Juniper Networks SRX1500, SRX4100, SRX4200 and SRX4600 Services Gateways

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.3

Date: November 15, 2023

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

Table of Contents

List of Tables

List of Figures

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. The JUNOS firmware is FIPS-compliant, when configured in FIPS-MODE called JUNOS-FIPS-MODE, version 19.2R1. The firmware image is junos-srxentedge-x86-64-19.2R1.8.tgz for the SRX1500, junos-srxmr-x86-64-19.2R1.8.tgz for the SRX 4100/4200 and junos-srxhe-x86-64-19.2R1.8.tgz for the SRX4600. The firmware status service identifies itself as "Junos 19.2R1.8".
This Security Policy covers the following models – the SRX1500, SRX4100, SRX4200 and SRX 4600 models. They are meant for mid-size enterprise and data center environments.

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

Table 1 – Cryptographic Module Configurations

Model	Hardware Versions	Firmware	Distinguishing Features
SRX1500	SRX1500 SYS-JB-AC SRX1500 SYS-JB-DC	JUNOS OS 19.2R1	12x1GbE ports; 4x1GbE SFP ports; 4x10GbE SFP ports+; 2 PIM slots (not used in validation)
SRX4100	SRX4100 SYS-JB-AC SRX4100 SYS-JB-DC	JUNOS OS 19.2R1	8 x 1GbE/10GbE ports
SRX4200	SRX4200 SYS-JB-AC SRX4200 SYS-JB-DC	JUNOS OS 19.2R1	8 x 1GbE/10GbE ports
SRX4600	SRX4600 (AC) SRX4600 (DC)	Junos OS 19.2R1	8 x 1GbE/10Gb Ethernet SFP+ ports, 4 x 40/100Gb Ethernet QSFP21 ports
All	JNPR-FIPS-TAMPER-LBLS	N/A	Tamper-Evident Seals

Each Hardware Version for a model is identical in physical form factor, materials, and assembly methods. The Hardware Version differences for a model are considered non-security relevant. The differences denoted by the various suffixes are described below:

- AC – Alternating current power
- DC – Direct current power
- JB – Junos Base licensing

The module is 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 non-modifiable 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 the module is out of the scope of this validation and require a separate FIPS 140-2 validation.

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

1.1 Hardware and Physical Cryptographic Boundary

The physical forms of the modules are depicted in Figures 1-4 below. The cryptographic boundary is defined as the outer edge of the chassis. The modules do not rely on external devices for input and output of critical security parameters (CSPs).

Figure 1 - SRX1500

Figure 2 - SRX4100

Figure 3 - SRX4200

Figure 4 - SRX4600

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Ethernet	SRX1500 (21: 1 Management, 12 10/100/1000 Base-T, 4 SFP, 4 SFP+), SRX4100 (9: 1 Management, 8 SFP+), SRX4200 (9: 1 Management, 8 SFP+) SRX4600 (13: 4 QSFP28, 8 SFP+, 1 Management,)	LAN Communications	Control in, Data in, Data out, Status out
Serial	SRX1500 (1), SRX4100 (1), SRX4200 (1), SRX4600 (1)	Console serial port	Control in, Status out
Power	SRX1500 (1), SRX4100 (1), SRX4200 (1), SRX4600 (2)	Power connector	Power
Reset	SRX1500 (1), SRX4100 (1), SRX4200 (1), SRX4600 (1)	Reset	Control in
LED	SRX1500 (6), SRX4100 (3), SRX4200 (3), SRX4600 (6)	Status indicator lighting	Status out
ToD	SRX4600 (1)	RJ-45 Time of Day Port	Control in, Status out
BITS	SRX4600(1)	BITS RJ-45 port	Control in, Status out
GPS	SRX4600(2: 1 input, 1 output)	10 Mhz clock synchronization	Control in, Status out
PPS	SRX4600(2: 1 input, 1 output)	1 pulse per second	Control in, Status out
Offline	SRX4600(1)	Offline button	Control in
HA	SRX1500 (1), SRX4100 (2), SRX4200 (2), SRX4600 (4)	Cluster Control Ports	Tamper Evident Label – Inaccessible
SSD	SRX4600(2)	Solid state storage	Tamper Evident Label – Inaccessible
USB	SRX1500 (1), SRX4100 (2), SRX4200 (2), SRX4600 (1)	Firmware load port/Storage device	Tamper Evident Label – Inaccessible

1.2 Mode of Operation

The JUNOS firmware image must be installed on the device. Once the image is installed, the Crypto-Officer (CO) shall follow the instructions in Section 5 to apply the tamper seals to the module. Next, the module is configured in FIPS-MODE, as described below, and rebooted. Once the module is rebooted and the integrity and self-tests have run successfully on initial power-on in FIPS-MODE, the module is operating in the FIPS-Approved mode. The Crypto-Officer (CO) must create a backup image of the firmware to ensure it is also a JUNOS-FIPS-MODE 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

The CO shall enable the module for FIPS mode of operation by performing the following steps.

1. Enable the FIPS mode on the device.
```
user@host# set system fips level 2
```
2. Commit and reboot the device.
```
user@host# commit
```

When AES GCM is configured as the encryption-algorithm for IKE or IPsec, the CO must configure the module to use IKEv2 by running the following commands:

IKE:

```
root@host# set security ike proposal <ike_proposal_name> encryption-algorithm aes-256-
gcm
```

IPSec:

```
root@host# set security ipsec proposal <ipsec_proposal_name> encryption-algorithm aes-
128-gcm

root@host# set security ike gateway <gateway_name> version v2-only

root@host# commit
```

In order to ensure compliance with [IG A.13], the module must be configured to limit the number of blocks encrypted by a specific key bundle with the Triple-DES algorithm to a value less than 2^20. Both IPsec and IKEv2 may utilize Triple-DES encryption. In IPsec, Triple-DES may be used for transfer of data packets and in IKEv2 Triple-DES may be utilized for re-keying operations that occur when the IPsec protocol reaches a configured limit for the number of packets transmitted.

When Triple-DES is configured as the encryption-algorithm for IPsec, the CO must configure the IPsec proposal lifetime-kilobytes to comply with [IG A.13] using the following command, setting <kilobytes> to a value less than or equal to 8192 which is the maximum amount of kilobytes permitted to be encrypted by a key:

```
co@fips-srx:fips# set security ipsec proposal <ipsec_proposal_name> lifetime-kilobytes
<kilobytes>”

co@fips-srx:fips# commit
```

Whenever <kilobytes> of data has been transmitted by the IPsec protocol, a re-key operation is triggered to establish a new key bundle for IPsec. This rekey operation is negotiated by the IKE protocol. If the IKE protocol is configured to use Triple-DES, it must also be configured to limit the number of blocks to a value less than 2^20. Because the Maximum lifetime of IKE key is 24 hours, the IPsec limit needs to be set to ensure that the number of rekey operations in a 24-hour period won’t cause the IKE protocol to encrypt more than 2^20 blocks. To reduce the number of rekey operations requested by the IPsec protocol, it is necessary to *increase* the number of blocks transmitted by the IPsec protocol. Therefore, when Triple-DES is the encryption-algorithm for IKE, the lifetime-kilobytes for the associated IPsec proposal in the above command must be greater than or equal to 6913080.

Because the lifetime-kilobytes cannot be set to a value that is less than 8192 *and* greater than 6913080, Triple-DES encryption may not be used for IKE and IPsec simultaneously. e.g. if IKE is configured to use Triple-DES, IPsec would be configured to use AES.

The `show version` command will display the version of the Junos OS on the device so that the CO can confirm it is the FIPS validated version. The CO should also verify the presence of the suffix string ":fips" in the cli prompt, indicating the module is operating in FIPS mode.

The `show configuration security ike` and `show configuration security ipsec` commands display the approved and configured IKE/IPsec configuration for the device operating in FIPS-approved mode.

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:

```
user@host> request system zeroize hypervisor
```

This command wipes clean all the CSPs/configs as well as the disk. After zeroization, the device will have to be reimaged to bring it back into FIPS mode, as all the disk partitions are securely erased. The CO must follow the instructions in Section 1.2, including installing the FIPs validated image on the device and new tamper evident labels after reimaging.

Use of the zeroize command is restricted to the Cryptographic Officer. The cryptographic officer shall perform zeroization in the following situations:

1. Before FIPS Operation: To prepare the device for operation as a FIPS cryptographic module by erasing all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module.
2. Before non-FIPS Operation: To conduct erasure of all CSPs and other user-created data on a device in preparation for repurposing the device for non-FIPS operation.

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 Tables 4, 5, 6, 7, 8 and 9 below. Although the module may have been tested for additional algorithms or modes, only those listed below are actually utilized by the module. Table 11 summarizes the allowed high-level protocol and algorithm support.

2.1 Approved Algorithms

Table 4 – Data Plane Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1046	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP800-38D	GCM	Key Sizes: 128, 192, 256	Encrypt, Decrypt, AEAD
	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128	
	SHS	PUB 180-4	SHA-1 SHA-256		Message Digest Generation
	Triple-DES[1]	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 5 – Control Plane QuickSec Approved Cryptographic Functions

Cert	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1045	AES	PUB 197-38A	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		SP800-38D	GCM	Key Sizes: 128, 256	Encrypt, Decrypt, AEAD
N/A[2]	CKG	SP800-133Rev2 (IKE)	Section 4		Asymmetric key generation using unmodified DRBG output
C1045	CVL	SP 800-135	IKEv1	SHA 256, 384	Key Derivation
			IKEv2	SHA 256, 384	
	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384)	KeyGen, SigGen, SigVer

---

[1] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

[2] Vendor Affirmed.

	HMAC	PUB 198	SHA-256	Key size: 256bits λ = 256	Message Authentication, KDF Primitive
			SHA-384	Key size: 384 bits, λ = 384	
N/A	KTS		AES Cert. #C1045 and HMAC Cert. #C1045		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Certs. #C1045 and HMAC Certs. # C1045		key establishment methodology provides 112 bits of encryption strength
C1045	RSA	PUB 186-4	PKCS1_V1_5	n=2048 (SHA 256) n=4096 (SHA 256)	SigGen, SigVer[3]
	SHS	PUB 180-4	SHA-256 SHA-384		Message Digest Generation
	Triple-DES[4]	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1049	AES	PUB 197-38A	CBC CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
N/A[5]	KAS-SSC	SP800-56A Rev3	FFC DH	MODP-2048 (ID=14)	Key Agreement (IKE/SSH)
				MODP-2048 (ID=24)	Key Agreement (IKE)
			ECC DH	P-256 P-384	Key Agreement (IKE)
N/A[6]	CKG	SP800-133Rev2 (SSH)	Section 4		Asymmetric key generation using unmodified DRBG output
C1049	ECDSA	PUB 186-4		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer
	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 160	Message Authentication

---

[3] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

[4] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

[5] Vendor affirmed as per IG D.1-rev3.

[6] Vendor Affirmed.

			SHA-256	Key size: 256 bits, λ = 256	Message Authentication DRBG Primitive
			SHA-512	Key size: 512 bits, λ = 512	Message Authentication
N/A	KTS		AES Cert. #[C1049]() and HMAC Cert. #[C1049]()		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Cert. # [C1049]() and HMAC Cert. # [C1049]()		key establishment methodology provides 112 bits of encryption strength
[C1049]()	RSA	PUB 186-4	n=2048 (SHA 256) n=4096 (SHA 256)		KeyGen[7]
			n=2048 (SHA 256) n=4096 (SHA 256)		SigGen
			n=2048 (SHA 256) n=4096 (SHA 256)		SigVer[8]
	SHS	PUB 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
	Triple-DES[9]	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

Table 7 – OpenSSH Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
[C1050]()	CVL	SP 800-135	SSH	SHA 1, 256, 384	Key Derivation

Table 8 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
[C1043]()	HMAC	PUB 198	SHA-1	Key size:160 bits, λ = 160	Password Hashing
			SHA-256	Key size:256bits,	

---

[7] RSA 4096 KeyGen was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 KeyGen was tested and testing for RSA 4096 KeyGen is not available.

[8] RSA 4096 SigVer was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 2048 SigVer was tested and testing for RSA 4096 SigVer is not available.

[9] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

				λ = 256	
	SHS	PUB 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 9 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1044	DRBG	SP 800-90A	HMAC	SHA-256	Random Bit Generation
	HMAC	PUB 198	SHA-256	Key size:256 bits, λ = 256	DRBG Primitive
	SHS	PUB 180-4	SHA-1 SHA-256		Message Authentication DRBG Primitive

2.2 Allowed Algorithms

Table 10 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
NDRNG [IG] 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DRBG

2.3 Allowed Protocols

Table 11 – Protocols using approved algorithms in FIPS Mode

Protocol	Key Exchange	Groups	Auth	Cipher	Integrity
IKEv1[10]	KAS-FFC	MODP-2048 (ID=24) MODP-2048 (ID=14)	RSA 2048 RSA 4096 Pre-Shared Secret ECDSA P-256 ECDSA P-384	Triple-DES CBC[11] AES CBC 128/192/256	HMAC-SHA-256 HMAC-SHA-384
	KAS-ECC	P-256 P-384			
IKEv2[12]	KAS-FFC	MODP-2048 (ID=24) MODP-2048 (ID=14)	RSA 2048 RSA 4096	Triple-DES CBC[13]	HMAC-SHA-256

---

[10] RFC 2409 governs the generation of the Triple-DES encryption key for use with the IKEv1 protocol

[11] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

[12] IKEv2 generates the SKEYSEED according to RFC7296, from which all keys are derived, including Triple-DES keys.

[13] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

	KAS-ECC	P-256 P-384	Pre-Shared Secret ECDSA P-256 ECDSA P-384	AES CBC 128/192/256 AES GCM[14] 128/256	HMAC-SHA-384
IPsec ESP	IKEv1 with optional KAS-FFC	MODP-2048 (ID=24) MODP-2048 (ID=14)	IKEv1	Triple-DES CBC[15] AES CBC 128/192/256 AES GCM[16] 128/192/256	HMAC-SHA1-96 HMAC-SHA-256-128
	IKEv1 with optional KAS-ECC	P-256 P-384			
	IKEv2 with optional KAS-FFC	MODP-2048 (ID=24) MODP-2048 (ID=14)	IKEv2	Triple-DES CBC[17] AES CBC 128/192/256 AES GCM[18] 128/192/256	
	IKEv2 with optional KAS-ECC	P-256 P-384			
SSHv2[19]	KAS-FFC	MODP-2048 (ID=14)	RSA 2048 ECDSA P-256	Triple-DES CBC[20] AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1-96 HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

No part of these protocols, other than the KDF, have been tested by the CAVP and CMVP. The IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 10 above: each column of options for a given protocol is independent

---

[14] The AES GCM IV is generated according to RFC5282 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[15] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

[16] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[17] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

[18] The AES GCM IV is generated according to RFC4106 and is used only in the context of the IPSec protocol as allowed in IG A.5. Rekeying is triggered after 2^{32} AES GCM transformations.

[19] RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol

[20] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per SP 800-131A.

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.

- RSA with key size less than 2048
- ECDSA with ed25519 curve
- ECDH with ed25519 curve
- ECDH with P-256, P-384 and P-521 (used with SSH)
- ARCFOUR
- Blowfish
- CAST
- DSA (SigGen, SigVer; non-compliant)
- 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 12 – Critical Security Parameters (CSPs)

Name	Description and usage
DRBG Seed	Seed material used to seed or reseed the HMAC DRBG
DRBG State	V and Key values for the HMAC DRBG
DRBG Entropy Input	256 bits entropy (min) input used to instantiate HMAC DRBG
DH Shared Secret	The shared secret used in Diffie Hellman (DH) key agreement (256 bits).
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. RSA 2048, ECDSA P-256. Used to identify the host.
SSH DH	SSH Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in SSH. DH (L=2048, N=2047)
SSH-SEKs	SSH Session Keys: SSH Session Encryption Key: TDES (3key) or AES; SSH Session Integrity Key: HMAC
ESP-SEKs	IPSec ESP Session Keys: IKE Session Encryption Key: TDES (3key) or AES; IKE Session Integrity Key: HMAC
IKE-PSK	Pre-Shared Key used to authenticate IKE connections.
IKE-Priv	IKE Private Key. RSA 2048, RSA 4096 ECDSA P-256, or ECDSA P-384
IKE-SKEYID	IKE SKEYID. IKE secret used to derive IKE and IPsec ESP session keys.
IKE-SEKs	IKE Session Keys: IKE Session Encryption Key: TDES (3key) or AES; IKE Session Integrity Key: HMAC
IKE-DH-PRI	IKE Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in IKE. DH (L = 2048, N = 256), ECDH P-256, or ECDH P-384

HMAC key	The libMD HMAC keys: message digest for hashing password and critical function test.
CO-PW	Password used to authenticate the CO.
User-PW	Password used to authenticate the User.

Table 13 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. RSA 2048, ECDSA P-256.
SSH-DH-PUB	Diffie-Hellman public component. Ephemeral Diffie-Hellman public key used in SSH key establishment. DH (L=2048, N=2047)
IKE-PUB	IKE Public Key. RSA 2048, RSA 4096, 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, N = 256), ECDH P-256, or ECDH P-384
Auth-User Pub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P256, P-384, P-512, RSA 2048, RSA 3072 or RSA 4096
Auth-CO Pub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P256, P-384, P-512, RSA 2048, RSA 3072 or RSA 4096
Root-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	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.

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 of the identity-based operator authentication methods in section 3.2.

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 and establish VPN tunnels.

The User role monitors the router via the console or SSH. The user role cannot 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; thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1,000,000.

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. 4th failed attempt = 10-second delay, 5th failed attempt = 15-second delay, 6th failed attempt = 20-second delay, 7th 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.

Signature verification

Public key authentication in SSH uses either RSA or ECDSA signatures. Let x denote the maximum number of signature verifications that the IUT can perform in a minute. Assuming a minimum security strength of 112 bits for the signature algorithm (corresponding to 2048-bit key RSA signatures as per SP800-57 Part1 Rev3), the probability of success for a single random attempt is at most 1/2^112 , which is less than 1/10^6. It follows that the probability of a successful brute-force attack with multiple consecutive attempts in a one-minute period is at most $x/2\text{^}112$. For this probability to be greater than 1/100,000, the number of verifications per minute should be $x > 2\text{^}112/10\text{^}5 \cong 2\text{^}197$, which is clearly an infeasible amount of signature verifications. To see this, note that if the IUT was able to compute one signature verification per CPU cycle, this would amount to $60 \times 3.2 \times 10\text{^}9 \cong 2\text{^}37 \ll 2\text{^}197$, for the fastest processor, which is 3.2GHz for the SRX1500. Thus, the success probability of a brute-force attack during a one-minute period is less than 1/100,000, as required by FIPS 140-2.

3.3 Services

All services implemented by the module are listed in the tables below. Table 16 lists the access to CSPs by each service.

Table 14 – 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	
Load image	Verification and loading of a validated firmware image into the switch.	X	

Table 15 – Unauthenticated traffic

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

Table 16 – CSP Access Rights within Services

SERVICE	CSP															
	DRBG Seed	DRBG State	DRBG Entropy Input	DH Shared Secret	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYID	IKE-SEK	IKE-DH-PRI	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	--	GWR	--	--	--	WR	GWR	--	--	--	G	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	--	--	E	--	--	--	E	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	--	Z	Z	Z	Z	Z	Z	--	--	--	--	Z	Z
SSH connect	--	E	--	GE	E	GE	GE	--	--	--	--	--	--	--	E	E
IPsec connect	--	E	--	GE	--	--	--	G	E	E	GE	G	GE	--	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	GEZ	GZ	GZ	Z	--	Z	Z	Z	--	--	Z	Z	Z	Z	Z	Z
Local reset	GEZ	GZ	GZ	Z	--	Z	Z	Z	--	--	Z	Z	Z	--	Z	Z
Traffic	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

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 except for SSH Connect (non-compliant) and IPSec Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.4 and the SSHv2 row of Table 10. The IPsec (non-compliant) supports the DSA in Section 2.4 and the IKEv1, IKEv2 and IPSec rows of Table 10.

Table 17 – 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	
Load image (non-compliant)	Verification and loading of a validated firmware image into the router.	X	

Table 18 – 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
    - AES-GCM (128/192/256) Decrypt KAT
- **Control Plane QuickSec KATs**
    - SP 800-90A HMAC DRBG KAT
        - Health-tests initialize, re-seed, and generate
    - 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-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
    - DH (L=2048, N=256) KAT
        - Derivation of the expected shared secret.
    - 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-512 KAT
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - SHA-384 KAT
- **OpenSSH KATs**
  - KDF-SSH KAT
- **LibMD KATs**
  - HMAC SHA-1
  - HMAC SHA-256
  - SHA-512
- **Kernel KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - HMAC SHA-256 KAT
  - SHA-1
- Critical Function Test
  - The cryptographic module performs a verification of a non-modifiable 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.
- SP800-56A assurances as per SP 800-56A Sections 5.5.2,5.6.2, and/or 5.6.3, in accordance to IG 9.6.
- 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 19 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper seals (part # JNPR-FIPS-TAMPER-LBLS), 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 and then follow the steps in Section 1.2 to place the module back into a FIPS-Approved mode of operation.

5.1 General Tamper Evident Label 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 SRX1500 (10 seals)

Six tamper evident labels (TEL) must be applied to the following location:

- The front of the SRX1500 has two slot covers. The slot covers should be secured with two screws each and then tamper evident labels (TEL #1 & #2) applied as shown by the red boxes in following two figures. The TEL go from the front of the SRX1500 to the top (Figures 4 & 5).
- 2 Tamper labels (#5 & #6) are used to cover the USB port and two tamper labels (#3 & #4) are used to cover the High Availability port (Figure 4).

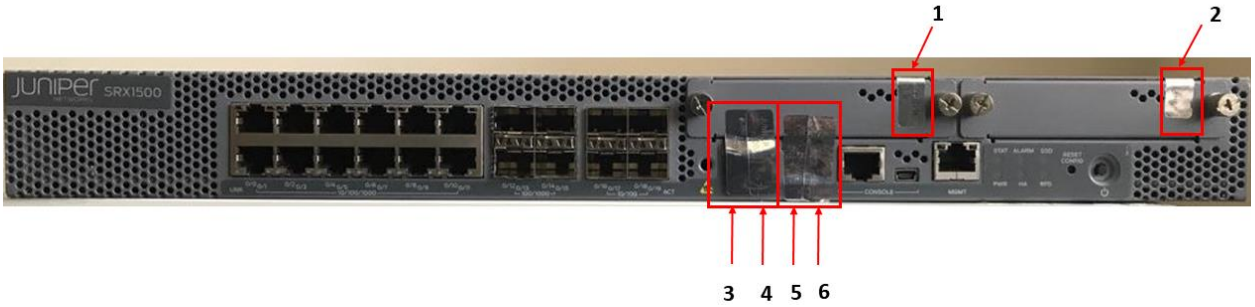

Figure 5 - SRX1500 Front View: TEL 1 - 6

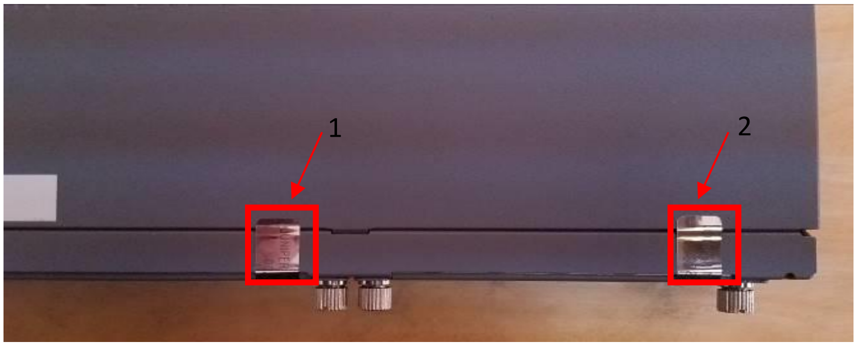

Figure 6 - SRX1500 Top-Front View: TEL 1 & 2

- The rear of the SRX1500 has two TELs (TEL #7 and TEL #8). The TEL #7, at the top of the rear-view wraps to the top of the device and covers the fourth screw from side containing the power supply (see Figure 7). TEL #8 wraps from the rear of the SRX1500, on the SSD slot cover, to the bottom of the SRX1500 (see Figure 8).

Figure 7 - SRX1500 Rear View: TEL 7 & 8

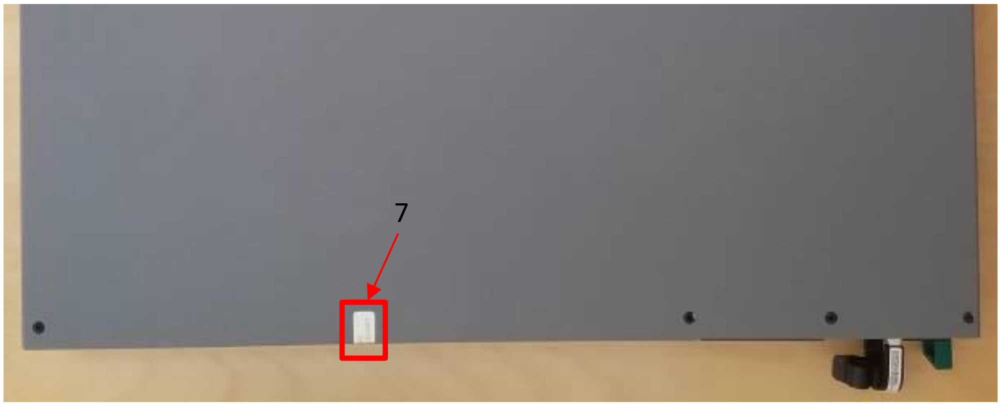

Figure 8 - SRX1500 Top - Rear View: TEL 7

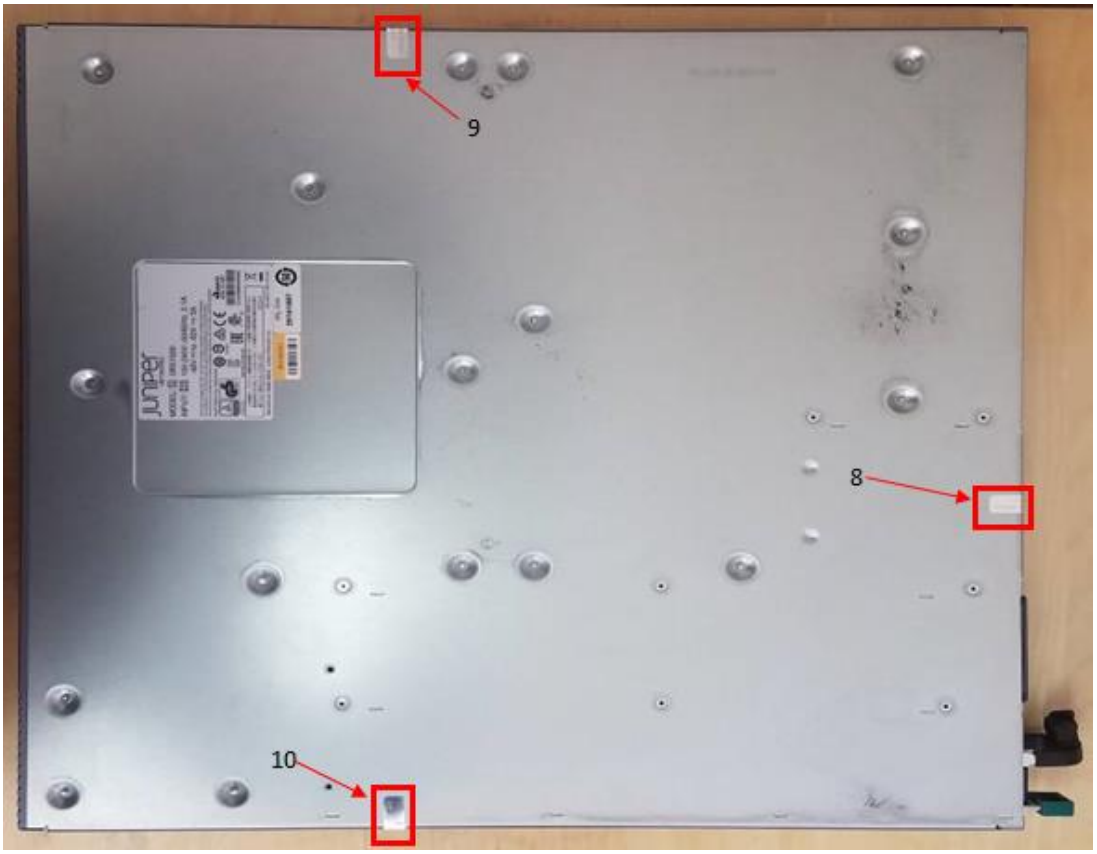

Figure 9 - SRX1500 Bottom View: TEL 8, 9 & 10

- TEL #9 and TEL #10 cover the indicated screw on the left and right side of the SRX1500 (Figure 10 andFigure 11) and wrap to the bottom of the SRX1500 as shown in Figure 8.

Figure 10 - SRX1500 Right Side View: TEL 9

Figure 11 - SRX1500 Left Side View: TEL 10

5.3 SRX4100 & SRX4200 (13 seals)

The placement of the tamper evident labels for the SRX4100 and SRX4200 are the same in that the outside of the devices is identical. Thirteen tamper-evident seals must be applied to the following locations:

- The top of the chassis, covering one screw on the top-back left and one screw on the top-back right (TEL #1 and TEL #2). The TELs cover the screws on the top of the chassis and wrap down each side of the chassis.

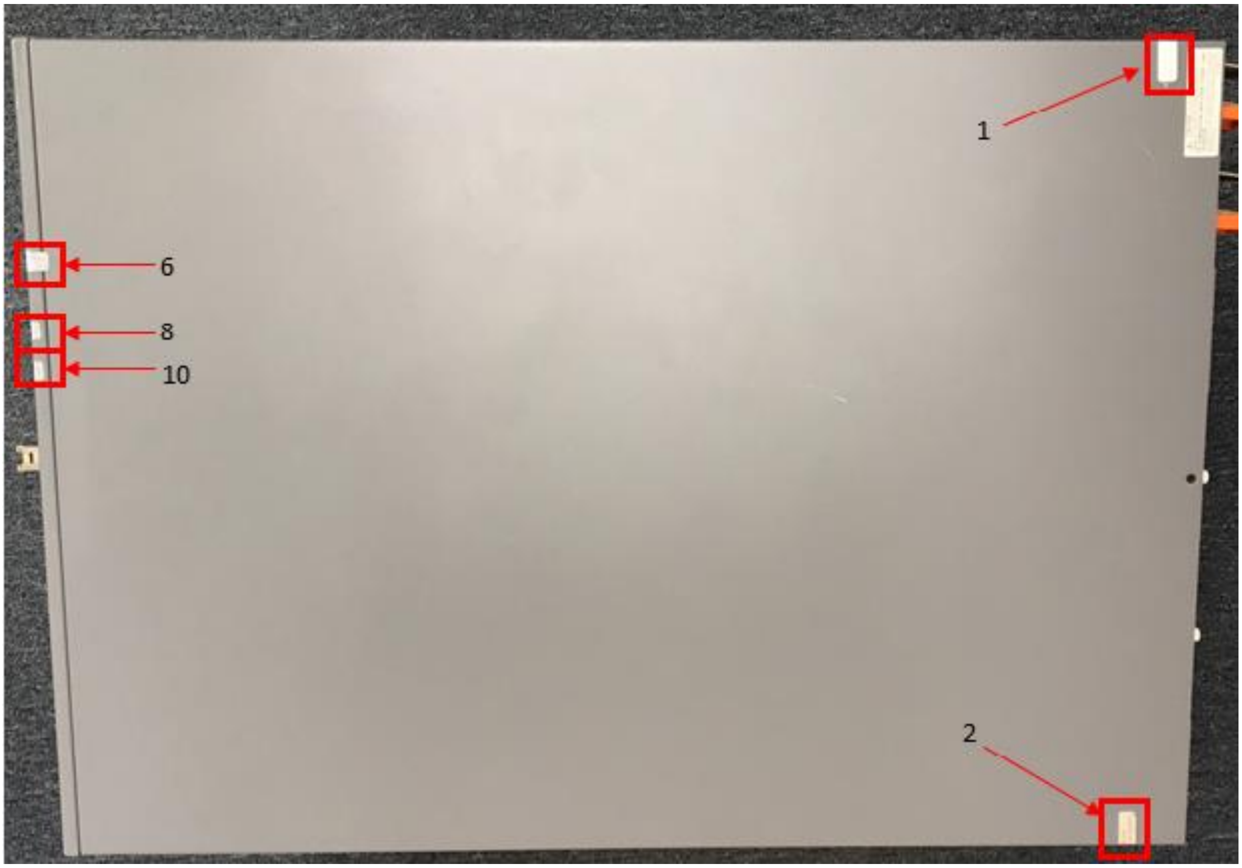

Figure 12 - SRX4100 & SRX4200 Top View: TEL 1, 2, 6, 8 & 10

Figure 13 - SRX4100 & SRX4200 Left-Side View: TEL 1

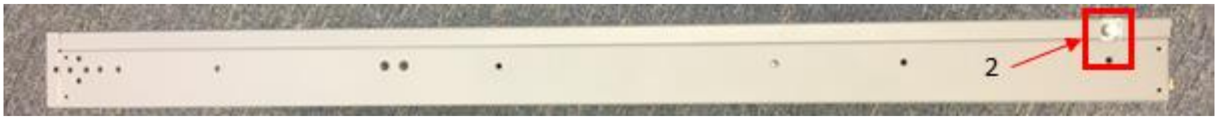

Figure 14 - SRX4100 & SRX4200 Right-Side View: TEL 2

- Bottom chassis, covering 3 screws that secure the faceplates on the front of the chassis. TEL #3, #4, #5 are entirely on the bottom of the chassis they do not wrap around to any other portion of the chassis

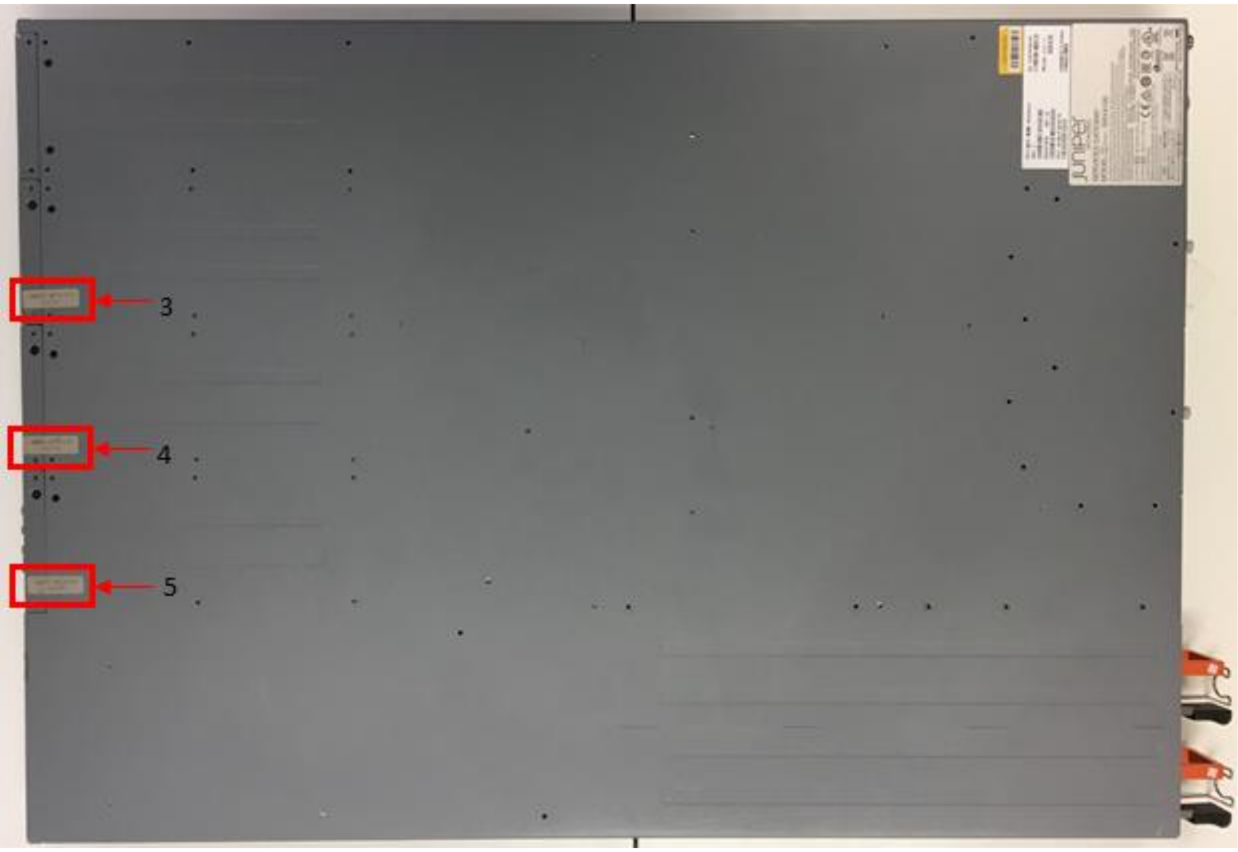

Figure 15 - SRX4100 & SRX4200 Bottom View: TEL 3, 4, 5

- Tamper evident seals 6 & 7 cover the two USB ports on the front of the SRX4100 and the SRX4200
- Two tamper evident labels cover each HA port. Tamper evident labels #8 & #9 cover one HA port and tamper evident labels #10 & #11 cover the second HA port.

Figure 16 - SRX4100 & SRX4200 Front View: TEL 6-11

- The rear of the SRX4100 & SRX4200 require 2 tamper evident labels (TEL #12 and #13) as shown in Figure 17. Each label is applied on the power supply plate and wraps around the bottom.

Figure 17 - SRX4100 & SRX4200 Rear View: TEL 12-13

5.4 SRX4600 (15 seals)

Fifteen tamper evident labels (TEL) must be applied to the following location:

- The front of the SRX4600 has 4 HA ports, 1 USB port, and 2 Solid State Drives (SSDs) that must be protected with 8 tamper evident labels.
- Referring to Figure 18 and Figure 19, the front panel requires 4 tamper evident labels (#1 - #4) cover the HA ports, 2 tamper evident labels cover the USB port and top screw (#5, #6), 1 tamper evident label (#7) to cover the first SSD, and 1 tamper evident label (#8) to cover the second SSD.

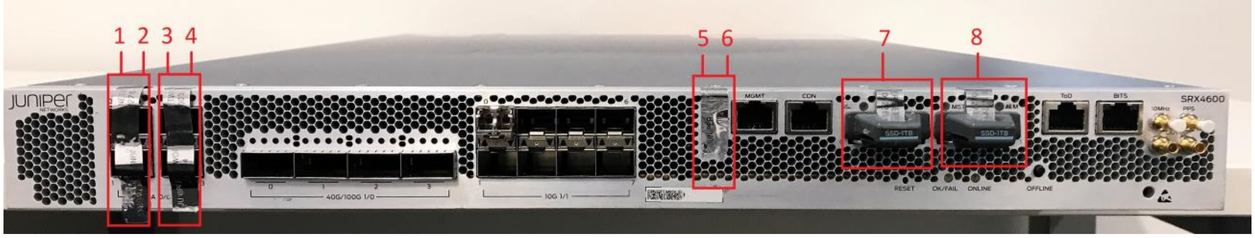

Figure 18 - SRX4600 Front View: TEL 1 – 8

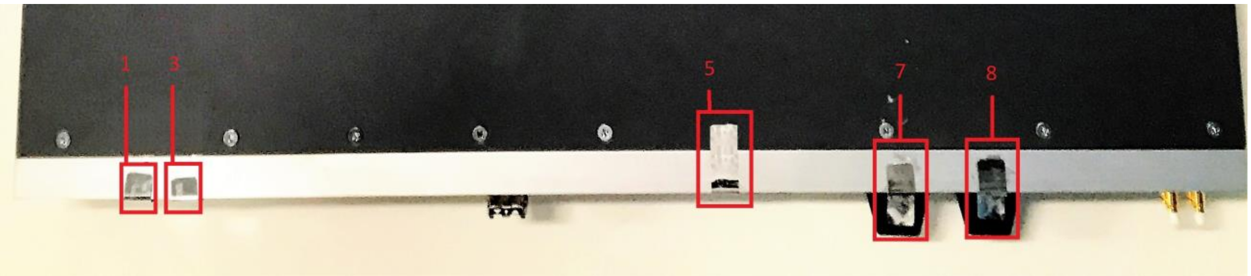

Figure 19 - SRX4600 Top Front View: TEL 1, 3, 5, 7, 8

- The rear of the SRX4600 requires 7 tamper evident labels (TEL #9 -#15) as shown in Figure 20 TEL #9 and TEL #10 wrap over the top and cover the back plate of each power supply and the adjacent chassis edge. Each of TEL#11 to TEL #15 = wraps over the top and attaches to a fan cover.

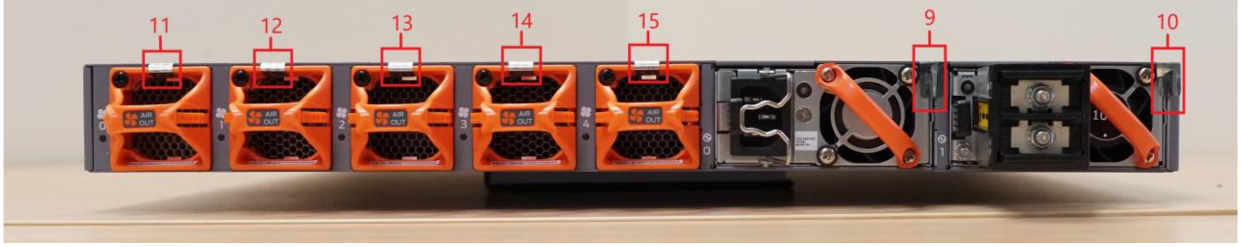

Figure 20 - SRX4600 Rear View: TEL 9-15

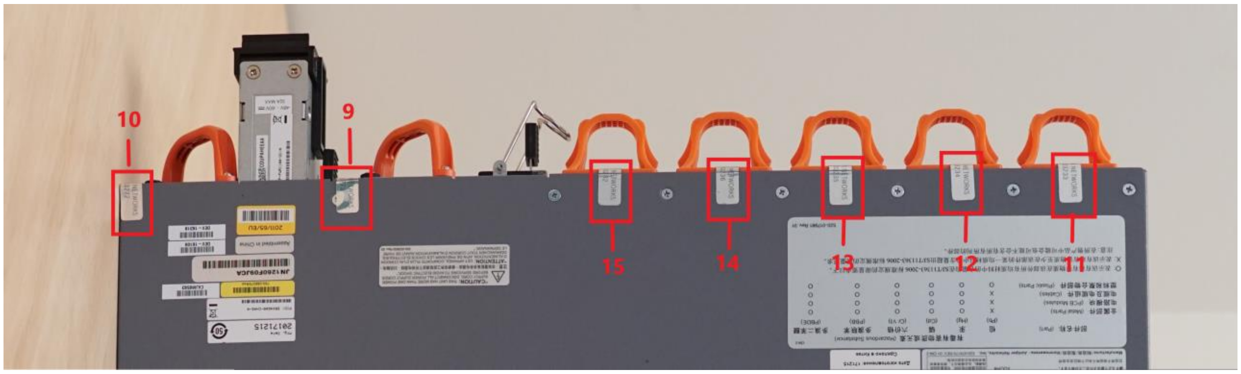

Figure 21 - SRX4600 Top Rear View: TEL 9 – 10

- The right and left sides have 1 TEL each (TEL 11 and 12) over the 4th screw from the front and wrapping around to the bottom. Figures 6 & 7 show the placement of the side TELs.

Figure 22 - SRX4600 Right Side View: TEL 12

Figure 23 - SRX4600 Left Side View: TEL 11

- The bottom view (Figure 8) shows the TELs wrapping around from the front and sides of the SRX4600.

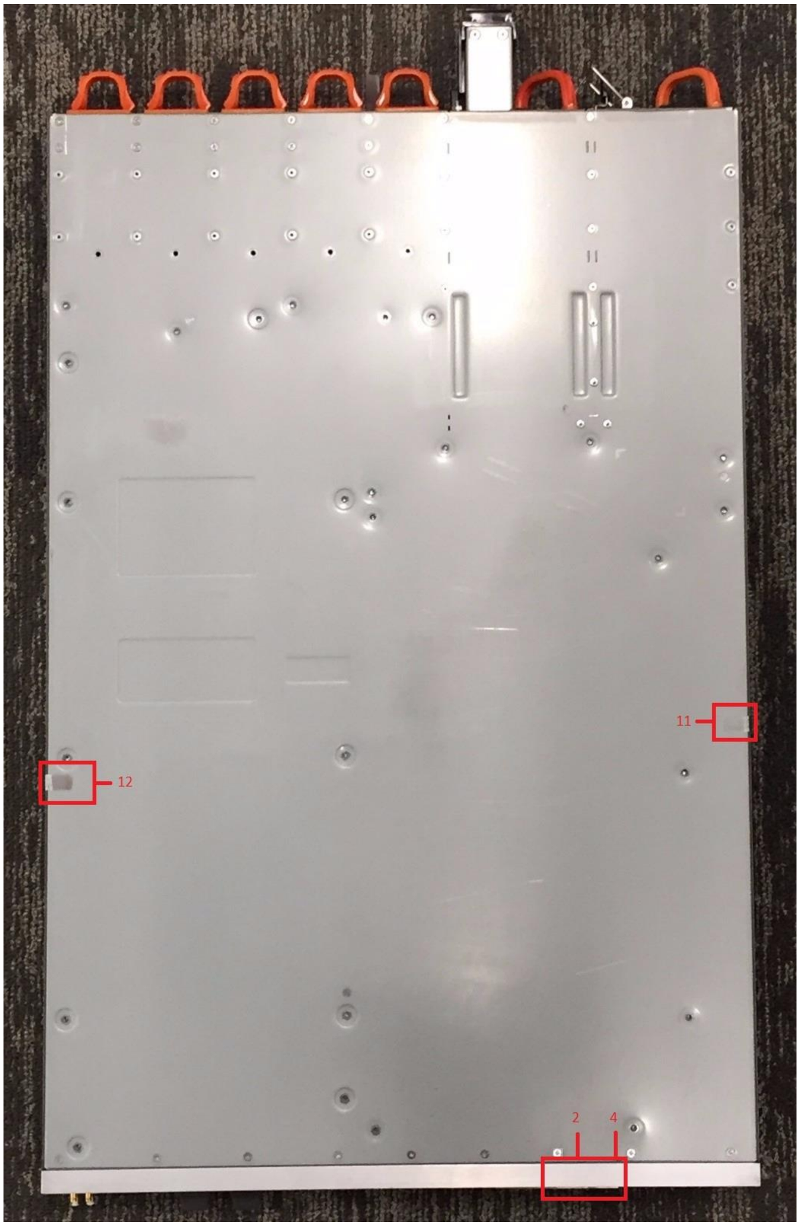

Figure 24 - SRX4600 Bottom View: TEL 2, 4, 11, 12

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 two independent internal actions to be performed prior to outputting 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.
13. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
14. The cryptographic officer must configure the module to IPsec ESP lifetime-kilobytes to ensure the module does not encrypt more than 2^20 blocks with a single Triple-DES key when Triple-DES is the encryption-algorithm for IKE or IPsec ESP. The operator is required to ensure that Triple-DES keys used in SSH do not perform more than 2^20 encryptions.
15. The module must be configured to disallow the use of ECDH in SSH by using the following CLI command:

    ```
    co@fips-qfx# set system services ssh key-exchange dh-group14-sha1
    ```

16. Triple-DES is only allowed until December 31st, 2023, as per SP 800-131A. From January 1st, 2024, the module should be configured to disallow the use of Triple-DES.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 20 – 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*, Revision 1, March 2019
[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.
[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*
[56A]	National Institute of Standards and Technology, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A, March 2007
[56ARev3]	National Institute of Standards and Technology, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A Revision 3, April 2018
[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*
[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, Revision 2, November 2017*
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.

Abbreviation	Full Specification Name
[133Rev2]	National Institute of Standards and Technology, Recommendation for Cryptographic Key Generation, Special Publication 800-133, Revision 2, June 2020

Table 21 – Acronyms and Definitions

Acronym	Definition
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IPsec	Internet Protocol Security
MD5	Message Digest 5
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 22 – Datasheets

Model	Title	URL
SRX1500	SRX1500 Services Gateway	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000551-en.pdf
SRX4100 SRX4200	SRX4100 and SRX4200 Services Gateways	http://www.juniper.net/assets/de/de/local/pdf/datasheets/1000600-en.pdf
SRX4600	SRX4600 Services Gateway	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000628-en.pdf