Juniper Networks SRX5400, SRX5600, and SRX5800 Services Gateways

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.3

Date: August 25, 2016

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

Table of Contents

1 Introduction 4

1.1 Hardware and Physical Cryptographic Boundary 6
1.2 Mode of Operation 11
1.3 Firmware Load 12
1.4 Zeroization 13

2 Cryptographic Functionality 14

2.1 Disallowed Algorithms 16
2.2 Critical Security Parameters 17

3 Roles, Authentication and Services 19

3.1 Roles and Authentication of Operators to Roles 19
3.2 Authentication Methods 19
3.3 Services 19

4 Self-tests 20

5 Physical Security Policy 24

5.1 General Tamper Seal Placement and Application Instructions 24
5.2 SRX5400 (13 seals) 24
5.3 SRX5600 (17 seals) 25
5.4 SRX5800 (24 seals) 27

6 Security Rules and Guidance 29

7 References and Definitions 30

List of Tables

Table 1 – Cryptographic Module Configurations 4
Table 2 - Security Level of Security Requirements 5
Table 3 - Ports and Interfaces 11
Table 4 - Approved and CAVP Validated Cryptographic Functions 14
Table 5 - Non-Approved but Allowed Cryptographic Functions 15
Table 6 - Protocols Allowed in FIPS Mode 15
Table 7 - Critical Security Parameters (CSPs) 17
Table 8 - Public Keys 17
Table 9 - Authenticated Services 19
Table 10 - Unauthenticated traffic 20
Table 11 - CSP Access Rights within Services 20
Table 12 – Physical Security Inspection Guidelines 24
Table 13 – References 30
Table 14 – Acronyms and Definitions 30
Table 15 – Datasheets 31

List of Figures

Figure 1 – SRX5400 Front View 6
Figure 2 – SRX5400 Bottom View 7
Figure 3 – SRX5600 Profile View 7
Figure 4 – SRX5600 Rear View 8
Figure 5 – SRX5600 Left View 8
Figure 6 – SRX5800 Top View 9
Figure 7 – SRX5800 Rear View 10
Figure 8 – SRX5800 Left View 10
Figure 9 - SRX5400- Tamper-Evident Seal Locations on Front- Six Seals 25
Figure 10 - SRX5400- Tamper-Evident Seal Locations on Rear- Seven Seals 25
Figure 11 - SRX5600- Tamper-Evident Seal Locations on Front-11 Seals 26
Figure 12 - SRX5600- Tamper-Evident Seal Locations on Rear- Seven Seals 26
Figure 13 - SRX5800- Tamper-Evident Seal Locations on Front- 19 Seals 27
Figure 14 - SRX5800- Tamper-Evident Seal Locations on Rear- Five Seals 28

1 Introduction

The Juniper Networks SRX Series Services Gateways are a series of secure routers that provide essential capabilities to connect, secure, and manage work force locations sized from handfuls to hundreds of users. By consolidating fast, highly available switching, routing, security, and applications capabilities in a single device, enterprises can economically deliver new services, safe connectivity, and a satisfying end user experience. All models run Juniper's JUNOS firmware – in this case, a specific FIPS-compliant version called JUNOS-FIPS, version 12.1X46-D40. The firmware image is junos-srx5000-12.1X46-D40.4-fips.tgz and the firmware Status service identifies itself as in the "Junos 12.1X46-D40.4 (FIPS edition)".

This Security Policy covers the SRX5400, SRX5600, and SRX5800 models. They are meant for service providers, large enterprise networks, and public-sector networks.

The cryptographic modules are defined as multiple-chip standalone modules that execute JUNOS-FIPS firmware on any of the Juniper Networks SRX-Series gateways listed in the table below.

Table 1 – Cryptographic Module Configurations

Model	Hardware Versions	Firmware	Distinguishing Features
SRX5400	SRX5400B2-AC SRX5400B2-DC SRX5400BB-AC SRX5400BB-DC with SRX5K-SPC-2-10-40 SRX5K-SPC-4-15-320	JUNOS-FIPS 12.1X46-D40	2 SPC slots; 2 IOC slots
SRX5600	SRX5600BASE-AC SRX5600BASE-DC with SRX5K-SPC-2-10-40 SRX5K-SPC-4-15-320	JUNOS-FIPS 12.1X46-D40	8 slots, with a maximum of 5 SPCs and 5 IOCs
SRX5800	SRX5800BASE-AC SRX5800BASE-DC with SRX5K-SPC-2-10-40 SRX5K-SPC-4-15-320	JUNOS-FIPS 12.1X46-D40	14 slots with a maximum of 11 SPCs and 11 IOCs
All	JNPR-FIPS-TAMPER-LBLS		Tamper-Evident Seals

The modules are designed to meet FIPS 140-2 Level 2 overall:

Table 2 - Security Level of Security Requirements

Area	Description	Level
1	Module Specification	2
2	Ports and Interfaces	2
3	Roles and Services	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Key Management	2
8	EMI/EMC	2
9	Self-test	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	2

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 are out of the scope of this validation and require a separate FIPS 140-2 validation.

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

1.1 Hardware and Physical Cryptographic Boundary

The physical forms of the module's various models are depicted in Figures 1-11 below. For all models the cryptographic boundary is defined as the outer edge of the chassis. The modules exclude the power supply and fan components from the requirements of FIPS 140-2. The power supplies and fans do not contain any security relevant components and cannot affect the security of the module. The excluded components are identified with red borders in the following figures. The module does not rely on external devices for input and output.

Figure 1 – SRX5400 Front View

Figure 2 – SRX5400 Bottom View

Figure 3 – SRX5600 Profile View

Figure 4 – SRX5600 Rear View

Figure 5 – SRX5600 Left View

Figure 6 – SRX5800 Top View

Figure 7 – SRX5800 Rear View

Figure 8 – SRX5800 Left View

Table 3 - Ports and Interfaces

Port	Description	Logical Interface Type
Ethernet	LAN Communications	Control in, Data in, Data out, Status out
Serial	Console serial port	Control in, Status out
Power	Power connector	Power
Reset	Reset	Control in
LED	Status indicator lighting	Status out
USB	Firmware load port	Control in, Data in
WAN	SHDSL, VDSL, T1, E1	Control in, Data in, Data out, Status out

1.2 Mode of Operation

Follow the instructions in Section 5 to apply the tamper seals to the module. Once the tamper seals have been applied as shown in this document, the JUNOS-FIPS firmware image is installed on the device, and integrity and self-tests have run successfully on initial power-on, the module 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.

If the module was previously in a non-Approved mode of operation, the Cryptographic Officer must zeroize the CSPs by following the instructions in Section 1.3.

Then, the CO must run the following commands to configure SSH to use FIPS approved and FIPS allowed algorithms:

```
co@fips-srx# set system services ssh hostkey-algorithm ssh-ecdsa
co@fips-srx# set system services ssh hostkey-algorithm no-ssh-rsa
co@fips-srx# set system services ssh hostkey-algorithm no-ssh-dss
co@fips-srx# set system services ssh hostkey-algorithm no-ssh-ed25519
co@fips-srx# commit
```

The CO can change the preference of SSH key exchange methods using the following command:

```
co@fips-srx# set system services ssh key-exchange <algorithm>
      <algorithm> - dh-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384,
      group-exchange-sha1, or group-exchange-sha2
```

Note: These methods are always proposed during SSH session negotiation. Explicitly specifying a method moves the algorithm up in the list of proposed algorithms during the SSH session establishment.

The CO can change the preference of SSH cipher algorithms using the following command:

```
co@fips-srx# set system services ssh ciphers <algorithm>
      <algorithm> - 3des-cbc, aes128-cbc, aes128-ctr, aes192-cbc, aes192-ctr,
      aes256-cbc, aes256-ctr
```

Note: These algorithms are always proposed during SSH session negotiation. Explicitly specifying an algorithm moves the algorithm up in the list of proposed algorithms during the SSH session establishment.

The CO can change the preference of SSH MAC algorithms or enable additional Approved algorithms using the following command:

```
co@fips-srx# set system services ssh macs <algorithm>
```

```
<algorithm> - hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512,
hmac-sha1-96-etm@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha2-256-
etm@openssh.com, hmac-sha2-512-etm@openssh.com
```

Note: hmac-sha1 and hmac-sha1-96 are always proposed during SSH session negotiation. Explicitly specifying either algorithm moves it up in the list of proposed algorithms during the SSH session establishment. Specifying any other MAC algorithm adds it to the list of algorithms proposed.

For each IPsec tunnel configured, the CO must run the following command to configure the algorithms:

```
co@fips-srx# set system security ipsec <name> authentication-algorithm
<algorithm>
```

```
<algorithm> - hmac-sha-256-128, hmac-sha1-96
```

```
co@fips-srx# set system security ipsec <name> encryption-algorithm
<algorithm>
```

```
<algorithm> - 3des-cbc, aes-128-cbc, aes-128-gcm, aes-192-cbc, aes-192-
gcm, aes-256-cbc, aes-256-gcm
```

Note: Use of AES-GCM is only FIPS approved when it is configured for use in conjunction with IKEv2.

The "show version" command will indicate if the module is operating in FIPS mode (e.g. JUNOS Software Release [12.1X46-D40] (FIPS edition)), run "`show system services ssh`", and run "`show security ipsec`" to verify that only the FIPS approved and FIPS allowed algorithms are configured for SSH and IPsec as specified above.

1.3 Firmware Load

The cryptographic module implements a firmware load service allows the loading of legacy firmware (legacy-use of digital signature verification using SHA-1 as defined by SP800-131Ar1). To comply with SP 800-131Ar1, the Crypto Officer must manually determine when a legacy firmware load is being performed and determine if the correct type of signature is being verified.

Warning: Legacy firmware might not be FIPS 140-2 Validated or meet SP 800-131Ar1 requirements. The Crypto Officer must determine whether legacy firmware meets their organization's compliance and certification requirements.

When newer firmware is being loaded, the Crypto Officer must verify the presence of an ECDSA signature for the junos and junos-boot portions of the image by running:

```
% tar ztf <firmware_image>.tgz | grep esig
```

The Crypto Officer must verify the output show presence of an esig file for both the junos and junos-boot portions of the image. For example:

```
% tar ztf junos-srx5000-12.1X46-D40.4-fips.tgz | grep esig
junos-boot-srx5000-12.1X46-D40.4-fips.esig
```

```
junos-srx5000-12.1X46-D40.4-fips.esig
```

If the two esig files are not present, the Crypto Officer must not install the image.

If the two esig files are present or the Crypto Officer is installing a legacy image, installation may continue using the following command:

```
co@fips-srx> request system software add [no-validate] [no-copy]
<firmware_image>.tgz [reboot]
```

The module will automatically verify that the image signature(s) are valid.

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 Approved mode of operation, the Cryptographic Officer must run the following commands to zeroize the Approved mode CSPs:

```
co@fips-srx> start shell

co@fips-srx% rm –P <keyfile>

      <keyfile> - each persistent private or secret key other than the SSH
      host keys and the X.509 keys for IKE.

co@fips-srx% rm –P /var/db/certs/common/certificate-request/*

co@fips-srx% exit

co@fips-srx> request system zeroize
```

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 the tables below. Table 6 summarizes the high level protocol algorithm support. The module does not implement algorithms that require vendor affirmation.

Table 4 - Approved and CAVP Validated Cryptographic Functions

Implementation	Reference	Mode	Functions	Strength	Cert
IPsec Triple-DES	SP 800-20	TCBC	Encrypt and decrypt	112 (3-Key)	2037, 2038
IPsec AES	FIPS 197 SP 800-38A SP 800-38D	CBC GCM[1]	Encrypt and decrypt	128, 192, 256	3662, 3663
IPsec SHA	FIPS 180-4		Hash generation	80 (SHA-1) 128 (SHA-256)	3080, 3081
IPsec HMAC	FIPS 198-1		HMAC Gen, Ver	128 (HMAC-SHA-1) 256 (HMAC-SHA-256)	2412, 2413
IKE Triple-DES	SP 800-20	TCBC	Encrypt and decrypt	112	2035
IKE AES	FIPS 197 SP 800-38A	CBC	Encrypt and decrypt	128, 192, 256	3656
IKE SHA	FIPS 180-4		Hash generation	80 (SHA-1) 128 (SHA-256) 192 (SHA-384)	3074
IKE HMAC	FIPS 198-1		HMAC Gen, Ver	128 (HMAC-SHA-1) 256 (HMAC-SHA-256, HMAC-SHA-384)	2406
IKE KDF	SP 800-135		IKE v1/v2 KDF	112-256	659
IKE ECDSA	FIPS 186-4		KeyGen, SigGen, SigVer	128 (P-256) 192 (P-384)	769, 770
IKE RSA	FIPS 186-4		SigGen, SigVer	112 (2048 bit)	1895, 1896
IKE DSA	FIPS 186-4		KeyGen	112 (2048 bit)	1032, 1033
SSH Triple-DES	SP 800-20	TCBC	Encrypt and decrypt	112 (3-Key)	2036
SSH AES	FIPS 197 SP 800-38A	CBC CTR	Encrypt and decrypt	128, 192, 256	3650
SSH SHA	FIPS 180-4		Hash generation	80 (SHA-1) 128 (SHA-256) 256 (SHA-512)	3068
SSH HMAC	FIPS 198-1		HMAC Gen, Ver	128 (HMAC-SHA-1) 256 (HMAC-SHA-256, HMAC-SHA-	2400

[1] The SRX5K-SPC-2-10-40 does not support GCM.

				512)	
SSH RSA	FIPS 186-4		KeyGen, SigVer	112 (2048 bit)	1885
			SigVer	128 (3072 bit)	
SSH ECDSA	FIPS 186-4		KeyGen, SigGen, SigVer	112 (P-224) 128 (P-256) 192 (P-384)	758
SSH DSA	FIPS 186-4		KeyGen	112 (2048 bit)	1022
DRBG	SP 800-90A	HMAC	Random generation	256 (HMAC-SHA-256)	981
SSH KDF	SP 800-135		SSHv2 KDF	112-256	660

Table 5 - Non-Approved but Allowed Cryptographic Functions

Algorithm	Reference
Non-SP 800-56A Compliant Diffie-Hellman	[IG] D.8 Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 192 bits of encryption strength).
Non-SP 800-56A Compliant Elliptic Curve Diffie-Hellman	[IG] D.8 EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength).
NDRNG	[IG] 7.11 Hardware Non-Deterministic RNG used to seed the FIPS Approved DRBG.
HMAC-SHA-1-96	[IG] A.8 Hash Message Authentication Code truncated to 96-bits. Allowed for use in FIPS mode.

Table 6 - Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1/v2	Oakley Group 14 (DH L = 2048 bit, N = 224 bit) Oakley Group 19 (P-256) Oakley Group 20 (P-384) Oakley Group 24 (DH L = 2048 bit, N = 224 bit)	RSA 2048 Pre-Shared Secret ECDSA P-256 ECDSA P-384	3 Key Triple-DES AES CBC 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256 HMAC-SHA-384
IPsec ESP	IKEv1 with optional: • Oakley Group 14 (DH L = 2048 bit, N = 224 bit) • Oakley Group 19 (P-256) • Oakley Group 20 (P-384) • Oakley Group 24 (DH L = 2048 bit, N = 224 bit)	IKEv1	3 Key Triple-DES AES CBC 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256-128
	IKEv2 with optional: • Oakley Group 14 (DH L = 2048 bit, N = 224 bit) • Oakley Group 19 (P-256) • Oakley Group 20 (P-384)	IKEv2	3 Key Triple-DES AES CBC 128/192/256 AES GCM 128/192/256 16	

	• Oakley Group 24 (DH L = 2048 bit, N = 224 bit)		octet ICV[2]	
SSHv2	Diffie-hellman-group-exchange-sha1 (L = 2048 bit, 3072 bit, 4096 bit, 6144 bit, 7680 bit, or 8192 bit; N = 256 bit, 320 bit, 384 bit, 512 bit, or 1024 bit) Diffie-hellman-group-exchange-sha2 (L = 2048 bit, 3072 bit, 4096 bit, 6144 bit, 7680 bit, or 8192 bit; N = 256 bit, 320 bit, 384 bit, 512 bit, or 1024 bit) Diffie-hellman-group14-sha1 (L = 2048 bit; N = 256 bit, 320 bit, 384 bit, 512 bit, or 1024 bit) ECDH-sha2-nistp256 ECDH-sha2-nistp384	ECDSA P-256	3 Key Triple-DES AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1-96 HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

These protocols have not been reviewed or tested by the CAVP and CMVP.

The IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 6 above, each column of options for a given protocol is independent, and may be used in any viable combination.

2.1 Disallowed Algorithms

These algorithms are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation. These security functions are available in the SSH connect (non-compliant) service.

- ssh-dss (DSA non-compliant)
- dh-group1-sha1 (Diffie-Hellman (non-compliant key agreement; key establishment methodology provides less than 112 bits of encryption strength)
- hmac-md5
- hmac-md5-96
- hmac-md5-96-etm@openssh.com
- hmac-md5-etm@openssh.com
- hmac-ripemd160
- hmac-ripemd160-etm@openssh.com
- umac-128-etm@openssh.com
- umac-64-etm@openssh.com
- umac-64@openssh.com
- arcfour
- arcfour128

[2] The SRX5K-SPC-2-10-40 does not support GCM.

- arcfour256
- blowfish-cbc
- cast128-cbc

2.2 Critical Security Parameters

All CSPs and public keys used by the module are described in this section.

Table 7 - 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
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256. Used to identify the host.
SSH DH	SSH Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in SSH. DH (N = 256 bit, 320 bit, 384 bit, 512 bit, or 1024 bit[3]), ECDH P-256, or ECDH P-384
SSH-SEK	SSH Session Key; Session keys used with SSH. TDES (3key), AES, HMAC.
ESP-SEK	IPSec ESP Session Keys. TDES (3 key), AES, HMAC.
IKE-PSK	Pre-Shared Key used to authenticate IKE connections.
IKE-Priv	IKE Private Key. RSA 2048, ECDSA P-256, or ECDSA P-384
IKE-SKEYID	IKE SKEYID. IKE secret used to derive IKE and IPsec ESP session keys.
IKE-SEK	IKE Session Keys. TDES (3 key), AES, HMAC.
IKE-DH-PRI	IKE Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in IKE. DH N = 224 bit, ECDH P-256, or ECDH P-384
CO-PW	ASCII Text used to authenticate the CO.
User_PW	ASCII Text used to authenticate the User.

Table 8 - Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256.
SSH-DH-PUB	Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in SSH key establishment. DH (L = 2048 bit, 3072 bit, 4096 bit, 6144 bit, 7680 bit, or 8192 bit), ECDH P-256, or ECDH P-384
IKE-PUB	IKE Public Key RSA 2048, ECDSA P-256, or ECDSA P-384
IKE-DH-PUB	Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in IKE key establishment. DH L = 2048 bit, ECDH P-256, or ECDH P-384
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

[3] SSH generates a Diffie-Hellman private key that is 2x the bit length of the longest symmetric or MAC key negotiated.

Root-CA	JuniperRootCA. RSA 2048 X.509 Certificate; Used to verify the validity of the Juniper Package-CA at software load.
RootEC CA	JuniperRootEC CA. ECDSA P-256 X.509 Certificate; Used to verify the validity of the Juniper Package CA at software load and also at runtime for integrity.
Package-CA	PackageCA. RSA 2048 X.509 Certificate; Used to verify the validity of legacy Juniper Images at software load.
PackageEC CA	PackageEC CA. ECDSA P-256 X.509 Certificate; Used to verify the validity the Juniper Image at software load and also at runtime for 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 either 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 seven (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.

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 and P-384). The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{128})$.

3.3 Services

All services implemented by the module are listed in the tables below. Table 11 lists the access to CSPs by each service.

Table 9 - Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	IPsec protected connection (ESP)	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	

SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
IPsec connect	Initiate IPsec connection (IKE)	x	
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset	x	

Table 10 - Unauthenticated traffic

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

Table 11 - CSP Access Rights within Services

Service	CSPs												
	DRBG_Seed	DRBG_State	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYI	IKE-SEK	IKE-DH-PRI	CO-PW	User-PW
Configure security	--	E	GW	--	--	--	W	GW	--	--	--	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	E	--	--	--	E	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	--	Z	Z	--	--	--	Z	Z	--	--	--	Z	Z
SSH connect	--	E	E	GE	GE	--	--	--	--	--	--	E	E
IPsec connect	--	E	--	--	--	G	E	E	G	G	G	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	GE	G	--	Z	Z	Z	--	--	Z	Z	Z	Z	Z
Local reset	GE	G	--	Z	Z	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 2.1 and the SSHv2 row of Table 6.

Table 12 - 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)	IPsec protected connection (ESP)	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
IPsec connect (non-compliant)	Initiate IPsec connection (IKE)	x	
Console access (non-compliant)	Console monitoring and control (CLI)	x	x
Remote reset (non-compliant)	Software initiated reset	x	

Table 13 - 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. If one of the KATs fails, the module enters the Critical Failure error state.

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

- Firmware Integrity check using ECDSA P-256 with SHA-256
- QuickSec JSF Hardware Accelerated KATs
    - AES-CBC Encrypt KAT
    - ASE-CBC Decrypt KAT
    - AES-GCM Encrypt KAT (Note: Except on SRX5K-SPC-2-10-40 which does not support AES GCM)
    - ASE-GCM Decrypt KAT (Note: Except on SRX5K-SPC-2-10-40 which does not support AES GCM)
    - RSA 2048 w/ SHA-256 Sign KAT
    - RSA 2448 w/ SHA-256 Verify KAT
    - ECDSA P-256 w/ SHA-256 Sign/Verify PCT
- QuickSec Hardware Accelerated KATs
    - Triple-DES-CBC Encrypt KAT
    - Triple-DES-CBC Decrypt KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
- OpenSSL KATs
    - 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.
    - RSA 2048 w/ SHA-256 Sign KAT
    - RSA 2048 w/ SHA-256 Verify KAT
    - Triple-DES-CBC Encrypt KAT
    - Triple-DES-CBC Decrypt KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - SHA-256 KAT
    - AES-CBC Encrypt KAT
    - ASE-CBC Decrypt KAT
    - KDF-SSH KAT
- QuickSec KATs
    - Triple-DES-CBC Encrypt KAT
    - Triple-DES-CBC Decrypt KAT

  - HMAC-SHA1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - AES-CBC Encrypt KAT
  - ASE-CBC Decrypt KAT
  - KDF-IKE-V1 KAT
  - KDF-IKE-V2 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 DSA, ECDSA, and RSA key pairs.
- Firmware Load Test (ECDSA or RSA signature verification)

5 Physical Security Policy

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 for any sort of observation of any component contained within the cryptographic boundary. Tamper-evident seals allow the operator to tell if the enclosure has been breached. These seals are not factory-installed and must be applied by the Cryptographic Officer. (Seals are available for order from Juniper using part number JNPR-FIPS-TAMPER-LBLS.) The tamper-evident seals shall be installed for the module to operate in a FIPS mode of operation.

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.

Table 14 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper seals, opaque metal enclosure.	Once per month by the Cryptographic Officer.	Seals should be free of any tamper evidence.

5.1 General Tamper Seal Placement and 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.
- Before applying a seal, ensure the location of application is clean, dry, and clear of any residue.
- Place the seal on the module, applying firm pressure across it to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

5.2 SRX5400 (13 seals)

Tamper-evident seals shall be applied to the following locations:

- Front Pane:
  - Two seals, vertical, connected to the topmost (non-honeycomb) sub-pane. They extend to the thin pane below and the honeycomb panel above.
  - One seal, vertical, across the thin pane. Extends to the blank pane below and the sub-pane above.
  - Three seals, vertical, one on each “long” horizontal sub-pane. Each attaches to the sub-pane above and the one below (or the chassis, if it’s the bottommost sub-pane). Ensure one of the seals extends to the left sub-pane below the thin sub-pane.
- Back Pane:
  - Four seals, vertical: one on each of the top four sub-panes, extending to the large chassis plate below.
  - One seal, vertical: on the horizontal screwed-in plate resting on the large central chassis. Should extend to the chassis in both directions.
  - Two seals, horizontal: placed on the low side sub-panes, extending to the large central chassis area and wrapping around to the neighboring side panes.

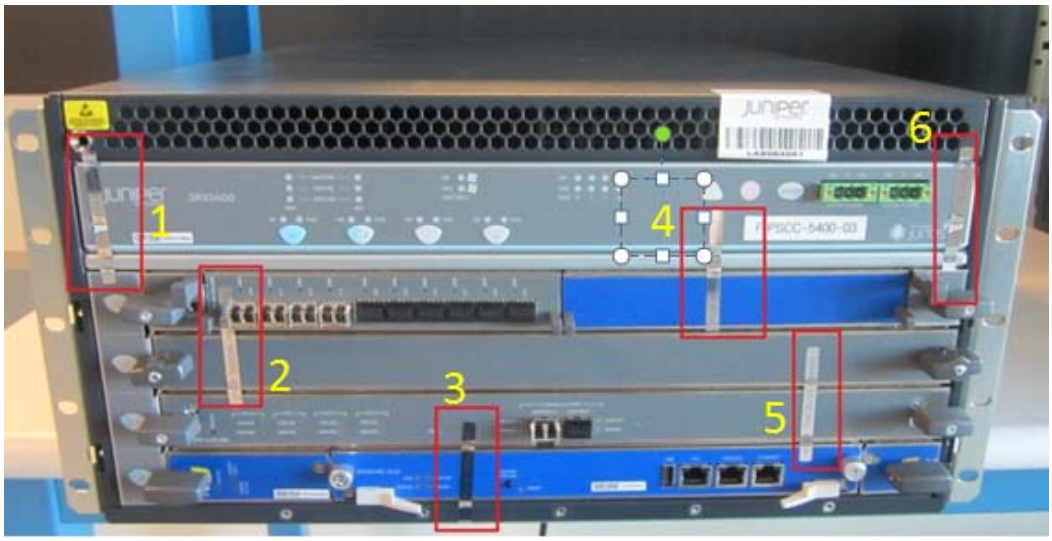

Figure 9 - SRX5400- Tamper-Evident Seal Locations on Front- Six Seals

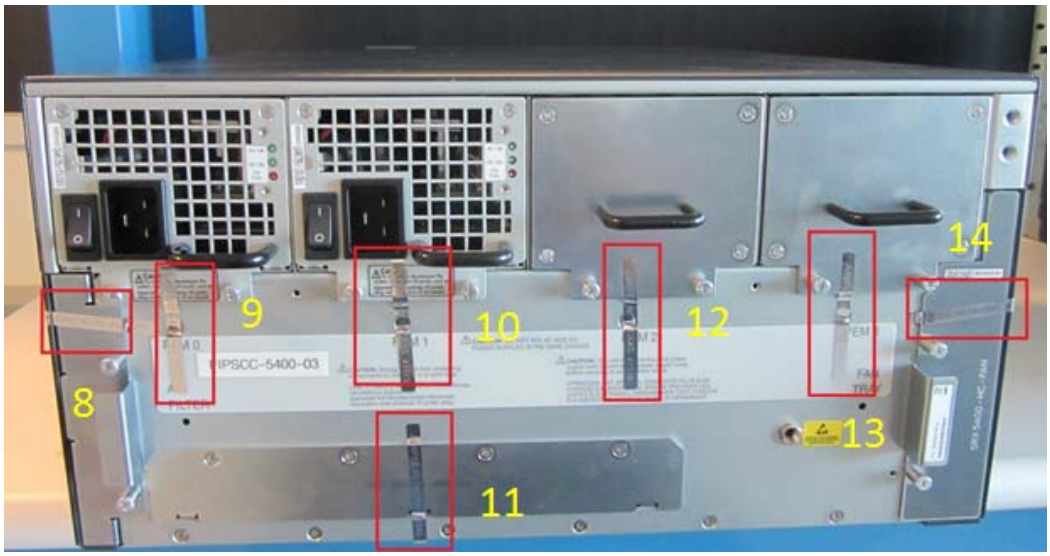

Figure 10 - SRX5400- Tamper-Evident Seal Locations on Rear- Seven Seals

5.3 SRX5600 (17 seals)

Tamper-evident seals must be applied to the following locations:

- Front Pane:
  - Eleven seals, vertical: one for each horizontal sub-pane (excluding the honeycomb plate on the top and the thin sub-pane a little below), a second for the top (non-honeycomb) sub-pane, and an extra for the bottom. The seals should attach to vertically adjacent sub-panes. The extra on the bottom attaches to the lowermost sub-pane and wraps around attaching to the bottom pane. It should be ensured that one of the seals spans across the thin plate with ample extra distance on each side.
- Back Pane:

- Four seals, vertical: one on each of the upper four sub-panes, attaching to the large plate below.
- Two seals, horizontal: one on each of the vertical side sub-panes, extending to both the large central plate and the side panes.

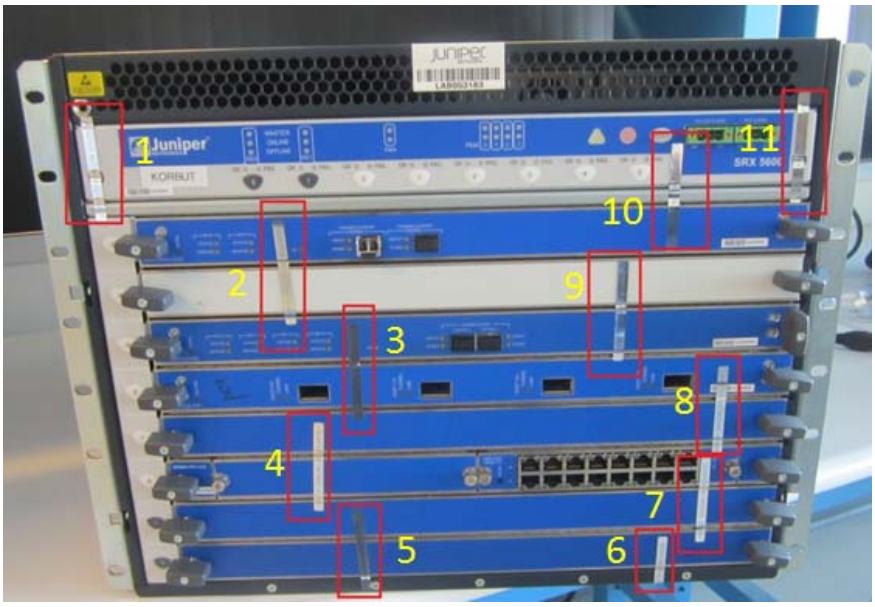

Figure 11 - SRX5600- Tamper-Evident Seal Locations on Front-11 Seals

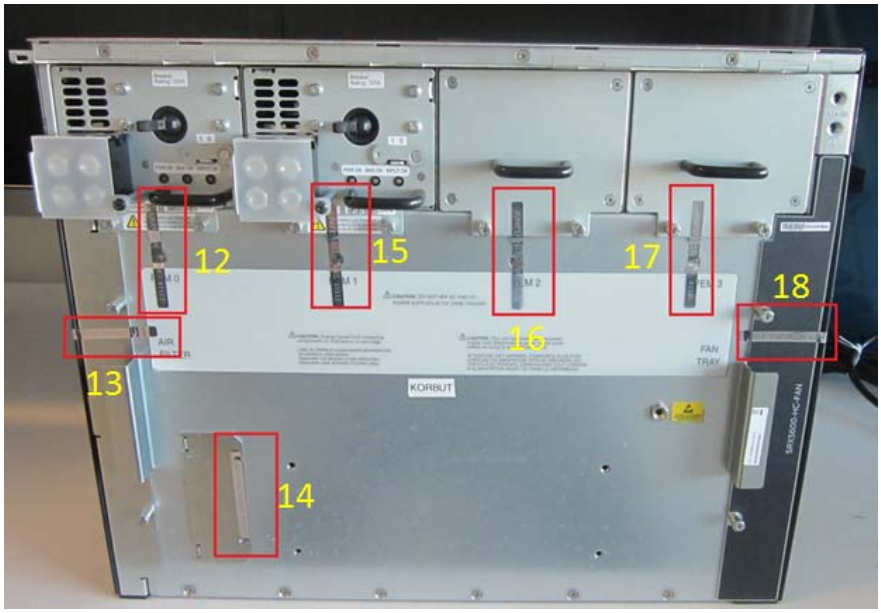

Figure 12 - SRX5600- Tamper-Evident Seal Locations on Rear- Seven Seals

5.4 SRX5800 (24 seals)

Tamper-evident seals shall be applied to the following locations:

- Front Pane:
  - Fourteen (14) seals, horizontal: one on each of the long vertical sub-panes, extending to the neighboring two. If on an end sub-pane, seal should wrap around to the side.
  - Three seals, vertical: One over each of the thin panes – two near the bottom, one near the top of the lower half.
  - Two seals, vertical: both on the console area at the top of the module, one extending to the top and the other extending to the chassis area below.
- Back Pane:
  - Five seals, horizontal: Three spanning the gaps between the vertical sub-panels, and then two more, one each on the far edges of the left and right panels. (These last two should wrap around to the sides.)

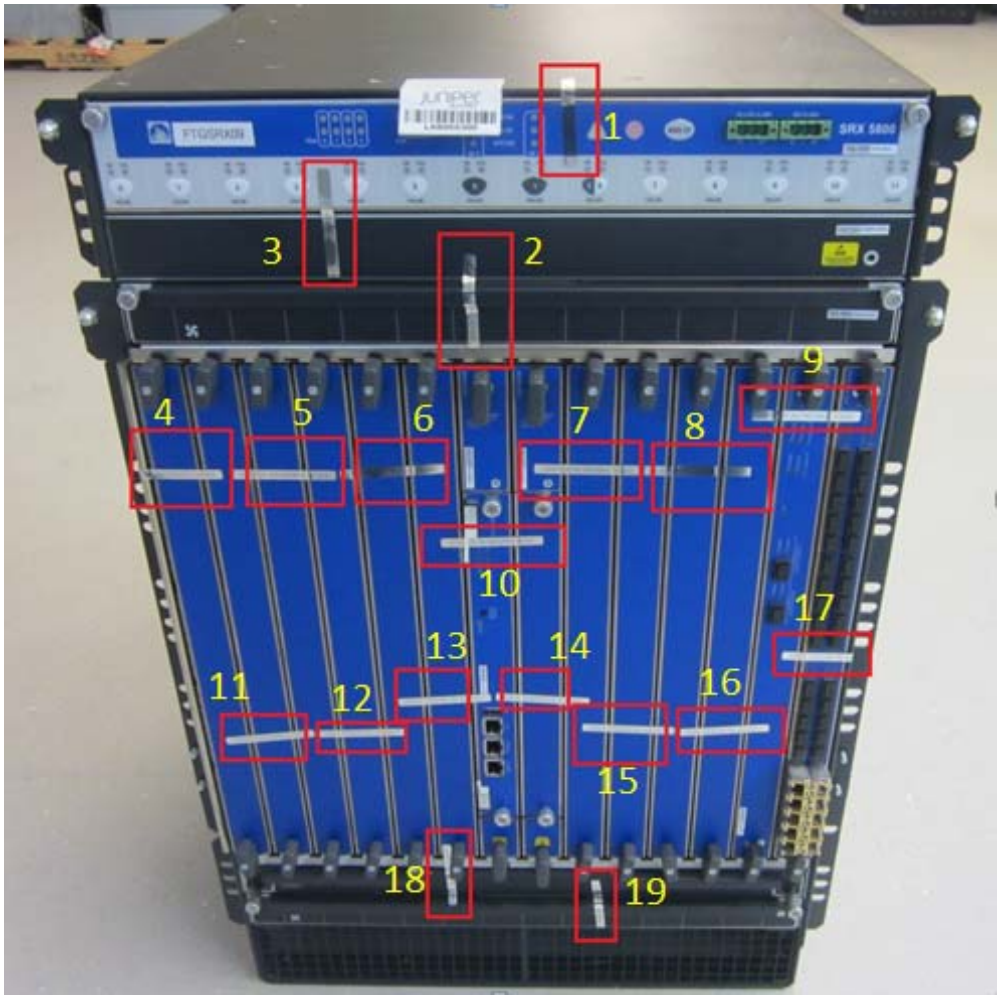

Figure 13 - SRX5800- Tamper-Evident Seal Locations on Front- 19 Seals

Figure 14 - SRX5800- Tamper-Evident Seal Locations on Rear- Five Seals

6 Security Rules and Guidance

The module design corresponds to the security rules below. The term *must* 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 to independent internal actions to be performed prior to outputing plaintext CSPs.
11. The cryptographic officer must determine whether firmware being loaded is a legacy use of the firmware load service.
12. The cryptographic officer must retain control of the module while zeroization is in process.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – 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*

Table 16 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
ICV	Integrity Check Value (i.e. Tag)
IKE	Internet Key Exchange Protocol
IOC	Input/Output Card
IPsec	Internet Protocol Security
MD5	Message Digest 5
NPC	Network Processing Card
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SHA	Secure Hash Algorithms
SPC	Services Processing Card
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 17 – Datasheets

Model	Title	URL
SRX5400 SRX5600 SRX5800	SRX Series Service Gateways for service provider, large enterprise, and public sector networks.	http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000254-en.pdf