Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 (NDcPP20E) Security Target

Version 0.6
05/31/18

Prepared for:

Aruba, a Hewlett Packard Enterprise Company

8000 Foothills Blvd.
Roseville, CA 95747

Prepared By:

Gossamer Laboratories

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 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 provided by 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 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 (NDcPP20E) Security Target

ST Version – Version 0.6

ST Date – 05/31/18

1.2 TOE Reference

TOE Identification – Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04

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 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04.

The following models are included in the evaluation:

Series	Hardware Models	Processor
Aruba 2930F Switch Series	2930F 24G 4SFP+ Switch (JL253A) 2930F 48G 4SFP+ Switch (JL254A) 2930F 8G PoE+ 2SFP+ Switch (JL258A) 2930F 24G PoE+ 4SFP+ Switch (JL263A) 2930F 48G PoE+ 4SFP+ Switch (JL264A)	Dual Core ARM Coretex
Aruba 2930M Switch Series	2930M 24G 1-slot Switch (JL319A) 2930M 24G PoE+ 1-slot Switch (JL320A) 2930M 48G 1-slot Switch (JL321A) 2930M 48G PoE+ 1-slot Switch (JL322A) 2930M 40 Port 1G + 8 Port SmartRate PoE+ (JL323A) 2930M 24 Port SmartRate PoE+ (JL324A)	Dual Core ARM Coretex
Aruba 3810M Switch Series	3810M 24G 1-slot Switch (JL071A) 3810M 48G 1-slot Switch (JL072A) 3810M 24G PoE+ 1-slot Switch (JL073A) 3810M 48G PoE+ 1-slot Switch (JL074A) 3810M 16SFP+ 2-slot Switch (JL075A) 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch (JL076A)	Freescale P2020 Dual Core
Aruba 5400R Switch Series	5406R zl2 Switch (J9821A) 5412R zl2 Switch (J9822A) 5406R/5412R-24-port 10/100/1000Base-T PoE+ MACsec (No PSU) v3 zl2 Card (J9986A) 5406R/5412R-24p 1000BASE-T (No PSU) v3 zl2 Card (J9987A) 5406R/5412R-24p SFP (No PSU) v3 zl2 Card (J9988A) 5406R/5412R-12p PoE+ / 12p 1GbE SFP (No PSU) v3 zl2 Card (J9989A) 5406R/5412R-20p PoE+ / 4p SFP+ (No PSU) v3 zl2 Card (J9990A) 5406R/5412R-20p PoE+ / 4p 1/25/5/XGT PoE+ (No PSU) v3 zl2 Card (J9991A) 5406R/5412R-20p PoE+ / 1p 40GbE QSPF+ (No PSU) v3 zl2 Card (J9992A) 5406R/5412R-8p 1G/10GbE SFP+ v3 (No PSU) v3 zl2 Card (J9993A) 5406R/5412R-2-port 40GbE QSFP+ (No PSU) v3 zl2 Card (J9996A)	Freescale P2020 Dual Core

Table 1 TOE Models

The TOE offers comprehensive Layer 2 and Layer 3 feature sets including RIP, BGP, PoE+, and IPv4 and IPv6 functionalities. The Aruba 2930F, 2930M, 3810M, and 5400R Switch Series provides security, scalability, and ease of use for enterprise edge deployments.

1.4 TOE Description

The TOE is the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04. 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

The Aruba 2930F, 2930M, 3810M, and 5400R Switch Series TOE is a set of hardware appliances. Each 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, and processor 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 in this security target are enforced.

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the Aruba 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. The TOE can also sync its time with an NTP server. Figure 1 shows the TOE depicted in its intended environment.

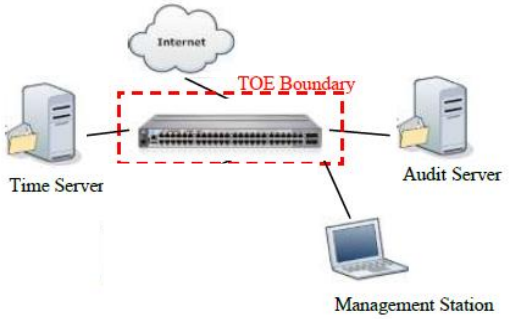

Figure 1TOE Environment

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04:

- 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 TLS 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 and TLS protocol implementations. 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. The TOE also provides X.509 certificate checking for its TLS connections.

1.4.1.2.4 Security management

The TOE provides Command Line Interface (CLI) commands and a web GUI 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: Manager, Operator. The Manager role can make changes to the TOE configuration while the Operator 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 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 for CLI and TLS for the web GUI to ensure both integrity and disclosure protection. 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 TLS connections to prevent unintended disclosure or modification of logs.

1.4.2 TOE Documentation

HPE offers a series of documents that describe the installation of the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series as well as guidance for subsequent use and administration of the applicable security features. The following document was examined as part of the evaluation: Common Criteria Configuration Guidance Network Device Collaboration Protection Profile, Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series, Version 1.4, May 14, 2018.

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 20180314, 14 March 2018 (NDcPP20E)
- NIAP Technical Decisions
    - TD0228, TD0257, TD0259, TD0260, TD0281, TD0289, TD0290, TD0291

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 2930F, 2930M, 3810M, and 5400R 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.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_HTTPS_EXT.1: HTTPS Protocol
- FCS_RBG_EXT.1: Random Bit Generation
- FCS_SSHS_EXT.1: SSH Server Protocol
- FCS_TLSC_EXT.1: TLS Client Protocol
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- FIA_X509_EXT.2: X.509 Certificate Authentication
- FIA_X509_EXT.3: X.509 Certificate Requests
- 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 2930F, 2930M, 3810M, and 5400R 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/SigGen: Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1: Random Bit Generation
	FCS_HTTPS_EXT.1: HTTPS Protocol
	FCS_SSHS_EXT.1: SSH Server Protocol
	FCS_TLSC_EXT.1: TLS Client Protocol
	FCS_TLSS_EXT.1: TLS 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
	FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	FIA_X509_EXT.2: X.509 Certificate Authentication
	FIA_X509_EXT.3: X.509 Certificate Requests
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 (Admin)

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 3.

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/SigGen		
FCS_COP.1/Hash		
FCS_COP.1/KeyedHash		
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_RBG_EXT.1		
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish a TLS 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).
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate.	Reason for failure.
FIA_X509_EXT.2		
FIA_X509_EXT.3		
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
FMT_MTD.1/CoreData	All management activities of TSF data.	
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 3.

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 audit records are written in a circular buffer]***] 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: [
- 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] 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].
(TD0291 applied)

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

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-pass] overwrite consisting of [zeroes]]]
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, GCM***] 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, GCM as specified in ISO 19772***].

5.1.2.5 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 bits]***]
that meet the following:
[***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3***].

5.1.2.6 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-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] that meet the following: ISO/IEC 10118-3:2004.

5.1.2.7 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***] and cryptographic key sizes [***160***] and message digest sizes [***160***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.8 HTTPS Protocol (FCS_HTTPS_EXT.1)

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 require client authentication***] if the peer certificate is deemed invalid.

5.1.2.9 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 [***[2] software-based noise sources***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011, of the keys and CSPs that it will generate.

5.1.2.10 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***].

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 [***35000 bytes***] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4

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

FCS_SSHS_EXT.1.5

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

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha1-96***] and [***no other MAC algorithms***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

The TSF shall ensure that [***diffie-hellman-group14-sha1***] and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8

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

5.1.2.11 TLS Client Protocol (FCS_TLSC_EXT.1)

FCS_TLSC_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [***TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,***
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FCS_TLSC_EXT.1.2

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

FCS_TLSC_EXT.1.3

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.1.4

The TSF shall [***present the Supported Elliptic Curves Extension with the following NIST curves: secp256r1, secp384r1***] in the Client Hello.

5.1.2.12 TLS Server Protocol (FCS_TLSS_EXT.1)

FCS_TLSS_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [***TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,***
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FCS_TLSS_EXT.1.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [***none***].

FCS_TLSS_EXT.1.3

The TSF shall [***generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1] and no other curves***].

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 [***8***] and [***64***].

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;
- [***network switching services***].

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.

5.1.3.6 X.509 Certificate Validation (FIA_X509_EXT.1/Rev)

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 certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- 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.

5.1.3.7 X.509 Certificate Authentication (FIA_X509_EXT.2)

FIA_X509_EXT.2.1

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

FIA_X509_EXT.2.2

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

5.1.3.8 X.509 Certificate Requests (FIA_X509_EXT.3)

FIA_X509_EXT.3.1

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

FIA_X509_EXT.3.2

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

5.1.4 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 list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,
o Ability to configure the cryptographic functionality
o
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, synchronise time with external time sources***].

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: [

- AES Encrypt and Decrypt Known Answer Tests (KATs)
- CTR DRBG KATs (DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
- HMAC-SHA1 KAT
- RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
- SHA1/256/512 KATs
- Triple-DES Encrypt and Decrypt KATs

].

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 [***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.

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 [***TLS***] 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 [***exporting audit records***].

5.1.7.2 Trusted Path (Admin) (FTP_TRP.1/Admin)

FTP_TRP.1/Admin.1

The TSF shall be capable of using [***SSH, TLS***] 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/Admin.2

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

FTP_TRP.1/Admin.3

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: info, debug, warning and fatal. 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 Events**. For cryptographic keys, the act of importing and deleting a key is audited and the associated administrator account that performed the action is recorded. Note that there no notion of changing a key – it is either imported or deleted.

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 up to 6400 log entries locally. The local audit log is a circular buffer and when the maximum number of entries is reached, the oldest log entries are overwritten automatically and a warning audit event is created when the log reaches 80%. By default, all event logs are sent to the set of configured syslog servers as well as the local store with the exception of console commands. The console commands must be sent to the syslog server using a manual procedure described in the evaluated Guidance document (see Section 1.4.2). The Guidance recommends manually sending the audit logs when the warning message is received. The TOE uses the TLS protocol to send generated audit records to an 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**.
- 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 the use of TLS.

6.2 Cryptographic support

The TOE has been CAVP tested. The following functions have been CAVP tested to meet the associated SFRs.

Functions	Requirement	Certificates
Encryption/Decryption		
AES CBC, GCM (128 or 256 bits)	FCS_COP.1/DataEncryption	4853
Cryptographic signature services		
RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FCS_COP.1/SigGen	2665
Cryptographic hashing		

SHA-1, SHA-256, SHA-384, SHA-512 (digest sizes 160, 256, 384, 512)	FCS_COP.1/Hash	3991
Keyed-hash message authentication		
HMAC-SHA-1 (digest size 160)	FCS_COP.1/KeyedHash	3249
Random bit generation		
AES-256 CTR_DRBG with software based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	1705
Key generation		
RSA Key Generation (2048 bits)	FCS_CKM.1	2665
ECDSA Key Generation (P-256, P-384)	FCS_CKM.1	1243
Key Establishment		
CVL ECC KAS	FCS_CKM.2	1490

Table 5 Cryptographic Functions

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

The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, and 4254. The TOE supports public key-based and password-based authentication. SSH_RSA public key algorithm is used for authentication. AES-CBC-128, AES-CBC-256 algorithms are used for data encryption. hmac-sha1 and hmac-sha1-96 are used for data integrity. Diffie-hellman-group14-sha1 for the key exchange method is used for key exchange. The TOE's SSHv2 implementation limits SSH packets to a size of 35000 bytes. Anything larger will be dropped by the TOE. There is a TOE initiated rekey before 1 hour or before 1GB whichever comes first.

The TOE provides TLS v1.1 and 1.2 for use when exporting audit records to a SYSLOG server and when acting as web server for administration. The following ciphersuites are supported when configured by the administrator as instructed in the guidance:

- TLS_RSA_WITH_AES_128_CBC_SHA,
- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_RSA_WITH_AES_128_CBC_SHA256,
- TLS_RSA_WITH_AES_256_CBC_ SHA256,
- TLS_RSA_WITH_AES_128_GCM_SHA256,
- TLS_RSA_WITH_AES_256_GCM,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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 RSA private key	On Disk	Command	Overwriting with zeros
SSH host RSA public key	On Disk	Command	Overwriting with zeros
SSH client RSA public key	On Disk	Command	Overwriting with zeros
SSH session key	In Memory	Close of session	Overwriting with zeros
TLS session key	In Memory	Close of session	Overwriting with zeros
Password hash	On Disk	Command	Overwriting once with zeros

Table 6 Key Zeroziation

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE generates RSA and ECDH asymmetric keys as part of TLS key establishment as part of TLS as described in the section above. The TOE acts as both a client and a server. The TOE supports Diffie-Hellman key generation for SSH key establishment where the TOE is acting as a server.

The TOE also provides the administrator the ability to generate or import either an ECDSA (P-256 or P-384) or RSA (2048) key to use for TLS.

- FCS_CKM.2: See FCS_CKM.1. The TOE implementation of Diffie-Hellman-group-14 meets RFC 3526, Section 3 by virtue of using a 2048-bit MODP group for key establishment.
- FCS_CKM.4: Keys are zeroized when they are no longer needed by the TOE. **Table 6 Key Zeroziation** identifies when keys are cleared.
- FCS_COP.1/DataEncryption: The TOE performs encryption and decryption using AES in CBC and GCM mode with key sizes of either 128 or 256. The corresponding CAVP certificate is identified in the table above.
- FCS_COP.1/SigGen: The TOE supports the use of RSA with 2048 bit key sizes for cryptographic signatures. Digital signatures are used in TLS communications and on product updates. The corresponding CAVP certificate is identified in the table above.
- FCS_COP.1/Hash: The TOE supports cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512, with digest sizes 160, 256, 384, and 512. The corresponding CAVP certificate is identified in the table above.
- FCS_COP.1/KeyedHash: The TOE supports keyed-hash message authentication using HMAC-SHA-1 with 160-bit keys to produce a 160 output MAC. The SHA-1algorithm has a block size of 512-bits. The corresponding CAVP certificate is identified in the table above.
- FCS_HTTPS_EXT.1: The TOE provides a web interface for remote administration and fully supports RFC 2818. The TOE acts as an HTTPS server and waits for client connections on TCP port 443. The TOE's HTTPS server supports TLS version 1.1/1.2 only and will deny connection requests from TLS clients with lower versions.
- FCS_RBG_EXT.1: The product uses an SP 800-90A AES-256 CTR_DRBG with two software based noise sources with a minimum of 256 bits of non-determinism.
- FCS_SSHS_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FCS_TLSC_EXT.1: The TOE supports TLS when exporting audit logs to an external server.
- FCS_TLSS_EXT.1: The TOE supports TLS v1.1 and v1.2 with the ciphersuites listed above for the web management interface. The TOE will reject all SSL and older TLS versions (1.0) for connection attempts.

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 provide 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 as well as using a web GUI protected via TLS. 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. The default value is three failed attempts. If the count is exceeded, the targeted account is locked for an administrator-configurable time limit. The lockout mechanism is only applicable to remote administration and does not apply to the local console.

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, a settable time period must pass.
- 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 the switching of network traffic and displaying warning banner, without requiring a user to be identified and authenticated.
- FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. The following fields are verified:
  - Chain length
  - Certificate revocation check with OCSP
  - Certificate Validity
  - CA validity check
  - keyUsage verification
  - Signature verification
  - SAN/CN check with wild card support
- FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the certificate is not accepted.
- FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.

6.4 Security management

The TOE provides two roles: Manager (Security Administrator) and Operator. The manager user is simply the admin and has full control over the device whereas the Operator user may view status information only. Upon successful authentication to the TOE, the Manager role 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. The TOE also offers a web GUI. The web GUI allows administrators a second method for managing the TOE as it provides a full set of capabilities.

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-stamp

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 the cryptographic functions and associated functions, configure the warning banner, manage user accounts, set the time, manage authentication failures, 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. The TOE uses the clock to support the following security functions: timestamps for audit records, timing elements of cryptographic functions, and inactivity timeouts. The TOE also has the ability to sync its time with an NTP server.

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, the TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE can be configured to reboot or to stop with errors displayed when non-critical errors are encountered. The cryptographic library performs self-tests during startup as listed in section 5.1.5.4; the messages are displayed on the console and syslog records generated for both successful and failed tests.

Upgrading the ArubaOS firmware is a manual process performed by an authorized administrator. The firmware is digitally signed with RSA. The TOE uses the public key to verify the digital signature. The firmware is readily available on the HPE website. Uploading the firmware to the devices does require successful authentication to the devices. The downloaded image maybe uploaded to the appliances using a secure method such as secure copy. The firmware performs validation during the download process and will reject the firmware if validation fails. The firmware images are signed by HPE, and the HPE public certificate is stored in the running firmware.

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.
- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM_EXT.1: The TOE includes its own hardware clock and can sync with an NTP server.
- FPT_TST_EXT.1: The TOE performs a suite of self-tests to verify its integrity.
- FPT_TUD_EXT.1: The TOE provides a means for obtaining an installing digitally signed 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 and optionally in seconds). 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, SSH, and web 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 terminates 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 TLS to protect communications between itself and the audit server. Remote administration is performed using SSHv2. The use of TLS and 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 TLS 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 SSHv2and TLS to ensure secure 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.