Extreme Networks SLX 9640, SLX 9150 and SLX 9250 Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.6

Revision History

Revision Date	Revision	Summary of Changes
06/06/2019	1.0	Initial Release
12/02/2019	1.1	Updates/comments reply
01/24/2020	1.2	Removed 9540
03/12/2020	1.3	Joey - Merged comments from UL. Mohan – Fixed 9150 device pictures. Changed # of characters allowed in password from 96 to 90. Changed the CPU frequency from 1.5 to 2.2 GHz.
04/02/2020	1.4	Addressed review comments from UL Lab.
09/24/2020	1.5	Addressed tech review comments
06/10/2021	1.6	Addressed CMVP comments

This Extreme Networks Security Policy for Extreme Networks SLX 9640, SLX 9150 and SLX 9250 series of switches embodies Extreme Networks' confidential and proprietary intellectual property. Extreme Networks Systems retains all title and ownership in the Specification, including any revisions.

This Specification is supplied AS IS and may be reproduced only in its original entirety [without revision]. Extreme Networks makes no warranty, either express or implied, as to the use, operation, condition, or performance of the specification, and any unintended consequences it may have on the user environment.

Contents

1 Introduction 5

1.1 Module Description and Cryptographic Boundary 6
1.2 Ports and Interfaces 8
1.3 Modes of Operation 10

2 Cryptographic Functionality 10

2.1 Critical Security Parameters 14
2.2 Public Keys 15

3 Roles, Authentication and Services 16

3.1 Assumption of roles 16
3.2 Authentication Methods 16
3.3 Services 17

4 Self-Tests 20

5 Physical Security Policy 21

6 Operational Environment 21

7 Mitigation of Other Attacks Policy 21

8 Security Rules and Guidance 21

9 CO Initialization 21

10 Definitions and Acronyms 23

Table of Tables:

Table 1 – Security Level of Security Requirements 5
Table 2 – SLX Configurations 5
Table 3 – Mapping of HW/PN to 'show chassis' Output 6
Table 4 - Physical/Logical Interface Correspondence 8
Table 5 – Ports and Interfaces 9
Table 6 – Approved Algorithms 10
Table 7 – Non-Approved but Allowed Cryptographic Functions 11
Table 8 – Security Relevant Protocols Used in FIPS Mode 12
Table 9 - Non-Approved Algorithms 14
Table 10 – Critical Security Parameters (CSPs) 14
Table 11 – Public Keys 15
Table 12 - Roles and Required Identification and Authentication 16
Table 13 - Strengths of Authentication Mechanism 16
Table 14 - Service Descriptions 17
Table 15 – Unauthenticated Services 18
Table 16 - CSP Access Rights within Roles & Services 18

Table of Figures

Figure 1 - Block Diagram 6
Figure 2 –SLX Module 7

1 Introduction

This document defines the Security Policy for the Extreme Networks SLX 9640, SLX 9150 and SLX 9250 Switches, hereafter denoted as, "the Module." The Module is a Gigabit Ethernet routing network switch that provides secure network services and network management.

The FIPS 140-2 security levels for the Module are as follows:

Table 1 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall	1

The Module configurations are listed in Table 2.

Table 2 – SLX Configurations

Module	HW P/N[1]	Firmware	Description
SLX 9640	EN-SLX- 9640-24S-12C-AC-F	SLXOS 20.1.1aa	Extreme SLX 9640-24S Switch. Supports 24x1GE/10GE SFP+ ports, 12x10GE/25GE/40Gb/50GE/100GE capable QSFP28 ports, and one power supply.
	EN-SLX- 9640-24S-12C-AC-R		
SLX 9150	SLX 9150-48Y-8C-AC-F		Extreme SLX 9150-48Y Switch. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies.
	SLX 9150-48Y-8C-AC-R		
SLX 9150	SLX 9150-48XT-6C-AC-F		Extreme SLX 9150-48XT 10GBaseT Switch. Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies.
	SLX 9150-48XT-6C-AC-R		
SLX 9250	SLX 9250-32C-AC-F		Extreme SLX 9250-32C Switch. Supports 32x100GE/40GE with dual power supplies.
	SLX 9250-32C-AC-R		

[1] The module SKU#s are the HW P/Ns above appended with "AC-F" or "AC-R" suffix for fan configuration. "AC-F" indicates, AC with Front to Back Airflow and "AC-R" indicates, AC with Back to Front Airflow.

Table 3 – Mapping of HW/PN to 'show chassis' Output

Item#	HW P/N	'show chassis' output
1.	EN-SLX- 9640-24S-12C	BR-SLX9640
2.	SLX9250-32C	SLX9250-32C
3.	SLX-9150-48Y-8C	SLX9150-48Y
4.	SLX-9150-48XT-6C	SLX9150-48XT

The firmware version is: SLXOS 20.1.1aa.

1.1 Module Description and Cryptographic Boundary

The Module is a multi-chip standalone embodiment. The cryptographic boundary is the metal chassis enclosure. The physical form of the Module is depicted in the Figures below.

Figure 1 - Block Diagram

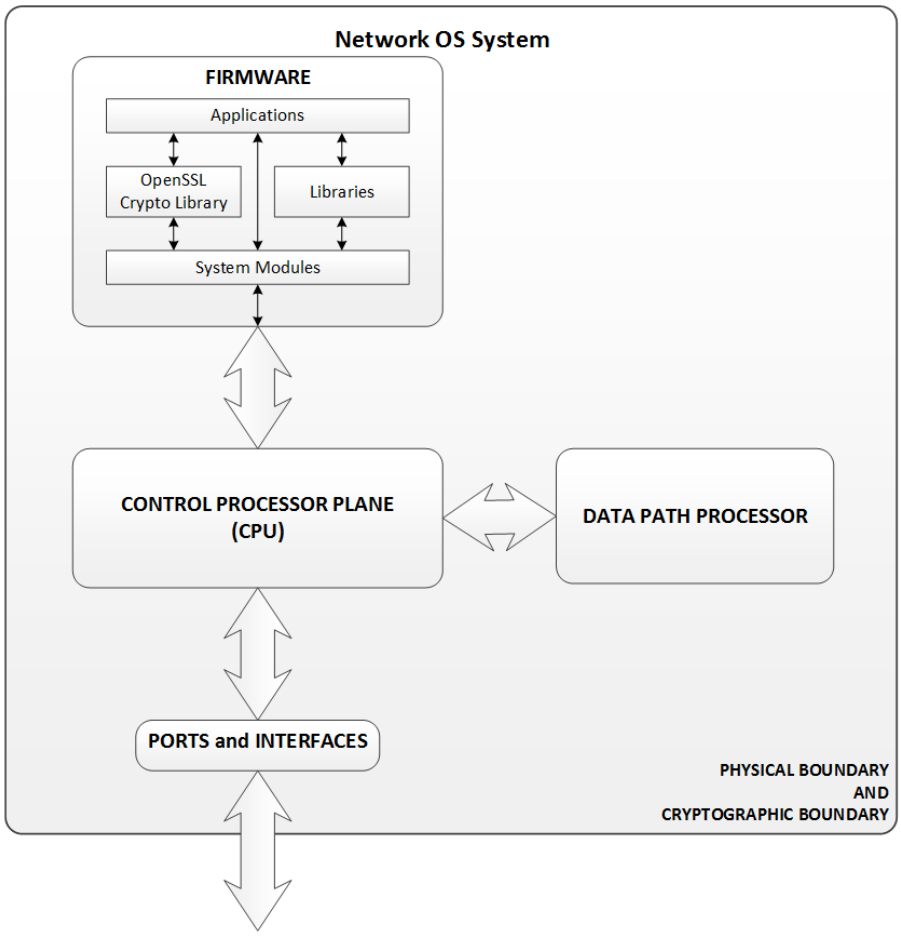
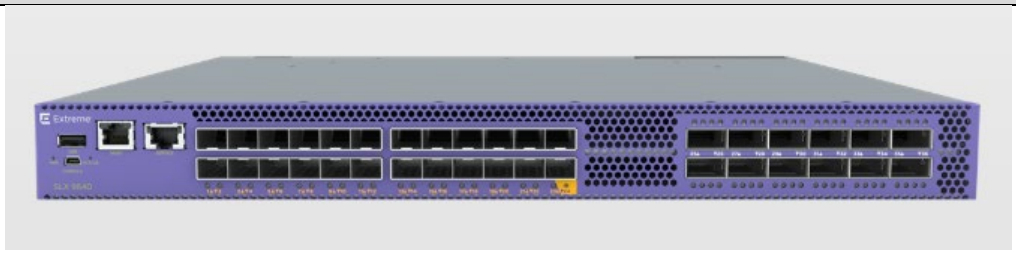
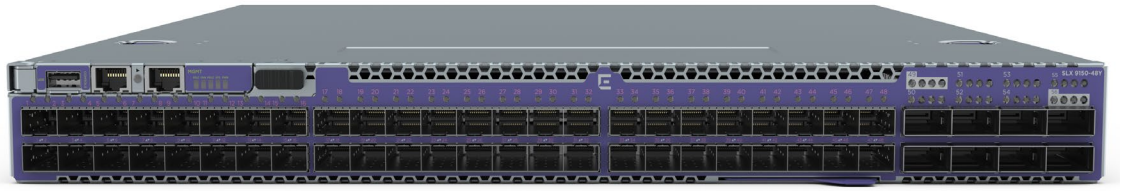


Figure 2 –SLX Module

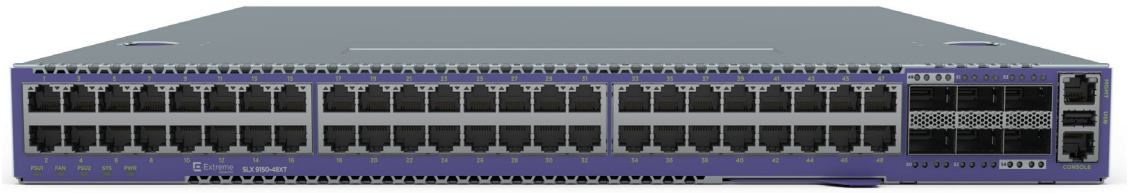
SLX 9640



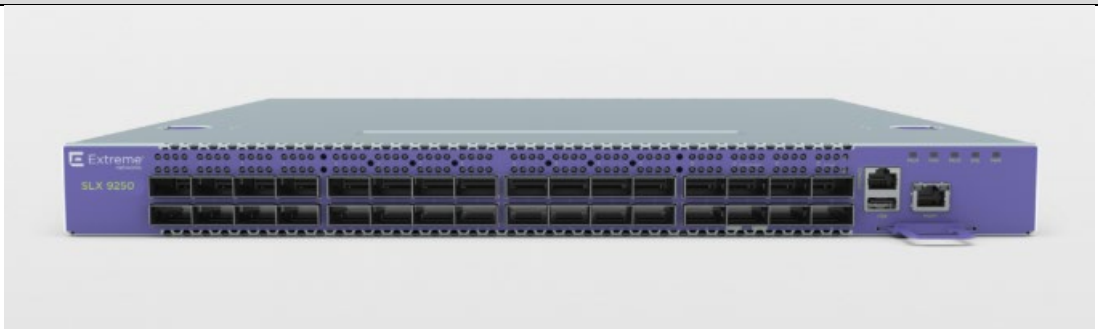
SLX 9150-48Y



SLX 9150-48XT



SLX 9250



1.2 Ports and Interfaces

Each module provides Networking ports, USB ports, Management Ethernet port, Serial port, Power Supply connectors and LEDs. This section describes the physical ports and the interfaces they provide for Data input, Data output, Control input, and Status output.

Table 4 below shows the correspondence between the physical interfaces of the modules and logical interfaces defined in FIPS 140-2.

Table 4 - Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports (including Management Ethernet port)	Data input
USB port(disabled)	
Networking ports (including Management Ethernet port)	Data output
USB port (disabled)	
Management Ethernet port	Control input
Networking ports	
Serial port	
Management Ethernet port	Status output
Serial port	
Networking ports	
USB port (disabled)	
LED	
Power Supply connector(s)	Power

Table 5 below shows the Ports and Interfaces of the modules.

Table 5 – Ports and Interfaces

Physical Interface	SLX 9640	SLX 9150-48Y	SLX 9150-48XT	SLX 9250
Networking ports	1 GbE / 10 GbE SFP+ (x24) 10GbE / 25 GbE / 40 GbE / 50GbE / 100 GbE QSFP28 (x12)	1 GbE/ 10 GbE / 25 GbE (x48) 40 GbE / 100 GbE QSFP28 (x8)	1 GbE / 10 GbE BaseT (x48) 40 GbE / 100 GbE QSFP28 (x6)	40 GbE / 100 GbE QSFP (x32)
Management Ethernet port	RJ-45 10/100/1000 Ethernet out-of-band management port (x1)	RJ-45 10/100/1000 Ethernet out-of-band management port (x1)	RJ-45 10/100/1000 Ethernet out-of-band management port (x1)	RJ-45 10/100/1000 Ethernet out-of-band management port (x1)
Serial port	RJ-45 used for console (x1)	RJ-45 used for console (x1)	RJ-45 used for console (x1)	RJ-45 used for console (x1)
USB port (Disabled in FIPS Mode)	USB used for data downloads and FW uploads (x1)	USB used for data downloads and FW uploads (x1)	USB used for data downloads and FW uploads (x1)	USB used for data downloads and FW uploads (x1)
LED	System Power (x1) System Status (x1) Status Port LEDs SFP+ Ports(x24) Status LEDs for QSFP ports (10Gb/25Gb/40Gb /50Gb/100Gb) The Ethernet LEDs are integrated with the RJ45 connector. The Power supply LEDs are integrated with the PSU.	System Power (x1) System Status (x1) Power Supply (x2) Fan (x5) Port (x48)	System Power (x1) System Status (x1) Power Supply (x2) Fan (x5) Port (x146)	System Power (x1) System Status (x1) Power Supply (x2) Fan (x4) Port (x146)
Power Supply connector(s)	Connectors (x1)	Connectors (x1)	Connectors (x1)	Connectors (x1)

1.3 Modes of Operation

The Module supports an Approved mode of operation and a non-Approved mode of operation. The initial state of the cryptographic module is the non-Approved mode of operation. The Crypto-Officer shall follow the procedures in Section 9 to initialize the module into the Approved mode of operation.

In the non-Approved mode, an operator will have no access to CSPs used within the Approved mode. When switching from the non-Approved mode of operation to the Approved-mode, the module performs zeroization of the module's plaintext CSPs as indicated in the procedure in Section 9. Failure to follow the steps outlined to enter the Approved mode will result in a non-Approved mode of operation.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 6 and 7 below. The function descriptions reflect the CAVP testing.

Table 6 – Approved Algorithms

Label	Cryptographic Function	Certificate Number
AES	FIPS 197, SP800-38A Advanced Encryption Algorithm ECB, CBC, CTR; Encrypt/Decrypt; 128, 192 and 256-bit CFB-128; Encrypt/Decrypt; 128-bit [NOTE: ECB Decrypt Mode is not used or called by any service in FIPS mode.]	C1676
CVL	SP800-135 KDF TLS TLS v1.0/1.1 and v1.2 SHA-256, 384	C1676
CVL	SP 800-135 KDF SNMP PW len: 64-128 SHA-1	C1676
CVL	SP800-135 KDF SSH (v2) AES-128, 192, 256 SHA-1, SHA-256, 384, 512	C1676
CVL	SP 800-56A KAS FFC dhEphem (Initiator & Responder) FC, SHA-256	C1676
CVL	SP800-56A KAS ECC Ephemeral Unified (Initiator & Responder) Curve: P-384, SHA-384	C1676
CVL	SP800-56A ECC CDH Primitive Curves: P-256, P-384	C1676
DRBG	SP800-90A Deterministic Random Bit Generator Mode: AES-256 CTR_DRBG (Derivation Function and Prediction Resistance Enabled)	C1676

Label	Cryptographic Function	Certificate Number
DSA	Digital Signature Algorithm FIPS 186-4 Key Gen: L = 2048, N = 256	C1676
ECDSA	FIPS 186-4 Elliptic Curve Digital Signature Algorithm FIPS 186-4 Key Gen: P-256, P-384, P-521 FIPS 186-4 PKV: P-256, P-384, P-521 FIPS 186-4 SigGen: P-256 with SHA-256, 384, 512; P-384 with SHA-256, 384, 512, P-521 with SHA-256, 384, 512 FIPS 186-4 SigVer: P-256 with SHA-256,384,512; P-384 with SHA-256, 384, 512, P-521 with SHA-256,384,512 [NOTE: SHA-512 is not used for ECDSA signature generation/verification.]	C1676
HMAC	Keyed-Hash Message Authentication code MACs: HMAC-SHA-1 (λ=96, 160), HMAC-SHA-224 (λ=224), HMAC-SHA-256 (λ=256), HMAC SHA-384(λ=320), HMAC-SHA-512 (λ=512) [NOTE: HMAC-SHA-224 is not used or called by any service in FIPS mode]	C1676
RSA	Rivest Shamir Adleman Signature Algorithm FIPS 186-4 Key Generation: RSA 2048-bit RSASSA-PKCS1_V1_5 Signature Generation: RSA 2048-bit with SHA-256, 384, 512 RSASSA-PKCS1_V1_5 Signature Verification: RSA 2048-bit with SHA-1 (legacy use only) or SHA-256, 384, 512 [NOTE: RSA 1024-bit and RSA 3072-bit is not used or called by any service in FIPS Mode. SHA—224 and SHA-512 are not used for RSA signature generation/ verification. SHA-1 is not used for RSA signature generation]	C1676
SHS	Secure Hash Algorithm Message Digests: SHA-1, SHA-256, SHA-384, SHA-512 [NOTE: SHA-224 is not used or called by any service in FIPS Mode]	C1676

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES (No Security Claimed)	[IG 1.23] Cert. #C1676 CFB-128 used to encrypt SNMPv3 packets. Non-compliant key generation use in legacy protocol.
Diffie-Hellman	[IG D.8] CVL Cert. #C1676, Key agreement; key establishment methodology provides 112 bits of encryption strength.
EC Diffie-Hellman	[IG D.8] CVL Cert. #C1676, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength

Algorithm	Description
HMAC (No Security Claimed)	[IG 1.23] SHA-1, 256, 384, or 512 used to authenticate OSPFv2/3 packets using non-compliant keys.
MD5 (No Security Claimed)	[IG 1.23] Used for User/ CO password hash and legacy use in industry protocols (Note: The use of MD5 does not provide cryptographic protection and Is considered as plaintext).
NDRNG	[IG G.13] Non-Deterministic RNG. The NDRNG output is used to seed the FIPS Approved DRBG with a minimum of 307 bits of entropy.
RSA	[IG D.9] RSA based key encapsulation; key establishment methodology provides 112 or 128 bits of encryption strength.

Table 8 – Security Relevant Protocols[1] Used in FIPS Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
SSHv2 [IG D.8 and SP 800-135]	diffie-hellman-group-exchange-sha256 (2048 bit)	RSA	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-CTR-128, AES-CTR-192, AES-CTR-256	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
	diffie-hellman-group14-sha1	RSA	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-CTR-128, AES-CTR-192, AES-CTR-256	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
	ecdh-sha2-nistp256	ECDSA P-256	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-CTR-128, AES-CTR-192, AES-CTR-256	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
	TLS_RSA_WITH_AES_128_CBC_SHA		**TLS v1.1, v1.2**	
	RSA	RSA	AES-CBC-128	SHA-1

[1] No parts of these protocols, other than the KDFs, have been tested by the CAVP and CMVP

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
TLS/ HTTPS (both client and server) [IG D.8 and SP 800-135]	**TLS_RSA_WITH_AES_256_CBC_SHA**			**TLS v1.1, v1.2**
	RSA	RSA	AES-CBC-256	SHA-1
	TLS_RSA_WITH_AES_128_CBC_SHA256			**TLS v1.2**
	RSA	RSA	AES-CBC-128	SHA-256
	TLS_RSA_WITH_AES_256_CBC_SHA256			**TLS v1.2**
	RSA	RSA	AES-CBC-256	SHA-256
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256			**TLS v1.1, v1.2**
	Static ECDH	RSA	AES-CBC-128	SHA-256
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384			**TLS v1.1, v1.2**
	Static ECDH	RSA	AES-CBC-256	SHA-384
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256			**TLS v1.1, v1.2**
	Static ECDH	ECDSA	AES-CBC-128	SHA-256
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384			**TLS v1.1, v1.2**
	Static ECDH	ECDSA	AES-CBC-256	SHA-384
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256			**TLS v1.1, v1.2**
	Ephemeral ECDH	RSA	AES-CBC-128	SHA-256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384			**TLS v1.1, v1.2**
	Ephemeral ECDH	RSA	AES-CBC-256	SHA-384
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256			**TLS v1.1, v1.2**
	Ephemeral ECDH	ECDSA	AES-CBC-128	SHA-256
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384			**TLS v1.1, v1.2**
	Ephemeral ECDH	ECDSA	AES-CBC-256	SHA-384
SNMPv3 in authPriv mode	N/A	N/A	AES-CFB-128	HMAC-SHA-1 (λ=96)

The module provides the following non-Approved algorithms only available in a non-Approved mode of operation, sorted by protocol use.

Table 9 - Non-Approved Algorithms

Crypto Function/Service	User Role Change	Additional Details
MD5	Crypto-Officer	NTP authentication key, SSH MACs: hmac-md5, hmac-md5-96, hmac-md5-etm@openssh.com
DES	Crypto-Officer	Simple Network Management Protocol. SNMPv1, SNMPv2c and SNMPv3 in noAuthNoPriv, authNoPriv mode (all Plaintext; no cryptography) Non-approved algorithms used in SNMPv3authPriv: HMAC-MD5 Modes: Not Applicable Key sizes: Not Applicable DES Modes: CBC Key sizes: 56-bits
RSA	Crypto-Officer	RSA key size 1024 bits for SSH and TLS
HTTP	Crypto-Officer	N/A – No cipher (plaintext), MD5 for auth digest
Triple-DES, blowfish, cast, arcfour, rijndael, chacha20, umac, ripemd	Crypto-Officer	Non-approved ciphers for SSH and TLS.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 10 – Critical Security Parameters (CSPs)

CSP	Description / Usage
SSHv2 DH Private Keys	2048-bit DSA keys used in SSHv2 to establish a shared secret.
SSHv2 DH Shared Secret Keys	2048-bit DH shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
SSHv2 ECDH Private Keys	P-256 private key from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys.
SSHv2 ECDH Shared Secret Keys	P-256 shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys.
SSHv2/SCP/SFTP Session Keys	AES (CBC, CTR; 128, 192, 256-bit) used to secure SSHv2/SCP/SFTP sessions.
SSHv2/SCP/SFTP Session MAC Keys	Session authentication key used to authenticate and provide integrity of SSHv2 session (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512).
Host Authentication Private Keys	ECDSA P-256, P-384, P-521 or RSA-2048, 3072 private keys used to authenticate server to client for SSH and TLS. Also, for SSH client auth.
TLS Private Key	ECDH P-256, P-384 host private key used for key establishment for a server mode TLS session.

CSP	Description / Usage
TLS Pre-Master Secret	Secret value used to establish the Session and Authentication key
TLS Master Secret	48-byte secret value used to establish the Session and Authentication key.
TLS Session Keys	128/ 256-bit AES-CBC key used to secure TLS sessions.
TLS Authentication Key	HMAC-SHA-1 and HMAC-SHA-256/384 key used to provide data authentication for TLS sessions.
DRBG Seed	384-bit output of NDRNG used to seed the SP800-90A DRBG (CTR_DRBG AES-256) with at least 307 bits of entropy.
DRBG Internal State	Internal State of SP800-90A AES-256 CTR DRBG (Key and V).
Passwords	Password used to authenticate operators (8 to 40 characters).
SNMPv3 Passphrases	Used to derive SNMPv3 auth key and SNMPv3 privacy keys (8-16 characters).
SNMPv3 auth key	Used to authenticate SNMPv3 packet using HMAC-SHA-1 (λ=96).
SNMPv3 privacy key	Used to encrypt SNMPv3 packet using AES-CFB-128.

2.2 Public Keys

Table 11 – Public Keys

Key	Description / Usage
SSHv2 DH Public Keys	2048-bit public keys used to establish shared secret (SSHv2). Used in SSHv2 KDF to derive session keys.
SSHv2 ECDH Public Keys	P-256 public keys used to establish shared secret. Used in SSHv2 KDF to derive session keys.
TLS ECDH Public Keys	P-256, P-384 public key used in TLS key agreement.
Authentication Public Keys	ECDSA P-256, P-384, P-521 or RSA-2048, 3072 peer server and client keys as well as module server and client keys for use in TLS and SSH.
Firmware Download Public Key	RSA-2048 public key used to update the FW of the module.
Syslog ROOT CA certificate	RSA-2048 public key used to authenticate Syslog server.
RADIUS ROOT CA certificate	RSA-2048 public key used to authenticate RADIUS server.

3 Roles, Authentication and Services

3.1 Assumption of roles

The cryptographic module supports two (2) operator roles. The cryptographic module shall enforce the separation of roles using role-based and identity-based operator authentication.

Thirty-two (32) concurrent operators are allowed on the Module.

Table 12 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data	Authentication Mechanism
User: User role has the permission to execute a subset of the commands via the console, SSH and HTTPS services.	Identity-based	Username and Password and PKI	Password and PKI
Admin (Crypto-Officer): Admin role has the permission to access and execute all the commands via the console, SSH and HTTPS services.	Identity-based	Username and Password and PKI	Password and PKI

3.2 Authentication Methods

Table 13 - Strengths of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Password	90 possible characters can be used with a minimum length of eight (8) characters. The probability that a random attempt will succeed, or a false acceptance will occur is 1/90^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum possible within one (1) minute is 20. The probability of successfully authenticating to the module within one minute is 20/90^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	ECDSA with at least P-256 and RSA-2048 or better with SHA-256 is used for signature verification. Both digital signatures are associated with a security strength of at least 112 bits. The probability that a random attempt will succeed, or a false acceptance will occur is 1/2^112 which is less than 1/1,000,000. The module will restrict the number of consecutive failed authentication attempts to 10. The probability of successfully authenticating to the module within one minute is 10/2^112 which is less than 1/100,000.

Note: SNMPv3 protocol is supported but is not a method of module security administration as it does not allow read/write access of CSPs. As such, it is characterized as an unauthenticated service.

3.3 Services

The table below lists authenticated and unauthenticated services provided by the Module.

Legend: Mode: Approved – A

Non-Approved – N

Both - B

Table 14 - Service Descriptions

Role / Service	Description	Mode	User	Admin
Configuration Service	Configuration of the device	B	X	X
Console	This service provides console access to the module. Also facilitates the zeroization service.	B	X	X
SSH Server	This service provides secure inbound connection to the module, including Secure Copy (SCP) operation. Also facilitates the zeroization service.	B	X	X
SSH Client	This service provides a secure outbound connection	B	X	X
Telnet Server	This service provides an inbound connection between Telnet server and remote Telnet client	N	X	X
Telnet Client	This service provides an outbound connection between remote Telnet server and module	N	X	X
HTTP Server	This service provides an inbound HTTP connection to the module inclusive of authentication of the user.	N	X	X
HTTPS Server	This service provides a secure inbound HTTP connection to a remote client inclusive of authentication of the user.	B	X	X
Copy Service	This service provides authenticated user a non-secure way to copy files or images using FTP, and TFTP.	N	X	X
Firmware Upload Service	Used within the console or an SSH session to install firmware into the device	B		X
Zeroization Service	Provide zeroization of Keys and CSPs	B	X	X

Table 15 – Unauthenticated Services

Service	Mode	Description
External Authentication	B	This service provides a way to authenticate user using an external server, like RADIUS, LDAP and TACACS+. (Note that only RADIUS is used in approved mode over TLS.)
Self-Tests	B	Executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated on-demand by power-cycling the module.
Show Status	B	Status output provided by requesting any service specified above, as well as the LED interfaces.
Network Switching Service	B	This service provides non-security relevant switching operations: L2 protocols, L3 routing protocols, L4 services like ACL, Rate Limiting, service ethernet operation, NTP.
SNMP	B	This service provides SNMPv3 protocol in authPriv and authNoPriv mode for MIB access. It does not modify CSPs or affect the modules security.

Services listed in Table 16 below are the only services which have access to CSPs and Public Keys within the module.

Legend:

N – Not used
R - Read
W - Write
Z - Zeroize

Table 16 - CSP Access Rights within Roles & Services

Services \ CSPs / Public Keys	SSHv2 incl. SCP & SFTP CSPs & Public Keys	TLS CSPs & Public Keys	DRBG CSPs	Operator Authentication/Passwords	Radius/Syslog Root CAs	SNMP CSPs
Configuration of the device	RW Z	RW Z	RW Z	RW Z	RW Z	RW Z
Console	RW Z	RW Z	N*	RW Z	RW Z	RW Z
SSH Server	RW Z	RW Z	R*	RW Z	N	N
SSH Client	RW	N	R	N	N	N

Services \ CSPs / Public Keys	SSHv2 incl. SCP & SFTP CSPs & Public Keys	TLS CSPs & Public Keys	DRBG CSPs	Operator Authentication/Passwords	Radius/Syslog Root CAs	SNMP CSPs
Telnet Server	N	N	N	N	N	N
Telnet Client	N	N	N	N	N	N
HTTP Server	N	N	N	N	N	N
HTTPS Server	N	RW	R	N	N	N
Copy Service	N	N	N	N	N	N
Firmware Upload Service	N	N	N	N	N	N
Zeroization Service	Z	Z	Z	Z	Z	Z
External Authentication	N	RW Z	N	RW	RW Z	N
Self-tests	N	N	N	N	N	N
Show Status	N	N	N	N	N	N
Network Switching Service	N	N	N	N	N	N
SNMP	N	N	R	N	N	R

* Although not explicitly zeroized by the Console or SSH Server services, DRBG CSPs may be zeroized by power cycling the module.

4 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-2, these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters an error state and outputs status in the format "<Self-test Name> failed!", otherwise it indicates successful completion by outputting a status message in the format "<Self-test Name>…successful."

The module performs the following algorithm KATs on power-up.

(1) Firmware Integrity Test (128-bit CRC)
(2) AES-128 CBC KATs (encrypt/decrypt)
(3) SP800-90A AES-256 CTR_DRBG KAT
(4) SHA-1, 256, 512 KATs
(5) HMAC SHA-1, 224, 256, 384, 512 KATs
(6) RSA 2048 SHA-1 Encrypt/Decrypt KATs
(7) RSA 2048 SHA 256 Sign KAT
(8) RSA 2048 SHA 256 Verify KAT
(9) SP800-135 TLS v1.0/1.1 KDF KAT
(10) SP800-135 TLS v1.2 KDF KAT
(11) SP800-135 SNMP KDF KAT
(12) SP800-135 SSHv2 KDF KAT
(13) ECC CDH KAT
(14) ECDSA P-384 SHA-256 sign/ verify KATs
(15) Diffie-Hellman KAT
(16) RSA encrypt/ decrypt PCT
(17) DSA KAT

The module performs the following conditional self-tests as indicated. Tests are also performed during startup.

(1) Continuous Random Number Generator (RNG) test – performed on Non-deterministic hardware based random number generator (NDRNG)
(2) Continuous Random Number Generator (RNG) test – performed on SP800-90A DRBG
(3) Periodic DRBG health test as specified in SP 800-90A, Section 11
(4) RSA 2048 SHA- 256 Pairwise Consistency Test (Sign and Verify)
(5) RSA 2048 Pair wise Consistency Test (Encrypt/Decrypt)
(6) ECDSA Pairwise Consistency test (Sign/Verify)
(7) Firmware Load Test (RSA 2048 SHA-256 Signature Verification)

5 Physical Security Policy

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components with standard passivation and production-grade opaque enclosure.

6 Operational Environment

FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code signed by RSA 2048 with SHA256 digest may be executed. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

8 Security Rules and Guidance

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module allows passwords that have a minimum length of eight (8) characters.
2. The cryptographic module provides two (2) distinct operator roles.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
4. Data output is inhibited during self-tests and while in an error state.
5. Data output is logically disconnected from processes performing key generation and zeroization.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.
8. The module does not support manual key entry.
9. The module does not provide bypass services or ports/ interfaces.
10. The CO shall configure its own password and the initial password for all applicable roles created by the CO.

9 CO Initialization

The cryptographic module may be configured for FIPS 140-2 mode by logging into the switch as an admin and entering the following commands:

1. unhide fips
2. Steps 1 requires password which will be "fibranne"
3. fips enable
4. It will ask for (yes/no) to proceed the on fips enable

The “fips enable” command will zeroize all CSPs, disable Telnet, HTTP, TFTP, remove the existing configuration if any in the switch, enable POST and reboot. The admin must then configure the passwords, rekey and configure desired services and settings. You can use the command “show fips” to verify the FIPS is enabled after fips enabled. Detailed instructions are described in the ‘Configuring the switch in FIPS mode’ from the Extreme SLX-OS FIPS Configuration Guide, 20.1.1aa. To access, go to the My Extreme Networks website at http://my.ExtremeNetworks.com.

To acquire FIPS approved firmware for the module the following steps are necessary if it is not already installed:

1. Download the image from the extreme website listed above
    a. A valid support contract is required
2. Untar or unzip the image file downloaded on any server where SCP or FTP is supported
3. Perform the below command,

firmware download <fullinstall> <SCP or FTP> host <IP of the SCP or FTP server where the build is available> user <username of the SCP or FTP server> password <password of the SCP or FTP server> directory <path of the Build location>
Note: Performing above command will reboot the switch twice and will not be reachable during the upgrade process.

10 Definitions and Acronyms

10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CLI	Command Line interface
CSP	Critical Security Parameter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
LDAP	Lightweight Directory Access Protocol
LIC	License
MAC	Message Authentication Code
MM	Management Module
NTP	Network Time Protocol
NOS	Network Operating System (SLX OS)
PKI	Public Key Infrastructure
PROM	Programmable read-only memory
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SNMPv3	Simple Network Management Protocol Version 3
SSHv2	Secure Shell Protocol
TLS	Transport Layer Security Protocol