Extreme Networks Switching Engine version 33.4.100 Security Target

Version 0.4
August 4, 2026

Prepared for:

Extreme Networks, Inc.

6480 Via Del Oro, San Jose, CA 95119

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the Extreme Networks Switching Engine version 33.4.100 provided by Extreme Networks, Inc. The TOE is being evaluated as a network device.

The Security Target contains the following additional sections:

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

Conventions

The following conventions have been applied in this document:

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

Acronyms

AAR	Authentication, Authorization and Accounting
AAR	Assurance Activity Report
AES	Advanced Encryption Standard
ARM	Advanced RISC Machines
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCTL	CC Testing Laboratory
CEM	Common Evaluation Methodology
CI	Configuration Item
CLI	Command line interface

CM	Configuration Management
CSP	Critical Security Parameter
DoD	Department of Defense
DTR	Detailed Test Report
ETR	Evaluation Technical Report
FOM	FIPS Object Module
FSP	Functional Specification
IT	Information Technology
MIPS	Microprocessor without Interlocked Pipelined Stages
NDcPP30e	collaborative Protection Profile for Network Devices
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OCSP	Online certificate status protocol
OS	Operating System
PP	Protection Profile
RBAC	Role-based Access Control
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSHv2	Secure shell version 2
ST	Security Target
TLS	Transport Layer security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

1.1 Security Target Reference

ST Title – Extreme Networks Switching Engine version 33.4.100 Security Target

ST Version – Version 0.4

ST Date – August 4, 2026

1.2 TOE Reference

TOE Identification – Extreme Networks Switching Engine version 33.4.100

TOE Developer – Extreme Networks, Inc.

Evaluation Sponsor – Extreme Networks, Inc

1.3 TOE Overview

The TOE is the Extreme Networks Switching Engine version 33.4.100. The TOE provides high density layer 2/3 switching with low latency cut-through switching and IPv4 and IPv6 unicast and multicast routing to enable enterprise aggregation and core backbone deployments. The TOE consists of a hardware appliance with embedded software components.

All TOE appliances are shipped ready for immediate access through a Command Line Interface [CLI], with some basic features enabled by default. However, to ensure secure use the product must be configured prior to being put into a production environment as specified in the TOE guidance.

1.4 TOE Description

The TOE consists of both hardware and software components. The TOE consists of the following series of appliances all running software version 33.4.100:

Platform	Model	Processor
Switching Engine 33.4.100	U5320	Broadcom BCM56175, BCM56274 (ARMv8)
	U5420	Broadcom BCM56274, BCM56275 (ARMv8)
	U5520	Broadcom BCM56375 (ARMv8)
	U5720	Intel Atom C3338, C3538 Denverton
	U7520	Intel Atom C3758 Denverton
	U7720	Intel Atom C3758 Denverton

Each hardware profile provides a defined set of performance characteristics - switching bandwidth, latency, and port density while offering the same level of security features.

Switch Engine 5320 Series:

The ExtremeSwitching 5320 Series are standalone Ethernet switches. The x435 Series offers comprehensive Layer 2 switching, static routing, advanced PoE, role-based policy and comprehensive security services. The 5320 Series is ideal for enterprises looking for Ethernet connectivity in their branch/small sites or at their network edge.

The Switch Engine 5320 Series consists of the following switches:

Models	Model Specifications
5320-48T-8XE	ExtremeSwitching 5320 48 10/100/1000BASET FDX/HDX, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-48P-8XE	ExtremeSwitching 5320 48 10/100/1000BASET FDX/HDX PoE+, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-24T-8XE	ExtremeSwitching 5320 24 10/100/1000BASET FDX/HDX, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-24P-8XE	ExtremeSwitching 5320 24 10/100/1000BASET FDX/HDX PoE+, 8 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-16P-4XE	ExtremeSwitching 5320 16 10/100/1000BASET FDX/HDX PoE+, 4 10G unpopulated SFP+, MACSec capable, internal fixed PSU, fans
5320-16P-4XE-DC	ExtremeSwitching 5320 16 10/100/1000BASET FDX/HDX PoE+, 4 10G unpopulated SFP+, MACSec capable, internal fixed DC PSU, fans

Table 1-1 5320 Series

Switch Engine 5420 Series:

The ExtremeSwitching 5420 Series is a stackable switch family providing secure Gigabit and multi-Gigabit Ethernet connectivity. The 5420 Series offers routing and switching, high-speed stacking, modular uplink options, advanced

PoE, and comprehensive security. This makes the x465 Series an ideal choice for high-end wiring closet and network edge deployments.

The Switch Engine 5420 Series consists of the following switches:

Models	Model Specifications
5420F-24T-4XE	24 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-24P-4XE	24 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-24S-4XE	24 x 1000Base-X (SFP) ports (unpopulated) - Full / Half-Duplex (autosensing) 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48T-4XE	48 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48P-4XE	48 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-48P-4XL	48 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable - LRM-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-8W-16P-4XE	8 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 16 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420F-16W-32P-4XE	16 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port

Models	Model Specifications
5420F-16MW-32P-4XE	16 x 100M/1G/2.5GBase-T 802.3bt (90W) ports - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 1/10Gb SFP+ uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-24T-4YE	24 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-24W-4YE	24 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-48T-4YE	48 x 10/100/1000Base-T ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-48W-4YE	48 x 10/100/1000Base-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port
5420M-16MW-32P-4YE	16 x 100M/1G/2.5GBase-T 802.3bt (90W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 32 x 10/100/1000Base-T 802.3at (30W) ports - Full / Half-Duplex (autosensing) - MACsec-capable 4 x 10/25Gb SFP28 uplink ports - MACsec-capable 2 x 10Gb SFP+ stack ports 1 x Serial console port (RJ-45) 1 x 10/100/1000BASE-T out-of-band management port 2 x USB A ports for management or external USB flash 1 x USB Micro-B console port

Table 1-2 5420 Series

Switch Engine 5520 Series:

The 5520 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. The 5520 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 5520 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 5520 Series consists of the following switches:

Models	Model Specifications
5520-24T	5520 Universal Switch with 24 x 10/100/1000BASE-T full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 2 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-24W	5520 Universal Switch with 24 x 10/100/1000BASE-T full/half duplex 802.3bt 90W PoE MACseccapable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1 VIM slot, 2

Models	Model Specifications
	unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48T	5520 Universal Switch with 48 x 10/100/1000BASE-T full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48W	5520 Universal Switch with 48 x 10/100/1000BASE-T full/half duplex 802.3bt 90W PoE MACseccapable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-12MW-36W	5520 Universal Switch with 12 x 100Mb/1Gb/2.5Gb/5Gb 802.3bt 90W PoE MACsec-capable ports plus 36 x 10/100/1000BASE-T 802.3bt 90W PoE full/half duplex MACsec-capable ports, includes 2 x Stacking/QSFP28 ports, 3 fan modules, 1VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-48SE	5520 Universal Switch with 48 x 100M/1Gb SFP MACsec-capable ports, includes 2 x Stacking/ QSFP28 ports, 3 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription
5520-24X	5520 Universal Switch with 24 x 100Mb/1Gb/10Gb SFP+ ports, includes 2 Stacking/QSFP28 ports, 2 fan modules, 1 VIM slot, 2 unpopulated modular PSU slots, Base software license, includes 1-year XIQ Pilot subscription

Table 1-3 5520 Series

Switch Engine 5720 Series:

The 5720 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. The 5720 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 5720 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 5720 Series consists of the following switches:

Models	Model Specifications
5720-24MW	24 port 802.3bt 90w PoE Switch, multi-rate up to 5G, MACSEC
5720-48MW	48 port 802.3bt 90w PoE Switch, multi-rate up to 5G, MACSEC
5720-24MXW	24 port 802.3bt 90w PoE Switch, multi-rate up to 10G, MACSEC
5720-48MXW	48 port 802.3bt 90w PoE Switch, multi-rate up to 10G, MACSEC

Table 1-4 5720 Series

Switch Engine 7520 Series:

The 7520 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. The 7520 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 7520 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 7520 Series consists of the following switches:

Models	Model Specifications
7520-48XT-6C	7520 – A high-performance, fixed-form switch with 48 × 10GbE SFP+ ports and 6 × 40/100GbE uplinks, designed for data center leaf/spine or high-density aggregation with advanced Layer 2/3 and VXLAN/EVPN support.

Models	Model Specifications
7520-48Y-8C	7520 – A high-performance, fixed-form switch with 48 × 25GbE SFP28 ports and 6 × 40/100GbE uplinks, ideal for data center leaf/spine or high-density aggregation with advanced Layer 2/3 and VXLAN/EVPN support.

Table 1-5 7520 Series

Switch Engine 7720 Series:

The 7720 Series is a family of feature-rich edge and aggregation switches designed for the next generation digital enterprise. Powered by Extreme Networks ExtremeXOS (EXOS), the 7720 Series universal hardware provides end-to-end secure network segmentation and advanced policy capabilities. The 7720 platform can be deployed across a range of edge, aggregation and wiring-closet environments.

The Switch Engine 7720 Series consists of the following switches:

Models	Model Specifications
7720-32C	7720 – A high-performance, fixed-form switch with 32 × 100GbE QSFP28 ports, delivering up to 6.4 Tbps for data center spine or core deployments with advanced Layer 2/3 and VXLAN/EVPN support.

Table 1-6 7720 Series

1.4.1 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the EXOS software is shared across all platforms.

EXOS is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. A dedicated cryptographic module is integrated with protocol libraries that implement secure channel functionality. A control plane subsystem that includes Internet Protocol (IP) host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. A system management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements an administrative interface and maintains configuration information.

The figure below outlines the TOE Architecture:

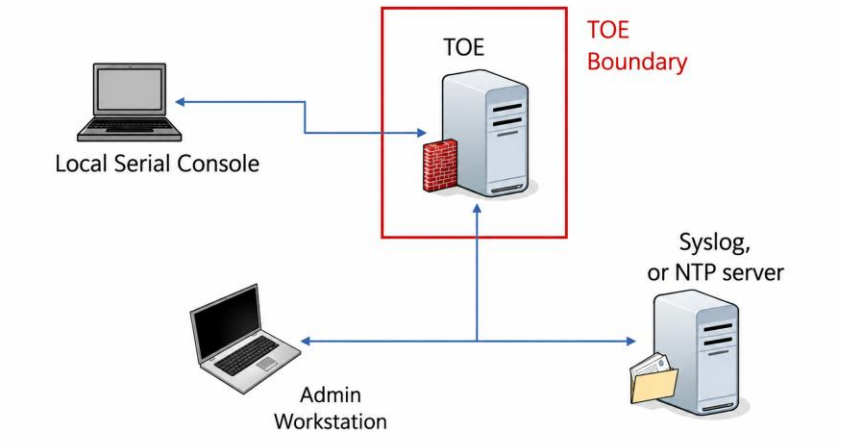

Figure 1TOE Operational Environment

The TOE supports a number of features that are not part of the core functionality. These features are not included in the scope of the evaluation:

- The use of SNMPv3 is excluded.
- Use of the FTP server is excluded and it is disabled by default.
- Integration with AAA server is not evaluated.
- Virtualized products are not included in the scope and are not evaluated.

1.4.1.1 Physical Boundaries

The physical boundary of the TOE is Extreme Networks Switching Engine version 33.4.100. EXOS is based on Linux Kernel version 5.10.177.

The Operational Environment of the TOE includes:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- Audit server for external storage of audit records
- NTP server for synchronizing system time
- Certificate Authority and OCSP servers to support X.509

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by Extreme Networks Switching Engine version 33.4.100:

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

1.4.1.2.1 Security audit

The TOE generates audit records for all security-relevant events. For each audited event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The resulting records are stored locally and can be sent securely to a designated audit server for archiving. Security Administrators, using the appropriate CLI commands, can also view audit records locally. The TOE provides a reliable timestamp relying on the appliance's built-in clock or using an NTP server.

1.4.1.2.2 Cryptographic support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing a dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSHv2
  - TLS v1.2
- Entropy is collected and used to support seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X509 Certificate authentication integrated with TLS protocol.

The TOE uses a dedicated cryptographic module to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

1.4.1.2.3 Identification and authentication

The TOE supports Role-Based Access Control (RBAC) managed by an Authentication, Authorization, and Accounting (AAA) module that stores and manages permissions of all users and their roles. The TOE requires users to provide their assigned unique username and password before any administrative access to the system is granted. Alternatively, the TOE can be configured to rely on an external Radius server for authentication.

Each authorized user is associated with an assigned role and role-specific permissions that determine their access to TOE features. The AAA module stores the assigned role of each user along with all other information required for that user to access the TOE. All TOE management functions are restricted to the Security Administrator.

The TOE supports X509v3 certificate validation during negotiation of TLS protected syslog, TLS protected Radius, and SSH X509 authentication. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.

1.4.1.2.4 Security management

The TOE allows remote administration using an SSHv2 session, and local administration using a console. Both remote and local administration are conducted over a Command Line Interface (CLI) terminal that facilitates access to all of the management functions used to administer the TOE.

There are two types of administrative users within the system: Security Administrator and User. All of the management functions are restricted to Security Administrators, including: managing user accounts and roles, rebooting and applying software updates, administering the system configuration, and reviewing audit records. The term “Security Administrator” is used to refer to any administrative user with the appropriate role to perform the relevant functions.

1.4.1.2.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

- The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable or accessible in plaintext.
- The TOE ensures that reliable time information is available for both log accountability and synchronization with the operating environment.
- The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

1.4.1.2.6 TOE access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which any inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

1.4.1.2.7 Trusted path/channels

The TOE protects remote sessions by establishing a trusted path secured using SSH between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel using TLS between itself and the audit server. Mutual authentication using client-side x.509v3 certificates is supported by the TOE’s TLS client for syslog over TLS.

1.4.2 TOE Documentation

The following administrator guidance is available:

- Extreme Switch Engine Common Criteria Configuration Guide, 33.4.100, June 2026

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e)
    - Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10)

Package	Technical Decision	Applied	Notes
CPP_ND_V3.0E	TD1033 - NIT Technical Decision: Sunset Dates for NDcPP Configurations PP_APP_V2.0	Yes	
CPP_ND_V3.0E	TD0990 - NIT Technical Decision: CTR_DRBG in FCS_RBG_EXT.1.2	Yes	
CPP_ND_V3.0E	TD0973 - NIT Technical Decision: FCS_(D)TLSS_EXT.1.3 Test 2 DHE Ciphersuite Conditionality	No	TLSS is not claimed
CPP_ND_V3.0E	TD0923 - NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	Yes	
CPP_ND_V3.0E	TD0921 - NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	Yes	
CPP_ND_V3.0E	TD0900- NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	Yes	
CPP_ND_V3.0E	TD0899 - NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	Yes	
CPP_ND_V3.0E	TD0886 – Clarification to FAU_STG_EXT.1 Test 6	Yes	
CPP_ND_V3.0E	TD0880 – NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	Yes	
CPP_ND_V3.0E	TD0879 - NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Yes	
CPP_ND_V3.0E	TD0868 - NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	Yes	
CPP_ND_V3.0E	TD0836 - NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	Yes	
PKG_SSH_V1.0	TD1023 - Clarifications to FCS_SSH_EXT.1.5 When aes256-gcm@openssh.com Is Selected	Yes	
PKG_SSH_V1.0	TD1015 - Addition of ECD to PKG_SSH_V1.0	Yes	
PKG_SSH_V1.0	TD0967 - Allowance of Kex-strict in PKG_SSH_V1.0	Yes	
PKG_SSH_V1.0	TD0909 - Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	Yes	
PKG_SSH_V1.0	TD0777 - Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	Yes	
PKG_SSH_V1.0	TD0732 - FCS_SSHS_EXT.1.3 Test 2 Update	Yes	
PKG_SSH_V1.0	TD0695 - Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	Yes	
PKG_SSH_V1.0	TD0682 - Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	Yes	

Table 2-1 Technical Decisions

2.1 Conformance Rationale

The ST conforms to the NDcPP30e/SSH10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP30e/SSH10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP30e/SSH10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP30e/SSH10 should be consulted if there is interest in that material.

In general, the NDcPP30e/SSH10 has defined Security Objectives appropriate for network devices and as such are applicable to the Extreme Networks Switching Engine version 33.4.100 TOE.

3.1 Security Objectives for the Operational Environment

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

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

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the it's own VM, and does not include other VMs or the VS.

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

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

OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

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

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to

- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP30. The NDcPP30 defines the following extended requirements and since they are not redefined in this ST the NDcPP30 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP30e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP30e:FCS_NTP_EXT.1: NTP Protocol
- NDcPP30e:FCS_RBG_EXT.1: Random Bit Generation – per TD0990
- SSH10:FCS_SSH_EXT.1: SSH Protocol - per TD0967 & TD1023
- SSH10:FCS_SSHS_EXT.1: SSH Protocol - Server - per TD0682
- NDcPP30e:FCS_TLSC_EXT.1: TLS Client Protocol
- NDcPP30e:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
- NDcPP30e:FIA_PMG_EXT.1: Password Management
- NDcPP30e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP30e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP30e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP30e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP30e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP30e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
- NDcPP30e:FPT_STM_EXT.1: Reliable Time Stamps
- NDcPP30e:FPT_TST_EXT.1: TSF testing - per TD0836
- NDcPP30e:FPT_TUD_EXT.1: Trusted update
- NDcPP30e:FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

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

The SFRs have all been drawn from the NDcPP30e/SSH10. The refinements and operations already performed in the NDcPP30e/SSH10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP30e/SSH10 and any residual operations have been completed herein. Of particular note, the NDcPP30e/SSH10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP30e/SSH10. The NDcPP30e/SSH10 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Extreme Networks Switching Engine version 33.4.100 TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP30e:FAU_GEN.1: Audit Data Generation
	NDcPP30e:FAU_GEN.2: User identity association
	NDcPP30e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP30e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP30e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP30e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP30e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP30e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP30e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP30e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP30e:FCS_NTP_EXT.1: NTP Protocol
	NDcPP30e:FCS_RBG_EXT.1: Random Bit Generation – per TD0990
	SSH10:FCS_SSH_EXT.1: SSH Protocol - per TD0967 & TD1023
	SSH10:FCS_SSHS_EXT.1: SSH Protocol - Server - per TD0682
	NDcPP30e:FCS_TLSC_EXT.1: TLS Client Protocol
	NDcPP30e:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
FIA: Identification and authentication	NDcPP30e:FIA_AFL.1: Authentication Failure Management
	NDcPP30e:FIA_PMG_EXT.1: Password Management
	NDcPP30e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP30e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP30e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP30e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP30e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP30e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP30e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP30e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP30e:FMT_SMF.1: Specification of Management Functions - per TD0880
	NDcPP30e:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP30e:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP30e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
	NDcPP30e:FPT_STM_EXT.1: Reliable Time Stamps
	NDcPP30e:FPT_TST_EXT.1: TSF testing - per TD0836

	NDcPP30e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP30e:FTA_SSL.3: TSF-initiated Termination
	NDcPP30e:FTA_SSL.4: User-initiated Termination
	NDcPP30e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP30e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP30e:FTP_ITC.1: Inter-TSF trusted channel
	NDcPP30e:FTP_TRP.1/Admin: Trusted Path

Table 5-1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP30e:FAU_GEN.1)

NDcPP30e: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 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).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

NDcPP30e: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 5-2.

Requirement	Audit Event	Additional Contents
NDcPP30e:FAU_GEN.1	None	None
NDcPP30e:FAU_GEN.2	None	None
NDcPP30e:FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration
NDcPP30e:FCS_CKM.1	None	None
NDcPP30e:FCS_CKM.2	None	None
NDcPP30e:FCS_CKM.4	None	None
NDcPP30e:FCS_COP.1/DataEncryption	None	None
NDcPP30e:FCS_COP.1/Hash	None	None
NDcPP30e:FCS_COP.1/KeyedHash	None	None
NDcPP30e:FCS_COP.1/SigGen	None	None
NDcPP30e:FCS_NTP_EXT.1	Configuration of a new time server. Removal of configured time server.	Identity if new/removed time server.
NDcPP30e:FCS_RBG_EXT.1	None	None
NDcPP30e:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP30e:FCS_TLSC_EXT.2	None	None

Requirement	Audit Event	Additional Contents
NDcPP30e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP30e:FIA_PMG_EXT.1	None	None
NDcPP30e:FIA_UAU.7	None	None
NDcPP30e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP30e: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.
NDcPP30e:FIA_X509_EXT.2	None	None
NDcPP30e:FIA_X509_EXT.3	None	None
NDcPP30e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
NDcPP30e:FMT_MTD.1/CoreData	None	None
NDcPP30e:FMT_MTD.1/CryptoKeys	None	None
NDcPP30e:FMT_SMF.1	All management activities of TSF data.	None
NDcPP30e:FMT_SMR.2	None	None
NDcPP30e:FPT_APW_EXT.1	None	None
NDcPP30e:FPT_SKP_EXT.1	None	None
NDcPP30e: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).
NDcPP30e:FPT_TST_EXT.1	None	None
NDcPP30e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
NDcPP30e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
NDcPP30e:FTA_SSL.4	The termination of an interactive session.	None
NDcPP30e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session lock.	None
NDcPP30e:FTA_TAB.1	None	None
NDcPP30e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	None None Reason for failure
NDcPP30e: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

Table 5-2 Audit Events

5.1.1.2 User identity association (NDcPP30e:FAU_GEN.2)

NDcPP30e:FAU_GEN.2.1
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Protected Audit Event Storage (NDcPP30e:FAU_STG_EXT.1)

NDcPP30e: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.
NDcPP30e:FAU_STG_EXT.1.2
The TSF shall be able to store generated audit data on the TOE itself. In addition [***The TOE shall consist of a single standalone component that stores audit data locally***]
NDcPP30e:FAU_STG_EXT.1.3
The TSF shall maintain a [***log file, buffer***] of audit records in the event that an interruption of communication with the remote audit server occurs.
NDcPP30e:FAU_STG_EXT.1.4
The TSF shall be able to store [***persistent***] audit records locally with a minimum storage size of [**20KB for nvram and 200-20000 records for memory-buffer**].
NDcPP30e:FAU_STG_EXT.1.5
The TSF shall [***overwrite previous audit records according to the following rule: [events are written to a circular buffer and oldest events are overwritten first]***] when the local storage space for audit data is full.
NDcPP30e:FAU_STG_EXT.1.6
The TSF shall provide the following mechanisms for administrative access to locally stored audit records [***ability to view locally***].

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP30e:FCS_CKM.1)

NDcPP30e:FCS_CKM.1.1
The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [
- RSA schemes using cryptographic key sizes of [2048-bits, 3072-bits] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1,
- ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4, or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.,
- 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]].(TD0921 applied)

5.1.2.2 Cryptographic Key Establishment (NDcPP30e:FCS_CKM.2)

NDcPP30e:FCS_CKM.2.1
The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 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 [groups listed in RFC 3526]].

5.1.2.3 Cryptographic Key Destruction (NDcPP30e:FCS_CKM.4)

NDcPP30e:FCS_CKM.4.1

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

- For plaintext keys in volatile storage, the destruction shall be executed by a [
  - ***single overwrite consisting of [***
    - ***zeroes,***

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

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP30e:FCS_COP.1/DataEncryption)

NDcPP30e:FCS_COP.1.1/DataEncryption

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

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP30e:FCS_COP.1/Hash)

NDcPP30e:FCS_COP.1.1/Hash

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

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP30e:FCS_COP.1/KeyedHash)

NDcPP30e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [**256 bits, 384 bits, 512 bits**] and message digest sizes [***256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP30e:FCS_COP.1/SigGen)

NDcPP30e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [***RSA Digital Signature Algorithm***] and cryptographic key sizes [***For RSA [2048, 3072 bits]***] that meet the following:

[***- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3***]. (TD0921 applied)

5.1.2.8 NTP Protocol (NDcPP30e:FCS_NTP_EXT.1)

NDcPP30e:FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [***NTP v3 (RFC 1305***].

NDcPP30e:FCS_NTP_EXT.1.2
The TSF shall update its system time using [***Authentication using [SHA256] as the message digest algorithm(s);***].

NDcPP30e:FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

NDcPP30e:FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.1.2.9 Random Bit Generation - per TD0990 (NDcPP30e:FCS_RBG_EXT.1)

NDcPP30e:FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP30e:FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***one] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to [***the greatest security strength according to ISO/IEC 18031:2011 Table C.2 — "Security strengths, Entropy and Seed length requirements for the AES-128, 192 and 256 Block Cipher"]***. (TD0990 applied)

5.1.2.10 SSH Protocol - per TD0967 & TD1023 (SSH10:FCS_SSH_EXT.1)

SSH10:FCS_SSH_EXT.1.1
The TOE shall implement SSH acting as a [***server***] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [***4344, 6187, 6668, 8268, 8308, 8332, 8731***] and no other standard.

SSH10:FCS_SSH_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [
'password' (RFC 4252),
'publickey' (RFC 4252): [
ssh-rsa (RFC 4253),
x509v3-rsa2048-sha256 (RFC 6187)]]
and no other methods.

SSH10:FCS_SSH_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**262,126**] in an SSH transport connection are dropped.

SSH10:FCS_SSH_EXT.1.4
The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [***aes128-ctr (RFC 4344), aes256-ctr (RFC 4344), aes128-cbc (RFC 4253), aes256-cbc (RFC 4253)***] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.5
The TSF shall protect data in transit from modification, deletion, and insertion using: [***hmac-sha2-256 (RFC 6668), hmac-sha2-512 (RFC 6668)***] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.6
The TSF shall establish a shared secret with its peer using: [
diffie-hellman-group16-sha512 (RFC 8268),

diffie-hellman-group18-sha512 (RFC 8268)]
and no other mechanisms.

SSH10:FCS_SSH_EXT.1.7
The TSF shall use SSH KDF as defined in [***RFC 4253 (Section 7.2***] to derive the following cryptographic keys from a shared secret: session keys.

SSH10:FCS_SSH_EXT.1.8
The TSF shall ensure that [***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.

5.1.2.11 SSH Protocol - Server - per TD0682 (SSH10:FCS_SSHS_EXT.1)

SSH10:FCS_SSHS_EXT.1.1
The TSF shall authenticate itself to its peer (SSH Client) using: [
ssh-rsa (RFC 4253),
x509v3-rsa2048-sha256 (RFC 6187)].

5.1.2.12 TLS Client Protocol (NDcPP30e:FCS_TLSC_EXT.1)

NDcPP30e:FCS_TLSC_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] supporting the following ciphersuites: [***[***
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (only for Radius),
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]]
and no other ciphersuites.

NDcPP30e:FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 Section 6***].

NDcPP30e:FCS_TLSC_EXT.1.3
The TSF shall not establish a trusted channel if the server certificate is invalid: [***without any administrator override mechanism.***].

NDcPP30e:FCS_TLSC_EXT.1.4
The TSF shall [***present the Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096] and no other curves/groups***] in the Client Hello.[1]

NDcPP30e:FCS_TLSC_EXT.1.5
The TSF shall [
present the signature_algorithms extension with support for the following algorithms: [
rsa_pkcs1 with sha256(0x0401),
rsa_pkcs1 with sha512(0x0601)],
and no other algorithms].

NDcPP30e:FCS_TLSC_EXT.1.6
The TSF [***provides, does not provide***] the ability to configure the list of supported ciphersuites as defined in NDcPP30e:FCS_TLSC_EXT.1.1.

NDcPP30e:FCS_TLSC_EXT.1.7
The TSF shall prohibit the use of the following extensions:
- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

NDcPP30e:FCS_TLSC_EXT.1.8
The TSF shall [

[1] Radius over TLS does not present the Supported Groups Extension.

- ***not use PSKs***].

NDcPP30e:FCS_TLSC_EXT.1.9

The TSF shall [***support TLS 1.2 secure renegotiation through use of the 'renegotiation_info' TLS extension in accordance with RFC 5746***].

Application Note: The TOE supports two TLSC channels, syslog and radius. The syslog channel allows configuration of the TLS ciphers, while the radius channels does not. Both “provides” and “does not provide” have been claimed in FCS_TLSC_EXT.1.6 to reflect this.

5.1.2.13 TLS Client Support for Mutual Authentication (NDcPP30e:FCS_TLSC_EXT.2)

NDcPP30e:FCS_TLSC_EXT.2.1

The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP30e:FIA_AFL.1)

NDcPP30e:FIA_AFL.1.1

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

NDcPP30e:FIA_AFL.1.2

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

5.1.3.2 Password Management (NDcPP30e:FIA_PMG_EXT.1)

NDcPP30e:FIA_PMG_EXT.1.1

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')'***];
b) Minimum password length shall be configurable to between [**1**] and [**32**] characters.

5.1.3.3 Protected Authentication Feedback (NDcPP30e:FIA_UAU.7)

NDcPP30e:FIA_UAU.7.1

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

5.1.3.4 User Identification and Authentication (NDcPP30e:FIA_UIA_EXT.1)

NDcPP30e:FIA_UIA_EXT.1.1

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

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

NDcPP30e: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.

NDcPP30e:FIA_UIA_EXT.1.3

The TSF shall provide the following remote authentication mechanisms [***SSH password, SSH***

public key, X.509 certificate] and ***[external authentication server]***] and local authentication mechanisms [***password-based, [Radius authentication]***]. (TD0900 applied)

NDcPP30e:FIA_UIA_EXT.1.4

The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in NDcPP30e:FIA_UIA_EXT.1.3.

5.1.3.5 X.509 Certificate Validation (NDcPP30e:FIA_X509_EXT.1/Rev)

NDcPP30e: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 [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- 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 DTLS/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 DTLS/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.

NDcPP30e:FIA_X509_EXT.1.2/Rev

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

5.1.3.6 X.509 Certificate Authentication (NDcPP30e:FIA_X509_EXT.2)

NDcPP30e:FIA_X509_EXT.2.1

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

NDcPP30e:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***allow the Administrator to choose whether to accept the certificate in these cases***].

5.1.3.7 X.509 Certificate Requests (NDcPP30e:FIA_X509_EXT.3)

NDcPP30e:FIA_X509_EXT.3.1

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

NDcPP30e:FIA_X509_EXT.3.2

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (NDcPP30e:FMT_MOF.1/ManualUpdate)

NDcPP30e:FMT_MOF.1.1/ManualUpdate

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

5.1.4.2 Management of TSF Data (NDcPP30e:FMT_MTD.1/CoreData)

NDcPP30e:FMT_MTD.1.1/CoreData

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

5.1.4.3 Management of TSF Data (NDcPP30e:FMT_MTD.1/CryptoKeys)

NDcPP30e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Specification of Management Functions - per TD0880 (NDcPP30e:FMT_SMF.1)

NDcPP30e: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 remote 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; [
- ***Ability to modify the behavior of the transmission of audit data to an external IT entity,***
- ***Ability to manage the cryptographic keys,***
- ***Ability to configure the cryptographic functionality,***
- ***Ability to configure thresholds for SSH rekeying,***
- ***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,***
- ***Ability to manage the trusted public keys database***].

(TD0880 applied)

5.1.4.5 Restrictions on Security Roles (NDcPP30e:FMT_SMR.2)

NDcPP30e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP30e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP30e:FMT_SMR.2.3

The TSF shall ensure that the conditions

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

are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP30e:FPT_APW_EXT.1)

NDcPP30e:FPT_APW_EXT.1.1
The TSF shall store administrative passwords in non-plaintext form.
NDcPP30e:FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of TSF Data (for reading of all symmetric keys) (NDcPP30e:FPT_SKP_EXT.1)

NDcPP30e:FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.5.3 Reliable Time Stamps (NDcPP30e:FPT_STM_EXT.1)

NDcPP30e:FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.
NDcPP30e:FPT_STM_EXT.1.2
The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server,***].

5.1.5.4 TSF testing - per TD0836 (NDcPP30e:FPT_TST_EXT.1)

NDcPP30e:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests:
- During initial start-up (on power on) to verify the integrity of the TOE firmware and software
- Prior to providing any cryptographic service and [***at no other time***] to verify correct operation of cryptographic implementation necessary to fulfil the TSF
- [***no other***] self-tests [**none**]

to demonstrate the correct operation of the TSF.
(TD0836 applied)
NDcPP30e:FPT_TST_EXT.1.2
The TSF shall respond to [***all failures***] by [***rebooting***].

5.1.5.5 Trusted update (NDcPP30e:FPT_TUD_EXT.1)

NDcPP30e:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***the most recently installed version of the TOE firmware/software***].
NDcPP30e:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].
NDcPP30e:FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP30e:FTA_SSL.3)

NDcPP30e:FTA_SSL.3.1
The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.6.2 User-initiated Termination (NDcPP30e:FTA_SSL.4)

NDcPP30e:FTA_SSL.4.1
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.6.3 TSF-initiated Session Locking (NDcPP30e:FTA_SSL_EXT.1)

NDcPP30e:FTA_SSL_EXT.1.1
The TSF shall, for local interactive sessions, [***selection: lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator re-authenticate to the TSF prior to unlocking the session, terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.6.4 Default TOE Access Banners (NDcPP30e:FTA_TAB.1)

NDcPP30e:FTA_TAB.1.1
Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel (NDcPP30e:FTP_ITC.1)

NDcPP30e:FTP_ITC.1.1
The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***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.

NDcPP30e:FTP_ITC.1.2
The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

NDcPP30e:FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server, authenticating to a Radius server**].

5.1.7.2 Trusted Path (NDcPP30e:FTP_TRP.1/Admin)

NDcPP30e:FTP_TRP.1.1/Admin
The TSF shall be capable of using [***SSH***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP30e:FTP_TRP.1.2/Admin
The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP30e:FTP_TRP.1.3/Admin

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

5.2 TOE Security Assurance Requirements

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

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

Table 5-3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

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

ADV_FSP.1.1c

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

ADV_FSP.1.2c

The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

ADV_FSP.1.3c

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

ADV_FSP.1.4c

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

ADV_FSP.1.1e

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

ADV_FSP.1.2e

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

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

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

AGD_OPE.1.2c
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c
The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c
The operational user guidance shall be clear and reasonable.

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

5.2.2.2 Preparative Procedures (AGD_PRE.1)

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

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

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

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

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

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

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

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

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

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

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

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

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

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

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

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

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

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

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

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

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

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

AVA_VAN.1.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e
The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

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

6.1 Security audit

The TOE has the capability to generate audit records. For each audit captured, the generated record contains: the date and time, the type of event, the subject identity (e.g. IP address or User Name), and the outcome.

The TOE implements configurable audit filters, with a global filter called DefaultFilter that provides the defining default audit behavior for all targets. Authorized administrators can add, remove, or apply different filters for each target. The TOE implements the following audit targets, each with its own unique behavior:

Target	Description
console	Local CLI
session	Remote CLI
memory-buffer	Volatile local storage, wiped on reboot
nvram	Non-volatile local storage
syslog	External audit storage

Table 6-1 Audit Targets

The TOE categorizes audit records by severity levels as follows: critical, error, warning, notice, informational and extended debugging. By default, the memory-buffer and syslog targets are configured to capture log information at levels debug-data through critical, while nvram captures log information at levels warning through critical. An authorized administrator can configure log information levels and apply filters using the configure log target command.

The TOE is a standalone TOE that stores audit data locally and can also export all logs to an external audit server. The audit trail consists of individual audit records, with a unique audit record generated for each event that occurred. An administrator-configurable number of log messages can be stored locally on the appliance. Approximately, 20KB for nvram and 200-20000 records for memory-buffer can be stored locally. All local audit records exist in a circular buffer, FIFO manner; when the buffer gets full, the oldest message is overwritten first. There is no access to audit data storage; the CLI allows displaying of logs but there is no access to log files. Only Security Administrators can view the audit records. In this way, the audit records are protected against unauthorized access and deletion. Clearing the local audit trail is done per target and it wipes all audit records for that target.

The transmission of audit logs to the external audit server is done in real time, with audit records transferred as they are generated. If the connection to the external audit server is lost, the TOE continues to save local audit logs so there is no loss of audit. There is automated log reconciliation process (syncing) between the locally stored records with the external audit server upon the re-establishment of the connection.

The TOE audits the following administrative tasks related to cryptographic keys and certificates:

- Association of a public RSA key with an administrative identity
- Installation of a trusted authority certificate
- Generation of a CSR and import of a signed TOE certificate
- Generation of a TOE's RSA key pair

In the audit logs, the X509 certificates are identified by “CN” and RSA keys by a hash.

The Security audit function satisfies the following security functional requirements:

- NDcPP30e:FAU_GEN.1: The TOE can generate all the required auditable events as specified in **Error! Reference source not found.**. Within each audit event is date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 6-1 Audit Targets**. For cryptographic keys, the act of generating, importing, changing or deleting a key is audited by key name and the associated administrator account is identified.
- NDcPP30e:FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- NDcPP30e:FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with the use of TLS.

6.2 Cryptographic support

All cryptography is implemented using the Extreme Networks Cryptographic Provider 3, version 3.0.10 with KP_1.2. The following Cryptographic Algorithm Validation Program (CAVP) certificates are applicable to the TOE.

Functions	Requirement	Standard	Cert #
Encryption/Decryption			
AES CBC (128 and 256 bits)	NDcPP30:FCS_COP.1/ DataEncryption	FIPS Pub 197 ISO 10116	A5892
AES CTR (128 and 256 bits)	NDcPP30:FCS_COP.1/ DataEncryption	FIPS Pub 197 ISO 10116	A5892
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512 (digest sizes 160, 256, 384,512)	NDcPP30:FCS_COP.1/ Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A5892
Keyed-hash message authentication			
HMAC-SHA-256, HMAC_SHA-384, HMAC-SHA-512 (digest sizes 256, 384, 512)	NDcPP30:FCS_COP.1/ KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A5892
Cryptographic signature services			
RSA Digital Signature Algorithm (modulus 2048, 3072)	NDcPP30:FCS_COP.1/ SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A5892
Random bit generation			
CTR_DRBG with SW based noise sources with a minimum of 256 bits of non-determinism	NDcPP30: FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A5892
Key Generation			
RSA Key Generation (2048, 3072 bit)	NDcPP30:FCS_CKM.1	FIPS Pub 186-4	A5892
ECDSA Key Generation with Curves P-256, P-384 and P-521		FIPS Pub 186-4	A5892
FFC Scheme using Safe Primes		NIST SP 800-56A Rev 3	Tested with known good implementation
Key Establishment			
ECC Key Establishment with Curves P-256, P-384 and P-521	NDcPP30:FCS_CKM.2	NIST SP 800-56A Rev 3	A5892
FFC Schemes using safe-prime groups		NIST SP 800-56A Rev 3	Tested with known good implementation

Table 6-2: Algorithm Certificates

The TSF supports RSA key generation scheme using cryptographic key sizes of 2048 bit or greater that meet the FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3; standard. The TSF also supports ECDSA (appendix B.4), and FFC schemes using 'safe-prime' groups that meet NIST SP 800-56A Revision 3 and RFC 3526. The key pairs can be used to generate a Certificate Signing Request (CSR).

In support of secure cryptographic protocols, the TOE supports key establishment schemes, including:

- RSA key establishment as specified in Section 7.2 of RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,
- ECC key establishment as specified in NIST SP 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 SP 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and groups listed in RFC 3526.

The TOE is fully compliant with the recommendations outlined in the schemes listed above.

The following table outlines key establishment schemes used in the TOE:

Scheme	SFRs	Service
ECC	FCS_TLSC_EXT.1	Remote Audit Server (client)
RSA	FCS_SSHS_EXT.1	Remote Administration (server)
FFC	FCS_TLSC_EXT.1 FCS_SSHS_EXT.1	Remote Audit Server (client) Remote Administration (server)

Table 6-3: Key Establishment Schemes

The TOE is designed to destroy Critical Security Parameters (CSPs) when no longer required for use to mitigate the possibility of disclosure. Volatile memory (RAM) is cleared with overwriting zeros. Non-volatile EEPROM, is destructed with overwrite consisting of zeros. For non-volatile flash memory, destruction is done by direct overwrite consisting of zeros. The table below describes each type of plaintext key material and its origin and storage location and the method of zeroization.

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP1	SSH Server Private Key	RSA	RSA based host private key. SSH session establishment	NVRAM, RAM (plain text), FLASH	The following are done upon execution of the "unconfigure switch all/erase" command. • The Key in NVRAM is zeroized by overwriting it with zeros. • The Key in RAM is zeroized by memset with 0. Keys are stored in FLASH temporarily. Once it is loaded into RAM, a key stored in FLASH- is zeroized.
CSP2	SSH Server Public Key	RSA	RSA based host public key. SSH session establishment	RAM (plain text)	Zeroized by memset with 0 upon execution of the "unconfigure switch all/erase" command. No read verification is done. Keys are stored in FLASH temporarily. Once it is loaded into RAM, a key stored in FLASH- is zeroized.
CSP3	SSH Session Keys	Generated using SSH KDF	SSH keys – server to client, client to server	RAM (plain text)	Session keys are cleared with 0x00 on session termination.

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP4	Diffie-Hellman shared secret	DH	Key agreement for SSH sessions	RAM (plain text)	Overwritten with zeroes after being used by the consuming application
CSP5	Diffie-Hellman private and public parameters	DH	Key agreement for SSH sessions	RAM (plain text)	Overwritten with zeroes after key exchange completion
CSP6	TLS Client key	X509v3	TLS session establishment	NVRAM	Zeroized upon execution of the “unconfigure switch erase” command
CSP7	Administrative Passwords	AES-CBC	Credentials used to authenticate the administrator login.	FLASH (ciphertext)	Encrypted passwords exist locally in a startup configuration file and are replaced when that file is edited and saved. The passwords are stored in the file in protected form only. Overwritten with zeroes when the “unconfigure switch erase” command is run
CSP8	PRNG Seed key	/dev/random	Seed key for PRNG	RAM (plain text)	Cleared when device is powered down or during reboot by the new seed.

Table 6-4: Platforms CSPs

The TOE uses SSH for to facilitate secure remote administrative sessions (CLI). The TOE's SSH implementation supports the following:

- Use of 2048-bit RSA keys in support of SSH_RSA for public key-based authentication;
- Dropping SSH packets greater than 262126 bytes. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet;
- Strict compliance with RFCs 4251, 4252, 4253, 4254, 4344, 6187, 6668, 8268, 8308, 8332, and 8731.
- No options included in the RFCs have been implemented;
- Encryption algorithms aes128-cbc, aes256-cbc, aes128-ctr and aes256-ctr to ensure confidentiality of the session;
- Password based authentication;
- Public key-based authentication. The TOE ensures and verifies that the SSH client's presented public key matches one that is stored within the TOE's SSH server's authorized keys database;
- Hashing algorithm hmac-sha2-256, and hmac-sha2-512 to ensure the integrity of the session;
- Enforcement of diffie-hellman-group16-sha512, diffie-hellman-group18-sha512 as allowed key exchange methods.
- SSH session rekey limits are administrator configurable such that an SSH connection is rekeyed before 60 minutes of connection time or 1 GB of data traffic, whichever threshold is met first.

The TOE exclusively supports TLS v1.2 secure communication protocol that complies with RFC 5246. The TOE supports mutual X509v3 certificate-based authentication and the following ciphers by default in FIPS mode (non-configurable):

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The TOE implements reference identifier matching according to RFC 6125. The reference identifier is specified during configuration of the TLS connection. Supported reference identifiers are DNS names for the SAN and CN. As part of negotiating TLS connections, the TOE will verify that the peer certificate's Subject Alternative Name (SAN) or Common Name (CN) contains the expected identifier. The CN is checked only if the SAN is absent. The TOE only establishes a connection if the peer certificate is valid, trusted, and has a matching reference identifier and if the revocation check passed. The TOE does not implement certificate pinning. The TOE does not support identifiers that include wildcards or IP addresses. The TOE supports X509v3 certificates as defined by RFC 5280 to mutually authenticate TLS connections. By default, the TOE presents the Elliptic Curves/ Groups Extension in the Client Hello with the following curves/groups: secp256r1, secp384r1and secp521r1.Also by default, the TOE presents the signature_algorithms extension with support for rsa_pkcs1 with sha256 and rsa_pkcs1 with sha512. The TOE supports TLS 1.2 secure renegotiation. The TOE advertises this support by signaling ciphersuite value TLS_EMPTY_RENEGOTIATION_INFO_SCSV in the initial ClientHello message.

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP30e:FCS_CKM.1: The TOE supports asymmetric key generation using RSA, ECDSA and FFC key establishment as part of TLS and SSH as described in the section above. The TOE acts as a client for TLS (ECDSA, FFC) and a server for SSH (RSA, FFC).
- NDcPP30e:FCS_CKM.2: See FCS_CKM.1
- NDcPP30e:FCS_CKM.4: All data is cleared as identified above.
- NDcPP30e:FCS_COP.1/DataEncryption: The TOE provides symmetric encryption and decryption capabilities using AES in CBC and CTR modes (128, 256 bits). AES is implemented in support of the following protocols: TLS, and SSH.
- NDcPP30e:FCS_COP.1/Hash: The TOE supports hashing using SHA-1, SHA-256, SHA-384, and SHA-512 validated conforming to ISO/IEC 10118-3:2004. SHS hashing is used within several services including, NTP hashing, TLS, and SSH. SHA-256 is used in conjunction with RSA signatures for verification of software image integrity.
- NDcPP30e:FCS_COP.1/KeyedHash: The TOE supports keyed hash HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512 conforming to ISO/IEC 9797-2:2011 with cryptographic key sizes: 256, 384, 512 bits, message digest sizes: 256, 384, 512 bits and a 256/384/512 output MAC. The SHA256 and 384/512 algorithms have block sizes of 512 and 1024 bits respectively.
- NDcPP30e:FCS_COP.1/SigGen: The TOE supports RSA signature generation and verification according to RSASSA-PKCS1v1_5 with 2048-bit and 3072-bit key sizes utilizing SHA-1, SHA-256, SHA-512.
- NDcPP30e:FCS_NTP_EXT.1: The TOE implements the NTPv3 protocol to synchronize with an external time server. The TOE authenticates updates using an administrator-configured SHA256-based message authentication. The TOE does not synchronize based on broadcast and multicast time updates. The TOE supports configuration of multiple simultaneous time servers and follows RFC 5905 algorithm to prioritize them.
- NDcPP30e:FCS_RBG_EXT.1: The TOE implements a NIST-approved platform-based AES-CTR Deterministic Random Bit Generator (DRBG), in accordance with ISO/IEC 18031:2011. The DRBG is seeded by an entropy source that is at least 256-bit value. The TOE implements a random bit generator in support of various cryptographic operations, including, RSA key establishment schemes, Diffie-Hellman key establishment schemes and SSH session establishment. All random number generation functionality is continuously health tested as per the tests defined in section 11.3 of SP 900-90A. Any initialization or system errors during bring-up or processing of this system causes a reboot resulting in the DRBG being reseeded.
- NDcPP30e:FCS_SSH_EXT.1 and NDcPP30eFCS_SSHS_EXT.1: The TOE supports SSHv2 as described above for CLI management.

- NDcPP30e:FCS_TLSC_EXT.1: The TOE supports TLS v1.2 with the ciphersuites listed above for its syslog connections. The TOE supports two TLSC channels, syslog and radius. The syslog channel allows configuration of the TLS ciphers, while the radius channels does not.
- NDcPP30e:FCS_TLSC_EXT.2: The TOE supports mutual authentication when connecting to a syslog server using TLS.

6.3 Identification and authentication

The TOE requires any user to be identified and authenticated before any management action. In the evaluated configuration, the TOE does not allow unauthenticated configuration of the TOE's network routing/switching services and does not allow any unauthenticated management action.

A requesting user will be prompted to enter a user name and password upon establishing a successful connection. The TOE will then compare the entered credentials against the known user database. If the combinations match, the TOE will then attribute (bind) the administratively-assigned role (a predetermined group of privileges that dictate access to TOE functions) to that user for the duration of their logged-in management session.

For remote administration (implemented as a CLI over SSH) the TOE can be configured to authenticate using a public key mechanism (RSA), or a password-based mechanism. If a user attempts public key-based authentication and it succeeds, the authentication process is completed and the user is granted access. If the user fails to authenticate using a public key certificate, then the TOE falls back to password-based authentication and requires the user to enter a valid username and password. When a user attempts to authenticate using password based authentication, they are prompted to enter in a valid username and password. If the user succeeds, the authentication process is completed and the user is granted access to the command line prompt for the CLI. If the authentication process fails, then the user will be prompted to re-enter their credentials. When RSA authentication is used, the TOE checks the presented public key against its authorized keys database and verifies the user's possession of a private key by negotiating a secure channel using the public key associated with that private key.

For local administration, the CLI is accessed by connecting to the console port with the provided RJ45-to-DB9 cable. Local administration supports only password-based authentication.

Both local and remote administration also supports authentication using a remote Radius server.

Upon successful authentication, the TOE assigns an administratively defined role to the user for the duration of the user's logged-in session. The TOE facilitates all administrative actions through the CLI. Successful login is indicated by TOE offering a CLI command prompt.

A user account will be locked after an administrator-configurable (1 to 10) number of unsuccessful authentication attempts. Once the user is locked out, all further authentication attempts are reported as unsuccessful, even when correct information is provided. To regain access, the user has to wait an administrator-configurable time duration before being allowed to successfully authenticate. The TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, by distinguishing between local and remote login attempts.

The TOE supports the use of X.509v3 certificates as defined by RFC 5280 to mutually authenticate external IT entities. When a X509 certificate is presented during a TLS handshake, the TOE verifies the trust chain, performing validation of the certificates and carries out revocation checking of each certificate. The revocation check is performed by sending an OCSP request to a trusted OCSP responder and verifying the signed response. An administrator can configure the behavior, if the TOE cannot establish a connection to the OCSP Responder to determine the revocation status of a certificate. The administrator can configure the TOE to accept the certificate or not accept the certificate and in this case the session will not be established. Certificate pinning is not supported.

The TOE supports the use of X.509v3 certificates as defined by RFC 5280 to authenticate connections with authorized IT entities. When certificate-based authentication is used, the TOE validates the presented certificate, checking its chain of trust against the TOE's internal trusted store, and performs a certificate revocation check. Certificate validation includes path validation (including checking CA certificates) certificate processing (including validating the extendedKeyUsage field), and extension processing (including checking the BasicConstraints extension).

Verifying the chain of trust includes validating each certificate in the chain, verifying that the certificate path consists of trusted CA certificates, and performing revocation checks on all certificates in the path. Revocation checking is implemented using OCSP. If any part of the authentication fails, the connection is terminated at the handshake stage. Specifically, the TOE implements a mutually authenticated secure channel, using TLSv1.2, to connect to a trusted external audit server.

The TOE supports the following methods to obtain a certificate from a trusted CA

- Manually import certificates in PEM format from an external server.

Once the CA certificate is downloaded, and prior to adding it to an existing list of trusted certificates, the TOE verifies the following:

- The Basic constraints extension with the CA flag is set to true
- The Key usage extension with the “keyCertSign” bit is set
- The Certificate is not expired

All certificates are stored in a private, persistent location on the TOE. There is no direct access to stored certificates using regular interfaces.

The Identification and authentication function satisfies the following security functional requirements:

- NDcPP30e:FIA_AFL.1: The administrator can set a maximum remote login failure from 1-10 unsuccessful authentication attempts. If that is exceeded, the account is locked until a configured amount of time passes.
- NDcPP30e:FIA_PMG_EXT.1: Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”,“*”, “(“, and “)”. The minimum password length is settable by the Authorized Administrator and is configurable to between 1 and 32 characters. In the evaluated configuration, a minimum password length of 15 characters is recommended.
- NDcPP30e:FIA_UAU.7: For a local administrative session, password character entries are not echoed to the screen. For a remote administrative session, user credentials are protected by a secure channel.
- NDcPP30e:FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for the displaying a message of the day banner, without requiring a user to be identified and authenticated. The TOE uses local password-based authentication and SSH public key to login authorized administrative users remotely and locally. The TOE also supports authentication using a remote Radius server.
- NDcPP30e:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation for TLS. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.
- NDcPP30e:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the certificate is accepted or not accepted based on the configuration set by the administrator.
- NDcPP30e:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates. Once the certificate has been issued, the administrator can import the X.509v3 certificate into the TOE. This allows the TOE to determine which CA certificate(s) to use during the validation process. In order to verify the revocation status of the presented certificates Online Certificate Status Protocol (OCSP) is used. If the connection to determine the certificate validity cannot be established, the TOE does not accept the certificate.

6.4 Security management

The TOE allows remote administration via SSHv2 session and local administration via a directly connected console cable. Both remote and local administration utilize a Command-Line Interface (CLI). The CLI provides access to all management functions used to administer the TOE. The TOE requires each user to be successfully authenticated

before allowing any other action on behalf of that user. All other remote management interfaces (e.g. Secure HTTP) are not evaluated and are disabled in the evaluated configuration.

The TOE supports two separate privilege levels: User and Security Administrator. There is no way to enable a "privileged" or "supervisor" level from a User account. All of the management functions are restricted to the Security Administrators of the TOE.

A user-level account has viewing access to all manageable parameters, and changing their password, with the exception of no access to:

- The user account database
- SNMP community strings

A person with an administrator-level account can view and change all switch parameters. With this level, users can be added and deleted, and the password associated with any account name can be changed.

The term "Security Administrator" is used to refer to any administrative user with the appropriate role with sufficient privilege to perform all relevant functions. All administrators have the same permissions and all users have the same permissions. The privilege level determines the functions the user can perform.

The Security management function satisfies the following security functional requirements:

- NDcPP30e:FMT_MOF.1/ManualUpdate: The TOE does not provide automatic updates to the software version running on the TOE. The TOE restricts the ability to perform manual update to the Security Administrator. The Security Administrators can query the software version running on the TOE and can manually initiate updates.
- NDcPP30e:FMT_MTD.1/CoreData: Security management is restricted to administrators. The trust store is accessed when administrators import/remove certificates as described in the Admin Guide. The trust store is protected by default and is restricted such that only administrators have access.
- NDcPP30e:FMT_MTD.1/CryptoKeys: Only administrators can perform management operations including the command to generate and delete cryptographic keys. Administrators can also import and delete CA certificates and their keys into the trust store. All of these administrative actions on keys are described by the Admin Guide.
- NDcPP30e:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified in section 5.1.4.4.
- NDcPP30e:FMT_SMR.2: The TOE support two roles: Security Administrator and User. A user-level account has viewing access to all manageable parameters, and can change their own password. A person with an administrator-level account can view and change all switch parameters can add and delete users, and change the password associated with any account name.

6.5 Protection of the TSF

The TOE protects Critical Security Parameters (CSP) such as stored passwords and cryptographic keys so they are not directly accessible via normal administrative interfaces. All passwords are encrypted using AES256-CBC. Passwords are stored in the TOE's configuration file in encrypted format. The master key used for AES encryption of passwords is generated randomly; the salt part involved in the key generation is also random. This key is generated afresh for every usage and stored in RAM. The salt is generated using cryptographically strong pseudo-random bytes. The fixed string, salt and the cipher name (AES) are passed to OpenSSL's EVP_BytesToKey key derivation function. EVP_BytesToKey will return the derived key and initialization vector (IV) that will be used by the cipher AES-CBC to encrypt the password(s). Additionally, when login-related configuration information is accessed through regular TOE interfaces, it is obfuscated with a series of asterisks.

The TOE performs diagnostic self-tests during start-up and generates audit records to capture any failures. Some low-level critical failure modes can prevent TOE start-up, and as a result will not generate audit records. In such cases, the TOE will enter a failure mode displaying error codes, typically on the console. The TOE can be configured to reboot

or to stop with errors displayed when non-critical errors are encountered. The cryptographic module performs self-tests during startup; messages from the module are displayed on the console and audit records are generated for both successful and failed tests. These self-tests comply with the FIPS 140-2 requirements for self-testing. The module performs known-answer algorithm testing (KAT), and integrity testing. For each KAT test, the TOE uses known data as inputs into each cryptographic function, computes a cryptographic result, and compares the calculated result to the expected/known value. The integrity testing verifies the digital signature of the image (as described below) to ensure that it has not been tampered with or corrupted. These self-tests cover all anticipated modes of failure, and therefore are sufficient to ensure that the TSF operates correctly. Failure of any of the FIPS mode tests during the boot process will stop the start-up process and prompt the user to reload. For all start-up tests, successful completion is indicated by the TOE reaching operational status.

The TOE is a hardware appliance that implements a hardware-based real-time clock that is managed by the embedded OS, which also controls the exposure of administrative functions. This clock is used to produce reliable timestamps that are available for audit trail generation, synchronization with the operational environment, session inactivity checks, and certificate expiration validation. The TOE also has the option to use NTP for network time.

The TOE implements two boot partitions - primary and secondary. An authorized administrator can configure the partition that is to be used after rebooting of the TOE. Firmware updates are always installed into the inactive partition. The default patching behavior is to upload the image, verify image, install it into the inactive partition, change the boot partition, and reboot the TOE. Administrators can override this behavior but are trusted not to. Upgrading the TOE software is a multi-step process performed by a Security Administrator.

An authorized user must authenticate to the Extreme Portal website at https://extremeportal.force.com where the software downloads are available. The downloaded image must be transferred to the appliance using a method such as TFTP. The TOE image files are digitally signed using a RSA mechanism. SHA-256 is used in conjunction with RSA signatures for verification of software image integrity. The TOE uses a public key to verify the digital signature; upon successful verification of this signature the TOE will apply the new image upon rebooting. If the signature verification cannot be carried out then the installation is terminated. The digital certificate used by the update verification mechanism is contained on the TOE. The version of the software can be queried by issuing the command: “show version”.

The Protection of the TSF function satisfies the following security functional requirements:

- NDcPP30e:FPT_APW_EXT.1: No passwords are ever stored as clear text. All passwords are encrypted using AES256-CBC. Passwords are stored in the TOE’s configuration file in encrypted format.
- NDcPP30e:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- NDcPP30e:FPT_STM_EXT.1: The TOE includes its own hardware clock and can synchronize with a NTP server.
- NDcPP30e:FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics and cryptographic self-tests that will serve to ensure the TOE is functioning properly. The tests are described above.
- NDcPP30e:FPT_TUD_EXT.1: The TOE provides functions to query the version and upgrade the software embedded in the TOE appliance. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by Extreme Networks.

6.6 TOE access

The TOE implements remote and local administrative access via the CLI. The TOE’s minimum lockout value must be configured to a non-zero value to enforce an administrator-defined inactivity timeout, after which the inactive session is automatically terminated. The inactivity timeout value is between 1-240 minutes, and the default value is 20 minutes. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

The administrator can force termination of current session by issuing the logout function: exit.

The TOE will display a customizable banner when a user initiates an interactive session either locally or remotely.

The TOE access function satisfies the following security functional requirements:

- NDcPP30e:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP30e:FTA_SSL.4: The TOE provides the function to terminate both local and remote user sessions as directed by the user using the 'logout' or 'exit' command.
- NDcPP30e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- NDcPP30e:FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, allowing administrators to terminate their session prior to performing any functions.

6.7 Trusted path/channels

The TOE protects communications with an external audit server and external Radius server by establishing a trusted channel between itself and the audit/Radius server. To implement this trusted channel, the TOE uses TLS v1.2 protocol with certificate-based authentication. For certificate-based authentication, the X.509v3 certificate presented by the external audit/Radius server is first validated and then compared to the authorized certificates database.

The TOE protects remote management sessions by establishing a trusted path (using SSH) between itself and the administrator. The SSHv2 session is encrypted using AES encryption. The remote administrators are able to initiate the SSHv2 secure channel with the TOE.

The Trusted path/channels function satisfies the following security functional requirements:

- NDcPP30e:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that exported audit records or Radius authentication request are sent only to the configured server so they are not subject to inappropriate disclosure or modification. The TOE validates the audit or Radius server against the TOE configuration using the certificates presented during TLS negotiation.
- NDcPP30e:FTP_TRP.1/Admin: The TOE provides SSH to ensure secure remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP tested cryptographic operations, and all remote security management functions require the use of this secure channel.