Juniper Networks MX240, MX480, MX960, MX2010, and MX2020 3D Universal Edge Routers with RE-S-X6-64G /REMX2K-X8-64G Routing Engine and Multiservices MPC

Firmware: Junos OS 18.1R1

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.3

Date: February 7, 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 Multiservices Modular PIC Concentrator (MS-MPC). 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.

This MX Series validation includes five models: the MX240, MX480, MX960, MX2010 and MX2020, each loaded with the MS-MPC, which provides hardware acceleration for an array of packet processing-intensive services such as Session Border Control functions, stateful firewall, NAT, flow monitoring, and anomaly detection. This integration allows customers to eliminate external firewalls that consume router ports and additional management resources. The FIPS validated version of firmware is Junos OS 18.1R1.

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

- the outer edge of the chassis and including the Routing Engine (RE), the MS-MPC, Switch Control Board/Switch Fabric Board (SCB)/(SFB) and slot covers in the following configurations:
    - For MX240 (2 available RE slots, 2 additional slots): 1 SCB, 1 RE, and at least 1 MS-MPC. All empty module bays must have a slot cover installed for proper cooling air circulation.
    - For MX480 (2 available RE slots, 6 additional slots): 1 SCB, 1 RE, at least 1 MS- MPC. 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, 1 RE, at least 1 MS-MPC. 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, 1 RE, at least 1 MS-MPC. 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 SCB, 1 RE, at least 1 MS-MPC. 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 module is defined as a multiple-chip standalone module that executes Junos OS 18.1R1firmware on any of the Juniper Networks MX 3D Universal Edge Routers listed in the table below.

Table 1 – Cryptographic Module Hardware Configurations

Chassis PN	Power PN	SCB PN	RE PN	MS PN
MX240	PWR-MX480-2400-DC PWR-MX480-2520-AC	SCBE2-MX	RE-S-X6-64G	MS-MPC
MX480	PWR-MX480-2400-DC PWR-MX480-2520-AC	SCBE2-MX	RE-S-X6-64G	MS-MPC
MX960	PWR-MX960-4100-DC PWR-MX960-DC PWR-MX960-4100-AC PWR-MX960-AC	SCBE2-MX	RE-S-X6-64G	MS-MPC
MX2010	MX2K-PDM-OP-DC MX2000-PDM-DC MX2K-PDM-AC-1PH MX2K-PDM-OP-AC	MX2K-SFB	REMX2K-X8-64G	MS-MPC
MX2020	MX2K-PDM-OP-DC MX2000-PDM-DC MX2K-PDM-AC-1PH MX2K-PDM-OP-AC	MX2K-SFB	REMX2K-X8-64G	MS-MPC

The parts tested for this FIPS 140-2 validation are identified in Table 1.

Juniper also offers an enhanced routing engine that can be used in the MX series routers (RE-S-X6-128G, REMX2K-X8-128G). The enhanced routing engine offers SSDs with more storage capacity (2x100G), and RAM with more memory (128G) than the routing engines tested.

Juniper affirms that the enhanced routing engines use the same cryptographic functions that are available in the routing engines listed in Table 1. However, the RE-S-X6-128G and REMX2K-X8-128G routing engines were not tested for this FIPS 140-2 validation. No claim can be made as to the conformance of the MX series routers with the enhanced routing engine for they were not tested by a CSTL or reviewed by the CMVP.

The module is 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 module has 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 this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

The module does 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. The boundary includes the Routing Engine, MS-MPC, and SCB/SFB. 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)

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 three FIPS Approved modes of operation and one non-Approved mode of operation. The three FIPS Approved modes are identified as FIPS Standard, FIPS Reduced Throughput, and FIPS Recovery. 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 Modes

The Crypto-Officer places the module in an Approved mode of operation by following the instructions in the crypto-officer guidance (section 6.1).

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#) and the output of the "show version" command will include "JUNOS Packet Forwarding Engine Support (fips) [18.1R1]".

In the Standard and Reduced Throughput Approved modes, the module supports the Approved and allowed algorithms, functions and protocols identified in Tables 4 - 11. The services available in these modes are described in Table 13 and Table 15.

The Reduced Throughput mode is automatically selected by the module at power-up when the RE self-tests pass, at least one PIC (each MS-MPC contains 4 PIC) passes its self-tests, and at least one PIC fails its

self-tests. In this mode, the module offers reduced throughput VPN services.

In the Recovery Approved mode, the module supports the OpenSSL, SSH, and LibMD algorithms in Table 4 and Table 5, and the SSH protocol in Table 6. The Recovery mode is automatically selected by the module at power-up if all of the MS-MPC cards fail their power-up self-tests but the RE self-tests pass. In this mode, the module does not offer VPN services. The services available in the Recovery mode are described in Table 14 and Table 15.

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 in the crypto-officer guidance (section 6.1).

1.3 Zeroization

The cryptographic module provides a non-Approved mode of operation in which non-approved cryptographic algorithms are supported. When transitioning between the non-Approved mode of operation and the Approved mode of operation, the Cryptographic Officer must run the following commands to zeroize the Approved mode CSPs:

```
co@device> request vmhost zeroize no-forwarding
```

This command wipes clean all the CSPs and configurations and then reboots the device and sets it to the factory-default configuration.

Use of the zeroize command is restricted to the Cryptographic Officer. The cryptographic officer shall perform zeroization in the following situations:

1. Before FIPS Operation: To prepare the device for operation as a FIPS cryptographic module by erasing all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module.
2. Before non-FIPS Operation: To conduct erasure of all CSPs and other user-created data on a device in preparation for repurposing the device for non-FIPS operation.

Note: The Cryptographic Officer must retain control of the module while zeroization is in process.

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. The Allowed Protocols in Table 10 summarizes the high-level protocol algorithm support.

Table 4 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
2146	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
3623	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication, DRBG Primitive
			SHA-256	Key size: 256 bits, λ = 128, 256	
4386	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation

Table 5 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
3622	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128, 256	
4385	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
5466	AES[1]	PUB 197-38A	CBC, ECB, CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
N/A[2]	CKG	SP 800-133	Section 6.1 Section 6.2		Asymmetric key generation using unmodified DRBG output
1917	CVL (KAS)	SP 800-56A	ECC DH	P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme
1918	CVL	SP 800-135	SSH	SHA 1, 256, 384, 512	Key Derivation
2147	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
1462	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer
3624	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 160	Message Authentication
			SHA-224	Key size: 224 bits, λ = 192	
			SHA-512	Key size: 512 bits, λ = 512	
			SHA-256	Key size: 256, λ = 256	Message Authentication, DRBG Primitive
N/A	KTS		AES Cert. #5466 and HMAC Cert. #3624		Key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #2751 and HMAC Cert. #3624		Key establishment methodology provides

[1] AES GCM in the OpenSSL implementation, was validated by CAVP but is not used for any services
[2] Vendor Affirmed

					112 bits of encryption strength
2936	RSA	PUB 186-4		n=2048 (SHA 256, 512) n=3072 (SHA 256, 512) n=4096 (SHA 256, 512)	KeyGen, SigGen, SigVer[3]
4387	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
			SHA-224		Message Digest Generation
2751	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 7 – QuickSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
5467	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
2148	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
N/A[4]	CKG	SSH-PUB 133	Section 6.1 Section 6.2		Asymmetric key generation using unmodified DRBG output
1919	CVL	SP 800-135	IKEv1	SHA-1, SHA-256, SHA-384	Key Derivation
			IKEv2	SHA-1, SHA-256, SHA-384	
3625	HMAC	PUB 198	SHA-1 SHA-256 SHA-384	Key size: 160 bits, λ = 160	Message authentication
				Key size: 256 bits, λ = 256	
				Key size: 384 bits, λ = 192, 384	
N/A	KTS		AES Cert. #5467 and HMAC Cert. #3625		Key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #2752 and HMAC Cert. #3625		Key establishment methodology provides 112 bits of encryption strength

[3] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.
[4] Vendor Affirmed

4388	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
2752	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 8 – XLP (MS-MPC) Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
5479	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP 800-38D	GCM	Key Sizes: 128,192, 256	Encrypt, Decrypt
1932	CVL (KAS)	SP 800-56A	FFC DH	2048 (SHA 256)	Key Agreement Scheme
			ECC DH	P-256 (SHA 256) P-384 (SHA 384)	Key Agreement Scheme
1468	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384)	SigGen, SigVer
3634	HMAC	PUB 198	SHA-256	Key size: 256, λ = 128	Message authentication.
2943	RSA	PUB 186-4		n=2048 (SHA 256) n=3072 (SHA 256) n=4096 (SHA 256)	SigGen, SigVer[5]
4397	SHS	PUB 180-4	SHA-256		Message Digest ESP Generation
2758	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 9 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
Diffie-Hellman [IG] D.8	Provides 112 bits of encryption strength.	key agreement; key establishment
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

[5] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

Table 10 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1[6]	Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	RSA 2048 RSA 4096 Pre-Shared Secret ECDSA P-256 ECDSA P-384	3 Key Triple-DES CBC AES CBC 128/192/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384
IKEv2[7]	Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	RSA 2048 RSA 4096 Pre-Shared Secret ECDSA P-256 ECDSA P-384	3 Key Triple-DES CBC AES CBC 128/192/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384
IPsec ESP	IKEv1 with optional: Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	IKEv1	3 Key Triple-DES CBC AES CBC 128/192/256 AES GCM[8] 128/192/256	HMAC-SHA-256
	IKEv2 with optional: Diffie-Hellman (L = 2048, N = 256) EC Diffie-Hellman P-256, P-384	IKEv2	3 Key Triple-DES CBC AES CBC 128/192/256 AES GCM[9] 128/192/256	
SSHv2[10]	EC Diffie-Hellman P-256, P-384, P-521	RSA 2048 ECDSA P-256	3 Key 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 IKE and SSH

[6] RFC 2409 governs the generation of the Triple-DES encryption key for use with the IKEv1 protocol
[7] IKEv2 generates the SKEYSEED according to RFC7296, from which all keys are derived to include Triple-DES keys.
[8] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.
[9] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.
[10] RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol

algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 6 above, each column of options for a given protocol is independent and may be used in any viable combination.

2.2 Disallowed 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 with key size less than 2048
- 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

2.3 Critical Security Parameters

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

Table 11 – 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
DH Shared Secret	The shared secret used in Diffie Hellman (DH) key exchange. 256 bits. Established per the Diffie-Hellman key agreement.
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. RSA2048
SSH ECDH	Ephemeral EC Diffie-Hellman private key used in SSH. ECDH P-256, P-384, or P-521
SSH-SEK	SSH Session Keys: SSH Session Encryption Key: 3-Key Triple-DES or AES (128,192,256); SSH Session Integrity Key: HMAC.
ESP-SEK	IPSec ESP Session Keys: ESP Session Encryption Key: 3-Key Triple-DES or AES (128, 192, 256); Session Integrity Key: HMAC. ESP Session Integrity Key: HMAC
IKE-PSK	Pre-Shared Key used to authenticate IKE connections.
IKE-Priv	IKE Private Key. RSA 2048.
IKE-SKEYID	IKE SKEYID. IKE secret used to derive IKE and IPsec ESP session keys.
IKE-SEK	IKE Session Keys: IKE Session Encryption Key: 3-Key Triple-DES or AES (128,192,256); IKE Session Integrity Key: HMAC
IKE-DH-PRI	Ephemeral Diffie-Hellman or EC Diffie-Hellman private key used in IKE. DH (L = 2048, N = 256), ECDH P-256, or ECDH P-384
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 12 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256, RSA 2048, RSA 3072 or RSA 4096
SSH-DH-PUB	Ephemeral EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, P-384, or P-521
IKE-PUB	IKE Public Key ECDSA P-256, ECDSA P-384, RSA 2048.
IKE-DH-PUB	Ephemeral Diffie-Hellman or EC Diffie-Hellman public key used in IKE key establishment. DH 2048 modp, ECDH P-256, or ECDH P-384
Auth-User Pub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P-256, P-384, P-521, RSA 2048, RSA 3072 or RSA 4096
Auth-CO Pub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P-256, P-384, P-521, RSA 2048, RSA 3072 or RSA 4096
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 and establish VPN tunnels.

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 or RSA 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 1/1,000,000.

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 attacks of either 2^{128}, 2^{192} or 2^{256} depending on the curve. 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.

RSA signature verification: SSH public-key authentication. Processing constraints allow for a maximum of 5.6e7 RSA attempts per minute. The module supports RSA (2048, 4096), which has a minimum equivalent computational resistance to attack of 2^{112} (2048). Thus, the probability of a successful random attempt is $1/ (2^{112})$, 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^{112}), which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Table 12 lists the access to CSPs by each service.

Table 13 – Standard and Reduced Throughput Mode Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	IPsec protected routing	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
IPsec connect	Initiate IPsec connection (IKE)	x	
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset, Performs self-tests on demand	x	
Load image	Verification and loading of a validated firmware image into the switch.	x	

Table 14 – Recovery Mode Authenticated Services

Service	Description	CO	ser
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, Performs self-tests on demand	x	
Load image	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

Table 16 – CSP Access Rights within Services

Service	CSPs																
	DRBG_Seed	DRBG_State	Entropy Input String	DH Shared Secret	ECDH Shared Secret	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GW R	GW R	GW R	--	--	--	W R	GW R	--	--	--	G	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	--	--	--	E	--	--	--	E	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z		Z	Z
SSH connect	--	E	--	--	E	E	GE	GE	--	--	--	--	--	--	--	E	E
IPsec connect	--	E	--	E	E	--	--	--	G	E	E	GE	G	GE	--	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	GEZ	GZ	GZ	Z	Z	--	Z	Z	Z	--	--	Z	Z	Z	Z	--	--
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Local reset	GEZ	GZ	GZ	Z	Z	--	Z	Z	Z	--	--	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) and IPSec Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.2 and the SSHv2 row of Table 10. The IPsec (non-compliant) supports the DSA in Section 2.2 and the IKEv1, IKEv2 and IPSec rows of Table 10.

Table 17 – Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	Non-security relevant configuration	x	
Secure Traffic (non-compliant)	IPsec protected routing	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
IPsec connect (non-compliant)	Initiate IPsec connection (IKE)	x	
Console access (non-compliant)	Console monitoring and control (CLI)	x	x
Remote reset (non-compliant)	Software initiated reset, Performs self-tests on demand	x	
Load image (non-compliant)	Verification and loading of a validated firmware image into the switch.	x	

Table 18 -- Non-Approved Recovery Mode Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	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, Performs self-tests on demand	x	
Load image (non-compliant)	Verification and loading of a validated firmware image into the switch.	x	

Table 19 – Unauthenticated traffic

Service	Description
Local reset (non-compliant)	Hardware reset or power cycle
Traffic (non-compliant)	Traffic requiring no cryptographic services

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 for the selected Approved mode of operation must be completed successfully prior to any other use of cryptography by the module. If one of the Routing Engine KATs fails, the module enters the Error state. If one or more of the Multiservices MPC KATs fails, the module selects the Reduced Throughput or Recover Approved mode of operation.

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

Routing Engine:

- Firmware Integrity check using ECDSA P-256 with SHA-256
- Critical Function Test
    - The cryptographic module performs a verification of a limited operational environment, and verification of optional non-critical packages.
- Kernel KATs
    - SP 800-90A HMAC DRBG KAT
        - Health-tests initialize, re-seed, and generate
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - SHA-384 KAT
    - SHA-512 KAT
- QuickSec 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
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - KDF-IKE-V1 KAT
    - KDF-IKE-V2 KAT
    - Triple-DES-CBC Encrypt KAT
    - Triple-DES-CBC Decrypt 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
    - ECDH P-256 KAT
        - Derivation of the expected shared secret.
    - HMAC-SHA-1 KAT

  - HMAC-SHA-224 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-512 KAT
  - KAS-ECC
  - KDF-SSH KAT
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - SHA-384 KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
- LibMD KATs
  - HMAC SHA-1 KAT
  - HMAC SHA-256 KAT
  - SHA-512 KAT

MS-MPC

- XLP (MS MPC) KATs
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - AES-GCM (128/256) Encrypt KAT
  - AES-GCM (128/256) Decrypt KAT
  - ECDSA P-256 Sign/Verify
  - HMAC-SHA-256 KAT
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT

The module also performs the following conditional self-tests:

- Continuous RNG Test on the OpenSSL and QuickSec SP 800-90A HMAC-DRBG
- Continuous RNG test on the NDRNG
- Pairwise consistency test when generating ECDSA, and RSA 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

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 verify that the firmware image to be loaded on the module is a FIPS validated image. If any other non-validated image is loaded the module will no longer be a FIPS validated module.
12. The cryptographic officer must retain control of the module while zeroization is in process.
13. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
14. The operator is required to ensure that Triple-DES keys used in IPsec and SSH do not perform more than 2^20 encryptions.
15. Virtual Chassis is not supported in FIPS mode and shall not be configured on the modules.
16. RSA key generated shall only be 2048 bits or greater.

6.1 Crypto-Officer Guidance

6.1.1 Enabling FIPS-Approved Mode of Operation

The crypto-officer is responsible for initializing the module in a FIPS Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The Crypto-officer should execute the following steps to put the module into the FIPS-Approved Mode of operation:

1. Zeroize the device according to the instructions in the section 1.3.

2. To enable FIPS mode in Junos OS on the device:

   a. Enter configuration mode:

      ```
      co@deivce> configure
      Entering configuration mode
      [edit]
      co@device#
      ```

   b. Enable FIPS mode on the device by setting the FIPS level to 1, and verify the level:

      ```
      [edit]
      co@device# set system fips chassis level 1
      [edit]
      co@device# show system fips chassis level
      level 1;
      ```

   c. Commit the configuration:

      ```
      [edit]
      co@device# commit
      configuration check succeeds
      [edit]
        'system'
          reboot is required to transition to FIPS level 1
      commit complete
      ```

   d. Reboot the device:

      ```
      [edit]
      co@device# run request system reboot
      Reboot the system ? [yes,no] (no) yes
      ```

No further configuration is necessary for the purpose of placing the module in one of the Approved modes of operation. The module will enter the FIPs Standard mode. Section 1.2.1 explains the conditions that will cause the module to enter the FIPS Reduced Throughput or the FIPS Recovery mode of operation.

6.1.2 Placing the Module in a Non-Approved Mode of Operation

As cryptographic officer, the operator needs to disable the FIPS-Approved mode of operation on the device to return it to a non-Approved mode of operation. To disable any of the three FIPS-Approved modes, the module must be zeroized. Follow the steps found in section 1.3 to zeroize the module.

6.2 User Guidance

The user should verify that the module is operating in the desired mode of operation (FIPS-Approved mode or non-Approved mode) by observing the command prompt when logged into the device. If the string ":fips" is present then the device is operating in a FIPS-Approved mode. Otherwise it is operating in a non-Approved mode.

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

All FIPS users must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow below 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 20 – 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 21 – 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
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IPsec	Internet Protocol Security
MD5	Message Digest 5
MIC	Modular Interface Card
MPC	Modular PIC Concentrator
MS	Multiservices
PIC	Port Interface Card
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 22 - 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
MS-MPC	MX Series MS-MPC and MS-MIC Service Cards	http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/ms-mic-and-mpc-overview.html