FIPS 140-3 Non-Proprietary Security Policy

Juniper Networks EX4300-48MP Ethernet Switch

Firmware Version: Junos OS 22.4R2.8

Document Version: 1.0

Date: December 28th, 2023

Prepared by:

intertek acumen security

www.acumensecurity.net

Table of Contents

List of Tables

List of Figures

1. General

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-3 program. The NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program.

About this Document

This non-proprietary Cryptographic Module Security Policy for the Juniper Networks, Inc. Juniper Networks EX4300-48MP Ethernet Switch provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-3.

The Juniper Networks EX4300-48MP Ethernet Switch may also be referred to as the “module” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Juniper Networks shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

This document describes the cryptographic module security policy for the Juniper Networks, Inc. Juniper Networks EX4300-48MP Ethernet Switch (Hardware version EX4300-48MP) cryptographic module (also referred to as the "module" hereafter) with firmware version Junos OS 22.4R2.8. The module has a multi-chip standalone embodiment. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

The following table lists the level of validation for each area in FIPS 140-3:

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	3
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A

Table 1 - Security Levels

The module claims an overall Security Level 1.

2. Cryptographic Module Specification

The version of the module are as follows:

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
EX4300-48MP	EX4300-48MP	Junos OS 22.4R2.8	Power PN: JPSU-1400-AC-AFO RE PN: Built-in Routing Engine (EX4300-48MP RE)

Table 2 – Cryptographic Module Tested Configuration

Module Usage and Cryptographic Boundary

The cryptographic module provides for an encrypted connection, using SSH, between the management station and the module. The cryptographic module also provides for an encrypted connection, using MACsec, between devices.

The cryptographic module's operational environment is a limited operational environment. The images below depict the cryptographic boundary of the hardware module (the entirety of the module/chassis, demarked with the red outline in Figure 5). This includes the Routing Engine (RE). No components have been excluded from the cryptographic boundary of the module.

Figure 1 – EX4300-48MP (Front Panel)

Figure 2 - EX4300-48MP (Rear Panel)

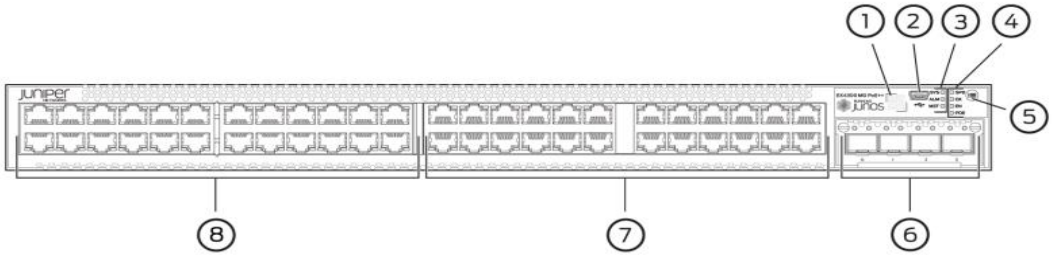

Figure 3 - EX4300-48MP Schematic (Front Panel)

1 —QR code

2 —Mini-USB console port

3 —Chassis status LEDs

4 —Port status mode LEDs

5 — Factory Reset/Mode button

6 — 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet SFP+ uplink module

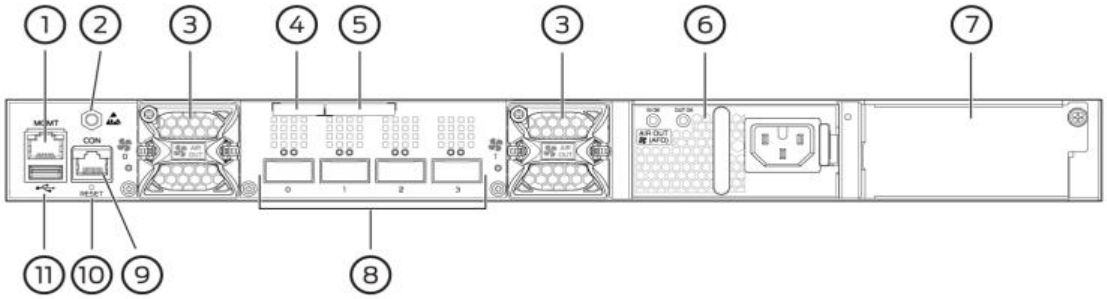

Figure 4 - EX4300-48MP Schematic (Rear Panel)

1 —Management port

2 —ESD point

3—Fan module

4—Serial number label

5—CLEI code label

6—AC power supply in slot 0

7—Empty slot for AC power supply

8—QSFP+ ports (dedicated Virtual Chassis ports)

9—Console port

10—Reset button

11—USB port

The module claims an overall Security Level of 1 with all individual sections at a Security Level 1 with the exceptions of Roles, Services and Authentication (claimed at Security Level 3). The module does not implement any non-invasive security mitigations or mitigations of other attacks and thus the requirements per these sections are inapplicable.

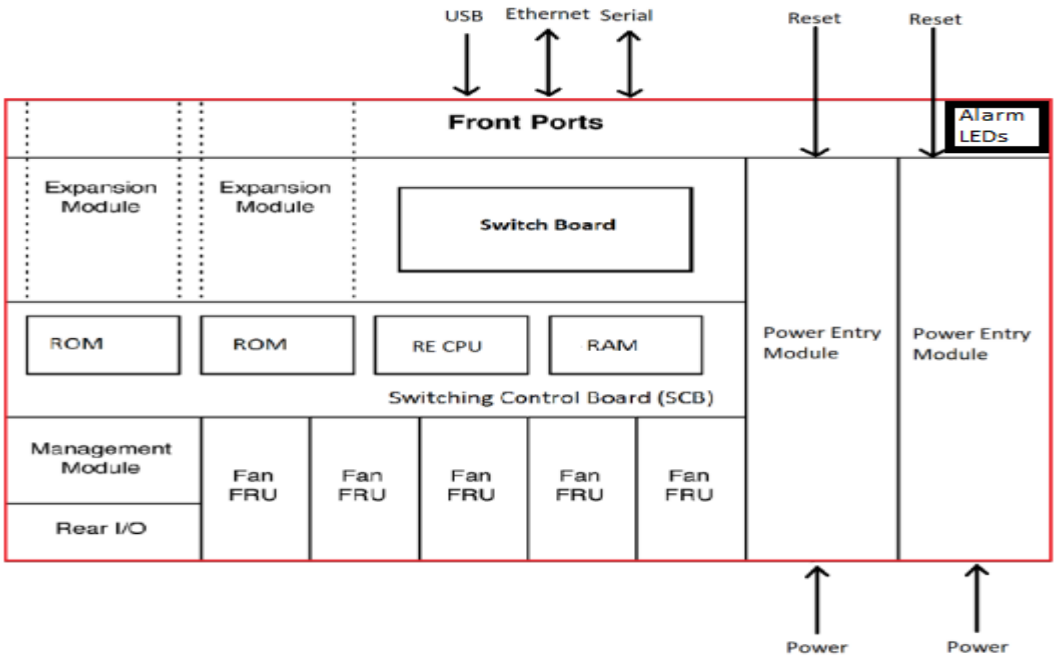

Figure 5 – Block Diagram for EX4300-48MP

Modes Of Operation

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

Approved Mode

The hardware versions contained in Table 2, with Junos OS 22.4R2.8 installed, contain one Approved mode of operation and a non-Approved mode of operation. The Junos OS 22.4R2.8 firmware image must be installed on the module. The module is configured during initialization by the Crypto Officer to operate in the Approved mode or the non-Approved mode. The Crypto Officer can place the module in the Approved mode of operation by following the instructions specified in Section 11 Life-Cyle Assurance in this document (Crypto Officer guidance).

The Crypto Officer can verify that the cryptographic module is in the Approved mode by observing the console prompt and running the “show version” command. When operating in the Approved mode, the prompt will read “<operator>@<device name>:fips#” (e.g. crypto-officer@ EX4300-48MP: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 (returns “level 1”) to determine if the module is operating in the Approved mode.

The Approved mode is entered when the module is configured for it and successfully passes all self-tests (both pre-operational and conditional cryptographic algorithm self-tests (CASTs)). The CASTs must pass in both the routing engine (RE).

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 non-Approved algorithms identified below in this section as well as the algorithms supported in the Approved mode of operation. The Crypto Officer can place the module into the non-Approved mode of operation by following the instructions in the Section 11 Life-Cyle Assurance in this document (Crypto Officer guidance).

Degraded Operation

The module does not support a degraded mode of operation.

Overall Security Rules of Operation

The module design corresponds to the security rules below. The term *shall* 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. Self-tests do not require any operator action.
4. Data output is inhibited during SSP generation, self-test execution, zeroisation, and error states.
5. Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which SSPs are zeroised by the zeroisation service.
7. The module does not support a maintenance interface or role.
8. The module does not output intermediate key values.
9. The module does not output plaintext CSPs.
10. The Crypto officer shall verify that the firmware image to be loaded on the module is a FIPS 140-3 validated image. If any non-validated firmware image is loaded the module will no longer be a validated module.
11. The Crypto Officer shall retain control of the module while zeroisation is in process.
12. The virtual chassis feature is not supported in Approved mode and shall not be configured on the module.
13. MACsec protocol IV generation:
    - The AES GCM IV construction is performed internal to the module in compliance with IEEE 802.1AEand its amendments. The IV length is 96 bits (per SP 800-38D). The module ensures the IV is constructed deterministically per Section 8.2 in SP 800-38D and the MACsec standard IEEE 802.1AE as a result of concatenating the fixed field (SCI) and invocation field (PN).
    - The module can take on the role of Peer or Authenticator in reference to the MACsec protocol.
    - The module shall only be used with other FIPS 140-3 validated modules when supporting the MACsec protocol in the role of a Peer/Authenticator for providing the remaining functionalities.
    - 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.
    - 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.
14. The module shall not be configured to use a radius server and the radius server capability shall be disabled.
15. No parts of the SSH and MACsec protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4301	AES-CBC	CBC	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt
A4301	AES-CTR	CTR	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt
A4301	AES-ECB	ECB	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt
A4301	AES-GCM	GCM	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt
A4301	ECDSA KeyGen (FIPS186-4)	ECDSA KeyGen	Curve sizes P-256, P-384, P-521 with 128 to 256 bits of strength	Key Generation
A4301	ECDSA KeyVer (FIPS186-4)	ECDSA KeyVer	Curve sizes P-256, P-384, P-521 with 128 to 256 bits of strength	Key Verification
A4301	ECDSA SigGen (FIPS186-4)	ECDSA SigGen	Curve sizes P-256 (SHA2-256), P-384 (SHA2-384), P-521 (SHA2-512) with 128 to 256 bits of strength	Signature Generation
A4301	ECDSA SigVer (FIPS186-4)	ECDSA SigVer	Curve sizes P-256 (SHA2-256), P-384 (SHA2-384), P-521 (SHA2-512) with 128 to 256 bits of strength	Signature Verification
A4301	HMAC DRBG	HMAC-SHA2-256	Key size 256-bits with 256-bits of key strength	Random Bit Generation
A4301	HMAC-SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Authentication, DRBG Primitive

[1] There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4301	HMAC-SHA2-256	SHA2-256	SHA2-256: Key size: 256 bits with 256-bits of key strength	Message Authentication, DRBG Primitive
A4301	HMAC-SHA2-512	SHA2-512	SHA2-512: Key size: 512 bits with 512-bits of key strength	Message Authentication, DRBG Primitive
A4301	KAS-ECC-SSC SP800-56Ar3	Ephemeral Unified	Curve sizes P-256, P-384, P-521 with 128 bits to 256 bits of strength	Key Agreement Shared Secret Computation
A4301	KAS-FFC-SSC SP800-56Ar3	dhEphemeral	Domain Parameter Generation Method: MODP-2048 with 2048 bits of strength	Key Agreement Shared Secret Computation
A4301	KDF SSH	SSH	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Key Derivation Function
A4301	RSA KeyGen (FIPS186-4)	RSA KeyGen	Moduli 2048, 3072 and 4096 bits with 112, 128 and 152 bits of strength	Key Generation
A4301	RSA SigGen (FIPS186-4)	RSA SigGen	Moduli 2048 (SHA2-256, SHA2-512), 3072 (SHA2-256, SHA2-512) and 4096 (SHA2-256, SHA2-512) bits with 112, 128 and 152 bits of strength	Signature Generation
A4301	RSA SigVer (FIPS186-4)	RSA SigVer	Moduli 2048 (SHA2-256, SHA2-512), 3072 (SHA2-256, SHA2-512) and 4096 (SHA2-256, SHA2-512) bits with 112, 128 and 152 bits of strength	Signature Verification
A4301	SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Digest Generation
A4301	SHA2-256	SHA2-256	SHA2-256: Key size 256 bits with 256-bits of key strength	Message Digest Generation

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4301	SHA2-384	SHA2-384	SHA2-384: Key size 384 bits with 256-bits of key strength	Message Digest Generation
A4301	SHA2-512	SHA2-512	SHA2-512: Key size 512 bits with 256-bits of key strength	Message Digest Generation
A4303	HMAC DRBG	HMAC-SHA2-256	Key size 256-bits with 256-bits of key strength	Random Bit Generation
A4303	HMAC-SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Authentication, DRBG primitive
A4303	HMAC-SHA2-256	SHA2-256	SHA2-256: Key size: 256 bits with 256-bits of key strength	Message Authentication, DRBG primitive
A4303	SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Digest Generation
A4303	SHA2-256	SHA2-256	SHA2-256: Key size 256 bits with 256-bits of key strength	Message Digest Generation
A4303	SHA2-384	SHA2-384	SHA2-384: Key size 384 bits with 256-bits of key strength	Message Digest Generation
A4303	SHA2-512	SHA2-512	SHA2-512: Key size 512 bits with 256-bits of key strength	Message Digest Generation
A4304	AES-CBC	CBC	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt
A4304	AES-CMAC	CMAC	Key sizes 128 and 256 with 128 to 256 bits of key strength	Generate, Verify
A4304	AES-ECB	ECB	Key sizes 128, 192, 256 with 128 to 256 bits of key strength	Encrypt, Decrypt

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4304	AES-KW	KW	Key size 128 bits with 128 bits of key strength	Encrypt, Decrypt
A4304	KDF SP 800-108	Counter	Key sizes 128 and 256 with 128 to 256 bits of key strength	Key Derivation
A4306	HMAC-SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Authentication, DRBG primitive
A4306	HMAC-SHA2-256	SHA2-256	SHA2-256: Key size: 256 bits with 256-bits of key strength	Message Authentication, DRBG primitive
A4306	SHA-1	SHA-1	SHA-1: Key size 160 bits with 160 bits of key strength	Message Digest Generation
A4306	SHA2-256	SHA2-256	SHA2-256: Key size 256 bits with 256-bits of key strength	Message Digest Generation
A4306	SHA2-512	SHA2-512	SHA2-512: Key size 512 bits with 256-bits of key strength	Message Digest Generation
Vendor Affirmed	CKG NIST SP 800-133r2	Section 4 Section 5.1 Section 5.2 Section 6.2.1	Section 4: Asymmetric seed generation using an unmodified output from an Approved DRBG; Section 5.1: Key Pairs for Digital Signature Schemes; Section 5.2: Key Pairs for Key Establishment; Section 6.2.1: Derivation of symmetric keys	Cryptographic Key Generation

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
KAS-ECC-SSC SP800-56Ar3/A4301 KDF SSH/A4301	KAS-1	SP 800-56Arev3 KAS-ECC per IG D.F Scenario 2 path (2)	P-256, P-384, P-521 curves	Key Agreement for SSHv2
KAS-FFC-SSC SP800-56Ar3/A4301 KDF SSH/A4301	KAS-2	SP 800-56Arev3 KAS-FFC per IG D.F Scenario 2 path (2)	MODP-2048	Key Agreement for SSHv2
AES-CBC/A4301 AES-CTR/A4301 HMAC-SHA-1/A4301 HMAC-SHA2-256/A4301 HMAC-SHA2-512/A4301	KTS-1	SP 800-38A AES CBC, CTR and HMAC 198 per IG D.G	128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	Key Transport for SSHv2
AES-KW/A4304	KTS-2	SP 800-38D and SP 800-38F KTS (key wrapping) per IG D.G	128 bit keys providing 128 bits of encryption strength	Key Transport for MACsec

Table 3 – Approved Algorithms

The following protocols are supported by the module in the Approved mode:

- SSHv2 (EC Diffie-Hellman P-256, P-384, P-521; Diffie-Hellman MODP2048; RSA 2048, 4096; ECDSA P-256; AES CBC 128, 192, 256 bits; AES CTR 128, 192, 256 bits, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512)

- MACsec (MACsec Key Agreement (MKA); AES GCM 128 and 256 bits; HMAC-SHA2-256)

The MACsec and SSH protocols allow independent selection of key exchange, authentication, cipher and integrity algorithms.

The module does not support any non-Approved algorithms in the Approved mode, i.e., it does not support *Non-Approved Algorithms Allowed in the Approved Mode of Operation and Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed.*

In addition to all Approved algorithms supported in the Approved mode of operation, the following *non-Approved Algorithms Not Allowed in the Approved Mode of Operation* are supported only in the non-Approved mode:

Algorithm/Function	Use/Function
RSA with key size less than 2048	SSH
ECDSA with ed25519 curve	SSH
EC Diffie-Hellman with ed25519 curve	SSH
ARCFOUR	SSH
Blowfish	SSH
CAST	SSH
DSA (SignGen, SigVer, non-compliant)	SSH
HMAC-MD5	SSH
HMAC-RIPEMD160	SSH
UMAC	SSH

Table 4 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

3. Cryptographic Module Interfaces

Physical port	Logical interface	Data that passes over port/interface
Ethernet (Management Port)	Control input interface, Data input interface, Data output interface, Status output interface	LAN, Communications/remote management
Serial	Control input interface, Data input interface, Data output interface, Status output interface	Console Serial Port
USB	Control input interface, Data input interface	USB port, load Junos Image
Power	Power interface	Power connector, Power over Ethernet
Alarm LEDs	Status output interface	Status indicator lighting
Reset Button	Control input interface	Reset signal

Table 5 – Ports and Interfaces

The module does not support control output.

4. Roles, Services, and Authentication

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 module implements two forms of identity-based authentication, username, and password over the console and SSH connections, as well as username and an ECDSA or RSA public key-based authentication over SSH.

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 configure passwords and public keys within the module. The User role monitors the module via the console or SSH. The User role does not have the permission to modify the configuration.

Role	Service	Input	Output
Crypto Officer	Configure security (security relevant)	Commands (SSH configuration: set system services ssh root-login allow; MACsec configuration: set security macsec connectivity-association connectivity-association-name; set security macsec connectivity-association connectivity-association-name security-mode static-cak)	Traffic
	Configure (non-security relevant)	Commands (miscellaneous commands e.g., for IP address configuration, routing protocols, etc.)	Traffic
	Show status	Command (show)	CLI output
	Show status (LED)	N/A	LED
	Show module's versioning information	Command (show version)	CLI output
	Perform zeroisation	Command (request system zeroize)	N/A
	Perform approved security functions (SSH connection)	Command (set system services ssh root-login allow)	SSH session
	Perform approved security functions (MACsec connection)	Commands (set security macsec connectivity-association connectivity-association-name;	MACsec session

Role	Service	Input	Output
		set security macsec connectivity-association connectivity-association-name security-mode static-cak)	
	Console access	Username, password (set system login user <username> class <crypto-officer/user class> operator authentication plaintext-password)	N/A
	Perform self-tests (remote reset)	Control input/reset signal (request system reboot)	N/A
	Perform self-tests (local reset)	Control input/reset signal	N/A
	Load image	Image, commands	N/A
User	Show status	Command (show)	CLI Output
	Show status (LED)	N/A	LED
	Show module's versioning information	Command (show version)	CLI output
	Perform approved security functions (SSH connection)	Commands (set system services ssh root-login allow)	SSH session
	Console access	Username, password (set system login user <username> class <crypto-officer/user class> operator authentication plaintext-password)	N/A
	Perform self-tests (remote reset)	Control input/reset signal (request system reboot)	N/A
	Perform self-tests (local reset)	Control input/reset signal	N/A

Table 6 – Roles, Service Commands, Input and Output

Role	Authentication Method	Authentication Strength
Crypto Officer (CO), User	1. Username and password over the console and SSH 2. Username and ECDSA public key over SSH 3. Username and RSA public key over SSH	1. For Password Authentication: The module enforces 10-character passwords (at minimum) chosen from the 96 human readable ASCII characters;

Role	Authentication Method	Authentication Strength
		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 (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

Role	Authentication Method	Authentication Strength
		9/(96^10), which is less than 1/100,000 2. 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 (million) 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 3. RSA signature verification: SSH public-key authentication; The module supports RSA (2048, 4096 bits), which has a minimum equivalent computational resistance to attack of 2^{112} (2048 bits); Thus, the probability of a successful random attempt is $1/ (2^{112})$, which is less than 1/1,000,000 (million)

Role	Authentication Method	Authentication Strength
		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

Table 7 – Roles and Authentication

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
Configure security (security relevant)	Security relevant configuration	All (per Table 3)	SSH Private Host Key SSH ECDH Private Key SSH DH Private Key SSH Session Key User Password CO Password HMAC_DRBG Key Value HMAC_DRBG V value HMAC_DRBG entropy input HMAC_DRBG seed HMAC_DRBG output MACsec PSK MACsec CAK MACsec CKN MACsec SAK MACsec KEK MACsec ICK ECDH Shared Secret DH Shared Secret HMAC Key SSH Public Host Key User Authentication Public Keys	Crypto Officer (CO)	(G, E) (G, E) (G, E) (G, E) (W, E) (W, E) (G, E) (G, E) (G, E) (G, E) (G, E) (W, E) (W, E) (W, E) (G, E, R) (G, E) (G, E) (G, E) (G, E) (G, E) (G, E) (W, E)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
			CO Authentication Public Keys JuniperRootCA PackageCA SSH ECDH Public Key SSH DH Public Key		(W, E) (W, E) (W, E) (G, E) (G, E)	
Configure (non-security relevant)	Non-security relevant configuration	N/A	N/A	Crypto Officer (CO)	N/A	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service
Show status	Query the module status	N/A	N/A	Crypto Officer (CO), User	N/A	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service
Show status (LED)	LEDs on the module provide physical status output	N/A	N/A	Crypto Officer (CO), User, Unauthorised	N/A	LED(s) on the chassis turned on
Show module's	Query the module's	N/A	N/A	Crypto Officer	N/A	Global Approved

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
versioning information	versioning information			(CO), User		Mode indicator "fips" at the CLI combined with successful completion of each service
Perform zeroisation	Destroy all SSPs	N/A	SSH Private Host Key SSH ECDH Private Key SSH DH Private Key SSH Session Key User Password CO Password HMAC_DRBG Key Value HMAC_DRBG V value HMAC_DRBG entropy input HMAC_DRBG seed HMAC_DRBG output MACsec PSK MACsec CAK MACsec CKN MACsec SAK MACsec KEK MACsec ICK ECDH Shared Secret DH Shared Secret HMAC Key SSH Public Host Key User Authentication Public Keys CO Authentication Public Keys JuniperRootCA PackageCA SSH ECDH Public Key SSH DH Public Key	Crypto Officer (CO)	(Z)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
Perform approved security functions (SSH connection)	Initiate SSH connection for SSH monitoring and control (CLI)	ECDSA (P-256, SHA2-256, KeyGen, SIgVer, Cert. #A4301), RSA (2048 bits, SHA2-256, SHA2-512, KeyGen, SIgVer, Cert. #A4301), KAS-ECC-SSC (P-256, P-384, P-512, Cert. #A4301), KAS-FFC-SSC (MODP 2048, Cert. #A4301), AES (CBC, CTR 128, 192, 256 bits, Cert. #A4301), KDF SSH (Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, CAVP Certs. A4303, A4301), HMAC (SHA-1, SHA2-256, SHA2-512, CAVP Certs. #A4303, #A4301, #A4306; SHA2-384, CAVP Certs. #A4303); SHA (SHA-1, SHA2-256, SHA2-512, CAVP Certs. #A4303, #A4301, #A4306; SHA2-384, CAVP Certs. #A4303), CKG	SSH Private Host Key SSH ECDH Private Key SSH DH Private Key SSH Session Key HMAC_DRBG Key Value HMAC_DRBG V value HMAC_DRBG entropy input HMAC_DRBG seed HMAC_DRBG output ECDH Shared Secret DH Shared Secret HMAC Key SSH Public Host Key User SSH ECDH Public Key SSH DH Public Key	Crypto Officer (CO), User	(G, E)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
Perform approved security functions (MACsec connection)	Initiate MACsec connection	AES (GCM, CMAC, 128, 256 bits, KW, 128 bits, Cert. #4369), SP 800-108 KDF (Cert. #A4304)	MACsec PSK MACsec CAK MACsec CKN MACsec SAK, MACsec KEK, MACsec ICK	Crypto Officer (CO)	(W, E) (W, E) (W, E) (G, R, E) (G, E) (G, E)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service
Console Access	Console monitoring and control (CLI)	N/A	N/A	Crypto Officer (CO), User	N/A	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service
Perform self-tests (remote reset)	Software initiated reset, performs self-tests on demand	All (per Table 3)	SSH ECDH Private Key, SSH DH Private Key, SSH Session Key, HMAC_DRBG Key Value HMAC_DRBG V value HMAC_DRBG entropy input HMAC_DRBG seed	Crypto Officer (CO), User	(Z) (Z) (Z) (G, Z, E) (G, Z, E) (G, Z, E) (G, Z, E) (G, Z, E)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
			HMAC_DRBG output MACsec PSK (Z) MACsec CAK (Z) MACsec CKN (Z) MACsec SAK (Z) MACsec KEK (Z) MACsec ICK (Z) ECDH Shared Secret DH Shared Secret HMAC Key SSH ECDH Public Key SSH DH Public Key		(Z) (Z) (Z) (Z) (Z) (Z) (Z) (Z) (G, Z, E) (G, E) (G, E)	
Perform self-tests (local reset)	Hardware reset or power cycle	All (per Table 3)	SSH ECDH Private Key, SSH DH Private Key, SSH Session Key, HMAC_DRBG Key Value HMAC_DRBG V value HMAC_DRBG entropy input HMAC_DRBG seed HMAC_DRBG output MACsec PSK MACsec CAK MACsec CKN MACsec SAK MACsec KEK MACsec ICK ECDH Shared Secret DH Shared Secret HMAC Key SSH ECDH Public Key SSH DH Public Key	Crypto Officer (CO), User, Unauthorised	(Z) (Z) (Z) (G, Z, E) (G, Z, E) (G, Z, E) (G, Z, E) (G, Z, E) (Z) (Z) (Z) (Z) (Z) (Z) (Z) (Z) (G, Z, E) (G, E) (G, E)	Global Approved Mode indicator "fips" at the CLI combined with successful completion of each service
Load Image	Verification and loading of a validated firmware image into the router/switch	ECDSA (P-256, SHA2-256, SigVer, CAVP Cert. #A4301)	N/A	Crypto Officer (CO)	N/A	Global Approved Mode indicator "fips" at the CLI combined with successful completion

Service	Description	Approved Security Functions	Keys and/or SSP's	Roles	Access rights to Keys and/or SSP's	Indicator
						of each service

Table 8 – Approved Services

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Service	Description	Algorithms Accessed	Role	Indicator
Configure security (security relevant)	Security relevant configuration	All (per Table 3)	Crypto Officer (CO)	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Configure (non-security relevant)	Non-security relevant configuration	N/A	Crypto Officer (CO)	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Show status	Query the module status	N/A	Crypto Officer (CO), User	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Show status (LED)	LEDs on the module provide physical status output	N/A	Crypto Officer (CO), User, Unauthorised	LED(s) on the chassis turned on
Show module's versioning information	Query the module's versioning information	N/A	Crypto Officer (CO), User	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Perform zeroisation	Destroy all SSPs	N/A	Crypto Officer (CO)	Lack of the global Approved Mode indicator "fips" at

Service	Description	Algorithms Accessed	Role	Indicator
				the CLI combined with successful completion of the service
Perform approved security functions (SSH connection)	Initiate SSH connection for SSH monitoring and control (CLI)	AES (CBC, CTR, 128, 192 and 256 bits); KAS-ECC-SSC (P-256, P-384, P-521); KAS-FFC-SSC (MODP 2048) RSA (2048, 4096 bits); ECDSA (P-256); HMAC (SHA-1, SHA2-256, SHA2-512); SHA (SHA-1, SHA2-256, SHA2-512); SSH KDF; RSA (key size <= 2048); ECDSA (ed25519 curve); EC DH (ed25519 curve); ARCFOUR ; Blowfish; CAST; DSA (SignGen, SigVer, non-compliant); HMAC-MD5; HMAC-RIPEMD160; UMAC	Crypto Officer (CO), User	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Perform approved security functions (MACsec connection)	Initiate MACsec connection	AES (GCM, 128, 256 bits), SP 800-108 KDF AES (CTR 128, 256 bits), HMAC (SHA2-256) SHA (SHA2-256)	Crypto Officer (CO)	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Console Access	Console monitoring and control (CLI)	N/A	Crypto Officer (CO), User	Lack of the global Approved Mode indicator "fips" at

Service	Description	Algorithms Accessed	Role	Indicator
				the CLI combined with successful completion of the service
Perform self-tests (remote reset)	Software initiated reset, performs self-tests on demand	All (per Table 3)	Crypto Officer (CO), User	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Perform self-tests (local reset)	Hardware reset or power cycle	All (per Table 3)	Crypto Officer (CO), User, Unauthorised	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service
Load Image	Verification and loading of a validated firmware image into the router/switch.	ECDSA (P-256, SHA2-256)	Crypto Officer (CO)	Lack of the global Approved Mode indicator "fips" at the CLI combined with successful completion of the service

Table 9 – Non-Approved Services

The module supports self-initiated cryptographic output capability in the form of the MACsec service provided and performs two internal checks (firmware flags set) prior to activating the service. The following command can be used by the operator as the indicator to verify that the self-initiated cryptographic output capability has been activated, for e.g.:

operator@device> show security macsec connections
Interface name: xe-0/1/0
CA name: CA1
Cipher suite: GCM-AES-128 Encryption: on
Key server offset: 0 Include SCI: no
Replay protect: off Replay window: 0

5. Software/Firmware Security

The module performs the firmware integrity check using ECDSA P-256 with SHA2-256. The operator can initiate the integrity test on demand by rebooting the module. The module firmware image is delivered in the form of a pre-compiled tarball (.tgz). The module supports loading of firmware from an external source and a firmware load test using ECDSA P-256 with SHA2-256 is performed in support of the load.

6. Operational Environment

The module contains a limited operational environment. The Junos OS 22.4R2.8 operating system is contained within the module, i.e., the tested configurations listed in Table 2 of this document. Security rules and restrictions for configuration of the operational environment have been specified in Section 2 (Overall Security Rules of Operation) and Section 11 (Installing The Firmware Image and Enabling the Approved Mode of Operation) of this document.

7. Physical Security

The module's physical embodiment is that of a multi-chip standalone meeting 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 of 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. No actions are required by the operator to ensure that physical security is maintained.

8. Non-invasive Security

The module does not implement any non-invasive security mitigations and thus the requirements per this section do not apply to the module.

9. Sensitive Security Parameter Management

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
SSH Private Host Key CSP	128 bits for ECDSA, 112 bits for RSA	ECDSA (P-256, SHA2-256, KeyGen, Cert. #A4301), RSA (2048 bits, SHA2-256, SHA2-512, KeyGen, Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, Cert. #A4301) HMAC (SHA2-256, Cert. #A4301) SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: Persistent	Zeroisation command (request system zeroize)	Host keypairs generated, used to identify the host
SSH ECDH Private Key CSP	128 bits, 192 bits, 256 bits	KAS-ECC-SSC (P-256, P-384, P-512, Cert. #A4301), HMAC_DRBG	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle	Ephemeral EC Diffie-Hellman private key used in SSH

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
		(HMAC-SHA2-256, Cert. #A4301) HMAC (SHA2-256, Cert. #A4301) SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG						
SSH DH Private Key CSP	112 bits	KAS-FFC-SSC (MODP 2048, Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, Cert. #A4301) HMAC (SHA2-256, Cert. #A4301) SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle	Ephemeral Diffie-Hellman private key used in SSH

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
SSH Session Key CSP	128 bits, 192 bits, 256 bits	AES (CBC, CTR 128, 192, 256 bits, Cert. #A4301), KAS-ECC-SSC (P-256, P-384, P-512, Cert. #A4301), KAS-FFC-SSC (MODP 2048, Cert. #A4301), KDF SSH (Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, Cert. #A4301), HMAC (SHA-1, SHA2-256, SHA2-512, Cert. #A4301), SHA (SHA-1, SHA2-256, SHA2-512, Cert. #A4301), CKG	N/A	Import: N/A Export: N/A	Key Agreement Scheme (KAS), Derived using KDF SSH	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	SSH Session keys

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
User Password CSP	256 bits, 512 bits	SHA (SHA2-256, Cert. #A4306, SHA2-512, Cert. #A4306)	Password hash generated internally (Password is configured by the Crypto Officer)	Import: Manual entry via CLI, manual SSP entry test perfor med Export: N/A	N/A	Non-Plaintext: Persistent (Password Hash)	Zeroisation command (request system zeroize) and explicit delete command	Used to authenticate users to the module
CO Password CSP	256 bits, 512 bits	SHA (SHA2-256, Cert. #A4306, SHA2-512, Cert. #A4306)	Password hash generated internally (Password is configured by the Crypto Officer)	Import: Manual entry via CLI, manual SSP entry test perfor med Export: N/A	N/A	Non-plaintext: Persistent (Password Hash)	Zeroisation command (request system zeroize) and explicit delete command	Used to authenticate COs to the module
HMAC_DRBG V value CSP	256 bits	HMAC_DRBG (HMAC-SHA2-256), HMAC (SHA2-256), SHA (SHA2-256, CAVP Certs. A4303, A4301)	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Power cycle	A critical value of the internal state of DRBG

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
HMAC_DRBG Key value CSP	256 bits	HMAC_DRBG (HMAC-SHA2-256), HMAC (SHA2-256), SHA (SHA2-256, CAVP Certs. A4303, A4301)	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Power cycle	A critical value of the internal state of DRBG
HMAC_DRBG entropy input CSP	256 bits	HMAC_DRBG (HMAC-SHA2-256), HMAC (SHA2-256), SHA (SHA2-256, CAVP Certs. A4303, A4301)	NIST SP 800-90B ENT (NP) entropy source	Import: N/A Export: N/A	N/A	Plaintext: RAM	Power cycle	Entropy input to the HMAC_DRBG
HMAC_DRBG seed CSP	256 bits	HMAC_DRBG (HMAC-SHA2-256), HMAC (SHA2-256), SHA (SHA2-256, CAVP Certs. A4303, A4301)	NIST SP 800-90B ENT (NP) entropy source	Import: N/A Export: N/A	N/A	Plaintext: RAM	Power cycle	Seed provided to the HMAC_DRBG

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
HMAC_DRBG output CSP	256 bits	HMAC_DRBG (HMAC-SHA2-256), HMAC (SHA2-256), SHA (SHA2-256, CAVP Certs. A4303, A4301)	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Power cycle	Unmodified output of the HMAC_DRBG used in SSP generation
MACsec PSK CSP	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #A4304)	N/A	Import: Configured by the Crypto Officer in plaintext via console port or encrypted via SSH connection Export: MACsec connection establishment	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Credential used for device-to-device authentication, consists of the CAK and CKN
MACsec CAK CSP	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #A4304)	N/A	Import: Pre-Shared Key entered by the	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	A secret key possessed by members of a MACsec connectivity association

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
				Crypto Officer Export: N/A				entered as a pre-shared key
MACsec CKN	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #A4304)	N/A	Import: Pre-Shared Key entered by the Crypto Officer Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Connectivity Key Name: Identifies the CAK Entered as a pre-shared key
MACsec SAK CSP	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #A4304) SP 800-108 KDF (Cert. #A4304)	Derived from the CAK using SP 800-108 KDF	Import: N/A Export: Encrypted with the KEK	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Security Association Key used for creating Security Associations for encryption/ decryption of MACsec traffic
MACsec KEK CSP	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #4304) SP 800-108 KDF (Cert. #A4304)	Derived from the CAK using SP 800-108 KDF	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Used to transmit SAKs to other members of a MACsec connectivity association

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
MACsec ICK CSP	128 bits, 256 bits	AES (GCM, 128, 256 bits, Cert. #A4304) SP 800-108 KDF (Cert. #A4304)	Derived from the CAK using SP 800-108 KDF	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Used to verify the integrity and authenticity of MACsec protocol data units
ECDH Shared Secret CSP	128 bits, 192 bits, 256 bits	KAS-ECC-SSC (P-256, P-384, P-521, Cert. #A4301)	N/A	Import: N/A Export: N/A	KAS-ECC-SSC Ephemeral Unified scheme	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Used in EC Diffie-Hellman (ECDH) exchange
DH Shared Secret CSP	112 bits	KAS-FFC-SSC (MODP 2048, Cert. #A4301)	N/A	Import: N/A Export: N/A	KAS-FCC-SSC dhEphemeral scheme	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle, session termination	Used in Diffie-Hellman (DH) exchange
HMAC Key CSP	160 bits, 256 bits, 384 bits, 512 bits	HMAC_DRBG (HMAC-SHA2-256, CAVP Certs. A4303, A4301), HMAC (SHA-1, SHA2-256, SHA2-512, CAVP Certs. #A4303,	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle	HMAC Key

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
		#A4301, #A4306; SHA2-384, CAVP Certs. #A4303); SHA (SHA-1, SHA2-256, SHA2-512, CAVP Certs. #A4303, #A4301, #A4306; SHA2-384, CAVP Certs. #A4303)						
SSH Public Host Key PSP	128 bits for ECDSA, 112 bits for RSA	ECDSA (P-256, SHA2-256, KeyGen, Cert. #A4301), RSA (2048 bits, SHA2-256, SHA2-512, KeyGen, Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256,	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: Persistent	Zeroisation command (request system zeroize)	Host keypairs generated, used to identify the host

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
		Cert. #A4301) HMAC (SHA2-256, Cert. #A4301) SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG						
User Authentication Public Keys PSP	128 bits, 192 bits, 256 bits for ECDSA, 112 bits, 152 bits for RSA	ECDSA SigVer (P-256, P-384, P-521, Cert. #A4301); RSA SigVer (2048, 4096 bits, Cert. #A4301)	N/A	Import: Entered by the Crypto Officer Export: N/A	N/A	Plaintext: Persistent	Zeroisation command (request system zeroize)	Used to authenticate users to the module
CO Authentication Public Keys PSP	128 bits, 192 bits, 256 bits for ECDSA, 112 bits, 152 bits for RSA	ECDSA SigVer (P-256, P-384, P-521, Cert. #A4301); RSA SigVer (2048, 4096 bits, Cert. #A4301)	N/A	Import: Entered by the Crypto Officer Export: N/A	NA	Plaintext: Persistent	Zeroisation command (request system zeroize)	Used to authenticate the CO to the module

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
JuniperRootCA PSP	128 bits	ECDSA (P-256, Cert. #A4301)	N/A	Import: Loaded at manufacture time Export: N/A	N/A	Plaintext: Persistent	Zeroisation command (request system zeroize)	ECDSA prime256v1 X.509 V3 Certificate Used to verify the validity of the PackagCA
PackageCA PSP	128 bits	ECDSA (P-256, Cert. #A4301)	N/A	Import: Loaded at manufacture time Export: N/A	N/A	Plaintext: Persistent	Zeroisation command (request system zeroize)	ECDSA prime256v1 X.509 V3 Certificate Certificate that holds the public key for the signing key used to generate all the signatures used on the packages and signature lists
SSH ECDH Public Key PSP	128 bits, 192 bits, 256 bits	KAS-ECC-SSC (P-256, P-384, P-512, Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, Cert. #A4301) HMAC (SHA2-256, Cert. #A4301)	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle	Ephemeral EC Diffie-Hellman public key used in SSH

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
		SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG						
SSH DH Public Key PSP	112 bits	KAS-FFC-SSC (MODP 2048, Cert. #A4301), HMAC_DRBG (HMAC-SHA2-256, Cert. #A4301) HMAC (SHA2-256, Cert. #A4301) SHA (SHA2-256, SHA2-512, Cert. #A4301), CKG	Generated internally using NIST SP 800-90Ar1 HMAC_DRBG	Import: N/A Export: N/A	N/A	Plaintext: RAM	Zeroisation command (request system zeroize), power-cycle	Ephemeral Diffie-Hellman public key used in SSH

Table 10 – SSPs

Entropy sources	Minimum number of bits of entropy	Details
SP 800-90B ENT (NP) ESV Cert. #E104	The module generates a minimum of 448 bits of overall entropy per 512-bit output sample, 0.875 bits of entropy per bit for SSP generation	Entropy input for seeding the approved NIST SP 800-90Ar1 DRBGs

Table 11 – Non-Deterministic Random Number Generation Specification

10. Self-tests

The module performs the following self-tests:

- **Pre-operational Self-Tests:**
  - Firmware Integrity Test: using ECDSA P-256 with SHA2-256

- **Conditional Self-Tests:**
  - Conditional Cryptographic Algorithm Self-tests (CAST):
    - Kernel KATs (CAVP Cert. #A4303)
      - HMAC-SHA2-256 DRBG KAT
        - Generate, Instantiate and Reseed
      - HMAC-SHA-1 KAT
      - HMAC-SHA2-256 KAT
      - SHA2-384 KAT
      - SHA2-512 KAT

    - OpenSSL KATs (CAVP Cert. #A4301)
      - AES CBC 128 bits Encrypt KAT
      - AES CBC 192 bits Encrypt KAT
      - AES CBC 256 bits Encrypt KAT
      - AES CBC 128 bits Decrypt KAT
      - AES CBC 192 bits Decrypt KAT
      - AES CBC 256 bits Decrypt KAT
      - AES GCM 128 bits Encrypt KAT
      - AES GCM 192 bits Encrypt KAT
      - AES GCM 256 bits Encrypt KAT
      - AES GCM 128 bits Decrypt KAT
      - AES GCM 192 bits Decrypt KAT
      - AES GCM 256 bits Decrypt KAT
      - HMAC-SHA2-256 DRBG KAT
        - Generate, Instantiate and Reseed
      - HMAC-SHA-1 KAT
      - HMAC-SHA2-256 KAT
      - HMAC-SHA2-512 KAT
      - KAS-ECC-SSC P-256 KAT
      - KAS-ECC-SCC P-384 KAT
      - KAS-FFC-SSC MODP-2048 KAT
      - KDF SSH KAT
      - RSA 2048 bits SHA2-256 Sign KAT
      - RSA 2048 bits SHA2-256 Verify KAT
      - ECDSA P-256 Sig Gen KAT
      - ECDSA P-256 Sig Ver KAT
      - ECDSA P-384 Sig Gen KAT
      - ECDSA P-384 Sig Ver KAT
      - SHA2-384 KAT

- LibMD KATs (CAVP Cert. #A4306)
  - HMAC-SHA-1
  - HMAC-SHA2-256
  - SHA2-512

- MACsec KATs (CAVP Cert. #A4304)
  - AES CMAC 128 bits Generate KAT
  - AES CMAC 128 bits Verify KAT
  - AES CMAC 256 bits Generate KAT
  - AES CMAC 256 bits Verify KAT
  - AES ECB 128 bits Encrypt KAT
  - AES ECB 192 bits Encrypt KAT
  - AES ECB 256 bits Encrypt KAT
  - AES ECB 128 bits Decrypt KAT
  - AES ECB 192 bits Decrypt KAT
  - AES ECB 256 bits Decrypt KAT
  - AES KW 128 bits Encrypt KAT
  - AES KW 128 bits Decrypt KAT
  - NIST SP 800-108 KDF KAT

- NIST SP 800-90B Repetitive Count Test (RCT)
- NIST SP 800-90B Adaptive Proportion Test (APT)

- Pairwise consistency test when generating ECDSA key pairs (for signature generation/verification and KAS-ECC SSP agreement)
- Pairwise consistency test when generating RSA key pairs (for signature generation/verification)
- Pairwise consistency test when generating DSA key pairs (for KAS-FFC SSP agreement)
- Firmware Load Test (ECDSA P-256 SHA2-256 signature verification)

Each time the module is powered up it tests that all the cryptographic algorithms operate correctly, and that sensitive data have not been damaged. Pre-operational as well as Conditional Cryptographic Algorithm Self-tests (CAST) are performed on each power up/boot of the module and on demand by power cycling the module (Perform self-tests (remote reset) service). The module performs a CAST for ECDSA P-256 with SHA2-256 prior to executing the firmware integrity check on each boot.

The pre-operational firmware integrity test as well as all CASTs must be completed successfully prior to any other use of cryptography by the module in the Approved mode of operation. These tests can also be performed periodically by rebooting the module. If the pre-operation firmware integrity test or if any of the CASTs fail, then the module returns the error indicator “FIPS error: self-test failure”, inhibits all data output and enters the hard error state.

Conditional Self-Tests are performed by the module when the corresponding condition is met. The pairwise consistency tests are performed on key pair generation for use in signature generation/verification (ECDSA and/or RSA tests) and/or for use in KAS-ECC SSP agreement (ECDSA tests). The firmware load test is performed when a firmware image is loaded onto the module from an external source. If the conditional self-tests fail, the module enters the soft error state, i.e., it rejects the generated keypair/loaded image, returns an error indicator and resumes normal operation. The error indicator is the return code -1 in case of a pairwise consistency test failure and “ERROR: Failed signature check” for the firmware load test failure.

11. Life-cycle Assurance

The Crypto Officer must follow the procedures defined below for secure installation, initialization, startup and operation of the module.

Crypto Officer Guidance

The Crypto Officer must check to verify the firmware image being loaded on the module is the FIPS 140-3 validated version/image. If the image is the FIPS 140-3 validated image, then proceed with installation of the image.

Installing The Firmware Image

Download the validated firmware image from 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 using the following command: operator@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, junos-install-ex-4300mp-x86-64-22.4R2.8.tgz. This is your last chance to stop the installation.

Reboot the device to complete the load and start the installation:
operator@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.

Enabling Approved Mode of Operation

The Crypto Officer is responsible for initializing the module in the Approved mode of operation. The Approved mode of operation is not automatically enabled. The Crypto Officer shall place the module in the Approved mode by first zeroising it to ensure no SSPs are present. Next, the cryptographic officer shall follow the steps found in the Junos OS FIPS Evaluated Configuration Guide for Juniper Networks EX4300-48MP Ethernet Switch, Release 22.4R2.8 document Chapters 3 & 7 to place the module into an Approved mode of operation. The steps from the before mentioned document have been reiterated below.

To enable the Approved mode in Junos OS on the module:

1. Zeroise the module using the “request system zeroize” command. Once the module comes up in the “amnesiac mode” post zeroisation, connect to it using the console port with username “root”, enter the configuration mode and configure the root-authentication password (i.e., Crypto Officer credentials) as follows:

root@device> edit

Entering configuration mode

[edit]

root@device# set system root-authentication plain-text-password

New password:

Retype new password:

[edit]

root@device# commit

configuration check succeeds

commit complete

2. Enable Approved mode on the device by setting the Approved level to 1, and verify the level:

[edit]

root@device# set system fips chassis level 1

[edit]

root@device# show system fips chassis level

level 1;

4. Commit the configuration

[edit]

root@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

'system' reboot is required to transition to fips level 1

commit complete

5. Reboot the device:

[edit]

root@device# run request system reboot

Reboot the system ? [yes,no] (no) yes

During the reboot, the device runs the pre-operational firmware integrity test and all CASTs. It returns a login prompt.

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

root@device:fips > show version

The tester verified that the prompt contained "fips" indicating it was in the approved mode of operation. No further configuration is required.

Placing the Module in the Non-Approved Mode of Operation

As Crypto Officer, the operator needs to disable the Approved mode of operation on the device to return it to the non-Approved mode of operation. To disable the Approved mode on the device, the module must be zeroised (step 1 defined above).

No other maintenance requirements apply for operation of the module in the Approved/non-Approved modes as defined above. For further information and for the Administrator and non-Administrator guidance, please see the Junos OS FIPS Evaluated Configuration Guide for Juniper Networks EX4300-48MP Ethernet Switch, Release 22.4R2.8 document.

12. Mitigation of Other Attacks

The module does not implement any mitigation of other attacks and thus the requirements per this section do not apply to the module.