Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series (NDcPP20E) Security Target

Version 0.3
10/22/2018

Prepared for:

Aruba, a Hewlett Packard Enterprise Company

8000 Foothills Blvd. Roseville, CA 95747

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series provided by Aruba, a Hewlett Packard Enterprise Company. The TOE is being evaluated as a network device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series (NDcPP20E) Security Target

ST Version – Version 0.3

ST Date – 10/22/2018

1.2 TOE Reference

TOE Identification – Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series running ArubaOS-CX version 10.01

TOE Developer – Aruba, a Hewlett Packard Enterprise Company

Evaluation Sponsor – Aruba, a Hewlett Packard Enterprise Company

1.3 TOE Overview

The Target of Evaluation (TOE) is Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series running Aruba OS-CX version 10.01

The following models are included in the evaluation:

Series Identifier	Hardware Models
Aruba 8320 Switch Series	JL479A – Aruba 8320 48p 10G SFP/SFP+ and 6p 40G QSFP+ Switch JL579A - Aruba 8320 32p 40G QSFP+ Switch JL581A - Aruba 8320 48p 1G/10GBase-T and 6p 40G QSFP+ Switch
Aruba 8400 Switch Series	JL376A – Aruba 8400 Bundle includes: • JL375A – Aruba 8400 8-slot chassis • JL363A – Aruba 8400 32p 10G SFP+ MACsec • JL365A – Aruba 8400 8p 40G QSFP+ Adv Module • JL367A – Aruba 7.2Tbps Fabric Module • JL368A – Management Module JL366A – Aruba 8400 6p 40G/100G QFSP 28p Adv Module

Table 1 TOE Models

The TOE offers comprehensive Layer 2 and Layer 3 features. The Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series provides security, scalability, and ease of use for enterprise edge deployments.

1.4 TOE Description

The TOE is a family of switches designed to support scalability, security and high performance for campus networks.

For the purpose of evaluation, the TOE will be treated as a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

1.4.1 TOE Architecture

Each TOE appliance provides a set of physical interfaces.

Table 1 identifies the models included in the evaluation. The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor (the 8320 includes an Intel Atom C2538 [Rangley microarchitecture] while the 8400 incorporates an Intel Xeon D15-17 [Broadwell microarchitecture]) and software that implements switching functions, configuration information and drivers. While hardware varies between different appliance models, the software code is shared across all platforms. It is in the software code that all the security functions claimed this security target are enforced.

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the ArubaOS-CX software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external SYSLOG server in the network environment. Figure 1 shows the TOE depicted in its intended environment.

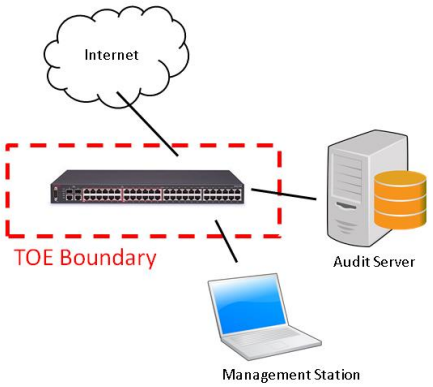

Figure 1: TOE Environment

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by 8320 & 8400 Switches:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using SSH to protect the logs while in transit on the network

1.4.1.2.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its SSHv2 protocol implementation. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing

1.4.1.2.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching rules and reading the login

banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

1.4.1.2.4 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of roles that can be assigned to TOE users. The TOE supports the following roles: Administrators, Operators. The Administrator role can make changes to the TOE configuration while the Operators role is a read-only role.

1.4.1.2.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operation environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

1.4.1.2.6 TOE access

The TOE can be configured to display a logon banner before and after (a post-login banner) a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

1.4.1.2.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSH to protect the CLI interface, ensuring integrity and preventing disclosure. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using SSH connections to prevent unintended disclosure or modification of logs.

1.4.2 TOE Documentation

Aruba offers a series of documents that describe the installation of the Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series as well as guidance for subsequent use and administration of the applicable security features. The following list of documents was examined as part of the evaluation:

Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.1, October 24, 2018 **[Admin Guide]**

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant
- Package Claims:
    - collaborative Protection Profile for Network Devices, Version 2.0 + Errata, 14 March 2018 (NDcPP20E)
- Technical Decisions as of October 04, 2018:
    - TD0339, TD0338, TD0336, TD0324, TD0291, TD0290, TD0281, TD0260, TD0259, TD0228

TD No.	Applied?	Rationale/Description
TD0343	No	IPsec not claimed
TD0342	No	TLS not claimed
TD0341	No	TLS not claimed
TD0340	No	X509 not claimed
TD0339	Yes	Affects SSH SFR selections
TD0338	Yes	Affects FTA_TAB.1 TSS requirements
TD0337	No	FCS_SSH*_EXT.1.6 does not claim gcm ciphers
TD0336	Yes	FCS_SSHS_EXT.1.8 included
TD0335	No	FCS_DTLS not claimed
TD0334	No	FCS_SSHC not claimed
TD0333	No	X509 does not apply
TD0324	Yes	Corrected section numbers in SD Table 1
TD0323	No	DTLS not claimed
TD0322	No	TLS not claimed
TD0321	No	NTP not claimed
TD0291	Yes	NIT technical decision for DH14 and FCS_CKM.1
TD0290	Yes	NIT technical decision for physical interruption of trusted path/channel.
TD0289	No	TLS not claimed. NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e
TD0281	Yes	NIT Technical Decision for Testing both thresholds for SSH rekey
TD0262	No	TLS not claimed. NIT Technical Decision for TLS server testing - Empty Certificate Authorities list
TD0260	Yes	NIT Technical Decision for Typo in FCS_SSHS_EXT.1.4
TD0259	Yes	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187
TD0257	No	TLS not claimed. NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4
TD0256	No	TLS not claimed. NIT Technical Decision for Handling of TLS connections with and without mutual authentication
TD0228	Yes	NIT Technical Decision for CA certificates - basicConstraints validation

2.1 Conformance Rationale

The ST conforms to the NDcPP20E. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP20E and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP20E offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

In general, the NDcPP20E has defined Security Objectives appropriate for network devices and as such are applicable to the Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.COMPONENTS_RUNNING (applies to distributed TOEs only) For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

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

OE.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.

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

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

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP20E. The NDcPP20E defines the following extended requirements and since they are not redefined in this ST the NDcPP20E should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- FAU_STG_EXT.1: Protected Audit Event Storage
- FCS_RBG_EXT.1: Random Bit Generation
- FCS_SSHS_EXT.1: SSH Server Protocol
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FPT_APW_EXT.1: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- FPT_STM_EXT.1: Reliable Time Stamps
- FPT_TST_EXT.1: TSF testing
- FPT_TUD_EXT.1: Trusted update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP20E. The refinements and operations already performed in the NDcPP20E are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP20E and any residual operations have been completed herein. Of particular note, the NDcPP20E made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP20E which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDcPP20E that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDcPP20E should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	FCS_RBG_EXT.1: Random Bit Generation
	FCS_SSHS_EXT.1: SSH Server Protocol
FIA: Identification and authentication	FIA_AFL.1: Authentication Failure Management
	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	FMT_MTD.1/CoreData: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Administrator Passwords
	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

	FPT_STM_EXT.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF testing
	FPT_TUD_EXT.1: Trusted update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1/Admin: Trusted Path

Table 2 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

Requirement	Auditable Events	Additional Content
FAU_GEN.1		
FAU_GEN.2		
FAU_STG_EXT.1		
FCS_CKM.1		
FCS_CKM.2		
FCS_CKM.4		
FCS_COP.1/DataEncryption		
FCS_COP.1/Hash		
FCS_COP.1/KeyedHash		
FCS_COP.1/SigGen		
FCS_RBG_EXT.1		
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1		
FIA_UAU.7		
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).

FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
FMT_MTD.1/CoreData	All management activities of TSF data.	
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	
FMT_SMF.1		
FMT_SMR.2		
FPT_APW_EXT.1		
FPT_SKP_EXT.1		
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1		
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
FTA_SSL.4	The termination of an interactive session.	
FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	
FTA_TAB.1		
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.	

Table 3 Audit Events

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 2.

5.1.1.2 User identity association (FAU_GEN.2)

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.

5.1.1.3 Protected Audit Event Storage (FAU_STG_EXT.1)

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 log file is cleared]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: ***- 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 (per TD0291)].

5.1.2.2 Cryptographic Key Establishment (FCS_CKM.2)

FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [***- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 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].

5.1.2.3 Cryptographic Key Destruction (FCS_CKM.4)

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] overwrite consisting of [zeroes],***
o instructs a part of the TSF to destroy the abstraction that represents the key]
that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (FCS_COP.1/DataEncryption)

FCS_COP.1.1/DataEncryption

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

5.1.2.5 Cryptographic Operation (Hash Algorithm) (FCS_COP.1/Hash)

FCS_COP.1.1/Hash

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

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

FCS_COP.1.1/KeyedHash

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

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

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]]
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].

5.1.2.8 Random Bit Generation (FCS_RBG_EXT.1)

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 [***[one] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.9 SSH Server Protocol (FCS_SSHS_EXT.1)

FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFC(s) [***4251, 4252, 4253, 4254, 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 [***256KB***] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-cbc (TD0260 applied), aes256-cbc, aes128-ctr, aes256-ctr***].

FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [***ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms. (TD0259 applied)

FCS_SSHS_EXT.1.6

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

FCS_SSHS_EXT.1.7

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

FCS_SSHS_EXT.1.8

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

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [***1-10***] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed***].

5.1.3.2 Password Management (FIA_PMG_EXT.1)

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***] and [***32***].

5.1.3.3 Protected Authentication Feedback (FIA_UAU.7)

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.

5.1.3.4 Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, and [***no other authentication mechanism***] to perform local administrative user authentication.

5.1.3.5 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1

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

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

FIA_UIA_EXT.1.2

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (FMT_MOF.1/ManualUpdate)

FMT_MOF.1.1/ManualUpdate

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

5.1.4.2 Management of TSF Data (FMT_MTD.1/CoreData)

FMT_MTD.1.1/CoreData

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

5.1.4.3 Specification of Management Functions (FMT_SMF.1)

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;
- [***o Ability to configure audit behavior,***
  o Ability to configure the cryptographic functionality,
  o Ability to set the time which is used for time-stamps;].

5.1.4.4 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (FPT_APW_EXT.1)

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.

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

FPT_SKP_EXT.1.1

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

5.1.5.3 Reliable Time Stamps (FPT_STM_EXT.1)

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***].

5.1.5.4 TSF testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [***integrity, AES, SHS, HMAC, RSA, ECDSA and DRBG***].

5.1.5.5 Trusted update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1

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

FPT_TUD_EXT.1.2

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

FPT_TUD_EXT.1.3

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

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1

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

5.1.6.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1

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

5.1.6.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***- terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.6.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1

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

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1

The TSF shall be capable of using [***SSH***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***no other capabilities***] 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 [***no services***].

5.1.7.2 Trusted Path (FTP_TRP.1/Admin)

FTP_TRP.1.1/Admin

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

FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin

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

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 4 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

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

ADV_FSP.1.1c

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

ADV_FSP.1.2c

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

ADV_FSP.1.3c

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

ADV_FSP.1.4c

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

ADV_FSP.1.1e

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

ADV_FSP.1.2e

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

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

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

AGD_OPE.1.2c

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

AGD_OPE.1.3c

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

AGD_OPE.1.4c

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

AGD_OPE.1.5c

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

AGD_OPE.1.6c

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

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

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

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d
The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c
The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c
The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e
The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c
The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing Conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

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

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

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

AVA_VAN.1.2e

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

AVA_VAN.1.3e

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

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is able to generate audit records of security relevant events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in **Table 3 Audit Events**.

The different types of audit records that are provided by the TOE are: emergency, alert, critical, error, warning, notice, info, debug, and event (note that only the Event Log supports the event type). Audit logs are stored as strings and have a format which includes the severity, date and time of the event, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent responsible for the event.

The audit records are protected against unauthorized access by only allowing authorized administrators to have access to local audit logs. The logged audit records also include event-specific content that includes at least all of the content required in **Table 3 Audit EventsError! Reference source not found.**. For cryptographic keys, the act of importing a key is audited and the associated administrator account that performed the action is recorded.

There is a method of specifying the minimum severity level of the audit logs that shall be sent to a syslog server. Locally stored audit logs are kept regardless of severity level. The severity level of audit is configured through the syslog server configuration. The TOE supports local log entries for each of the three types of logs maintained by the TOE: accounting, event, and authentication log. The administrator “logrotate” CLI command controls the log file threshold (10-200MB) and rotation frequency (hourly, daily, weekly, monthly) for each log type. The TOE will check each hour to determine whether or not to rotate its logs based upon log size and time elapsed. If needed, the TOE will rotate the logs, deleting the oldest.

The accounting log predominately includes the TOE’s audit records of CLI commands. The TOE relies upon auditd for maintenance of the accounting log, and the TOE holds two logs (a working and one old) in memory and stores the last 10,000 lines of logs to persistent storage (Flash) at each shutdown. An administrator can locally view this log through the CLI (“show accounting log all”).

The TOE stores SSH related audit records in its authentication log. The TOE stores one working log and three old, compressed logs in memory. An administrator can export the authentication log audit records to a remote syslog server.

The TOE stores audit records related to client SSH public key operations (add/remove) time/date changes, and trusted updates (initiation and success/failure) in its event log. Like the authentication log, the TOE also stores one working copy and three old, compressed logs in memory. The TOE uses journald to maintain the authentication and event logs, and the TOE also stores event logs persistently in Flash.

By default, the TOE forwards audit messages from its event log to the configured syslog server, and additionally, when configured by an administrator, the TOE also forwarded messages from its accounting and authentication logs to the configured syslog server. Once configured to export audit records, the TOE attempts to transmit all logs in

real-time, will temporarily maintain unsent records in the event of a disrupted syslog connection, and send those records when the remote audit server successfully reestablishes the connection. The TOE uses the SSH protocol to protect audit records transmitted to the external syslog server.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: Each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 3 Audit EventsError! Reference source not found.**. When logging the administrative tasks of generating/importing/deleting cryptographic keys, the TOE logs the type of key and its SHA256 hash as the key identifier.
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with SSH.

6.2 Cryptographic support

The TOE's internal cryptographic library (the CryptoComply Server Engine version 2.1) has been CAVP tested. The following functions have been CAVP tested to meet the associated SFRs.

SFR	Algorithm	NIST Standard	Cert#
FCS_CKM.1 (Key Gen)	ECDSA ECC Key Generation	FIPS 186-4, ECDSA	1496
FCS_CKM.2 (Key Establishment)	ECC-based Key Exchange	SP 800-56A, CVL KAS ECC	1988
FCS_COP.1/DataEncryption	AES 128/256 CBC, CTR	FIPS 197, SP 800-38A	5552
FCS_COP.1/Hash	SHA Hashing	FIPS 180-4	4455
FCS_COP.1/KeyedHash	HMAC-SHA	FIPS 198-1 & 180-4	3700
FCS_COP.1/SigGen	RSA Sign/Verify	FIPS 186-4, RSA	2982
	ECDSA Sign/Verify	FIPS 186-4, ECDSA	1496
FCS_RBG_EXT.1 (Random)	DRBG Bit Generation	SP 800-90A	2207

Table 5 TOE Cryptographic Algorithms

The product implements and uses an SP 800-90A AES-256 CTR_DRBG.

FCS_CKM.1/2: For asymmetric key pairs used for authentication. the TOE can generate ECDSA SSH host keys (public and private) of size P-256, P-384, and P-521 and can, upon command, regenerate a new ECDSA host key. Additionally, the administrator can load and remove user SSH public keys, that the TOE will use to authenticate SSH clients.

For asymmetric key pairs used for key exchange, the TOE supports generating ephemeral ECDH keys and DH keys for the SSHv2 key exchange methods selected in FCS_SSHS_EXT.1.7 in section 5.1.2.9. This implies that the TOE generates ephemeral 256/384-bit ECDH keys using ECC schemes for P-256/384 curves and 2048-bit keys using FFC schemes for DH keys for prime group DH14. TOE supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability. Because the TOE is an SSH server, it always acts as the recipient/responder in the key exchange process.

FCS_CKM.4: The following table presents the crypto security parameters (CSPs), secret keys, and private keys provided by the TOE. The table also identifies when each CSP or key is cleared.

CSP or Key:	Stored in	Zeroized upon:	Zeroized by:
SSH host ECDSA private key	On Disk	Command	Overwriting with zeros
SSH host ECDSA public key	On Disk	Command	Overwriting with zeros
SSH client ECDSA public key	On Disk	Command	Overwriting with zeros
SSH session key	In Memory	Close of session	Overwriting with zeros
Password hash	On Disk	Command	Overwriting with zeros

Table 6 Key Zeroziation

Keys are zeroized when they are no longer needed by the TOE, and additionally, the TOE saves keys to persistent storage. Whether saving or destroying keys, the TOE delays the operation at the physical layer until the administrator issues the "write memory" command, which saves the running configuration to the startup configuration.

FCS_COP.1/DataEncryption: As seen in **Table 5** above, the TOE supports the CBC and CTR modes of AES as available ciphers for SSH (with both 128 and 256-bit keys).

FCS_COP.1/Hash: The TOE uses the SHA-1, 256, and 512 hashing algorithms as part of SSHv2 integrity algorithms (see FCS_SSHS_EXT.1.6). The TOE also uses SHA-256 during verification of a new image (trusted updates).

FCS_COP.1/KeyedHash: The TOE uses the HMAC algorithms described below as part of SSHv2 (for integrity).

HMAC Algorithm	Hash Alg	Key size	Block Size	Output MAC
HMAC-SHA-1	SHA-1	160	512	160 bits
HMAC-SHA-256	SHA-256	256	512	256 bits
HMAC-SHA-512	SHA-512	512	1024	512 bits

Table 7 HMAC Details

FCS_COP.1/SigGen: As seen in **Table 5** above, the TOE supports both RSA and ECDSA signing and verification. The TOE verifies RSA signatures on firmware updates (see FPT_TUD_EXT.1 in section 6.5 below) and supports ECDSA authentication during SSH.

FCS_RBG_EXT.1: See **Table 5** above. The TOE instantiates its AES-256 CTR_DRBG with a 384-bit seed (containing a minimum of 365 bits of entropy) from a software-based noise source.

FCS_SSHS_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions and syslog export as indicated above. The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, 4254, 5656, 6668. The TOE supports public key-based and password-based authentication. The TOE allows use of the ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521 algorithms for public key authentication. The TOE supports AES-CBC and AES-CTR (both 128 and 256 keyed variants) ciphers for data encryption and hmac-sha1/sha2-256/sha2-512 for data integrity (and does not allow the "none" MAC algorithm). The TOE uses Diffie-hellman-group14-sha1 (using the 2048-bit prime specified in section 3 of RFC 3526) along with ecdh-sha2-nistp256/384 for SSHv2 key exchange. The TOE's SSHv2 implementation limits SSH packets to a size of 256 kilobytes. Anything larger will be dropped by the TOE. The TOE initiates a rekey before 1 hour has passed or before 1GB of data transfer occurs, whichever comes first.

6.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can access any of the TOE functions except to display a warning banner and to permit network switching services without identification or authentication. In the evaluated configuration, users can connect to the TOE via a local console or remotely using SSHv2.

The user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1). When logging in the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

The Authorized Administrator can set a lockout failure count for login attempts as the TOE's default configuration does not enforce a failed login limit. If the count is exceeded, the targeted account is locked (preventing remote administrators from logging in through SSH under the locked account/username) for an administrator-configurable time limit. Note that the TOE does not lock administrative access through local console, only remote/SSHv2 administrator access.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: An administrator account can be locked after failed authentication attempts. In order to re-establish the account, an administrator configured time period must elapse.

- FIA_PMG_EXT.1: The TOE offers a wide range of characters for passwords as described above.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.2: The TOE uses local password-based authentication.
- FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for displaying warning banner, without requiring a user to be identified and authenticated.

6.4 Security management

The TOE provides two roles: Administrators (Security Administrator) and Operators. The Security Administrator role is simply an admin and has full control over the device whereas the Operator role may view status information only. Upon successful authentication to the TOE, the admin can manage the TSF data.

The TOE offers command line functions which are accessible via the CLI. The CLI is a text based interface which can be accessed from a directly connected terminal or via a remote terminal using SSHv2. These command line functions can be used to manage every security policy, as well as the non-security relevant aspects of the TOE.

Once authenticated (none of these functions is available to any user before being identified and authenticated), authorized administrators have access to the following security functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- Ability to configure a login banner as well as network switching functions;
- Ability to configure the cryptographic functionality
- Ability to configure the session inactivity time before session termination or locking;
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to configure audit behavior;
- Ability to set the time which is used for time-stamps,

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1/(ManualUpdate): Only the administrator can initiate product updates.
- FMT_MTD.1/(CoreData): Only the administrator can configure TSF-related functions.
- FMT_SMF.1: The TOE includes the functions necessary to manage its cryptographic functionality and associated functions, configure the warning banner, manage user accounts, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes a manager account that corresponds to the required ‘Authorized Administrator’ also referred to as ‘Security Administrator’ in some requirements or text.

6.5 Protection of the TSF

The TOE is an appliance and does not offer general purpose operating system interfaces to users. The TOE is designed to not provide access to locally stored passwords and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE.

The TOE is a hardware appliance that includes a real-time clock (note that 8400 model also has a battery to maintain time across power cycles). The TOE uses the clock to support several security functions including timestamps for audit records, timing elements of cryptographic functions, and inactivity timeouts. The TOE provides the administrator the ability to manually set the clock.

The TOE performs diagnostic self-tests during start-up and generates audit records to document failure. Some low-level critical failure modes can prevent TOE start-up and as a result will not generate audit records. In such cases, TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE will reboot with errors displayed when non-critical errors are encountered. The cryptographic library performs self-tests during startup; the messages are displayed on the console and syslog records generated for both successful and failed tests.

Upgrading the ArubaOS-CX firmware is a manual process performed by an authorized administrator. An administrator can use the "show version" and "show images" commands to query the TOE's loaded and active firmware versions. The firmware is digitally signed with RSA 3072 using SHA-256. The TOE uses one of two embedded (within the TOE's firmware images) public keys to verify the digital signature (the vendor includes a primary and a backup signing public key). The firmware is readily available on the HPE website. Uploading the firmware to the devices does require successful authentication to the devices in order to issue the CLI commands needed to update. The TOE will validate the firmware validation during the loading process and will reject the firmware if validation fails. HPE signs the firmware images and includes the HPE signing public keys within the running firmware. Once the TOE has successfully loaded a new firmware image, it becomes active upon the next reboot.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Furthermore, locally defined passwords are not stored in plaintext form, instead the TOE stores the password as salted SHA-512 hashes.
- FPT_SKP_EXT.1: The TOE stores its SSH host private keys in plaintext form but does not offer any functions to output the cryptographic key value.
- FPT_STM_EXT.1: The TOE includes its own hardware clock and allows the administrator to manually configure the time.
- FPT_TST_EXT.1: The TOE performs a suite of self-tests to verify its integrity. The TOE performs an integrity test of its firmware (by validating the firmware's RSA digital signature) product and also performs a set of power-up self-tests including AES, SHS, HMAC, RSA, ECDSA and DRBG known answer tests. The TOE automatically performs its known answer power on self-tests (POST) on its CryptoComply cryptography library by computing a trial cryptographic operation (e.g., AES encryption) and then comparing the calculated result to the known correct result (already compiled into the library). This ensures that the TOE's implementations work correctly. Should any of the tests fail, the TOE halts the boot process.
- FPT_TUD_EXT.1: The TOE provides the administrator a CLI command to manually install digitally signed (using RSA 3072 with SHA-256) updates.

6.6 TOE access

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes). The inactivity timeout is disabled by default. This session timeout value is applicable to both local and remote sessions. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to re-enter their user ID and their password so they can establish a new session once a session is terminated. If the user ID and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

The TOE can be configured to display administrator-configured advisory banners. A login banner can be configured to display warning information along with login prompts. The banners will be displayed when accessing the TOE via the console and SSH interfaces.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE allows a user to logout (or terminate) both local and remote sessions.
- FTA_SSL_EXT.1: The TOE locks local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display a warning banner when administrators successfully establish interactive sessions with the TOE, allowing users to terminate their session prior to performing any functions.

6.7 Trusted path/channels

The TOE uses SSHv2 to protect communications between itself and the audit server as well to protect remote administration. The use of SSHv2 ensures traffic is not modified or disclosed.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use a reverse SSH tunnel to ensure that any exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides SSHv2 secured remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP tested cryptographic operations, and all remote security management functions require the use of one of these secure channels.