Juniper Networks SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 Services Gateways

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 1.3

Date: March 1, 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 OS 20.2R1 firmware. The Junos OS firmware is FIPS-compliant when configured in FIPS-MODE called JUNOS-FIPS-MODE, version 20.2R1.
This Security Policy covers the

- SRX345,
- SRX345-DUAL-AC,
- SRX380 and
- SRX1500 models.

The firmware image is junos-srxsme-20.2R1.10.tgz for the models SRX345, SRX345-DUAL-AC and SRX380; and junos-srxentedge-x86-64-20.2R1.10.tgz for the SRX1500 model. The firmware status service identifies itself as "Junos 20.2R1.10".
The cryptographic module is defined as a multiple-chip standalone module that executes the Junos OS 20.1R1 firmware on the Juniper Networks SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 models listed in the table below.

Table 1 – Cryptographic Module Configuration

Model	Hardware Versions	Firmware	Distinguishing Features
SRX345	SRX345	Junos OS 20.2R1	8 x 10/100/1000 4x SFP 4x MPIM expansion slots 1x 10/100/1000 management port
SRX345-DUAL-AC	SRX345-DUAL-AC	Junos OS 20.2R1	8 x 10/100/1000 4x SFP 4x MPIM expansion slots 1x 10/100/1000 management port Dual AC PSU
SRX380	SRX380	Junos OS 20.2R1	16 x 10/100/1000 4x SFP 4x MPIM expansion slots 1x 10/100/1000 management port
SRX1500	SRX1500 SYS-JB-AC	Junos OS 20.2R1	12x1GbE ports; 4x1GbE SFP ports; 4x10GbE SFP ports+; 2 PIM slots (not used in validation) AC PSU
	SRX1500 SYS-JB-DC	Junos OS 20.2R1	12x1GbE ports; 4x1GbE SFP ports; 4x10GbE SFP ports+; 2 PIM slots (not used in validation) DC PSU
All	JNPR-FIPS-TAMPER-LBLS	N/A	Tamper-Evident Seals

The difference between the hardware versions of the SRX1500 model is regarding the use of AC or DC current power. This difference is considered non-security relevant.

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 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 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 form of the module is depicted in Figures 1-8 below. The cryptographic boundary is defined as the outer edge of the chassis. The module does not rely on external devices for input and output of critical security parameters (CSPs).

Figure 1– SRX345 (Front)

Figure 2 – SRX345 (Rear)

Figure 3 – SRX345-DUAL-AC (Front)

Figure 4 – SRX345 -DUAL-AC(Rear)

Figure 5 – SRX380 (Front)

Figure 6 – (Rear)

Figure 7 - SRX1500 (Front)

Figure 8– SRX1500 (Rear)

The following table maps each logical interface type defined in the FIPS 140-2 standard to one or more `physical interfaces.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Ethernet (data)	LAN Communications	Control in, Data in, Data out, Status out
Ethernet (mgmt.)	Remote management.	Control in, Data in, Status out, Data out
Serial	Console serial port	Control in, Status out
Power	Power connector	Power in
Reset Button	Reset	Control in
LED	Status indicator lighting	Status out
USB	Firmware load port/Storage device	Tamper Evident Label – Inaccessible
HA	Cluster Control Ports	Tamper Evident Label – Inaccessible

1.2 Mode of Operation

The Junos OS firmware image must be installed on the device by executing the following command from the command line interface in the version of Junos OS running on the device:

```
user@host> request system software add /<image-path>/<junos package> no-copy no-validate reboot
```

where `/<image path>/<junos package>` point to the Junos OS 20.2R1 firmware image file.

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. Set the root password.
   ```
   user@host# set system root-authentication plain-text-password

   New password: type password here

   Retype new password: retype password here
   ```
3. 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.

According to SP800-131A Rev3, the use of Triple-DES is no longer allowed after 2023. Thus, from January 1st, 2024

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
```

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, 6, 7, 8, 9 and 10 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 – SRX Data Plane Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C2034 C2036	AES	[38A]	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
C2035 C2036	AES	[38D]	GCM	Key Sizes: 128, 192, 256	Encrypt, Decrypt, AEAD
C2034 C2036	HMAC	[198]	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128	
	SHS	[180]	SHA-1 SHA-256		Message Digest Generation
	Triple-DES[1]	[67]	TCBC	Key Size: 192	Encrypt, Decrypt
N/A[2]	KAS-SSC	[56ARev3]	FFC DH dhEphem	MODP-2048 (ID=14) MODP-2048 (ID=24)	Key Agreement Scheme (IKE in SRX345, SRX345-DUAL-AC and SRX380)
			ECC DH Ephemeral Unified	P-256 (SHA 256) P-384 (SHA 384)	

Table 5 – Control Plane QuickSec Approved Cryptographic Functions

Cert	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C2028 C2094	AES	[197]	CBC	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		[38D]	GCM	Key Sizes: 128, 256	Encrypt, Decrypt, AEAD
	CVL	[135]	IKEv1	SHA 256, 384	Key Derivation
			IKEv2	SHA 256, 384	
	DRBG	[90A]	HMAC	SHA-256	Random Bit Generation
	HMAC	[198]	SHA-256	Key size: 256bits λ = 256	Message Authentication, KDF Primitive

[1] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A].

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

			SHA-384	Key size: 384 bits, λ = 384	
	SHS	[180]	SHA-256 SHA-384		Message Digest Generation
	Triple-DES[3]	[67]	TCBC	Key Size: 192	Encrypt, Decrypt
N/A	KTS		AES-CBC Certs. C2028 and C2094, and HMAC Certs. C2028 and C2094		key establishment methodology provides between 128 and 256 bits of encryption strength
			AES-GCM Certs C2028 and C2094		
			Triple-DES-CBC Certs. C2028 and C2094, and HMAC Certs. C2028 and C2094		key establishment methodology provides 112 bits of encryption strength
C2032 C2094	RSA	[186]	PKCS1_V1_5	n=2048 (SHA 256) n=4096 (SHA 256)	SigGen, SigVer[4]
	ECDSA	[186]		P-256 (SHA 256) P-384 (SHA 384)	KeyGen, SigGen, SigVer

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C2031 C2039	AES	[38A]	CBC CTR	Key Sizes: 128, 192, 256	Encrypt, Decrypt
	DRBG	[90A]	HMAC	SHA-256	Random Bit Generation
N/A[5]	KAS-SSC	[56ARev3]	FFC DH dhEphem	MODP-2048 (ID=14)	Key Agreement Scheme (IKE/SSH)
				MODP-2048 (ID=24)	Key Agreement Scheme (IKE)
			ECC DH Ephemeral Unified	P-256 (SHA 256) P-384 (SHA 384)	Key Agreement Scheme (IKE)
C2031 C2039	ECDSA	[186]		P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer
	HMAC	[198]	SHA-1	Key size: 160 bits, λ = 160	Message Authentication
			SHA-256	Key size: 256 bits, λ = 256	Message Authentication DRBG Primitive

[3] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A].

[4] 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.

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

			SHA-512	Key size: 512 bits, λ = 512	Message Authentication
N/A	KTS		AES-CBC Certs. C2031 and C2039, and HMAC Certs. C2031 and C2039		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES Certs. C2031 and C2039, and HMAC Certs. C2031 and C2039		key establishment methodology provides 112 bits of encryption strength
C2031 C2039	RSA	[186]	n=2048 (SHA 256) n=4096 (SHA 256)		KeyGen[6]
			n=2048 (SHA 256) n=4096 (SHA 256)		SigGen
			n=2048 (SHA 256) n=4096 (SHA 256)		SigVer[7]
	SHS	[180]	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
	Triple-DES[8]	[67]	TCBC	Key Size: 192	Encrypt, Decrypt

Table 7 – OpenSSH Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C2033 C2040	CVL	[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
C2030 C2038	HMAC	[198]	SHA-1	Key size:160 bits, λ = 160	Password Hashing
			SHA-256	Key size:256bits, λ = 256	
	SHS	[180]	SHA-1 SHA-256 SHA-512		Message Digest Generation

[6] 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.

[7]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.

[8] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A]

Table 9 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C2029 C2037	DRBG	[90A]	HMAC	SHA-256	Random Bit Generation
	HMAC	[198]	SHA-256	Key size:256 bits, λ = 256	DRBG Primitive
	SHS	[180]	SHA-1 SHA-256		Message Authentication DRBG Primitive

2.2 Allowed Algorithms

Table 10 – Allowed Cryptographic Functions

Algorithm	Mode	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[9]	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[10] AES CBC 128/192/256	HMAC-SHA-256 HMAC-SHA-384
	KAS-ECC	P-256 P-384			
IKEv2[11]	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[12] AES CBC 128/192/256 AES GCM[13] 128/256	HMAC-SHA-256 HMAC-SHA-384

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

[10] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A].

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

[12] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A].

[13] 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.

	KAS-ECC	P-256 P-384			
IPsec ESP	IKEv1 with optional KAS-FFC	MODP-2048 (ID=24) MODP-2048 (ID=14)	IKEv1	Triple-DES CBC[14] AES CBC 128/192/256 AES GCM[15] 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 [16] AES CBC 128/192/256 AES GCM[17] 128/192/256	
	IKEv2 with optional KAS-ECC	P-256 P-384			
SSHv2[18]	KAS-FFC	MODP-2048 (ID=14)	RSA 2048 ECDSA P-256	Triple-DES CBC[19] 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 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.

[14] Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A]

[15] 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.

[16] Use of Triple-DES in this module is only allowed until December 31st, 2023.

[17] 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.

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

[19] Use of Triple-DES in this module is only allowed until December 31st, 2023.

- 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 DRBG
DRBG_State	V and Key values for the HMAC_DRBG
Entropy Input String	256 bits entropy (min) input used to instantiate the 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 $60 \times 16 \times 2.2 \times 10\text{^}9 \cong 2\text{^}41 \ll 2\text{^}197$ verifications per minute for the fastest processor, corresponding to the Cavium CN7360 processor, which consists of 16 cores at a clock rate of 2.2 GHz. 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

	CSP															
SERVICE	DRBG Seed	DRBG State	DRBG Entropy Input	DH/ECDH 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
  - DH (L=2048, N=256) KAT
    - Derivation of the expected shared secret.
  - ECDH P-256 KAT
    - Derivation of the expected shared secret.
- **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 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.
- 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 SRX380 (14 seals)

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

- Five (5) seals (TEL 1-5). Applied to the top of the chassis, covering one of the five chassis screws each.
- Four (4) seals (TEL 6-9). Applied vertically covering the front I/O Slots.
- Two (2) seals (TEL 10 & 11). Applied to the rear panel, one covering the blank faceplate, the other placed vertically wrapping around onto the base of the device.
- One (1) seal (TEL 15). Applied across the grounding connection, if it is not in use.
- Two (2) seals (TEL 12 & 13). Applied to the front panel on either side of the LED matrix on the left of the device.

- One (1) seal (TEL 14). Covering the Front USB port.

Figure 9 – SRX380 Tamper-Evident Seal Placement (front)

TEL1-5 covering one of the five chassis screws each; TEL 6-9 covering the front I/O Slots; TEL 12-13 on either side of the LED matrix; TEL 14 covering the Front USB port.

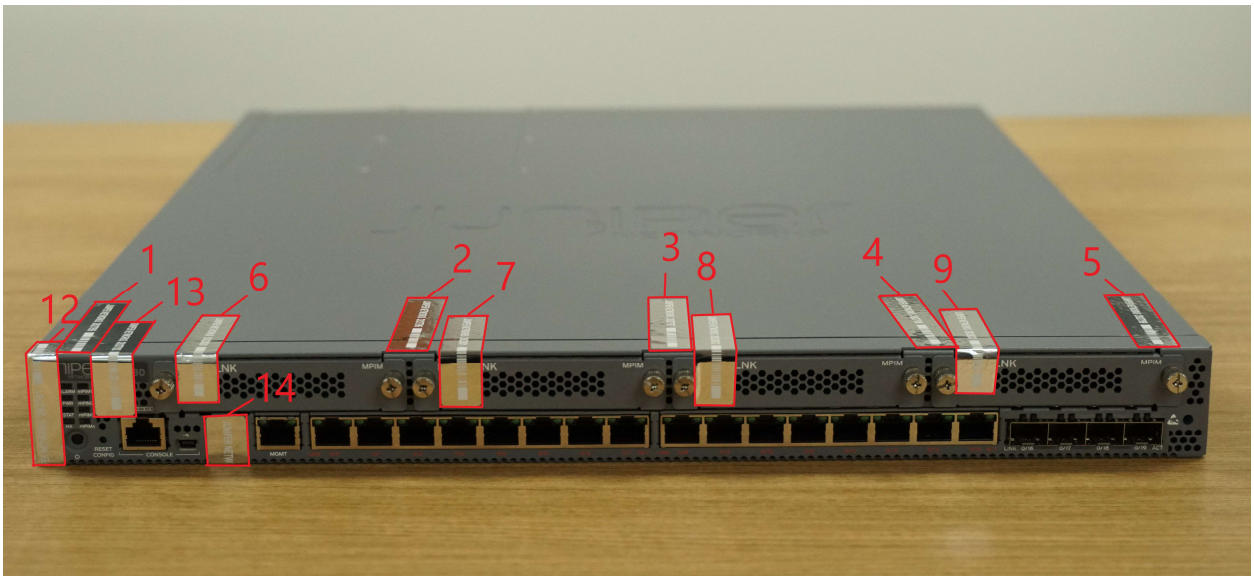
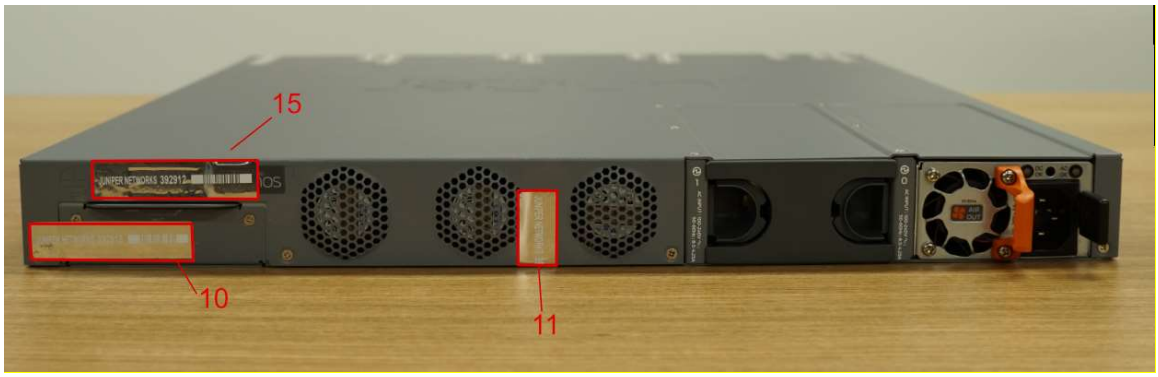


Figure 10 – SRX 380 Tamper-Evident Seal Placement (Rear)

TEL10 covering the blank faceplate, TEL11 placed vertically wrapping around onto the base of the device and TEL15 across the grounding connection.



5.3 SRX345 (23 seals)

Tamper evident seals must be applied to the following locations:

- Five (5) seals (TEL 1-5). Applied to the top of the chassis, covering one of the five chassis screws each.
- Four (4) seals (TEL 6-9). Applied vertically covering the front I/O Slots. TEL 6 shall also be used to cover the front USB data port. All shall wrap around the top of the device.

- Two (2) seals (TEL 10 & 11). Applied to the rear panel, one covering the blank faceplate, the other placed vertically next to the right-most fan vent. Both shall wrap around onto the base of the device.
- Six (6) seals (TEL 12-17). Applied to cover the chassis screws on the left-hand side of the device.
- Six (6) seals (TEL 18-23). Applied to cover the chassis screws on the right-hand side of the device.

Figure 11 – SRX345 Tamper-Evident seal placement (Front)

TEL 1-5 covering each of the five chassis screws. TEL 6-9 covering the front I/O Slots with TEL 6 also covering the USB data port.

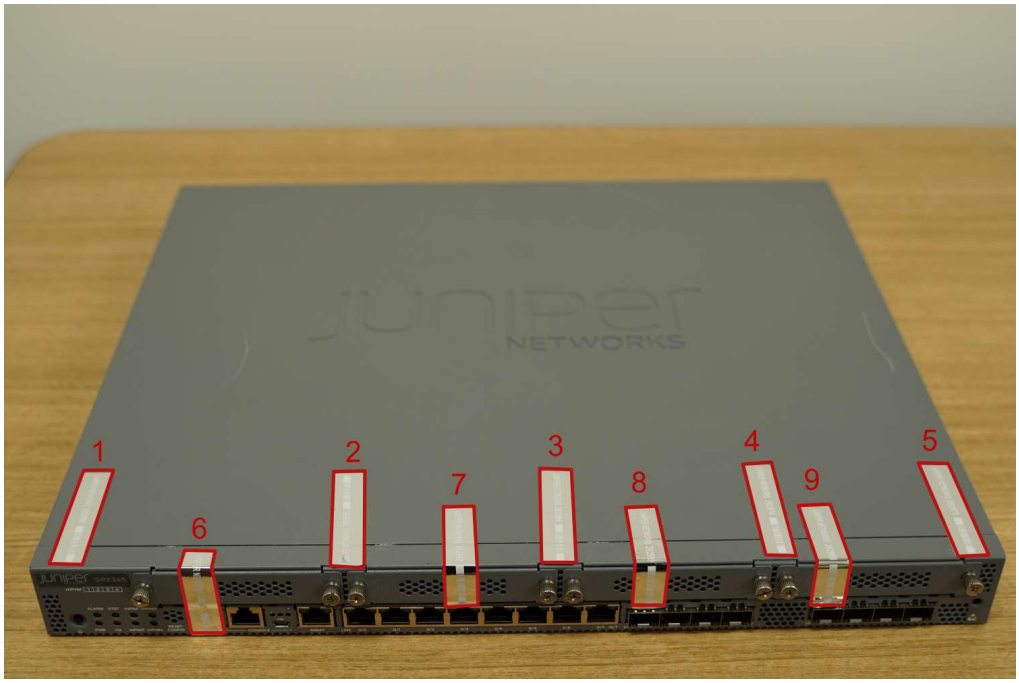


Figure 12 – SRX 345 Tamper-Evident Seal Placement (Rear)

TEL 10 covering the blank faceplate, TEL 11 placed vertically wrapping around onto the base of the device.

Figure 13 – SRX 345 Tamper-Evident seal placement (LHS)

TEL 12-17 covering the chassis screws on the left-hand side of the device.

Figure 14 – SRX345 Tamper-Evident seal placement (RHS)

TEL 18-23 covering the chassis screws on the right-hand side of the device.

5.4 SRX345 Dual-AC (23 seals)

Tamper evident seals must be applied to the following locations.

- Four (4) seals (TEL 1-4). Applied vertically covering the front I/O Slots. TEL 1 shall also be used to cover the front USB data slot. All shall wrap around the top of the device.
- Five (5) seals (TEL 5-9). Applied to the top of the chassis, covering one of the five chassis screws each.
- Two (2) seals (TEL 10 & 11). Applied to the rear panel, one covering the blank faceplate, the other placed vertically next to the AC power-input. Both shall wrap around onto the base of the device.
- Six (6) seals (TEL 12-17). Applied to cover the chassis screws on the left-hand side of the device.
- Six (6) seals (TEL 18-23). Applied to cover the chassis screws on the right-hand side of the device.

Figure 15 – SRX345 Dual-AC Tamper-Evident seal placement (Front)

TEL 1-4 covering the front I/O slots with TEL 1 also covering the USB data port.

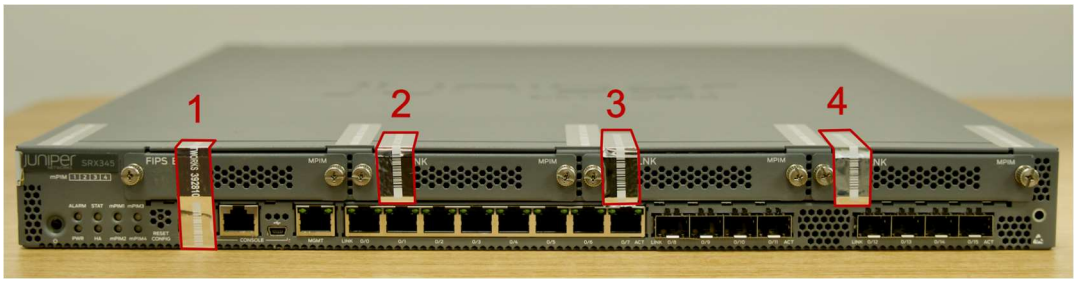


Figure 16 – SRX345 Dual-AC Tamper-Evident seal placement (Top)

TEL 5-9 covering each of the five chassis screws.

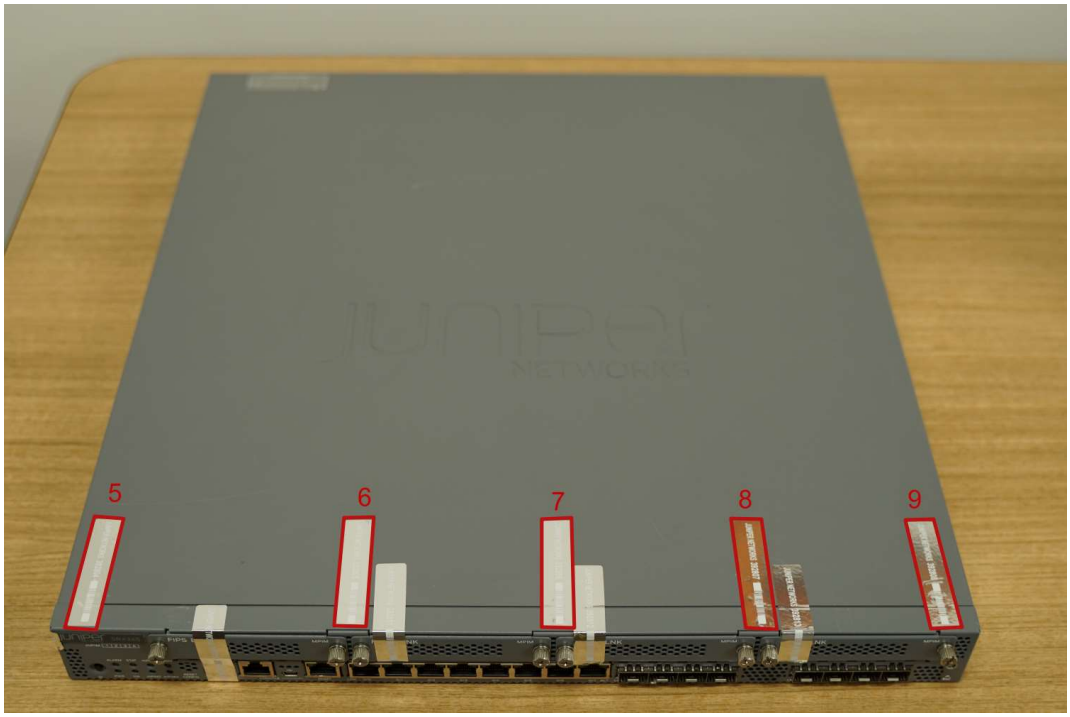


Figure 17 – SRX345 Dual-AC Tamper-Evident Seal Placement (Rear)

TEL 11 covering the blank faceplate, TEL 10 placed vertically wrapping around onto the base of the device.

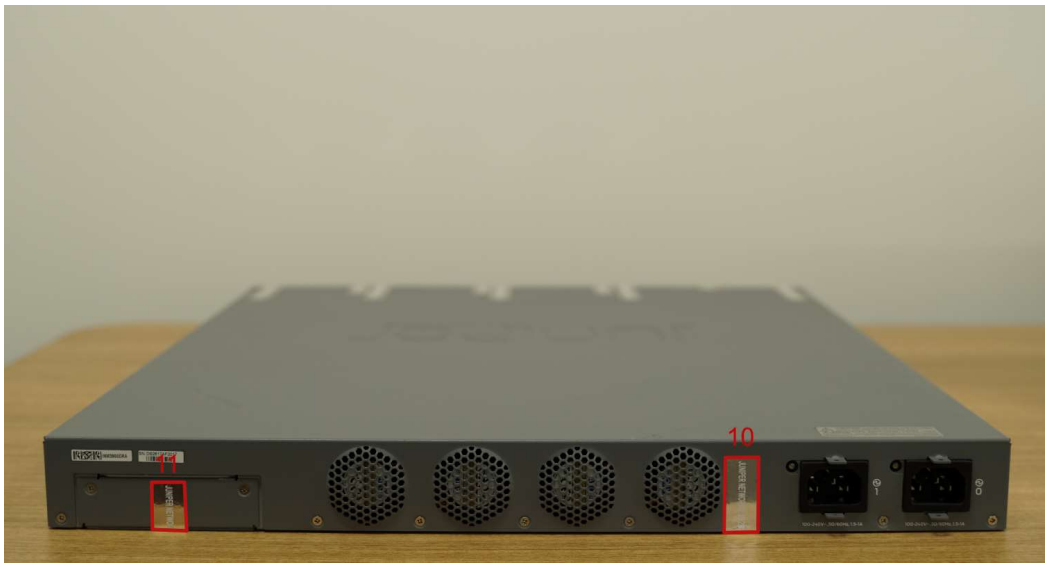


Figure 18 – SRX345 Dual-AC Tamper-Evident seal placement (LHS)

TEL 12-17 covering the chassis screws on the left-hand side of the device.

Figure 19 - SRX345 Dual-AC Tamper-Evident seal placement (RHS)

TEL 18-23 covering the chassis screws on the right-hand side of the device.

5.5 SRX1500 (8 seals)

Tamper evident seals must be applied to the following locations:

- Two (2) seals (TEL 1 & 2). Applied vertically to the front of the chassis, one covering the USB port and the other covering the High Availability (HA) port. Both of these shall also cover part of the front I/O slot.
- Two (2) seals (TEL 3 & 4). Applied vertically covering the front I/O Slots and wrapping around to the top of the device.

- Two (2) seals (TEL 5 & 6). Applied to the rear panel, one covering the blank faceplate and wrapping around the bottom of the device, the other placed vertically between the right-most and second-right-most fan vent and wrapping around onto the top of the device.
- One (1) seals (TEL 7). Applied to cover the chassis screw on the left-hand side of the device. This should wrap around the bottom of the device.
- One (1) seals (TEL 8). Applied to cover the chassis screw on the right-hand side of the device. This should wrap around the bottom of the device.

Figure 20 – SRX1500 Tamper-Evident seal placement (Front)

TEL 1 - 2 covering the USB data port and the HA port, in addition to part of the front I/O slot; TEL 3 - 4 covering the front I/O Slots.

Figure 21 – SRX1500 Tamper-Evident seal placement (Rear)

TEL 6 covering the blank faceplate; TEL 5 between the two fan vents wrapping around on top of the device.

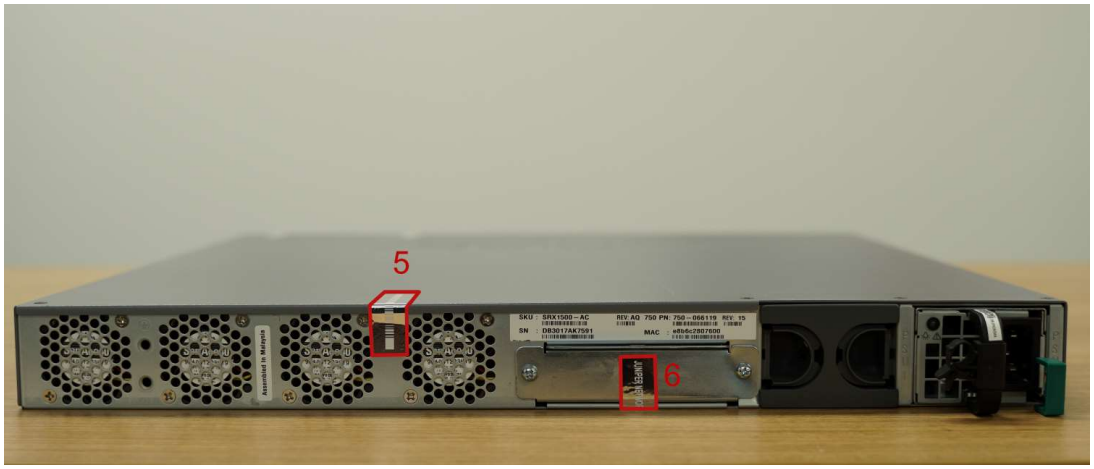


Figure 22 – SRX1500 Tamper-Evident seal placement (LHS)

TEL 7 covering cover the chassis screw on the left-hand side.

Figure 23 – SRX1500 Tamper-Evident seal placement (RHS)

TEL 8 covering cover the chassis screw on the right-hand side.

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. Use of Triple-DES in this module is only allowed until December 31st, 2023, as per [SP800-131A]. 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 2, 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*
[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*
[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
[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
[133]	National Institute of Standards and Technology, Recommendation for Cryptographic Key Generation, Special Publication 800-133, Revision 1, July 2019

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 – Datasheet

Model	Title	URL
SRX345, SRX345-DUAL-AC, SRX380	SRX300 Line of Services Gateways for the Branch	https://www.juniper.net/assets/uk/en/local/pdf/datasheets/1000550-en.pdf
SRX1500	SRX1500 Services Gateway	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000551-en.pdf