Juniper Networks EX3300, EX4200, EX4500 Ethernet Switches

Security Policy

Document Version: 1.6

Date: March 6, 2014

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

List of Tables

1. Product Overview

The Juniper Networks EX3300, EX4200 and EX4500 Ethernet switches exhibit five key characteristics that, working together, deliver a true enterprise switching solution: carrier-class reliability, security risk management, network virtualization, application control, and reduced total cost of ownership (TCO). EX Series Ethernet Switches leverage much of the same field-proven Juniper Networks technology—including high-performance application-specific integrated circuits (ASICs), system architecture and Juniper Networks Junos® operating system—that power the world's largest service provider networks. The Juniper Networks EX Series Ethernet Switches are fully compatible with the Juniper Networks Unified Access Control (UAC), delivering an extra layer of security by first authenticating users and performing virus checks, then enforcing precise, end-to-end security policies that determine who can access what network resources, as well as quality of service (QoS) policies to ensure delivery of business processes.

The Juniper Networks EX3300 Ethernet Switch delivers a high-performance, flexible solution for converged data, voice, and video enterprise access environments, while providing a level of flexibility and ease of management previously available only with higher end access switches. The EX3300 switch is available with 24 or 48 10/100/1000BASE-T ports with or without PoE+.

The Juniper Networks EX4200 Ethernet switches are truly unique, delivering the best elements of chassis-based systems in a compact and efficient form factor. Designed for access and aggregation deployments, the EX4200 switches are a superset of the EX3200 switches, available offering 24 or 48-port 10/100/1000BASE-T configurations with optional GbE and 10GbE uplink modules. The EX4200 offers full and partial PoE options.

The Juniper Networks EX4500 Ethernet switches offer scalable, compact, high performance platforms for supporting high-density 10 gigabit per second (Gbps) data center top-of-rack as well as data center, campus, and service provider aggregation deployments. Featuring up to 48 wire-speed dual Gigabit Ethernet (GbE) and 10GbE pluggable ports in a two rack unit platform, the EX4500 switch delivers full Layer 2 and Layer 3 connectivity to networked devices such as servers and other switches.

2. Module Overview

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks EX3300, EX4200 and EX4500 Ethernet Switches Cryptographic Module from Juniper Networks. It provides detailed information relating to each of the FIPS 140-2 security requirements relevant to Juniper Networks EX3300, EX4200 and EX4500 Ethernet Switches Cryptogrpahic 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 EX switch. All other data input or output from the switch is considered plaintext for this FIPS 140-2 validation.

The EX switches run JUNOS. The validated version of JUNOS is 12.1R6.6; the image for each of the EX3300, EX4200 and EX4500 hardware platforms are:

ex-3300-12.1R6.6-domestic-signed.tgz

ex-4200-12.1R6.6-domestic-signed.tgz

ex-4500-12.1R6.6-domestic-signed.tgz

The Juniper Networks EX3300, EX4200 and EX4500 Ethernet Switches are cryptographic modules that are defined as multiple-chip standalone modules that execute JUNOS 12.1R6.6 firmware on the EX3300, EX4200 and EX4500 Ethernet Switches listed in Table 1. The cryptographic boundaries for the EX3300, EX4200 and EX4500 Ethernet Switches are defined as the outer edge of each 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-EX3300, EX4200, EX4500 Configurations

Models	Hardware Versions	Processor	RAM	Ethernet Ports	Power Over Ethernet	Airflow
EX3300	EX3300-24P	ARMv5	1GB/64 bit data width/667 MHz DDR2	24	24	Front-to-back
	EX3300-24T			24	N/A	Front-to-back
	EX3300-24T-DC			24	N/A	Front-to-back
	EX3300-48T			48	N/A	Front-to-back
	EX3300-48T-BF			48	N/A	Back-to-Front
	EX3300-48P			48	48	Front-to-back
EX4200	EX4200-24P	Freescale PowerPC	1GB DDR	24	24	Side Front-to-back
	EX4200-24PX			24	24	Side Front-to-back
	EX4200-24T			24	8	Side Front-to-back
	EX4200-24F			24	N/A	Side Front-to-back
	EX4200-48P			48	48	Side Front-to-back
	EX4200-48PX			48	48	Side Front-to-back
	EX4200-48T			48	8	Side Front-to-back
EX4500	EX4500-40F-FB	Freescale PowerPC	1GB DDR	40	N/A	Front-to-back
	EX4500-40F-BF			40	N/A	Back-to-Front

Images of the Cryptographic Modules

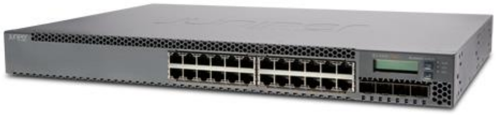

Figure 1 EX3300-24P, EX3300-24T, EX3300-24T-DC

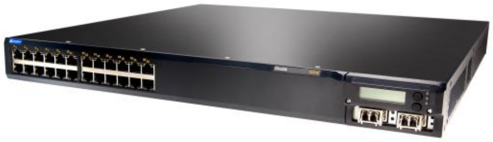

Figure 4 EX4200-24P, EX4200-24PX, EX4200-24T

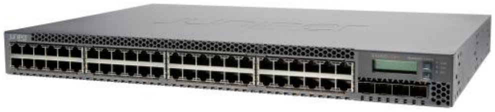

Figure 2 EX3300-48P, EX3300-48T, EX3300-48T-BF

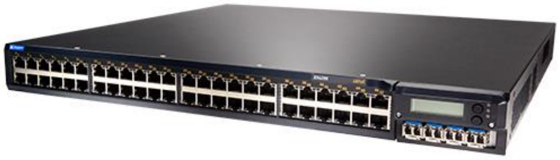

Figure 5 EX4200-48P, EX4200-48PX, EX4200-48T

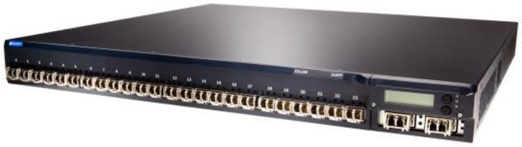

Figure 3 EX4200-24F

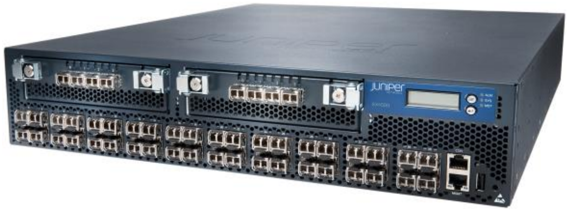

Figure 6 EX4500-40F-FB, EX4500-40F-BF

3. Security Level

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 per FIPS 140-2 Individual Sections

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	1

4. Modes of Operation

Approved Mode of Operation

The EX switches support a FIPS Approved mode of operation. The cryptographic officer can configure the module to run in a FIPS Approved mode of operation by following the instructions in the crypto-officer guidance. The FIPS Approved mode of operation supports the following FIPS Approved algorithms[1]:

- AES 128, 192, 256 for encryption/decryption
- DSA with 1024-bit keys for digital signature verification
- RSA with 1024 or 2048-bit keys for digital signature verification
- Triple-DES (three key) for encryption/decryption
- SHA-1 for hashing
- SHA-2 for hashing (SHA-224, SHA-256, SHA-384, SHA-512)

[1] The user of the module should review the Algorithm Transition Tables, available at the CMVP website (http://csrc.nist.gov/groups/STM/cmvp/) to determine the current status of algorithms and key lengths used in the module.

- HMAC-SHA-1
- HMAC-SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
- AES-128-CMAC
- SP 800-90 HMAC DRBG
- FIP 186 -2 (used for IV's, salt and passwords)
- SSH KDF

(See Appendix A – Cryptographic Algorithm Validation (CAVS) for Certificates)

The cryptographic modules also support the following non-Approved algorithms, which are allowed for use in FIPS mode:

- Diffie-Hellman with 2048-bit keys (key agreement; key establishment methodology provides 112 bits of encryption strength)
- ECDH P256, P384, P521 (key agreement; key establishment methodology provides 128 to 256 bits of encryption strength)
- Non-Deterministic Random Number Generators (NDRNG) used for entropy to seed the Approved HMAC-DRBG

The cryptographic module supports the commercially available SSH protocol for key establishment in accordance with FIPS 140-2 Annex D.

Placing the Module in the Approved Mode of Operation

The cryptographic officer shall place the module in FIPS Approved mode by following the instruction in the *Junos OS for EX Series Ethernet Switches, Release 12.1R6 FIPS* document.

The operator can verify that the module is in FIPS Approved mode by observing the prompt in cli and config modes which will have the format "<device name>:fips" where the device name is configured in under host-name.

Non-FIPS Mode of Operation

The module has a Non-Approved mode 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 *Junos OS for EX Series Ethernet Switches, Release 12.1R6 FIPS.*

The Non-Approved mode of operation supports the same algorithms that are supported in the Approved mode of operation.

5. Ports and Interfaces

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 Out Interface
- Data Control 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- FIPS 140-2 Ports/Interfaces

FIPS 140-2 Logical Interface	Port/Interface
Data Input	Ethernet, Serial
Data Output	Ethernet, Serial
Control Input	Ethernet, Serial, LCD
Status Output	Ethernet, Serial, LED, LCD
Power Interface	Power input, Power over Ethernet

The flow of input and output of data, control, and status is managed by the cryptographic module.

Details of each model’s hardware are available in the guides listed in Table 4.

Table 4 – EX Switches Hardware Guides

Model	Document Title	Download location
EX3300	EX3300 Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/ex3300/ex3300.html
EX4200	EX4200 Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/ex3200-ex4200/ex4200.html
EX4500	EX4500 Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/ex4500/ex4500.html

6. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports operator roles as follows:

- Cryptographic Officer (CO)
- User
- The cryptographic module shall enforce the separation of roles using either identity-based or role-based operator authentication; the cryptographic module meets Level 2 requirements because identity-based authentication is not enforced for all authorized services.

Table 5- Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Via Console: Username and password Via SSH-2: Password or RSA signature verification or DSA signature verification
	Role-based authentication	Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters
Cryptographic Officer	Identity-based operator authentication	Via Console: Username and password Via SSH-2: Password or RSA signature verification or DSA signature verification
	Role-based authentication	Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters

Table 6- Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and password	The module enforces 10-character passwords (at minimum) chosen from the 96+ human readable ASCII characters. The module enforces a timed access mechanism as follows: For the first two failed attempt (assuming 0 time to process), no timed access is enforced. The module enforces a 5-second delay before the third attempt is exercised. A new getty is spawned, by default, after the third attempt. If the module is configured to allow more attempts before spawning a new getty then the module enforces an additional 5-second delay for each attempt (e.g. 3rd failed attempt = 10-second delay, 4th failed attempt = 15-second delay, 5th failed attempt = 20-second delay, 6th failed attempt = 25-second delay). The best approach for the attacker would be for the module to be configured to allow greater than 3 attempts before spawning a new getty. The attacker should,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.
RSA signature	The module supports RSA (1024 or 2048-bit), which has a minimum equivalent computational resistance to attack of either 2^{80} or 2^{112} depending on the modulus size. Thus the probability of a successful random attempt is $1/(2^{80})$ or $1/ (2^{112})$, which are both less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one-minute period is $1125/(2^{80})$ or $1125/(2^{112})$, which are both less than 1/100,000.
DSA signature	The module supports DSA (1024-bit only) which have an equivalent computational resistance to attack of 2^{80}. Thus the probability of a successful random attempt is $1/ 2^{80}$, which is less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one-minute period is $1125/(2^{80})$, which is less than 1/100,000.

7. Access Control Policy - Roles and Services

Crypto Officer Role

The Crypto-Officer (CO) configures and monitors the module via a console or SSH connection. The cryptographic Officer has permission to view and edit secrets within the module Descriptions of the services available to the Crypto-Officer role are provided in the Table 7.

User Role

The User role accesses the module's cryptographic services that include configuring and monitoring the EX Switch via the console or SSH. The User Role may not change the configuration. Table 7 lists the services available to the User Role.

Table 7- Services Authorized for Roles in Approved FIPS mode

Role	Authorized Services
User: Configures and monitors the switch via the console, SSH.	Configuration Management: Allows the user to perform configuration on the switch that does not access CSPs. Status Checks: Allows the user to get the current status of the switch SSH-2: Provides encrypted login via the SSH-2 protocol. Console Access: Provides direct login access via the console.
Cryptographic Officer: Configures and monitors the switch via the console, SSH.	Configuration Management: Allows the CO to configure the switch. Switch Control: Allows the CO to modify the state of the switch. (Example: shutdown, reboot) Status Checks: Allows the CO to get the current status of the switch. Zeroize: Allows the CO to zeroize the configuration (all CSPs) within the module. Load Juniper image: Allows the verification and loading of a new validated firmware image into the switch. Note: Loading of non-validated firmware invalidates the module's FIPS 140-2 validation. SSH-2: Provides encrypted login via the SSH-2 protocol. Console Access: Provides direct login access via the console. Account Management: Allows the crypto-officer to create other administrative accounts. Self-tests: Allows the crypto-officer to perform cryptographic self-tests by restarting the module. Change Mode: Configure the module to run in a non-Approved mode.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module (LEDs and LCD).

Non-FIPS Mode Services

The cryptographic module supports the following services in a non-FIPS Approved mode of operation in addition to all the service that are listed above as available in the FIPS Approved mode of operation:

- Change Mode- Configure the module to run in a FIPS Approved mode: Enabled by crypto-officer
- Telnet and Rlogin, FTP, Finger, RSH, TFTP: Enabled by crypto-officer

Table 8 - Definition of Critical Security Parameters (CSPs)

CSP	Description	Zeroizaton	Use
SSH-2 Private Host Key	The first time SSH-2 is configured, the key is generated. DSA. Used to identify the host.	Zeroize command	Used to identify the host.
SSH-2 Session Key	Session keys used with SSH-2, TDES (3 key), AES 128, 192, 256, HMAC-SHA-1 key (160), DH Private Key 2048	Power Cycle	Symmetric key used to encrypt data between host and client
User Authentication Key	HMAC-SHA-1 Key Used to authenticate users to the module.	Zeroize command	Used to authenticate user to the module
CO Authentication Key	HMAC-SHA-1 Key Used to authenticate COs to the module.	Zeroize command	Used to authenticate CO to the module
RADIUS shared secret	Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block	Zeroize command	Used to authenticate COs and Users
TACACS+ shared secret	Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block	Zeroize command	Used to authenticate COs and Users
HMAC DRBG Seed	Seed for DRBG	Power Cycle	For seeding DRBG
HMAC DRBG V value	The value *V* of *outlen* bits, which is updated each time another *outlen* bits of output are produced	Power Cycle	A critical value of the internal state of DRBG
HMAC DRBG Key value	The current value of key. The *outlen*-bit *Key*, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits	Power Cycle	A critical value of the internal state of DRBG
NDRNG entropy	Used as entropy input string to the HMAC DRBG	Power Cycle	Entropy input to HMAC DRBG

Table 9 - Definition of Public Keys

Key	Description/Usage
SSH-2 Public Host Key	First time SSH-2 is configured, the key is generated. DSA. Identifies the host.
User Authentication Public Keys	Used to authenticate users to the module. RSA (1024 or 2048-bit) or DSA
CO Authentication Public Keys	Used to authenticate CO to the module. RSA (1024 or 2048-bit) or DSA
JuniperRootCA	RSA 2048-bit X.509 certificate Used to verify the validity of the Juniper image at software load and also at runtime for integrity.
EngineeringCA	RSA 2048-bit X.509 certificate Used to verify the validity of the Juniper image at software load and also at runtime for integrity.
PackageCA	RSA 2048-bit X.509 certificate Used to verify the validity of the Juniper image at software load and also at runtime for integrity.
PackageProduction	RSA 2048-bit X.509 certificate Certificate that holds the public key of the signing key that was used to generate all the signatures used on the packages and signature lists.
DH Public Keys	Used within SSH-2 for key establishment.

Definition of CSP Modes of Access

Table 8 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 10- CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSP Access Operation
CO	User		R=Read, W=Write, D=Delete
X		Configuration Management	All CSPs (**R, W, D**)
	X	Configuration Management	No access to CSPs
X		Switch Control	No access to CSPs
X	X	Status Checks	No access to CSPs
X		Zeroize	All CSPs (**D**)
X		Load New Software	No access to CSPs
X	X	SSH-2	SSH-2 session key (**R**)
X	X	Console Access	CO Authentication Key, User Authentication Key (**R**)
X		Account Management	Creates or removes passwords (**W, D**)
X		Self-tests	No access to CSPs

8. Operational Environment

The FIPS 140-2 Operational Environment is a limited operational environment. The module's operating system is JUNOS OS version 12.1R6.6.

9. Security Rules

The cryptographic module design corresponds to the cryptographic module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of a FIPS 140-2 Level 1 module.

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. This cryptographic module performs the following self-tests:

- Power-Up Self-Tests:
  - Cryptographic Algorithm Tests
    - TDES Encrypt/Decrypt Known Answer Test (KAT)
    - AES Encrypt/Decrypt KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA2 KAT (SHA-224, SHA-256, SHA-384, SHA-512)
    - RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
    - DSA pairwise consistency test (sign/verify) and KAT
    - FIPS 186-2 RNG KAT
    - FIPS 800-90 HMAC DRBG
    - ECDSA (failure of self-test will cause an error state, algorithm not available for use in module)
    - ECDH
    - KDF SSH
    - KDF IKE-V1 KATs (failure of self-test will cause an error state, algorithm not available for use in module)
  - Firmware integrity test:
    - RSA digital signature verification (PKCS1.5, 2048-bit key, SHA-1) and SHA-1 hash verification.
  - Critical functions tests
    - Verification of Limited Environment

- Conditional self-tests:
  - Pairwise consistency tests
    - RSA pairwise consistency test (sign/verify and encrypt/decrypt)
    - DSA pairwise consistency test (sign/verify)
  - Firmware load test: RSA digital signature verification (2048-bit key)
  - Manual key entry test: Duplicate key entries test
  - Continuous random number generator test: performed on the Approved FIPS 186-2, Appendix 3.1 RNG, Approved DRBG and on the NDRNGs before each use.
  - Bypass test is not applicable.

If any of the self-test fail, the module enters a panic state (error state) and shuts down.

Any time the cryptographic module is in an idle state, the operator is capable of commanding the modules to perform the power-up self-test by power-cycling the module.

Data output is inhibited during key generation, self-tests, zeroization, and error states.

Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the modules.

The module supports concurrent operators.

The module is validated with JUNOS is 12.1R6.6 firmware. The loading of non-validated firmware nullifies the FIPS 140-2 validation.

10. Physical Security Policy

The modules physical embodiment is that of a multi-chip standalone device that meets the FIPS 140-2 Level 1 physical security requirements. The module is completely enclosed in rectangular, cold rolled steel, plated steel, and brushed aluminum enclosure with a nickel or clear zinc coating.

11. Mitigation of Other Attacks Policy

A tamper evident label shall be installed over the USB port on the EX3300, EX4200 and EX4500. A tamper-evident label must be installed over the Virtual Chassis ports on the EX4200 and EX4500. The tamper evident label will show evidence if the USB port is used or if the Virtual Chassis. See Crypto Officer Guidance for placement and instructions on applying the tamper evident label over the USB port.

12. Guidance

Crypto-Officer Guidance

Enabling FIPS Approved Mode of Operation

The crypto-officer is responsible for initializing the module in a FIPS Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The crypto-officer should follow the steps found in the *Junos OS for EX Series Ethernet Switches, Release 12.1R6 FIPS* document Chapter 2. The crypto-officer must apply the tamper evident label on the module for a FIPS Approved mode of operation.

Placing the Module in a Non-Approved Mode of Operation

As Crypto Officer, the operator may need to disable FIPS mode of operation on the switch to return it to non-FIPS operation. To disable FIPS mode on the switch follow the steps found in the *Junos OS for EX Series Ethernet Switches, Release 12.1R6 FIPS* document Chapter 2 in the section titled Disabling FIPS Mode.

Tamper Evident Labels

The EX3300, EX4200 and EX4500 Ethernet switches require a tamper evident seal over the USB port and over the virtual chassis ports (EX4200 and EX4500) to operate in a FIPS Approved mode of operation. The crypto-officer can obtain tamper evident seals from Juniper Networks using the part number **520-052564**

The crypto-officer is responsible for applying and checking the labels on the EX switch periodically to verify the security of the module is maintained.

Tamper Evident Seal Instructions:
Each switch platform requires a tamper-evident seal on its USB port. In addition, the AUX port or Mini-USB port on certain switches requires a seal and virtual chassis ports on the EX4200 require tamper-evident seals (For details, see the specific instructions for your switch.) For all seal applications, follow these general instructions:

1. Handle the seals with care. Do not touch the adhesive side. Do not cut a seal to make it fit.
2. Make sure all surfaces to which the seals are applied are clean and dry and clear of any residue.
3. Apply the seals with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

EX3300 Tamper-Evident Seal Application –One tamper-evident seal

Apply one tamper-evident seal to the USB port to secure the EX3300 cryptographic module.

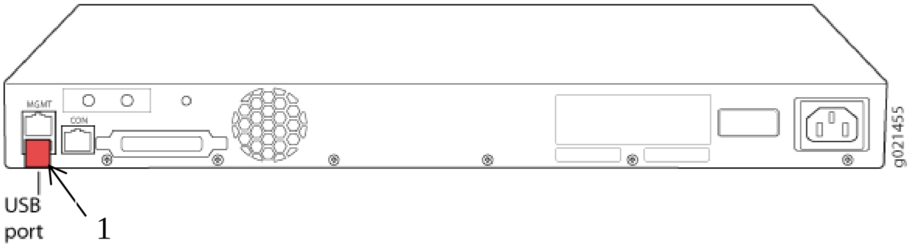

Figure 7: EX3300- 24P, EX3300-24T, EX3300-24T-DC, EX3300-48T, EX3300-48T-BF, EX3300-48P Tamper-Evident Seal Location—Switch Rear

EX4200 Tamper-Evident Seal Application –Three tamper-evident seals

Apply three tamper-evident seals to the EX4200. One tamper-evident seal is applied to cover the USB port. One tamper-evident label is applied to cover virtual chassis port 0 (VC0) and one tamper-evident label is applied to cover virtual chassis port 1 (VC1). All tamper evident-labels must be applied to secure the EX4200 cryptographic module.

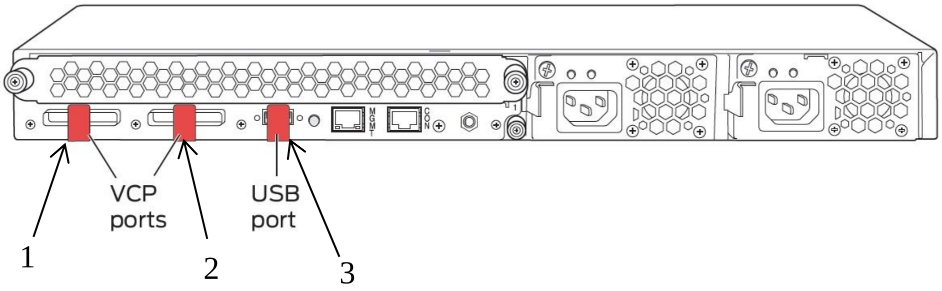

Figure 8: EX4200-24P, EX4200-24PX, EX4200-24T, EX4200-24F, EX4200-48P, EX4200-48PX, EX4200-48T Tamper-Evident Seal Location—Switch Rear

EX4500 Tamper-Evident Seal Application –Three tamper-evident seals

Apply one tamper-evident seal to the USB port on the front of the EX4500 cryptographic module.

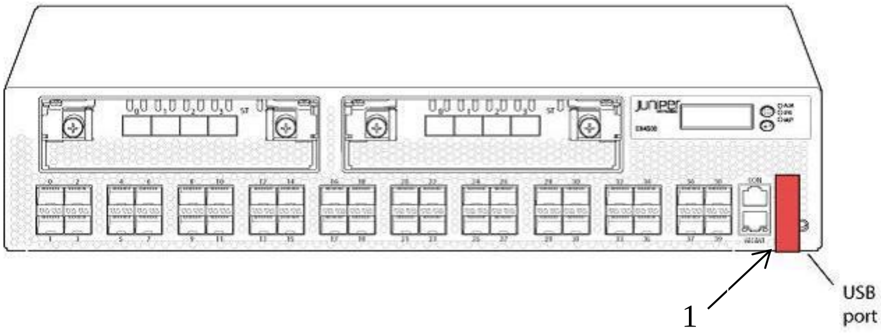

Figure 9: EX4500-40F-FB & EX4500-40F-BF Tamper-Evident Seal Location—Switch Front

Apply two tamper evident seals to the back of the EX4500. One tamper-evident label is applied to cover virtual chassis port 0 (VC0) and one tamper-evident label is applied to cover virtual chassis port 1 (VC1). All tamper evident-labels must be applied to secure the EX4500 cryptographic module.

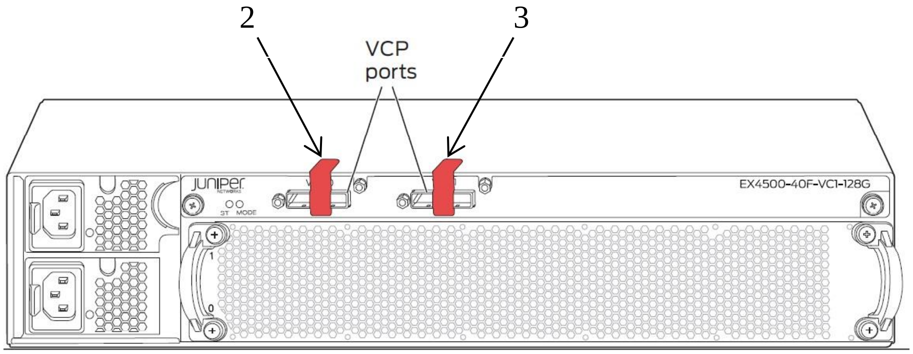

Figure 10 EX4500-40F-FB & EX4500-40F-BF Tamper-Evident Seal Location -Switch Back

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.

```
login: fips-user1
Password:

--- JUNOS 12.1Rx.x built 2013-05-03 08:05:43 UTC
{master:0}
fips-user1@cst-ex3300:fips>
```

13. Acronyms

Table 11- Acronyms

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC-SHA-1	Keyed-Hash Message Authentication Code
RADIUS	Remote Authentication Dial-In User Service
RSA	Public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman.
SHA-1	Secure Hash Algorithms
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TDES	Triple - Data Encryption Standard
UDP	User Datagram Protocol

Appendix A — Cryptographic Algorithm Validation (CAVS) Certificates

Table 12- Algorithm Certifications

	Algorithm	CAVS Validation
RNG	RNG	1187
QUICKSEC	AES	2419
	TDES	1507
	SHA	2076
	RSA	1251
	HMAC	1504
	DRBG 800-90A	324
SSH-IPSEC	AES	2420
	TDES	1508
	SHA	2077
	HMAC	1505
	DRBG 800-90A	325
	RSA	1252
Kernel	AES	2396
	TDES	1494
	SHA	2058
	HMAC	1488
MD	SHA	2059
	HMAC	1489

OpenSSL	AES	2475
	TDES	1514
	DSA	762
	SHA	2094
	RSA	1264
	HMAC	1518
	DRBG 800-90A	338
	KDF 800-135	81

About Juniper Networks

Juniper Networks was founded on a simple but incredibly powerful vision for the future of the network: "Connect everything. Empower everyone."

We believe the network is the single greatest vehicle for knowledge, understanding, and human advancement the world has ever known. We are dedicated to uncovering new ideas and creating the innovations that will serve the exponential demands of the networked world. To do this, we're leading the charge to architecting the new network, built on simplicity, security, openness and scale.