Extreme VDX 6740, VDX 6740T, VDX 6940 and VDX 8770 Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.1

Revision History

Revision Date	Revision	Summary of Changes
08/28/2018	1.0	Initial Release
03/01/2019	1.1	Updated Algorithm Tables

Contents

Table of Tables:

Table of Figures

1 Introduction

This document defines the Security Policy for the Extreme Networks VDX 6740, VDX 6740T, VDX 6940, and VDX 8770 modules, hereafter denoted 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	2
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 Tables 2 and 3.

Table 2 - Firmware Version

Firmware
Network OS (NOS) v7.3.0aa

Table 3 – VDX Configurations

Module	HW P/N	Description
VDX_6740	P/N: 80-1007483-05	VDX 6740 system, 10 GbE SFP+ (x48), 40 GbE QSFP (x4), Non-port side exhaust[1] airflow
VDX 6740T	P/N: 80-1007486-01	VDX 6740T system, 10 GbE BaseT (x48), 40 GbE QSFP (x4) Port side exhaust[1] airflow
	P/N: 80-1007864-03	VDX 6740T-1G system, 1000BASE-T (x48), 40 GbE QSFP (x2), Port-side exhaust[1] airflow
VDX 6940	P/N: 80-1008009-02	VDX 6940-36Q system, 40 GbE QSFP+ (x36), Non-port side exhaust[1] airflow
	P/N: 80-1008531-01	VDX 6940-144S system, 10 GbE SFP+ (x96), QSFP (x12), Port side exhaust[1] airflow
VDX 8770	P/N: 80-1005850-01	VDX 8770-4 I/O Four (4) Slot chassis with one (1) Management Module (P/N: 80-1006294-03), Additional components may be ordered separately, refer to Tables 4 and 18.

[1] Port side (-R) and non-port side exhaust (-F) indicates whether the external fan direction causes air to be drawn into the non-port side air vents and exhausted from the port side air vents or vice versa.

VDX 8770 modules allow field replaceable units to be swapped within the physical cryptographic boundary. The Management Module listed in the table below must be included to be FIPS validated. All other field replaceable units have been excluded from FIPS 140-2 requirements (refer to Section 11).

Table 4 - VDX 8770 Management Module

HW P/N and Version	Description
P/N: 80-1006294-03	Field Replaceable Unit - Management Module (MM)

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

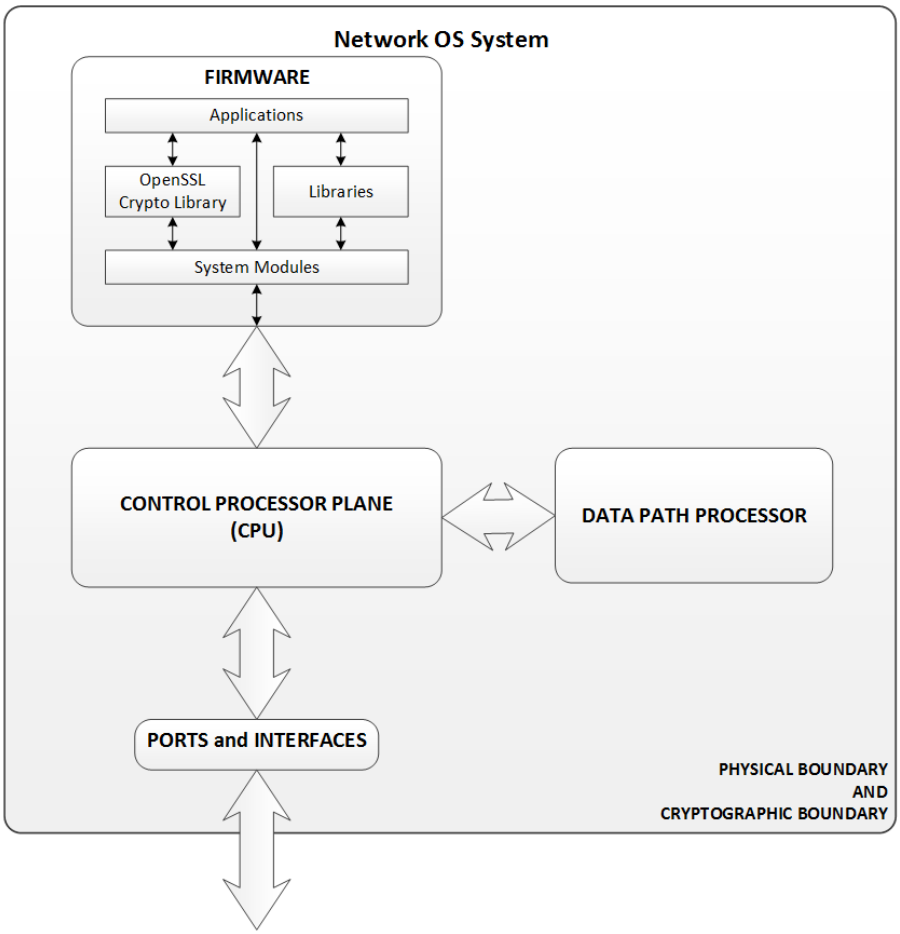

Figure 2 – VDX Module

VDX 6740

VDX 6740T

VDX 6740T-1G


VDX 6940-36Q

VDX 6940-144S

VDX 8770-4


[1] Each removable module in the chassis (except the fans) has a matching filler panel that must be in place if no module is installed in a slot. The two modules shown in this picture are fully populated with field replaceable units.

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

Table 5 - Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports	Data input
USB port	
Networking ports	Data output
USB port	
Management Ethernet port	Control input
Networking ports	

Physical Interface	Logical Interface
Serial port	
Management Ethernet port	Status output
Serial port	
Networking ports	
USB port	
LED	
Power Supply connector(s)	Power

Table 6 – Ports and Interfaces

Physical Interface	VDX 6740	VDX 6740T	VDX 6740T-1G	VDX 6940-36Q	VDX 6940-144S	VDX 8770
Networking ports	10 GbE SFP+ (x48) 40 GbE QSFP (x4)	10 GbE BaseT (x48) 40 GbE QSFP (x4)	10 GbE BaseT (x48) 40 GbE QSFP (x2)	40 GbE QSFP (x36)	10 GbE SFP+ (x96) 40 GbE QSFP (x12)	Chassis slots (x2)* for any combination of the following: - twelve (12) 40GE QSFP Line Card – forty-eight (48) 1/10G SFP+ Line Card * Note: the other two (2) slots must be occupied by the Switch Fabric Module and Management Module
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)	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)	RJ-45 used for console (x1)	RJ-45 used for console (x1)

Physical Interface	VDX 6740	VDX 6740T	VDX 6740T-1G	VDX 6940-36Q	VDX 6940-144S	VDX 8770
USB port	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)	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) Power Supply w/ embedded Fan (x2) Port (x48)	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 (x48)	System Power (x1) System Status (x1) Power Supply (x2) Fan (x5) Port (x146)	System Power (x1) System Status (x1) Power Supply (x4) Fan (x4) Port (x146)	System Power (x1) System Status (x1) Active (x1) Port (x146)
Power Supply connector(s)	Connectors (x2)	Connectors (x2)	Connectors (x2)	Connectors (x2)	Connectors (x2)	Connectors (x4)

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 operator is required to perform 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. Transitioning between the Approved and non-Approved modes of operation requires that the operator zeroize all CSPs.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 7 and 8 below.

Table 7 – Approved Algorithms

Label	Cryptographic Function	Certificate Number
AES	Advanced Encryption Algorithm Modes: CBC, CFB, CTR Sizes: 128, 256 [NOTE: AES-192 is not used or called by any service in FIPS mode. ECB Mode is not used or called by any service in FIPS mode. AES-CFB has only been implemented and tested for a 128-bit key length.]	5666
CKG	SP 800-133 Sections 6.1, 6.2 and 7.1	Vendor Affirmed
CVL	SP800-135 KDF (TLS v1.0/1.1 and v1.2)	2050
CVL	SP 800-135 KDF (SNMP)	2050
CVL	SP800-135 KDF (SSHv2)	2050
CVL	SP800-56A ECC CDH Primitive Curves: P-256, P-384, P-521	2049
DRBG	SP800-90A Deterministic Random Bit Generator Mode: AES-256 CTR_DRBG (Prediction Resistance Enabled)	2288
ECDSA	Elliptic Curve Digital Signature Algorithm FIPS 186-4 KPG: P-256 FIPS 186-4 PKV: P-256 FIPS 186-4 SigGen: P-256 with SHA-256/ 384 FIPS 186-4 SigVer: P-256 with SHA-256/ 384 [NOTE: P-384 and P-521 curves are not used or called by any service in FIPS Mode. SHA-512 is not used for ECDSA signature generation/ verification.]	1532
HMAC	Keyed-Hash Message Authentication code MACs: HMAC-SHA-1 (112-bit key), HMAC-SHA-256, HMAC SHA-384, HMAC-SHA-512 [NOTE: HMAC-SHA-224 is not used or called by any service in FIPS mode]	3771
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 RSASSA-PKCS1_V1_5 Signature Verification: RSA 2048-bit with SHA-1 (legacy use only) or SHA-256/ 384 [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]	3048
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]	4540

Table 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Diffie-Hellman	[IG D.8] Key agreement; key establishment methodology provides 112 bits of encryption strength.
Key Encapsulation	[IG D.9] RSA based key encapsulation; key establishment methodology provides 112 bits of encryption strength.
NDRNG	[IG G.13] Non-Deterministic RNG; minimum of 80 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG.
HMAC-MD5 (No Security Claimed)	[IG 1.23] Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator).
MD5 (No Security Claimed)	[IG 1.23] Used for User/ CO password hash (Note: The use of MD5 does not provide cryptographic protection, and Is considered as plaintext).

Table 9 – 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, 3072 bit)	RSA	AES-CBC-128, AES-CBC-256	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
	diffie-hellman-group14-sha1	RSA	AES-CBC-128, AES-CBC-256	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512
TLS/ HTTPS (both client and server) [IG D.8 and SP 800-135]	**TLS_RSA_WITH_AES_128_CBC_SHA**		**TLS v1.1, v1.2**	
	RSA	RSA	AES-CBC-128	SHA-1
	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

[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
SNMPv3 in authPriv mode	N/A	N/A	AES-CFB-128	HMAC SHA-1
OSPFv2/OSPF v3	N/A	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	N/A	N/A
NTP	N/A	HMAC-SHA-1	N/A	N/A
RADIUS	N/A	HMAC-MD5	N/A	N/A

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

Table 10 - Non-Approved Algorithms

Crypto Function/Service	*User Role Change*	*Additional Details*
SNMP	Crypto-Officer	Simple Network Management Protocol. SNMPv1, SNMPv2c and SNMPv3 in noAuthNoPriv, authNoPriv mode (all Plaintext; no cryptography) Unsupported 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

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 11 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DH Private Keys	Used in SSHv2 to establish a shared secret
SSHv2/SCP/SFTP Session Keys	AES (AES-128-CBC, AES-256-CBC) used to secure SSHv2/SCP/SFTP sessions
SSHv2/SCP/SFTP Authentication Key	Session authentication key used to authenticate and provide integrity of SSHv2 session (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512)
SSHv2 KDF Internal State	Used to generate Host encryption and authentication key

CSP	Description / Usage
SSHv2 DH Shared Secret Key	2048-bit shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
SSHv2 Host Private Key	ECDSA P-256 or RSA-2048 private key used to authenticate SSHv2 server to client
Value of K during SSHv2 256 ECDSA session	ECDSA K Value
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 KDF Internal State	Values of the TLS KDF internal state
TLS v1.1/1.2 Host Private Key	RSA-2048 host private key used to sign a server certificate and decrypt a server mode TLS session
TLS Session Keys	128/ 256-bit AES-CBC key used to secure TLS sessions
TLS Authentication Key	HMAC-SHA-1 and HMAC-SHA-256 key used to provide data authentication for TLS sessions
DRBG Seed	Seeding material for the SP800-90A DRBG (CTR_DRBG AES-256)
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)
RADIUS Secret	Used to authenticate the RADIUS Server (8 to 40 characters)
NTP Key	Used to authenticate the NTP client with the server (8-32 characters)
OPFv2 Key	Used to authenticate OSPFv2 packet (8-15 characters)
OSPFv2 Key	Used to authenticate OSPFv2 packet (8-32 characters)
OSPFv3 Key	Used to authenticate OSPFv3 packet (8-32 characters)
SNMPv3 Passphrase	Used to derive SNMPv3 auth key and SNMPv3 privacy key (8-32characters)
SNMPv3 auth key	Used to authenticate SNMPv3 packet using HMAC-SHA-1
SNMPv3 privacy key	Used to encrypt SNMPv3 packet using AES-CFB-128

2.2 Public Keys

Table 12 – Public Keys

Key	Description / Usage
DH Public Key	2048-bit public key used to establish shared secrets (SSHv2)
SSHv2 DH Peer Public Key	2048-bit public key used to establish shared secrets (SSHv2)

Key	Description / Usage
SSHv2 Peer Public Key	RSA-2048 public key used to authenticate SSHv2 session Client
SSHv2 Host Public Key	ECDSA P-256 or RSA-2048 public key used to authenticate SSHv2 session
SSHv2 ECDSA Peer Public Key	P-256 public key used to authenticate SSHv2 server to Client
TLS v1.1/1.2 Host Public Key	RSA-2048 host public key used by client to authenticate TLS host and encrypt TLS Pre-Master secret
Firmware Download Public Key	RSA-2048 public key used to update the FW of the module.
LDAP ROOT CA certificate	RSA-2048 public key used to authenticate LDAP server

3 Roles, Authentication and Services

3.1 Assumption of roles

The cryptographic module supports five operator roles. The cryptographic module shall enforce the separation of roles using role-based and identity-based operator authentication.

Forty-eight (48) concurrent operators are allowed on the Module.

Table 13 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data	Authentication Mechanism
User (User role): User role has the permission to execute a subset of the commands within the SSH and HTTPS services.	Identity-based	Username and Password	Password
Admin (Crypto-Officer): Admin role has the permission to access and execute all the commands within the SSH Server and HTTPS Server services.	Identity-based	Username and Password	Password
SNMP Role: Provides role to perform SNMPv3 operations	Identity-based	Username and SNMP Passphrase	Shared Secret
User Authentication Role: Provides a role to perform user authentication using external authentication servers	Identity-based	Username and RADIUS Secret hashed with MD5	Shared Secret
		LDAP Root CA certificate	Digital Signature Verification

Role	Type of Authentication	Authentication Data	Authentication Mechanism
Protocol Authentication Role: Provides a role to perform various protocol authentications.	Role-based	TLS Session Keys	Encryption
		SSHv2/SCP/SFTP Session Keys	Encryption
		NTP Passphrase hashed with SHA-1	Shared Secret
		OSPFv2 Password hashed with SHA-1, SHA-256, SHA-384 or SHA-512	Shared Secret
		OSPFv3 Password hashed with SHA-1, SHA-256, SHA-384 or SHA-512	Shared Secret

3.2 Authentication Methods

Table 14 - Strengths of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
Password	96 possible characters can be used with a minimum length of 8 characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 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 minute is 20. The probability of successfully authenticating to the module within one minute is 20/96^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	RSA-2048 with SHA-256 is used for signature verification. 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.
Encryption	Data is transmitted over a session encrypted with an AES-128 key or stronger. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^128 which is less than 1/1,000,000. The module's processor runs at 1.5MHz, The probability of successfully authenticating to the module within one minute is (1.5*10^6)/2^128 which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is at least 1/96^8 which is less than 1/1,000,000. The module's processor runs at 1.5MHz, The probability of successfully authenticating to the module within one minute is (1.5*10^6)/96^4 which is less than 1/100,000.

3.3 Services

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

Table 15 - Service Descriptions

Role / Service	Description	Mode	User	Admin	User Authentication	Protocol Authentication	SNMP
Console	This service provides console access to the module. Also acts as the zeroization service.	B	X	X			
SSH Server	This service provides secure inbound connection to the module, including Secure Copy (SCP) operation. Also acts as the zeroization service.	B	X	X			
SSH Client	This service provides a secure outbound connection	B				X	
Telnet Server	This service provides an inbound connection between Telnet server and remote Telnet client	N	X	X			
HTTP Server	This service provides an inbound HTTP connection to the module	N	X	X			
HTTPS Server	This service provides a secure inbound HTTP connection between server and remote client	B	X	X	X		
HTTPS Client	This service provides a secure outbound HTTP connection					X	

Role / Service	Description	Mode	User	Admin	User Authentication	Protocol Authentication	SNMP
User Authentication	This service provides way to authenticate user using an external server, like LDAP or RADIUS	B			X		
Protocol Authentication	This service provides way to send authenticated protocol packets to remote peers. At this time, NTP, OSPFv2 and OSPFv3 will use this service	B				X	
SNMP-Approved	This service provides SNMPv3 protocol in authPriv mode for secure MIB access	B					X
SNMP-NA	This service provides insecure SNMPv1, SNMPv2c, SNMPv3 (noAuthNoPriv, authNoPriv) protocol access to the MIB	N					X
Copy Service	This service provides authenticated user a non-secure way to copy files or images using FTP, and TFTP.	N	X	X			

Legend: Mode: Approved – A, Non-Approved – N, Both - B

Table 16 – 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.
Switching Service	B	This service provides non-security relevant switching operations like Clock, debug, license, platform, L2 protocols, L3 protocols, L4 services like ACL, Rate Limiting, PKI, service ethernet operation.
Telnet Client	N	This service provides an outbound connection between a Telnet client and remote Telnet server
HTTP Client	N	This service provides an outbound HTTP connection to the module

Services listed in Table 17 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 17 - CSP Access Rights within Roles & Services

Services \ CSPs / Public Keys	SSHv2 and SCP CSPs & Public Keys	TLS CSPs & Public Keys	DRBG CSPs	Operator Authentication/Passwords	NTP/OSPF authentication keys	LDAP Public Keys	SNMP CSPs
Console	RW Z	RW Z	N*	RW Z	RW Z	RW Z	RW Z
SSH Server	RW Z	RW Z	R*	RW Z	RW Z	RW Z	RW Z
SSH Client	RW	N	R	N	N	N	N
Telnet Server	N	N	N	N	N	N	N
Telnet Client	N	N	N	N	N	N	N
HTTP Server	N	N	N	N	N	N	N
HTTP Client	N	N	N	N	N	N	N
HTTPS Server	N	RW	R	N	N	N	N
HTTPS Client	N	RW	R	N	N	N	N
User Authentication	N	N	N	RW	N	N	N
Protocol Authentication	N	N	N	N	RW	N	N
SNMP-Approved	N	N	R	N	N	N	RW
SNMP-NA	N	N	N	N	N	N	N
Switching Service	N	N	N	N	N	N	N
Copy Service	N	N	N	N	N	N	N
Self-tests	N	N	N	N	N	N	N
Show Status	N	N	N	N	N	N	N

* 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) PROM Integrity Test (CRC-32)
(2) Firmware Integrity Test (128-bit CRC)
(3) AES-128 CBC KAT (encrypt/decrypt)
(4) SP800-90A AES-256 CTR_DRBG KAT
(5) SHA-1, 256, 384, 512 KAT
(6) HMAC SHA-1, 224, 256, 384, 512 KAT
(7) RSA 2048 SHA-1 Encrypt/Decrypt KAT
(8) RSA 2048 SHA 256 Sign KAT
(9) RSA 2048 SHA 256 Verify KAT
(10) SP800-135 TLS v1.0/1.1 KDF KAT
(11) SP800-135 TLS v1.2 KDF KAT
(12) SP800-135 SSHv2 KDF KAT
(13)SP 800-135 SNMP KDF KAT
(14) ECC CDH KAT
(15) ECDSA P-384 SHA-256 sign/ verify KAT
(16) Diffie-Hellman KAT
(17)RSA encrypt/ decrypt PCT

The module performs the following conditional self-tests as indicated.

(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

The 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.

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 operator must ensure that all passwords have a minimum length of 8 characters
2. The cryptographic module provides five 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.

9 CO Initialization

The cryptographic module may be configured for FIPS 140-2 mode via execution of the following procedures:

1. Login to the switch as admin.
2. Enable **fips selftests** using the following commands:

   device#unhide fips
   device#fips selftests

   Note:This command cannot be undone.
   device#fips selftests

3. Enter **fips zeroize** command to zeroize all the existing security configurations and parameters:

   device#fips zeroized

   Note: This command will reboot the switch with default configuration. New SSH key pairs are generated for RSA and ECDSA so SSH can work after module is booted.

4. After the module successfully reboots and performs all Power-Up Self-tests successfully, login as admin to disable boot prom:

device#prom-access disable

5. Enter the **cipherset ldap** command to configure TLS 1.1 and TLS 1.2 ciphers for LDAP authentication:

   sw0#cipherset ldap

6. Use IP ACLs to block Telnet, HTTP, and Extreme Networks internal ports 7110, 7710, 8008, 9110, and 9710 for IPv4 and IPv6. If SSH access is required, enter **seq permit** commands to allow access on port 22. If remote access is required, such as through SCP or LDAP, enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535.

   Configure IP ACLs using **ip access-list** command and use **ip access-group** command to apply the rules to the management interface:

   device(config)# ip access-list extended <User defined name (i.e.FIPS-ACL4)>
   device(config-ip-ext)# seq 1 deny tcp any any eq 23
   device(config-ip-ext)#seq 2 deny tcp any any eq 80
   device(config-ip-ext)#seq 4 deny tcp any any eq 7110
   device(config-ip-ext)#seq 5 deny tcp any any eq 7710
   device(config-ip-ext)#seq 6 deny tcp any any eq 8008
   device(config-ip-ext)#seq 7 deny tcp any any eq 9110
   device(config-ip-ext)#seq 8 deny tcp any any eq 9710
   device(config-ip-ext)#seq 10 permit udp any any eq 123
   device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
   device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
   device(config-ip-ext)#seq 13 permit tcp any any eq 22
   device(config-ip-ext)#seq 14 permit tcp any any eq 830

   device(config-ip-ext)#exit
   device(config)# interface Management <ID for Management Interface (i.e. 1/0)>
   device(config-Management-1/0)# ip access-group <User defined name (i.e.FIPS-ACL4)> in

   device(config)# ipv6 access-list extended <User defined name (i.e.FIPS-ACL6)>
   device(config-ip-ext)# seq 1 deny tcp any any eq 23
   device(config-ip-ext)#seq 2 deny tcp any any eq 80
   device(config-ip-ext)#seq 4 deny tcp any any eq 7110
   device(config-ip-ext)#seq 5 deny tcp any any eq 7710
   device(config-ip-ext)#seq 6 deny tcp any any eq 8008
   device(config-ip-ext)#seq 7 deny tcp any any eq 9110
   device(config-ip-ext)#seq 8 deny tcp any any eq 9710
   device(config-ip-ext)#seq 10 permit udp any any eq 123
   device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
   device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
   device(config-ip-ext)#seq 13 permit tcp any any eq 22
   device(config-ip-ext)#seq 14 permit tcp any any eq 830

   device(config-ip-ext)#exit
   device(config)# interface Management <ID for Management Interface (i.e. 1/0)>
   device(conf-Management-1/0)# ipv6 access-group <User defined name (i.e.FIPS-ACL6)> in

   NOTE
   Do not use FTP mode for the operations such as copying startup or running configuration, copy support, and firmware download.

   NOTE
   Do not configure TACACS+ protocol for authentication.

7. Enter the following command to remove any tacacs+ server configuration
   device(config)# no tacacs-server <host>

8. Configure LDAP authentication:

   a)Enter the crypto import command in privileged EXEC mode to import the LDAP CA certificate.

   device# crypto import ldapca protocol SCP host <IP> user <user-id> directory / <full-path> crypto file cacert.pem
   Password: **********
   The CA certificate imported must be generated using RSA2048 with SHA256.

   b) Enter the **ldap-server host** *ip-address* **basedn** *domain-name* [**port** *portnum*] [**retransmit** *num* command in global configuration mode to configure the LDAP server.

   device(config)# ldap-server host <name, eg. pad112r2.1a12security.xyz.com> basedn <domain, eg.1a12security.xyz.com>

   c) Enter the **ip dns** command to configure the DNS domain and server.

   device(config)# ip dns domain-name <name, eg. 1a12security.xyz.com>

   device(config)# ip dns name-server <server IP>

   d) Enter the **aaa authentication login ldap local-auth-fallback** command.

   device(config)# aaa authentication login ldap local-auth-fallback

   .

9. If required to set up a syslog server, follow the steps below to enable secure logging:
   a) Enter the **crypto import** command in privileged EXEC mode to import the SYSLOG CA certificate.

   device# crypto import syslogca protocol SCP host <IP> user <user-id> directory /<full-path>crypto file cacert.pem
   Password: **********

   The CA certificate imported must be RSA2048 with SHA256 encryption.

   b) Enter the **logging syslog-server host** *ip-address* **use-vrf** *vrf-name* **secure** command in global configuration mode to
   configure the Syslog server

10. Enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **login** *login-id* **password** *password* **user** user-account command in privileged EXEC mode to import SSH public key, if required:
    *device# certutil import sshkey directory /usr/sshkeys file id_rsa.pub protocol SCP host <IP> user admin login remoteuser password *****.*

To support passwordless SSH authentication, externally generated RSA key pairs must be RSA2048 only.

11. Configure ntp server using commands in global configuration mode, if required:

a) Enter the **ntp authentication key** *key-id* **sha1** *key-string* to configure NTP authentication key of type SHA1.

device(config)# ntp authentication key 1 sha1 <string>

b)Enter the **ntp server** *ip-address* **key** *key-id* **secure** command to configure the Syslog server.

device(config)# ntp server 10.20.8.1 key 1

12 . Configure VDX 6740, VDX 6740T-1G and VDX 6740T to disable Access Gateway (AG) mode using the following command in local rbridge-id specific configuration mode.

device(config-rbridge-id-1)# ag
device(config-rbridge-id-1-ag)# no enable

13. Vcenter, dot1x(802.1x) feature is not FIPS compliant.

a) If dot1x is enabled, execute the following CLI in config mode to disable dot1x globally:

no dot1x enable

b)If vcenter is configured, remove the configuration using the following CLI:

no vcenter<name>

14. If SNMP needs to used, enter the **snmp-server v3host** *ip username* command to allow only SNMPv3 notifications to be sent.

See the *Extreme Network OS Command Reference* for information on SNMPv3 configuration.

switch(config)# snmp-server v3host <ip> <username>

15. Passwords of the default accounts (admin and user) must be changed to maintain FIPS 140-2 compliance:

device#username admin password <enter password>
device #username user password <enter password>

16. Disable telnet service with the following command:

device(config-rbridge-id-1)#telnet server shutdown

17. Enter the **copy running-config startup-config** to save all the settings to the startup configuration file.

device#copy running-config startup-config

Note: For more information, please refer to additional Extreme Networks manuals on MyExtreme Networks website. To access them online, go to the MyExtreme Networks website at http://my.Extreme Networks.com.

10 Definitions and Acronyms

10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
Blade	Blade server
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
FOS	Fabric Operating System
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
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

11 Components Excluded from FIPS 140-2 Requirements

The following components may be used within validated Extreme Networks VDX 8770-4 configurations; they do not have any security relevance and have been excluded from FIPS 140-2 requirements:

Justification and Rationale.

Security impact of these components listed in Table 18 : NONE

Components listed in below Table 18

- Do not perform any security relevant function.
- Do not control or communicate any cryptographic CSPs.
- Do not have access to critical security parameters.
- If these components failed, misused, or otherwise compromised, the security of the cryptographic module is not affected in anyway.

Table 18 - Components for the VDX 8770

SKU / Part Number	Description
SKU: XBR-BLNK-PSU P/N: 80-1006430-01	Field Replaceable Unit - Blank Panel for Power Supply Unit (PSU) Slots
SKU: BR-VDX8770-SFM-1 P/N: 80-1006295-01	Field Replaceable Unit - Switch Fabric Module (SFM)
SKU: BR-VDX8770-12X40G-QSFP-1 P/N: 80-1006293-02	Field Replaceable Unit – twelve (12) 40GE QSFP Line Card. No Optics
SKU: BR-VDX8770-48X10G-SFPP-1 P/N: 80-1006048-02	Field Replaceable Unit – forty-eight (48) 1/10G SFP+ Line Card, No Optics
SKU XBR-BLNK-FULL P/N 80-1006431-01	Field Replaceable Unit - Filler Panel for Line Card Slot
SKU XBR-BLNK-HALF P/N 80-1006429-01	Field Replaceable Unit - Half-Slot Filler Panel for Switch Fabric Module Slot or Management Module Slot
SKU: XBR-ACPWR-3000 P/N: 80-1006540-01	Field Replaceable Unit - Power Supply Unit (PSU)– AC
SKU: XBR-FAN-FRU P/N: 80-1006080-01	Field Replaceable Unit - Fan Module (FAN)