Juniper Networks EX4300 Ethernet Switches

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.2

Date: November 30, 2020

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

Table of Contents

List of Tables

List of Figures

1 Introduction

The EX4300 line features 24 and 48-port 10/100/1000BASE-T models and a 32-port 100BASE-FX/1000BASE-X SFP model. On the fiber-based switches, four fixed front-panel uplink ports accommodate 1GbE or 10GbE optics for high-speed backbone or link aggregation connections. The four 40GBASE quad small form-factor pluggable plus transceiver (QSFP+) ports available on each model can also be used for high-speed backbone or link aggregation connections. Power over Ethernet (PoE)-enabled EX4300 models offer standards-based 802.3at PoE+, delivering up to 30 watts on all ports for supporting high-density IP telephony, surveillance camera, or wireless access point deployments.

1.1 Module Overview

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks EX4300 Ethernet Switch Cryptographic Module from Juniper Networks. It provides detailed information relating to each of the FIPS 140-2 security requirements relevant to Juniper Networks EX4300 Ethernet Switch Cryptographic Modules along with instructions on how to run the module in a secure FIPS 140-2 mode.

The cryptographic module provides for an encrypted connection, using SSH, between the management console and the switch. The switch also provides for an encrypted connection, using MACSec, between devices. All other data input or output from the switch is considered plaintext for this FIPS 140-2 validation.

The EX4300 switches run Junos OS firmware. The validated version of firmware is Junos OS 17.4 R1-S4. Any other version of firmware loaded onto the module is out of scope for this validation. The image for the hardware platforms is:

- jinstall-ex-4300-17.4R1-S4-signed.tgz

The Juniper Networks EX4300 Ethernet Switch are cryptographic modules that are defined as multiple-chip standalone modules that execute JUNOS 17.4 R1-S4 firmware on the EX 4300 Ethernet Switches listed in Table 1. The cryptographic boundary is defined as the outer edge of the switch. The cryptographic modules' operational environment is a limited operational environment.

Table 1 gives a list of the hardware versions that are part of the module validation and the basic configuration of the hardware.

Table 1 – Cryptographic Module Configurations

Model	Hardware Versions	Firmware	Supported Uplink Modules
EX4300-24	EX4300-24T EX4300-24P	Junos OS 17.4R1-S4	EX-UM-4X4SFP
EX4300-32	EX4300-32F	Junos OS 17.4R1-S4	EX-UM-8X8SFP
EX4300-48	EX4300-48T	Junos OS 17.4R1-S4	EX-UM-4X4SFP

P = 10/100/1000Base-T Power over Ethernet

T = 10/100/1000Base-T

F = 100/1000Base-X

The cryptographic modules meet the overall requirements applicable to Level 1 security of FIPS 140-2. The following table lists the level of validation for each area 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 and Services	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	NA
7	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	1

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

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

1.2 Hardware and Physical Cryptographic Boundary

The physical forms of the module's various models are depicted in Figures 1-4 below. For all models, the cryptographic boundary is defined as the outer edge of the chassis. The modules do not rely on external devices for input and output of critical security parameters (CSPs). Figures 5-6 are the uplink modules that are contained in the EX4300 chassis for the FIPS 140-2 validation and are inside the cryptographic module boundary.

The EX-UM-4X4SFP is the uplink module for the EX4300-24 and the EX4300-48 and is seen in the front view of the EX4300 chassis in Figure 1 and Figure 2. The EX-UM-8X8SFP is the uplink module for the EX4300-32 and is seen in the front view of the EX4300 in Figure 3.

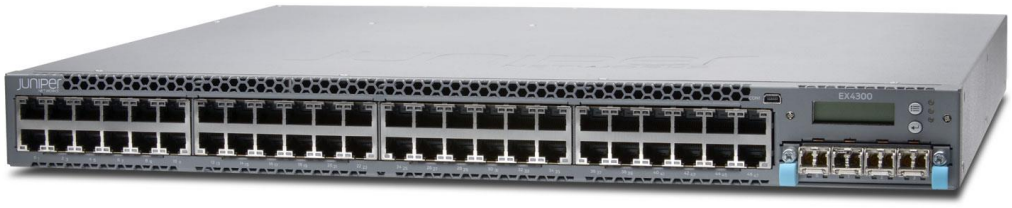

Figure 1 EX4300 48 ports Front View

Figure 2 EX4300 24 ports Front View

Figure 3 EX4300 32 ports Front View

Figure 4 EX4300 Back View (EX4300-24P, EX4300-24T & EX4300-48T)

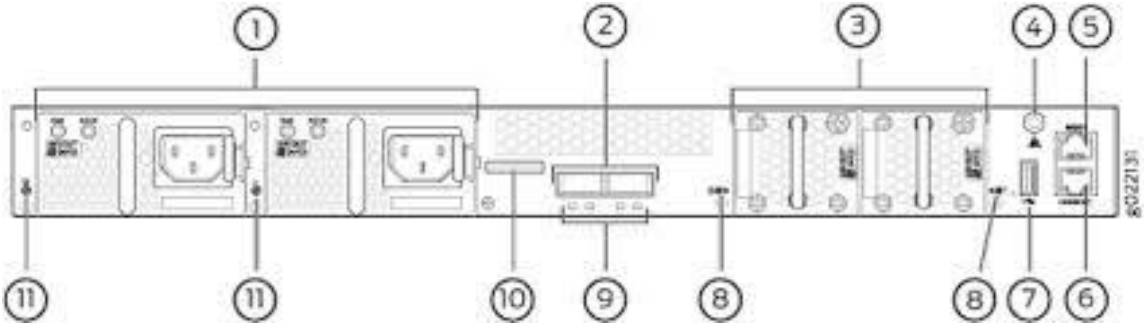

Figure 5 EX4300-32F Back View

1: Power supplies (slots 0,1)
2: QSFP + ports
3: Fan Modules (slots 0,1)
4: ESD point
5: Management port
6: Console port
7: USB port
8: Fan modules slot numbers
9: QSFP+ port LEDs
10: Serial number label
11: Power supply slot numbers

Figure 6 EX-UM-4X4SFP

The EX-UM-4X4SFP is for use in the EX4300-24 and the EX4300-48

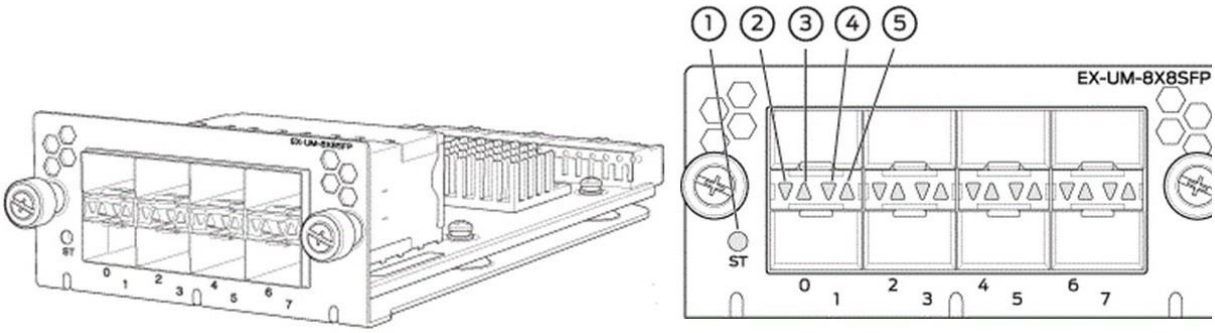

Figure 7 EX-UM-8X8SFP

The EX-UM-8X8SFP is for use in the EX4300-32

1: Status LED of Uplink module

2: Link Activity: Lower port

3: Link Activity: Upper port

4: Status LED: Lower port

5: Status LED: Upper port

The cryptographic module supports the physical ports and corresponding logical interfaces identified below. The flow of the data, control and status through the interfaces is controlled by the cryptographic module. The interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

The physical ports can be mapped to the logical interfaces. The mapping of the logical interfaces to the physical ports is shown in the following table:

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Ethernet	EX4300-24: 29 built-in (1 Management, 24 10/100/1000 Base-T, 4 QSFP+), 4 uplink module ports EX4300-32: 39 built-in (1 Management, 32 10/100/1000 Base-T, 4 SFP+, 2 QSFP+), 8 uplink module ports EX4300-48: 53 built-in (1 Management, 48 10/100/1000 Base-T, 4 QSFP+), 4 uplink module ports	LAN Communications	Control in, Data in, Data out, Status out
Serial	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Console serial port	Control in, Data in, Data out, Status out
USB	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Console mini-USB port	Control in, Data in, Data out, Status out
	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	USB port - load Junos image	Data in, Data out
Power	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Power connector, Power over Ethernet (EX4300-24P)	Power
Chassis LEDs	EX4300-24 (3), EX4300-32 (3), EX4300-48 (3)	Status indicator lighting	Status out
LCD Display	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Status Output	Status out
LCD Menu Button	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Control of the LCD status display	Control in

LCD Enter Button	EX4300-24 (1), EX4300-32 (1), EX4300-48 (1)	Control of the LCD status display	Control in

Table 4 – Network Port Configuration

Switch Models	Built -in Ports	Supported Uplink Module
EX4300-24	24 10/100/1000BASE-T Ethernet ports and four QSFP+ ports	4-port 10-Gigabit Ethernet SFP+ uplink module
EX4300-32	32 SFP ports, four SFP+ ports, and two QSFP+ ports	2-port 40-Gigabit Ethernet QSFP+ uplink module and 8-port 10-Gigabit Ethernet SFP+ uplink module
EX4300-48	48 10/100/1000BASE-T Ethernet ports and four QSFP+ ports	4-port 10-Gigabit Ethernet SFP+ uplink module

Table 5 – PHY Ports

Switch Models	1 G Phy copper BCM54380 (one core)	1 G Phy Fiber BCM54340 (one core)	10 G phy fiber/copper BCM84756 (four cores).
EX4300-24	3	0	1 if the uplink module is inserted.
EX4300-32	0	8	1 on base board, 2 on uplink module (if inserted)
EX4300-48	6	0	1 if the uplink module is inserted.

1.3 Modes of Operation

1.3.1 FIPS-Approved Modes

The EX4300 hardware versions contained in Table 1, with Junos OS 17.4R1-S4 installed, contains two FIPS-Approved modes of operation and a non-Approved mode of operation. The Junos OS 17.4R1-S4 firmware image must be installed on the device. The module is configured during initialization to operate in an approved mode or a non-approved mode.

The cryptographic officer shall place the module in a FIPS-Approved mode by following the instructions in the cryptographic officer guidance. 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 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 packet forwarding engine (PFE). The FIPS Standard Mode supports the approved and allowed algorithms, functions and protocols identified in Table 6 – 12. The services available in this mode are described in Tables 15 and 17.

The FIPS Recovery Mode is entered when the module is configured for FIPS mode and if at power-up any of the PFE POST fails but the RE POST all pass successfully. In the FIPS Recovery Mode, the module does not allow MACsec services and shuts down all data ports. The module supports the OpenSSL, LibMD and Kernel algorithms in Table 6-8; the algorithms in Table 11, and the SSH protocol in Table 12 when in the FIPS Recovery mode. The services available in the Recovery mode are described in Table 16 and Table 18.

1.3.2 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 2.4 as well as the algorithms supported in the FIPS-approved modes of operation.

If the module has been in a FIPS- Approved mode of operation, the cryptographic officer can configure the module to run in a non-Approved mode by following the instruction in the cryptographic officer guidance.

1.4 Zeroization

The cryptographic module provides a non-Approved mode of operation in which non-Approved cryptographic algorithms are supported. When transitioning between the non-Approved mode of operation and the FIPS-Approved mode of operation, or vice-versa, the cryptographic officer shall zeroize all keys and CSPs.

Zeroization completely erases all configuration information on the EX4300. The Crypto Officer initiates the zeroization process by entering the "*request system zeroized" (FIPS)* operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto Officer. (To zeroize the system *before* enabling FIPS mode, use the "request system zeroize media" command.)

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

To zeroize your switch:

1. From the CLI, enter
   root@switch> **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 Cryptographic 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 6, 7, 8, 9, 10 and 11 below. Table 12 summarizes the high-level protocol algorithm support.

2.1 Approved Algorithms

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
5506	AES	PUB 197-38A	CBC CTR	Key Sizes: 128, 192, 256	SSH Encrypt, Decrypt
N/A[1]	CKG	SSH-SP800- 133	Section 6.1 Section 6.2		Asymmetric seed generation using unmodified DRBG output
1956	CVL	SP800- 135	SSH	SHA 1, 256, 384, 512	Key Derivation
2177	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation
1479	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SSH KeyGen, SigGen, SigVer
3665	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 160	SSH Message Authentication
			SHA-384	Key size: 384 bits, λ = 384	
			SHA-512	Key size: 512 bits, λ = 512	
			SHA-256	Key size: 256 bits, λ = 256	SSH Message Authentication DRBG Primitive
N/A	KTS		AES Cert. # 5506 and HMAC Cert. # 3665		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. # 2773 and HMAC Cert. # 3665		key establishment methodology provides 112 bits of encryption strength
2956	RSA	PUB 186-4		n=2048 (SHA 256) n=4096 (SHA 256)	KeyGen[2] , SigGen, SigVer[3]

[1] Vendor Affirmed - asymmetric seed generation.

[2] 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.

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

4421	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
			SHA-512		Message Digest Generation
2773	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt
N/A[4]	KAS-SSC	SP 800-56Arev3	ECC DH	P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme - Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135 (SSH KDF CVL Cert. #1956)

Table 7 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
3663	HMAC	PUB 198	SHA-1 SHA-256	Key size: 160 bits, λ = 160	Password Hashing
				Key size: 256 bits, λ = 256	
4419	SHS	PUB 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 8 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
3664	HMAC	PUB 198	SHA-1 SHA-256	Key size: 160, λ = 160	Message Authentication
				Key size: 256, λ = 256	
4420	SHS	PUB 180-4	SHA-1 SHA-256		Message Digest

Table 9 – Control Plane QuickSec Approved Cryptographic Functions

Cert	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
5509	AES	PUB 197-38A	CBC, ECB	Key Sizes: 128, 256	AES CMAC
		SP800-38D	CMAC	Key Sizes: 128, 256	Key Derivation SP 800-108: Used to generate MACsec keys
		SP800-35F	KW	AES 128	Key Wrapping for MACsec keys
229	KBKDF	SP 800-108	CTR	CMAC AES 128, 256	KDF for MACsec keys
N/A	KTS		AES #5509		Key Wrapping

[4] Vendor Affirmed per IG D.1rev3.

Table 10 – MACsec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
5332	AES	SP800-38D	GCM	128	MACsec messaging
1269		PUB 198-38A	ECB	128	AES GCM

2.2 Allowed Algorithms

Table 11 – 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

2.3 Allowed Protocols

Table 12 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
MACsec MKA	MACsec Key Agreement	Shared secret	AES-GCM-128	HMAC-SHA256
SSHv2[5]	EC Diffie-Hellman P-256, P-384, P-521	ECDSA P-256 RSA	Triple-DES CBC AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1-96 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 MACsec and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 10 above: each column of options for a given protocol is independent, and may be used in any viable combination. These security functions are also available in the SSH connect (non-compliant) service.

The EX4300 switch can take on the role of Peer or Authenticator in reference to the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments.

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

2.4 Disallowed Algorithms

These algorithms are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation.

- RSA with keys less than 2048 bits
- DSA
- AES-GCM
- arcfour
- arcfour128
- arcfour256
- blowfish-cbc
- cast128-cbc
- Diffie-Hellman
- MD5
- HMAC-MD5
- ripemd160
- umac-64
- umac-128

2.5 Critical Security Parameters

All CSPs and public keys used by the module are described in this section. The CSPs in Table 13 are used in the FIPS Standard Mode. The FIPS Recovery Mode uses a subset of the CSPs found in Table 13. The MACsec CSPs are not available for use in FIPS Recovery Mode of operation.

Table 13 – Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the DRBG.
DRBG_State	V and Key values for the HMAC_DRBG.
Entropy Input String	256 bits entropy (min) input used to instantiate the DRBG.
ECDH Shared Secret	The Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256, RSA. Used to identify the host.
SSH ECDH	SSH Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in SSH. ECDH P-256, or ECDH P-384, ECDH P-521.
SSH SEKs	SSH Session Keys: SSH Session Encryption Key: TDES (3key) or AES; SSH Session Integrity Key: HMAC.
MACsec CAK	User-configured PSK entered when MACsec using static connectivity association key (CAK) security mode is enabled (32 characters).
MACsec CKN	User-configured PSK used to identify the CAK (64 characters).
MACsec SAK	Security Association Key used to encrypt/decrypt traffic for a given session. Derived from CAK using KDF SP 800-108. (128 bit AES)
MACsec KEK	Key Encryption Key used to transmit SAK to other members of a MACSec connectivity association. Derived from CAK using KDF SP 800-108. (128 bit AES).

MACsec ICK	Integrity Check Key used to verify the integrity and authenticity of MPDUs. Derived from CAK using KDF SP 800-108. (128/256 bit CMAC).
CO-PW	ASCII Text used to authenticate the CO.
User-PW	ASCII Text used to authenticate the User.

Table 14 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256.
SSH-ECDH-PUB	EC Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in SSH key establishment. ECDH P-256, ECDH P-384 or ECDH P-521
Auth-UPub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P256 or P-384
Auth-COPub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P256 or P-384
Root-CA	JuniperRootCA. ECDSA P-256 or P-384 X.509 Certificate; Used to verify the validity of the Juniper Package-CA at software load.
Package-CA	PackageCA. ECDSA P-256 X.509 Certificate; Used to verify the validity of Juniper Images at software load and also at runtime integrity.

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

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

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

The User role monitors the router via the console or SSH. The user role may not 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 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.

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

This leads to a maximum of nine (9) 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. Thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a one-minute period is $9/(96^{10})$, which is less than 1/100,000.

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

RSA signature verification: SSH public-key authentication. Processing constraints allow for a maximum of 5.6e7 RSA attempts per minute. The module supports RSA (2048, 4096), which has a minimum equivalent computational resistance to attack of 2^{112} (2048). Thus, the probability of a successful random attempt is $1/ (2^{112})$, which is less than 1/1,000,000. Processing speed (partial establishment of an SSH session) limits the number of failed authentication attempts in a one-minute period to 5.6e7 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{112})$, which is less than 1/100,000.

3.3 Approved and Allowed Services

All services implemented by the module are listed in the tables below. Table 19 lists the access to CSPs by each service.

Table 15 – Authenticated Services in FIPS Standard Mode

Service	Description	CO	User
Configure security	Security relevant configuration	X	
Configure	Non-security relevant configuration	X	
Secure Traffic	MACsec encrypted transfer of data	X	
Status	Show status	X	x
Zeroize	Destroy all CSPs	X	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	X	x
MACsec connect	Initiate MACsec connection	X	
Console access	Console monitoring and control (CLI)	X	x
Remote reset	Software initiated reset. Performs self-tests on demand.	X	
Load Image	Verification and loading of a validated firmware image into the switch.	X	
Account Management	Create administrative accounts.	X	

Table 16 – Authenticated Services in FIPS Recovery Mode

Service	Description	CO	User
Configure security	Security relevant configuration	X	
Configure	Non-security relevant configuration	X	
Status	Show status	X	x
Zeroize	Destroy all CSPs	X	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	X	x
Console access	Console monitoring and control (CLI)	X	x
Remote reset	Software initiated reset. Performs self-tests on demand.	X	
Load Image	Verification and loading of a validated firmware image into the switch.	X	
Account Management	Create administrative accounts.	X	

Table 17 – Unauthenticated Services in FIPS Standard Mode

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services

Table 18 – Unauthenticated Services in FIPS Recovery Mode

Service	Description
Local reset	Hardware reset or power cycle

Table 19 – CSP Access Rights within Services

		CSPs											
Service	DRBG_Seed	DRBG_State	Entropy Input String	SSH PHK	SSH DH	SSH-SEK	MACsec SAK	MACsec CAK	MACsec CKN	MACsec KEK	MACsec ICK	CO-PW	User-PW
Configure security	--	E	--	GW	--	--	GWR	WR	WR	GW	GW	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	--		--	--	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect	--	E	--	E	GE	GE	--	--	--	--	--	E	E
MACsec connect	--	E	--	--	--	--	E	--	--	E	E	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	E	E
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--
Account Management	--	--	--	--	--	--	--	--	--	--	--	W	W
Remote reset	GEZ	GZ	GZ	--	Z	Z	Z	--	--	--	Z	Z	Z
Local reset	GEZ	GZ	GZ	--	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
Z = Zeroize: The module zeroizes the CSP.

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. The security functions provided by the non-Approved services are identical to the Approved counterparts with the exception of SSH Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.4 and the SSHv2 row of Table 12.

Table 20 – Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	X	
Configure (non-compliant)	Non-security relevant configuration	X	
Secure Traffic (non-compliant)	MACsec encrypted transfer of data	X	
Status (non-compliant)	Show status	X	x
Zeroize (non-compliant)	Destroy all CSPs	X	
SSH connect (non-compliant)	Initiate SSH connection for SSH monitoring and control (CLI)	X	x
MACsec connect (non-compliant)	Initiate MACsec connection	X	
Load Image (non-compliant)	Verification and loading of a validated firmware image into the switch.	X	
Account Management (non-compliant)	Create administrative accounts.	X	
Console access (non-compliant)	Console monitoring and control (CLI)	X	x
Remote reset (non-compliant)	Software initiated reset. Performs self-tests on demand.	X	

Table 21 – Unauthenticated traffic

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

4 Self-tests

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

On power up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module in the FIPs Standard Mode of operation. If any one of the Routing Engine KATs fail, the module enters the Error state. If all the RE KATs pass and one or more of the PFE KATs fail, the module selects the FIPs Recover Mode of operation and all PFE algorithms are prevented from being used.

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

- Firmware Integrity check using ECDSA P-256 with SHA-256

Routing Engine (RE)

- **OpenSSL KATs**
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - KDF-SSH KAT
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate.
  - ECDSA P-256 Sign/Verify PCT
  - ECDH P-256 KAT
    - Derivation of the expected shared secret.
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
- **LibMD KATs**
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256
  - SHA-512
- **Kernel KATs**
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT

Packet Forwarding Engine (PFE)

- **Control Plane QuickSec KATs**
  - AES-ECB (128) Encrypt KAT
  - AES-ECB (128) Decrypt KAT

  - AES CMAC (128)
- **MACsec KATs**
  - AES-GCM (128) Encrypt KAT
  - AES-GCM (128) Decrypt KAT

- **Critical Function Test**
  - The cryptographic module performs a verification of a limited operational environment, and verification of optional non-critical packages.

The module also performs the following conditional self-tests:

- Continuous RNG Test on the SP 800-90A HMAC-DRBG
- Continuous RNG test on the NDRNG
- Pairwise consistency test when generating ECDSA, and RSA key pairs.
- Firmware Load Test (ECDSA signature verification)

5 Physical Security Policy

The module's physical embodiment is that of a multi-chip standalone device that meets Level 1 Physical Security requirements. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure. 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 *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. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The module requires two independent internal actions to be performed prior to outputting plaintext CSPs.
11. The cryptographic officer shall verify that the firmware image to be loaded on the module is a FIPS validated image. If any non-validated firmware image is loaded the module will no longer be a FIPS validated module.
12. The cryptographic officer shall retain control of the module while zeroization is in process.
13. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
14. The operator shall ensure the module does not encrypt more than 2^20 blocks with a single Triple-DES key when Triple-DES is the encryption-algorithm for SSH.
15. Virtual Chassis is not supported in FIPS mode and shall not be configured on the EX4300 device.
16. The module shall not be configured to use a radius server and the radius server capability shall be disabled.
17. The module shall only be used with CMVP FIPS 140-2 validation modules when supporting the MACsec protocol for providing Peer, Authenticator functionality.
18. The link between the Peer and Authenticator, used in the MACsec communication, shall be secure to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

6.1 Cryptographic-Officer Guidance

The cryptographic officer must check to verify the firmware image on the EX4300 is the FIPS 140-2 validated image. If the image is the FIPS 140-2 validated image, then proceed to section 6.1.2.

6.1.1 Installing the FIPS-Approved firmware image

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

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

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

NOTE: If you need to terminate the installation, do not reboot your switch; instead, finish the installation and then issue the request system software delete *package*.tgz command, where *package*.tgz is, for example, jinstall-ex-4300-17.4R1-S4-signed.tgz. This is your last chance to stop the installation.

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

user@switch> request system reboot (EX Series)

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 cryptographic officer is responsible for initializing the module in a FIPS-Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The cryptographic officer shall place the module in FIPS-Approved mode by first zeroizing the device to delete all keys and CSPs. The zeroizing instructions are in section 1.4 of this document. Next, the cryptographic officer shall follow the steps found in the *Junos OS FIPS Evaluated Configuration Guide for EX4300 Devices, Release 17.4 R1-S4* document Chapters 3 & 7 to place the module into a FIPS-Approved mode of operation. The steps from the aforementioned document are repeated below:

The FIPS Modes are not automatically enabled once the firmware image is installed on the platform. These steps are for putting the module into the FIPS Standard Mode 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 of RE power-on self-test pass successfully but one or more of the PFE power-on self-tests fail.

To enable FIPS mode in Junos OS on the switch:

1. Establish the root password access according to the FIPS guidelines
2. Enter configuration mode:
   root@switch> configure
   Entering configuration mode
   [edit]
   root@switch#
3. Enable FIPS mode on the switch by setting the FIPS level to 1, and verify the level:
   [edit]
   root@switch# **set system fips level 1**
   [edit]
   root@switch# **show system fips level**
   level 1;
4. Commit the configuration

   {master:0}[edit]
   root@switch# **commit**
   configuration check succeeds
   Generating RSA key /etc/ssh/fips_ssh_host_key
   Generating RSA2 key /etc/ssh/fips_ssh_host_rsa_key
   Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
   [edit]
   'system'
   reboot is required to transition to FIPS level 1
   commit complete

5. Reboot the switch:

   [edit]
   root@switch# **run request system reboot**
   Reboot the system ? [yes,no] (no) **yes**

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

   root@switch:fips>

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

   root@switch:fips> show version local

7. Configure local login authentication for Crypto Officer access and other FIPS users.
8. Configure the console port to log out automatically when you unplug the cable and

require the root password for single-user mode (Junos OS in FIPS mode automatically logs out of your user account when you disconnect because the log-out-on-disconnect configuration statement is enabled by default).

9. Configure the EX4300 to disable root password recovery

   ```
   [edit]
   crypto-officer@switch:fips# set system ports console insecure
   ```

10. Configure FIPS logging to record events.

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

As cryptographic officer, the operator may need to disable the FIPS-Approved mode of operation on the switch to return it to a non-Approved mode of operation. To disable FIPS-Approved mode on the switch, the EX4300 must be zeroized. Follow the steps found in section 1.4 to zeroize the EX4300.

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 switch. If the string ":fips" is present then the switch 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 switches and documentation in a secure area.
- Deploy switches in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
- Users are trusted.
- Users abide by all security guidelines.
- Users do not deliberately compromise security.
- Users behave responsibly at all times.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 22 – 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*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.

Table 23 – Acronyms and Definitions

Acronym	Definition
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CAK	Connectivity Association Key
CKN	Connectivity Association Key Name
DH	Diffie-Hellman
DSA	Digital Signature Algorithm

Acronym	Definition
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
ICV	Integrity Check Value (i.e. Tag)
ICK	Integrity Check Key
KEK	Key Encrypting Key
MACsec	Media Access Control Security
MD5	Message Digest 5
PSK	Pre-Shared Key
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SAK	Security Association Key
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 24 – Hardware Guide & Datasheets

Model	Document	URL
EX4300	EX4300 Hardware Guide	https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/topic-collections/hardware/ex-series/ex4300/book-hw-ex4300.pdf
EX4300	EX4300 Switches Datasheet	https://www.juniper.net/us/en/local/pdf/datasheets/1000467-en.pdf