuration: • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
FCS_SSHS_EXT.1 SSH Server Protocol	• The TOE supports SSH v2 protocol. • Supports password based authentication. • SSH public-key authentication uses rsa-ssh, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. • SSH transport uses the following encryption algorithms: AES256-CTR and AEAD_AES_256_GCM.

	• Packets greater than 256 000 bytes in an SSH transport connection are dropped. • SSH transport uses the following data integrity MAC algorithms: hmac-sha2-256, and hmac-sha2-512 and AEAD_AES_256_GCM. • Key exchange algorithms supported are: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. • The TOE ensures that within SSH connections the same session keys are used for a threshold of no longer than one hour and no more than 512 MB of transmitted data.

Table 4 TOE Cryptography Implementation

Cryptographic Algorithms	CAVPs
AES	C193
RSA	C193
ECDSA	C193
KAS/CVL	C193
HMAC	C193
SHS	C193
DRBG	C193
CVL SSH v2	C193
CVL TLS v1.2	C193

Table 5 Cryptographic Algorithm Certificates

1.6.3 Identification and Authentication

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password based authentication and public key based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

1.6.4 Security Management

The TOE supports local and remote management of its security functions including:

o Local console CLI administration
o Remote CLI administration via SSHv2
o Timed user lockout after multiple failed authentication attempts
o Password configurations.
o Role Based Access Control – Superuser (Security Administrator), Admin and limited user (User)
o Configurable banners to be displayed at login
o Timeouts to terminate administrative sessions after a set period of inactivity
o Protection of secret keys and passwords

1.6.5 TOE Access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 10 minutes of session inactivity. An administrator can terminate their GUI session by clicking on the logout button. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

1.6.6 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

1.6.7 Trusted Path/Channels

The TOE supports TLS v 1.2 for secure communication to the following IT entities: Syslog server and Radius server. The TOE supports HTTPS/TLS (WebUI) and SSH v2 (remote CLI) for secure remote administration.

NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.

1.7 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

- NTP server (optional)
- The Web UI management interface is out of scope (All HTTPS and TLSS requirements were evaluated and tested)
- gRPC is disabled

1.8 TOE Documentation

Documentation	Version
Ciena Waveserver Ai Rel 1.3 Common Criteria Guidance document	1.0

Table 6 TOE Documentation

1.9 Other References

[NDcPP v2.0e] collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e

2 Conformance Claims

2.1 CC Conformance

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017.

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 conformant

2.2 Protection Profile Conformance

This TOE is conformant to:

- collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e

2.3 Conformance Rationale

This Security Target provides exact conformance to Version 2.0e of the Collaborative Protection Profile for Network Devices. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

2.4 NIAP Technical Decisions

NIAP Technical Decisions for NDcPP v2.0e (TDs)		
Technical Decisions	**Applicable**	**Exclusion Rationale (if applicable)**
TD0412: NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	Yes	
TD0411 - NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	No	FCS_SSHC_EXT.1 is not applied.
TD0410: NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	Yes	
TD0409: NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	Yes	
TD0408: NIT Technical Decision for local vs. remote administrator accounts	Yes	
TD0407: NIT Technical Decision for handling Certification of Cloud Deployments	No	The TOE is not a cloud platform.
TD0402 – NIT Technical Decision for RSA-based FCS_CKM.2 Selection	Yes	
TD0401 – NIT Technical Decision for Reliance on external servers to meet SFRs	No	TOE does not rely on the Authentication Server to satisfy FIA requirements
TD0400 – NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	Yes	
TD0399 – NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	No	The TOE does not support CRL.

NIAP Technical Decisions for NDcPP v2.0e (TDs)		
TD0398 – NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	Yes	
TD0397 – NIT Technical Decision for Fixing AES-CTR Mode Tests	Yes	
TD0396 – NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	Yes	
TD0395 – NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2	Yes	
TD0394: NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys	Yes	
TD0343: NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	No	The TOE does not support IPSEC functionality.
TD0342: NIT Technical Decision for TLS and DTLS Server Tests	Yes	
TD0341: NIT Technical Decision for TLS wildcard checking	Yes	
TD0340: NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	Yes	
TD0339: NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	Yes	
TD0338: NIT Technical Decision for Access Banner Verification	Yes	
TD0337: NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	Yes	
TD0336: NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	Yes	
TD0335: NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	Yes	
TD0334: NIT Technical Decision for Testing SSH when password-based authentication is not supported	No	TD0334 is not applied since FCS_SSHC_EXT.1 is not selected.
TD0333: NIT Technical Decision for Applicability of FIA_X509_EXT.3	Yes	
TD0324 – NIT Technical Decision for Correction of section numbers in SD Table 1	Yes	
TD0323: NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	No	The TOE does not support DTLS functionality.
TD0322: NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	Yes	

NIAP Technical Decisions for NDcPP v2.0e (TDs)		
TD0321 – Protection of NTP communications	No	Support for NTP is optional.
TD0291 – NIT technical decision for DH14 and FCS_CKM.1	Yes	
TD0290 – NIT technical decision for physical interruption of trusted path/channel.	Yes	
TD0289 – NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e	Yes	
TD0281 – NIT Technical Decision for Testing both thresholds for SSH rekey	Yes	
Archived TD0262: NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	Not Applied	Not applied as the TD is archived.
Archived TD0260: NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4	Not Applied	Not applied as the TD is archived.
TD0259 – NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	Yes	
TD0257 – NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	Yes	
TD0256 – NIT Technical Decision for Handling of TLS connections with and without mutual authentication	Yes	
TD0228: NIT Technical Decision for CA certificates - basicConstraints validation	Yes	

Table 7 NIAP Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [NDcPP v2.0e] and is reproduced here for the convenience of the reader.

3.1 Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below.

3.1.1 Communications with the Network Device

A network device communicates with other network devices and other network entities. The endpoints of this communication can be geographically and logically distant and may pass through a variety of other systems. The intermediate systems may be untrusted providing an opportunity for unauthorized communication with the network device or for authorized communication to be compromised. The security functionality of the network device must be able to protect any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.). The communication with the network device falls into two categories: authorized communication and unauthorized communication.

Authorized communication includes network traffic allowable by policy destined to and originating from the network device as it was designed and intended. This includes critical network traffic, such as network device administration and communication with an authentication or audit logging server, which requires a secure channel to protect the communication. The security functionality of the network device includes the capability to ensure that only authorized communications are allowed and the capability to provide a secure channel for critical network traffic. Any other communication is considered unauthorized communication.

The primary threats to network device communications addressed in this cPP focus on an external, unauthorized entity attempting to access, modify, or otherwise disclose the critical network traffic. A poor choice of cryptographic algorithms or the use of non-standardized tunneling protocols along with weak administrator credentials, such as an easily guessable password or use of a default password, will allow a threat agent unauthorized access to the device. Weak or no cryptography provides little to no protection of the traffic allowing a threat agent to read, manipulate and/or control the critical data with little effort. Non-standardized tunneling protocols not only limit the interoperability of the device but lack the assurance and confidence standardization provides through peer review.

3.1.1.1 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.

3.1.1.2 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.

3.1.1.3 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.

3.1.1.4 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.

3.1.2 Valid Updates

Updating network device software and firmware is necessary to ensure that the security functionality of the network device is maintained. The source and content of an update to be applied must be validated by cryptographic means; otherwise, an invalid source can write their own firmware or software updates that circumvents the security functionality of the network device. Methods of validating the source and content of a software or firmware update by cryptographic means typically involve cryptographic signature schemes where hashes of the updates are digitally signed.

Unpatched versions of software or firmware leave the network device susceptible to threat agents attempting to circumvent the security functionality using known vulnerabilities. Non-validated updates or updates validated using non-secure or weak cryptography leave the updated software or firmware vulnerable to threat agents attempting to modify the software or firmware to their advantage.

3.1.2.1 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.

3.1.3 Audited Activity

Auditing of network device activities is a valuable tool for administrators to monitor the status of the device. It provides the means for administrator accountability, security functionality activity reporting, reconstruction of events, and problem analysis. Processing performed in response to device activities may give indications of a failure or compromise of the security functionality. When indications of activity that impact the security functionality are not generated and monitored, it is possible for such activities to occur without administrator awareness. Further, if records are not generated and retained, reconstruction of the network and the ability to understand the extent of any compromise could be negatively affected. Additional concerns are the protection of the audit data that is recorded from alteration or unauthorized deletion. This could occur within the TOE, or while the audit data is in transit to an external storage device.

Note this cPP requires that the network device generate the audit data and have the capability to send the audit data to a trusted network entity (e.g., a syslog server).

3.1.3.1 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.

3.1.4 Administrator and Device Credentials Data

A network device contains data and credentials which must be securely stored and must appropriately restrict access to authorized entities. Examples include the device firmware, software, configuration authentication credentials for secure channels, and administrator credentials. Device and administrator keys, key material, and authentication credentials need to be protected from unauthorized disclosure and modification. Furthermore, the security functionality of the device needs to require default authentication credentials, such as administrator passwords, be changed.

Lack of secure storage and improper handling of credentials and data, such as unencrypted credentials inside configuration files or access to secure channel session keys, can allow an attacker to not only gain access to the network device, but also compromise the security of the network through seemingly authorized modifications to configuration or though man-in-the-middle attacks. These attacks allow an unauthorized entity to gain access and perform administrative functions using the Security Administrator's credentials and to intercept all traffic as an authorized endpoint. This results in difficulty in detection of security compromise and in reconstruction of the network, potentially allowing continued unauthorized access to administrator and device data.

3.1.4.1 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 include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

3.1.4.2 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.

3.1.5 Device Failure

Security mechanisms of the network device generally build up from roots of trust to more complex sets of mechanisms. Failures could result in a compromise to the security functionality of the device. A network device self-testing its security critical components at both start-up and during run-time ensures the reliability of the device's security functionality.

3.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

This section describes the assumptions made in identification of the threats and security requirements for network devices. The network device is not expected to provide assurance in any of these areas, and as a result, requirements are not included to mitigate the threats associated.

3.2.1 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. [OE.PHYSICAL]

3.2.2 A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). [OE.NO_GENERAL_PURPOSE]

3.2.3 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). [OE.NO_THRU_TRAFFIC_PROTECTION]

3.2.4 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. [OE.TRUSTED_ADMIN]

3.2.5 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. [OE.UPDATES]

3.2.6 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. [OE.ADMIN_CREDENTIALS_SECURE]

3.2.7 A.RESIDUAL_INFORMATION

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

3.3 Organizational Security Policy

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. For the purposes of this cPP a single policy is described in the section below.

3.3.1 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. [FTA_TAB.1]

4 Security Objectives

The security objectives have been taken from [NDcPP v2.0e] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

The following subsections describe objectives for the Operational Environment.

4.1.1 OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

4.1.2 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.

4.1.3 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.

4.1.4 OE.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

4.1.5 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.

4.1.6 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.

4.1.7 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.

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold** text and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined text*;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear below in Table 8 are described in more detail in the following subsections.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Failure to establish an SSH session

Requirement	Auditable Events	Additional Audit Record Contents
FCS_TLSC_EXT.2	Failure to establish a TLS Session	Failure to establish a TLS Session
FCS_TLSS_EXT.2	Failure to establish a TLS Session	Failure to establish a TLS Session
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Failure to establish a HTTPS Session.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g. IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of 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).
FIA_UAU.7	None.	None
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1 (if “terminate the session” is selected)	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.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions	None.

Table 8 TOE Security Functional Requirements and Auditable Events

5.2.1 Class: Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions comprising:*
   - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
   - *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
   - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
   - *Resetting passwords (name of related user account shall be logged).*
   - *Starting and stopping services (if applicable)*
   - *[no other actions];*

   Specifically defined auditable events listed in Table 8.

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *information specified in column three of Table 8*.

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.

FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

5.2.2 Class: Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation (Refined)

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

- *RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;*
- *ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*
- *FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3*

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

FCS_CKM.2 Cryptographic Key Establishment (Refined)

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

- *RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*
- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;*

] ~~that meets the following: [assignment: *list of standards*].~~

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*

o logically addresses the storage location of the key and performs a [single-pass] overwrite consisting of [zeros];

]]

that meets the following: No Standard.

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, GCM, CTR] mode* and cryptographic key sizes *[256 bits]* that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772]*.

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, 3072],*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]*

] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~

that meet the following: [

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

].

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-256, SHA 384, SHA-512*] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and **message digest sizes** [***256, 384, 512***] **bits** that meet the following: ISO/IEC 10118-3:2004.

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

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *[HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512]* and cryptographic key sizes [*256, 384, 512 (in bits) used in HMAC]* **and message digest sizes *[256, 384, 512] bits*** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

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] of hardware-based 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.

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [*not establish the connection*] if the peer certificate is deemed invalid.

FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [*4251, 4252, 4253, 4254, 4344, 5647, 5656, 6668*].

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256000*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms*: [aes256-ctr, AEAD_AES_256_GCM]*.

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [*ssh-rsa, ecdsa-sha2-nistp256*] *and* [*ecdsa-sha2nistp384, ecdsa-sha2-nistp521*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses *[hmac-sha2-256, hmac-sha2-512]* and *[AEAD_AES_256_GCM]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

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

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

FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

FCS_TLSC_EXT.2.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

].

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

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

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

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

FCS_TLSS_EXT.2 TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.2.1 The TSF shall implement [*TLS 1.2 (RFC 5246*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

].

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [*TLS 1.1*].

FCS_TLSS_EXT.2.3 The TSF shall [selection: perform RSA key establishment with key size *[2048, 3072 bits];* generate EC Diffie-Hellman parameters over NIST curves *[secp256r1, secp384r1, secp521r1] and no other curves; generate DiffieHellman parameters of size [3072 bits].*

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 The TSF shall not establish a trusted channel if the client certificate is invalid. If the client certificate is deemed invalid, then the TSF shall [*not establish the connection*].

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

5.2.3 Class: Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*2-10*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password.*

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

FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, *[“ ?”, “ ‘“, “, “ + “, “ / “, “ : ”, “ ; “, “ < “, “ > “, “ = “, “ [“, “] “, “, “ ` “, “ ~ “, “ { “, “ } “, “ |”, “ “*]]
b) Minimum password length shall be configurable *to [1 character] and [128 characters].*

FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall require the following actions prior to allowing 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

FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

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.**

FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation supporting a **minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate.
  The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960]
  The TSF shall validate the extendedKeyUsage field according to the following rules:
  o *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS] and [[*no additional uses*]].

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

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Class: Security Management (FMT)

FMT_MOF.1/ManaulUpdate 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.*

FMT_MTD.1/CoreData Management of TSF Data

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

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 behavior;*
    - *Ability to configure the cryptographic functionality;*
    - *Ability to set the time which is used for time-stamps;*
    - *Ability to configure the reference identifier for the peer;*
      ]

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 the user with roles

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.2.5 Class: Protection of the TSF (FPT)

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.

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.

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*].

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 [*no other TOE firmware/software version*].

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.

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), and at the request of the authorized user, at the conditions [by performing a system or card level restart command],*to demonstrate the correct operation of the TSF:

[

- Software integrity test
- AES Known Answer Test
- HMAC-SHA-256/384/512 Known Answer Test
- SHA-256/384/512 Known Answer Test
- RSA Signature Known Answer Test

- ECDSA Signature Known Answer Test
- RNG Known Answer Test

]]]

5.2.6 Class: TOE Access (FTA)

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.

FTA_SSL.3 TSF-initiated Termination

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

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Refinement: 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.

5.2.7 Class: Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be **capable of using [*TLS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*authentication server*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*audit server, authentication server*].

FTP_TRP.1/Admin Trusted Path

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

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

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

NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.

5.3 TOE SFR Dependencies Rationale for SFRs

The Collaborative Protection Profile for Network Devices contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Collaborative Protection Profile for Network Devices which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Security Target(ASE)	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic functional specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life cycle support (ALC)	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

Table 9 Security Assurance Requirements

5.5 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it,

what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6 Assurance Measures

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

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

Table 10 TOE Security Assurance Measures

6 TOE Summary Specification

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

TOE SFR	Rationale
FAU_GEN.1	The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 8. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event. All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection. Administrative tasks of generating, deleting cryptographic keys contain the necessary audit information as mandated by FAU_GEN.1.1. Audit events for deleting keys, generating keys are listed below: SSH server key delete: November 21, 2018 16:30:42.092 [local] Sev:7 chassis(1): SSH IP 10.10.10.30 User ccadmin:Ssh server key delete SSH Generate key: November 21, 2018 16:31:02.347 [local] Sev:7 chassis(1): SSH IP 10.10.10.30 User ccadmin:Ssh Generate Key X509 device certificate installed: November 21, 2018 16:30:09.338 [local] Sev:7 chassis(1): SSH IP 10.10.10.30 User ccadmin:X.509 device certificate with name rsa4096 installed
FAU_GEN.2	For audit events that result from actions of identified users, the TOE is able to associate each auditable event with the identity of the user that caused the event.
FAU_STG_EXT.1	The TOE can be configured to export audit events securely to a syslog server using TLS v1.2 protocol using X.509 certificates. The TOE stores up to 4 files each holding up to 10,000 audit data locally. When a file is full, a new file is created. When the local data is full, the oldest audit events are overwritten to allow new audit events to be created. Security Administrators can access the audit events and have the ability to clear the audit events. This way, audit events are protected against unauthorized access. The TOE transmits audit data to an external syslog server in real time. If there is a TLS connection failure, the TOE will continue to store local audit events on the TOE , and will transmit any locally stored contents when connectivity to the syslog server is restored.
FCS_CKM.1	The TOE supports RSA key sizes of 2048 bits (must be enabled in the evaluated configuration), 3072 bits and 4096 bits. 4096 bits support was not tested/evaluated, for key generation conforming to Cryptographic key generation

TOE SFR	Rationale
	conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3. The RSA keys are used in support of digital signature for both TLS and SSH communications. The TOE supports Elliptical NIST curve sizes of P-256, P-384 and P-521 conforming to Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4. The Elliptic keys are used in support of ECDH key exchange. The TOE supports FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3. Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.
FCS_CKM.2	The TOE supports Cryptographic Key Establishment using the following schemes: • RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. The TOE implements RSA key establishment scheme with key sizes of 2048 (must be enabled in the evaluated configuration), 3072 and 4096 bits. 4096 bits support was not tested/evaluated. • Elliptical curve based establishment conforming to NIST Special Publication 800-56A Revision 2. RSA and ECC schemes are used in support of TLS communications. • Key establishment using Diffie-Hellman group 14 conforming to RFC 3526, Section 3. The TOE acts as both a sender and receiver for RSA based key establishment scheme and Elliptic curve-based key establishment scheme. Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.
FCS_CKM.4	The TOE satisfies all requirements as specified in FCS_CKM.4 of NDcPP v2.0e for destruction of keys and CSPs. Please refer to Table 12 Zeroization Table.
FCS_COP.1/DataEncryption	The TOE supports AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772. The AES key size supported is 256 bits and the AES modes supported are: CBC, CTR and GCM. Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for AES.

<table>
<tr><th>TOE SFR</th><th>Rationale</th></tr>
<tr><td></td><td></td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides Cryptographic signature generation and verification in accordance with the following cryptographic algorithms:
RSA digital signature conforming to 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.
The RSA key sizes supported are: 2048 (must be enabled in the evaluated configuration), 3072 and 4096 bits. 4096 bits support was not tested/evaluated.
The TOE uses Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4
The Elliptical curve key size supported is 256 bits.
Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in TLS and SSH connections.
The following hashing algorithms supported: SHA-256, SHA-384 and SHA-512.
The message digest sizes supported are: 256, 384 and 512 bits.

Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs SHS.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE supports Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm. HMAC algorithms is used in support of TLS and SSH sessions.<table><tr><th>HMAC Algorithms</th><th>Hash Functions</th><th>Block Size</th><th>Key lengths</th><th>MAC lengths</th></tr><tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr><tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr><tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr></table>Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for HMAC.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TOE uses CTR_DRBG conforming to ISO/IEC 18031:2011.
The CTR_DRBG is seeded with HW_TRNG with a minimum of 256 bits of entropy.
Since this is third party TRNG, the vendor does not have access to the collection of</td></tr>
</table>

TOE SFR	Rationale
	the raw noise. The 3rd party claims that there is 5.9 bits of entropy per every 8 bits, which provides a minimum entropy rate of 0.73 entropy/bit. Please refer to Table 5 Cryptographic Algorithm Certificates for NIST CAVPs for DRBG.
FCS_HTTPS_EXT.1	The TOE supports remote management of the TOE over an HTTPS connection using TLS v1.2 implementation. In this scenario, the TOE acts as a server. The HTTPS protocol complies with RFC 2818. The TOE web GUI operates on an explicit port designed to natively speak TLS: it does not attempt STARTTLS or similar multi-protocol negotiation which is described in section 2.3 of RFC 2818. The web server attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.
FCS_SSHS_EXT.1.1	The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 5656, and 6668.
FCS_SSHS_EXT.1.2	The TOE supports password-based authentication and public key authentication. The following public key algorithms: rsa-ssh, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. This list is conforms to FCS_SSHS_EXT.1.5.
FCS_SSHS_EXT.1.3	The TOE accepts packet size up to 256K and meets the requirements of RFC 4253.
FCS_SSHS_EXT.1.4	The TOE supports the following encryption algorithms: AES256-CTR and AEAD_AES_256_GCM for SSH transport. There are no optional characteristics specified for FCS_SSHS_EXT.1.4. This list is identical to those claimed for FCS_SSHS_EXT.1.4.
FCS_SSHS_EXT.1.5	The following public key algorithms: rsa-ssh, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. There are no optional characteristics specified for FCS_SSHS_EXT.1.5. This list is identical to those claimed for FCS_SSHS_EXT.1.5.
FCS_SSHS_EXT.1.6	The TOE supports the following data integrity MAC algorithms: hmac-sha2-256, and hmac-sha2-512 and AEAD_AES_256_GCM. This list corresponds to the list in FCS_SSHS_EXT.1.6.
FCS_SSHS_EXT.1.7	The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. This list corresponds to the list in FCS_SSHS_EXT.1.7.
FCS_SSHS_EXT.1.8	The TOE is capable of rekeying. The TOE verifies the following thresholds: • No longer than one hour • No more than 512MB of transmitted data The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.
FCS_TLSC_EXT.2.1	The TOE implements TLS v.1.2 (RFC 5246) and rejects all other TLS and SSL versions The TOE supports TLS v1.2 protocol for use with X.509v3 based authentication. The TOE supports the following ciphersuites: • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

TOE SFR	Rationale
	• TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • 5246 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The ciphersuites specified are those listed in FCS_TLSC_EXT.2
FCS_TLSC_EXT.2.2	The TOE verifies that the presented identifier matches the reference identifier per RFC 6125 section 6. The reference identifiers supported are: DNS names or IP addresses. The TOE shall verify the peer certificate fingerprint against a configured value and verify certificate fields against locally configured peer DNS name or IP address (Subject Name Authorization) as per RFC6125 Section 6. The TOE does support wildcards.
FCS_TLSC_EXT.2.4	The TOE supports the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. This behavior is performed by default.
FCS_TLSC_EXT.2.5	The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication shall be performed when TOE acts as TLS Server. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certificate path validation supporting a **minimum path length of three certificates**. • The certificate path must terminate with a trusted CA certificate. The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE • The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TSF shall validate the extendedKeyUsage field according to the following rules: o *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.* *o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.* *o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.* *o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field*

TOE SFR	Rationale
	The TOE only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection.
FCS_TLSS_EXT.2.1	The TOE supports TLS v1.2 protocol with mutual authentication for use with X.509v3 based authentication. The TOE supports the following ciphersuites: • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The ciphersuites specified are those listed in FCS_TLSS_EXT.2
FCS_TLSS_EXT.2.2	The TOE denies connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.
FCS_TLSS_EXT.2.3	The TOE performs RSA key establishment supporting keys sizes of 2048 bits (must be enabled in the evaluated configuration), 3072 and 4096 bits. 4096 bits support was not tested/evaluated. The TOE implements EC Diffie-Hellman supporting NIST curves: secp256r1, secp384r1, secp521r1. The Diffie-hellman key agreement parameters are restricted to 3072 bits.
FCS_TLSS_EXT.2.4 and FCS_TLSS_EXT.2.5	The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication shall be performed when TOE acts as TLS Server. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certificate path validation supporting a **minimum path length of three certificates**. • The certificate path must terminate with a trusted CA certificate. The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE • The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TSF shall validate the extendedKeyUsage field according to the following rules:

TOE SFR	Rationale
	o *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.* *o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.* *o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.* *o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field* The TOE only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection.
FCS_TLSS_EXT.2.6	The TOE supports DNS name and IP addresses as its reference identifiers. When the syslog client receives an X.509 certificate from their respective servers, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type in the certificate, then the TSF will compare the reference identifier to the Common Name (CN) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes and additional verification actions can proceed. The TOE does support wildcards.
FIA_AFL.1	The Administrator can configure the maximum number of failed attempts for the CLI interface. The lockout feature can be configured from 2-10 unsuccessful attempts. When the defined number of unsuccessful attempts have been met, the TOE will not allow the user to login until the defined time period has elapsed. If the lockout attempts is set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct. The authentication failures cannot lead to a situation where no administrator access is available as the local CLI access would be accessible to the user as the local CLI cannot be locked out.
FIA_PMG_EXT.1	The TOE provides the following password management capabilities for administrator passwords;

TOE SFR	Rationale
	• Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“ ?”, “ ‘ “, “, “ + “, “ / “, “ : ”, “ ; “, “ < “, “ > “, “ = “, “ [“, “] “, “, “ ` “, “ ~ “, “ { “, “ } “, “ |”, and “ “. • Minimum password lengths shall be configurable to 1 character to maximum of 128 characters. The default minimum password length is 8 characters.
FIA_UIA_EXT.1	The TOE does not permit any actions prior to Administrators logging into the TOE. They are able to view the banner at the login prompt. Administrative access to the TOE is facilitated through one of several interfaces: • Connecting to the console port using RJ45-DB9 cable or USB-C-to-USB-C, USB-C-to-USB-A cables for the USB-C port. • Remotely connecting to each appliance via SSHv2 • Remotely connecting to appliance WebUI via HTTPS/TLS *NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.* Regardless of the interface at which the administrator interacts, the TOE prompts the user for a username and password. When the user provides the correct username and password, this is compared to the known user database and if they match then the user is granted access. Otherwise, the user will not be granted access to the TOE. The TOE does not provide a reason for failure in the cases of a login failure. For remote administration, the TOE supports RSA public key authentication and password based authentication. If the user uses public key based authentication and it is successful then the user is granted access to the TOE. If the user uses password based authentication and they provide valid username and password then the user is granted access to the TOE. If the user enters invalid user credentials, they will not be granted access and will be presented the login page.
FIA_UAU_EXT.2	The TOE provides a local password based authentication mechanism to perform local administration user authentication.
FIA_UAU.7	For all authentication at the local CLI the TOE displays only "*" characters when the administrative password is entered so that the password is obscured.
FIA_X509_EXT.1	The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication is performed when Waveserver acts as TLS Server. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules:

TOE SFR	Rationale
	• RFC 5280 certificate validation and certificate path validation supporting a **minimum path length of three certificates**. • The certificate path must terminate with a trusted CA certificate. The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE • The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TSF shall validate the extendedKeyUsage field according to the following rules: o *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.* *o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.* *o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.* *o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field* If it is a customer enrolled certificate, the validity period of the certificate is verified at the time of installation as well as a periodic checks is used to ensure validity. When the TOE receives a remote certificate during the secure channel establishment, the validity of the remote entity certificate is verified. The TOE also verifies the chain of trust by validating each certificate contained in the chain and verifying that a certificate path consists of trusted CA certificates and verify the validity of the certificates. These checks are done prior to loading the certificates onto the TOE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection.
FIA_X509_EXT.2	X.509 certificate can be used to authenticate and establish secure communication channel for RADIUS, and Syslog servers. The X.509 certificates are also used for establishing secure communication using HTTPS/TLS for the Web GUI. The TOE supports RSA based certificates and ECC based certificate in PKCS#12. The TOE supports X509 certificates to authenticate RSA Based Certificates The supported RSA key size shall be 2048 bits (must be enabled in the evaluated configuration), 3072 bits and 4096 bits. 4096 bits support was not tested/evaluated. The TOE supports the following signing algorithms for RSA based certificates: • RSA with SHA256

TOE SFR	Rationale
	• RSA with SHA384 • RSA with SHA512 ECC Based Certificate The supported Elliptic Curves are: • secp256 • secp384 • secp521 The TOE supports the following signing algorithms for ECC based certificates: • ECDSA with SHA256 • ECDSA with SHA384 • ECDSA with SHA512 The TOE allows each TLS service (RADIUS, Syslog and HTTPS/TLS) to be configured with its own certificate. Once a certificate is configured for RADIUS server, that certificate will be used for all RADIUS server connection authentication. Likewise, once a certificate is configured for TLS Syslog, that certificate will be used for all TLS Syslog collector server connection authentication. Finally, once a certificate is configured for HTTP Server, that certificate will be used for all HTTPS connection authentication. The TOE allows user to specify one X.509 Certificate/Private Key to be used for authentication with remote TLS Syslog server and RADIUS server. The TOE when operating as a TLS Client will check the validity of the TLS Server certificate prior to making a TLS connection with the TLS server. The TOE when operating as a TLS Server will check the validity of the TLS Client certificate prior to making a TLS connection with the TLS client. The X.509 certificate validation is determined based on reference ID verification, certificate path, extendedKeyUsage field, certificate expiry date and the certificate revocation status. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection.
FIA_X509_EXT.3	The CSR includes a mandatory auto generated public key and a mandatory user provisioned Common Name. The TOE allows the user to optionally enter the following information in the CSR: • Company Name or Organization (O); • Department or Organization Unit (OU); • Country (C);

TOE SFR	Rationale
	The TOE can import and validate the certificate chain of the CA that signs the CSR response. The CSR response shall also be validated against the current outstanding CSR signing request. It shall be removed once the corresponding CSR response is imported and validated. The TOE is capable of generating a Certificate Request as specified by RFC 2986. The TOE does not support the "device-specific information" within Certificate Request message.
FMT_MOF.1(1)/ManualUpdate	Only Security Administrators can perform manual software updates.
FMT_MTD.1/CoreData	The TOE implements Role Based Access Control (RBAC). Administrative users are required to login before being provided with access to any administrative functions. The TOE restricts the ability to manage the TOE to Security Administrators. The TOE maintains the following roles: Security administrator (super user), Admin user, and User (Limited user). Each role defined has a set of permissions that will grant them access to the TOE data.
FMT_SMF.1	The Security Administrator (Super user) has the following privileges: • Can configure user accounts and manage users and their associated privileges. • 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 signatures capability prior to installing those updates • Ability to configure the authentication failure parameters • Ability to configure audit behavior • Ability to set the time which is used for time-stamps • Ability to configure the reference identifier for the peer The User (Limited user) has the following privileges: • Able to carry out system monitoring and gather information about the configuration and performance of the system. • Can change their own password, but not other user's passwords
FMT_SMR.1	The TOE maintains the following user roles: Super user (Security Administrator), Admin and Limited user (User). The Security Administrator is able to manage the TOE both locally and remotely.
FPT_SKP_EXT.1	The TOE stores all private keys in a secure storage and is not accessible through an interface to administrators. Refer to section 7 Cryptographic Key Destruction, Table 12 Zeroization Table for all detail on key storage.

TOE SFR	Rationale
FPT_APW_EXT.1	All passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored as SHA-512 salted hash.
FPT_TST_EXT.1	All crypto algorithms used by the management interface must go through power up self-tests (KAT) before they can be used to provide service. The TOE executes the following power-on self-tests: • Software integrity test – the digital signature of software is validated to ensure its authenticity and integrity before the software is loaded into memory for execution. • AES Known Answer Test – the AES encryption and AES decryption algorithms are tested using test vectors. The results are compared against pre-computed results to ensure the algorithms are operating properly. • HMAC-SHA-256/384/512 Known Answer Test – the HMAC algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • SHA-256/384/512 Known Answer Test – the SHA algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • RSA Signature Known Answer Test – the RSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • ECDSA Signature Known Answer Test – the ECDSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. RNG Known Answer Test – the RNG is seeded with a pre-determined entropy and the RNG output is compared with output values expected for the pre-determined seed. When Waveserver Ai detects a failure during one or more of the self-tests, it raises an alarm. The administrator can attempt to reboot the TOE to clear the error. If rebooting the Waveserver Ai does not resolve the issue, then the administrator should contact their next level of support or their Ciena support group for further assistance. All power up self-tests execution are logged for both successful and unsuccessful completion. The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.
FPT_TUD_EXT.1	Security Administrators have the ability to query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the “software show” command. When software updates are available via the http://www.ciena.com website, they can obtain, verify the integrity and install the updates. The software images are digitally signed using RSA digital signature mechanism. The

TOE SFR	Rationale
	TOE will use a public key in order to verify the digital signature, upon successful verification the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.
FPT_STM.1	The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. The following security functions make use of the time: • Audit events • Session inactivity • X.509 certificate expiration validation
FTA_SSL_EXT.1	The TOE will terminate the session after a Security Administrator defined period of inactivity.
FTA_SSL.3	A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local CLI and remote SSH interfaces. The inactivity time period can range from 1 to 30 minutes for the CLI interface. The default value is 10 minutes for both the CLI and SSH interface. The configuration of inactivity periods are applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	The Security Administrator is able to terminate their CLI.
FTA_TAB.1	Security Administrators can create a customized login banner that will be displayed at the following interfaces: • Local CLI • Remote CLI This banner will be displayed prior to allowing Security Administrator access through those interfaces.
FTP_ITC.1	The TOE supports secure communication to the following IT entities: Syslog server and RADIUS server. The TOE uses TLS v1.2 protocol with X.509 certificate based authentication. The protocols listed are consistent with those included in the requirements in the ST.
FTP_TRP.1	The TOE supports HTTPS/TLS and SSH v2.0 for secure remote administration of the TOE. SSH v2.0 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect integrity of traffic. Remote GUI connections take place over a TLS connection. The TLS session is encrypted using AES encryption and uses HMACs to protect integrity. The protocols listed are consistent with those specified in the requirement. *NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.*

Table 11 TOE Summary Specification SFR Description

7 Cryptographic Key Destruction

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Diffie-Hellman Shared Secret	Provide Perfect Forward secrecy	RAM	Overwritten with zeros.
Passwords	User authentication	Only salted hash is stored in file system.	The configuration file is updated when the administrator issues a "configuration save" CLI command. Waveserver Ai also supports a Secure Erase feature that will reset the chassis back to factory default. All content, including the user credentials, will be removed as part of this operation.
Diffie Hellman private exponent	Diffie Hellman key generation	RAM	Overwritten with zeros.
SSH Private Key	SSH server	SSD/File system	Overwritten with zeros.
AES Key	Encrypt/decrypt, X509 certificate passphrase	SSD/File system	Overwritten with zeros.
SSH Session Key	SSH server	SSH Session Key is stored only in RAM.	Overwritten with zeros.
RNG Seed	Output from TRNG is used to seed the DRBG	RAM	Overwritten with zeros.
TLS Session Key	TLS syslog, RADsec, HTTPS	RAM	Overwritten with zeros.

Table 12 Zeroization Table

8 Terms and Definitions

Abbreviations/Acronyms	Description
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CLI	Command Line Interface
CSR	Certificate Signing Request
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol Secure
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
MB	Megabyte
PKCS	Public Key Cryptography Standards
RAM	Random Access Memory
RFC	Requests for Comments
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security

Table 13 TOE Abbreviations and Acronyms

Abbreviations/Acronyms	Description
CC	Common Criteria
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

Table 14 CC Abbreviations and Acronyms