BROADCOM®

Layer7 API Gateway v10.1.00

Security Target

Version 1.13

June 2024

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	18-Oct-2022	M. Baldock	Version to 1.0
1.1	01-Dec-2022	M. Baldock	Addressing OR01
1.2	02-Feb-2023	M. Baldock	Addressing OR05
1.3	08-May-2023	M. Baldock	Addressing OR06
1.4	14-Jun-2023	M. Baldock	Addressing OR08
1.5	6-Jul-2023	L. Turner	Addressing OR09
1.6	27-Sept-2023	M. Baldock	Addressing OR11
1.7	08-Nov-2023	M. Baldock	Addressing QA comments
1.8	18-Dec-2023	M. Baldock	Addressing OR14
1.9	13-Feb-2024	M. Torabi	Addressing OR15
1.10	25-Mar-2024	M. Baldock	Addressing OR16
1.11	16-Apr-2024	M. Baldock	Update doc version
1.12	23-May-2024	M. Baldock	Addressing OR18
1.13	19-Jun-2024	M. Baldock	Update document title

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Layer7 API Gateway v10.1.00 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The Layer7 API Gateway (TOE) is an XML firewall and service gateway that controls how web services are exposed to and accessed by external client applications.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Layer7 API Gateway v10.1.00 Build: v10.1.00-17078-CR02
Security Target	Layer7 API Gateway v10.1.00 Security Target, v1.13

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) collaborative Protection Profile for Network Devices, v2.2e (NDcPP)

e) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Rationale if n/a
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	
TD0536	NIT Technical Decision for Update Verification Inconsistency	
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	DTLS not claimed
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	

TD #	Name	Rationale if n/a
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	
TD0556	NIT Technical Decision for RFC 5077 question	
TD0563	NiT Technical Decision for Clarification of audit date information	
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	
TD0592	NIT Technical Decision for Local Storage of Audit Records	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	

TD #	Name	Rationale if n/a
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	FCS_TLSC_EXT.2 not claimed
TD0738	NIT Technical Decision for Link to Allowed-With List	
TD0790	NIT Technical Decision: Clarification Required for testing IPv6	FCS_TLSC_EXT.1, FCS_DTLSC_EXT.1 not claimed
TD0792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	
TD0800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	IPsec not claimed

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
NDcPP	collaborative Protection Profile for Network Devices
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
Policy Manager	TLS client used for remote management
Firewall	Network security system that monitors and controls incoming and outgoing network traffic
NTP Server	Network time protocol server for clock synchronization
Syslog Server	Remote server for storing audit logs

2 TOE Description

2.1 Type

4 The Layer7 API Gateway (TOE) is a Case 1 virtual network device.

2.2 Usage

2.2.1 Deployment

5 The TOE (enclosed in red) is a virtual appliance deployed in a network that provides access control to a corporate network. The TOE provides access control to web services that are exposed to and accessed by external client applications.

6 Figure 1 depicts an example deployment of the TOE devices (enclosed in red).

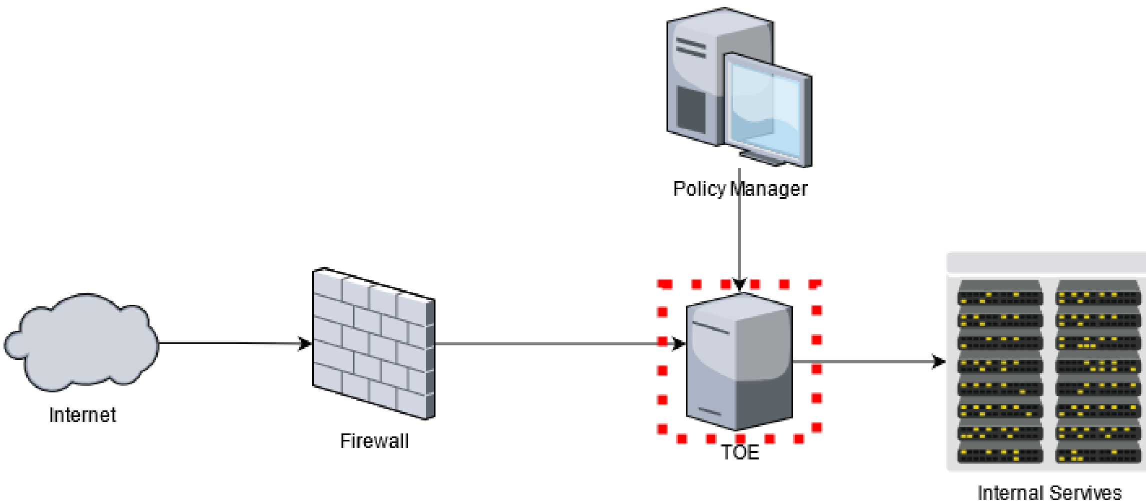

Figure 1: Example TOE deployment

2.2.2 Interfaces

7 The TOE communication channels are shown in Figure 2.

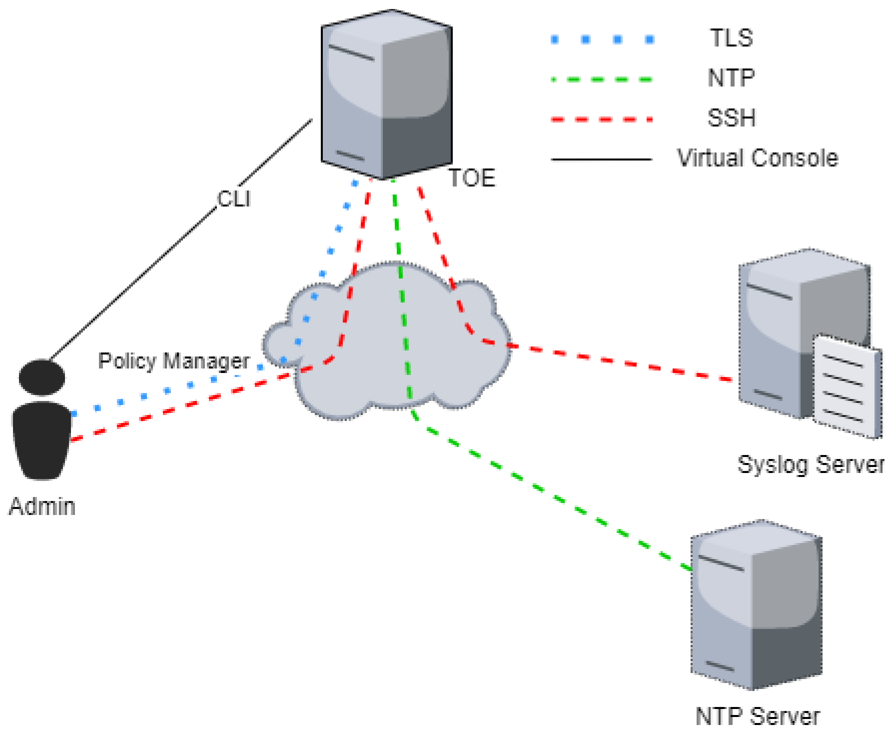

Figure 2: TOE interfaces

8 The TOE interfaces are as follows:

a) **CLI.** Command line management interface via virtual console or remote SSH.

b) **Policy Manager.** Thick client GUI management interface via TLS with the use of a TLS proxy application.

c) **Logs.** Transmission of logs to a syslog server via SSH**.**

d) **NTP.** The TOE synchronizes time via NTP.

2.3 Security Functions / Logical Scope

9 The TOE provides the following security functions:

a) **Protected Management.** The TOE protects the integrity and confidentiality of remote management as noted in section 2.2.2 above.

b) **Protected Communications.** The TOE protects the integrity and confidentiality of remote auditing as noted in section 2.2.2 above.

c) **Secure Administration.** The TOE enables secure management of its security functions, including:

   i) Administrator authentication with public keys and passwords

   ii) Configurable password policies

   iii) Role Based Access Control

   iv) Access banners

   v) Management of critical security functions and data
   vi) Protection of cryptographic keys and passwords

d) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through digital signatures.

e) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

f) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

g) **Cryptographic Operations.** The TOE implements a cryptographic module. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

Algorithm Capability	Certificate
AES-CBC-128 AES-CBC-256	A3606
AES-GCM-128 AES-GCM-256	
KAS-FFC	
AES-CTR-128 AES-CTR-256	A3606 A2926
ECDSA Key Gen (186-4) ECDSA Sig Gen (186-4) ECDSA Sig Ver (186-4)	
RSA Key Gen (186-4) RSA Sig Gen (186-4) RSA Sig Ver (186-4)	
SHA-1, SHA-256, SHA-384, SHA-512	
HMAC-SHA-256, HMAC-SHA-512	
KAS-ECC	
Counter DRBG HMAC DRBG	

2.4 Physical Scope

10 The TOE boundary includes the Gateway 10.1.00.17078-CR02 VMware Centos7 OVA software that runs inside a virtual machine. The TOE is downloaded from the Broadcom portal.

2.4.1 Guidance Documents

11 The TOE includes the following guidance documents (PDF):

a) Layer7 API Gateway v10.1.00v10.1.00-17078-CR02 Common Criteria Guide, v1.10 2024-04-16

b) Layer7 API Gateway 10.1 Last Updated November 4, 2022

12 Users can download the guidance documents from Broadcom's web portal. https://techdocs.broadcom.com/us/en/ca-enterprise-software/layer7-api-management/api-gateway/10-1.html

2.4.2 Non-TOE Components

13 The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE sends audit events to a syslog server.

b) **NTP Server.** The TOE synchronizes time via NTP.

c) **TLS Proxy.** TLS application used with Policy Manager from the remote endpoint.

d) **VMware hypervisors (ESX, ESXi, vSphere).** The TOE operates on VMware ESXi 6.7.

2.4.3 Functions not included in the TOE Evaluation

14 The functions evaluated are limited to those identified at section 2.3. The following functions have not been assessed as part of this evaluation:

a) XML firewall and policy enforcement features.

b) vSphere High Availability feature

c) Identity and Access Management feature

d) Hardware Security Module feature

e) Rest API

3 Security Problem Definition

15 The Security Problem Definition is reproduced from section 4 of the NDcPP.

3.1 Threats

Table 5: Threats

Identifier	Description
T.UNAUTHORIZED_ ADMINISTRATOR_ ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_ CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_ AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_ COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and

Identifier	Description
	the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_ FUNCTIONALITY_ COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_ CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_ FUNCTIONALITY_ FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

Table 6: Assumptions

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.

Identifier	Description
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_AD MINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UP DATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Identifier	Description
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

3.3 Organizational Security Policies

Table 7: Organizational Security Policies

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

4 Security Objectives

16 The security objectives are reproduced from section 5 of the NDcPP.

Table 8: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

Identifier	Description
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_ INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

5 Security Requirements

5.1 Conventions

17 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

18 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

19 The Extended Components are defined in Appendix C of the NDcPP.

Table 9: Extended Components

Requirement	Title	Applicable TDs
FAU_STG_EXT.1	Protected Audit Event Storage	
FCS_NTP_EXT.1	NTP Protocol	TD0528
FCS_RBG_EXT.1	Random Bit Generation	
FCS_SSHC_EXT.1	SSH Client Protocol	TD0636
FCS_SSHS_EXT.1	SSH Server Protocol	TD0631
FCS_TLSC_EXT.1	TLS Client Protocol Without Mutual Authentication	TD0634
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication	TD0635
FIA_PMG_EXT.1	Password Management	
FIA_UIA_EXT.1	User Identification and Authentication	
FIA_UAU_EXT.2	Password-based Authentication Mechanism	
FIA_X509_EXT.1	X.509 Certificate Validation	TD0527
FIA_X509_EXT.2	X.509 Certification Authentication	

Requirement	Title	Applicable TDs
FIA_X509_EXT.3	X.509 Certificate Requests	
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	
FPT_APW_EXT.1	Protection of Administrator Passwords	
FPT_TST_EXT.1	TSF Testing	
FPT_TUD_EXT.1	Trusted Update	
FPT_STM_EXT.1	Reliable Time Stamps	
FTA_SSL_EXT.1	TSF-initiated Session Locking	

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_NTP_EXT.1	NTP Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHC_EXT.1	SSH Client Protocol
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication

Requirement	Title
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on Security Roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

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

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**~~ **Table 11**.*

Table 11: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
FCS_RBG_EXT.1	None.	None.
FCS_SSHC_EXT.1	Failure to establish an SSH Session	Reason for failure
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate. • Any addition, replacement or removal of trust anchors in the TOE's trust store.	• Reason for failure of certificate validation. • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.

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

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**~~ **Table 11**.*

FAU_GEN.2 User Identity Association

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

FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*overwrite oldest record first*], [*no other action*]] when the local storage space for audit data is full.

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

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

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]

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

FCS_CKM.2 Cryptographic Key Establishment

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

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526];

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

FCS_CKM.4 Cryptographic Key Destruction

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

- *For plaintext keys in volatile storage, the destruction shall be executed by a [destruction of reference to the key directly followed by a request for garbage collection];*
- *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 [*
    - *instructs a part of the TSF to destroy the abstraction that represents the key*

] that meets the following: *No Standard*.

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

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC, CTR, 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, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

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

FCS_COP.1.1/SigGen The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256 bits*],

] that meet the following: [

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

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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

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

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

FCS_NTP_EXT.1 NTP Protocol

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

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

- Authentication using [SHA1] as the message digest algorithm(s)]

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

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

FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [HMAC_DRBG(SHA512), 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 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [4344, 5656, 6668, 8268, 8308 section 3.1, 8332].

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

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256 kilo*]bytes in an SSH transport connection are dropped.

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

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

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

FCS_SSHC_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1] and [diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

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

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

FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [4344, 5656, 6668, 8268, 8308 section 3.1, 8332].

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 [*256 kilo*]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-ctr, aes256-ctr].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa,rsa-sha2-256,rsa-sha2-512,ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] 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 [diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

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

FCS_TLSS_EXT.1 TLS Server Protocol

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_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
- 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_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_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_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]

and no other ciphersuites.

FCS_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 perform key establishment for TLS using [RSA with key size [2048 bits], Diffie-Hellman groups [ffdhe2048], ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [no session resumption or session tickets].

5.3.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-20*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

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

FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"];

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

FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

FIA_UAU.7 Protected Authentication Feedback

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

FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

FIA_X509_EXT.2 X.509 Certificate Authentication

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

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

FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.3.4 Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of security functions behaviour

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

FMT_MTD.1/CoreData Management of TSF Data

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

FMT_MTD.1/CryptoKeys Management of TSF data

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

FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to manage the cryptographic keys;
    - Ability to configure the cryptographic functionality;
    - Ability to configure NTP;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;

- Ability to import X.509v3 certificates to the TOE's trust store;

]

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.3.5 Protection of the TSF (FPT)

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

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

FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

FPT_TST_EXT.1 TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on), at the request of the authorised user] to demonstrate the correct operation of the TSF: [

- *Image integrity validation*
- *Cryptographic module tests*].

FPT_TUD_EXT.1 Trusted update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

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

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

FPT_STM_EXT.1 Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall [synchronize time with an NTP server].

5.3.6 TOE Access (FTA)

FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session]

after a Security Administrator-specified time period of inactivity.

FTA_SSL.3 TSF-initiated Termination

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

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 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.

5.3.7 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall **be capable of using [SSH] to provide** a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [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 [*audit server*].

FTP_TRP.1 /Admin Trusted Path

FTP_TRP.1.1/Admin 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.1.2 /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*.

5.4 Assurance Requirements

20 The TOE security assurance requirements are summarized in Table 12

Table 12: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

21 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

a) **ASE_TSS.1.1C Refinement:** The TOE summary specification shall describe how the TOE meets each SFR. **In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.**

6 TOE Summary Specification

22 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1

23 The TOE generates the audit records specified at FAU_GEN.1 containing fields that include the timestamp, IP address (if applicable), action, user (if applicable) and a contextual message indicating success or failure of the action.

24 The following information is logged as a result of the Security Administrator generating/importing or deleting cryptographic keys:

a) **Generate SSH Private Key**. Action and key reference.

b) **Generate TLS Server Private Key**. Action and key reference.

6.1.2 FAU_GEN.2

25 The TOE includes the user identity in audit events resulting from actions of identified users.

6.1.3 FAU_STG_EXT.1

26 Log files are transferred via SSH (see FCS_SSHC_EXT.1) to the external syslog server. Logs are transmitted in real time.

27 Logs are stored locally in rotating log files as follows:

a) **/var/log log files.** Logs are rotated weekly and up to 4 weeks of logs are kept before being removed.

b) **Policy Manager ssg log file.** up to 20MB of log data is kept until they are rotated. A total of 9 previous logs are kept (plus the live log).

28 Logs are overwritten by removing the oldest records first.

29 Only authorized administrators may view audit records and no capability to modify the audit records is provided.

6.2 Cryptographic Support

6.2.1 FCS_CKM.1

30 The TOE supports key generation for the following asymmetric schemes:

a) **RSA Scheme.** Key sizes of 2048 used in SSH and 2048-bit used in TLS communications.

b) **ECC P-256, P-384, P-521.** P-256 is used in SSH authentication and key exchange and P-256, P-384, P-521 used in TLS.

c) **FFC Safe Primes.** Used in SSH key exchange and TLS.

31 The OpenSSL cryptographic module is implemented when generating SSH keys and the CryptoComply cryptographic module is implemented when generating TLS keys.

6.2.2 FCS_CKM.2

32 The TOE supports the following key establishment schemes:

a) **RSA schemes.** Used in SSH and TLS communications.

b) **ECC schemes.** Used in SSH key exchange and TLS. TOE is both sender and receiver.

c) **FFC schemes using safe primes.** Used in SSH key exchange and TLS. TOE is both sender and receiver. The following Diffie Helman groups are supported for SSH:

i) Group 14 per RFC 3526 section 3

ii) Group 16 per RFC 3526 section 5

iii) Group 18 per RFC 3526 section 7

33 The OpenSSL cryptographic module is implemented in SSH communications and the CryptoComply cryptographic module is implemented in TLS communications.

34 Table 13 below identifies the scheme being used by each service.

Table 13: Key Agreement Mapping

Scheme	SFR	Service
RSA Schemes	FCS_TLSS_EXT.1	Administration
ECC	FCS_SSHS_EXT.1	Administration
	FCS_SSHC_EXT.1	Audit Server
	FCS_TLSS_EXT.1	Administration
FFC Safe Primes	FCS_SSHS_EXT.1	Administration
	FCS_SSHC_EXT.1	Audit Server
	FCS_TLSS_EXT.1	Administration

6.2.3 FCS_CKM.4

35 Table 15 shows the origin, storage location and destruction details for cryptographic keys. Unless otherwise stated, the keys are generated by the TOE.

6.2.4 FCS_COP.1/DataEncryption

36 The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in CTR, CBC and GCM mode. AES is implemented in SSH.

37 The relevant NIST CAVP certificate numbers are listed Table 4.

6.2.5 FCS_COP.1/SigGen

38 The TOE provides cryptographic signature generation and verification services using:

a) RSA Signature Algorithm with key size of 2048 bits in SSH and in TLS

b) Elliptic Curve Digital Signature Algorithm with key sizes of 256 in SSH, and 256, 384 and 521 for TLS.

39 The RSA signature verification services are used in the SSH and TLS protocol and TOE firmware integrity checks.

40 The ECDSA signature verification services are used in the SSH and TLS protocol.

41 The relevant NIST CAVP certificate numbers are listed in Table 4.

42 The OpenSSL cryptographic module is implemented in SSH communications and TOE firmware integrity checks.

43 The CryptoComply cryptographic module is implemented in TLS communications.

6.2.6 FCS_COP.1/Hash

44 The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512.

45 SHA is implemented in the following parts of the TSF:

a) SSH;

b) Digital signature verification as part of trusted update validation; and

c) Hashing of passwords in non-volatile storage.

46 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.7 FCS_COP.1/KeyedHash

47 The TOE provides keyed-hashing message authentication services using HMAC-SHA-256, and HMAC-SHA-512.

48 HMAC is implemented in SSH.

49 The characteristics of the HMACs used in the TOE are given in Table 14.

Table 14: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-512	1024 bits	512 bits	512 bits

50 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.8 FCS_NTP_EXT.1

51 The TOE supports NTPv4 using SHA-1 authentication. The TOE allows configuration of up to 3 NTP servers. The TOE uses pre-shared keys for authentication and integrity of the NTP server when synchronizing the time.

6.2.9 FCS_RBG_EXT.1

52 The TOE contains two cryptographic modules. The OpenSSL module implements a CTR_DRBG that is seeded from a software provided entropy source. Entropy from the noise is conditioned and used to seed the DRBG with 384 bits of full entropy. The CryptoComply Java cryptographic module implements an HMAC_DRBG that is seeded from a software provided entropy source. Entropy from the noise is conditioned and used to seed the DRGB with 512 bits of full entropy.

53 Additional detail is provided the proprietary Entropy Description.

6.2.10 FCS_SSHC_EXT.1

54 The TOE implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8268, 8308 section 3.1 and 8332.

55 The TOE supports public key authentication with the following algorithms, rsa-sha2-512, ecdsa-sha2-nistp256 for user public keys.

56 In the case of public keys, the TOE authenticates the identity of the SSH server using a local database associating authorized hosts with its corresponding public key. The TOE supports ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256 host key algorithms to associate server identity when authenticating external SSH servers.

57 The TOE examines the size of each received SSH packet. If the packet is greater than 256 KB, it is automatically dropped.

58 The TOE utilises AES-CTR-128 and AES-CTR-256 for SSH encryption.

59 The TOE provides data integrity for SSH connections via HMAC-SHA2-256 and HMAC-SHA2-512.

60 The TOE supports diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512 and ecdh-sha2-nistp521 for SSH key exchanges.

61 The TOE will re-key SSH connections after 30 minutes or after an aggregate of 512 megabytes of data has been exchanged (whichever occurs first).

6.2.11 FCS_SSHS_EXT.1

62 The TOE implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8268, 8308 section 3.1 and 8332.

63 The TOE supports password-based or public key authentication (rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256). In the case of public keys, the TOE authenticates the identity of the SSH client using a local database associating authorized hosts with its corresponding public key.

64 The TOE supports the following host key algorithms, ssh-rsa, rsa-sha2-256, rsa-sha2-512.

65 The TOE examines the size of each received SSH packet. If the packet is greater than 256 KB, it is automatically dropped.

66 The TOE utilises AES-CTR-128 and AES-CTR-256 for SSH encryption.

67 The TOE provides data integrity for SSH connections via HMAC-SHA2-256 and HMAC-SHA2-512.

68 The TOE supports diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512 and ecdh-sha2-nistp521 for SSH key exchanges.

69 The TOE will re-key SSH connections after 30 minutes or after an aggregate of 512 megabytes of data has been exchanged (whichever occurs first).

6.2.12 FCS_TLSS_EXT.1

70 The TOE accepts TLS 1.2, TLS 1.1 and rejects all other TLS and SSL versions.

71 The TOE restricts TLS to the following ciphersuites:

a) TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
b) TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
c) TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
d) TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
e) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
f) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
g) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
h) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
i) TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
j) TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
k) TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
l) TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
m) TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
n) TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
o) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
p) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
q) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
r) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
s) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
t) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
u) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
v) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
w) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
x) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

72 Ciphersuites are user configurable.

73 The TOE performs key establishment for TLS using RSA with key size of 2048-bit, Diffie-hellman group ffdhe2048, and ECDHE curves secp256r1, secp384r1, secp521r1 and no other curves.

74 The TOE does not support session resumption or session tickets.

6.3 Identification and Authentication

6.3.1 FIA_PMG_EXT.1

75 The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

76 The minimum password length is configurable by the Administrator and can range from 8 to 128 characters.

6.3.2 FIA_UIA_EXT.1

77 The TOE requires all users to be successfully identified and authenticated. The TOE warning banner is displayed prior to authentication.

78 Administrative access to the TOE is facilitated through several interfaces:

a) **CLI.** Administrative CLI via virtual serial connection.

b) **SSH CLI.** Administrative CLI via SSH.

c) **Policy Manager.** Administrative thick client GUI over connected to a TLS Proxy application from the Client machine then connected to the TOE via TLS.

6.3.3 FIA_UAU_EXT.2

79 Regardless of the interface at which the administrator interacts, the TOE prompts the user for a credential. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.

80 The TOE provides a local password-based authentication mechanism and also supports SSH public key authentication.

81 The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative credential associated with the user account (e.g. password or SSH public/private key response). The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

6.3.4 FIA_UAU.7

82 For all authentication at the local CLI the TOE provides no feedback when the administrative password is entered so that the password is obscured.

6.3.5 FIA_AFL.1

83 The TOE is capable of tracking authentication failures of remote administrators.

84 When a user account has sequentially failed authentication the configured number of times the account will be locked for a Security Administrator defined time period.

85 The local console does not implement the lockout mechanism.

6.3.6 FIA_X509_EXT.1/Rev

86 The TOE performs X.509 certificate validation at the following points:

a) TOE TLS client validation of server X.509 certificates;

b) When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates

c) In all scenarios, certificates are checked for several validation characteristics:

d) If the certificate ‘notAfter’ date is in the past, then this is an expired certificate which is considered invalid;

e) The certificate chain must terminate with a trusted CA certificate;

f) Server certificates consumed by the TOE TLS client must have a ‘serverAuthentication’ extendedKeyUsage purpose;

g) The TOE validates a certificate path and treats a certificate as a CA certificate when certificates include the basicConstraints extensions and that the CA flag is set to “TRUE” for all CA certificates.

87 Certificate revocation checking for the above scenarios is performed using CRLs.

88 As X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication, the code-signing and clientAuthentication purpose is not checked in the extendedKeyUsage for related certificates.

89 The TOE ensures that the X.509 certificates adhere to RFC 5280 Section 6.3 (certificate validation and certificate path validation), which can be summarized as follows:

a) The public key algorithm and parameters are checked

b) The current date/time is checked against the validity period revocation status is checked

c) Issuer name of X matches the subject name of X+1

d) Name constraints are checked

e) Policy OIDs are checked

f) Policy constraints are checked; issuers are ensured to have CA signing bits

g) Path length is checked

h) Critical extensions are processed

90 If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted.

6.3.7 FIA_X509_EXT.2

91 The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope. The use of the trust store is restricted to Security Administrators.

92 Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.

93 As part of the verification process, a CRL route is used to determine whether the certificate is revoked or not. If the validity of the certificate cannot be established, the validation will pass.

6.3.8 FIA_X509_EXT.3

94 The TOE generates Certificate Requests that provide public key, Common Name, Organization, Organizational Unit and Country information.

95 The TOE validates the chain of certificates from the Root CA when receiving the CA Certificate Response.

6.4 Security Management

6.4.1 FMT_MOF.1/ManualUpdate

96 The TOE restricts the ability to perform software updates to Security Administrators.

6.4.2 FMT_MTD.1/CoreData

97 Users are required to login before being provided with access to any administrative functions.

6.4.3 FMT_SMR.2

98 The following user accounts are available, which are all Security Administrators:

a) **ssgconfig.** This account is used to access the CLI and SSH CLI.

b) **ssgadmin.** This account is used to access the CLI and SSH CLI

c) **Admin.** This account is used to access the Policy Manager thick client GUI.

99 Management of TSF data is restricted to Security Administrators.

6.4.4 FMT_SMF.1

100 The TOE provides the following management capabilities:

a) Ability to administer the TOE locally (virtual serial) and remotely (SSH and thick client GUI)

b) Ability to configure the access banner via CLI, SSH CLI or thick client GUI

c) Ability to configure the session inactivity time before session termination

  i) The CLI / SSH CLI timeout value is set via the CLI, SSH CLI

  ii) The thick client GUI timeout value is via the thick client GUI

d) Ability to update the TOE and to verify the updates via CLI or SSH CLI

e) Ability to configure the authentication failure parameters via CLI, SSH CLI or thick client GUI

f) Ability to manage the cryptographic keys (generating, importing, modifying, and deleting SSH keys) via CLI or SSH CLI

g) Ability to manage the cryptographic keys (generating, importing, modifying, and deleting X509 keys) via thick client GUI

h) Ability to configure the cryptographic functionality (SSH configuration and X509 configuration) via CLI or SSH CLI

i) Ability to configure the cryptographic functionality (X509 configuration) via thick client GUI

j) Ability to configure NTP via the CLI or SSH CLI

6.4.5 FMT_MTD.1/CryptoKeys

101 The TOE restricts management of cryptographic keys to Security Administrators

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

102 Keys are protected as described in Table 15. In all cases, plaintext keys cannot be viewed through an interface designed specifically for that purpose.

Table 15: Keys

Key	Algorithm	Storage	Zeroization
SSH Private Keys	ECDSA, RSA	Flash - plaintext	Stored in a protected file on the Gateway OS with root access only. The administrator may zeroize this key using the shred command. This causes a three pass overwrite of the file holding the key.
SSH Ephemeral Keys	AES / DH / ECDH	RAM – plaintext	OpenSSL ensures that keys (including re-keyed keys) are overwritten with zeroes when no longer required.
NTP Key	SHA-1	Flash - plaintext	Keys are destroyed when generating new keys by deleting the previous file and creating a new file. Initiated via CLI command by the Security Administrator.
TLS Server Private Keys	ECDSA, RSA	Encrypted PKCS#12	Stored in encrypted PKCS#12 keystore in the Internal DB using AES-256 (CBC).
TLS Server Ephemeral Keys	ECDHE, DHE, RSA	RAM - plaintext	CryptoComply ensures that keys are overwritten with zeroes when no longer required.

6.5.2 FPT_APW_EXT.1

103 Passwords are protected as describe in Table 16. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 16: Passwords

Key/Password	Generation/ Algorithm	Storage
Locally stored administrator passwords	User generated	Flash - SHA-512 hash
Policy Manager administrator passwords	User generated	Stored in encrypted fields in the Internal DB using AES-256 (CBC). TOE logic prevents display of plaintext passwords and PEM keys to users.

6.5.3 FPT_TST_EXT.1

104 At startup, the TOE undergoes the following tests:

a) Image verification and integrity validation.

b) CryptoComply cryptographic self-tests.

c) OpenSSL cryptographic module self-tests

The Administrator can also perform integrity validation tests manually via SSH or local CLI.

105 These tests ensure the correct operation of the cryptographic functionality of the TOE and verify that the correct TOE image is being used. The cryptographic functionality will not be available if the tests fail, and any operation of the TOE supported by this functionality will not be available. When the device completes the boot up operation, this is evidence that the self-tests have passed, and that the TOE, and the cryptographic functions are operating correctly.

6.5.4 FPT_TUD_EXT.1

106 The current firmware version may be queried using the CLI or SSH CLI.

107 The Security Administrator manually initiates TOE updates from the CLI or SSH CLI. TOE update files must first be copied to the TOE and then using the “Patch Management” menu, select “Upload” then “Install” via the appropriate menu options.

108 TOE update files are digitally signed (RSA) and the signature is verified using a hardcoded public key prior to installation of the update. If verification fails, the update is aborted, and an error message is displayed. If the update succeeds, a message indicating the TOE must be rebooted to apply all changes will appear.

6.5.5 FPT_STM_EXT.1

109 The TOE makes use of NTP to maintain date and time.

110 The TOE makes use of time for the following:

a) Audit record timestamps

b) Session timeouts (lockout enforcement)

c) Certificate Expiration Validation.

d) Cryptographic functions.

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

111 The Security Administrator may configure the TOE to terminate an inactive local interactive session following a specified period of time. This is applicable to the local CLI.

6.6.2 FTA_SSL.3

112 The Security Administrator may configure the TOE to terminate an inactive remote interactive session following a specified period of time. This is applicable to the CLI, SSH CLI and thick client GUI.

6.6.3 FTA_SSL.4

113 Administrative users may terminate their own sessions at any time.

6.6.4 FTA_TAB.1

114 The TOE displays an administrator configurable message to users prior to login at the CLI, SSH CLI, and Policy Manager GUI.

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

115 The TOE supports secure communication with the following IT entities:

a) Audit server per FCS_SSHC_EXT.1

6.7.2 FTP_TRP.1/Admin

116 The TOE provides the following trusted paths for remote administration:

a) **SSH.** Administrative CLI via SSH per FCS_SSHS_EXT.1.

b) **Policy Manager.** Administrative Java Client via TLS per FCS_TLSS_EXT.1.

7 Rationale

7.1 Conformance Claim Rationale

117 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is network device, consistent with the NDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the NDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the NDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the NDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

118 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

119 All security requirements are drawn directly from the NDcPP. Table 17 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 17: NDcPP SFR Rationale

Identifier	SFR Rationale
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	• The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData, with optional additional capabilities in FMT_MOF.1/Services and FMT_MOF.1/Functions • The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1 • The requirement for the Administrator authentication process is described in FIA_UAU_EXT.2 • Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions) • The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin • (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY)

Identifier	SFR Rationale
	• (Protection of the Administrator credentials is separately addressed by T.PASSWORD_CRACKING).
T.WEAK_CRYPTOGRAPHY	• Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively • Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash • Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1 • Management of cryptographic functions is specified in FMT_SMF.1
T.UNTRUSTED_COMMUNICATION_CHANNELS	• The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1 • Requirements for the use of secure communication protocols are set for all the allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 • Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
T.WEAK_AUTHENTICATION_ENDPOINTS	• The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1 • Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1 and FTP_TRP.1/Join.
T.UPDATE_COMPROMISE	• Requirements for protection of updates are set in FPT_TUD_EXT.1 • Additional optional use of certificate-based protection of signatures can be specified using FPT_TUD_EXT.2, supported by the X.509 certificate processing requirements in FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3

Identifier	SFR Rationale
	• Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate, with optional requirements for automatic updates in FMT_MOF.1/AutoUpdate
T.UNDETECTED_ACTIVITY	• Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1 • Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1 • Requirements for secure transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1 • Optional additional requirements for dealing with potential loss of locally stored audit records are specified in FAU_STG_EXT.2/LocSpace, and FAU_STG_EXT.3/LocSpace • If (optionally) configuration of the audit functionality is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MOF.1/Functions.
T.SECURITY_FUNCTIONALITY_COMPROMISE	• Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1 • Secure destruction of keys is specified in FCS_CKM.4 • If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys • (Protection of passwords is separately covered under T.PASSWORD_CRACKING)
T.PASSWORD_CRACKING	• Requirements for password lengths and available characters are set in FIA_PMG_EXT.1 • Protection of password entry by providing only obscured feedback is specified in FIA_UAU.7 • Actions on reaching a threshold number of consecutive password failures are specified in FIA_AFL.1 • Requirements for secure storage of passwords are set in FPT_APW_EXT.1.
T.SECURITY_FUNCTIONALITY_FAILURE	• Requirements for running self-test(s) are defined in FPT_TST_EXT.1
P.ACCESS_BANNER	• An advisory notice and consent warning message is required to be displayed by FTA_TAB.1