Juniper Networks MX104 3D Universal Edge Router with the Multiservices MIC

Firmware: Junos OS 19.1R2

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.0

Date: April 27, 2021

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

Copyright Juniper, 2021

Version 1.0

Juniper Networks Public Material – May be reproduced only in its original entirety (without revision).

Page 3 of 26

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks MX104 3D Universal Edge Router with Multiservices MIC.

The Juniper Networks MX104 3D Universal Edge Router is optimized for aggregating mobile, enterprise WAN, business, and residential access services. The MX104 router is designed for high-density access and pre-aggregation and is environmentally hardened to allow outside deployments in cabinets and remote terminals. The router is a high-performance router functioning as a universal aggregation platform for mobile broadband and metro Ethernet applications. It also acts as a universal edge platform supporting all types of private WAN, data center interconnect, Internet edge, business edge, and residential edge services.

The router is powered by the Junos Trio chipset and runs the Junos® operating system (Junos OS) for high-performance routing and routering. The FIPS validated version of firmware is Junos OS 19.1R2.

The cryptographic module is defined as a multiple-chip standalone module that executes Junos OS 19.1R2 firmware on the MX-104 chassis. The cryptographic boundary is defined in section 1.1. Tested hardware configurations are listed in the table below:

Table 1 – Cryptographic Module Hardware Configurations

Chassis PN	Power PN	Blank Cover	RE PN	MIC PN
MX104	PWR-MX104-DC PWR-MX104-AC	Blank MIC cover	RE-MX104	MS-MIC-16G

The module is designed to meet FIPS 140-2 Level 1 overall. Table 2 specifies the security levels for each area defined in FIPS 140-2:

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. Any firmware versions other than Junos OS 19.1R2, loaded into the modules are 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.

Figure 1 depicts the physical boundary of the module. The boundary is the outer edge of the chassis including the Routing Engine (RE), MS-MIC-16G, System Control Board (SCB) and slot covers. The cryptographic boundary excludes the non-crypto-relevant line cards with the backplane port serving as the physical interfaces. 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.
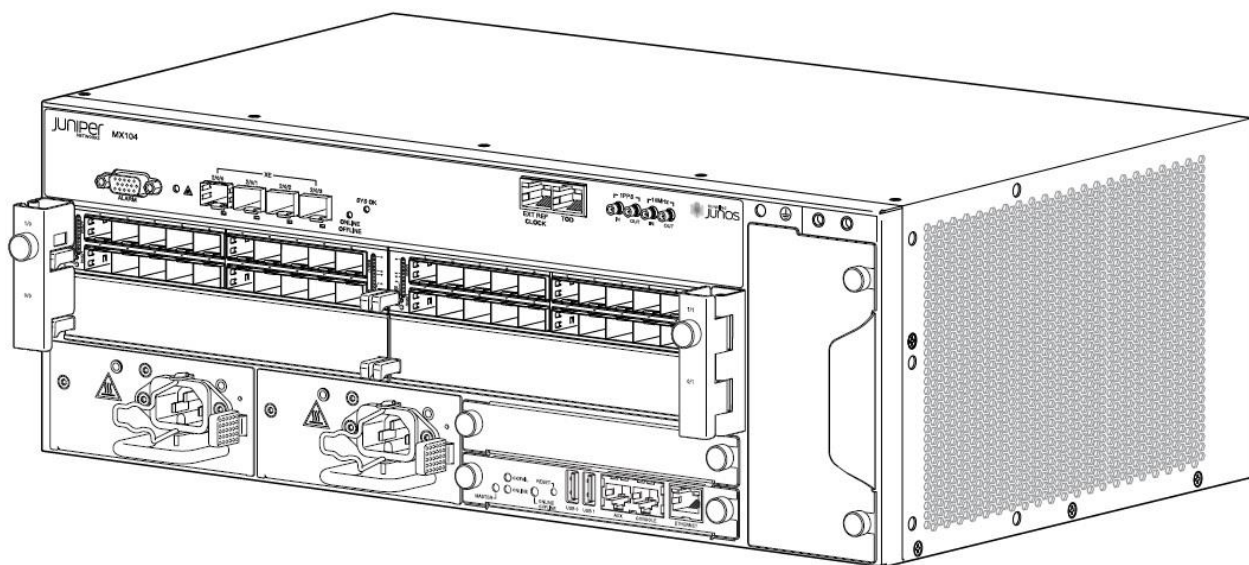

Figure 1 – MX104 Cryptographic Boundary

Figure 2 shows the physical ports that are identified in Table 3. The line card is not within the cryptographic boundary and obscures the backplane ports in the diagram.
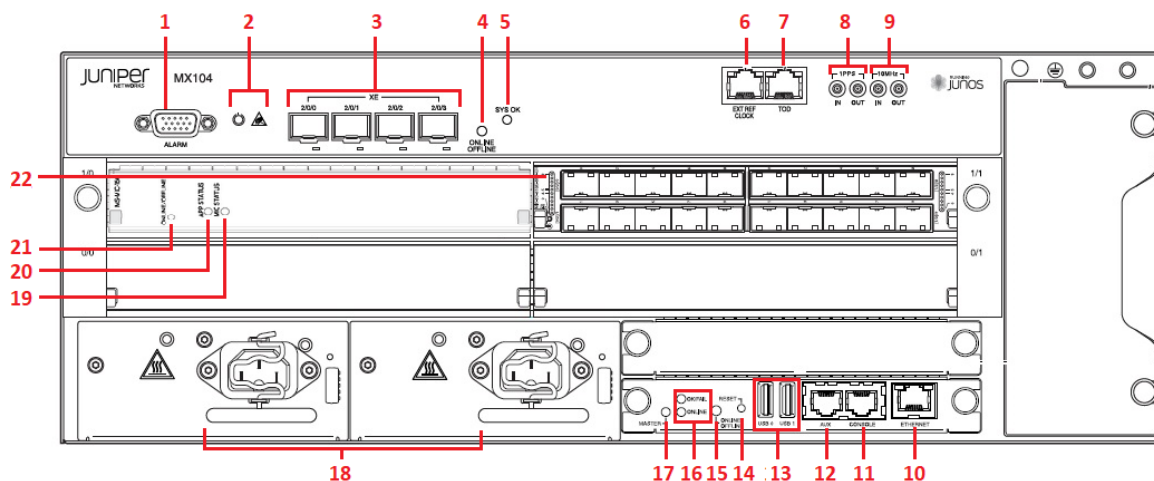

Figure 2 – MX104 – Ports and Interfaces

Table 3 – Ports and Interfaces

Index	Description(Quantity)	Logical Interface Type
1	Alarm input and output contacts(1)	Status out
2	Alarm LEDs(2)	Status out
3	10-Gigabit Ethernet SFP+ ports(4)	Data in, Data out
4	Online/offline button(1)	Control in
5	System status LED(1)	Status out
6	External reference clocking port(1)	Control in, Status out
7	Time-of-day (ToD) port(1)	Control in, Status out
8	1-PPS input port(1) 1-PPS output port(1)	Control in, Status out
9	10-MHz GPS input port(1) 10-MHz GPS output port(1)	Control in, Status out
10	Ethernet management port(1)	Data in, Data out, Control in, Status out
11	Serial Console(1)	Data in, Data out, Control in, Status out
12	Aux (not supported) (1)	N/A
13	USB Ports(2)	Data in, Control in
14	Reset Button(1)	Control in
15	Online/Offline Button(1)	Control in
16	OK/Fail Indicator(1) Online/Offline Indicator(1)	Status out
17	Master/Slave Indicator(1)	Status out
18	Power Distribution Modules[1](2)	Power
19	MIC Status Indicator(1)	Status out
20	App Status Indicator(1)	Status out
21	MIC Online/Offline Button(1)	Control in
22	Line Card Backplane Interface[2](1)	Data in, Data out

1.2 Modes of Operation

The module supports two FIPS Approved modes of operation and a non-Approved mode of operation. The module must always be zeroized when routering 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 may place the module in an Approved mode by following the instructions in the Crypto Officer guidance (section 6.1). The operator can verify that the module is in FIPS-Approved mode by observing the console prompt in the CLI and running the "show version" command. When operating in FIPS-Approved mode, the prompt will read "<user>@<device name>: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 chassis level" command to determine if the module is

---

[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.

[2] The backplane line card interface is obscured by the line card in the diagram.

operating in FIPS mode.

The module supports two Approved modes of operation. The two modes are identified as "FIPS Standard 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 the Multiservices MIC. The FIPS Standard Mode supports the approved and allowed algorithms, functions and protocols identified in Table 4 – 10. The services available in this mode are described in Tables 13 and 15.

The FIPS Recovery Mode is entered when the module is configured for FIPS mode and if at power-up any of the Multiservices MIC POST fails but the RE POST all pass successfully. In the FIPS Recovery Mode, the module does not allow IPsec services. The module supports the OpenSSL, LibMD and Kernel algorithms in Tables 4-6; the ECDH and NDRNG algorithms in Table 9, and the SSH protocol in Table 10 when in the FIPS Recovery mode. 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 Crypto Officer must zeroize the module while routering from a FIPS Approved mode of operation to the Non-Approved mode of operation and vice versa. Zeroization completely erases all configuration information on the router. Use of the zeroize command is restricted to the Crypto Officer. The Crypto 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 device is returned to the factory default state, without any configured users or configuration files.

To zeroize the device:

1. From the CLI, enter

> crypto-officer@device> 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)

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 Crypto Officer must retain control of the module while zeroization is in process.

2 Cryptographic Functionality

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 used by the module in FIPS mode. 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
C1179	DRBG	SP800-90A	HMAC SHA-256	SP800-90A HMAC SHA-256 DRBG	Random Bit Generation
C1179	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128 , 256	
C1179	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
C1180	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication, KDF Primitive
			SHA-256	Key size: 256 bits, λ = 128, 256	
C1180	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
C1181	AES	PUB 197-38A	CBC, ECB, CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
N/A[3]	CKG	SSH-SP 800-133rev2	Section 5.1 Section 5.2		Asymmetric key generation using unmodified DRBG output
			Section 6.2.1		Derivation of symmetric keys

---

[3] Vendor Affirmed

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
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 - Shared Secret Computation
C1181	CVL	SP 800-135	SSH	SHA 1, 256, 384, 512	Key Derivation
C1181	DRBG	SP 800-90A	HMAC	SHA-256	Random Number Generation
C1181	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer, PKV
C1181	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, bits, λ = 256	Message Authentication, DRBG Primitive
N/A	KTS		AES Cert. #C1181 and HMAC Cert. #C1181		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #C1181 and HMAC Cert. #C1181		key establishment methodology provides 112 bits of encryption strength
C1181	RSA	PUB 186-4		n=2048 (SHA 256, 512) n=3072 (SHA 256, 512) n=4096 (SHA 256, 512)	KeyGen[5], SigGen, SigVer[6]
C1181	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
			SHA-224		Message Digest Generation
C1181	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

[4] Vendor Affirmed per IG D.1rev3

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

[6] 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 7 – QuickSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description		Functions
C1182	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256		Encrypt, Decrypt
C1182	DRBG	SP 800-90A	HMAC	SHA-256		Random Bit Generation
N/A[7]	CKG	SP 800-133rev2	Section 5.1 Section 5.2			Asymmetric key generation using unmodified DRBG output
			Section 6.2.1			Derivation of symmetric keys
C1182	CVL	SP 800-135	IKEv1	SHA-1, SHA-256, SHA-384		Key Derivation
			IKEv2	SHA-1, SHA-256, SHA-384		
C1182	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. #C1182 and HMAC Cert. #C1182			key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. #C1182 and HMAC Cert. #C1182			key establishment methodology provides 112 bits of encryption strength
C1182	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384			Message Digest Generation
C1182	Triple-DES	SP 800-67	TCBC	Key Size: 192		Encrypt, Decrypt

Table 8 – XLP (MS-MIC-16G) Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
C1203	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP800-38D	GCM	Key Sizes: 128,192, 256	Encrypt, Decrypt
N/A[8]	KAS-SSC	SP 800-56Arev3	FFC DH	mod 2048 (SHA-256)	Key Agreement Scheme - Shared
			ECC DH	P-256 (SHA 256)	

---

[7] Vendor Affirmed

[8] Vendor Affirmed per IG D.1rev3

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
				P-384 (SHA 384)	Secret Computation
C1203	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384)	SigGen, SigVer
C1203	HMAC	PUB 198	SHA-256	Key size: 256, λ = 128	Message authentication.
C1203	RSA	PUB 186-4		n=2048 (SHA 256) n=3072 (SHA 256) n=4096 (SHA 256)	SigGen, SigVer[9]
C1203	SHS	PUB 180-4	SHA-256		Message Digest ESP Generation
C1203	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 9 – 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 10 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1[10]	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[11]	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[12] 128/192/256	HMAC-SHA-256

[9] 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.

[10] RFC 2409 governs the generation of the Triple-DES encryption key for use with the IKEv1 protocol

[11] IKEv2 generates the SKEYSEED according to RFC7296, from which all keys are derived to include Triple-DES keys.

Protocol	Key Exchange	Auth	Cipher	Integrity
	IKEv2[12] 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[13] 128/192/256	
SSHv2[14]	EC Diffie-Hellman P-256, P-384, P-521	RSA 2048 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 IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 10 above, each column of options for a given protocol is independent and may be used in any viable combination.

2.1 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

---

[12] IKEv2 is compliant with RFC 7296 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived.

[13] 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. The implementation of the management logic for the last 64 bits of the "nonce" (the IV in RFC 5282) inside the module ensures that when the nonce (i.e. IV in RFC 5282) exhausts the maximum number of possible values for a given security association, i.e., after $0.8*2^{32}$ values have been used (which is less than the $(2^{64})-1$ requirement), either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association per RFC 7296.

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

- OpenSSL AES GCM

Protocols

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

2.2 Critical Security Parameters

All CSPs and public keys used by the module are described in this section. The CSPs in Table 11 are used in the FIPS Standard Mode. The FIPS Recovery Mode uses a subset of the CSPs found in Table 11. The IPsec CSPs are not available for use in FIPS Recovery Mode of operation.

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. RSA 2048
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: TDES (3key) 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); ESP Session Integrity Key: HMAC
IKE-PSK	Pre-Shared Key used to authenticate IKE connections. RSA 2048, RSA 4096, ECDSA P-256, or ECDSA P-384
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: TDES (3key) or AES; 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, RSA 4096
SSH-ECDH-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 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 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: Crypto 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 Crypto Officer role configures and monitors the module via a console or SSH connection. As root or super-user, the Crypto 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 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 16 lists the access to CSPs by each service.

Table 13 – Authenticated Services in FIPS Standard Mode

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 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 into the router.	x	

Table 14 – 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 conducted over SSH connection to the management port. The remote reset service is used to perform self-tests on demand.	x	

Service	Description	CO	User
Load Image	Verification and loading of a validated firmware image into the router.	x	

Table 15 – Unauthenticated Services in FIPS Standard Mode

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

Table 16 – Unauthenticated Services in FIPS Recovery Mode

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

Table 17 – CSP Access Rights within Services

Service	DRBG_Seed	DRBG_State	Entropy Input String	DH Shared Secret	ECDH Shared Secret	SSH PHK	SSH ECDH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GWR	GWR	GWR	--	--	--	WR	GWR	--	--	--	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	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	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Service	CSPs																
	DRBG_Seed	DRBG_State	Entropy Input String	DH Shared Secret	ECDH Shared Secret	SSH PHK	SSH ECDH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
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 18 – Non-Approved Authenticated Services in non-FIPS Mode

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	

Service	Description	CO	User
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 router.	x	

Table 19 – Non-Approved Unauthenticated Services in non-FIPS Mode

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services
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 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 the Multiservices MIC KAT fails, the module selects the Recovery FIPS mode of operation.

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

Routing Engine (RE):
- 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
- 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 PCT
  - 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

- o RSA 2048 w/ SHA-256 Verify KAT
- o SHA-384 KAT
- o Triple-DES-CBC Encrypt KAT
- o Triple-DES-CBC Decrypt KAT
- LibMD KATs
  - o HMAC SHA-1
  - o HMAC SHA-256
  - o SHA-512

MS-MIC-16G:
- XLP (MS-MIC-16G) KATs
  - o AES-CBC (128/192/256) Encrypt KAT
  - o AES-CBC (128/192/256) Decrypt KAT
  - o AES-GCM (128/256) Encrypt KAT
  - o AES-GCM (128/256) Decrypt KAT
  - o ECDSA P-256 Sign/Verify PCT
  - o HMAC-SHA-256 KAT
  - o RSA 2048 w/ SHA-256 Sign KAT
  - o RSA 2048 w/ SHA-256 Verify KAT
  - o Triple-DES-CBC Encrypt KAT
  - o Triple-DES-CBC Decrypt KAT

- **Critical Function Test**

  - o 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.
- SP800-90A Health-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. 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 Crypto 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 Crypto Officer must retain control of the module while zeroization is in process.
13. If the module loses power and then it is restored, a new key is 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.
17. 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 Crypto Officer (CO) must check to verify the firmware image on the module is the FIPS 140-2 validated image. If the image is the FIPS 140-2 validated image, then proceed to section 6.1.2. If the module does not contain the validated firmware, then the CO shall follow the instructions in the *Common Criteria and FIPS Evaluated Configuration Guide for MX104 Routers to* download and install the validated firmware.

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

> user@device> request system software add /var/tmp/*package*.tgz.

NOTE: If you need to terminate the installation, do not reboot your device; instead, finish the installation and then issue the request system software delete *package*.tgz command, where *package*.tgz is, for example, jinstall-ppc-19.1R2.8-signed.tgz. This is your last chance to stop the installation.

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

> user@device> request system 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.

6.1.2 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 shall place the module in the 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 Crypto Officer shall follow the steps found in the *Common Criteria and FIPS Evaluated Configuration Guide for MX104 Routers* 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 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 Recovery Mode is selected automatically if all the RE KATs pass and if each of the MS-MIC-16Gs in the chassis fails one or more of its KATs. To enable FIPS mode in Junos OS on the device:

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

2. After the device comes up in 'Amnesiac mode', login using the console port with username root and password " " (blank).

   Amnesiac (ttyu0)
   login: root
   --- JUNOS 19.1R2.8 built 2020-05-22 03:01:33 UTC

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. Configure the Crypto Officer and login with Crypto Officer credentials.

5. Install fips-mode package needed for Routing Engine KATS and the jpfe-fips package needed for MS-MIC-16G KATS.

   crypto-officer > request system software add /var/tmp/fips-mode-powerpc-19.1R2.8.tgz no-validate.
   crypto-officer > request system software add /var/tmp/jpfe-fips-powerpc-19.1R2.8.tgz no-validate

6. Configure fips mode by setting "set system fips chassis level 1" and commit.

   [edit]
   crypto-officer@device # **set system fips chassis level 1**
   [edit]
   crypto-officer@device # **show system fips chassis level**
   level 1;

   [edit]
   crypto-officer@device# **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

7. Reboot the device:
 [edit]
crypto-officer@device# **run request system reboot**
Reboot the system ? [yes,no] (no) **yes**

During the reboot, the device runs the Known Answer Tests (KATS). It returns a login
Prompt as follows:
crypto-officer@device:fips>

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 Recovery mode of operation.

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

As Crypto 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 two FIPS-Approved modes, the module must be zeroized. Follow the steps found in section 1.3 to zeroize the module. Zeroizing the module will return the module to the factory default state.

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 Port Concentrator
MS	Multiservices
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SCB	Router Control Board
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 22 – Datasheets

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