H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target

Version: 2.0

Date: 2023-08-21

H3C

Document history

Version	Date	Comment	Author
0.1	2022-06-09	Initial version	SGS Brightsight
0.2	2022-06-22	Update based on developer's documentation	SGS Brightsight
0.3	2022-07-01	Update after workshop and evidence delivery	SGS Brightsight
0.4	2022-07-07	Merge versions, review and update with comments	SGS Brightsight
0.5	2022-07-08	Draft version with comments to review	SGS Brightsight
0.6	2022-07-21	Updated after developer feedback	H3C & SGS Brightsight
0.7	2022-08-03	ST ready for KOM	SGS Brightsight
0.8	2022-08-23	Updates on TSS	SGS Brightsight
1.0	2022-08-31	First release	SGS Brightsight
1.1	2022-10-28	Feedback from CCN	SGS Brightsight
1.2	2022-11-11	Feedback from CCN	H3C
1.3	2023-03-06	Updated product guidance	SGS Brightsight
1.4	2023-04-05	After evaluation round	SGS Brightsight
1.5	2023-04-11	After consultancy feedback	H3C
1.6	2023-04-21	After evaluation feedback. Updated guidance version	SGS Brightsight
1.7	2023-05-12	Update product list and product guidance	SGS Brightsight
1.8	2023-07-23	Address evaluation observation reports	SGS Brightsight
1.9	2023-08-09	Fix pending issues	H3C & SGS Brightsight
2.0	2023-08-21	New release	H3C & SGS Brightsight

Contents

1 Security Target 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 Reference

Title	H3C S10500 Series, S7500 Series, S6500 Series, S5100 Series, S5500 Series, S12500 Series, S9800 Series and S6800 Series Switches Security Target
Version	See Document History
Date	See Document History
Author	SGS Brightsight

Table 1 Security Target reference

1.2 TOE Reference

TOE Developer	H3C
TOE Name	H3C Switch Series
TOE Version	1.0

Table 2 TOE reference

1.3 TOE Overview

The Target of Evaluation (TOE) is the H3C Switch Series running Comware. Each series of this family consists of a set of distinct Switches 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 composed of hardware and firmware and are used to provide a network infrastructure supporting the switching of network traffic between connected networks.

While the Switches 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 network layers 2 and 3 switching.

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 switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote (SSH) 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, it can also be configured to work with a Network Time Server (NTP Server) and supports authentication against an external server. These three communication channels are protected with IPsec.

Figure 1 shows the TOE depicted in its intended environment.

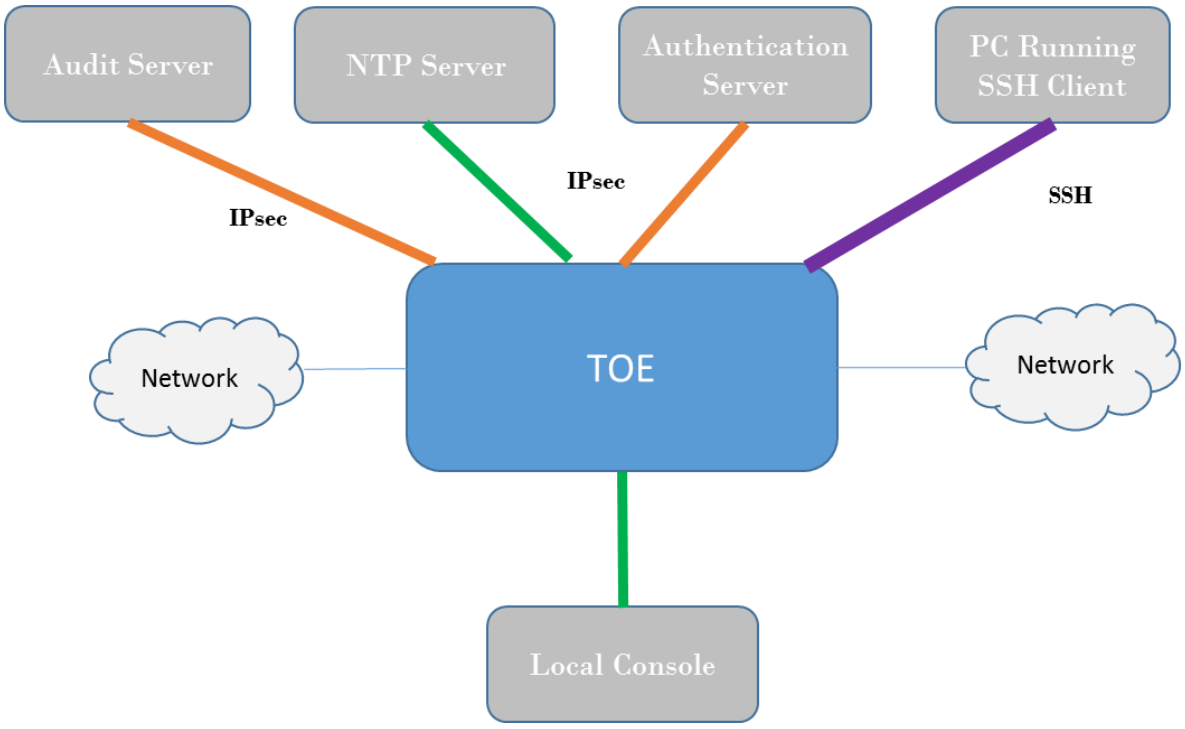

Figure 1 TOE usage scenario.

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 fibber), 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.
- Management Workstation – 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.
- 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.

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.
SSH Client	Mandatory	This includes any device with an SSH client installed that is used to establish a protected channel with the TOE.
Local console	Mandatory	This includes any Console 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	Optional	AAA (Authentication Authorization Accounting), implemented in accordance with related RFC, provides authentication, authorization and accounting functionalities.
NTP Server	Optional	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

1.4 **TOE Description**

1.4.1 Physical Scope

The TOE includes a total of 8 different switch series:

Product Series	Models	Firmware
S10500 Series	S10506X, S10508X, S10510X	H3C Comware Software, Version 7.1.070, Release 7640P01
	S10506X-G, S10508X-G, S10512X-G	H3C Comware Software, Version 7.1.070, Release 7760P01
S7500 Series	S7503X,S7503E-M, S7506X-POE, S7506X-S, S7510X-POE	H3C Comware Software, Version 7.1.070, Release 7640P01
	S7503X-M-G, S7503X-G, S7506X-G-POE, S7510X-G-POE	H3C Comware Software, Version 7.1.070, Release 7760P01
S6500 Series	S6520X-18C-SI, S6520X-26C-SI, S6520X-26MC-UPWR-SI,S6520X-26MC-SI,S6520X-16ST-SI,S6520X-24ST-SI, S6520X-10XT-SI, S6520X-16XT-SI, S6520X-26XC-UPWR-SI, S6520X-54XC-UPWR-SI,S6520X-30HC-EI, S6520X-30QC-EI, S6520X-54HC-EI, S6520X-54QC-EI,S6520X-54HC-HI, S6520X-54QC-HI, S6520X-30HC-HI,S6520X-30QC-HI,S6520X-54HF-EI,S6520X-54HF-HI,S6520X-30HF-EI,S6520X-30HF-HI	H3C Comware Software, Version 7.1.070, Release 6628P92
S5100 Series	S5130S-28S-HI,S5130S-52S-HI,S5130S-28S-PWR-HI,S5130S-52S-PWR-HI,S5130S-28C-HI,S5130S-52C-HI,S5130S-28C-PWR-HI,S5130S-52C-PWR-HI	H3C Comware Software, Version 7.1.070, Release 6348P21
	S5130S-10P-EI, S5130S-12TP-EI,S5130S-20P-EI,S5130S-28P-EI,S5130S-52P-EI,S5130S-10P-HPWR-EI,S5130S-12TP-HPWR-EI,S5130S-20P-PWR-EI,S5130S-28P-PWR-EI,S5130S-28P-HPWR-EI,S5130S-52P-PWR-EI,S5130S-28S-EI,S5130S-52S-EI,S5130S-28F-EI,S5130S-52F-EI,S5130S-28TP-EI,S5130S-52TP-EI,S5130S-28S-PWR-EI,5130S-28S-HPWR-EI,S5130S-52S-PWR-EI	H3C Comware Software, Version 7.1.070, Release 6348P21
	S5170-28S-EI,S5170-54S-EI,S5170-54S-PWR-EI,S5170-28S-HPWR-EI	H3C Comware Software, Version 7.1.070, Release R1122P30
S5500 Series	S5570S-28S-EI, S5570S-54S-EI, S5570S-54F-EI, S5570S-36F-EI, S5570S-54S-PWR-EI-A, S5570S-28S-HPWR-EI-A	H3C Comware Software, Version 7.1.070, Release R1122P30
	S5560X-30C-EI, S5560X-54C-EI, S5560X-30C-PWR-EI, S5560X-54C-PWR-EI, S5560X-30F-EI, S5560X-54F-EI, 5560X-34S-EI, S5560X-54S-EI,S5560X-30F-EIF	H3C Comware Software, Version 7.1.070, Release 6628P92
	S5590-28T8XC-EI, S5590-48T4XC-EI, S5590-28S8XC-EI, S5590-48S4XC-EI, S5590-28P8XC-EI, S5590-48P6XC-EI	H3C Comware Software, Version 7.1.070, Release 8108P60
S12500 Series	S12504X-AF,S12508X-AF,S12516X-AF	H3C Comware Software, Version 7.1.070, Release 2830
	S12504G-AF,S12508G-AF,S12516G-AF	H3C Comware Software, Version 7.1.070, Release 7640P01
S9800 Series	S9820-8C, S9820-8C-SAN	H3C Comware Software, Version 7.1.070, Release 6715P01

	S9850-32H, S9850-4C, S9850-32H-H1, S9850-4C-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
	S9820-64H, S9820-64H-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
S6800 Series	S6890-54HF, S6890-30HF	H3C Comware Software, Version 7.1.070, Release 2830
	S6825-54HF	H3C Comware Software, Version 7.1.070, Release 6715P01
	S6800-54HT, S6800-54HF, S6800-32Q-H1, S6800-2C-H1, S6800-4C-H1, S6800-54QF-H3, S6800-54QT-H3, S6800-54QF-H5	H3C Comware Software, Version 7.1.070, Release 6715P01
	S6812-24X6C,S6812-48X6C	H3C Comware Software, Version 7.1.070, Release 6628P92
	S6813-24X6C,S6813-48X6C	H3C Comware Software, Version 7.1.070, Release 6628P92
	S6805-54HF, S6805-54HT, S6805-54HF-H1, S6805-54HT-H1	H3C Comware Software, Version 7.1.070, Release 6715P01
	S6850-56HF, S6850-2C, S6850-56HF-H1, S6850-56HF-SAN,	H3C Comware Software, Version 7.1.070, Release 6715P01

Table 4 TOE series, devices and firmware

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 the guidance documents described in Annex A.

1.4.2 Logical Scope

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

1.4.2.1 Security audit

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

The TOE can be configured to store the logs locally so they can be accessed by an administrator and 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.

1.4.2.2 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).

1.4.2.3 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 (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. Additionally, TOE can configure IPSEC connected RADIUS servers for authentication services to support e.g. centralized user management.

1.4.2.4 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.

1.4.2.5 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.

1.4.2.6 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.

1.4.2.7 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.

2 Conformance claims

2.1 CC Conformance Claim

The TOE and ST claim conformance to the CC Version 3.1 revision 5:

- Part 2 extended [CC31R5P2]
- Part 3 conformant [CC31R5P3].

2.2 Protection Profile Conformance

The TOE claims exact conformance to:

- collaborative Protection Profile for Network Devices v2.2e, 23-03-2020.

2.3 Conformance Rationale

This ST provides exact conformance to the PP stated in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile, performing only operations defined there.

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].

4 Security Objectives

4.1 Security Objectives for the TOE

In alignment with the Network Devices PP [PP-ND], no Security Objectives for the TOE are defined.

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].

5 Extended Component Definition

Extended Component Definition has been taken with no modification from the Network Devices PP [PP-ND].

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 [CC31R5P2] 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 [CC31R5P2] 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').

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 user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- [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, 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	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.

FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_IPSEC_EXT.1	Failure to establish an IPSEC SA.	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	Failure to establish an SSH session	Reason for failure
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
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.
FMT_MTD.1/CryptoKeys	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address)
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.

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

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 2048-bit 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 [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 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "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: RFC 3526].

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

6.2.1.3 FCS_CKM.4 Cryptographic Key Destruction

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

- *For plaintext keys in volatile storage, the destruction shall be executed by a [selection:* single overwrite consisting of *[selection:* zeroes*]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [selection:*
  - logically addresses the storage location of the key and performs a *[selection:* single-pass] overwrite consisting of *[selection:* zeroes*];*

that meets the following: *No Standard*.

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 (modulus) [assignment: 2048 bits or greater],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: 256 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,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

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 (Extended – FCS_RBG_EXT)

6.2.3.1 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: CTR_DRBG (AES)].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: *[assignment: 1]* software-based noise source with a minimum of [selection: 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength

Table for Hash Functions", of the keys and hashes that it will generate.

6.2.4 Cryptographic Protocols (Extended – FCS_ IPSEC_EXT, FCS_NTP_EXT, FCS_SSHS_EXT)

6.2.4.1 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: transport mode, tunnel 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 5996 and [selection: with mandatory support for NAT traversal as specified in RFC 5996, 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 [assignment: *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 [assignment: *1-168*] 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_EXT.1, and having a length of at least [assignment: *224 (for DH Group 14), 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: 14 (2048-bit MODP)] according to RFC 3526,
- [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 by default 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].

6.2.4.2 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.

6.2.4.3 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [selection: 4256, 4344, 5647, 5656, 6187, 6668]

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

FCS_SSHS_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_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [selection: ecdh-sha2-nistp256] and [selection: ecdh-sha2-nistp384] are the only allowed key exchange methods used for the SSH protocol.

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

6.3 Identification and Authentication (FIA)

6.3.1 Authentication Failure Management (FIA_AFL)

6.3.1.1 FIA_AFL.1 Authentication Failure Management (Refinement)

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 *[assignment: unlock*] is taken by an Administrator; prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

6.3.2 Password Management (Extended – FIA_PMG_EXT)

6.3.2.1 FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: "", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "[", "\", "]", "_", "`", "{", "}", *and "~"*]];

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

6.3.3 User Identification and Authentication (Extended – FIA_UIA_EXT)

6.3.3.1 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.

6.3.4 User authentication (FIA_UAU) (Extended – FIA_UAU_EXT)

6.3.4.1 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

6.3.4.2 FIA_UAU.7 Protected Authentication Feedback

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

6.3.5 Authentication using X.509 certificates (Extended – FIA_X509_EXT)

6.3.5.1 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].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

6.3.5.2 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].

6.3.5.3 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.

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 <u>enable</u> the functions *<u>to perform manual updates to Security Administrators</u>*.

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 <u>manage</u> the *<u>TSF data to Security Administrators</u>*.

6.4.2.2 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys	The TSF shall restrict the ability to *<u>manage</u>* the *cryptographic keys* 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 locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [selection: <u>digital signature</u>, <u>hash comparison</u>] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- *[selection:*
  - <u>Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full)</u>;
  - <u>Ability to modify the behaviour of the transmission of audit data to an external IT entity</u>;

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

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

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 Protection of Administrator Passwords (Extended – FPT_APW_EXT)

6.5.2.1 FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

6.5.3 TSF Testing (Extended – FPT_TST_EXT)

6.5.3.1 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 demonstrate the correct operation of the TSF: [*assignment: Software integrity, AES, SHS, HMAC, RSA, ECDSA and DRBG*].

6.5.4 Trusted Update (FPT_TUD_EXT)

6.5.4.1 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, published hash] prior to installing those updates.

6.5.5 Time stamps (Extended – FPT_STM_EXT))

6.5.5.1 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1	The TSF shall be able to provide reliable time stamps for its own use.
FPT_STM_EXT.1.2	The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with an NTP server].

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 **Administrator-**initiated termination of the **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 **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding 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 **authorized IT entities supporting the following capabilities: audit server, [selection: authentication server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**
FTP_ITC.1.2	The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*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** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.
FTP_TRP.1.2/Admin	The TSF shall permit remote **Administrators** to initiate communication via the trusted path.
FTP_TRP.1.3/Admin	The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

7 Security Assurance Requirements

This Security Target claims conformance to EAL1, augmented with ASE_SPD.1. This assurance level was chosen to keep the consistency with the Network Devices PP [PP-ND].

The description of the SARs is an exact copy of the Network Devices PP [PP-ND] Section 7.

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 (2048, 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 14 and DH group 24. The TOE supports DH group 14 key establishment scheme that meets standard RFC 3526 and 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 2407, 2408, 2409, 3526, 3602, 4106, 4109, 4301, 4303, 4868, 4945, 5114, 5996.

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 5996 and RFC 4868. Diffie-Hellman (DH) Groups 14, 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_EXT.1 and having possible lengths of 224 bits for DH group 14, 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_EXT.1 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).

A IPsec policy set can contain multiple entries, each with a different access 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 ssh-rsa, 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.4, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RGB_EXT.1, FCS_IPSEC_EXT.1, FCS_NTP_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.

The administrator can also configure the TOE to authenticate users using an external authentication server. The TOE supports RADIUS and HWTACACS 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 or an Administrator defined time period has elapsed.

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 validate the revocation status of the certificate using a Certificate Revocation List (CRL) and check the basicConstraints 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_EXT.2, FIA_UAU.7, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, FIA_X509_EXT.3.

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_MTD.1/CryptoKeys, 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 to configuration file in cryptographic form hashed with *scrypt* algorithms function, including username passwords, authentication passwords, console and virtual terminal line access passwords. 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.

The Protection of the TSF function is designed to satisfy the following security functional requirements: FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_TST_EXT.1, FPT_TUD_EXT.1, FPT_STM_EXT.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 all the assumptions against security objectives. It is informative only, as it is a representation of the tracing of assumptions to objectives as defined in [PP-ND] adopted in this ST.

9.1.1 Assumptions to Security Objectives Mapping

Objectives \ Threats and assumptions	A.PHYSICAL_PROTECTION	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION	A.TRUSTED_ADMINISTRATOR	A.REGULAR_UPDATES	A.ADMIN_CREDENTIALS_SECURE	A.RESIDUAL_INFORMATION
OE.PHYSICAL	X						
OE.NO_GENERAL_PURPOSE		X					
OE.NO_THRU_TRAFFIC_PROTECTION			X				
OE.TRUSTED_ADMIN				X			
OE.UPDATES					X		
OE.ADMIN_CREDENTIALS_SECURE						X	
OE.RESIDUAL_INFORMATION							X

Table 6 Threats and Assumptions to Security Objectives Mapping

9.2 Dependency Rationale

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

10 Abbreviations and glossary

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

11 References

[CC31R5P1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction to General Model, Version 3.1, Revision 5, April 2016.

[CC31R5P2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version 3.1, Revision 5, April 2016.

[CC31R5P3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, Version 3.1, Revision 5, April 2016.

[PP-ND] collaborative Protection Profile for Network Devices, v.2.2e, 23-03-2020

A. Product guidance

Product Series	Model series	Document name	Version
All	All	Preparative and Operative Procedures for CC NDPP Switch Series	2.0
S10500 Series	S10500X	H3C S10500X Switch Series Command References	6W100
		H3C S10500X Switch Series Configuration Guides	6W100
	S10500X-G	H3C S10500X-G Switch Series Command References	6W100
		H3C S10500X-G Switch Series Configuration Guides	6W100
S7500 Series	S7500X	H3C S7500X Switch Series Command References	6W100
		H3C S7500X Switch Series Configuration Guides	6W100
	S7500X-G	H3C S7500X-G Switch Series Command References	6W100
		H3C S7500X-G Switch Series Configuration Guides	6W100
S6500 Series	S6520X	H3C S6520X-EI & S6520X-HI & S6520X-SI Switch Series Command References	6W100
		H3C S6520X-EI & S6520X-HI & S6520X-SI Switch Series Configuration Guides	6W100
S5100 Series	S5130S	H3C S5130S-EI & S5130S-HI Switch Series Command References	6W100
		H3C S5130S-EI & S5130S-HI Switch Series Configuration Guides	6W100
	S5170-EI	H3C S5170-EI Switch Series Command References	6W100
		H3C S5170-EI Switch Series Configuration Guides	6W100
S5500 Series	S5570S-EI	H3C S5570S-EI&S5500V3-SI Switch Series Command References	6W100
		H3C S5570S-EI&S5500V3-SI Switch Series Configuration Guides	6W100
	S5560X	H3C S5560X-EI Switch Series Command References	6W100
		H3C S5560X-EI Switch Series Configuration Guides	6W100
	S5590-EI	H3C S5590-HI&S5590-EI&S5500V3-HI Switch Series Command References	6W100
		H3C S5590-HI&S5590-EI&S5500V3-HI Switch Series Configuration Guides	6W100
S12500 Series	S12500X-AF	H3C S12500X-AF Switch Series Command References	6W100
		H3C S12500X-AF Switch Series Configuration Guides	6W100
	S12500G-AF	H3C S12500G-AF Switch Series Command References	6W100
		H3C S12500G-AF Switch Series Configuration Guides	6W100
S9800 Series	S9820-8C	H3C S9820-8C Switch Command References	6W100
		H3C S9820-8C Switch Configuration Guides	6W100
	S9850	H3C S6805[S6825][S6850][S9850] Command References	6W100
		H3C S6805[S6825][S6850][S9850] Configuration Guides	6W100
	S9820-64H	H3C S9820-64H Switch Command References	6W100

		H3C S9820-64H Switch Configuration Guides	6W100
S6800 Series	S6890	H3C S6890 Switch Series Command References	6W100
		H3C S6890 Switch Series Configuration Guides	6W100
	S6825 S6850 S6805	H3C S6805[S6825][S6850][S9850] Command References	6W100
		H3C S6805[S6825][S6850][S9850] Configuration Guides	6W100
	S6800	H3C S6800[S6860][S6861] & S6820 Switch Series Command References	6W100
		H3C S6800[S6860][S6861] & S6820 Switch Series Configuration Guides	6W100
	S6812 S6813	H3C S6812 & S6813 Switch Series Command References	6W100
		H3C S6812 & S6813 Switch Series Configuration Guides	6W100