Juniper Networks
EX4300 Ethernet Switches

Non-Proprietary Security Policy

Document Version: 2.0

Date: December 6, 2016

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

1. Product Overview

The Juniper Networks EX4300 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 EX4300 Ethernet Switches deliver a full suite of Layer 2 and Layer 3 switching capabilities. The EX4300 switches can be interconnected over multiple 40GbE quad small form factor pluggable plus (QSFP+) transceiver ports to form a 320 gigabit per second (Gbps) backplane. A flexible uplink module that supports both 1GbE and 10GbE options is also available, enabling high-speed connectivity to aggregation- or core-layer switches which connect multiple floors or buildings.

2. Module Overview

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks EX4300 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 EX4300 Ethernet Switches 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. 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 14.1X53-D30.3; the image for the EX4300 hardware platforms is:

- jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz

The Juniper Networks EX4300 Ethernet Switches are cryptographic modules that are defined as multiple-chip standalone modules that execute JUNOS 14.1X53-D30.3 firmware on the EX4300 Ethernet Switches listed in Table 1. The cryptographic boundaries for the EX4300 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. Each hardware version requires use of a tamper seal (P/N 520-052564).

Table 1-EX4300 Configurations

Models	Hardware Versions	Processor	RAM	Ethernet Ports	Power Over Ethernet
EX4300	EX4300-24P	Freescale PowerPC	2GB DDR	24	24
	EX4300-24T			24	N/A
	EX4300-48P			48	48
	EX4300-48T			48	N/A
	EX4300-32F			32	N/A

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

T = 10/100/1000BASE-T

F = 100/1000BASE-X

Images of the Cryptographic Modules

EX4300-24P/24T

EX4300-48P/48T

EX4300-32F

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	3
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	N/A

4. Modes of Operation

Approved Mode of Operation

The EX4300 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.

Approved Algorithms

The FIPS Approved mode of operation supports the following FIPS Approved algorithms[1]:

Table 3-FIPS Approved Algorithms

Algorithm Implementation	Reference	Mode	Functions	Strength	Cert
OpenSSL AES	FIPS 197, SP 800-38A	CBC, CTR	SSH Enc/Dec	128, 192, 256	3655
OpenSSL SSH KDF	SP 800-135	SSHv2	SSH Key Derivation	128, 192, 256[2]	668
OpenSSL DRBG	SP 800-90A	HMAC-SHA-256	Random Bit Generation	256	984
OpenSSL ECDSA	FIPS 186-4	P-256	SSH SigGen, Package SigVer	128	763
		P-256, P-384, P-521	SSH KeyGen, SSH SigVer	128, 192, 256	763
MD HMAC	FIPS 198-1	SHA-1, SHA-256	Password HMAC	128, 256,	2404
OpenSSL HMAC	FIPS 198-1	SHA-1, SHA-256, SHA-512	SSH HMAC Gen/Ver	128, 256	2405[3]
MD SHA	FIPS 180-4	SHA-1, SHA-256, SHA-512	Hash for HMAC, Password Hash	128, 256	3072
OpenSSL SHA	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512	Hash for HMAC, Sig Gen, Sig Ver	128, 256	3073
OpenSSL Triple-DES	SP 800-20	TCBC	SSH Enc/Dec	112	2045

[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.

[2] The strength of the SSH KDF is the minimum of the Key Agreement method and the HMAC used.

[3] HMAC-SHA-384 is not used by any of the module's services.

Non-Approved but Allowed Cryptographic Functions

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

- non-SP 800-56A Elliptic Curve Diffie-Hellman P-256, P-384, P-521 (key agreement; key establishment methodology provides 128, 192, or 256 bits of encryption strength)
- Non-Deterministic Random Number Generators (NDRNG) used for entropy to seed the Approved HMAC-DRBG

Protocols Allowed in FIPS Mode

The cryptographic module supports the commercially available SSHv2 protocol. The following algorithms are utilized:

- Host Authentication
  - ecdsa-sha2-nistp256: ECDSA P-256 with SHA-256
- (optional) Client Authentication
  - ecdsa-sha2-nistp256: ECDSA P-256 with SHA-256
  - ecdsa-sha2-nistp384: ECDSA P-384 with SHA-384
  - ecdsa-sha2-nistp521: ECDSA P-521 with SHA-512
- Key Agreement
  - ecdh-sha2-nistp256: Elliptic Curve Diffie-Hellman P-256 with SHA-256
  - ecdh-sha2-nistp384: Elliptic Curve Diffie-Hellman P-384 with SHA-384
  - ecdh-sha2-nistp521: Elliptic Curve Diffie-Hellman P-521 with SHA-512
- Key Derivation
  - SSHv2 KDF
- Encryption
  - aes128/128/256-ctr
  - aes128/192/256-cbc
  - 3des-cbc: 3 key Triple-DES
- Message Authentication
  - hmac-sha1
  - hmac-sha2-256
  - hmac-sha2-512

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 14.1X53 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 Approved 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 14.1X53 FIPS.*

The module supports the following non-Approved and non-Compliant algorithms when it is configured in the non-FIPS Approved mode:

- arcfour
- blowfish
- cast128
- Diffie-Hellman (non-compliant; key agreement; key establishment methodology provides less than 112 bits of encryption strength)
- DSA
- HMAC-MD5
- HMAC-SHA-1-96 (non-compliant)
- MD5
- ripemd160
- RSA
- umac-64
- umac-128

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 module contains the following physical ports:

- Management Ethernet Port
- Packet Forwarding Engine (PFE) Ethernet Ports
- Console Serial Port
- Menu Buttons
- LEDs
- LCD Display
- Power Input Port
- USB – Disabled
- Virtual Chassis – Disable

The interfaces can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out 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 4- FIPS 140-2 Ports/Interfaces

FIPS 140-2 Logical Interface	Port/Interface
Data Input	Management, PFE, Console
Data Output	Management, PFE, Console
Control Input	Management, PFE, Console, Menu Buttons
Status Output	Management, PFE, Console, LED, LCD
Power Interface	Power input, PFE (Power over Ethernet)
N/A – Disabled	USB, Virtual Chassis

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 5.

Table 5 – EX Switches Hardware Guides

Model	Document Title	Download location
EX4300	EX4300 Datasheet	http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000467-en.pdf

6. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports operator roles as follows:

- Cryptographic Officer (CO)
- User

The cryptographic module enforces the separation of roles using identity-based operator authentication.

Table 6- 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: Username and password or ECDSA signature verification
Cryptographic Officer	Identity-based operator authentication	Via Console: Username and password Via SSH-2: Username and password or ECDSA signature verification

Table 7- 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.
ECDSA signature	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.

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 CO has permission to view and edit secrets within the module. Descriptions of the services available to the CO role are provided in Table 8.

User Role

The User role accesses the module's cryptographic services that include configuring and monitoring the module via the console or SSH. The User Role may not change the configuration. Table 8 lists the services available to the User Role.

Table 8- Services Authorized for Roles in Approved FIPS mode

Role	Authorized Services
User: Configures and monitors the switch via the console, SSH.	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 services 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

8. Critical Security Parameters

Table 9 - 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. ECDSA P-256. Used to identify the host.	Zeroize command	Used to identify the host.
SSH-2 Session Key	Session keys used with SSH-2, Triple-DES-CBC (3 key), AES-CBC/CTR 128, 192, 256, HMAC-SHA-512, HMAC-SHA-256, HMAC-SHA-1 key (160)	Session termination, Zeroize	Symmetric key used to encrypt and authenticate data

CSP	Description	Zeroizaton	Use
	Key Agreement Keys: ECDH Private Key (P-256, P-384, or P-521)	command, Power Cycle	between host and client
User Authentication Password	Stored Salted and hashed with SHA-1, SHA-256, or SHA-512 Used to authenticate users to the module.	Zeroize command	Used to authenticate user to the module
CO Authentication Password	Stored Salted and hashed with SHA-1, SHA-256, or SHA-512 Used to authenticate COs to the module.	Zeroize command	Used to authenticate COs to the module
HMAC DRBG Seed	Seed for DRBG	Zeroize command, 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	Zeroize command, 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	Zeroize command, Power Cycle	A critical value of the internal state of DRBG
NDRNG entropy pool	Used as entropy input string to the HMAC DRBG	Zeroize, command, Power Cycle	Entropy input to HMAC DRBG

Table 10 - Definition of Public Keys

Key	Description/Usage
SSH-2 Public Host Key	First time SSH-2 is configured, the key is generated. P-256 ECDSA key. Identifies the host.
User Authentication Public Keys	Used to authenticate users to the module. ECDSA (P-256, P-384, or P-521)
CO Authentication Public Keys	Used to authenticate CO to the module. ECDSA (P-256, P-384, or P-521)
JuniperRootCA	ECDSA P-256 w/ SHA-256 X.509 certificate Used to verify the validity of the PackageCA certificate.
PackageCA	ECDSA P-256 w/ SHA-256 X.509 certificate Used to verify the validity of the Package Production certificate.

Package Production	ECDSA P-256 w/ SHA-256 X.509 certificate Used to verify the validity of the Juniper image during the firmware load and power-up integrity tests.
ECDH Public Keys	ECDH (P-256, P-384, or P-521) Used within SSH-2 for key establishment.

Definition of CSP Modes of Access

Table 11 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 11- CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete, G=Generate
CO	User		
X		Configuration Management	All CSPs (**R, W, D**) SSH-2 Private Host Key (**W, D, G)**
	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, G**)
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
X		Change Mode	All CSPs (**D**)

9. Operational Environment

The FIPS 140-2 Operational Environment is a limited operational environment. The module's operating system is JUNOS OS version 14.1X53-D30.3.

10. 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
    - Triple-DES Encrypt Known Answer Test (KAT)
    - Triple-DES Decrypt KAT
    - AES-CBC 128 Encrypt KAT
    - AES-CBC 128 Decrypt KAT
    - AES-CBC 192 Encrypt KAT
    - AES-CBC 192 Decrypt KAT
    - AES-CBC 256 Encrypt KAT
    - AES-CBC 256 Decrypt KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - FIPS SP 800-90A HMAC DRBG KAT: includes instantiate, reseed, and generate
    - ECDSA P-256 pairwise consistency test (sign/verify)
    - ECDH P-256 KAT
    - KDF SSH KAT
    - MD HMAC-SHA-1 KAT
    - MD HMAC-SHA-256 KAT
    - MD SHA-512 KAT
  - Firmware integrity test:
    - ECDSA digital signature verification (P-256, SHA-256)
  - Critical functions tests
    - Verification of Limited Environment

- Conditional self-tests:
  - Pairwise consistency tests upon key generation:
    - ECDSA pairwise consistency test (sign/verify)
    - ECDH pairwise consistency test
  - Firmware load test: ECDSA digital signature verification (P-256, SHA-256)
  - Continuous random number generator test: performed on the Approved DRBG and on the NDRNGs before each use.

If any of the self-tests fail, the module enters the 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 cryptographic officer must maintain control of the module while zeroization is in process (approximately 10 minutes).

The module is validated with JUNOS 14.1X53-D30.3 firmware. The loading of non-validated firmware nullifies the FIPS 140-2 validation.

11. Physical Security Policy

The module's 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.

12. Mitigation of Other Attacks Policy

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

13. 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 14.1X53 FIPS* document Chapter 2. The steps from the aforementioned document are repeated below:

1. Enter configuration mode:

```
root@switch> configure
Entering configuration mode
[edit]
root@switch#
```

2. 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;
```

3. Commit the configuration:

```
root@switch# commit
```

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 14.1X53 FIPS* document Chapter 2 in the section titled Disabling FIPS Mode.

Tamper Evident Seal

The EX4300 Ethernet Switches require a tamper evident seal over the USB port and over the Virtual Chassis ports (EX4300) to operate in a FIPS Approved mode of operation. The tamper evident seal will show evidence if the USB or Virtual Chassis ports are used. 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 module 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 EX3300 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.

EX4300 Tamper-Evident Seal Application – One (1) tamper-evident seal

One (1) tamper-evident seal is applied to cover the USB port and must be applied to secure the EX4300 cryptographic module.

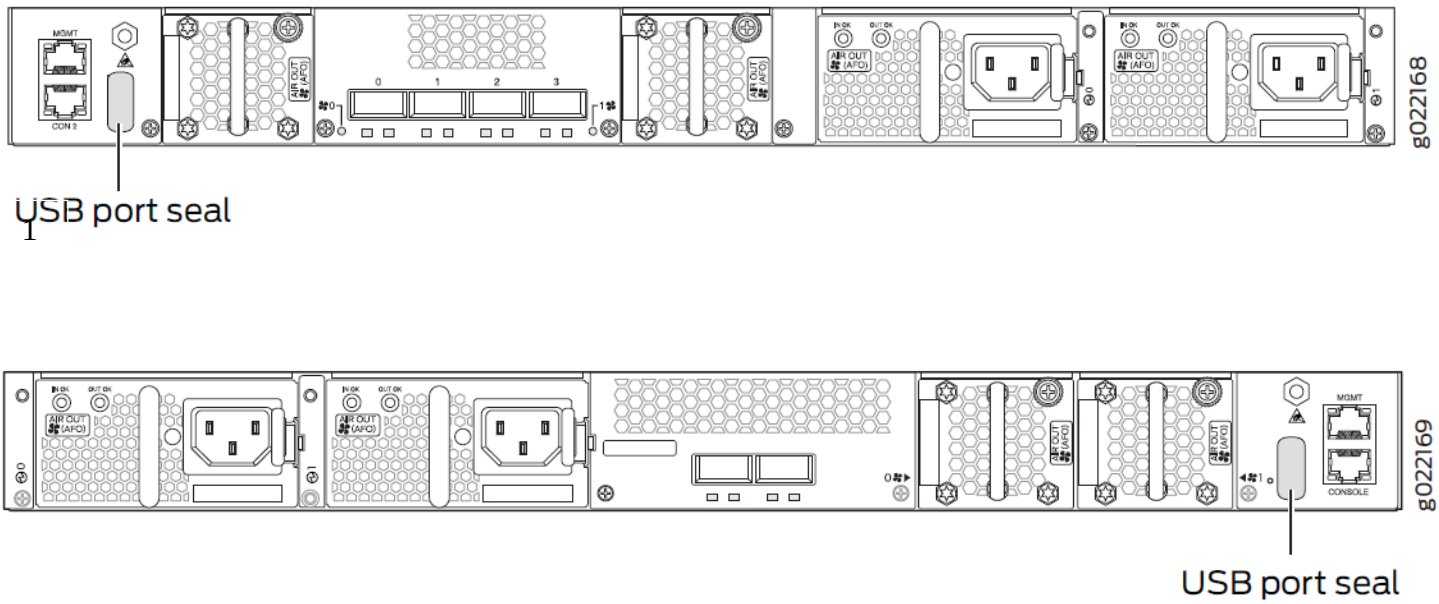

Figure 1: EX4300-24P, EX4300-24T, EX4300-48P, EX4300-48T, and EX4300-32F Tamper-Evident Seal Location—Switch Rear

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 14.1X53-D30.3 built 2015-10-02 09:51:00 UTC
{master:0}
fips-user1@cst-ex4300:fips>
```

14. Acronyms

Table 12- Acronyms

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
CLI	Command Line Interface
ECDSA	Elliptic Curve Digital Signature Algorithm

EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC-SHA-1	Keyed-Hash Message Authentication Code
PFE	Packet Forwarding Engine
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
TCP	Transmission Control Protocol
Triple-DES	Triple - Data Encryption Standard
UDP	User Datagram Protocol

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.