Extreme Networks
SLX 9540 and SLX 9740 Switches

FIPS 140-2
Non-Proprietary
Security Policy

Document Version 1.2

Revision History

Revision Date	Revision	Summary of Changes
07/29/2021	1.0	Initial Release
05/12/2022	1.1	Tables 2, 6, 7, 13 and Sections 4, 6, 9 updated to address NIST comments
07/18/2022	1.2	Update made to KAS-ECC-SSC bit strength in Table 6 to address NIST comments

Contents

Table of Tables:

Table of Figures

1 Introduction

This document defines the Security Policy for the Extreme Networks SLX 9540 and SLX 9740 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	Description
SLX9740-40C	SLX9740-90C	Extreme SLX 9740-40C Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots. Intel Atom C3758
SLX9740-80C	SLX9740-80C	Extreme SLX 9740-S0C Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4 unpopulated power supply slots, 4 unpopulated fan slots. Intel Atom C3758
SLX9540-24S	BR-SLX-9540-24S-AC-F[1]	SLX 9540-24S Switch AC with front-to-back airflow. Supports 24×10 GbE/1 GbE + 24×1 GbE ports. Intel Xeon D-1527
SLX9540-24S	BR-SLX-9540-24S-DC-F[1]	SLX 9540-24S Switch DC with front-to-back airflow. Supports 24×10 GbE/1 GbE + 24×1 GbE ports. Intel Xeon D-1527
SLX9540-24S	BR-SLX-9540-24S-AC-R[1]	SLX 9540-24S Switch AC with back-to-front airflow. Supports 24×10 GbE/1 GbE + 24×1 GbE ports. Intel Xeon D-1527

SLX9540-24S	BR-SLX-9540-24S-DC-R[1]	SLX 9540-24S Switch DC with back-to-front airflow. Supports 24×10 GbE/1 GbE + 24×1 GbE ports. Intel Xeon D-1527
SLX9540-48S	BR-SLX-9540-48S-AC-F[1]	SLX 9540-48S Switch AC with front-to-back airflow. Supports 48×10 GbE/1 GbE + 6×100 GbE/40 GbE ports. Intel Xeon D-1527
SLX9540-48S	BR-SLX-9540-48S-DC-F[1]	SLX 9540-48S Switch DC with front-to-back airflow. Supports 48×10 GbE/1 GbE + 6×100 GbE/40 GbE ports. Intel Xeon D-1527
SLX9540-48S	BR-SLX-9540-48S-AC-R[1]	SLX 9540-48S Switch AC with back-to-front airflow. Supports 48×10 GbE/1 GbE + 6×100 GbE/40 GbE ports. Intel Xeon D-1527
SLX9540-48S	BR-SLX-9540-48S-DC-R[1]	SLX 9540-48S Switch DC with back-to-front airflow. Supports 48×10 GbE/1 GbE + 6×100 GbE/40 GbE ports. Intel Xeon D-1527

[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.	SLX9740-40C	SLX9740-80C
2.	SLX970-80C	SLX9740-80C
3.	BR-SLX-9540-24S-*	BR-SLX9540
4.	BR-SLX-9540-48S-*	BR-SLX9540

The firmware version is: SLXOS 20.2.1aa.

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

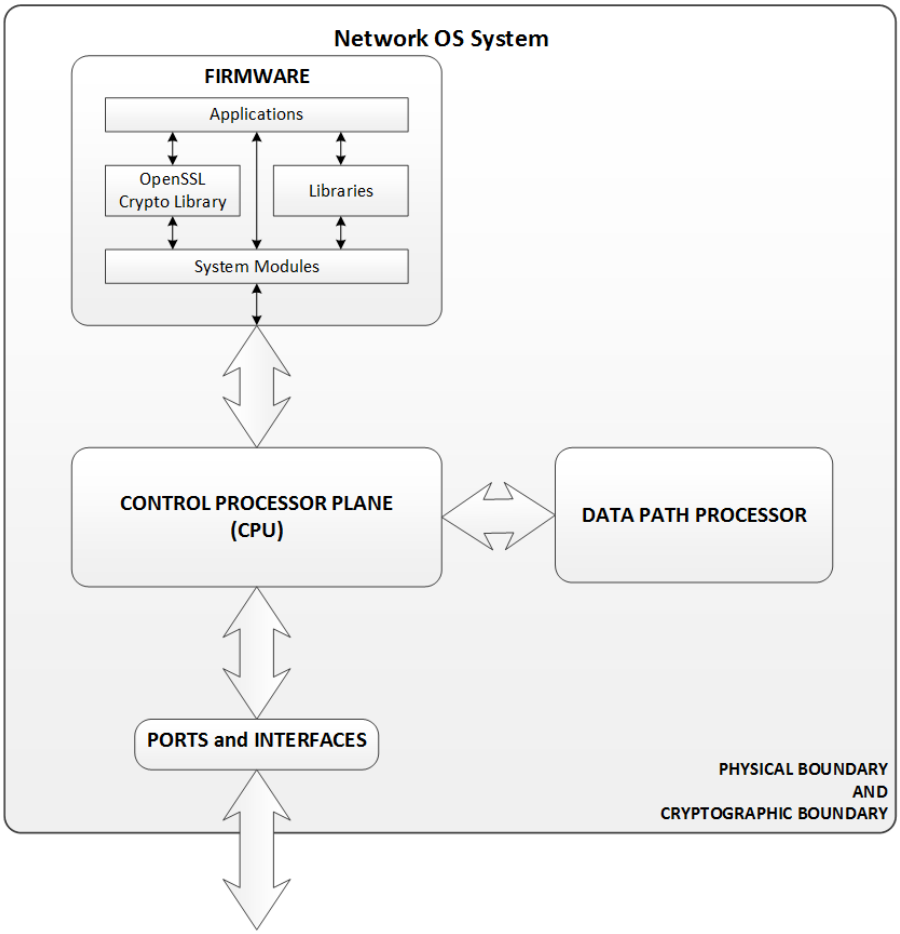
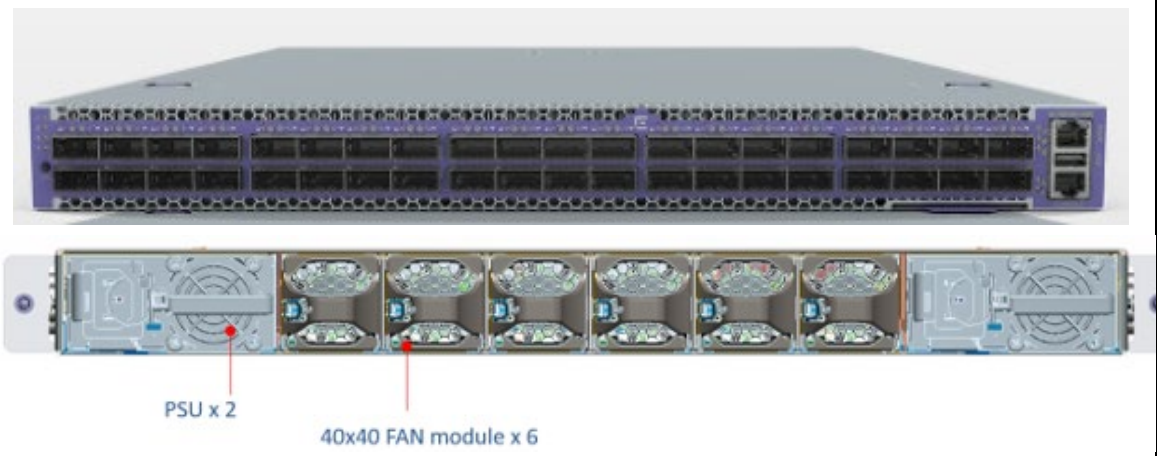
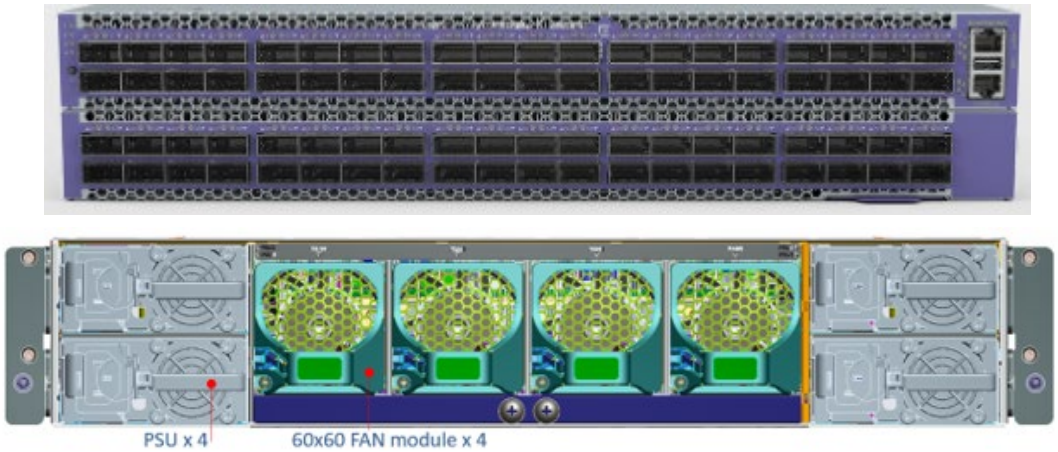
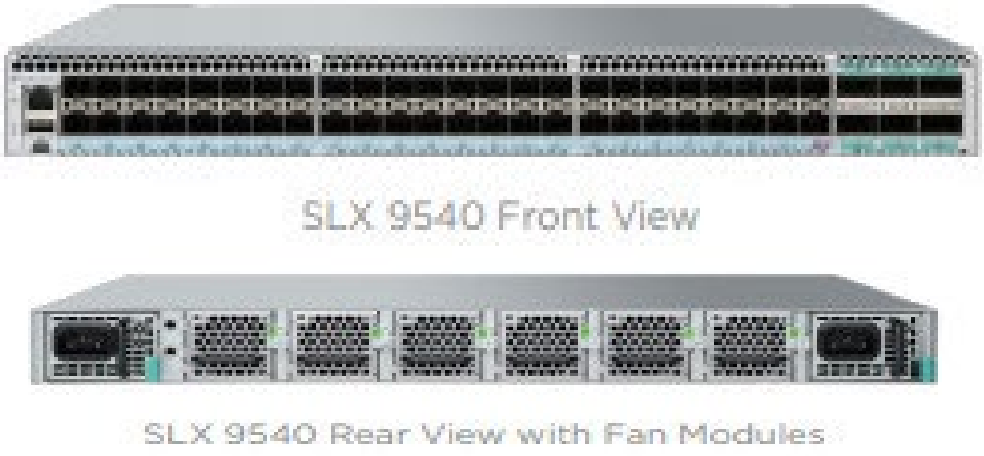
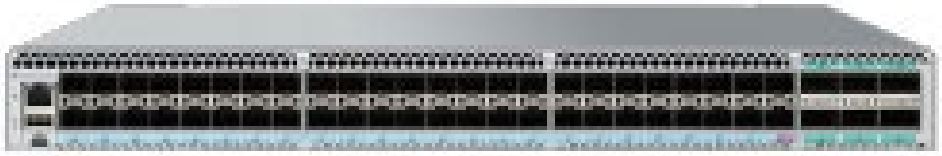


Figure 2 –SLX Modules

SLX 9740-40C

SLX 9740-80C

SLX 9540-24S


SLX 9540-48S
 SLX 9540 Front View  SLX 9540 Rear View with Fan Modules

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 9740-24S	SLX 9740-48S	SLX 9540-24S	SLX 9540-48S
Networking ports	40x100Gbe QSFP28 or max 72 with breakout cable (18*4) supporting 10Gbe or 25Gbe	80x100Gbe QSFP28 or Max 144 with breakout cable (36 * 4) supporting 10Gbe or 25Gbe	24x10Gbe/1Gbe+2 4x1Gbe	48×10 GbE/1 GbE + 6×100 GbE/40 GbE ports
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 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) 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 (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.]	A1076
CKG	SP800-133 Sections 5, 6.2	Vendor Affirmed
CVL	SP800-135 KDF TLS TLS v1.0/1.1 and v1.2 SHA-256, 384 [NOTE: TLS 1.0 is not supported in FIPS mode]	A1076
CVL	SP 800-135 KDF SNMP PW len: 64-128 SHA-1	A1076
CVL	SP800-135 KDF SSH (v2) AES-128, 192, 256 SHA-1, SHA-256, 384, 512	A1076
DRBG	SP800-90A Deterministic Random Bit Generator Mode: AES-256 CTR_DRBG (Derivation Function and Prediction Resistance Enabled)	A1076
DSA	Digital Signature Algorithm FIPS 186-4 Key Gen: L = 2048, N = 256	A1076

Label	Cryptographic Function	Certificate Number
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 tested, but not used for ECDSA signature generation/verification.]	A1076
ENT (NP)	SP800-90B Entropy Source. The DRBG is seeded with 2048 bytes of entropy from the entropy source, which provides at least 256 bits of security strength.	
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 tested, but not used or called by any service in FIPS mode]	A1076
KAS-SSC	Diffie-Hellman Key agreement; key establishment methodology provides 112 bits of encryption strength. dhEphem using 2048-bit EC Diffie-Hellman Key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength. Ephemeral Unified using P-256, P-384, P-521	A1076
KAS	KAS-SSC Cert. #A1076, CVL Cert. #A1076)	
KTS	AES (CBC or CTR) and HMAC within TLS or SSH; key establishment methodology provides between 128 and 256 bits of encryption strength	A1076
RSA	Rivest Shamir Adleman Signature Algorithm FIPS 186-4 Key Generation: RSA 2048, 3072-bit RSASSA-PKCS1_V1_5 Signature Generation: RSA 2048-bit with SHA-224, 256, 384, 512; 3072-bit with SHA-224, 256, 384, 512 RSASSA-PKCS1_V1_5 Signature Verification: RSA 1024-bit (legacy use) with SHA-1, SHA-224, 256, 384, 512; RSA 2048-bit with SHA-1 (legacy use only), SHA-224, 256, 384, 512; RSA 3072-bit with SHA-1 (legacy use only), SHA-224, 256, 384, 512 [NOTE: RSA 3072-bit is tested, but 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. RSA 1024-bit signature verification is also tested, but not used in the Approved mode]	A1076
SHS	Secure Hash Algorithm Message Digests: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA3-256 [NOTE: SHA-224 is not used or called by any service in FIPS Mode]	A1076
SHA-3	Secure Hash Algorithm Message Digest: SHA-3-256	A1076

Table 7 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
HMAC (No Security Claimed)	[IG 1.23, Scenario 2b] SHA-1, 256, 384 or 512 used to authenticate OSPFv2/3 packets using non-compliant keys.
HMAC-MD5	[IG 1.23, Scenario 2a] Used in RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator) Also used in the SP800-135 TLS 1.0/1.1 KDF
MD5 (No Security Claimed)	[IG 1.23, Scenario 1 and 2b] Used for User/ CO password hash and legacy use in industry protocols (Note: The use of MD5 does not provide cryptographic protection and the resultant MD5 digest is considered plaintext).

Table 8 – Security Relevant Protocols[2] 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_ECDH_RSA_WITH_AES_128_CBC_SHA256			TLS v1.1, v1.2

[2] 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]	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 in the non-Approved mode of operation:

Table 9 - Non-Approved Algorithms

Crypto Function/Service	User Role Change	Additional Details
ARCFOUR	Crypto-Officer	Non-approved cipher for SSH and TLS.
Blowfish	Crypto-Officer	Non-approved cipher for SSH and TLS.
CAST	Crypto-Officer	Non-approved cipher for SSH and TLS.
CHACHA20	Crypto-Officer	Non-approved cipher for SSH and TLS.
DES	Crypto-Officer	Non-approved cipher for SNMPv3
HMAC-MD5	Crypto-Officer	Non-approved within SNMPv3
MD5	Crypto-Officer	NTP authentication key, SSH MACs: hmac-md5, hmac-md5-96, hmac-md5-etm@openssh.com
RIJNDAEL	Crypto-Officer	Non-approved cipher for SSH and TLS
RIPEMD	Crypto-Officer	Non-approved cipher for SSH and TLS
RSA	Crypto-Officer	RSA operations with key size 1024 bits and RSA Key Transport within SSH and TLS
SNMP		SNMPv1, SNMPv2c, and SNMPv3 in noAuthNoPriv, authNoPriv mode
Triple-DES	Crypto-Officer	Non-approved cipher for SSH and TLS.
UMAC	Crypto-Officer	Non-approved cipher 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 3.

Table 10 – Critical Security Parameters (CSPs)

CSP	Description / Usage
KAS Private Keys	2048-bit DH or P-256, P-384, P-521 ECDH private keys used in SSH or TLS to establish a shared secret.
KAS Shared Secret	2048-bit shared secret from KAS-SSC. Used in SSH or TLS KDF to derive (client and server) session keys.
Session Encryption Keys	AES (CBC, CTR; 128, 192, 256-bit) used to secure SSH (including SCP and SFTP) or TLS sessions.
Session MAC Keys	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 Session authentication key used to provide integrity of SSHv2 (including SCP and SFTP) or TLS sessions.
Host Authentication Private Keys	ECDSA P-256, P-384, P-521 or RSA-2048, 3072-bit private keys used to authenticate to external entities for SSH and TLS.
DRBG Entropy Input	2048-bytes output from the SP800-90B Entropy Source; used to seed the SP800-90A DRBG (CTR_DRBG AES-256) to a security strength of 256-bits.
DRBG Internal State	Internal State of SP800-90A AES-256 CTR DRBG (256-bit Key and 128-bit V).
Passwords	Password used to authenticate operators (8 to 40 characters).

CSP	Description / Usage
RADIUS Secret	Used to facilitate session establishment with the RADIUS server (6 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
KAS Public Keys	DH 2048-bit or ECDH P-256, P-384, P-521 public keys used in SSH or TLS to establish a shared secret.
Authentication Public Keys	ECDSA P-256, P-384, P-521 or RSA-2048, 3072-bit external entity public keys, as well as module public keys for use in TLS and SSH authentication.
Firmware Download Public Key	RSA-2048-bit public key used to update the FW of the module.
Syslog ROOT CA certificate	RSA-2048-bit public key used to authenticate Syslog server.
RADIUS ROOT CA certificate	RSA-2048-bit 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 TLS 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 TLS 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, which is enforced by the module. 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, which is the default value for maximum consecutive failed authentication attempts. The probability of successfully authenticating to the module within one minute is 20/90^8 which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
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 that when using a RADIUS server over TLS in the Approved mode, the strength of authentication is also based on PKI, as the RADIUS server itself must be authenticated.

3.3 Services

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

Mode Legend:

Approved – A

Non-Approved – N

Both - B

Table 14 - Service Descriptions

Role / Service	Description	Mode	User	Admin
Configuration	Configuration of the device	B	X	X
Console	Provides console access to the module. Also facilitates the zeroization service.	B	X	X
External Authenticate	Provides a way to authenticate the operator using an external server, like RADIUS, LDAP and TACACS+. (Note only RADIUS is used in approved mode over TLS.)	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

Role / Service	Description	Mode	User	Admin
HTTPS Server	This service provides a secure inbound HTTPS 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
SNMP	This service provides SNMPv3 protocol in authPriv and authNoPriv mode for MIB access. It does not modify CSPs or affect the modules security.	B	X	X

Table 15 – Unauthenticated Services

Service	Mode	Description
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.

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

"Session CSPs and Public Keys" refers to KAS Private Keys, KAS Public Keys, KAS Shared Secret, Session Encryption Keys, and Session MAC Keys.

“DRBG CSPs” refers to DRBG Entropy Input and DRBG Internal State.

Table 16 - CSP Access Rights within Roles & Services

Services \ CSPs / Public Keys	Session CSPs and Public Keys	Host Authentication Private Keys	DRBG CSPs	Passwords	RADIUS Secret	Host Authentication Public Key	Firmware Download Public Key	Radius/Syslog Root CAs	SNMP CSPs
Configuration	RWZ	RW	RW	RW	RW	RW	N	RW	RWZ
Console	N	RW	N	RW	RW	RW	N	RW	RWZ
External Authentication	RWZ	RW	RW	R	R	R	N	RW	N
SSH Server	RWZ	RW	R	RW	RW	R	N	N	N
SSH Client	RWZ	N	R	N	N	R	N	N	N
Telnet Server	N	N	N	N	N	N	N	N	N
Telnet Client	N	N	N	N	N	N	N	N	N
HTTP Server	N	N	N	N	N	N	N	N	N
HTTPS Server	RWZ	RW	R	N	RW	R	N	N	N
Copy Service	N	N	N	N	N	N	N	N	N
Firmware Upload Service	N	N	N	N	N	N	RW	N	Z
Zeroization Service	Z	Z	Z	Z	Z	Z	N	Z	N
SNMP	N	N	R	N	N	N	N	N	R
Self-tests	N	N	N	N	N	N	N	N	N
Show Status	N	N	N	N	N	N	N	N	N
Network Switching Service	N	N	N	N	N	N	N	N	N

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 KAT (encrypt/decrypt)
(3) SP800-90A AES-256 CTR_DRBG KAT
(4) SHA-1, 256, 512 KATs
(5) SHA-3-256 KAT
(6) HMAC SHA-1, 224, 256, 384, 512 KATs
(7) RSA 2048 PKCS#1 SHA 256 Sign/Verify KATs
(8) SP800-135 TLS v1.0/1.1 KDF KAT
(9) SP800-135 TLS v1.2 KDF KAT
(10) SP800-135 SNMP KDF KAT
(11) SP800-135 SSHv2 KDF KAT
(12) KAS-ECC-SSC KAT
(13) KAS-FFC-SSC KAT
(14) ECDSA P-256 SHA-256 sign/verify KATs

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 Entropy Source and DRBG
(2) Continuous APT and RCT SP800-90B Health Tests – performed on SP800-90B Entropy Source
(3) Periodic DRBG health test as specified in SP 800-90A, Section 11 (i.e., Instantiate, Generate, Reseed)
(4) RSA 2048 SHA- 256 Pairwise Consistency Test (Sign/Verify)
(5) ECDSA Pairwise Consistency Test (Sign/Verify)
(6) 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 Extreme Networks using a trusted RSA 2048-bit private key may be loaded. 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 enforces passwords with a minimum length of eight (8) characters.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Data output is inhibited during self-tests and while in an error state.
4. Data output is logically disconnected from processes performing key generation and zeroization.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. 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.
7. The module does not support manual key entry.
8. The module does not provide bypass services or ports/ interfaces.

9 CO Initialization

The cryptographic module may be configured for FIPS 140-2 mode by logging into the switch as an admin (i.e., Cryptographic Officer) and entering the following commands:

1. Log into the switch as an admin.
2. Enable the **unhide fips** command to unhide FIPS-specific commands.

   device# unhide fips
3. Enter the **fips selfttests** command to move the crypto module to FIPS mode.

   NOTE: This command cannot be undone.

   device# fips selftests
4. Enter the **fips zeroize** command to zeroize all the existing security configurations and parameters.

   device# fips zeroize

   This command will reboot the switch.
5. After the module successfully reboots and performs all Power-Up Self-tests successfully, login as an administrator to disable the boot prom.

   device# prom-access disable

The “fips enable” procedure will zeroize all CSPs, disable Telnet, HTTP and TFTP, enable POST and reboot. The admin must then configure the passwords, rekey and configure desired services and settings.

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