H3C CR 16000 Series, CR19000 Series, RA Series, SR6600 Series and MSR Series Routers

Security Target Lite

Version: 2.0

Date: 2025-12-02

H3C

Contents

1 Security Target Lite Introduction

The ST describes what is evaluated, including the exact security properties of the TOE in a manner that the potential consumer can rely on.

1.1 Security Target Lite Reference

Title	H3C CR16000 Series, CR 19000 Series, RA Series, SR6600 Series and MSR Series Routers Security Target Lite
Version	V2.0
Date	2025-12-02
Author	New H3C Technologies Co., Ltd

Table 1 Security Target Lite reference

1.2 TOE Reference

TOE Developer	New H3C Technologies Co., Ltd
TOE Name	H3C Series Routers
TOE Version	TOE hardware: H3C CR16000 Series, CR 19000 Series, RA Series, SR6600 Series and MSR Series Routers. TOE firmware: H3C Comware Software, Version 7.1.064, H3C Comware Software, Version 7.1.075, H3C Comware Software, Version 9.1.083

Table 2 TOE reference

1.3 TOE Overview

The Target of Evaluation (TOE) is the H3C Series Routers running Comware. Each series of this family consists of a set of distinct Routers which vary primarily according to power delivery, performance, and port density. Each TOE Device is running the same Comware software with only the modules applicable for the specific hardware installed. These TOE Devices are used to provide a network infrastructure supporting the switching of network traffic between connected networks.

While the Routers have fixed ports, they also support plug-in modules, transceivers, memory, and power supplies that provide additional functionality (e.g., various numbers and types of network connection ports). These plug-in accessories do not serve to change the security characteristics of the TOE and as such can optionally be used in the evaluated configuration.

1.3.1 TOE Type

The TOE is a network device that is connected to the network and has an infrastructure role within the network, it is composed of hardware and firmware that implements supporting network communications, with data forwarding and routing capabilities.

1.3.2 TOE Usage and Major Security Features

Each TOE appliance runs Comware software and has physical network connections to its environment to facilitate the forwarding 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 audit server in the network environment, and this audit server is connected to the TOE through an IPsec tunnel.

The TOE can also be configured to work with a Network Time Server (NTP Server), and the NTP communication is protected through IPsec tunnel.

TOE supports authentication server connection through IPsec tunnel.

SSH clients on PCs can also connect to TOE through encrypted channels.

Figure 1 shows the TOE depicted in its intended environment.

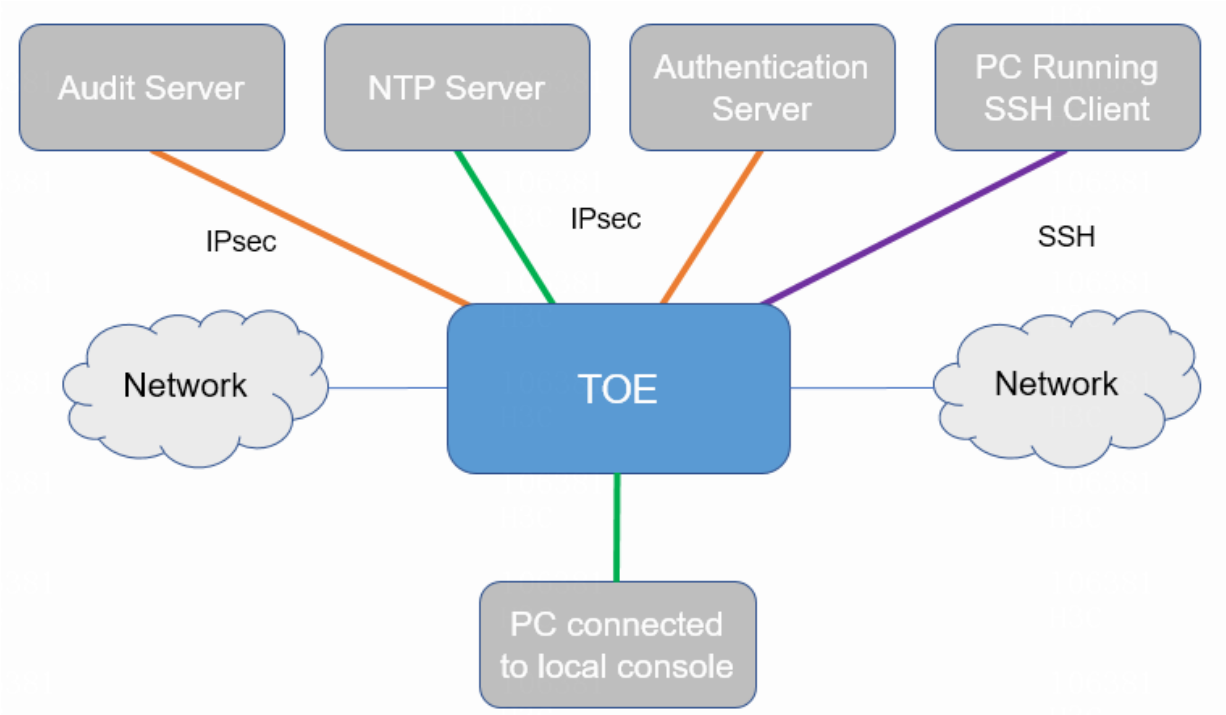


Figure 1 TOE usage scenario.

The hardware of the TOE is a physical network rack-mountable router that supports modules that serve to offer a wide range of network ports varying in number, form factor (copper or fiber), and performance. The software of the TOE executes entirely within the TOE hardware.

The TOE can be configured to rely on and utilize a number of other components in its operational environment:

- Audit server – to receive audit records when the TOE is configured to deliver them to an external server.
- Authentication server – The TOE can be configured to utilize external authentication servers.
- PC connected to local console – The TOE supports CLI access and as such an administrator would need a terminal emulator to utilize those administrative interfaces.
- NTP server – to keep the local hardware-based real-time clock synchronized with other network devices.
- PC running SSH client – SSH remote connection can access TOE.

The TOE provides the following functionality:

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

See section 8 and section 1.4 for details.

Note: TOE must be used in FIPS mode. The cryptographic engines were evaluated and tested in FIPS mode during the CC evaluation.

1.3.3 Non-TOE Hardware/Software/Firmware

Component	Required	Description
Audit Server	Mandatory	This includes any audit server to which the TOE would transmit audit records messages.
PC running SSH Client	Mandatory	This includes any device with an SSH client installed that is used to establish a protected channel with the TOE
PC connected to local console	Mandatory	This includes any PC that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Authentication Server	Mandatory	A server used to verify the identity of users or devices, typically through usernames and passwords, digital certificates, or biometric methods, ensuring that only authorized entities can access system resources. Commonly used AAA servers include FreeRADIUS running on a Linux system.
NTP Server	Mandatory	The Network Time Protocol (NTP) is an application layer protocol in the TCP/IP protocol suite. NTP synchronizes the time among a set of distributed time servers and clients.

Table 3 Components of the environment

Guidance documents

The documentations can be found at website. As can be seen devices are covered with the same documentation. No extra effort is required for this assurance evidence.

CR16006-F/CR16010-F/CR16010H-F/CR16018-F/ CR16005E-F/CR16010E-F/CR16003E-F:

Configuration/Installation Guides:
https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/CR16000-F/CR16000-F/default.htm

CR16000-M8/CR16000-M16/CR16000-M1A:

Configuration/Installation Guides:
https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/CR16000-M/CR16000-M/

CR19000-X8/CR19000-X16:

Configuration/Installation Guides:
https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/CR19000-X/CR19000-X/

RA5300/RA5100-G-HI/RA5100-G:

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/5G_IPRAN/5G_IPRAN/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_RA5300_Router_IG-13904/

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/5G_IPRAN/5G_IPRAN/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_IG-13908/

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/5G_IPRAN/5G_IPRAN/Technical_Documents/Install___Upgrade/Installation_Guides/RA5100[RA5100-G]_IG/

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/5G_IPRAN/5G_IPRAN/Technical_Documents/Configure___Deploy/Configuration_Guides/H3C_CG-13905/00/

SR6604/SR6608

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/SR6600/SR6600/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_SR6604[6608]_IG/

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_SR6600_SR6600-X_CG(V7)-R7821/00/

SR6602-I

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/SR6602-I[IE]/SR6602-I[IE]/Technical_Documents/Install___Upgrade/Installation_Guides/SR6602-I[IE]_AI_IG/?CHID=469127

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/SR6602-I[IE]/SR6602-I[IE]/Technical_Documents/Configure___Deploy/Configuration_Guides/R9119_CG/00/?CHID=780955

SR6608-M

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/SR6600-M/SR6600-M/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_IG-11982/?CHID=1001451

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/SR6600-M/SR6600-M/Technical_Documents/Configure___Deploy/Configuration_Guides/H3C_CG-18453/00/?CHID=1008222

MSR3620-X1/MSR3640-X1/MSR3640-X1-HI

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Install___Upgrade/Installation_Guides/H3C_MSR_3600_IG/

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_MSR610_3600_Routers_V7_R6749-10519/00/

MSR3610-I

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR3600_ICT/MSR3600_ICT/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_MSR3610-I-DP[IE-DP]_IG-13136/

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_MSR610_3600_Routers_V7_R6749-10519/00/?CHID=1017361

MSR2600-15-X1

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR2600/MSR2600/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_MSR_2600_IG/?CHID=713305

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_MSR610_3600_Routers_V7_R6749-10519/00/?CHID=1017358

MSR1004S-5G-GL/MSR1104S-W-CAT6/MSR1104S-W/MSR1104S-W-5GGL

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Public/00-Public/Technical_Documents/Install___Upgrade/Installation_Guides/H3C_MSR1000_IG/?CHID=981770

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_MSR610_3600_Routers_V7_R6749-10519/00/?CHID=1018187

MSR810-LM-EA

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR810/MSR810/

MSR5660-X3

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR5600_V9/MSR5600_V9/

MSR3610E-X1-DP

Installation Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Install___Upgrade/Installation_Guides/H3C_MSR_3600_IG/?CHID=901373

Configuration Guides:

https://www.h3c.com/en/Support/Resource_Center/EN/Home/Routers/00-Public/Configure___Deploy/Configuration_Guides/H3C_MSR1000_3600_Routers_CGs_V9_R9141-25241/00/?CHID=1136234

MSR2630E-X1

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR2600_V9/MSR2600_V9/

MSR1008/ MSR1104-G/ MSR1104-G-DSL-CAT6/ MSR1104-G-LMEA/ MSR1104-G-LMEAS

https://www.h3c.com/en/Support/Resource_Center/EN/Routers/Catalog/MSR1000_V9/MSR1000_V9/

Note: The guidance to configure the TOE as per Common Criteria is provided in the AGD document. The links mentioned above consists of the hardware installation and configuration for all the routers which are non-TOE related as well.

1.4 TOE Description

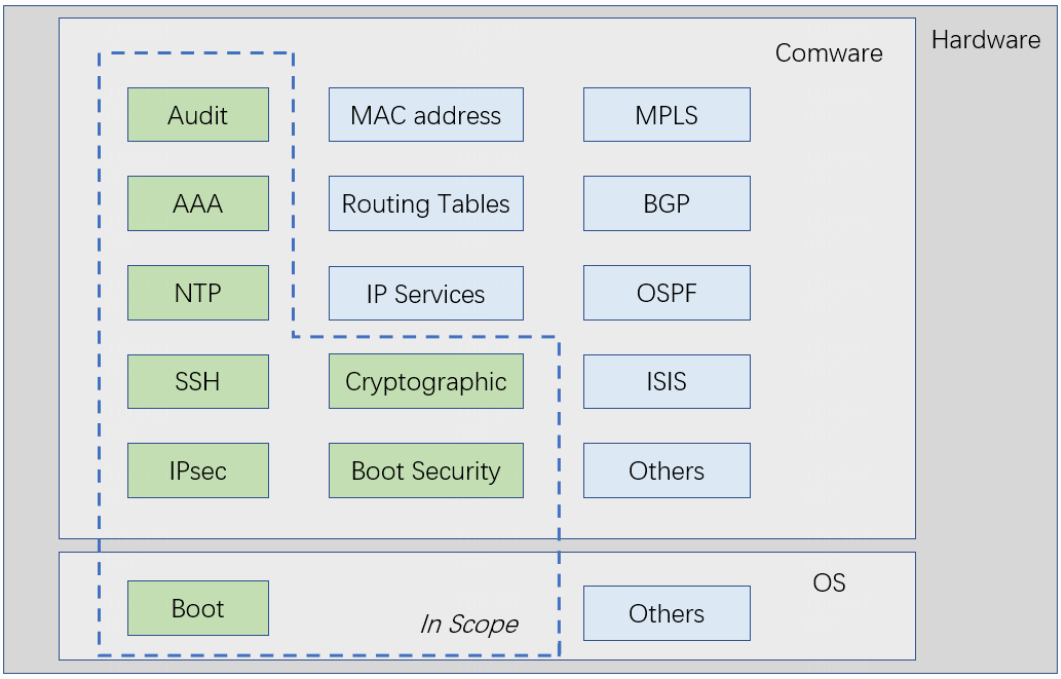
1.4.1 Introduction

This section introduces TOE from an architectural view. The TOE scope consists of a part of the software running in the router device.

The Operating System (OS) is based on a Linux Kernel, which provides basic services including file management, device management, memory management, etc.

The Comware software is a network operating platform, which is responsible for network functions, such as routing information, MAC address management, traffic forwarding and other services.

The figure below shows the composition of the TOE. Among these, AAA does not refer to the authentication server, but rather to an internal module within the TOE, primarily responsible for managing local users on the TOE device and serving as an authentication client to communicate with external authentication servers.



The table below lists all the software functional modules in the router and specifies which of them are in scope or not.

Modules	In Scope	Description
Audit	Yes	The information center on the device receives logs generated by source modules and outputs logs to different destinations according to log output rules (logbuffer, logfiles, etc.)
AAA	Yes	Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management.
BGP	No	Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP). It is called internal BGP (IBGP) when it runs within an AS and called external BGP (EBGP) when it runs between ASs.
Boot Security	Yes	Secure Boot for routers to block unauthorized code execution. typically involves firmware signature verification, bootloader integrity checks, etc.
Cryptographic	Yes	cryptography algorithms: RSA, ECC, ECDSA, SHA, HMAC-SHA, AES, RBG
IPsec	Yes	IP Security (IPsec) is defined by the IETF to provide interoperable, high-

Modules	In Scope	Description
		quality, cryptography-based security for IP communications. It is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways).
IP Services	No	IP Services, such as DNS, DHCP, NAT, etc.
ISIS	No	IS-IS is an IGP used within an AS. It uses the SPF algorithm for route calculation.
MAC address	No	An Ethernet device uses a MAC address table to forward frames. When the device receives a frame, it uses the destination MAC address of the frame to look for a match in the MAC address table.
MPLS	No	Multiprotocol Label Switching (MPLS) provides connection-oriented label switching over connectionless IP backbone networks. It integrates both the flexibility of IP routing and the simplicity of Layer 2 switching.
NTP	Yes	The Network Time Protocol (NTP) is used to synchronize system clocks among distributed time servers and clients on a network. However, in its evaluated configuration works, the TOE only as NTP client uses the NTP Server, located in the operating environment, to get reliable time synchronization.
OSPF	No	Open Shortest Path First (OSPF) is a link-state IGP developed by the OSPF working group of the IETF. OSPF version 2 is used for IPv4.
Routing table	No	IP routing directs IP packet forwarding on routers. Based on the destination IP address in the packet, a router looks up a route for the packet in a routing table and forwards the packet to the next hop. Routes are path information used to direct IP packets.
SSH	Yes	Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.
Others	No	Functionalities which are not within the scope of this evaluation.

1.4.2 Physical Scope

The TOE includes a total of 4 Router series:

Series name	Hardware version	Firmware version
CR Series	CR16006-F	Version 7.1.075
	CR16010-F	Version 7.1.075
	CR16010H-F	Version 7.1.075
	CR16018-F	Version 7.1.075
	CR16000-M8	Version 7.1.075
	CR16000-M16	Version 7.1.075
	CR16005E-F	Version 7.1.075
	CR16010E-F	Version 7.1.075
	CR16003E-F	Version 7.1.075

Series name	Hardware version	Firmware version
	CR16000-M1A	Version 7.1.075
	CR19000-X8	Version 9.1.083
	CR19000-X16	Version 9.1.083
RA Series	RA5300	Version 7.1.075
	RA5100-G-HI	Version 7.1.075
	RA5100-G	Version 7.1.075
SR Series	SR6604	Version 7.1.064
	SR6608	Version 7.1.064
	SR6602-I	Version 9.1.083
	SR6608-M	Version 9.1.083
MSR Series	MSR3620-X1	Version 7.1.064
	MSR3640-X1	Version 7.1.064
	MSR3640-X1-HI	Version 7.1.064
	MSR3610-I	Version 7.1.064
	MSR2600-15-X1	Version 7.1.064
	MSR1004S-5G-GL	Version 7.1.064
	MSR1104S-W-CAT6	Version 7.1.064
	MSR1104S-W	Version 7.1.064
	MSR1104S-W-5GGL	Version 7.1.064
	MSR810-LM-EA	Version 7.1.064
	MSR5660-X3	Version 9.1.083
	MSR3610E-X1	Version 9.1.083
	MSR2630E-X1	Version 9.1.083
	MSR1008	Version 9.1.083
	MSR1104-G	Version 9.1.083
	MSR1104-G-DSL-CAT6	Version 9.1.083
	MSR1104-G-LMEA	Version 9.1.083
	MSR1104-G-LMEAS	Version 9.1.083

Table 4 TOE models in scope

Note that all the models use the same Comware software version but they have difference releases. The changes introduced by using different releases are not security relevant.

TOE Delivery

The delivery of the TOE to the customer is performed by an authorized courier service. The TOE firmware will be pre-installed at factory.

The TOE deliverables include: the network device, the firmware already installed, and accessories included in the delivery list.

User Manual, Installation Guide (including AGD), and other documents can be obtained by logging into the H3C official website: https://www.h3c.com/en/Support/Resource_Center/Technical_Documents/Routers/ .

The certified guidance for this TOE can be found in the link under "H3C Series Routers Preparative and Operative Procedures", with the title "Preparative and Operative Procedures for CC NDPP Evaluated H3C Enterprise CR16000 Series, CR19000 Series, RA Series, SR6600 Series and MSR Series Routers" and version 1.1.

1.4.3 Logical Scope

This section outlines the logical boundaries of the security functionality of the TOE.

1.4.3.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events.

The TOE is configured to store the logs locally so they can be accessed by an administrator and to send the logs to a designated external SYSLOG server to mitigate the possibility of losing audit records when available space becomes exhausted on the TOE.

Locally stored audit records can be reviewed and managed by an administrator.

1.4.3.2 Cryptographic support

The TOE includes a cryptographic module that provides key management and encryption/decryption features in support of higher-level cryptographic protocols to provide a trusted path (e.g., for remote administration).

1.4.3.3 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (e.g., SSH) for interactive administrator sessions.
The TOE supports the local definition of users with usernames and roles that can be authenticated with passwords or Public-Key. The TOE has policies to force the passwords to meet security requirements and can prevent brute-forcing it. The TOE supports roles to control permissions for administrators (i.e., network- admin and security-auditor are authorized administrators). Additionally, TOE can configure IPSEC connected RADIUS servers for authentication services to support e.g., centralized user management.

1.4.3.4 Security management

The TOE provides Command Line (CLI) commands to access the wide range of security management functions. Security management commands are limited to administrators only after they have provided acceptable user identification and authentication data to the TOE.

1.4.3.5 Protection of the TSF

The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity.
The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading.

The TOE performs self-tests on its power on to ensure its correct behaviour.
The TOE verifies the packet before their installation and uses the digital signature.

1.4.3.6 TOE access

The TOE can be configured to display advisory banners when user's login and will enforce an administrator- defined inactivity timeout value after which an inactive session will be terminated, allowing also the capability of self-terminate its session for the administrator.

1.4.3.7 Trusted path/channels

The TOE protects communication with an associated Audit server using IPSEC primarily to protect exported audit records.
The TOE uses IPSEC to protect communications with the associated AAA server, primarily for authentication of accessing users.
The TOE also provides the capability of remote administration via SSH.

1.5 Evaluated Configuration

The Audit Server, NTP Server, and Authentication Server are connected to the TOE via Ethernet links, either directly through Ethernet cables connected to the TOE's Ethernet interface or through a switch. The servers are configured with log server software, NTP server, and authentication services respectively. The Servers configure IP parameters for the Ethernet link to ensure routable connectivity with the TOE, and use this IP address to establish an IPsec tunnel with the TOE for protected communication.
PC connected to local console, uses a console cable to connect to the TOE. Plug the DB-9 (female) connector of the console cable into the 9-pin (male) serial port of the PC, and the RJ-45 connector into the device's console port. Use a hyper terminal or terminal emulation program (such as Putty, SecureCRT, etc.) on the PC to establish connection with the device. Set the correct terminal parameters to establish connection with the TOE, and use the CLI command provided by the TOE to complete configuration or view device status, etc.
The PC configures the IP parameters of the Ethernet link to achieve routable connectivity with the TOE, and uses either the built-in or separately installed SSH client software, setting parameters matching the services configured on the TOE, to establish an SSH connection and interact through the SSH channel for information exchange and file transfer.
After power-on, the TOE operates in non-FIPS mode by default. Use the *fips mode enable* command before proceeding with secure operations.

2 Conformance claims

2.1 CC Conformance Claim

The TOE and ST claim conformance to the CC:2022 Release 1.

This ST is [CC2022R1P2] extended and [CC2022R1P3] conformant.

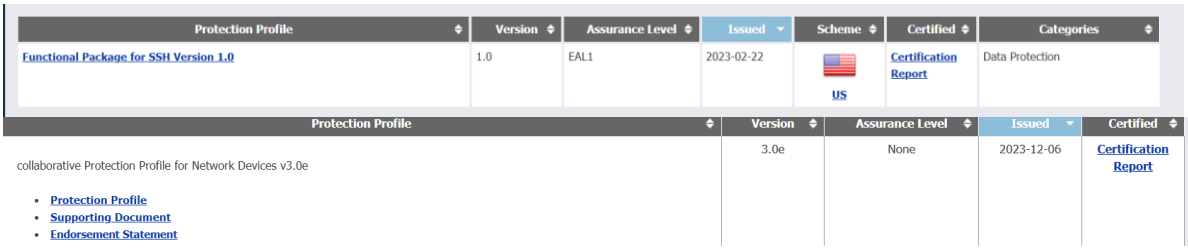
The Security Objectives for the Operational Environment, refer to section 4.2, are copied from [PP-ND].

This Security Target claims conformance to EAL2 augmented with ALC_FLR.2.

The TOE is heavily inspired by:

- Collaborative Protection Profile for Network Devices v3.0e, 06-12-2023 [PP-ND].
- Functional Package for Secure Shell (SSH) v1.0, 2021-05-13 [PPSSH].
- Evaluation Activities for Network Device cPP, Version: 3.0e, Date: 06-December-2023 [SD_ND]

Note: [PP-ND] and [PPSSH] are certified by CCRA.



Protection Profile	Version	Assurance Level	Issued	Scheme	Certified	Categories
Functional Package for SSH Version 1.0	1.0	EAL1	2023-02-22	US	Certification Report	Data Protection

Protection Profile	Version	Assurance Level	Issued	Certified
collaborative Protection Profile for Network Devices v3.0e • Protection Profile • Supporting Document • Endorsement Statement	3.0e	None	2023-12-06	Certification Report

2.2 Conformance Rationale

According to [CCTransitionPolicy], as [PP-ND] is based on CC v3.1 and this ST is based on CC:2022, extended components should be replaced by components in CC:2022 Part 2 or Part 3 if possible. The table as below presents the mapping between extended SFRs from [PP-ND] are replaced by SFRs from [CC2022R1P2], which are included in this ST.

Extended SFRs from [PP-ND]	**SFRs from [CC2022R1P2]**	**Rationale**
FCS_RBG_EXT.1	FCS_RBG.1 FCS_RBG.3 FCS_RBG.6	Requirements from FCS_RBG.1, FCS_RBG.3 and FCS_RBG.6 could fully replace all requirements from FCS_RBG_EXT.1.
FPT_STM_EXT.1	FPT_STM.1 FPT_STM.2	Requirements from FPT_STM.1 and FPT_STM.2 could fully replace all requirements from FPT_STM_EXT.1.
FCS_CKM.4	FCS_CKM.3 FCS_CKM.6	Requirements from FCS_CKM.3 and FCS_CKM.6 could fully replace all requirements from FCS_CKM.4.

3 SECURITY PROBLEM DEFINITION

The Security Problem Definition is taken from the Security Problem Definition (composed of organizational policies, threat statements, and assumption) described in the Network Devices PP [PP-ND].

This section describes the following security environment in which the TOE is intended to be used.

- Significant assumptions about the TOE's operational environment
- IT related threats to the organization countered by the TOE
- Environmental threats requiring controls to provide sufficient protection
- Organizational security policies for the TOE as appropriate

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name.

3.1 Threats

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

3.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

3.1.2 T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

3.1.3 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.

3.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

3.1.5 T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

3.1.6 *T.UNDETECTED_ACTIVITY*

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

3.1.7 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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.

3.1.8 T.SECURITY_FUNCTIONALITY_FAILURE

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

3.2 Assumptions

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

Note: The definitions and descriptions of a virtual TOE or a distributed TOE have been removed, because the TOE defined in this ST is neither a virtual TOE nor a distributed TOE:

- Part of A.PHYSICAL_PROTECTION
- Part of A.LIMITED_FUNCTIONALITY
- A.COMPONENTS_RUNNING (applies to distributed TOEs only)
- A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)
- A.VS_REGULAR_UPDATES (applies to vNDs only)
- A.VS_ISOLATION (applies to vNDs only)
- A.VS_CORRECT_CONFIGURATION (applies to vNDs only)

3.2.1 A.PHYSICAL_PROTECTION

The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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.

3.2.2 A.LIMITED_FUNCTIONALITY

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

3.2.3 A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ST. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

3.2.4 A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes 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).

3.2.5 A.REGULAR_UPDATES

The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

3.2.6 A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

3.2.7 A.RESIDUAL_INFORMATION

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

3.3 Organizational Security Policies

3.3.1 P.ACCESS_BANNER

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

4 SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

Security Objectives for the TOE are added to comply with ASE_OBJ.2 for EAL2.

4.1.1 O.ADMIN_AUTH

The TOE shall require identification and authentication of administrators before granting them access to the TOE management functions. The TOE management capabilities available to administrators shall be defined and limited, and actions available prior to authentication shall be limited and constrained. Administrators' authentication process shall consist in local authentication on the TOE using passwords through a secure communication channel, and authentication sessions will be closed by the TOE after a defined period of inactivity.

4.1.2 O.STRONG_CRYPTO

The TOE shall use robust cryptographic algorithms, compliant to industry approved standards, in order to provide robust cryptographic protection of network communications.

4.1.3 O.TRUSTED_COMM

The TOE shall implement secure channels that use standardized tunnelling protocols to protect the critical network traffic, ensuring protection of the communications between the TOE and trusted external entities in confidentiality, integrity, and protection against communication replays.

4.1.4 O.STRONG_AUTHENTICATION_ENDPOINT

The TOE shall implement methods for robust and reliable authentication of trusted entities with the TOE, preventing attacks based on weak authentication methods (e.g. guessing or transported shared keys).

4.1.5 O.SECURE_UPDATES

The TOE shall provide to administrators the capability of installing software or firmware updates only after a successful verification of their authenticity using sec ure and strong cryptographic algorithms based on digital signatures.

4.1.6 O.ACTIVITY_AUDIT

The TOE shall generate audit records for relevant management actions carried by administrators. Audit records will be marked with precise timestamps, associated to user identity, and protected from unauthorized modification or deletion.

4.1.7 O.PASSWORD_PROTECTION

The TOE shall protect the passwords user for local administrator authentication by enforcing complexity and quality rules. Also, the TOE shall limit failed authentication attempts and limit the feedback given to users on failed authentications, in order to prevent brute force or guessing attacks. Also, the TOE shall perform secure storage of passwords, refraining from storing them in plaintext.

4.1.8 O.SELF_TEST

The TOE shall perform self-tests of the TSF functionality in order to detect potential failures during start-up or operation and prevent further situations that could lead to malfunction.

4.1.9 O.BANNER

The TOE shall display an advisory notice and consent about use of the TOE to administrators before establishing an administrative user session.

4.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment are taken from the Security Objectives for the Operational Environment described in Section 5.1 of the Network Devices PP [PP-ND].

4.2.1 OE.PHYSICAL

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

4.2.2 OE.NO_GENERAL_PURPOSE

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

4.2.3 OE.NO_THRU_TRAFFIC_PROTECTION

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

4.2.4 OE.TRUSTED_ADMIN

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

4.2.5 OE.UPDATES

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

4.2.6 OE.ADMIN_CREDENTIALS_SECURE

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

4.2.7 OE.RESIDUAL_INFORMATION

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

4.3 Tracing SPDs to Security Objectives

The following section provides a tracing between SPDs and Security Objectives.

Threats	Security Objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	O.ADMIN_AUTH
T.WEAK_CRYPTOGRAPHY	O.STRONG_CRYPTO

T.UNTRUSTED_COMMUNICATION_CHANNELS	O.TRUSTED_COMM
T.WEAK_AUTHENTICATION_ENDPOINTS	O.STRONG_AUTHENTICATION_ENDPOINT
T.UPDATE_COMPROMISE	O.SECURE_UPDATES
T.UNDETECTED_ACTIVITY	O.ACTIVITY_AUDIT
T.SECURITY_FUNCTIONALITY_COMPROMISE	O.PASSWORD_PROTECTION
T.SECURITY_FUNCTIONALITY_FAILURE	O.SELF_TEST

Assumptions	Security Objectives for the Operational Environment
A.PHYSICAL_PROTECTION	OE.PHYSICAL
A.LIMITED_FUNCTIONALITY	OE.NO_GENERAL_PURPOSE
A.NO_THRU_TRAFFIC_PROTECTION	OE.NO_THRU_TRAFFIC_PROTECTION
A.TRUSTED_ADMINISTRATOR	OE.TRUSTED_ADMIN
A.REGULAR_UPDATES	OE.UPDATES
A.ADMIN_CREDENTIALS_SECURE	OE.ADMIN_CREDENTIALS_SECURE
A.RESIDUAL_INFORMATION	OE.RESIDUAL_INFORMATION

OSPs	Security Objectives
P.ACCESS_BANNER	O.BANNER

4.4 Security Objectives Rationale

4.4.1 Threats

4.4.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

This threat is countered by O.ADMIN_AUTH which requires identification and authentication of administrator before granting them access to the TOE and to management functions. It also enforces that the TOE requires identification and authentication of administrators before granting them access to the TOE management functions.
The TOE management capabilities available to administrators shall be defined and limited, and actions available prior to authentication shall be limited and constrained.
Administrators' authentication process shall consist in local authentication of the TOE using passwords through a secure communication channel, and authentication sessions will be closed by the TOE after a defined period of inactivity.

4.4.1.2 T.WEAK_CRYPTOGRAPHY

This threat is countered by O.STRONG_CRYPTO which requires usage of robust cryptographic algorithms, compliant to industry approved standards, in order to provide robust cryptographic protection of network communications.

4.4.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

This threat is countered by O.TRUSTED_COMM which requires secure communication channels that use standardized
tunnelling protocols to protect the critical network traffic, ensuring protection of the communications between the TOE and trusted external entities in confidentiality, integrity, and protection against communication replays.

4.4.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

This threat is countered by O.STRONG_AUTHENTICATION_ENDPOINT which requires methods for strong authentication of trusted entities with the TOE, preventing attacks based on weak authentication methods.

4.4.1.5 T.UPDATE_COMPROMISE

This threat is countered by O.SECURE_UPDATES which requires verification of updates authenticity by administrators based on cryptographic digital signatures..

4.4.1.6 T.UNDETECTED_ACTIVITY

O.ACTIVITY_AUDIT counters T.UNDETECTED_ACTIVITY by generating audit records for relevant management actions to prevent undetected activity.

4.4.1.7 T.SECURITY_FUNCTIONALITY_COMPROMISE

This threat is countered by O.PASSWORD_PROTECTION which requires the TOE to enforce password complexity and quality in passwords used by administrators for authentication, hence preventing successful attacks to weak passwords. The same objective also forbids plaintext storage of passwords in the TOE and prevents attacks based on massive authentication attempts or guessing passwords from feedback resulting from failed authentication attempts.

4.4.1.8 T.SECURITY_FUNCTIONALITY_FAILURE

This threat is countered by O.SELF_TEST which requires that The TOE carries outs TSF self-tests in order to detect potential failures during start-up or operation and prevent further situations that could lead to malfunction.

4.4.2 Assumptions

4.4.2.1 A.PHY SICAL_PROTECTION

This assumption is directly upheld by OE.PHYSICAL, which requires that physical protection to the TOE is provided by the operational environment.

4.4.2.2 A.LIMITED_FUNCTIONALITY

A.LIMITED_FUNCTIONALITY is upheld by OE.NO_GENERAL_PURPOSE.

4.4.2.3 A.NO_THRU_TRAFFIC_PROTECTION

This assumption is directly upheld by OE.NO_THRU_TRAFFIC_PROTECTION, which requires that the TOE does not provide any protection of traffic that traverses it, but such protection is covered by other security and assurance measures in the operational environment.

4.4.2.4 A.TRUSTED_ADMINISTRATOR

This assumption is directly upheld by OE.TRUSTED_ADMIN, which requires that TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.

4.4.2.5 A.REGULAR_UPDATES

This assumption is directly upheld by OE.UPDATES, which requires that 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.

4.4.2.6 A.ADMIN_CREDENTIALS_SECURE

This assumption is directly upheld by OE.ADMIN_CREDENTIALS_SECURE, which requires that the administrator's credentials (private key) used to access the TOE are protected on any other platform on which they reside.

4.4.2.7 A.RESIDUAL_INFORMATION

This assumption is directly upheld by OE.RESIDUAL_INFORMATION which requires administrators to ensure that there is no unauthorized access possible for sensitive residual information on networking equipment when the equipment is discarded or removed from its operational environment.

4.4.3 OSP

4.4.3.1 P.ACCESS_BANNER

This policy is enforced by O.BANNER which requires that the TOE displays an advisory notice and consent about use of the TOE to administrators before establishing an administrative user session.

5 Extended Component Definition

Extended Component Definition has been taken with no modification from the Network Devices PP [PP-ND].
Extended Component Definition has been taken from the Network Devices PP [PP-ND] with the modifications provided by the Functional package [PPSSH] .
There are no extended Security Assurance Requirements (SAR) for the TOE.

Extended SFRs:
PP-ND: FAU_STG_EXT.1: Protected Audit Event Storage
PP-ND: FIA_UIA_EXT.1: User Identification and Authentication
PP-ND: FIA_PMG_EXT.1: Password Management
PP-ND: FIA_X509_EXT.1/Rev: X.509 Certificate Validation
PP-ND: FIA_X509_EXT.2: X.509 Certificate Authentication
PP-ND: FIA_X509_EXT.3: X.509 Certificate Requests
PP-ND: FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
PP-ND: FPT_TUD_EXT.1: Trusted Update
PP-ND: FTA_SSL_EXT.1: TSF-initiated Session Locking
PP-ND: FCS_IPSEC_EXT.1: IPsec Protocol
PP-ND: FCS_NTP_EXT.1: NTP Protocol
PPSSH: FCS_SSH_EXT.1: SSH Protocol
PPSSH: FCS_SSHS_EXT.1: SSH Server Protocol

6 Security Functional Requirements

Operations done by the PP [PP-ND] are identified using the following typographical distinctions:

- Unaltered SFRs are stated in the form used in [CC2022R1P2] or their extended component definition (ECD);
- Refinement made in the PP or ST: the refinement text is indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP or ST: the selection values are indicated with underlined text

  e.g. '[selection: *disclosure, modification, loss of use*]' in [CC2022R1P2] or an ECD might become 'disclosure' (completion) or '[selection: disclosure, modification]' (partial completion) in the ST;
- Assignment wholly or partially completed in the PP or ST: indicated with *italicized text*;
- Assignment completed within a selection in the PP or ST: the completed assignment text is indicated with *italicized and underlined text*

  e.g. '[selection: *change_default, query, modify, delete, [assignment: other operations]*]' in [CC2] or an ECD might become 'change_default, select_tag' (completion of both selection and assignment) or '[selection: *change_default*, *select_tag*, *select_value*]' (partial completion of selection, and completion of assignment) in the ST;
- Iteration: indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash').

Extended SFRs are identified by having a label 'EXT' at the end of the SFR name.

All the application notes defined in the PP [PP-ND] have been considered when writing this document. Please refer to the PP [PP-ND] for specific details.

6.1 Security Audit (FAU)

6.1.1 Security Audit Data generation (FAU_GEN)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) All administrative actions comprising:

- *Administrative login and logout (name of Administrator account shall be logged if individual 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).*
- [selection: no other actions]*;*

d) Specifically defined auditable events listed in Table 5.

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 (~~if applicable~~), 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 5.

Requirement	**Auditable Events**	**Additional Audit Record Contents**
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.6	minimal: Success and failure of the activity;	basic: The object attribute(s), and object value(s) excluding any sensitive information.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG.1	minimal: Failure of the randomization process, failure to initialize or reseed (as supported by the technology).	None.
FCS_RBG.3 FCS_RBG.6	there are no auditable events foreseen.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_PMG_EXT.1	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_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.1	minimal: Changes to the time;	detailed: Providing a timestamp.
FPT_STM.2	minimal: Discontinuous changes to the time;	detailed: Changes to the time source.
FPT_FLS.1	basic: Failure of the TSF.	None.
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session lock	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.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel	• None • None

Requirement	Auditable Events	Additional Audit Record Contents
	functions.	• Reason for failure
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	• None • None • Reason for failure
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_SSHS_EXT.1	No events specified	
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
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.

Table 5 Security Functional Requirements and Auditable Events

6.1.1.2 FAU_GEN.2 User identity association

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

6.1.2 Security audit event storage (Extended – FAU_STG_EXT)

6.1.2.1 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 [selection:
the TOE shall consist of a single standalone component that stores audit data locally]

FAU_STG_EXT.1.3 The TSF shall maintain a [selection: log file, buffer] of audit records in

the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [selection: persistent] audit records locally with a minimum storage size of [assignment: *1 Megabyte (MB)*.]

FAU_STG_EXT.1.5 The TSF shall [selection: overwrite previous audit records according to the following rule: *oldest audit record is overwritten, no other action*] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [selection: manual export, ability to view locally].

6.2 Cryptographic Support (FCS)

6.2.1 Cryptographic Key Management (FCS_CKM)

6.2.1.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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

- RSA schemes using cryptographic key sizes of *3072 bits or greater* that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using 'NIST curves' [selection: 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 [selection: RFC 3526].

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

6.2.1.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2";
- 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 [selection: groups listed in RFC 3526].

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

6.2.1.3 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment: *private key*] in accordance with a specified cryptographic key access method [assignment: *Export the certificate and private key to a PKCS12 file*] that meets the following: [assignment: *PKCS#12*].

6.2.1.4 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy [assignment: *private key, keys and keying material of IPsec, keys and keying material of SSH*] when [selection: no longer needed, *administrator manually destroys*].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *single overwrite consisting of zeros*] that meets the following: [assignment: *NIST. 800-57 Part 1 Revision 5*].

6.2.2 Cryptographic Operation (FCS_COP)

6.2.2.1 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* [selection: GCM] *mode* and cryptographic key sizes [selection: 128 bits, 192 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3*, [selection: GCM as specified in ISO 19772].

6.2.2.2 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 [selection:

- RSA Digital Signature Algorithm,

]

and cryptographic key sizes [selection:

- For RSA: modulus 3072 bits or greater,]

that meet the following: [selection:

- 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,

].

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

6.2.2.4 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 [selection: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, implicit] and cryptographic key sizes [*assignment: 256, 384, 512*] **and message digest sizes [selection: 256, 384, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

6.2.3 Random Bit Generation (FCS_RBG)

6.2.3.1 FCS_RBG.1 Random Bit Generation

FCS_RBG.1.1	The TSF shall perform deterministic random bit generation services using [assignment: *CTR_DRBG (AES*)] in accordance with [assignment: *ISO/IEC 18031:2011*] after initialization with a seed.
FCS_RBG.1.2	The TSF shall use a [selection: TSF noise source *software-based noise source*] for initialized seeding.
FCS_RBG.1.3	The TSF shall update the RBG state by [selection: uninstantiating and reinstantiating] using a [selection: TSF noise source *software-based noise source*] in the following situations: [selection: on the condition: *new key generation*] in accordance with [assignment: *ISO/IEC 18031:2011*].

6.2.3.2 FCS_RBG.3 Random bit generation (internal seeding – single source)

FCS_RBG.3.1	The TSF shall be able to seed the RBG using a [selection: TSF software-based noise source][assignment: *software-based noise source*] with a minimum of [assignment: *256*] bits of min-entropy.

6.2.3.3 FCS_RBG.6 Random bit generation service

FCS_RBG.6.1	The TSF shall provide a [selection: software] interface to make the RBG output, as specified in FCS_RBG.1 Random bit generation (RBG), available as a service to entities outside of the TOE.

6.3 Identification and Authentication (FIA)

6.3.1 User Identification and Authentication (Extended – FIA_UIA_EXT)

6.3.1.1 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; • [selection: 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_UIA_EXT.1.3	The TSF shall provide the following remote authentication mechanisms [selection: SSH password, SSH public key] and local authentication mechanisms [selection: password-based]
FIA_UIA_EXT.1.4	The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

6.3.2 Authentication Failure Handling (Extended - FIA_AFL)

6.3.2.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1	The TSF shall detect when an administrator configurable positive integer within [assignment: *2-10*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met, the TSF shall [selection: prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until *unlock* is taken by an Administrator].

6.3.3 User authentication (FIA_UAU) (Extended – FIA_UAU)

6.3.3.1 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [assignment: *obscured feedback*] to the user while the authentication is in progress.

6.3.4 Password Management (Extended – FIA_PMG_EXT)

6.3.4.1 FIA_PMG_EXT.1 Password Management (Refinement)

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: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "'", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "[", "\", "]", " ", "`", "{", "}", and "~"];

b) Minimum password length shall be *configurable to between* [*assignment: 15*] *and [assignment: 63] characters*.

c) New passwords must contain a minimum of 4 characters' changes from the previous password;

6.4 Security Management (FMT)

6.4.1 Management of functions in TSF (FMT_MOF)

6.4.1.1 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*.

6.4.2 Management of TSF Data (FMT_MTD)

6.4.2.1 FMT_MTD.1/CoreData Management of TSF Data

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

6.4.3 Specification of Management Functions (FMT_SMF)

6.4.3.1 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 remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination;*

- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [selection:
  - Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
  - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
  - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
  - Ability to manage the cryptographic keys;
  - Ability to configure the cryptographic functionality;
  - Ability to configure thresholds for SSH rekeying;
  - Ability to configure the lifetime for IPsec SAs;
  - Ability to re-enable an Administrator account;
  - Ability to set the time which is used for time-stamps;
  - Ability to configure NTP;
  - Ability to configure the reference identifier for the peer;
  - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
  - Ability to generate Certificate Signing Request (CSR) and process CA certificate response;
  - Ability to administer the TOE locally;
  - Ability to configure the local session inactivity time before session termination or locking;
  - Ability to configure the authentication failure parameters for FIA_AFL.1;
  - No other capabilities]

6.4.4 Security management roles (FMT_SMR)

6.4.4.1 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:
- *Security Administrator*
- *Network-admin*
- *Network-operator*
- *Level-0 to level-15*
- *Security-audit*
- *Guest-manager*

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 remotely [and also by the local console].*
- *The TOE controls user access to commands and resources based on user role.*
- *Users are given permission to access a set of commands and resources based on their user role.*

are satisfied.

6.5 Protection of the TSF (FPT)

6.5.1 Protection of TSF Data (Extended – FPT_SKP_EXT)

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

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

6.5.2 TSF Testing (Extended – FPT_TST_EXT)

6.5.2.1 FPT_TST_EXT.1 TSF Testing (Extended)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [selection:

During initial start-up (on power on) to verify the integrity of the TOE firmware and software].

to demonstrate the correct operation of the TSF: [assignment: *integrity of the firmware and software (software digital signature), the correct operation of cryptographic functions*] and if failure detected [assignment: *fail to start and logs are recorded*].

FPT_TST_EXT.1.2 The TSF shall respond to [selection: all failures] by [selection: *rejecting the loading of wrong software*].

6.5.3 Trusted Update (FPT_TUD_EXT)

6.5.3.1 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 [selection: 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 [selection: no other update mechanism]

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

6.5.4 Time stamps (Extended – FPT_STM))

6.5.4.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.5.4.2 FPT_STM.2 Time source

FPT_STM.2.1 The TSF shall allow the [assignment*: Security Administrator*] to [assignment: *to set the time and/or synchronise time with an NTP server*].

6.5.5 Fail secure (FPT_FLS)

6.5.5.1 FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:[*failure of the self-tests*].

6.6 TOE Access (FTA)

6.6.1 TSF-initiated Session Locking (Extended – FTA_SSL_EXT)

6.6.1.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection: terminate the session*]* after a Security Administrator-specified time period of inactivity.

6.6.2 Session Locking and Termination (FTA_SSL)

6.6.2.1 FTA_SSL.3 TSF-initiated Termination (Refinement)

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

6.6.2.2 FTA_SSL.4 User-initiated Termination (Refinement)

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

6.6.3 TOE Access Banners (FTA_TAB)

6.6.3.1 FTA_TAB.1 Default TOE Access Banners (Refinement)

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

6.7 Trusted Path/Channels (FTP)

6.7.1 Trusted Channel (FTP_ITC)

6.7.1.1 FTP_ITC.1 Inter-TSF Trusted Channel (Refinement)

FTP_ITC.1.1	The TSF shall **be capable of using [selection: IPsec] to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [selection: authentication server, *NTP server*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure **and detection of modification of the channel data**.
FTP_ITC.1.2	The TSF shall permit [selection: the TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [assignment: *audit service, authentication service*].

6.7.2 Trusted Path (FTP_TRP)

6.7.2.1 FTP_TRP.1/Admin Trusted Path (Refinement)

FTP_TRP.1.1/Admin	The TSF shall **be capable of using [selection: SSH] to** provide a communication path between itself and **authorized** remote **Administrators** ~~users~~ 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** ~~users~~ to initiate communication via the trusted path.
FTP_TRP.1.3/Admin	The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

6.8 Selection-Based Requirements

6.8.1 Cryptographic Support (FCS)

6.8.1.1 FCS_IPSEC_EXT.1 IPsec Protocol

FCS_IPSEC_EXT.1.1	The TSF shall implement the IPsec architecture as specified in RFC 4301.
FCS_IPSEC_EXT.1.2	The TSF shall have a nominal, final entry in the SPD that matches

anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: AES-GCM-128 (RFC 4106), AES-GCM-192 (RFC 4106), AES-GCM-256 (RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [selection: no HMAC algorithm].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection:

- IKEv2 as defined in RFC 7296 and [selection: with mandatory support for NAT traversal as specified in RFC 7296, section 2.23)], and [selection: RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv2] protocol uses the cryptographic algorithms [selection: AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282)]

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection:
  - length of time, where the time values can be configured within *1-24* hours]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [selection:
  - number of bytes;
  - length of time, where the time values can be configured within *1-8* hours;]

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG.1, and having a length of at least [assignment: *256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20)*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [selection: IKEv2] exchanges of length [selection: at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection:

- [selection: 19 (256-bit Random ECP), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)] according to RFC 5114.

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv2 IKE SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv2 CHILD SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [selection: RSA, ECDSA] that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), CN: IP address, CN: Fully Qualified Domain Name (FQDN), Distinguished Name (DN)] and [selection: no other reference identifier type].

6.8.1.2 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [selection: NTP v3 (RFC 1305), NTP v4 (RFC 5905)].

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

- Authentication using [selection: SHA256, SHA384, SHA512] as the message digest algorithm(s);
- [selection: IPsec] to provide trusted communication between itself and an NTP time source.

].

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 in the Operational Environment.

6.8.1.3 FCS_SSH_EXT.1 SSH Protocol

This package requires the use of evaluation methods/ evaluation activities defined in [PPSSH]

FCS_SSH_EXT.1.1 The TOE shall implement *SSH* acting as [selection: server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254,

[selection: 4256, 4344, 5647, 5656, 6187, 6668] and [*no other standard*].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [selection:

- "password" (RFC 4252),
- "publickey" (RFC 4252): [selection:
  - ecdsa-sha2-nistp256 (RFC 5656),
  - ecdsa-sha2-nistp384 (RFC 5656)
  ]

] and no other methods.

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

FCS_SSH_EXT.1.4 The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [selection:

- AEAD_AES_128_GCM (RFC 5647),
- AEAD_AES_256_GCM (RFC 5647),
- aes128-gcm@openssh.com (RFC 5647),
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using: [selection:

- AEAD_AES_128_GCM (RFC 5647),
- AEAD_AES_256_GCM (RFC 5647),
- Implicit

] and no other mechanisms.

FCS_SSH_EXT.1.6 The TSF shall establish a shared secret with its peer using: [selection:

- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656)

] and no other mechanism.

FCS_SSH_EXT.1.7 The TSF shall use *SSH KDF* as defined in [selection:

- RFC 5656 (Section 4)

] to derive the following cryptographic keys from a shared secret: *session keys.*

FCS_SSH_EXT.1.8 The TSF shall ensure that [selection:

- a rekey of the session keys,

] occurs when any of the following thresholds are met:

- One hour connection time
- No more than one gigabyte of transmitted data, or

- No more than one gigabyte of received data.

6.8.1.4 FCS_SSHS_EXT.1 SSH Protocol – Server

FCS_SSHS_EXT.1.1 The TSF shall authenticate itself to its peer (SSH Client) using: [

- ecdsa-sha2-nistp256 (RFC 5656),
- ecdsa-sha2-nistp384 (RFC 5656),

].

6.8.2 Identification and Authentication (FIA)

6.8.2.1 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 [selection: a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
  -

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.

6.8.2.2 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 [selection: IPsec] and [selection: 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 [selection: not accept the certificate].

6.8.2.3 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 [selection: 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.

7 Security Assurance Requirements

This Security Target claims conformance to EAL2 augmented with ALC_FLR.2. The ALC-FLR.2 consists of the flaw remediation procedures that are followed in order to maintain the life-cycle of the product. The assurance is consistent with the current practice for modern IT products.

This Security Target claims conformance to EAL2 with the following SARs:

- ADV_ARC.1
- ADV_FSP.2
- ADV_TDS.1
- AGD_OPE.1
- AGD_PRE.1
- ALC_CMC.2
- ALC_CMS.2
- ALC_DEL.1
- ALC_FLR.2
- ASE_CCL.1
- ASE_ECD.1
- ASE_INT.1
- ASE_OBJ.2
- ASE_REQ.2
- ASE_SPD.1
- ASE_TSS.1
- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2
- AVA_VAN.2

8 TOE Summary Specification

8.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function as well as all of the events identified in Table 5 "Security Functional Requirements and Auditable Events".
In general, the logged audit records identify the date and time, 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 (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in Table 5 "Security Functional Requirements and Auditable Events".
The TOE includes an internal log implementation that can be used to store and review audit records locally. However, the internal audit log is a circular buffer that will overwrite the oldest records when it becomes full. The TOE can be configured to send generated audit records to an external Audit server in to mitigate the possibility of losing audit records.
The internal log can be accessed only by a user with the right role, who can review, delete (but not modify), or archive stored audit records using available CLI commands specifically designed for the management of the internal LOG. The functions available to review audit records allow the audit records to be sorted in forward or reverse order according to date/time and to be searched using regular expressions.
The Security audit function is designed to satisfy the following security functional requirements: FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1.

8.2 Cryptographic support

The TOE includes a crypto-module providing supporting cryptographic functions.
For asymmetric key pairs used for authentication, the TOE can generate RSA (3072, and 4096 bits) and ECDSA (P-256, P-384, and P-521) pair-wise keys. Additionally, the administrator can load and remove user SSH public keys that the TOE will use to authenticate SSH clients.
For asymmetric key pairs used for key exchange, the TOE supports generating ephemeral ECDH keys and DH keys for the IPsec and SSHv2 key exchange methods. The TOE generates ephemeral ECDH keys using ECC schemes for P-256/384 curves and 2048-bit keys using FFC schemes for DH keys for prime group DH group 24. The TOE supports DH group 24 key establishment scheme that meets standard RFC 5114.
Keys are zeroized when they are no longer needed by the TOE
The TOE encryption algorithm supports the GCM mode of AES as available ciphers, and all with key size 128, 192, and 256-bit.
The TOE hash algorithm supports the SHA-256, SHA-384, and SHA-512.
The TOE HMAC algorithms supports the HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512.
The TOE instantiates its AES-256 CTR_DRBG with a minimum of 256 bits of entropy from one software-based noise sources.
The TOE supports both RSA and ECDSA signing and verification. The TOE verifies RSA signatures on firmware updates and supports RSA and ECDSA authentication during SSH and IPsec.
The TOE includes an implementation of IPsec/IKE in accordance with RFC 4301, 4303, 4868, 4945, 5114, 5282, 7296.
The TOE supports IPsec in transport mode and tunnel mode. The IPsec ESP protocol is implemented in conjunction with AES-GCM-128, AES-GCM-192 and AES-GCM-256 (as specified by RFC 4106).

The TOE implements IKE2, with support for NAT traversal, as defined in RFC 4868. Diffie-Hellman (DH) Groups 24, 19, and 20 are supported for IKEv2 as are RSA and ECDSA certificates and pre-shared key IPsec authentication, AES-GCM-128, AES-GCM-192 and AES-GCM-256 algorithms as specified in RFC 5282 for encryption and integrity.
The TOE generates the secret value x used in the IKEv2 Diffie-Hellman key exchange ('x' in gx mod p) using the FIPS validated RBG specified in FCS_RBG.1, FCS_RBG.3, FCS_RBG.6, and having possible lengths of 256 bits for DH group 24, 256 bits for DH group 19, and 384 bits for DH group 20. The TOE generates nonces used in the IKEv2 exchanges of 256 bits in size. Nonces are generated using RBG meet the requirements specified in FCS_RBG.1, FCS_RBG.3, FCS_RBG.6 for random bit generation.
The Administrator is responsible for ensuring that IKE/IPsec policies are configured so that the strength of the negotiated symmetric algorithm (in terms of the number of bits in the key) in the IKEv2 CHILD_SA is less than or equal to the strength of the IKEv2 IKE_SA.
The TOE will only establish a trusted IPsec channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following type: IP address and Fully Qualified Domain Name (FQDN) in SAN or CN, Distinguished Name (DN).
An IPsec policy set can contain multiple entries, each with a different access control list (ACL). The IPsec policy entries are searched in a sequence - the TOE attempts to match the packet to the ACL specified in that entry.
The traffic matching the permit IPsec policy ACL would then flow through the IPsec tunnel and be classified as "PROTECTED".
Traffic that does not match a permit IPsec policy ACL and is also blocked by packet filter ACL on the interface would be DISCARDED.
Traffic that does not match a permit ACL in the IPsec policy, but that is not disallowed by packet filter ACLs on the interface is allowed to BYPASS the tunnel.
The TOE provides the ability to synchronize its time with a NTP server using NTP v3 and v4. The time data is protected by SHA256, SHA384, and SHA512.
The TOE supports SSHv2 interactive command-line secure administrator sessions. The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, 4254, 4256, 4344, 5647, 5656, 6187, 6668. The TOE supports public key-based and password-based authentication. The TOE allows use of the ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384 algorithms for public key authentication. The TOE establishes a user identity when an SSH client presents a public key or correct password. The TOE supports AEAD_AES_128_GCM, EAD_AES_256_GCM. aes128-gcm@openssh.com and aes256-gcm@openssh.com for both encryption and data integrity. The TOE uses ecdh-sha2-nistp256/384 for SSHv2 key exchange.
The Cryptographic support function is designed to satisfy the following security functional requirements: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.6, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG.1, FCS_RBG.3, FCS_RBG.6, FCS_IPSEC_EXT.1, FCS_NTP_EXT.1, FCS_SSH_EXT.1, FCS_SSHS_EXT.1.

8.3 Identification and authentication

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions.
The TOE supports the local definition of users with corresponding password and role. The passwords can be composed of any combination of upper- and lower-case letters, numbers, and special characters. Minimum password length is settable by the authorized security administrator, and supports password of 15 to 63 characters. By default, the password for new user accounts is none. Since this may lead to system vulnerability, passwords must be set during secure configuration of the device. Passwords shall have an appropriate lifetime.

The administrator can also configure the TOE to authenticate users using an external authentication server. The TOE supports RADIUS servers. A trusted channel using IPsec is established between TOE and external authentication server.

Administrators can connect to the TOE via a local console or remotely using SSHv2. Local administrators can access the TOE CLI interface via a serial console (direct) connection by using username and password. Remote administrators can access the CLI interface via an SSH protocol connection from an SSH client.

TOE provide password-based and public-key-based authentication mechanism for SSH. For public-key-based, administrator must import user public key into the configuration of TOE. The algorithm of public-key or certification public-key support RSA and ECDSA.

When logging via password, only obscured feedback is provided so the password is not visible when the user is inputting it.

The TOE provides the security administrator the ability to specify the maximum number of unsuccessful authentication attempts before administrator is locked out through the administrative CLI. While the TOE supports a range from 2-10.

When the defined number of unsuccessful authentication attempts has been met, the TOE shall prevent the offending Administrator from accessing TOE using any authentication method until unlock is taken by a Security Administrator.

IPsec supports X.509 certificate authentication. The certificate chain is a sequence of certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, TOE processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. TOE validate certificates in certificate chain according RFC 5280 certificate validation. The TOE also validates the revocation status of the certificate using a Certificate Revocation List (CRL) and check the basic Constraints extension and the CA flag to determine whether they are present and set to TRUE.

If the connection to determine the certificate validity cannot be established, the certificate is not accepted and the connection will not be established.

The Identification and authentication function is designed to satisfy the following security functional requirements: FIA_AFL.1, FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU.7, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, FIA_X509_EXT.3.

FIA_X509_EXT.1/Rev: The TOE performs X.509 certificate validation at the following points:

- When importing a certificate.
- During IPsec peer authentication

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

- If the certificate ‘notAfter’ date is in the past, then this is an expired certificate which is considered invalid;
- The certificate chain must terminate with a trusted CA certificate designated as a trust anchor;
- A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE;

Certificate revocation checking is performed when the certificate is presented to the TOE and when it is loaded into the TOE, and only the leaf certificate is validated.

The TOE does not use any extendedKeyUsage rules for FIA_X509_EXT.1/Rev.

FIA_X509_EXT.1/Rev focuses only on IPsec and does not involve code signing or web servers. Certificate checks support only CRL and not OCSP.

8.4 Security management

The TOE implements a role mechanism that is used to specify the role and corresponding permissions which authenticated users possess.
The TOE maintains Security Administrators that includes privileged and semi-privileged roles.
The privileged role can access all features and resources in the system except some specific commands, and can perform all of the operations defined in FMT_SMF.1. This is privilege level 15 or Network-admin or Network Administrator.
Semi-privileges roles are any that have a subset of the privileges of the level 15.
Privilege level 0, 1 (also known as network-operator) and 9 are defined by default and are customizable, privilege 2 to 8 and 10 to 14 are undefined by default and are customizable. It exists also a pre-defined privilege level called Security-audit with rights to display and maintain security log files.
Use of the level-0 through level-14 roles, as well as the network-operator role, is not required in order to properly administer a TOE. These roles possess a subset of the permissions of the network-admin role and thus are capable of only some of the management functions available to him.
The TOE offers command-line interface providing a range of security management functions for use by Security Administrators. Among the functions available are those functions that are necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.
Management of security functions behaviour related to manual updates is provided by FMT_MOF.1/ManualUpdate. In order to meet this SFR, The TSF restricts the ability to enable the functions to perform manual updates to Security Administrators. In addition, only security administrators have the right to create or delete users in the TOE. While changing the local user privilege level, the configured new level of the local user cannot be higher than that of the login-in user. In this way no user except administrators can change another user to be at the privilege level of administrator, and only administrators have the ability to perform manual update. Therefore, the manual update is restricted to administrators. The TOE uses groups to organize users.
Management of security functions behaviour related to transmission of audit data to external IT entities is provided FMT_SMF.1. The TOE meets this SFR by enforcing that:

- Only Security Administrators have right to configure audit servers where audit records are exported to.
- Only Security Administrators have the privilege to choose the trusted channel for external audit server and decide whether transmit the audit data to an external IT entity or not.
- Only Security Administrators have the privilege to modify the behaviour of TOE Security Functions (e.g. cryptographic algorithm, audit server).

The TOE also offers the following functions, which are limited to the privileged level Network Administrator:

- Start-up and shutdown the TOE.
- Manage user account definitions (create, delete, modify, and view user attributes that identify authorized users and their associated role).
- Manage password failure constraints (modify and set the threshold for the number of permitted authentication attempt failures).
- Restoration of disabled users (restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures).
- Manage the internal clock (modify and set the time and date).
- Manage remote authentication capabilities (enable, disable, and configure external RADIUS).
- Manage the internal audit log (archive, create, delete, empty, and review the audit trail).

The Security management function is designed to satisfy the following security functional requirements: FMT_MOF.1/ManualUpdate, FMT_MTD.1/CoreData, FMT_SMF.1, FMT_SMR.2.

8.5 Protection of the TSF

The TOE stores all pre-shared keys, symmetric keys, and private keys in the file system in Flash that can't be read, copy or extract by administrators; hence no interface access is available.
The administrator passwords are stored in cryptographic form. In this manner, the TOE ensures that plaintext user passwords will not be disclosed to anyone through normal interfaces including Security Administrators.
During start-up of the TOE, the TOE first checks the integrity of the firmware, and then runs a series of self-tests to ensure it is performing its cryptographic functions correctly. If any of these checks fails, the device will halt and require administrator intervention to successfully start-up.
Security administrators can check the version of the installed firmware through the command line and manually initiate a firmware update. There are means to authenticate those updates to the TOE using a digital signature and published hash prior to installing them.
The hardware of the TOE is a switch that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes clock-related functions for use by the TOE. The TOE software can also be configured to utilize the NTP protocol to keep the local hardware-based real-time clock synchronized with other network devices. The communication between TOE and NTP server will be protected by IPsec security channel. And the time synchronization is automatically performed, initiated by the TOE and negotiated with the NTP Server, based on NTP v3 (RFC 1305) and NTP v4 (RFC 5905).
The Protection of the TSF function is designed to satisfy the following security functional requirements: FPT_SKP_EXT.1, FPT_TST_EXT.1, FPT_TUD_EXT.1, FPT_STM.1, FPT_STM.2, FPT_FLS.1.

8.6 TOE access

The TOE can be configured by a Security Administrator to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, with 0 disabling the timeout – the default timeout is 10 minutes). A session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated, both for local and for remote sessions.
The user will be required to re-enter their user id and their password so they can be re-authenticated in order to establish a new session.
The user also has the ability to terminate his own sessions (log out).
The TOE can be configured to display administrator-configured advisory banners that will be displayed in conjunction with user login prompts. The banner contents are configured by a user in the Security Administrator role.
The TOE access function is designed to satisfy the following security functional requirements: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

8.7 Trusted path/channels

To support secure remote administration, the TOE includes implementations of SSH. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator.

In the case of SSH, the TOE offers secure command line interface (CLI) interactive administrator sessions. An administrator with appropriate SSH capable clients can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

As indicated earlier, the TOE can be configured to export audit records to an external audit server. In order to protect exported audit records from disclosure or modification, the TOE can be configured to utilize an IPSEC secure channel for this purpose. This protection is initiated by the TOE whenever Audit connections are established for the purpose of exporting audit records.

The communication with NTP server and authentication server also protect by IPsec secure channel.

All of the secure protocols are supported by the cryptographic operations provided by the FCS requirements in this Security Target.

The Trusted path/channels function is designed to satisfy the following security functional requirements: FTP_ITC.1, FTP_TRP.1/Admin.

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of a table mapping SFRs against security objectives.

Security Objectives	Security Functional Requirements
O.ADMIN_AUTH	FMT_SMR.2, FMT_SMF.1, FMT_MTD.1/CoreData, FIA_UIA_EXT.1, FTA_TAB.1, FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTP_TRP.1/Admin, FIA_AFL.1
O.STRONG_CRYPTO	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG.1, FCS_RBG.3, FCS_RBG.6, FMT_SMF.1
O.TRUSTED_COMM	FTP_ITC.1, FTP_TRP.1/Admin, FCS_IPSEC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
O.STRONG_AUTHENTICATION_ENDPOINT	FTP_ITC.1, FTP_TRP.1/Admin
O.SECURE_UPDATES	FPT_TUD_EXT.1, FMT_SMF.1, FMT_MOF.1/ManualUpdate
O.ACTIVITY_AUDIT	FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FPT_STM.2, FCS_NTP_EXT.1, FAU_STG_EXT.1
O.PASSWORD_PROTECTION	FPT_SKP_EXT.1, FCS_CKM.6, FIA_UAU.7, FIA_PMG_EXT.1
O.SELF_TEST	FPT_TST_EXT.1
O.BANNER	FTA_TAB.1

Below is the rationale for the security objectives mapping:

9.1.1 O.ADMIN_AUTH

- 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
- 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_UIA_EXT.1
- 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)
- If the TOE provides remote administration using a password-based authentication mechanism, FIA_AFL.1 provides actions on reaching a threshold number of consecutive password failures

9.1.2 O.STRONG_CRYPTO

- 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.1, FCS_RBG.3 and FCS_RBG.6
- Management of cryptographic functions is specified in FMT_SMF.1

Note: According to CC:2022, FCS_RBG_EXT.1 is replaced by FCS_RBG.1, FCS_RBG.3, and FCS_RBG.6.

9.1.3 O.TRUSTED_COMM

- 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
- Requirements for the use of secure communication protocols are set for allowed protocols in FCS_IPSEC_EXT.1
- Requirements for the use of secure communication protocols implemented by the packages specified in Section 2.2 may be found in the respective package's document.
- 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

9.1.4 O.STRONG_AUTHENTICATION_ENDPOINT

- 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

9.1.5 O.SECURE_UPDATES

- Requirements for protection of updates are set in FPT_TUD_EXT.1
- Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate

9.1.6 O.ACTIVITY_AUDIT

Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM.1, FPT_STM.2, and if applicable, protection of NTP channels in FCS_NTP_EXT.1Requirements for secure storage and transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1Note: According to CC:2022, FPT_STM_EXT.1 is replaced by FPT_STM.1 and FPT_STM.2.

9.1.7 O.PASSWORD_PROTECTION

- Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1
- Secure destruction of keys is specified in FCS_CKM.6

- If optional local administration using a password-based authentication mechanism is provided by the TOE, FIA_UAU.7 provides protection of password entry by providing only obscured feedback at the local console.
- If the TOE provides password-based authentication mechanisms, requirements for password lengths and available characters are set in FIA_PMG_EXT.1

Note: According to CC:2022, FCS_CKM.4 is replaced by FCS_CKM.6.

9.1.8 O.SELF_TEST

- Requirements for running self-test(s) are defined in FPT_TST_EXT.1

9.1.9 O.BANNER

- An advisory notice and consent warning message is required to be displayed by FTA_TAB.1

9.2 Dependency Rationale

This rationale provided in [PP-ND] annex E.1 shows that all dependencies of all security requirements have been addressed.

The table as below is shown that the dependencies between SFRs implemented by the TOE are addressed, which were updated in CC:2022R1.

SFR	**Dependencies**	**Rationale Statement**
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_CKM.2 FCS_CKM.3 FCS_RBG.1 FCS_CKM.6
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 FCS_CKM.3
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FCS_RBG.1	[FCS_RBG.2 or FCS_RBG.3] FPT_FLS.1 FPT_TST.1	FCS_RBG.3 FPT_FLS.1 FPT_TST.1
FCS_RBG.3	FCS_RBG.1	FCS_RBG.1
FCS_RBG.6	FCS_RBG.1	FCS_RBG.1
FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or	FCS_CKM.1 FCS_CKM.3

FCS_COP.1/KeyedHash	FCS_CKM.5] FCS_CKM.3	
FCS_IPSEC_EXT.1	FCS_RBG_EXT.1 is replaced by FCS_RBG.1, FCS_RBG.3 and FCS_RBG.6 in [CC2022]	FCS_RBG.1 FCS_RBG.3 FCS_RBG.6

Table 6 Dependency Rationale

10 Abbreviations and glossary

[CC]	Common Criteria
[EAL]	Evaluation Assurance Level
[ST]	Security Target
[TOE]	Target of Evaluation
[TSF]	TOE Security Functionality

11 References

[CC2022R1P1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction to General Model, Version CC:2022, Revision 1, November 2022.

[CC2022R1P2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version CC:2022, Revision 1, November 2022.

[CC2022R1P3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, Version CC:2022, Revision 1, November 2022.

[PP-ND] Collaborative Protection Profile for Network Devices, v3.0e, 06-12-2023

[PPSSH] Functional Package for Secure Shell (SSH), Version 1.0

[SD_ND] Evaluation Activities for Network Device cPP, Version: 3.0e, Date: 06-December-2023