Juniper Networks MX240, MX480, MX960, MX2010, MX2020 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE1800 Routing Engine

Firmware: Junos OS 17.3R2

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.1

Date: February 18, 2019

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Contents

List of Tables

List of Figures

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks MX Series 3D Universal Edge Routers with the RE1800 routing engine (the "MX Series") and the EX9200 series switches with the RE1800 routing engine. The MX series provides dedicated high-performance processing for flows and sessions and integrates advanced security capabilities that protect the network infrastructure as well as user data. The EX9200 series enables collaboration and provides simple and secure access for the delivery of mission-critical applications in the enterprise campus. In the data center, it simplifies operations to align the network with fast-changing business requirements.

This FIPS 140-2 validation includes the following MX series router models: the MX240, MX480, MX960, MX2010 and MX2020 and the following EX series switch models: EX9204, EX9208, EX9214. The FIPS validated version of firmware is Junos OS 17.3R2.

The cryptographic boundary for this MX Series and EX Series is defined as follows for the validation:

- the outer edge of the chassis includes the Routing Engine (RE), Switch Control Board (SCB/SFB/SF), slot cover in the following configurations:
  - For MX240 (2 available RE slots, 2 additional slots): 1 SCB and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - MX480 (2 available RE slots, 6 additional slots): 1 SCB and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For MX960 (2 available RE slots, 12 additional slots): 1 SCB and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For MX2010 (2 available RE slots, 10 additional slots): 1 SFB and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For MX2020 (2 available RE slots, 20 additional slots): 1 SFB and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For EX9204 (2 available RE slots, 2 additional slots): 1 SF module and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For EX9208 (2 available RE slots, 6 additional slots): 1 SF module and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For EX9214 (2 available RE slots, 12 additional slots): 1 SF module and 1 RE. All empty module bays must have a slot cover installed for proper cooling air circulation.
- includes the inverse three-dimensional space where non-crypto-relevant line cards fit, with the backplane port serving as the physical interface
- excluding the power distribution module on the rear of the device.

The cryptographic modules provide for an encrypted connection, using SSH, between the management station and the module. All other data input or output from the module is considered plaintext for this FIPS 140-2 validation.

The cryptographic modules are defined as multiple-chip standalone modules that execute Junos OS 17.3R2 firmware on any of the Juniper Networks MX 3D Universal Edge Routers listed in Table 1 below.

Table 1 – Cryptographic Module Hardware Configurations

Chassis PN	SCB PN	RE PN
MX240	SCBE2-MX	RE-S-1800X4-YYG (YY = 8, 16 or 32 GB memory)
MX480	SCBE2-MX	
MX960	SCBE2-MX	
MX2010	MX2K-SFB	
MX2020	MX2K-SFB	
EX9204	EX9200-SF2	RE-S-1800X4-YYG (YY = 8, 16 or 32 GB memory) *Note: This part is also known as the EX9200-RE*
EX9208	EX9200-SF2	
EX9214	EX9200-SF2	

The modules are designed to meet FIPS 140-2 Level 1 overall:

Table 2- Security Level of Security Requirements

Area	Description	Level
1	Module Specification	1
2	Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	1

The modules have a limited operational environment as per the FIPS 140-2 definitions. It includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation.

The modules do not implement any mitigations of other attacks as defined by FIPS 140-2.

1.1 Hardware and Physical Cryptographic Boundary

The cryptographic modules' operational environment is a limited operational environment.

The image below depicts the physical boundary of the modules, including the Routing Engine and SCB. The boundary excludes the non-crypto-relevant line cards included in the figure.

Figure 1 – Physical Cryptographic Boundary (Left to Right: MX240, MX480, MX960, MX2010, MX2020)

Figure 2 - Physical Cryptographic Boundary (Left to Right: EX9204, EX9208, EX9214)

Table 3 - Ports and Interfaces

Port	Description	Logical Interface Type
Ethernet (data)	LAN Communications	Control in, Data in, Status out, Data out
Ethernet (mgmt.)	Remote Management	Control in, Data in, Status out, Data out
Serial	Console serial port	Control in, Data in, Status out, Data out
Power	Power connector	Power
Reset Button	Reset	Control in
LED	Status indicator lighting	Status out
USB	Load Junos OS image	Control in, Data in
Backplane	Line card backplane interfaces	Control in, Data in, Status out, Data out
Chassis Cluster Control	Disabled	N/A
Aux	Disabled	N/A

1.2 Modes of Operation

The module supports a FIPS Approved mode of operation and a non-Approved mode of operation. The module must always be zeroized when switching between a FIPS Approved mode of operation and the non-Approved mode of operation and vice versa.

1.2.1 FIPS Approved Mode

The Crypto-Officer places the module in an Approved mode of operation by following the instructions in section 6.2.1 and 6.2.2.

The Crypto-Officer can verify that the cryptographic module is in an Approved mode by observing the console prompt and running the “show version” command. When operating in FIPS mode, the prompt will read “<user>@<device name>: fips#” (e.g. crypto-officer@mx240:fips#). The “show version” command will allow the Crypto-Officer to verify that the validated firmware version is running on the module. The Crypto-Officer can also use the “show system fips level” command to determine if the module is operating in FIPS mode.

1.2.2 Non-Approved Mode

The cryptographic module supports a non-Approved mode of operation. When operated in the non-Approved mode of operation, the module supports the algorithms identified in Section 2.1 as well as the algorithms supported in the Approved mode of operation.

The Crypto-Officer can place the module into a non-approved mode of operation by following the instructions for zeroizing the module found in section 6.2.2. Zeroizing the system will set it back to the factory default state.

2 Cryptographic Functionality

2.1 Allowed Algorithms and Protocols

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 4, 5, 6, 7, 8 and 9 below. Table 10 summarizes the high-level protocol algorithm support. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in these tables.

Table 4 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
1896	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation
3393	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication, DRBG Primitive
			SHA-256	Key size: 256 bits, λ = 128, 256	
4139	SHS	PUB 180-4	SHA-1 SHA-256		Message Digest Generation

Table 5 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
3394	HMAC	PUB 198	SHA-1	Key size: 112, 160 bits, λ = 160	Message Authentication
4140	SHS	PUB 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
5089	AES	PUB 197-38A	CBC CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
N/A[1]	CKG	SSH-PUB 133	Section 6.1 Section 6.2		Asymmetric key generation using unmodified DRBG output

[1] Vendor Affirmed

1641	CVL	SP 800-135	SSH	SHA 1, 256, 512	Key Derivation
1895	DRBG	SP 800-90A	HMAC		SHA-256
1319	ECDSA	PUB 186-4		P-256 (SHA 256, 384, 512) P-384 (SHA 256, 384, 512) P-521 (SHA 256, 384, 512)	SSH: SigGen, KeyGen, SigVer Package: SigVer
3392	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 160	Message Authentication
			SHA-512	Key size: 512 bits, λ = 512	
			SHA-256	Key size: 256, λ = 256	Message Authentication DRBG Primitive
N/A	KTS		AES Cert. #5089 and HMAC Cert. #3392		Key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #2622 and HMAC Cert. #3392		key establishment methodology provides 112 bits of encryption strength
4138	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
2622	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 7 - Allowed Cryptographic Functions

Algorithm	Caveat	Use
Elliptic Curve Diffie-Hellman [IG] D.8	Provides between 128 and 256 bits of encryption strength.	key agreement; key establishment
NDRNG [IG] 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DRBG

Table 8 - Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
SSHv2[2]	EC Diffie-Hellman P-256, P-384, P-521	ECDSA P-256	Triple-DES CBC AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

No part of these protocols, other than the KDF, have been tested by the CAVP and CMVP. The SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 8 above, each column of options for a given protocol is independent and may be used in any viable combination.

2.2 Disabled Algorithms and Protocols

These algorithms and protocols are non-Approved algorithms and protocols that are disabled when the module is operated in an Approved mode of operation. The algorithms are available as part of the SSH connect service when the module is operated in the non-Approved mode.

Algorithms

- RSA
- AES-GCM
- ECDSA with ed25519 curve
- ECDH with ed25519 curve
- ARCFOUR
- Blowfish
- CAST
- DSA (SigGen, SigVer; non-compliant)
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC

Protocols

- Finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

[2] RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol

2.3 Critical Security Parameters

All CSPs and public keys used by the module are described in this section.

Table 9 - Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the DRBG
DRBG_State	Values V and Key which comprise the HMAC_DRBG state
Entropy Input	256 bits entropy (min) input used to instantiate the DRBG
ECDH Shared Secret	The shared secret used in Elliptic Curve Diffie Hellman (ECDH) key exchange. 256, 384 or 521 bits. Established per the Elliptic Curve Diffie-Hellman key agreement.
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256. Used to identify the host.
SSH ECDH	Ephemeral EC Diffie-Hellman private key used in SSH. ECDH P-256, P-384, or P-521
SSH-SEKs	SSH Session Keys: SSH Session Encryption Key: 3-Key Triple-DES or AES (128,192,256); SSH Session Integrity Key: HMAC.
HMAC key	The LibMD HMAC keys: message digest for hashing password and critical function test.
User Password	Passwords used to authenticate Users to the module.
CO Password	Passwords used to authenticate COs to the module.

Table 10 - Public Keys

Name	escription and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256.
SSH-ECDH-PUB	Ephemeral EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, P-384, or P-521
Auth-User Pub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P-256, P-384, or P-521
Auth-CO Pub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P-256, P-384, or P-521
Root CA	ECDSA P-256 X.509 Certificate; Used to verify the validity of the Juniper Package CA at software load and also at runtime for integrity.
Package CA	ECDSA P-256 X.509 Certificate; Used to verify the validity the Juniper Image at software load and also at runtime for integrity.

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Cryptographic Officer (CO) and User. The module supports concurrent operators, but does not support a maintenance role and/or bypass capability. The module enforces the separation of roles using identity-based operator authentication.

The Cryptographic Officer role configures and monitors the module via a console or SSH connection. As root or super-user, the Cryptographic Officer has permission to view and edit secrets within the module..

The User role monitors the router via the console or SSH. The User role cannot change the configuration.

3.2 Authentication Methods

The module implements two forms of Identity-Based authentication, Username and password over the Console and SSH as well as Username and ECDSA public key over SSH.

Password authentication: The module enforces 10-character passwords (at minimum) chosen from the 96 human readable ASCII characters. The maximum password length is 20-characters. Thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million.

The module enforces a timed access mechanism as follows: For the first two failed attempts (assuming 0 time to process), no timed access is enforced. Upon the third attempt, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous (e.g. 4^{th} failed attempt = 10-second delay, 5^{th} failed attempt = 15-second delay, 6^{th} failed attempt = 20-second delay, 7^{th} failed attempt = 25-second delay).

This leads to a maximum of 7 possible attempts in a one-minute period for each getty. The best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $9/(96^{10})$, which is less than 1/100,000.

ECDSA signature verification: SSH public-key authentication. Processing constraints allow for a maximum of 5.6e7 ECDSA attempts per minute. The module supports ECDSA (P-256, P-384, and P-521), which has a minimum equivalent computational resistance to attack of 2^{128} depending on the curve. Thus the probability of a successful random attempt is $1/ (2^{128})$, which is less than 1/1,000,000. Processing speed (partial establishment of an SSH session) limits the number of failed authentication attempts in a one-minute period to 5.6e7 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{128})$, which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Table 13 lists the access to CSPs by each service.

Table 11 - Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset conducted over SSH connection to the management port. The remote reset service is used to perform self-tests on demand.	x	
Load Image	Verification and loading of a validated firmware image	x	

Table 12 - Unauthenticated Services

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services (e.g. OSPF, BGP)
LED Status	Basic

Table 13 - CSP Access Rights within Services

Service	CSPs									
	DRBG_Seed	DRBG_State	Entropy Input String	ECDH Shared Secret	SSH PHK	SSH ECDH	SSH-SEK	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GWR	GWR	--	--	G	W	W
Configure	--	--	--	--	--	--	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect	--	E	--	E	E	GE	GE	--	E	E
Console access	--	--	--	--	--	--	--	--	E	E
Remote reset	GEZ	GZ	GZ	Z	--	Z	Z	Z	--	--
Load Image	--	--	--	--	--	--	--	--	--	--
Local reset	GEZ	GZ	GZ	Z	--	Z	Z	--	--	--
Traffic	--	--	--	--	--	--	--	--	--	--

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g. the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module (persistent storage) Z = Zeroize: The module zeroizes the CSP.

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. The security functions provided by the non-Approved services are identical to the Approved counterparts with the exception of SSH Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.2 and the SSHv2 row of Table 8.

Table 14 - - Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Status (non-compliant)	Show status	x	x
Zeroize (non-compliant)	Destroy all CSPs	x	
SSH connect (non-compliant)	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
Console access (non-compliant)	Console monitoring and control (CLI)	x	x
Remote reset (non-compliant)	Software initiated reset	x	
Load Image (non-compliant)	Verification and loading of a validated firmware image into the switch.	x	

Table 15 - Unauthenticated Services

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services (e.g. OSPF, BGP)
LED Status	Basic

4 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module (Remote reset service).

On power up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the module enters the Critical Failure error state.

The module performs the following power-up self-tests:

- Firmware Integrity check using ECDSA P-256 with SHA-256
- **Kernel KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
- **OpenSSL KATs**
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - ECDSA P-256 Sign/Verify PCT
  - ECDH P-256 KAT
    - Derivation of the expected shared secret.
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-512 KAT
  - KDF-SSH KAT
  - SHA-384 KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
- **LibMD KATs**
  - HMAC SHA-1
  - HMAC SHA-256
  - SHA-512
- Critical Function Test
  - The cryptographic module performs a verification of a limited operational environment, and verification of optional non-critical packages.

The module also performs the following conditional self-tests:

- Continuous RNG Test on the OpenSSL SP 800-90A HMAC-DRBG
- Continuous RNG test on the NDRNG

- Pairwise consistency test when generating ECDSA key pairs.
- Firmware Load Test (ECDSA signature verification)

5 Physical Security Policy

The modules physical embodiment is that of a multi-chip standalone device that meets Level 1 Physical Security requirements. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure.

6 Security Rules and Guidance

6.1 Security Rules

The module design corresponds to the security rules below. The term *must* in this context specifically refers to a requirement for correct usage of the module in the Approved mode; all other statements indicate a security rule implemented by the module.

1. The module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The module requires two independent internal actions to be performed prior to outputting plaintext CSPs.
11. The cryptographic officer must determine whether firmware being loaded is a legacy use of the firmware load service.
12. The cryptographic officer must retain control of the module while zeroization is in process.
13. The Triple-DES encryption key is generated as part of recognized IETF protocols (RFC 4253 SSH). The operator shall ensure that the number of 64-bit blocks encrypted by the same key does not exceed 2^20.
14. Virtual Chassis is not supported in FIPS mode and shall not be configured on the modules.

6.2 Crypto-Officer Guidance

6.2.1 Enabling FIPS mode

When Junos OS is installed on a router and the router is powered on, it is ready to be configured. Initially, you log in as the user root with no password. When you log in as root, your SSH connection is enabled by default.

As Crypto Officer, you must establish a root password conforming to the FIPS password requirements:

1. Passwords must contain between 10 and 20 characters.
2. Passwords must contain at least three of the following five defined character sets:
    a. Uppercase letters
    b. Lowercase letters
    c. Digits
    d. Punctuation marks
    e. Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
3. Authentication requirements. All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size.

When you enable FIPS mode in Junos OS on the router , you cannot configure passwords unless they meet this standard.

To enable FIPS mode in Junos OS on the device:

1. Zeroize the device to delete all CSPs before entering FIPS mode. See section 6.2.2

2. After the device comes up in the factory default state, login using username root and password "" (blank).

3. Configure root authentication.
   root> **edit**
   Entering configuration mode
   [edit]
   root# **set system root-authentication plain-text-password**
   New password:
   Retype new password:
   [edit]
   root# **commit**
   commit complete

4. Load configuration onto device and commit new configuration.

5. Configure chassis boundary fips by setting “set system fips level 1” and commit.

6. The device needs to reboot to enter FIPS mode using the “request system reboot” command.

6.2.2 Zeroize

1. To zeroize the module:

If the module is not in FIPS mode use the command “request system zeroize”. Once the module is in FIPS mode and the module needs to be zeroized use the command “request system zeroize”.

From the CLI, enter:

```
user@router> request system zeroize
warning: System will be rebooted and may not boot without configuration
```

2. To initiate the zeroization process, type yes at the prompt:

```
Erase all data, including configuration and log files? [yes,no] (no) yes
re0:
--------------------------------------------------------------------------
warning: zeroizing re0
```

The entire operation can take considerable time depending on the size of the media, but all critical security parameters (CSPs) are removed within a few seconds. The physical environment must remain secure until the zeroization process is complete.

6.3 User Guidance

All FIPS users, including the Crypto Officer, must observe security guidelines at all times.
All FIPS users must:

- Keep all passwords confidential.
- Store router and documentation in a secure area.
- Deploy router or switches in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
    - Users are trusted.
    - Users abide by all security guidelines.
    - Users do not deliberately compromise security.
- Users behave responsibly at all times.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 - References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*

Table 17 - Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
MD5	Message Digest 5
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SCB	Switch Control Board
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 18 - Datasheets

Model	Title	URL
MX240 MX480 MX960	MX240, MX480, MX960 3D Universal Edge Routers	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000597-en.pdf
MX2010 MX2020	MX2000 3D Universal Edge Routers	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000417-en.pdf
EX9200	EX9200 Ethernet Switch	https://www.juniper.net/us/en/local/pdf/datasheets/1000432-en.pdf