Juniper Networks SRX5400, SRX5600, and SRX5800 Services Gateways

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.10

Date: June 09, 2017

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 Zeroization 12

2 Cryptographic Functionality 13

2.1 Approved Algorithms 13
2.2 Allowed Algorithms 14
2.3 Allowed Protocols 15
2.4 Disallowed Algorithms 16
2.5 Critical Security Parameters 16

3 Roles, Authentication and Services 18

3.1 Roles and Authentication of Operators to Roles 18
3.2 Authentication Methods 18
3.3 Services 18
3.4 Non-Approved Services 20

4 Self-tests 21

5 Physical Security Policy 23

5.1 General Tamper Seal Placement and Application Instructions 23
5.2 SRX5400 (13 seals) 23
5.3 SRX5600 (18 seals) 24
5.4 SRX5800 (24 seals) 26

6 Security Rules and Guidance 28

7 References and Definitions 29

List of Tables

Table 1 – Cryptographic Module Hardware Configurations 4
Table 2 - Security Level of Security Requirements 5
Table 3 - Ports and Interfaces 11
Table 4 - Data Plane Approved Cryptographic Functions 13
Table 5 - Control Plane Authentec Approved Cryptographic Functions 13
Table 6 - OpenSSL Approved Cryptographic Functions 14
Table 7 – Allowed Cryptographic Functions 14
Table 8 – Protocols Allowed in FIPS Mode 15
Table 9 – Critical Security Parameters (CSPs) 16
Table 10 – Public Keys 17
Table 11 – Authenticated Services 18
Table 12 – Unauthenticated traffic 19

Table 13 – CSP Access Rights within Services 19
Table 14 – Authenticated Services 20
Table 15 – Unauthenticated traffic 20
Table 16 – Physical Security Inspection Guidelines 23
Table 17 – References 29
Table 18 – Acronyms and Definitions 30
Table 19 – Datasheets 30

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 24
Figure 10 - SRX5400- Tamper-Evident Seal Locations on Rear- Seven Seals 24
Figure 11 - SRX5600- Tamper-Evident Seal Locations on Front- 11 Seals 25
Figure 12 - SRX5600- Tamper-Evident Seal Locations on Rear- Seven Seals 25
Figure 13 - SRX5800- Tamper-Evident Seal Locations on Front- 19 Seals 26
Figure 14 - SRX5800- Tamper-Evident Seal Locations on Rear- Five Seals 27

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 12.3X48-D30. The firmware image is junos-srx5000-12.3X48-D30.12-fips.tgz and the firmware Status service identifies itself as in the "Junos 12.3X48-D30.12 (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 Hardware Configurations

Chassis PN	RE PN	SCB PN	SPC PN	IOC PN	Power PN	Tamper Seals
SRX5400	SRX5K-RE-13-20	SRX5K-SCB	SRX5K-SPC-4-15-320	SRX5K-40GE-SFP	with AC HC or DC	JNPR-FIPS-TAMPER-LBLS
	SRX5K-RE-1800X4	SRX5K-SCBE	SRX5K-SPC-4-15-320	SRX-MIC-10XG-SFPP		
SRX5600	SRX5K-RE-13-20	SRX5K-SCB	SRX5K-SPC-2-10-40	SRX5K-40GE-SFP		
	SRX5K-RE-1800X4	SRX5K-SCBE	SRX5K-SPC-4-15-320	SRX-MIC-10XG-SFPP		
SRX5800	SRX5K-RE-13-20	SRX5K-SCB	SRX5K-SPC-2-10-40	SRX-MIC-10XG-SFPP		
	SRX5K-RE-1800X4	SRX5K-SCBE	SRX5K-SPC-4-15-320	SRX-MIC-10XG-SFPP		

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

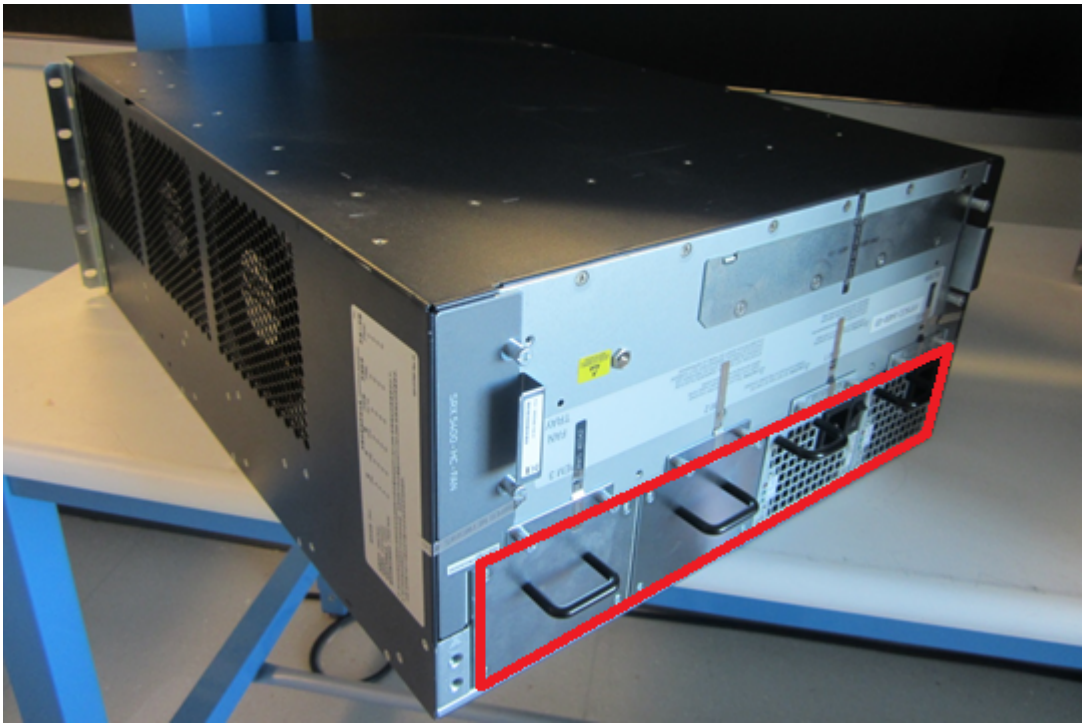

Figure 2 – SRX5400 Bottom View

Figure 3 – SRX5600 Profile View

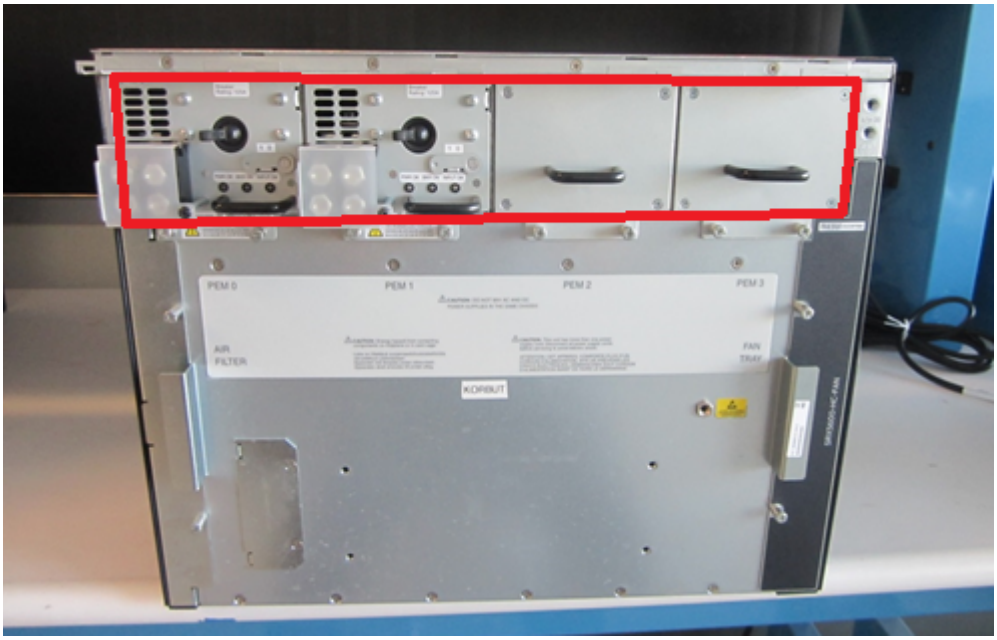

Figure 4 – SRX5600 Rear View

Figure 5 – SRX5600 Left View

Figure 6 – SRX5800 Top View

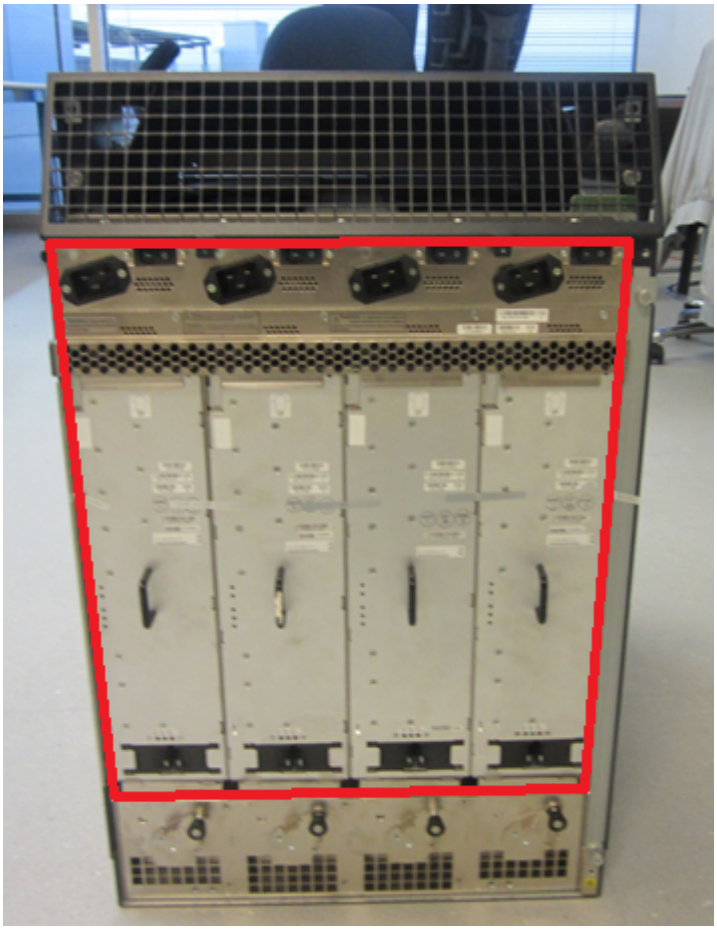

Figure 7 – SRX5800 Rear View

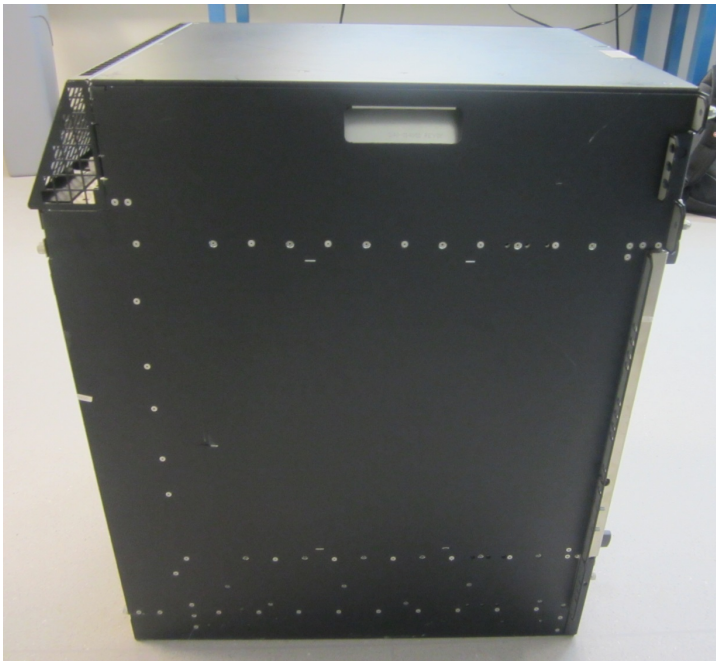

Figure 8 – SRX5800 Left View

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 in
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
```

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
```

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
```

When AES GCM is configured as the encryption-algorithm for IKE or IPsec , the CO must run the following command to configure the algorithms:

```
co@fips-srx# set security ike gateway <name> version v2-only

      <name> - the user configured name for the IKE gateway

co@fips-srx# commit
```

The "show version" command will indicate if the module is operating in FIPS mode (e.g. JUNOS Software Release [12.3X48-D30] (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 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

2.1 Approved Algorithms

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the Tables 4 to 6 below. Table 8 summarizes the high level protocol algorithm support. The module does not implement algorithms that require vendor affirmation.

Table 4 - Data Plane Approved Cryptographic Functions

CAVP Cert.	Algorithm	Mode	Description	Functions
4070, 4329	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
4070	AES [197]	GCM [38D][1]	Key Sizes: 128, 192, 256	Encrypt, Decrypt, AEAD
2657, 2867	HMAC [198]	SHA-1	λ = 96	Message Authentication
		SHA-256	λ = 128	
3353, 3571	SHS [180]	SHA-1 SHA-256		Message Digest Generation
2221, 2222	Triple-DES [67]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Table 5 - Control Plane Authentec Approved Cryptographic Functions

Cert	Algorithm	Mode	Description	Functions
4054, 4055	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
4055	AES [197]	GCM [38D][1]	Key Sizes: 128, 256	Encrypt, Decrypt, AEAD
926	CVL	IKEv1 [135]	SHA 1, 256, 384	Key Derivation
		IKEv2 [135]	SHA 1, 256, 384	
1103, 1104	DSA [186]		(L = 2048, N = 224) (L = 2048, N = 256)	KeyGen
916, 917	ECDSA[186]		P-256 (SHA 256) P-384 (SHA {256}, 384)	KeyGen, SigGen, SigVer
2646, 2647	HMAC [198]	SHA-1	λ = 96, 160	Message Authentication, KDF Primitive
		SHA-256	λ = 128, 256	
		SHA-384	λ = 192, 384	
N/A	KTS [38F]	(AES Cert. #4054 and HMAC Cert. #2646), (AES Cert. #4055 and HMAC Cert. #2647), (Triple-DES Cert. #2224 and HMAC Cert. #2646)		Key Wrapping/Unwrapping
2201, 2202	RSA [186]	PKCS1_V1_5	n=2048 (SHA 256) {n=3072 (SHA 256)}	SigGen, SigVer

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

3341, 3342	SHS [180]	SHA-1 SHA-256 SHA-384		Message Digest Generation
2224	Triple-DES [67]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Table 6 - OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Mode	Description	Functions
4056	AES [197]	CBC [38A] CTR [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
880	CVL	SSH [135]	SHA 1, 256, 384	Key Derivation
1216, 1399, 1401	DRBG [90A]	HMAC	SHA-256	Random Bit Generation
1096	DSA [186]		{(2048, 224)} (2048, 256)	KeyGen
909	ECDSA [186]		{P-224 (SHA 256)} P-256 (SHA 256) {P-384 (SHA 256)}	SigGen
			{P-224 (SHA 256)} P-256 (SHA 256) P-384 (SHA {256}, 384)	KeyGen, SigVer
2648	HMAC [198]	SHA-1	λ = 96, 160	Message Authentication DRBG Primitive
		SHA-256	λ = 256	
		SHA-512	λ = 512	
N/A	KTS [38F]	(AES Cert. #4056 and HMAC Cert. #2648), (Triple-DES Cert. #2223 and HMAC Cert. #2648)		Key Wrapping/Unwrapping
2087	RSA [186]		n=2048 (SHA 256) {n=3072 (SHA 256)}	KeyGen, SigGen, SigVer
	RSA [186-2]		{n=4096 (SHA 256)}	{SigGen}
3343	SHS [180]	SHA-1 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
		SHA-512		Message Digest Generation
2223	Triple-DES [67]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

2.2 Allowed Algorithms

Table 7 – Allowed Cryptographic Functions

Algorithm	Caveat	Use

Diffie-Hellman [IG] D.8	Provides between 112 and 192 bits of encryption strength.	key agreement; key establishment
Elliptic Curve Diffie-Hellman [IG] D.8	Provides 128 or 192 bits of encryption strength.	key agreement; key establishment
NDRNG		Seeding the DBRG

2.3 Allowed Protocols

Table 8 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1	Diffie-Hellman (L = 2048, N = 224, 256) EC Diffie-Hellman P-256, P-384	RSA 2048 Pre-Shared Secret ECDSA P-256 ECDSA P-384	Triple-DES CBC AES CBC 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256-128 HMAC-SHA-384-192
IKEv2[2]	Diffie-Hellman (L = 2048, N = 224, 256) EC Diffie-Hellman P-256, P-384	RSA 2048 Pre-Shared Secret ECDSA P-256 ECDSA P-384	Triple-DES CBC AES CBC 128/192/256 AES GCM[3] 128/256	HMAC-SHA-1-96 HMAC-SHA-256-128 HMAC-SHA-384-192
IPsec ESP	IKEv1 with optional: • Diffie-Hellman (L = 2048, N = 224, 256) • EC Diffie-Hellman P-256, P-384	IKEv1	3 Key Triple-DES CBC AES CBC 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256-128
	IKEv2 with optional: • Diffie-Hellman (L = 2048, N = 224), (2048, 256) • EC Diffie-Hellman P-256, P-384	IKEv2	3 Key Triple-DES CBC AES CBC 128/192/256 AES GCM[4] 128/192/256	
SSHv2	Diffie-Hellman (L = 2048, 3072, 4096, 6144, 7680, 8192; N = 256, 320, 384, 512, 1024) EC Diffie-Hellman P-256, P-384	ECDSA P-256	Triple-DES CBC AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1-96 HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

[2] IKEv2 generates the SKEYSEED according to RFC7296.

[3] The GCM IV is generated according to RFC5282.

[4] The GCM IV is generated according to RFC4106.

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

The IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 8 above, each column of options for a given protocol is independent, and may be used in any viable combination. These security functions are also available in the SSH connect (non-compliant) service.

2.4 Disallowed Algorithms

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

- ARCFOUR
- Blowfish
- CAST
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC

2.5 Critical Security Parameters

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

Table 9 – 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. Diffie-Hellman (N = 256 bit, 320 bit, 384 bit, 512 bit, or 1024 bit[5]), EC Diffie-Hellman P-256, or EC Diffie-Hellman P-384
SSH-SEK	SSH Session Key; Session keys used with SSH. Triple-DES (3key), AES, HMAC.
ESP-SEK	IPSec ESP Session Keys. Triple-DES (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. Triple-DES (3 key), AES, HMAC.
IKE-DH-PRI	IKE Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in IKE. Diffie-Hellman N = 224 bit, EC Diffie-Hellman P-256, or EC Diffie-Hellman P-384

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

CO-PW	ASCII Text used to authenticate the CO.
User-PW	ASCII Text used to authenticate the User.

Table 10 – 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. Diffie-Hellman (L = 2048 bit, 3072 bit, 4096 bit, 6144 bit, 7680 bit, or 8192 bit), EC Diffie-Hellman P-256, or EC Diffie-Hellman 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. Diffie-Hellman L = 2048 bit, EC Diffie-Hellman P-256, or EC Diffie-Hellman P-384
Auth-UPub	SSH User Authentication Public Keys. Used to authenticate users to the module. ECDSA P-256 or P-384
Auth-COPub	SSH CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P-256 or P-384
Root CA	Juniper Root CA. ECDSA P-256 or P-384 X.509 Certificate; Used to verify the validity of the Juniper Package CA at software load.
Package CA	Package CA. ECDSA P-256 X.509 Certificate; Used to verify the validity of Juniper Images at software load and also at runtime integrity.

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Cryptographic Officer (CO) and User. The module supports concurrent operators, but does not support a maintenance role and/or bypass capability. The module enforces the separation of roles using 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 13 – lists the access to CSPs by each service.

Table 11 – 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 12 – Unauthenticated traffic

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

Table 13 – CSP Access Rights within Services

	CSPs												
Service	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	--	--	--	RW	RGW	--	--	--	RW	RW
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	GEZ	G	--	Z	Z	Z	--	--	Z	Z	Z	Z	Z
Local reset	GEZ	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 2.4 and the SSHv2 row of Table 8.

Table 14 – 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 15 – 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
- **Data Plane KATs**
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - AES-GCM (128/192/256) Encrypt KAT (Note: Except on SRX5K-SPC-2-10-40, which does not support AES GCM)
  - ASE-GCM (128/192/256) Decrypt KAT (Note: Except on SRX5K-SPC-2-10-40, which does not support AES GCM)
- **Control Plane Authentec KATs**
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - ECDSA P-256 w/ SHA-256 Sign/Verify PCT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - AES-GCM (128/256) Encrypt KAT
  - AES-GCM (128/256) Decrypt KAT
  - KDF-IKE-V1 KAT
  - KDF-IKE-V2 KAT
- **OpenSSL KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate.
  - ECDSA P-256 Sign/Verify PCT
  - EC Diffie-Hellman 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-512 KAT
  - SHA (256/384/512) KAT
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - KDF-SSH KAT
- Critical Function Test
  - The cryptographic module performs a verification of a limited operational environment and verification of optional non-critical packages.

The module also performs the following conditional self-tests:

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

5 Physical Security Policy

The module's physical embodiment is that of a multi-chip standalone device that meets Level 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 16 – 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.

If the Cryptographic Officer observes tamper evidence, it shall be assumed that the device has been compromised. The Cryptographic Officer shall retain control of the module and perform Zeroization of the module's CSPs by following the steps in Section 1.3 of the Security Policy.

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.

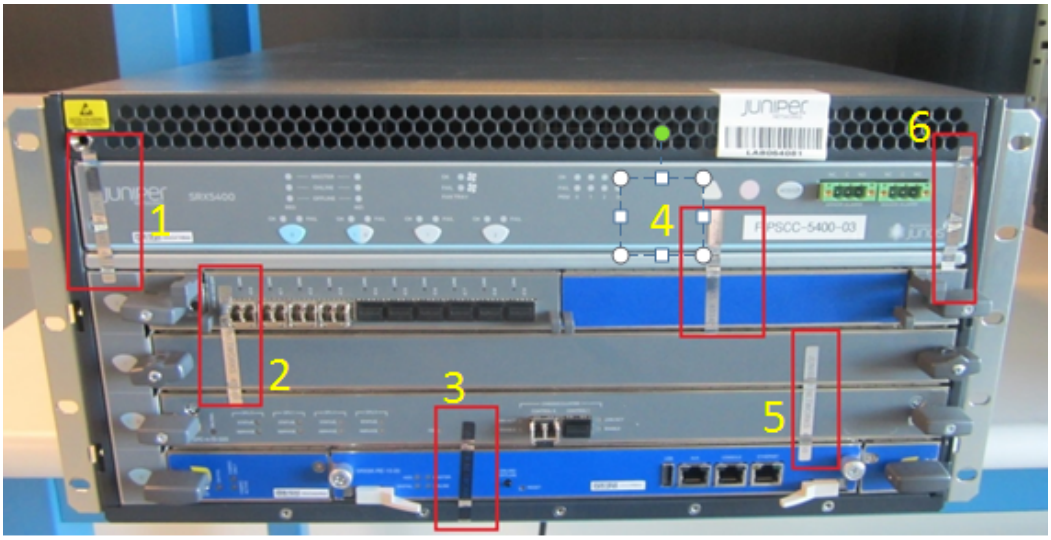

Figure 9 - SRX5400- Tamper-Evident Seal Locations on Front- Six Seals

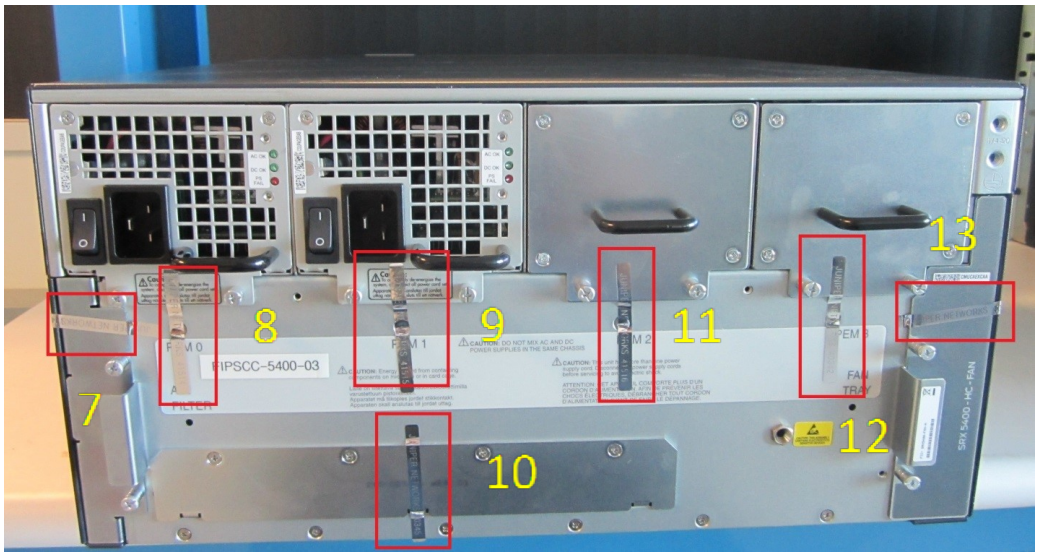

Figure 10 - SRX5400- Tamper-Evident Seal Locations on Rear- Seven Seals

5.3 SRX5600 (18 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:
  - Five 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.

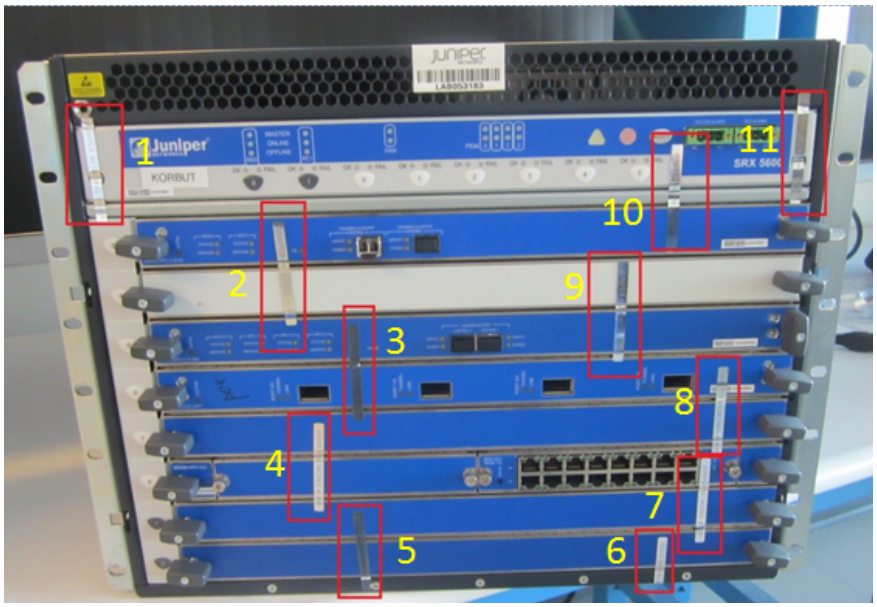

Figure 11 - SRX5600- Tamper-Evident Seal Locations on Front- 11 Seals

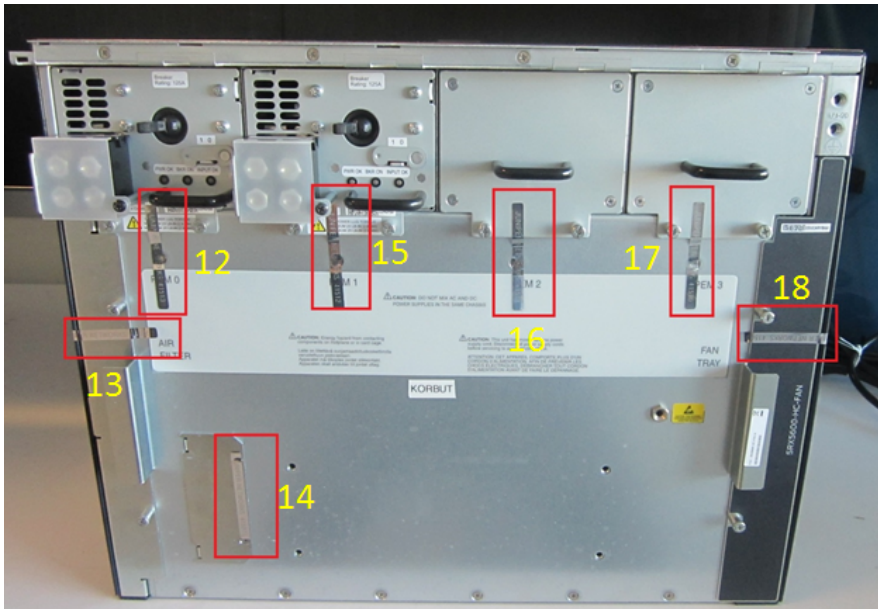

Figure 12 - SRX5600- Tamper-Evident Seal Locations on Rear- Seven Seals

5.4 SRX5800 (24 seals)

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

- Front Pane:
  - Fourteen 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.)

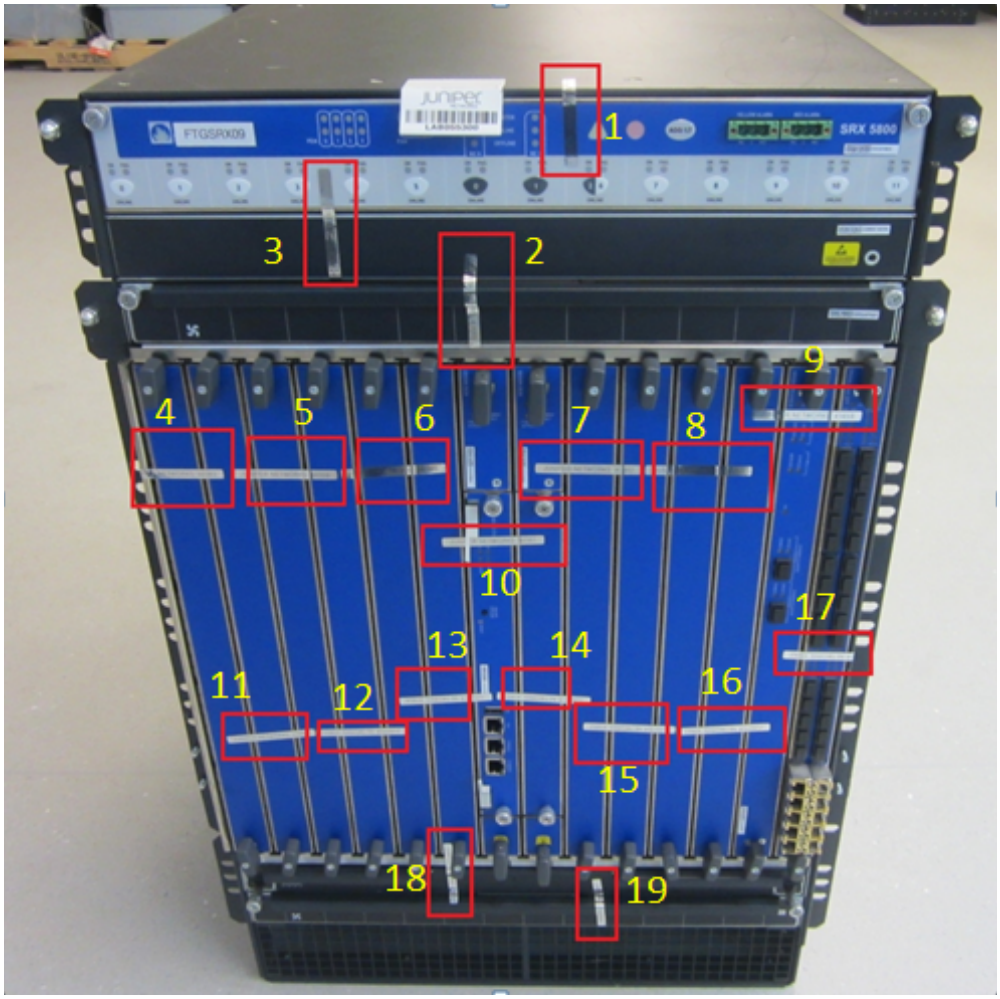

Figure 13 - SRX5800- Tamper-Evident Seal Locations on Front- 19 Seals

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 17 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Table 18 – 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 19 – 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