



Juniper Networks MX80, MX104, MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-64G/RE-S-X6-128G Routing Engine and MIC-MACSEC-20GE MACSec Card

Firmware: Junos OS 18.3R1-S1

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.0

Date: November 24, 2020



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

Contents

1	Introduction	4
1.1	Hardware and Physical Cryptographic Boundary	7
1.2	Modes of Operation	9
1.2.1	FIPS Approved Mode	10
1.2.2	Non-Approved Mode	11
1.3	Zeroization	11
2	Cryptographic Functionality	13
2.1	Allowed Algorithms and Protocols	13
2.2	Disallowed Algorithms and Protocols.....	17
2.3	Critical Security Parameters	17
3	Roles, Authentication and Services	19
3.1	Roles and Authentication of Operators to Roles.....	19
3.2	Authentication Methods	19
3.3	Approved and Allowed Services	20
3.4	Non-Approved Services	22
4	Self-tests.....	24
5	Physical Security Policy.....	25
6	Security Rules and Guidance	26
6.1	Cryptographic-Officer Guidance	27
6.1.1	Installing the FIPS-Approved firmware image	27
6.1.2	Enabling FIPS-Approved Mode of Operation	28
6.1.3	Placing the Module in a Non-Approved Mode of Operation.....	29
6.2	User Guidance	30
7	References and Definitions	31

List of Tables

Table 1 – Cryptographic Module Hardware Configurations	5
Table 2- Security Level of Security Requirements	6
Table 3 - Ports and Interfaces	8
Table 4 – Kernel Approved Cryptographic Functions	13
Table 5 – LibMD Approved Cryptographic Functions	13
Table 6 – OpenSSL Approved Cryptographic Functions	13
Table 7 - QuickSec Approved Cryptographic Functions	15
Table 8 - MACSec Approved Cryptographic Functions	15
Table 9 MACSEC-MIC-20GE VSC8584 and VSC8490 Chips	16
Table 10 – Allowed Cryptographic Functions	16
Table 11 - Protocols Allowed in FIPS Mode	16
Table 12 - Critical Security Parameters (CSPs)	17
Table 13 - Public Keys	18
Table 14 - Authenticated Services in FIPS Standard and Reduced Throughput Modes	20
Table 15 - Authenticated Services in FIPS Recovery Mode	20
Table 16 - Unauthenticated Services in FIPS Standard and Reduced Throughput Modes	20
Table 17 - Unauthenticated Services in Recovery Mode	21
Table 18 - CSP Access Rights within Services	21
Table 19 - Non-Approved Authenticated Services in FIPS Standard and Reduced Throughput Modes 22	
Table 20 - References	31
Table 21 - Acronyms and Definitions	31
Table 22 - Datasheet	32

List of Figures

Figure 1 – Physical Cryptographic Boundary (Left to Right: MX80, MX104, MX240, MX480, MX960)	7
Figure 2 – MIC-MACSEC-20GE MACSec	7
Figure 3 – Routing Engine for the MX240/480/960 devices (RE-S-X6-64G/RE-G-S6-128G)	8

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks MX Series 3D Universal Edge Routers with the RE-S-X6-64G/RE-S-X6-128G Routing Engine and the MACsec MIC (MIC-MACSEC-20GE). 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 FIPS 140-2 validation includes the following MX series router models: the MX80, MX104, MX240, MX480 and MX960. The FIPS validated version of firmware is Junos OS 18.3R1-S1.

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

- the outer edge of the chassis includes the Routing Engine (RE), MIC-MACSEC-20GE MACSec, Switch Control Board (SCB), slot cover in the following configurations:
 - For MX80 (1 Built-in Routing Engine (RE-MX80), 2 additional MIC slots): 1 built-in RE and at least 1 MIC-MACSEC-20GE MACSec. All empty module bays must have a slot cover installed for proper cooling air circulation.
 - For MX104 (2 available RE slots, 4 additional slots): 1 RE (RE-MX104) and at least 1 MIC-MACSEC-20GE MACSec. All empty module bays must have a slot cover installed for proper cooling air circulation.
 - For MX240 (2 available RE slots, 2 additional slots): 1 SCB, 1 RE (RE-S-X6-64G/ RE-S-X6-128G) and at least 1 MIC-MACSEC-20GE MACSec inserted into one MPC (MPC2E-3D-NG). 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 (RE-S-X6-64G/ RE-S-X6-128G) and at least 1 MIC-MACSEC-20GE MACSec inserted into one MPC (MPC2E-3D-NG). 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 (RE-S-X6-64G/ RE-S-X6-128G) and at least 1 MIC-MACSEC-20GE MACSec inserted into one MPC (MPC2E-3D-NG). 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. The cryptographic modules also provide for an encrypted connection, using MACSec protocol, between devices. All other data input or output from the modules are considered plaintext for this FIPS 140-2 validation.

The cryptographic modules are defined as multiple-chip standalone modules that execute Junos OS 18.3R1-S1 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	Power PN	SCB PN	RE PN	MACSec Card PN
MX80	PWR-MX80-T-AC PWR-MX80-T-DC	N/A	Built-in Routing Engine (RE-MX80)	MIC-MACSEC-20GE
MX104	PWR-MX104-DC PWR-MX104-AC	N/A	RE-MX104	MIC-MACSEC-20GE
MX240	PWR-MX480-2400-DC PWR-MX480-2520-AC	SCBE2-MX	RE-S-X6-64G / RE-S-X6-128G	MIC-MACSEC-20GE inserted into MPC2E-3D-NG
MX480	PWR-MX480-2400-DC PWR-MX480-2520-AC	SCBE2-MX	RE-S-X6-64G / RE-S-X6-128G	MIC-MACSEC-20GE inserted into MPC2E-3D-NG
MX960	PWR-MX960-4100-DC PWR-MX960-DC PWR-MX960-4100-AC PWR-MX960-AC-S	SCBE2-MX	RE-S-X6-64G / RE-S-X6-128G	MIC-MACSEC-20GE inserted into MPC2E-3D-NG

The enhanced routing engine RE-S-X6-128G that can be used in the MX series routers (MX240/ MX480/ MX960) offers SSDs with more storage capacity (2x100G), and RAM with more memory (128G) than the other routing engines. Both the RE-S-X6-64G and RE-S-X6-128G routing engines were tested for the FIPS 140-2 validation.

Juniper also offers the following MPCs:

- MPC MX-MPC1E-3D
- MPC MX-MPC1E-3D-Q
- MPC MX-MPC2E-3D
- MPC MX-MPC2E-3D-Q
- MPC MPC2E-3D-NG-Q
- MPC MX-MPC3E-3D
- MPC MPC3E-3D-NG
- MPC MPC3E-3D-NG-Q

Juniper confirms that the MPCs listed above can be used with the MX Series routers listed in Table 1. However, the MPCs listed above provide no cryptographic functionality and were not tested for this FIPS 140-2 validation. The MPCs listed above reside outside the cryptographic boundary and no claim can be made as to the conformance of these MPCs for they were not tested by a CSTL or reviewed by the CMVP.

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
	<i>Overall</i>	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 images below depict the physical boundary of the modules, including the Routing Engine, the MIC-MACSEC-20GE MACSec and the SCB. The cryptographic boundary excludes the non-crypto-relevant line cards included in the figure. The modules exclude the power supplies from the requirements of FIPS 140-2. The power supplies do not contain any security relevant components and cannot affect the security of the module.



Figure 1 – Physical Cryptographic Boundary (Left to Right: MX80, MX104, MX240, MX480, MX960)

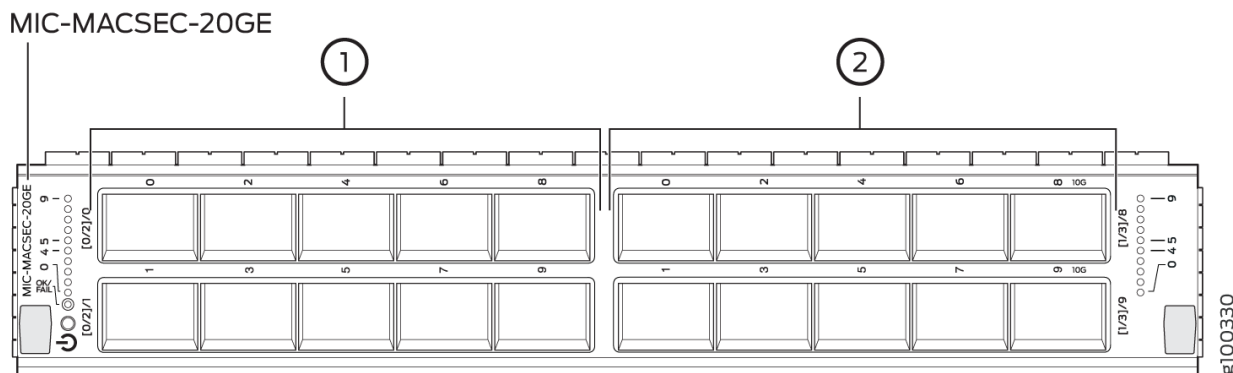


Figure 2 – MIC-MACSEC-20GE MACSec

1 - PICO ports 2 - PIC1 Ports (Ports 8 and 9 are 10-Gbps ports)

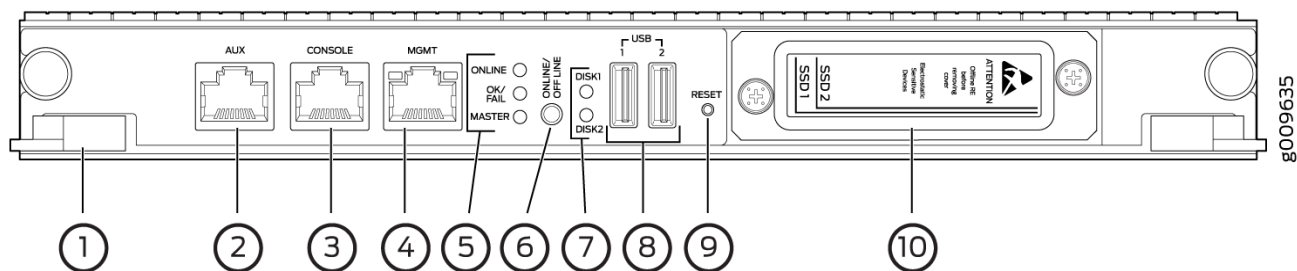


Figure 3 – Routing Engine for the MX240/480/960 devices (RE-S-X6-64G/RE-G-S6-128G)

- 1—Extractor clips
- 2—Auxiliary port (AUX)
- 3—Console port (CONSOLE)
- 4—Management port (MGMT)
- 5—LEDs—ONLINE, OK/FAIL, and MASTER
- 6—ONLINE/OFFLINE button
- 7—SSD LEDs—DISK1 and DISK2
- 8—USB ports—USB1 and USB2
- 9—RESET button
- 10—SSD slots—SSD 1 and SSD 2

Table 3 - Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Ethernet	MX80: Management port (1), 10-Gigabit Ethernet MIC uplink ports (4)	LAN Communications/Remote Management	Control in, Data in, Data out, Status out
	MX104: Management port (1), 10-Gigabit Ethernet SFP+ ports (4)		
	MX240/MX480/MX960 : Management port (1),		
	MIC-MACSEC-20GE interfaces: 1 Gigabit Ethernet SFP ports (20) or 2 10 GE SFP+ ports		

Serial	MX80(1), MX104(1), MX240 (1), MX480 (1), MX960 (1)	Console serial port	Control in, Data in, Data out Status out
USB	MX80(1), MX104(2), MX240 (2), MX480 (2), MX960 (2)	USB port - load Junos image	Control in, Data in
Power	MX80(2), MX104(2), MX240 (4), MX480 (4), MX960 (4)	Power Distribution Modules ¹	Power
Alarm LEDs	MX80(2), MX104(2), MX240 (2), MX480 (2), MX960 (2)	Status indicator lighting	Status out
System status LED (SYS OK)	MX80(1), MX104(1), MX240 (0), MX480 (0), MX960 (0)	Status indicator lighting	Status out
Online/Offline Indicator	MX80(0), MX104(1), MX240 (3), MX480 (3), MX960 (3)	Status indicator lighting	Status out
Master/Slave Indicator	MX80(0), MX104(1), MX240 (3), MX480 (3), MX960 (3)	Status indicator lighting	Status out
Reset Button	MX80(1), MX104(1), MX240 (1), MX480 (1), MX960 (1)	Reset	Control in
Aux	MX80(1), MX104(1), MX240 (1), MX480 (1), MX960 (1)	Disabled	N/A
Backplane	MX80(1), MX104(1), MX240 (1), MX480 (1), MX960 (1)	MIC/ Line card (MPC) backplane interfaces	Control in, Data in, Status out, Data out

1.2 Modes of Operation

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

¹ Power Supplies are excluded from the FIPS 140-2 requirements as they do not contain any security relevant components and cannot affect the security of the module.

1.2.1 FIPS Approved Mode

The hardware versions contained in Table 1, with Junos OS 18.3R1-S1 installed, contain three FIPS-Approved modes of operation and a non-Approved mode of operation. The Junos OS 18.3R1-S1 firmware image must be installed on the device. The module is configured during initialization to operate in an approved mode or a non-approved mode.

The Crypto-Officer places the module in an Approved mode of operation by following the instructions in cryptographic 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#). 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.

The module supports three Approved modes of operation. The three modes are identified as “FIPS Standard Mode”, “FIPS Reduced Throughput Mode” and “FIPS Recovery Mode.”

The FIPS Standard Mode is entered when the module is configured for FIPS mode and successfully passes all the power on self-tests (POST) in both the routing engine (RE) and in each MIC-MACSEC-20GE installed in the chassis of the module (in case of the MX80 routers, a maximum of 2 MIC-MACSEC-20GEs can be installed into the chassis, in case of the MX104 routers, a maximum of 4 MIC-MACSEC-20GEs can be installed into the chassis. For the MX240/MX480/MX960 routers, the MIC-MACSEC-20GE is inserted into a MPC2E-3D-NG line card which in turn is installed into the module chassis. In case of the MX240, MX480 and MX960 routers, a maximum of 2, 6 and 12 MPC2E-3D-NG line cards respectively can be installed into the chassis. A maximum of two MIC-MACSEC-20GEs can be inserted into each of the MPC2E-3D-NG line cards). . The FIPS Standard Mode supports the approved and allowed algorithms, functions and protocols identified in Table 4 – 11. The services available in this mode are described in Tables 14 and 16.

The FIPS Reduced Throughput mode is automatically selected by the module at power-up when all the power on self-tests (POST) in the routing engine (RE) pass successfully, at least one MIC-MACSEC-20GE in the module chassis fails one or more of its self-tests and at least one MIC-MACSEC-20GE in the module chassis passes all of its self-tests. In this mode, the module offers reduced throughput MACsec services. The FIPS Reduced Throughput Mode supports the approved and allowed algorithms, functions and protocols identified in Table 4 – 11. The services available in this mode are described in Tables 14 and 16.

The FIPS Recovery Mode is automatically selected when the module is configured for FIPS mode, at power-up, one or more of the POST fail for each MIC-MACSEC-20GE in the module chassis and all of the RE POST pass successfully. In the FIPS Recovery Mode, the module does not allow MACsec services and shuts down all data ports on each MIC-MACSEC-20GE. The module supports the OpenSSL, LibMD and Kernel algorithms in Table 4-6; the algorithms in Table 10, and the SSH protocol in Table 11 when in the FIPS Recovery mode. The services available in the Recovery mode are described in Table 15 and Table 17.

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 2.2 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 cryptographic 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 FIPS-Approved mode of operation, or vice-versa, the cryptographic officer shall zeroize all keys and CSPs.

Zeroization completely erases all configuration information on the router. To zeroize the system *before* enabling the FIPS mode of operation, the Crypto Officer uses the *“request system zeroize media”* operational command for the MX80 and MX104 routers and the *“request vmhost zeroize no-forwarding”* operational command for the MX240/MX480/MX960 routers from the CLI. The Crypto Officer initiates the zeroization process by entering the *“request system zeroize”* (FIPS) operational command for the MX80 and MX104 routers and by entering the *“request vmhost zeroize no-forwarding”* (FIPS) operational command for the MX240/MX480/MX960 routers from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto 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.

CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The router is returned to the factory default state, without any configured users or configuration files.

To zeroize the router:

1. From the CLI, enter:
For the MX80/MX104 routers:
crypto-officer@router> **request system zeroize**



warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes, no] (no)

For the MX240/MX480/MX960 routers:

crypto-oofficer@router> **request vmhost zeroize no-forwarding**

warning: System will be rebooted and may not boot without configuration

Erase all data, including configuration and log files? [yes, no] (no)

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

Erase all data, including configuration and log files? [yes, no] (no)

yes

3. When the system finishes rebooting the system will be in a factory default state.

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, 9 and 10 below. Table 11 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 this/these table(s).

Table 4 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
C484	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation
C484	HMAC	PUB 198	SHA-1	Key size: 160 bits, $\lambda = 96$	Message Authentication, DRBG Primitive
			SHA-256	Key size: 256 bits, $\lambda = 128, 256$	
C484	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
C485	HMAC	PUB 198	SHA-1	Key size: 160 bits, $\lambda = 96$	Message Authentication
			SHA-256	Key size: 256 bits, $\lambda = 128, 256$	
C485	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
C488	AES ²	PUB 197-38A	CBC, CTR, ECB	Key Sizes: 128, 192, 256	Encrypt, Decrypt

² The AES-ECB mode was used for testing the AES-CTR mode.

N/A ³	CKG	SSH-PUB 133	Section 6.1 Section 6.2		A generated seed used in asymmetric key generation using an unmodified DRBG output
N/A ⁴	KAS-SSC	SP 800-56Arev3	ECC DH	P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme - Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135 (CVL Cert. #C488)
C488	CVL	SP 800-135	SSH	SHA 1, 256, 384, 512	Key Derivation
C488	DRBG	SP 800-90A	HMAC	SHA-256	Random Number Generation
C488	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer, PKV
C488	HMAC	PUB 198	SHA-1	Key size: 160 bits, $\lambda = 160$	Message Authentication
			SHA-224	Key size: 224 bits, $\lambda = 192$	
			SHA-512	Key size: 512 bits, $\lambda = 512$	
			SHA-256	Key size: 256, bits, $\lambda = 256$	Message Authentication, DRBG Primitive
N/A	KTS		AES Cert. #C 488 and HMAC Cert. # C 488		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. # C 488 and HMAC Cert. # C 488		key establishment methodology provides 112 bits of encryption strength
C488	RSA	PUB 186-4		n=2048 (SHA 256, 512) n=3072 (SHA 256, 512)	KeyGen, SigGen, SigVer ⁵

³ Vendor Affirmed

⁴ Vendor Affirmed

⁵ RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA

				n=4096 (SHA 256, 512)	
C488	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
			SHA-224		Message Digest Generation
C488	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 7 - QuickSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
C486	HMAC	PUB 198	SHA-256	Key size: 128-32,768 bits, bits, $\lambda = 128-256$	
C486	SHS	SP800- 180-4	SHA-256		Message Digest Generation, KDF Primitive
C486	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation

Table 8 - MACSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
C502	AES	SP800- 197-38A	ECB, CBC	Key Sizes: 128, 256	AES CMAC
		SP800-38D	CMAC	Key Sizes: 128,256	Key Derivation SP 800-108: Used to generate MACsec keys
		SP800-35F	KW	Key Size: 128	Key Wrapping for MACsec keys
C502	KDF	SP 800-108	Counter	CMAC AES128 CMAC AES256	KDF for MACsec keys
N/A	KTS		AES #C502		Key Wrapping, key establishment methodology provides 128 bits of encryption strength

2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

Table 9 MACSEC-MIC-20GE VSC8584 and VSC8490 Chips

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
3504 (VSC8584), 3505 (VSC8490)	AES	SP800-38D	GCM	Key Sizes: 128,256	Key Derivation SP 800-108: Used to generate MACsec keys

Table 10 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
NDRNG IG 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DRBG

Table 11 - Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
MACsec MKA	MACsec Key Agreement	Shared secret	AES-GCM-128 AES-GCM-256	HMAC-SHA-256
SSHv2 ⁶	EC Diffie-Hellman P-256, P-384, P-521	RSA 2048,4096 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

⁶ RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol

MACsec and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 11 above, each column of options for a given protocol is independent and may be used in any viable combination.

The modules can take on the role of Peer or Authenticator in reference to the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments.

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. The CSPs in Table 12 are used in the FIPS Standard Mode and FIPS Reduced Throughput modes. The FIPS Recovery Mode uses a subset of the CSPs found in Table 12. The MACsec CSPs are not available for use in FIPS Recovery Mode of operation.

Table 12 - 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 Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
SSH PHK	SSH Private host key. 1 st 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-SEKs	SSH Session Keys: SSH Session Encryption Key: 3-Key Triple-DES or AES (128,192,256); SSH Session Integrity Key: HMAC.
MACsec CAK	User-configured PSK entered when MACsec using static connectivity association key (CAK) security mode is enabled (32 characters).
MACsec CKN	User-configured PSK used to identify the CAK (64 characters).
MACsec SAK	Security Association Key used to encrypt/decrypt traffic for a given session. Derived from CAK using KDF SP 800-108. (128-bit AES).
MACsec KEK	Key Encryption Key used to transmit SAK to other members of a MACSec connectivity association. Derived from CAK using KDF SP 800-108. (128-bit AES).
MACsec ICK	Integrity Check Key used to verify the integrity and authenticity of MPDUs. Derived from CAK using KDF SP 800-108. (128/256-bit CMAC).
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 13 - Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256, RSA 2048, 4096.
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 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 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. 4th failed attempt = 10-second delay, 5th failed attempt = 15-second delay, 6th failed attempt = 20-second delay, 7th 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. The module supports ECDSA (P-256, P-384, and P-521), which has a minimum equivalent computational resistance to attack of either 2^{128} , 2^{192} or 2^{256} depending on the curve. Thus, the probability of a successful random attempt is $1/(2^{128})$, which is less than 1/1,000,000. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $15,000/(2^{128})$, which is less than 1/100,000.

RSA signature verification: SSH public-key authentication. 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 $1/1,000,000$. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $15,000/(2^{112})$, which is less than $1/100,000$.

3.3 Approved and Allowed Services

All services implemented by the module are listed in the tables below. Table 18 lists the access to CSPs by each service.

Table 14 - Authenticated Services in FIPS Standard and Reduced Throughput Modes

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	MACsec encrypted transfer of data	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
MACsec connect	Initiate MACsec connection	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	x	

Table 15 - Authenticated Services in FIPS Recovery Mode

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, performs self-tests on demand	x	
Load Image	Verification and loading of a validated firmware image into the switch	x	

Table 16 - Unauthenticated Services in FIPS Standard and Reduced Throughput Modes

Service	Description
---------	-------------

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

Table 17 - Unauthenticated Services in Recovery Mode

Service	Description
Local reset	Hardware reset or power cycle
LED Status	Basic

Table 18 - CSP Access Rights within Services

Service	CSPs														
	DRBG_Seed	DRBG_State	Entropy Input String	ECDH Shared Secret	SSH PHK	SSH ECDH	SSH-SEK	MACsec SAK	MACsec CAK	MACsec CKN	MACsec KEK	MACsec ICK	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GW R	GW R	--	--	GW R	W R	W R	G W	G W	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
SSH connect	--	E	--	E	E	GE	GE	--	--	--	--	--	--	E	E
MACsec connect	--	E	--	--	--	--	--	GE	--	--	GE	GE	--	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	GE Z	GZ	GZ	Z	--	Z	Z	Z	--	--	--	Z	--	--	--
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Local reset	GE Z	GZ	GZ	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). SSH Connect (non-compliant) supports the security functions identified in Section 2.2 and the SSHv2 row of Table 11.

Table 19 - Non-Approved Authenticated Services in FIPS Standard and Reduced Throughput Modes

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	Non-security relevant configuration	x	
Secure Traffic (non-compliant)	MACsec encrypted transfer of data	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
MACsec connect (non-compliant)	Initiate MACsec connection	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 20 – Non-Approved Authenticated Services in FIPS Recovery Mode

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 21 – Non-Approved 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 in the FIPS Standard and Reduced Throughput Modes of operation. If any one of the Routing Engine KATs fails, the module enters the Error state. If all the RE KATs pass and at least one MIC-MACSEC-20GE in the module chassis fails one or more of its self-tests and at least one MIC-MACSEC-20GE in the module chassis passes all of its self-tests, the module selects the FIPS Reduced Throughput Mode of operation and the module offers reduced throughput MACsec services. If all the RE KATs pass and all of the KATs fail for each MIC-MACSEC-20GE in the module chassis, the module selects the FIPS Recovery Mode of operation and all MIC-MACSEC-20GE algorithms are prevented from being used.

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
 - SHA-384 KAT
 - SHA-512 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-224 KAT
 - HMAC-SHA-256 KAT
 - HMAC-SHA-512 KAT
 - KAS -ECC KAT
 - 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
 - HMAC SHA-256
 - SHA-512

- **QuickSec KATs**
 - SP 800-90A HMAC DRBG KAT
 - Health-tests initialize, re-seed, and generate
 - HMAC-SHA-256 KAT

- **MacSec KATs**
 - AES128-CMAC KAT
 - AES256-CMAC KAT
 - AES-ECB (128/256) Encrypt KAT
 - AES-ECB (128/256) Decrypt KAT
 - AES-KEYWRAP KAT

MIC MACSec 20GE

- VSC8584
 - AES GCM KAT
- VSC8490
 - AES GCM KAT
- 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 SP 800-90A HMAC-DRBGs in the OpenSSL and Quicksec libraries.
- 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 module's 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. The module enclosure is made from production grade materials. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow for any sort of observation of any component contained within the cryptographic boundary.

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. The Triple-DES encryption key is generated as part of recognized IETF protocols (RFC 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.
15. RSA key generated shall only be 2048 bits or greater.
16. 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.
17. The module shall only be used with CMVP FIPS 140-2 validation modules when supporting the MACsec protocol for providing Peer, Authenticator functionality.
18. The link between the Peer and Authenticator, used in the MACsec communication, shall be secure to prevent the possibility for an attacker to introduce foreign equipment into the local area network.
19. The module shall not be configured to use a radius server and the radius server capability shall be disabled.

6.1 Cryptographic-Officer Guidance

The cryptographic officer must check to verify the firmware image on the Router is the FIPS 140-2 validated image. If the image is the FIPS 140-2 validated image, then proceed to section 6.1.2.

6.1.1 Installing the FIPS-Approved firmware image

Download the validated firmware image from the <https://www.juniper.net/support/downloads/junos.html>. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives. Select the validated firmware image. Download the firmware image to a local host or to an internal software distribution site.

Connect to the console port on the router from your management device and log in to the Junos OS CLI. Copy the firmware package to the router to the `/var/tmp/` directory. Install the new package on the router:

For the MX 80/MX104 devices:

```
root@router> request system software add /var/tmp/package.tgz.
```

For the MX240/480/960 devices:

```
root@router> request vmhost software add /var/tmp/package.tgz.
```

NOTE: If you need to terminate the installation, do not reboot your router; instead, finish the installation and then issue the `request system software delete package.tgz` command, where `package.tgz` is, for example, `jinstall-ppc-18.3R1.S1-4-signed.tgz`. This is your last chance to stop the installation.

Reboot the router to load the installation and start the new firmware image:

For the MX 80/MX104 devices:

```
root@router> request system reboot
```

For the MX240/480/960 devices:

```
root@router> request vmhost reboot
```

After the reboot has completed, log in and use the `show version` command to verify that the new version of the firmware is successfully installed.

Also install the `fips-mode` package and `jpfe-fips` package needed for Routing Engine KATS and for MIC-MACSEC-20GE KATS. The following are the commands used for installing these packages:

For the MX80/MX104 devices:

```
root@router> request system software add fips-mode-powerpc-18.3R1.S1-4signed.tgz
```

```
root@router> request system software add jpfe-fips-powerpc-18.3R1.S1-4-signed.tgz
```

For the MX240/MX480/MX960 devices:

```
root@router > request system software add optional://fips-mode.tgz
```

```
root@router > request system software add optional://jpfe-fips.tgz
```

6.1.2 Enabling FIPS-Approved Mode of Operation

The cryptographic 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 cryptographic officer shall place the module in FIPS-Approved mode by first zeroizing the device to delete all keys and CSPs. The zeroizing instructions are in section 1.3 of this document. Next, the cryptographic officer shall follow the steps found in the *Junos OS FIPS Evaluated Configuration Guide for MX80, MX104, MX240, MX480, MX960 Devices, Release 18.3R1* document Chapters 3 & 7 to place the module into a FIPS-Approved mode of operation. The steps from the aforementioned document are repeated below:

The FIPS Modes are not automatically enabled once the firmware image is installed on the platform. These steps are for putting the module into the FIPS Standard Mode, FIPS Reduced Throughput Mode or FIPS Recovery Mode.

The FIPS Standard Mode will be selected automatically if all power-on self-tests pass successfully during the reboot after committing the module to FIPS mode. The FIPS Reduced Throughput Mode of operation is selected automatically if all the RE KATs pass and at least one MIC-MACSEC-20GE in the chassis fails one or more of its self-tests and at least one MIC-MACSEC-20GE in the module chassis passes all of its self-tests. The FIPS Recovery Mode is selected automatically if all the RE KATs pass and all of the KATs fail for each MIC-MACSEC-20GE in the module chassis. To enable FIPS mode in Junos OS on the router:

1. Zeroize the device as explained in Section 1.3.
2. Login to the device with crypto-officer credentials and enter configuration mode:


```
crypto-officer@router> edit
Entering configuration mode
[edit]
crypto-officer@router#
```
3. Enable FIPS mode on the router by setting the FIPS level to 1, and verify the level:


```
[edit]
crypto-officer@router# set system fips chassis level 1
```



```
crypto-officer@router# show system fips
chassis level 1;
```
4. Commit the configuration


```
[edit ]
crypto-officer@router# commit
configuration check succeeds
```

```
Generating RSA key /etc/ssh/fips_ssh_host_key
Generating RSA2 key /etc/ssh/fips_ssh_host_rsa_key
Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
[edit]
'system'
reboot is required to transition to FIPS level 1
commit complete
```

5. Reboot the router:

For the MX80/MX104 routers:

```
[edit]
crypto-officer@router> request system reboot
Reboot the system ? [yes,no] (no) yes
```

For the MX240/MX480/MX960 routers:

```
[edit]
crypto-officer@router> request vmhost reboot
Reboot the system ? [yes,no] (no) yes
```

During the reboot, the router runs Known Answer Tests (KATS). It returns a login prompt:

```
crypto-officer@router:fips>
```

6. After the reboot has completed, log in and use the show version local command to verify the firmware version is the validated version.

```
crypto-officer@router:fips> show version
```

7. Configure local login authentication for FIPS users.

8. Configure the console port to log out automatically when you unplug the cable and require the root password for single-user mode, this can be done by enabling the log-out-on-disconnect⁷ configuration statement.

9. Configure FIPS logging to record events.

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

As cryptographic officer, the operator may need to disable the FIPS-Approved mode of operation on the

⁷ The log-out-on-disconnect option is not operational on MX80 routers. On MX80 routers you must manually log out from the console with the request system logout u0 command

router to return it to a non-Approved mode of operation. To disable FIPS-Approved mode on the router, the router must be zeroized. Follow the steps found in section 1.3 to zeroize the router.

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 router. If the string “:fips” is present then the router 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 routers and documentation in a secure area.
- Deploy routers 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 20 - References

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

Table 21 - Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CAK	Connectivity Association Key
CKN	Connectivity Association Key Name
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
ICV	Integrity Check Value (i.e. Tag)
ICK	Integrity Check Key
KEK	Key Encrypting Key
MACsec	Media Access Control Security
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 22 - Datasheet

Model	Title	URL
MX80 MX104 MX240 MX480 MX960	MX Series 5G Universal Routing Platforms	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000597-en.pdf