Extreme Networks Summit Series Switches Security Target

Version 2.4

December 19, 2017

Table of Contents

Figures and Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title: Extreme Networks Summit Series Switches Security Target

ST Version: v2.4

ST Author: CygnaCom Solutions Inc.

ST Date: 12/19/2017

1.2 TOE Reference

TOE Developer: Extreme Networks

Evaluation Sponsor: Extreme Networks

TOE Identification: Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2

Table 1: TOE Platforms and Devices

Series	Platform	Build
Summit X870 Series	Summit X870-32c	EXOS v22.3.1.4-patch1CC-2
	Summit X870-96x-8c	EXOS v22.3.1.4-patch1CC-2
Summit X690 Series	Summit X690-48x-2q-4c	EXOS v22.3.1.4-patch1CC-2
	Summit X690-48t-2q-4c	EXOS v22.3.1.4-patch1CC-2
Summit X620 Series	Summit X620–16x	EXOS v22.3.1.4-patch1CC-2
	Summit X620–16t	EXOS v22.3.1.4-patch1CC-2
	Summit X620–10x	EXOS v22.3.1.4-patch1CC-2
	Summit X620–8t-2x	EXOS v22.3.1.4-patch1CC-2
Summit X440-G2 Series	Summit X440-G2-12t-10GE4	EXOS v22.3.1.4-patch1CC-2

Series	Platform	Build
	Summit X440-G2-12p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24t-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-48t-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-48p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24t-10GE4-DC	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-48t-10GE4-DC	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24x-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24fx-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-12t8fx-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X440-G2-24t-GE4	EXOS v22.3.1.4-patch1CC-2
Summit x450-G2 Series	Summit X450-G2-24t-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24p-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-48t-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-48p-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24t-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-48t-10GE4	EXOS v22.3.1.4-patch1CC-2

Series	Platform	Build
	Summit X450-G2-48p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24p-10GE4-FB-715-TAA	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-48p-10GE4-FB-1100-TAA	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24t-GE4-FB-TAA	EXOS v22.3.1.4-patch1CC-2
	Summit X450-G2-24p-GE4-FB-715-TAA	EXOS v22.3.1.4-patch1CC-2
Summit X460-G2 Series	Summit X460-G2-24t-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-48t-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-24p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-48p-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-24x-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-48x-10GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-24t-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-48t-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-24p-GE4	EXOS v22.3.1.4-patch1CC-2
	Summit X460-G2-48p-GE4	EXOS v22.3.1.4-patch1CC-2
Summit x670-G2 Series	Summit X670-G2-72x	EXOS v22.3.1.4-patch1CC-2
	Summit X670-G2-48x-4q	EXOS v22.3.1.4-patch1CC-2
	Summit X670-G2-48x-4q-FB-AC-TAA	EXOS v22.3.1.4-patch1CC-2

** These platforms include multiple appliances*

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

PP Identification: collaborative Protection Profile for Network Devices, Version 2.0, May 2017.

1.3 TOE Overview

1.3.1 *TOE Product Type*

The Target of Evaluation [TOE] is a Network Device as defined by the collaborative Protection Profile for Network Devices v2.0 [NDcPP]: “A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network”.

1.3.2 *TOE Usage*

The TOE is the Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2. In the evaluated configuration this consists of the Summit 870, Summit 690, Summit x620, Summit x440-G2, Summit x450-G2, Summit x460-G2, and Summit x670-G2 series switches. 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. 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 production environment as specified in the user guidance.

1.3.3 *TOE Security Functionality*

- Security Audit
  - Audit record generation for security-relevant events
  - Interoperability with a remote audit server
- Cryptographic Support
  - Validated cryptographic algorithms
  - Destruction of cryptographic keys
- Identification and Authentication
  - User access policies
  - Password and certificate based authentication
- Security Management
  - Local and remote administration
- Protection of the TOE Security Function (TSF)
  - Self-testing on power-up
  - Trusted update
- TOE Access
  - Role-based access control
  - Session timeout and lockout
- Trusted Path/Channels
  - Secure channel for remote administrators
  - Secure channel for authorized IT entities

1.4 TOE Description

The TOE is the Extreme Networks Summit Series Switches EXOS v22.3.1.4-patch1CC-2 that consist of Summit Series switches and includes the following appliances:

- Summit x870 Series
- Summit x690 Series
- Summit x620 Series
- Summit x440-G2 Series
- Summit x450-G2 Series
- Summit x460-G2 Series
- Summit x670-G2 Series

The TOE consists of both hardware and software components. Each software version is identifiable by the unique build number. Each hardware profile provides a defined set of performance characteristics - switching bandwidth, latency, and port density while offering the same level of security features.

Summit x870 Series
The X870 product family provides purpose-built 100Gb switches designed for high-performance enterprise and cloud data centers. With 32 QSFP28 ports, the X870 can support a range of interface speeds, including 10Gb, 25Gb, 40Gb, 50Gb and 100Gb, all in a compact 1RU form factor. This enables the Summit X870 to be flexibly deployed in either spine/leaf or high-density top of rack architectures. Low-latency cut-through switching and an advanced feature set make it ideal for high-performance data center applications.

The Summit x870 Series consists of the following switches:

Model	Specifications
Summit X870-32c	32 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports, unpopulated, 2 unpopulated power supply slots, 6 unpopulated fan module slots
Summit X870-96x-8c	96 10Gb ports on 24 QSFP28 ports, unpopulated, 8 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports, unpopulated, 2 unpopulated power supply slots, 6 unpopulated fan module slots

Summit x690 Series
The X690 product family provides purpose-built 10Gb/100Gb switches designed for high-performance enterprise and cloud data centers. The X690 can support a range of interface speeds, including 1Gb, 10Gb, 25Gb, 40Gb, 50Gb and 100Gb, all in a compact 1RU form factor. This enables Summit X690 to be flexibly deployed in either Enterprise LAN or high-density top of rack data center architectures. Low-latency cut-through switching and an advanced feature set make it ideal for high-performance data center applications.

The Summit x690 Series consists of the following switches:

Model	Specifications
Summit X690-48x-2q-4c	48 1Gb/10Gb SFP+ ports, 2 10Gb/40Gb QSFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports, unpopulated, 2 unpopulated power supply slots, 6 unpopulated fan module slots
Summit X690-48t-2q-4c	48 1Gb/10Gb 10GBASE-T ports, 2 10Gb/40Gb QSFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports, unpopulated, 2 unpopulated power supply slots, 6 unpopulated fan module slots

Summit x620 Series

The X620 product family is a compact 10Gb Ethernet switch designed for 10GB edge applications. The family includes 10-port and 16-port 10 GbE versions – all in a small 1RU form factor. These switches are ideal for high-performance workgroups requiring 10GB connectivity to servers, storage and clients. The X620 simplifies network operation with its ExtremeXOS modular operating system, used across all networking products, and supports intelligent Layer 2 switching, Layer 3 IPv4/IPv6 routing, as well as role-based policy capabilities. The high availability ExtremeXOS operating system provides operational efficiency through the use of one OS everywhere in the network.

The Summit x620 Series consists of the following switches:

Model	Specifications
Summit X620–16x	16 100Mb/1Gb/10GBASE-X SFP+ ports, 2 unpopulated power supply slots, 1 unpopulated Fan Module slot
Summit X620–16t	12 100Mb/1Gb/10GBASE-T ports with EEE, 4 100Mb/1Gb/10GBASE-T with EEE shared with 4 1Gb/10GBASE-X SFP+ ports, 2 unpopulated power supply slots, 1 unpopulated Fan Module slot
Summit X620–10x	10 100Mb/1Gb/10GBASE-X SFP+ ports, integrated power supply and fans
Summit X620–8t-2x	8 100Mb/1Gb/10GBASE-T with EEE, and 2 100Mb/1Gb/10GBASE-X SFP+ ports, integrated power supply and fans

Summit x440 Series

The X440-G2 series switches are scalable cost-effective family of edge switches powered by Extreme Networks ExtremeXOS, the OS providing continuous uptime, manageability and operational efficiency. The X440-G2 series switches provide high-performance routing and switching, flexible stacking, PoE-plus support and comprehensive security, while extending the benefits of ExtremeXOS to the campus edge.

The Summit x440 Series consists of the following switches:

Model	Specifications
Summit X440-G2-12t-10GE4	12 10/100/1000BASE-T, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-12p-10GE4	12 10/100/1000BASE-T POE+, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-24t-10GE4	24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-24p-10GE4	24 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-48t-10GE4	48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradable to 10GbE, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-48p-10GE4	48 10/100/1000BASE-T POE+, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradable to 10GbE, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-24t-10GE4-DC	24 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed DC PSU, 1 RPS port
Summit X440-G2-48t-10GE4-DC	48 10/100/1000BASE-T, 4 SFP combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+ (2 combo/2 non-combo), 2 1GbE copper combo upgradable to 10GbE, 1 Fixed DC PSU, 1 RPS port
Summit X440-G2-24x-10GE4	24 unpopulated 1000BASE-X SFP (4 combo), 4 10/100/1000 combo, 4 1GbE unpopulated SFP upgradable to 10GbE SFP+, 1 Fixed AC PSU, 1 RPS port
Summit X440-G2-24fx-GE4	24 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, 0ºC to 60ºC operation
Summit X440-G2-12t8fx-GE4	12 10/100/1000BASE-T plus 8 fixed 100BASE-FX LC connectors, 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, 0ºC to 60ºC operation
Summit X440-G2-24t-GE4	24 fixed 10/100/1000BASE-TX , 4 1GBASE-X unpopulated SFP, 1 Fixed AC PSU, 1 RPS port, 0ºC to 60ºC operation

Summit x450 Series

The Summit X450-G2 series is based on Extreme Networks ExtremeXOS, the OS provides continuous uptime, manageability and operational efficiency. Each switch offers the same high-performance, nonblocking hardware technology, in the Extreme Networks tradition of simplifying network deployments through the use of common hardware and software throughout the network.

The Summit x450 Series consists of the following switches:

Model	Specifications
Summit X450-G2-24t-GE4	10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports, 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated)
Summit X450-G2-24p-GE4	24 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports, 2 unpopulated power supply slots, fan module slot (unpopulated)
Summit X450-G2-48t-GE4	48 10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP), 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated)
Summit X450-G2-48p-GE4	48 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports, 2 unpopulated power supply slots, fan module slot (unpopulated)
Summit X450-G2-24t-10GE4	24 10/100/1000BASE-T, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports, 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated)
Summit X450-G2-24p-10GE4	24 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports), 2 unpopulated power supply slots, fan module slot (unpopulated)
Summit X450-G2-48t-10GE4	48 10/100/1000BASE-T, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports, 1 Fixed AC PSU, 1 RPS port, fan module slot (unpopulated)
Summit X450-G2-48p-10GE4	48 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports, 2 unpopulated power supply slots, fan module slot (unpopulated)
Summit X450-G2-24p-10GE4-FB-715-TAA	24 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports (QSFP), 2 power supply slots populated with 715W PS, fan module Front-to-Back
Summit X450-G2-48p-10GE4-FB-1100-TAA	48 10/100/1000BASE-T POE+, 4 10GBASE-X unpopulated SFP+, two 21Gb stacking ports (QSFP), 2 power supply slots populated with 1100W PS, fan module Front-to-Back
Summit X450-G2-24t-GE4-FB-TAA	24 10/100/1000BASE-T, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP), 1 Fixed AC PSU, 1 RPS port, fan module Front-to-Back
Summit X450-G2-24p-GE4-FB-715-TAA	24 10/100/1000BASE-T POE+, 4 1000BASE-X unpopulated SFP, two 21Gb stacking ports (QSFP), 2 power supply slots populated with 715W PS, fan module Front-to-Back

Summit x460 Series:
The Summit X460 series is based on Extreme Networks Extreme OS. Each switch offers the same high-performance, nonblocking hardware technology, in the Extreme Networks tradition of simplifying network deployments through the use of common hardware and software throughout the network.

The Summit x460 Series consists of the following switches:

Model	Specifications
Summit X460-G2-24t-10GE4	24 10/100/1000BASE-T, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-48t-10GE4	48 10/100/1000BASE-T, 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-24p-10GE4	24 10/100/1000BASE-T PoE-plus, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-48p-10GE4	48 10/100/1000BASE-T PoE-plus, 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-24x-10GE4	24 100/1000BASE-X unpopulated SFP, 8 10/100/1000BASE-T (4 10/100/1000BASE-T ports shared with SFP ports), 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-48x-10GE4	48 100/1000BASE-X unpopulated SFP, 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-24t-GE4	24 10/100/1000BASE-T, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1GBase-X unpopulated SFP ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)

Model	Specifications
Summit X460-G2-48t-GE4	48 10/100/1000BASE-T, 4 1GBaseX unpopulated SFP ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-24p-GE4	24 10/100/1000BASE-T PoE-plus, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared with 10/100/1000BASE-T ports), 4 1GBaseX unpopulated SFP ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)
Summit X460-G2-48p-GE4	48 10/100/1000BASE-T PoE-plus, 4 1GBaseX, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated)

Summit X670 Series
The Summit X670-G2-48t provides high density for 10 Gigabit Ethernet switching in a small 1RU form factor. These switches support up to 64 10GbE ports in one system and 448 10GbE ports in a stacked system which provides 160 Gbps throughput and distributed forwarding. These switches support up to 384 10GbE ports of 10GbE in a stacked system which provides 320 Gbps throughput and distributed forwarding. With its versatile design, the Summit X670 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 deployment in AC-powered and DC-powered environments. Summit X670 series simplifies network operation with the ExtremeXOS modular operating system (OS). The high availability ExtremeXOS operating system provides simplicity and ease of operation through the use of one OS everywhere in the network.

The Summit x670 Series consists of the following switches:

Model	Specifications
Summit X670-G2-72x	72 10GBASE-X SFP+, unpopulated dual PSU power slot and 5 unpopulated fan airflow slots
Summit X670-G2-48x-4q	48 10GBASE-X SFP+ and 4 40GBASE-X QSFP+, unpopulated dual PSU power slot , and 3 unpopulated fan airflow slots
Summit X670-G2-48x-4q-FB-AC-TAA	48 10GBASE-X SFP+ and 4 40GBASE-X QSFP+, 2 550W AC Power Supplies with Front-to-Back airflow, and 3 Front-to-Back airflow fan modules

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 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. Dedicated cryptographic module is integrated with protocol libraries that implement secure channel functionality. 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. System management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements administrative interface and maintains configuration information.

The figure below outlines the TOE Architecture and subsystem interactions:

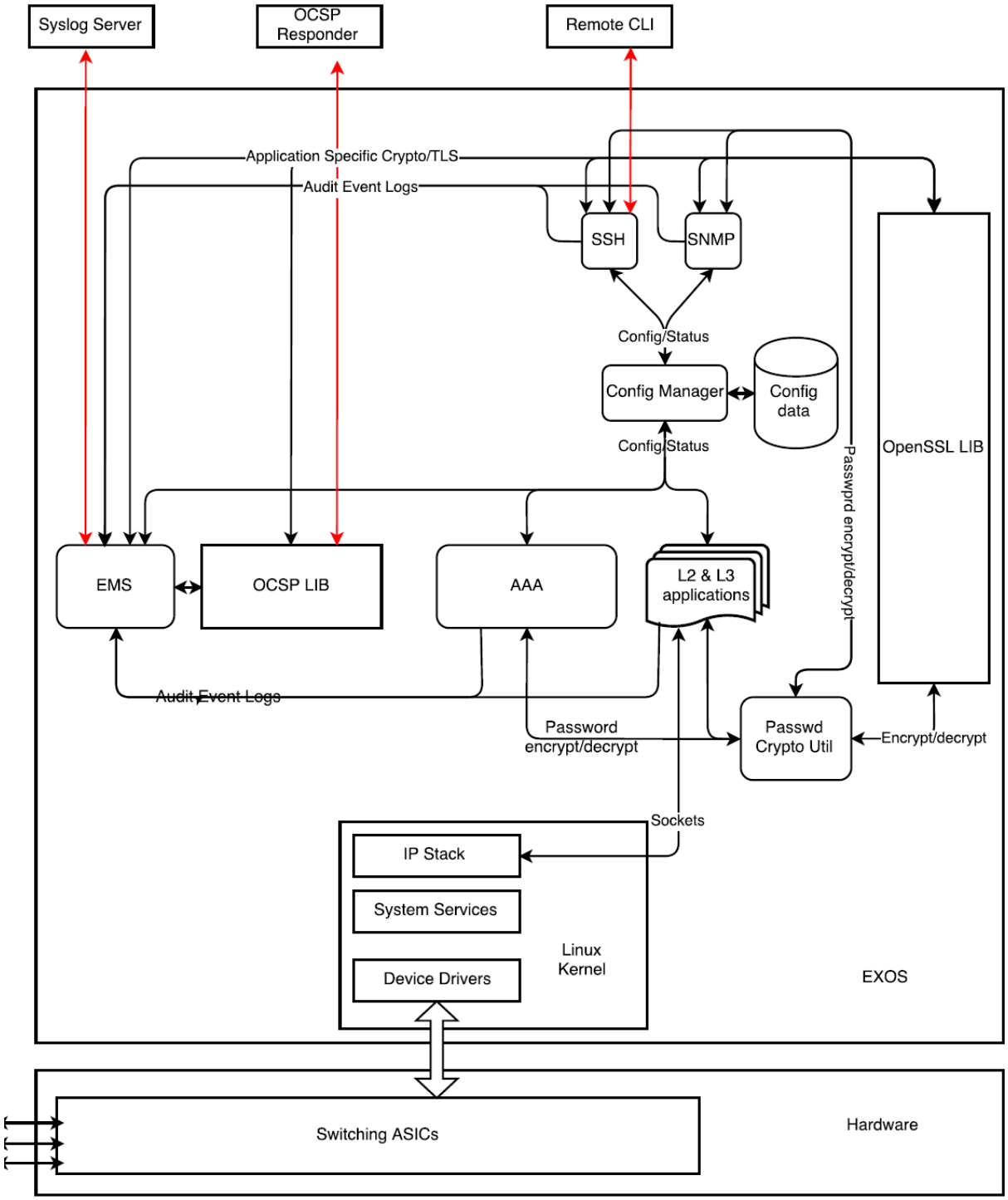

Figure 1: TOE Architecture

1.4.2 *TOE Components*

1.4.2.1 Hardware

The TOE consists of the following hardware:

Table 2: Extreme Networks Summit Series Switches

Model	Processor
Summit X870-32c	Intel Atom C series
Summit X870-96x-8c	Intel Atom C series
Summit X690-48x-2q-4c	Intel Atom C series
Summit X690-48t-2q-4c	Intel Atom C series
Summit X620–16x	Cavium Octeon II
Summit X620–16t	Cavium Octeon II
Summit X620–10x	Cavium Octeon II
Summit X620–8t-2x	Cavium Octeon II
Summit X440-G2-12t-10GE4	Cavium Octeon II
Summit X440-G2-12p-10GE4	Cavium Octeon II
Summit X440-G2-24t-10GE4	Cavium Octeon II
Summit X440-G2-24p-10GE4	Cavium Octeon II
Summit X440-G2-48t-10GE4	Cavium Octeon II
Summit X440-G2-48p-10GE4	Cavium Octeon II
Summit X440-G2-24t-10GE4-DC	Cavium Octeon II
Summit X440-G2-48t-10GE4-DC	Cavium Octeon II
Summit X440-G2-24x-10GE4	Cavium Octeon II
Summit X440-G2-24fx-GE4	Cavium Octeon II
Summit X440-G2-12t8fx-GE4	Cavium Octeon II
Summit X440-G2-24t-GE4	Cavium Octeon II
Summit X450-G2-24p-GE4	Cavium Octeon II
Summit X450-G2-48t-GE4	Cavium Octeon II
Summit X450-G2-48p-GE4	Cavium Octeon II
Summit X450-G2-24t-10GE4	Cavium Octeon II
Summit X450-G2-24p-10GE4	Cavium Octeon II
Summit X450-G2-48t-10GE4	Cavium Octeon II
Summit X450-G2-48p-10GE4	Cavium Octeon II

Model	Processor
Summit X450-G2-24p-10GE4-FB-715-TAA	Cavium Octeon II
Summit X450-G2-48p-10GE4-FB-1100-TAA	Cavium Octeon II
Summit X450-G2-24t-GE4-FB-TAA	Cavium Octeon II
Summit X450-G2-24p-GE4-FB-715-TAA	Cavium Octeon II
Summit X460-G2-24t-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-48t-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-24p-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-48p-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-24x-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-48x-10GE4	Cavium Octeon II – 2 core
Summit X460-G2-24t-GE4	Cavium Octeon II – 2 core
Summit X460-G2-48t-GE4	Cavium Octeon II – 2 core
Summit X460-G2-24p-GE4	Cavium Octeon II – 2 core
Summit X460-G2-48p-GE4	Cavium Octeon II – 2 core
Summit X670-G2-72x	Cavium Octeon II - 4 Core
Summit X670-G2-48x-4q	Cavium Octeon II - 4 Core
Summit X670-G2-48x-4q-FB-AC-TAA	Cavium Octeon II - 4 Core

1.4.2.2 Software

The TOE runs EXOS 22.3.1.4-patch1CC-2. EXOS is based on Linux Kernel version 3.18.48.This software utilizes a common code base of a modular nature with only the modules applicable to the specific hardware profile initialized on any given hardware appliance.

1.4.2.3 Management Interface(s)

The EXOS is configured and managed via a text-based Command Line Interface (CLI). The CLI is accessible from a directly- connected terminal or remotely using SSH. The CLI is structured into different operating modes for security and management purposes. Different sets of commands are available in each mode, and it is possible to limit access to specific commands using permissions.

1.4.3 *Physical Boundary of the TOE*

The physical boundary of the TOE is the Extreme Networks Summit Series Switches running EXOS 22.3.1.4-patch1CC-2**,** which includes:

- The appliance hardware
- RJ-45/RS-232 management ports
- USB port
- Dedicated Ethernet management port
- Embedded software installed on the appliance
- CLI management interface

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 (optional)
- Certificate Authority and OCSP servers to support X.509 (optional)
- DNS server (optional)

The TOE Boundary is outlined in the following figure:

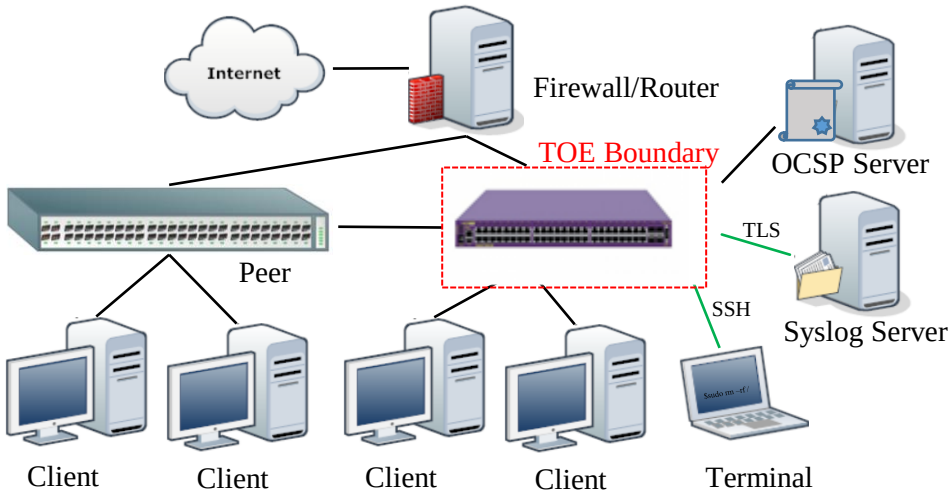

Figure 2: TOE Boundary

1.4.4 *Logical Boundary of the TOE*

The logical boundary of the TOE is defined by the implemented security functionality as summarized in Section 1.3.3 of this document.

1.4.4.1 Security Audit

The TOE generates audit records for all security-relevant events. For each audited events, 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 to built-in clock.

1.4.4.2 Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing 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.

1.4.4.3 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. 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.

1.4.4.4 Security Management

The TOE allows remote administration using an SSHv2 session over an out of band RJ-45 LAN management port, and local administration using a console via a separate RJ-45 port running RS-232 signaling for a serial connection. 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.

1.4.4.5 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.

1.4.4.6 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.

1.4.4.7 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.

1.4.5 *Excluded Functionality*

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:

- Any integration and/or communication with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control Systems (TACACS) is not evaluated.
- Any use of HTTP and HTTPS (web interface) is excluded, and the TOE's web interface is disabled by default.
- Routing protocols that integrate authentication or encryption, such as Routing Information Protocol (RIPv1, RIPv2), Open Shortest Path First (OSPFv2), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) are not evaluated. RFC-compliant implementations are unable to satisfy cryptographic requirements outlined in the PP.
- Use of the FTP server is excluded and it is disabled by default.
- Telnet is disabled in the evaluated configuration.
- The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- Virtualized EXOS is not evaluated.
- Synchronization with an external NTP server is not restricted; however, this functionality is not evaluated.
- The TOE's debug mode is not intended for normal use and is not evaluated.
- Python support is disabled in the evaluated configuration.

1.4.6 *TOE Guidance and Reference Documents*

The following user guidance documents are provided to customers and are considered part of the TOE:

Table 3: TOE Reference Documents

Reference Title	ID
ExtremeXOS User Guide for Version 22.3, published July 2017	[UG REF]
ExtremeXOS Command Reference Guide for Version 22.3, published July 2017	[CLI REF]
Extreme Networks Summit Series Switches Common Criteria Admin Guide v0.5, December 2017	[CC REF]

The documents in the following table were used as reference materials to develop this ST.

Table 4: ST Reference Documents

Reference Title	ID
Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002	[CC]
collaborative Protection Profile for Network Devices, Version 2.0, May 2017	[NDcPP]
Evaluation Activities for Network Device cPP, Version 2.0, May 2017	[SD]

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This Security Target [ST] and the Target of Evaluation [TOE] are conformant to the following Common Criteria [CC] specifications:

- *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components,* Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
- Part 2 Conformant with additional extended functional components as specified by the protection profile.
- *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components,* Version 3.1, Revision 5, April 2017, CCMB-2017-04-003
- Part 3 Conformant with additional assurance activities as specified by the protection profile.

2.2 Protection Profile Claim

The TOE claims exact compliance to collaborative Protection Profile for Network Devices, Version 2.0, May 2017 [NDcPP].

2.2.1 *Technical Decisions*

The following CCEVS technical decisions affect this evaluation:

- TD0228: NIT Technical Decision for CA certificates - basicConstraints validation

2.3 Package Claim

The TOE does not claim to be conformant with any pre-defined packages.

2.4 Conformance Rationale

This Security Target claims strict conformance to only one PP – the NDcPP and no extended packages.

The Security Problem Definition (SPD) of this ST is consistent with the statement of the SPD in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

3 Security Problem Definition

3.1 Threats

This section identifies the threats applicable to the TOE as specified in the PP.

Table 5: TOE Threats

Threat Name	Threat Definition
Communications with the Network Device	
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat Name	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
Valid Updates	
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
Audited Activity	
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
Administrator and Device Credentials and Data	
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

Threat Name	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
Device Failure	
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

3.2 Assumptions

This section identifies assumptions applicable to the TOE as specified in the PP.

Table 6: TOE Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

Assumption Name	Assumption Definition
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

This section identifies the organizational security policies applicable to the TOE as specified in the cPP.

Table 7: Organizational Security Policies

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

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its supporting environment in meeting the security needs.

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v2.0 does not define any security objectives for the TOE.

4.2 Security Objectives for the Operational Environment

This section identifies the security objectives as applicable to the operational environment as specified in the PP. These objectives

Table 8: Security Objectives for the Operational Environment

Objective Name	Environmental Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIAL_SECURE	The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

Objective Name	Environmental Security Objective Definition
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.

5 Extended Components Definition

The extended components listed in the Table 9 have been sourced from *collaborative Protection Profile for Network Devices, Version 2.0, May 2017* [NDcPP].

The extended components, as defined in Section 8.3 of *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5*, are identified by "_EXT" in the component name. NDcPP Appendix C contains the definitions for all extended components.

5.1 Extended Security Functional Components

Table 9: Extended Components

Functional Component		
1	FAU_STG_EXT.1	Protected Audit Event Storage
2	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
3	FCS_SSHS_EXT.1	SSH Server Protocol
4	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
5	FIA_PMG_EXT.1	Password Management
6	FIA_UIA_EXT.1	User Identification and Authentication
7	FIA_UAU_EXT.2	Password-based Authentication Mechanism
8	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
9	FIA_X509_EXT.2	X.509 Certificate Authentication
10	FIA_X509_EXT.3	X.509 Certificate Requests
11	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
12	FPT_APW_EXT.1	Protection of Administrator Passwords
13	FPT_TST_EXT.1	TSF Testing
14	FPT_TUD_EXT.1	Trusted Update
15	FTA_SSL_EXT.1	TSF-initiated Session Locking
16	FPT_STM_EXT.1	Extended: Reliable Time Stamps

5.2 Extended Security Functional Components Rationale

All extended security functional components are sourced directly from the NDcPP and applied verbatim. Exact compliance required by the NDcPP also mandates inclusion of all applicable extended components defined in the cPP.

6 Security Requirements

6.1 Security Functional Requirements

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 number in parenthesis placed at the end of the component. (e.g., SFR_ABC.1(**2**)). In the PP, the iteration sometimes indicated by a textual tag (e.g., SFT_ABC.1/**Text**), in such cases iteration nomenclature was copied verbatim.
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[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**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text*****.**

Note 1: Operations already performed in the NDcPP are not explicitly identified in this Security Target.

Note 2: Refinements made by the PP authors will not be identified as refinements in this ST. The “Refinement” identifier is reserved for identifying any refinements made by the ST author.

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified “_EXT” in the component name.)

The TOE security functional requirements are listed in Table 10. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the collaborative Protection Profile for Network Devices, Version 2.0, May 2017 [NDcPP].

Table 10: TOE Security Functional Components

Functional Components		
1	FAU_GEN.1	Audit Data Generation
2	FAU_GEN.2	User Identity Association
3	FAU_STG_EXT.1	Protected Audit Event Storage
4	FCS_CKM.1	Cryptographic Key Generation
5	FCS_CKM.2	Cryptographic Key Establishment
6	FCS_CKM.4	Cryptographic Key Destruction
7	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
8	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
9	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
10	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
11	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
12	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
13	FCS_SSHS_EXT.1	SSH Server Protocol
14	FIA_AFL.1	Authentication Failure Management
15	FIA_PMG_EXT.1	Password Management
16	FIA_UIA_EXT.1	User Identification and Authentication
17	FIA_UAU_EXT.2	Password-based Authentication Mechanism
18	FIA_UAU.7	Protected Authentication Feedback
19	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
20	FIA_X509_EXT.2	X.509 Certificate Authentication
21	FIA_X509_EXT.3	X.509 Certificate Requests
22	FMT_MOF.1/ManualUpdate	Manual Update
23	FMT_MTD.1/CoreData	Management of TSF Data
24	FMT_SMF.1	Specification of Management Functions
25	FMT_SMR.2	Restrictions on Security Roles
26	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
27	FPT_APW_EXT.1	Protection of Administrator Passwords
28	FPT_TST_EXT.1	TSF Testing
29	FPT_TUD_EXT.1	Trusted Update
30	FPT_STM_EXT.1	Reliable Time Stamps
31	FTA_SSL_EXT.1	TSF-initiated Session Locking
32	FTA_SSL.3	TSF-initiated Termination

Functional Components		
33	FTA_SSL.4	User-initiated Termination
34	FTA_TAB.1	Default TOE Access Banners
35	FTP_ITC.1	Inter-TSF Trusted Channel
36	FTP_TRP.1/Admin	Trusted Path

6.1.1 *Security Audit (FAU)*

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

(a) Start-up and shut-down of the audit functions;
(b) All auditable events for the not specified level of audit; and
(c) All administrative actions comprising:
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- ***[no other actions]***

(d) Specifically defined auditable events listed in ***Table 11***.

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 PP/ST, information specified in column three of ***Table 11.***

Table 11: Auditable Events (Table 2 of the NDcPP)

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.4	None	None
FCS_CKM_EXT.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_RBG_EXT.1	None	None
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.2	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.

Requirement	Auditable Events	Additional Audit Record Contents
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if "lock the session is selected)	Any attempts at unlocking of an interactive session.	None.
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment attempt.
	Termination of the trusted channel.	
	Failure of the trusted channel functions.	
FTP_TRP.1/Admin	Initiation of the trusted channel.	None.
	Termination of the trusted channel.	
	Failures of the trusted path functions.	

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

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

FAU_STG_EXT.1.3 The TSF shall ***[overwrite previous audit records according to the following rule: [the oldest message is overwritten first]]*** when the local storage space for audit data is full.

6.1.2 *Cryptographic Support (FCS)*

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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

[RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;]

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

6.1.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

[RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";

Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;

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

6.1.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

- For plaintext keys in volatile storage, the destruction shall be executed by a ***[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*.

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

FCS_COP.1.1/Data/Encryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm ***[AES used in [CBC]*** *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]]]***.

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

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

[RSA Digital Signature Algorithm (rDSA) with a key size (modulus) [2048 bits, 3072 bits]]

that meets the following:

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

6.1.2.3 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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

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

FCS_COP.1.1/KeyedHashThe TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm ***[HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512]*** and cryptographic key sizes ***[160-bit, 256-bit, 512-bit]*** and message digest sizes ***[160, 256, 512]*** bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.1.2.5 FCS_RBG_EXT.1 Random Bit Generation

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from ***[[1] software-based noise source, [1] hardware-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 of the keys and CSPs that it will generate.

6.1.2.6 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and ***[6668 and no other RFCS]***.

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than ***[262K]*** bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses ***[ssh-rsa]*** and ***[no other public key algorithms]*** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses ***[hmac-sha1, hmac-sha2-256, hmac-sha2-512]*** and ***[no other MAC algorithms]*** as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that ***[diffie-hellman-group14-sha1]*** and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

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

6.1.2.7 FCS_TLSC_EXT.2 TLS Client Protocol with authentication

FCS_TLSC_EXT.2.1 The TSF shall implement ***[TLS 1.2 (RFC 5246)]*** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246].

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125 section 6.

FCS_TLSC_EXT.2.3 The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall ***[not establish the connection]***

FCS_TLSC_EXT.2.4 The TSF shall ***[not present the Supported Elliptic Curves Extension]*** in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

6.1.3 *Identification and Authentication (FIA)*

6.1.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within ***[1-10]*** unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall ***[prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed]*.**

6.1.3.2 FIA_PMG_EXT.1 Password Management

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

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

Minimum password length shall be configurable to ***[between 1 character]*** and ***[32 characters]***.

6.1.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

Display the warning banner in accordance with FTA_TAB.1;

[no other actions]

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

6.1.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication

mechanism, ***[no other authentication mechanism(s)]*** to perform local administrative user authentication.

6.1.3.5 FIA_UAU.7 Protected Authentication Feedback

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

6.1.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using ***[the Online Certificate Status Protocol (OCSP) as specified in RFC 6960]***.

The TSF shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

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

6.1.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

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

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

6.1.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the

request: public key and ***[Common Name, Organization, Organizational Unit, Country]***.

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

6.1.4 *Security Management (FMT)*

6.1.4.1 FMT_MOF.1/ManualUpdate Functions Management of security functions behavior

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

6.1.4.2 FMT_MTD.1/CoreData Management of TSF Data

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

6.1.4.3 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using ***[digital signatures]*** capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;

[Ability to configure the reference identifier for the peer].

6.1.4.4 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions:

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

are satisfied.

6.1.5 *Protection of the TSF (FPT)*

6.1.5.1 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

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

and private keys.

6.1.5.2 FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

6.1.5.3 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests ***[during initial start-up (power-on),] at the conditions [as specified by FIPS PUB 140-2 Section 4.9.2]]*** to demonstrate the correct operation of the TSF: ***[***

Power-up self-tests:

Integrity check of the cryptographic module

Known Answer Tests (KAT) of cryptographic primitives

].

6.1.5.4 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and the ***[most recently installed version of the TOE firmware/software]***.

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

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

6.1.5.5 FPT_STM_EXT.1 Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall ***[allow the Security Administrator to set the time]***.

6.1.6 *TOE Access (FTA)*

6.1.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

[terminate the session]

after a Security Administrator-specified time period of inactivity.

6.1.6.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after a Security

Administrator-configurable time interval of session inactivity.

6.1.6.3 FTA_SSL.4 User-initiated Termination

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

6.1.6.4 FTA_TAB.1 Default TOE Access Banners

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

6.1.7 *Trusted Path/Channels (FTP)*

6.1.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using ***[TLS]*** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, ***[[no other capabilities]]*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server**].

6.1.7.2 FTP_TRP.1/Admin Trusted Path

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.

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

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

6.2 Security Assurance Requirements

6.2.1 *Security Assurance Requirements for the TOE*

This section defines the assurance requirements for the TOE. The assurance activities to be performed by the evaluator are defined in Sections 6 of the *collaborative Protection Profile for Network Devices v2.0* [NDcPP] and are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 12: Assurance Components

Assurance Class	Assurance Components	
Development	ADV_FSP.1	Basic Functional Specification
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability Survey

The following tables state the developer action elements, content and presentation elements and evaluator action elements for each of the assurance components.

Table 13: ADV_FSP.1 Basic Functional Specification

Developer action elements	
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.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
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.

Table 14: AGD_OPE.1 Operational User Guidance

Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and presentation elements	
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.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 15: AGD_PRE.1 Preparative Procedures

Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Content and presentation elements	
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.
Evaluator action elements	
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.

Table 16: ALC_CMC.1 Labeling of the TOE

Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
Evaluator action elements	
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 17: ALC_CMS.1 TOE CM Coverage

Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
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.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 18: ATE_IND.1 Independent Testing – Conformance

Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
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.

Table 19: AVA_VAN.1 Vulnerability Survey

Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
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.

6.2.2 *Security Assurance Requirements Rationale*

This ST conforms to the [NDcPP], which draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

6.3 Rationale

This ST claims Exact Compliance to the *collaborative Protection Profile for Network Devices v2.0* [NDcPP]. Therefore:

All secure usage assumptions, organizational security policies, and threats are completely covered by security objectives.

Each objective counters or addresses at least one assumption, organizational security policy, or threat.

The set of components (requirements) in the ST are internally consistent and complete.

6.3.1 *TOE SFR Dependencies*

The following table provides SFR dependency mapping. All SFRs were drawn from the [NDcPP]. For extended components that were derived from SFRs from CC Part 2 dependencies were based on unmodified SFRs, for all other extended components dependencies were determined based on Appendix C Extended Component Definitions.

Table 20: SFR Dependencies

SFR	Dependency	Rationale Statement
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1 included (which is hierarchic to FPT_STM.1)
FAU_GEN.2	FAU_GEN.1 FAU_UID.1	FAU_GEN.1 Included Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 included FTP_ITC.1 included
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	FCS_CKM.2 included FCS_CKM.4 included
FCS_CKM.2	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 included (also FTP_ITC.1 as a secure channel that could be used for import) FCS_CKM.4 included
FCS_CKM.4	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1	FCS_CKM.1 included (also FTP_ITC.1 as a secure channel that could be used for import)
FCS_COP.1/DataEncryption	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 included (also FTP_ITC.1 as a secure channel that could be used for import) FCS_CKM.4 included
FCS_COP.1/SigGen	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 included (also FTP_ITC.1 as a secure channel that could be used for import) FCS_CKM.4 included
FCS_COP.1/Hash	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 FCS_CKM.4	This SFR specifies keyless hashing operations, so initialisation and destruction of keys are not relevant

SFR	Dependency	Rationale Statement
FCS_COP.1/KeyedHash	FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 included (also FTP_ITC.1 as a secure channel that could be used for import) FCS_CKM.4 included
FCS_RBG_EXT.1	None	
FCS_SSHS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 included FCS_CKM.2 included FCS_COP.1/DataEncryption included FCS_COP.1/SigGen included FCS_COP.1/Hash included FCS_COP.1/KeyedHash included FCS_RBG_EXT.1 included
FCS_TLSC_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 included FCS_CKM.2 included FCS_COP.1/DataEncryption included FCS_COP.1/SigGen included FCS_COP.1/Hash included FCS_COP.1/KeyedHash included FCS_RBG_EXT.1 included
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator authentication
FIA_PMG_EXT.1	None	
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1 included
FIA_UAU_EXT.2	None	
FIA_UAU.7	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator authentication
FIA_X509_EXT.1/Rev	none	
FIA_X509_EXT.2	none	
FIA_X509_EXT.3	FCS_CKM.1	
FMT_MOF.1/ManualUpdate	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 included FMT_SMF.1 included

SFR	Dependency	Rationale Statement
FMT_MOF.1/AutoUpdate	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 included FMT_SMF.1 included
FMT_MTD.1/CoreData	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 included FMT_SMF.1 included
FMT_SMF.1	None	
FMT_SMR.2	FIA_UID.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification
FPT_SKP_EXT.1	None	
FPT_APW_EXT.1	None	
FPT_TST_EXT.1	None	
FPT_TUD_EXT.1	FCS_COP.1/SigGen or FCS_COP.1/Hash	FCS_COP.1/SigGen included FCS_COP.1/Hash included
FPT_TUD_EXT.2	FPT_TUD_EXT.1	FPT_TUD_EXT.1 included
FPT_STM_EXT.1	None	
FTA_SSL_EXT.1	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator authentication
FTA_SSL.3	None	
FTA_SSL.4	None	
FTA_TAB.1	None	
FTP_ITC.1	None	
FTP_TRP.1/Admin	None	

7 TOE Summary Specification

This chapter describes the security functions:

Table 21: TOE Security Functions

Security Objectives	SFR
7.1 Security Audit	FAU_GEN.1
	FAU_GEN.2
	FAU_STG_EXT.1
7.2 Cryptography	FCS_CKM.1
	FCS_CKM.2
	FCS_CKM.4
	FCS_COP.1/DataEncryption
	FCS_COP.1/SigGen
	FCS_COP.1/Hash
	FCS_COP.1/KeyedHash
	FCS_RBG_EXT.1
	FCS_SSHS_EXT.1
	FCS_TLSC_EXT.2
7.3 Identification and Authentication	FIA_AFL.1
	FIA_PMG_EXT.1
	FIA_UIA_EXT.1
	FIA_UAU_EXT.2
	FIA_UAU.7
	FIA_X509_EXT.1/Rev
	FIA_X509_EXT.2
	FIA_X509_EXT.3
7.4 Security Management	FMT_MOF.1/ManualUpdate
	FMT_MTD.1/CoreData
	FMT_SMF.1
	FMT_SMR.2
7.5 Protection of the security functionality	FPT_SKP_EXT.1
	FPT_APW_EXT.1
	FPT_TST_EXT.1
	FPT_TUD_EXT.1

Security Objectives	SFR
	FPT_STM_EXT.1
7.6 TOE access	FTA_SSL_EXT.1
	FTA_SSL.3
	FTA_SSL.4
	FTA_TAB.1
7.7 Trusted path/channels	FTP_ITC.1
	FTP_TRP.1/Admin

7.1 Security Audit

FAU_GEN.1 and FAU_GEN.2
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

The TOE categorizes audit records by severity levels as follows: critical, error, warning, notice, and informational with three severity levels for extended debugging. In log messages, these three severity levels are each indicated by four letter abbreviations.

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 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.

FAU_STG_EXT.1
The audit trail consists of individual audit records, with a unique audit record generated for each event that occurred. Administrator-configurable number of log messages can be stored locally on the appliance, and/or all logs can be sent to an external audit server. 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, CLI allows displaying of logs but there is no access to log files. Users cannot view the audit records. In this way, the audit records are protected against unauthorized access and deletion. Clearing 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 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.

7.2 Cryptography

FCS_CKM.1
The TSF supports RSA scheme using cryptographic key sizes of 2048 bit or greater.

FCS_CKM.2
The TOE follows recommendations outlined in the NIST SP 800-56B 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' requirements as part of RSA-based key establishment. However, to support RFC-compliant secure channel protocols the TOE implements NIST SP 800-135 TLS and SSH key derivation functions (KDF). TOE acts as a sender of secret keying material for RSA key establishment. The TOE uses Diffie-Hellman group 14 that meets follows RFC 3526, Section 3. Diffie-Hellman group 14 is used as part of SSH and TLS implementations.

The EXOS utilizes firmware cryptographic module based on OpenSSL. This cryptographic module exclusively implements all cryptographic functionality and operates in the FIPS mode. The cryptographic module does not include protocol key establishment functionality, NIST SP800-56B conformance is vendor affirmed. However, EXOS is separately certified for SSH and TLS KDF. The cryptographic library is capable of supporting additional, outside of the scope, cryptographic primitives but such functionality is disabled in the evaluated configuration.

The following Cryptographic Algorithm Validation Program (CAVP) certificates are applicable to the TOE:

Table 22: Extreme Networks Summit Series Switches Cryptography

Requirement Class	Requirement Component	Extreme Networks Platforms Implementation	Certificate #
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	Generating 2048-bit and 3072-bit RSA key pairs validated as conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	CAVP cert# 2725 (Intel Atom C series) CAVP cert# 2726 (Cavium Octeon II)
	FCS_CKM.2 Cryptographic Key Establishment	Key establishment according to NIST SP 800-56B Rev 1: SSH KDF conformant to SP 800-135 TLS KDF conformant to SP 800-135	CVL cert# 1590 (Intel Atom C series) CVL cert# 1591 (Cavium Octeon II)
	FCS_CKM.4 Cryptographic Key Destruction	Please refer to Table 23 for all details of key destruction.	n/a
	FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption / Decryption)	AES encryption and decryption used in CBC mode with 128-bit and 256-bit key sizes validated as conforming to ISO 18033-3 and CBC as specified in ISO 10116.	CAVP cert# 5036 (Intel Atom C Series) CAVP cert# 5037 (Cavium Octeon II)

	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	RSA signature generation and verification according to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3. Supporting 2048-bit key size and greater utilizing SHA-1 (protocol only), SHA-256, SHA-512.	CAVP cert# 2725 (Intel Atom C series) CAVP cert# 2726 (Cavium Octeon II)
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	Hashing using SHA-1, SHA-256, and SHA-512 validated as conforming to ISO/IEC 10118-3:2004.	CAVP cert#4103 (Intel Atom C series) CAVP cert#4104 (Cavium Octeon II)
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	Keyed hash HMAC-SHA1, HMAC-SHA256, and HMAC-SHA512 validated as conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2. Supported cryptographic key sizes: 160, 256, 512 bits and message digest sizes: 160, 256, 512 bits. Keyed hash use matches validated hash algorithms implemented by the cryptographic module.	CAVP cert#3358 (Intel Atom C series) CAVP cert#3359 (Cavium Octeon II)
	FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)	CTR_DRBG (AES-256) random bit generation validated as conforming to ISO/IEC 18031:2011.	CAVP cert#1857 (Intel Atom C series) CAVP cert#1858 (Cavium Octeon II)

	FCS_SSHS_EXT.1 SSH Server Protocol	The TOE implements the SSHv2 protocol and supports password-based authentication with the following ciphersuites: • AES-CBC-128, AES-CBC-256 for data encryption • SSH_RSA for public-key authentication • HMAC-SHA1, HMAC-SHA2-256, and HMAC-SHA2-512 for data integrity • diffie-hellman-group14-sha1 for key exchange	CVL cert# 1590 (Intel Atom C series) CVL cert# 1591 (Cavium Octeon II)
	FCS_TLSC_EXT.2 TLS Client Protocol	The TOE implements TLS 1.2 and supports certificate-based authentication with the following ciphersuites: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	CVL cert# 1590 (Intel Atom C series) CVL cert# 1591 (Cavium Octeon II)

FCS_CKM.4
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 done by direct overwrite consisting of zeros. Please refer to Table 23 – Extreme Networks Summit Series Switches CSPs for all of each type of plaintext key material and its origin and storage location and the method of zeroization.

Table 23: Extreme Networks Summit Series Switches Platforms CSPs

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 during unconfigure switch all/erase. • 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), FLASH	Zeroized by memset with 0 during unconfigure switch all/erase. 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.
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 on unconfigure switch erase CLI.
CSP7	Administrative Passwords	AES-CBC	Credentials used to authenticate the administrator login.	FLASH (ciphertext)	Encrypted passwords exist locally in a startup configuration file and replaced when that file is edited and saved. The passwords are stored in the file in protected form only.

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
					Overwritten with zeroes when unconfigure switch erase 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.

FCS_COP.1/DataEncryption
The TOE supports AES encryption and decryption in CBC mode with 128-bit and 256-bit key sizes validated as conforming to ISO 18033-3 and CBC as specified in ISO 10116.

FCS_COP.1/SigGen
The TOE supports RSA signature generation and verification according to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5;ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3 with 2048-bit and 3072-bit key sizes utilizing SHA-1 (protocol only), SHA-256, SHA-512.

FCS_COP.1/Hash
The TOE supports hashing using SHA-1, SHA-256, and SHA-512 validated as conforming to ISO/IEC 10118-3:2004.

FCS_COP.1/KeyedHash
The TOE supports keyed hash HMAC-SHA1, HMAC-SHA256, and HMAC-SHA512 validated as conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2. Supported cryptographic key sizes: 160, 256, 512 bits and message digest sizes: 160, 256, 512 bits. Keyed hash use matches the validated hash algorithms implemented by the cryptographic module.

FCS_RBG_EXT.1
The TOE uses a software-based pseudo-random number generator initialized with input from multiple independent entropy sources. The TOE utilizes the CTR_DRBG (AES) deterministic random bit generator that conforms to ISO/IEC 18031:2011 and is seeded with full entropy from the Linux Kernel Random Number Generator (LKRNG) operating in a blocking mode. All entropy is extracted, processed, and accumulated by LKRNG from multiple software sources based on the timing variations of internal kernel-level processes and mixed with CPU-based sources based on hardware noise generators. Accumulated entropy is not preserved across system reboots.

FCS_SSHS_EXT.1.1
The TOE implements the SSHv2 secure communication protocol that complies with RFCs 4251, 4252, 4253, 4254, 6668.

FCS_SSHS_EXT.1.2
The TOE implements SSH_RSA for public-key algorithm is used for authentication and this conforms to FCS_SSHS_EXT.1.5. Password-based authentication is also allowed.

FCS_SSHS_EXT.1.3
The TOE ensures that SSH packets that exceed 262K bytes (not including padding in the length size) are dropped at the application layer per RFC 4253.

FCS_SSHS_EXT.1.4
The TOE supports AES128-CBC, and AES256-CBC for data encryption.

FCS_SSHS_EXT.1.5
The TOE implements SSH_RSA for public-key algorithm.

FCS_SSHS_EXT.1.6
The TOE implements HMAC-SHA1, HMAC-SHA2-256 and HMAC-SHA2-512 for data integrity.

FCS_SSHS_EXT.1.7
The TOE implements diffie-hellman-group14-sha1 for key exchange.

FCS_SSHC_EXT.1.8
The TOE automatically rekeys the SSH connection after administrator-configurable thresholds. By default, the rekey happens after 60 minutes or 1 GB of data transfer, whichever happens first.

FCS_TLSC_EXT.2.1
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:
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

FCS_TLSC_EXT.2.2
The TOE implements reference identifier matching according to RFC 6125. The reference identifier specified during configuration of TLS connection. Supported reference identifiers are DNS names for the SAN and CN. The TOE does not implement certificate pinning. The TOE does not support identifiers that include wildcards.

FCS_TLSC_EXT.2.4
The TOE does not support Elliptic Curves in the evaluated configuration.

FCS_TLSC_EXT.2.5

As part of negotiating TLS connection, 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 supports X509v3 certificates as defined by RFC 5280 to mutually authenticate TLS connections.

7.3 Identification and Authentication

FIA_AFL.1
A user account would 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. Alternatively, an authorized administrator can manually unlock the user's account. 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.

FIA_PMG_EXT.1
The 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 can be configured for minimum password lengths of 15 characters.

FIA_UIA_EXT.1, FIA_UAU_EXT.2
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 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.

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.

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.

FIA_X509_EXT.1/Rev
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. If the TOE cannot establish a connection to the OCSP Responder to determine the revocation status of a certificate, it will not accept the certificate and the session will not be established. Certificate pinning is not supported.

FIA_X509_EXT.2
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 certificate path consist 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 over TFTP.

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 constrains extension with the CA flag 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.

FIA_X509_EXT.3
The TOE does not support "device specific information" within the Certificate Request Message.

7.4 Security Management

FMT_MTD.1/CoreData, FMT_SMF.1, FMT_MOF.1/ManualUpdate
The TOE allows remote administration via SSHv2 session over an out of band LAN management RJ-45 port 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 disabled in the evaluated configuration.

The TOE supports RBAC. 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 (to erase the password, use the "`unconfigure switch all`" command).

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. Specifically, the TOE restricts the ability to perform manual update to System Administrator.

FMT_SMR.1
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 (to erase the password, use the "unconfigure switch all" command).

7.5 Protection of the security functionality

FPT_SKP_EXT.1
The TOE protects Critical Security Parameters (CSP) such as stored passwords and cryptographic keys so they are not directly accessible via normal administrative interfaces.

FPT_APW_EXT.1
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.

FPT_TST_EXT.1
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, and integrity testing. These self-tests cover all anticipated modes of failure, and therefore are sufficient such 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.

FPT_STM_EXT.1
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.

FPT_TUD_EXT.1
The TOE implements two boot partitions - primary and secondary. An authorized administrator can configure the partition that is to be is 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 EXOS 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. 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 are

contained on the TOE. The version of the software can be queried by issuing the command: "`show version`".

7.6 TOE access

FTA_SSL.3
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.

FTA_SSL.4
The administrator can force termination of current session by issuing the logout function: `exit`.

FTA_TAB.1
The TOE will display a customizable banner when a user initiates an interactive session either locally or remotely.

7.7 Trusted path/channels

FTP_ITC.1
The TOE protects communications with the external audit server by establishing a trusted channel between itself and the audit 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 server is first validated and then compared to the authorized certificates database.

FTP_TRP.1/Admin
The TOE protects remote management sessions by establishing a trusted path (using SSH) between itself and the administrator connected to a dedicated RJ-45 LAN management port. When a client attempts to connect using SSHv2, the TOE and the client will negotiate the most secure algorithms available at both ends to protect the session. If the session cannot be negotiated, or the protocols cannot be agreed on, the connection is dropped. After initial connection, protocol negotiation, and key exchange, the diffie-hellman-group14-sha1 key exchange algorithm produces a shared secret that is used to derive the AES and the HMAC keys. After that point, all traffic between the TOE and the external entity is encrypted using AES-CBC-128 or AES-CBC-256 symmetric encryption algorithm. Authentication is encapsulated in this encrypted channel. For public key-based authentication, a RSA host key pair is generated by the TOE, or generated elsewhere and imported into the TOE. Client RSA public keys have to be generated elsewhere, imported into the TOE, and added to the authorized keys database.

8 Acronyms and Terminology

8.1.1 *Acronyms*

The following table defines CC and Product specific acronyms used within this Security Target.

Table 24: Acronyms

Acronym	Definition
CC	Common Criteria
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

8.1.2 *Product Acronyms and Terminology*

The following table defines the CC and Product-specific terminology used within this Security Target.

Table 25: Terminology

Terminology	Definition
AAA	Authentication, Authorization, and Accounting (AAA). A security architecture for distributing systems for controlling remote access to services.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) protocol that includes authentication and authorization.
RSA	Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman. Public-key cryptosystem algorithm.
Routing Protocol	A routing protocol is a means whereby network devices exchange information about the state of the network and used to make decision about the best path for packets to the destination.
TACACS+	Terminal Access Controller Access-Control System Plus, an access control network protocol.