Juniper Networks SRX3400 and SRX3600 Services Gateways

Security Policy

Document Version: 1.0

Date: October 4, 2011

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. Module Overview

The Juniper Networks SRX3000 Series line of services gateways is the next generation solution for securing the ever increasing network infrastructure and applications requirements for both enterprise and service provider environments. Designed from the ground up to provide flexible processing scalability, I/O scalability, and services integration, the SRX3000 Series line can meet the network and security requirements of data center hyper-consolidation, rapid managed services deployments, and aggregation of security solutions.

Incorporating the routing heritage and service provider reliability of Junos OS with the rich security heritage of ScreenOS, service provider reliability, and ScreenOS security heritage, the SRX Series also offers the high feature/service integration necessary to secure modern network infrastructure and applications.

The Juniper Networks SRX3000 Series Services Gateways consist of models SRX3400 and SRX3600 running JUNOS-FIPS, a version of JUNOS created specifically for FIPS compliance. The validated version of JUNOS-FIPS is 10.4R3; the image is `junos-srx1k3k-10.4R3.4-fips.tgz`.

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware on any of the Juniper Networks SRX-Series gateways listed in the table below. The cryptographic boundary for the SRX3400 and SRX3600 is defined as the outer edge of the chassis, excluding the power distribution module on the rear of the device. The cryptographic module's operational environment is a limited operational environment.

SRX Series Configurations

Series	Model	Hardware version
SRX Series	SRX3400	SRX3400BASE-AC, SRX3400BASE-DC
	SRX3600	SRX3600BASE-AC, SRX3600BASE-DC

Figure 1. Images of the Cryptographic Modules

SRX3400

SRX3600

Figure 1 depicts the SRX series without tamper seals. For depictions of the units with tamper seals, see section 9.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Security Level

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

3. Modes of Operation

Approved Mode of Operation

The cryptographic modules support FIPS-Approved algorithms as follows:

- AES 128, 192, 256 for encryption/decryption
- DSA with 1024-bit keys for digital signature generation and verification
- RSA with 1024 or 2048-bit keys for digital signature generation and verification
- Triple-DES for encryption/decryption
- SHA-1 for hashing
- SHA-2 for hashing (SHA-256)
- HMAC-SHA-1
- HMAC-SHA-256
- FIPS 186-2 RNG (with Change Notice)

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

- RSA with 1024-bit keys (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- Diffie-Hellman with 1536-bit keys (key agreement; key establishment methodology provides 96 bits of encryption strength)

The cryptographic modules support the commercially available IKEv1, and SSH protocols for key establishment in accordance with FIPS 140-2 Annex D.

The cryptographic module contains a non-FIPS validated deterministic random number generator (RNG) that is compliant with the FIPS 186-2.

Placing the Module in the Approved Mode of Operation

Once the JUNOS-FIPS firmware image `junos-srx1k3k-10.4R3.4-fips.tgz` is installed on the device, has successfully run its integrity and self-tests, it is operating in the approved mode. The Crypto-Officer must ensure that the backup image of the firmware is also a JUNOS-FIPS image by issuing the *request system* snapshot command. No further configuration is necessary for the purpose of placing it in FIPS mode.

Non-FIPS Mode of Operation

The cryptographic module does not provide a non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module supports the following physical ports and corresponding logical interfaces:

- **Ethernet:** Data Input, Data Output, Control Input, Status Outputs
- **Serial:** Control Input, Status Outputs
- **Power interface:** Power Input
- **Reset:** Control Input
- **LEDs:** Status Output

The flow of input and output of data, control, and status is managed by the cryptographic module. Details of each models hardware is available in the guides listed below.

Hardware Guides

Model	Document Title	Download location
SRX3400	SRX3400 Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/hardware/SRX3400/index.html
SRX3600	SRX3600 Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/hardware/SRX3600/index.html

Control input options and status output (not provided by the hardware) are described in the *JUNOS Software System Basics Configuration Guide, Release 10.4* which is available for download at: http://www.juniper.net/techpubs/software/junos-srx/junos-srx10.4/index.html.

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports operator roles as follows:

- Cryptographic Officer (CO)
- User (read-write)
- User (read-only)

The cryptographic module enforces the separation of roles using either identity-based or role-based operator authentication. Identity-based authentication occurs when authentication is performed via local authentication database; role-based authentication occurs when an external authentication server (e.g. RADIUS or TACACS) is used.

Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic Officer	Identity-based operator authentication	Via Console: Username and password Via SSH: Password or RSA/DSA signature verification when using public-key authentication
	Role-based authentication	Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters
User (read-write) and User (read-only)	Identity-based operator authentication	Via Console: Username and password Via SSH: Password or RSA/DSA signature verification when using public-key authentication
	Role-based authentication	Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters

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 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 7 possible attempts in a one-minute period for each getty. The best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. 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 $5.6e7/(2^{80})$ or $5.6e7/(2^{112})$, 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 $5.6e7/(2^{80})$, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Services Authorized for Roles

Role	Authorized Services
Cryptographic Officer: **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**	Configuration Mode: Allows the CO to configure the gateway. Operational Mode: Allows the user to modify the state of the gateway. (Example: shutdown, reboot) Status Checks: Allows the user to get the current status of the gateway, including logs and statistics. Zeroize: Allows the user to zeroize the configuration (all CSPs) within the module. SSH: Provides encrypted login via the SSH protocol. Console Access: Provides direct login access via the console. Self-tests: Allows the user to perform cryptographic self-tests by restarting the module. Account Management: Allows the user to create other administrative accounts. Tamper Seals: Ordering, installing, maintaining, storing and examining tamper-evident seals.
User (read-only): **Configures and monitors the gateway via the console or SSH. May not change the configuration.**	Configuration Mode: Allows the user to view the gateway configuration. Operational Mode: Allows the user to modify the state of the gateway. (Example: shutdown, reboot) Status Checks: Allows the user to get the current status of the gateway, including logs and statistics. SSH: Provides encrypted login via the SSH protocol. Console Access: Provides direct login access via the console. Self-tests: Allows the user to perform cryptographic self-tests by restarting the module.
User (read-write): **Configures and monitors the gateway via the console or SSH. May change the configuration.**	Configuration Mode: Allows the user to configure the gateway. Operational Mode: Allows the user to modify the state of the gateway. (Example: shutdown, reboot) Status Checks: Allows the user to get the current status of the gateway, including logs and statistics. Zeroize: Allows the user to zeroize the configuration (all CSPs) within the module. SSH: Provides encrypted login via the SSH protocol. Console Access: Provides direct login access via the console. Self-tests: Allows the user to perform cryptographic self-tests by restarting the module.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module
- Routing Protocols: Unauthenticated routing protocols (e.g., TCP, UDP)
- SNMP Traps (Status)

Definition of Critical Security Parameters (CSPs)

Table of CSPs

CSP	Description
SSH Private Host Key	The first time SSH is configured, the key is generated. RSA, DSA. Used to Identify the host. 1024-bit or 2048-bit length.
SSH Session Key	Session keys used with SSH, TDES (3 key), AES 128, 192, 256, HMAC-SHA-1 key (160), DH Private Key 1024
User Authentication Key	HMAC-SHA-1 Key SHA-1 hash of user password with hard-coded salt value. Used to authenticate the user to the module.
CO Authentication Key	HMAC-SHA-1 Key SHA-1 hash of user password with hard-coded salt value. Used to authenticate the CO to the module.
IPsec SAs	Session keys used within IPsec. TDES (3 key), HMAC-SHA-1
DH Private Key	Diffie-Hellman 1536-bit private key used in IKE and SSH protocol exchange
RADIUS shared secret	Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block
TACACS+ shared secret	Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block
Approved RNG State	RNG seed and seed key
SNMPv3 security key	Key used for privacy and/or authentication by SNMPv3 (AES, DES, 3DES, HMAC SHA-1)

Definition of Public Keys

Table of Public Keys

Key	Description/Usage
SSH Public Host Key	First time SSH is configured, the key is generated. RSA (1024 or 2048-bit), DSA. Identifies the host.
User Authentication Public Keys	Used to authenticate a user to the module via SSH. RSA (1024 or 2048-bit) or DSA
CO Authentication Public Keys	Used to authenticate the CO to the module via SSH. RSA (1024 or 2048-bit) or DSA
JuniperRootCA	RSA 2048-bit X.509 certificate Used to verify the integrity and authenticity of the firmware.
PackageCA	RSA 2048-bit X.509 certificate Used to verify the integrity and authenticity of the firmware..
DH Public Keys	Used within IKE and SSH 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:

CSP Access Rights within Roles & Services

Role			Service	Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete
CO	**User (RO)**	**User (RW)**		
X			Configuration Mode	All CSPs (**R, W, D**)
	X		Configuration Mode	Read access to CSPs (**R**)
		X	Configuration Mode	All CSPs except changing other account passwords (**R, W, D**)
X			Account Management	Creates or removes passwords (**W**, **D**)
X	**X**	**X**	Operational Mode	No access to CSPs
X	**X**	**X**	Status Checks	No access to CSPs
X		**X**	Zeroize	All CSPs (**D**)
X	**X**	**X**	SSH	SSH session key (**R**)
X	**X**	**X**	Console Access	CO Authentication Key, User Authentication Key (**R**)
X	**X**	**X**	Self-tests	No access to CSPs
X			Tamper Seals	No access to CSPs

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module has a limited operational environment.

8. 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 2 module.

The cryptographic module provides three distinct operator roles. These are the User (read-write) role, User (read-only) role and the Cryptographic Officer role.

The cryptographic module support both role-based and identity-based authentication mechanisms.

Authentication of identity to an authorized role is required for all services that modify, disclose, or substitute CSPs, use Approved security functions, or otherwise affect the security of the cryptographic modules.

The cryptographic module performs the following tests:

- Power up tests

- Cryptographic algorithm tests
  - Hardware (IPSec acceleration):
    - TDES KAT
    - AES KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
  - Software (general purpose):
    - TDES KAT
    - AES KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
    - DSA pairwise consistency test (sign/verify) and KAT
    - FIPS 186-2 RNG KAT
    - KDF KATs
- Firmware integrity test:
  - RSA digital signature verification (PKCS1.5, 2048-bit key, SHA-1) and SHA-1 hash verification

- Conditional 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, and on a non-Approved RNG that is used to seed the Approved RNG.
  - Bypass test is not applicable.

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.

Prior to each use, the internal RNG is tested using the continuous random number generation conditional test.

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.

9. Physical Security Policy

Physical Security Mechanisms

The modules physical embodiment is that of a multi-chip standalone device that meets Level 2 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 observation of any kind to any component contained within the physically contiguous cryptographic boundary. Tamper evident seals are used to provide evidence in

case the modules are physically tampered with. Tamper evident seals must be applied by the Cryptographic Officer to operate as FIPS 140-2 Approved modules. Seals are available for order from Juniper using part number JNPR-FIPS-TAMPER-LBLS.

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Tamper seals are applied in the same fashion regardless of the part number of the device.

Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper labels, opaque metal enclosure.	Upon receipt of the module and per security policy by the Cryptographic Officer.	Labels should be free of any tamper evidence.

Tamper Seal Placement

Seal Application Instructions

For all seal applications, the Cryptographic Officer should observe the following instructions.

- Handle the seals with care. Do not touch the adhesive side.
- All surfaces to which the seals will be applied must be clean and dry. Ensure all surfaces are clean and clear of any residue.
- Apply with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

SRX3400 (13 seals)

A tamper evident seal shall be applied to the following location (see highlighted pointers):

- Front:
    - Three overlapping seals, vertically across the each of the installed interface cards or slot cover plates on the left side of the module (see Fig. 2 below), extending on to the top and bottom of the chassis of the module.
    - Three overlapping seals, vertically across the each of the installed interface cards or slot cover plates on the right side of the module (see Fig. 2 below), extending on to the top and bottom of the chassis of the module.
- Rear:
    - Three overlapping seals, vertically across the each of the installed interface cards or slot cover plates on the left side of the module (see Fig. 3 below), extending on to the top and bottom of the chassis of the module.
    - Three overlapping seals, vertically across the each of the installed interface cards or slot cover plates on the right side of the module (see Fig. 3 below), extending on to the top and bottom of the chassis of the module.
    - One seal vertically from the top of the chassis extending on the access panel on the right side of the module.

Figure 2. SRX3400 Tamper Evident Seal Location (Top)

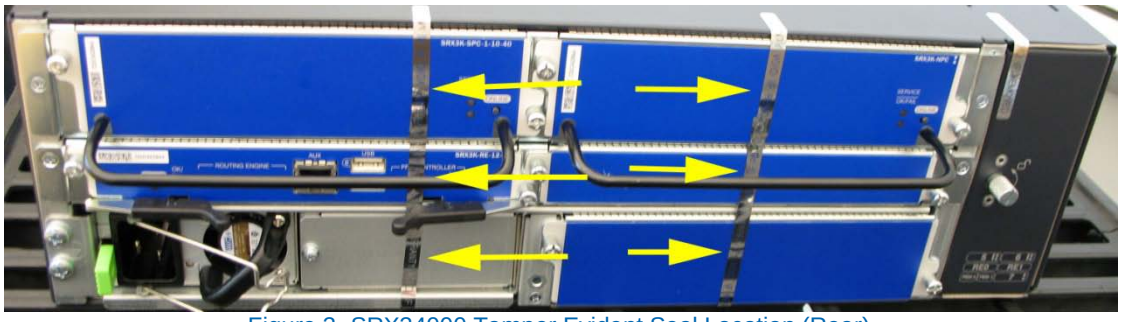

Figure 3. SRX34000 Tamper Evident Seal Location (Rear)

SRX3600 (29 seals)

Tamper evident seals shall be applied to the following locations (see highlighted pointers):

- Front:
  - One seal applied to the right side of the top cover plate, extending on to the right side of the chassis.
  - One seal applied to the left side of the top cover plate, extending on to the fan tray cover.
  - One seal applied to the right side of the Switch Fabric Board (SFB), extending on to the right side of the chassis.
  - One seal applied to the left side of the SFB, extending on to the fan tray cover.
  - For each of the three Common Form-factor Module (CFM) slots of the left side:
    - One seal applied to the left side of the cover plate or installed card, extending on to the fan tray cover.
    - One seal applied to the right side of the cover plate or installed card, extending on to the cover plate or installed card to the right.
  - For each of the three CFM slots on the right side:
    - One seal applied to the right side of the cover plate or installed card, extending on to the right side of the chassis.
- Rear:
  - One seal applied to each of the four installed power supplies or cover plates, extending on to the top of the chassis.
  - For each of the three slots of the left side:

- One seal applied to the left side of the cover plate or installed card, extending on to the left side of the chassis.
- One seal applied to the right side of the cover plate or installed card, extending on to the cover plate or installed card to the right.

- For each of the three slots on the right side:
  - One seal applied to the right side of the cover plate or installed card, extending on to the fan tray cover plate.
- One seal applied to the left side of the routing engine (RE) installed in the bottom left slot, extending on to the left side of the chassis.
- One seal applied to the right side of the RE, extending on to the cover plate or installed card to the right.
- One seal applied to the cover plate or installed cared to the right of the routing engine, extending on to the fan tray cover plate.

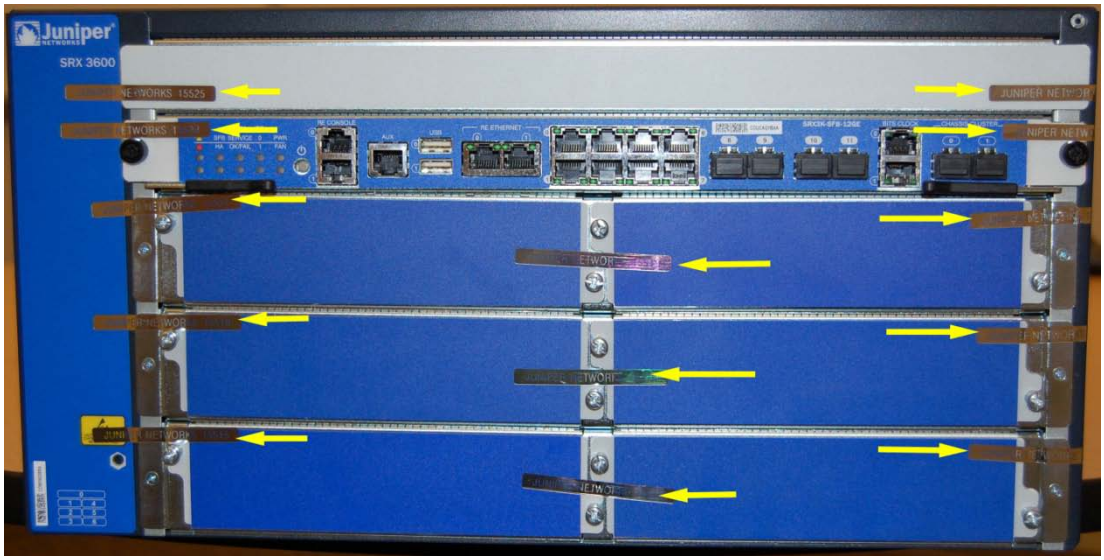

Figure 4. SRX3600 Tamper Evident Seal Location (Front)

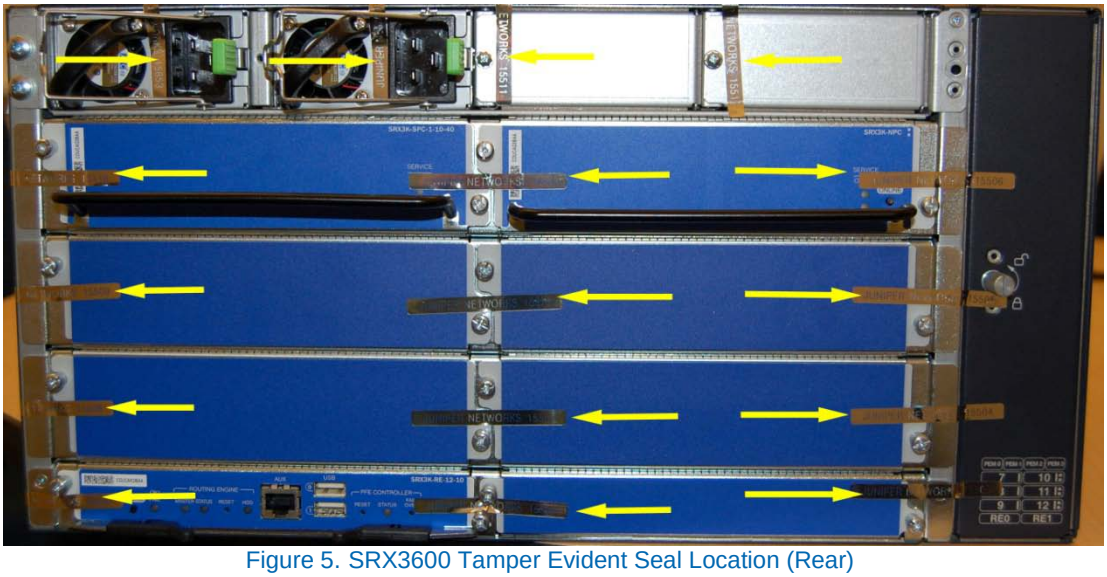

Figure 5. SRX3600 Tamper Evident Seal Location (Rear)

10. Cryptographic Algorithm Validation

Cryptographic Algorithm Validation Certificates

Algorithm	Software (General purpose)	Hardware (IPSec)
AES-CBC 128/192/256	1575	1577
3DES-CBC	1032	1033
SHA-1, SHA-256	1395	1396
HMAC SHA-1, HMAC SHA-256	922	923
FIPS 186-2 RNG	849	N/A
DSA 1024	486	N/A
RSA 1024/2048	768	N/A

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks that are outside the scope of FIPS 140-2.

Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

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
IKE	Internet Key Exchange Protocol
IPsec	Internet Protocol Security
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.
SA	Security Association
SHA-1	Secure Hash Algorithms
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TDES	Triple - Data Encryption Standard
UDP	User Datagram Protocol

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.