Juniper Networks
RE1800 and RE2600 Routing Engines
Cryptographic Modules

Non-Proprietary Security Policy

Document Version: 0.9

Date: August 6, 2015

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

List of Tables

1. Module Overview

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks RE1800 and RE2600 Routing Engines Cryptographic Modules from Juniper Networks. The Juniper Networks RE1800 and RE2600 Routing Engines, hereafter referred to as RE or cryptographic module, are multi-chip embedded cryptographic modules that control a router or switch's interfaces, chassis components, system management, and user access to the device. The RE runs Junos 14.1R4 with the FIPS mode utilities, a software package that restricts Junos Operating System to FIPS approved algorithms.

The RE is compatible with the Juniper Networks MX Series 3D Universal Edge, EX Series Switches, T Series Routers, M Series Multiservice Edge Routers, and PTX Series Packet Transport Routers. These devices provide dedicated high-performance processing for flows and sessions and integrate advanced security capabilities that protect the network infrastructure as well as user data.

The cryptographic module consists of one of the Routing Engines listed in the table below with firmware version Junos 14.1R4 with the FIPS mode utilities (also version 14.1R4).

Table 1 Platform and Routing Engine Hardware P/Ns

Series	Platform	Routing Engine Hardware P/N
MX	MX240	RE-S-1800X2-XXG or RE-S-1800X4-XXG (XX = 8, 16 or 32 GB memory)
	MX480	
	MX960	
	MX2010	
	MX2020	
EX9200	EX9204	RE-S-EX9200-1800X4-XXG (XX = 8, 16 or 32 GB memory) *Note: This part is also known as the EX9200-RE*
	EX9208	
	EX9214	
T	T640	RE-DUO-C1800-16G
	T1600	
	T4000	
M	M7i	RE-B-1800X1-4G

Series	Platform	Routing Engine Hardware P/N
	M10i	
	M120	RE-A-1800X2-XXG (XX = 8 or 16 GB)
	M320	
PTX	PTX3000	RE-DUO-C2600-16G
	PTX5000	
Tamper Evident Seal		**Part Number**
		520-052564

Images of the Cryptographic Modules

The physical forms of the module in all configurations are depicted in Figure 1 through Figure 5. The cryptographic boundary is surfaces and edges of the RE assembled printed circuit card assembly. The module relies on the chassis backplane and modular I/O subsystem cards for input and output.

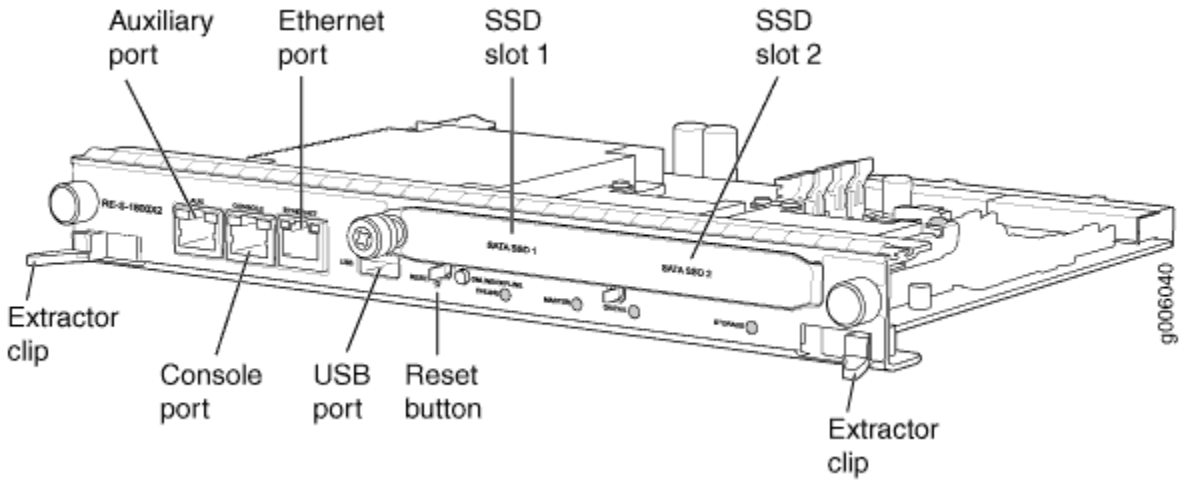

Figure 1 RE-S-1800X2-XXG, RE-S-1800X4-XXG, and RE-S-EX9200-1800X4-XXG Physical Form

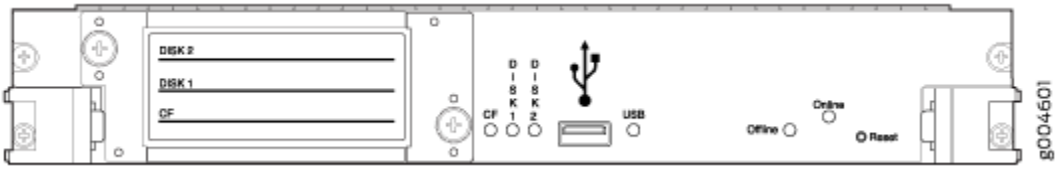

Figure 2 RE-DUO-C1800-16G Physical Form

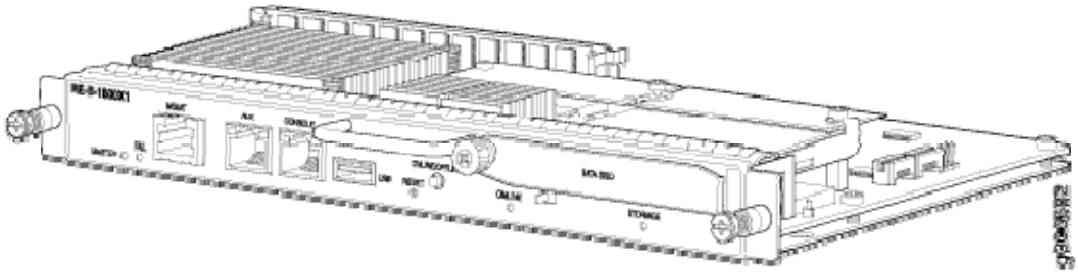

Figure 3 RE-B-1800X1-4G Physical Form

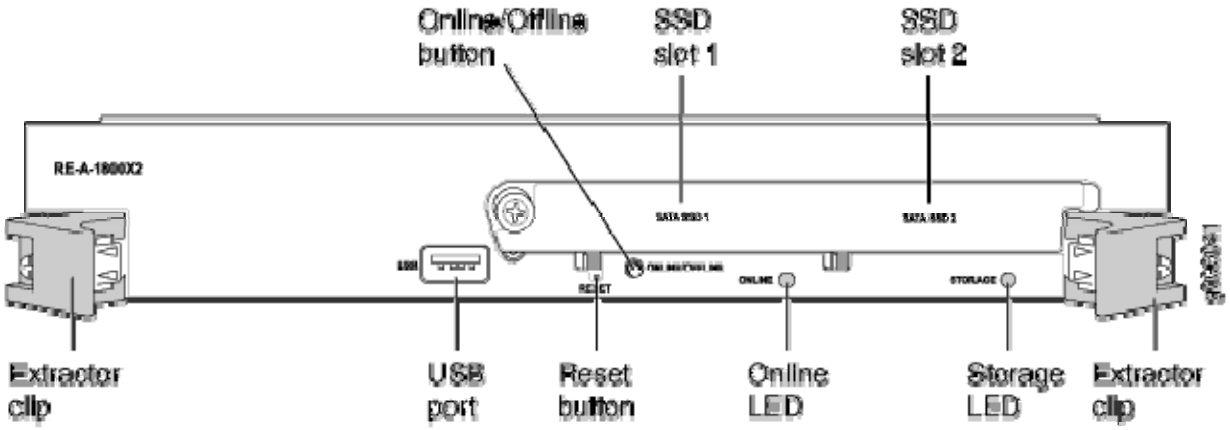

Figure 4 RE-A-1800X2-XXG Physical Form

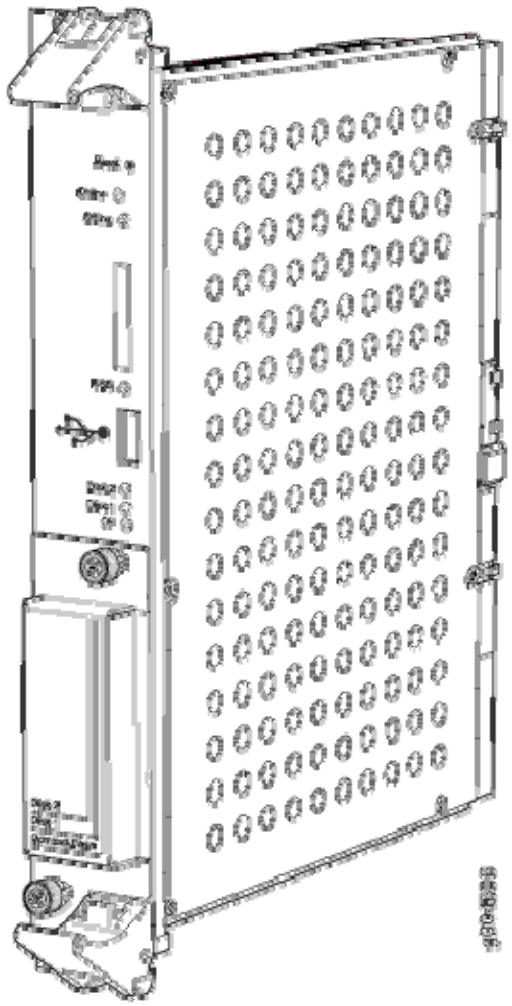

Figure 5 RE-DUO-C2600-16G Physical Form

2. Security Level

The cryptographic modules meet the overall requirements applicable to Level 1 security of FIPS 140-2. The following table lists the level of validation for each area in FIPS 140-2:

Table 2- Security Level per FIPS 140-2 Individual Sections

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved Mode of Operation

Once the Junos 14.1R4 firmware image and FIPS mode utilities are installed on the device, integrity and self-tests have run successfully, and the Crypto-Officer has performed the FIPS configuration; the module is operating in the approved mode. The Crypto-Officer must ensure that the backup image of the firmware is also Junos 14.1R4 with the FIPS mode utilities by issuing the request system snapshot command. The Crypto-Officer must also run the command “set system fips level 1” or “set system fips level 2”. The module only supports FIPS Level 1; however, the level 2 command was retained for backwards compatibility with scripts. Both commands put the module into a single approved mode of operation.

The Crypto-Officer can verify that the cryptographic module is in FIPS mode by observing the console prompt. When operating in FIPS mode, the prompt will read “<user>@<device name>:fips#” (e.g. admin@routing_engine:fips#). The Crypto-Officer can also use the “show system fips level” command to determine if the module is operating in FIPS mode.

The cryptographic module supports a non-Approved mode of operation. When in the non-approved mode of operation, the console prompt does not include “:fips”. The non-approved mode of operation enables unencrypted methods of communicating with the module (i.e., telnet, Rlogin, FTP, Finger, RSH and TFTP).

The FIPS Approved mode of operation supports the following FIPS Approved algorithms[1]:

Table 3 FIPS Approved Algorithms

Algorithm Implementation	Reference	Mode	Functions	Strength	Cert
OpenSSL TDES	SP 800-20	TCBC	SSH Enc/Dec	112	1880
OpenSSL AES	FIPS 197, SP 800-38A	CBC, CTR	SSH Enc/Dec	128, 192, 256	3296
OpenSSL SHA	FIPS 180-4	1, 256, 512	Hash for HMAC, Sig Gen, Sig Ver	128, 256	2736
OpenSSL HMAC	FIPS 198-1	1, 256, 512	SSH HMAC Gen/Ver, Password HMAC Gen/Ver	128, 256, 256	2094
OpenSSL ECDSA	FIPS 186-4	P-256	SSH KeyGen, SSH SigGen, Package SigVer	128	639
		P-256, P-384, P-521	SSH SigVer	128, 192, 256	639
OpenSSL RSA	FIPS 186-4	2048	Package SigVer	112	1685
OpenSSL SSH KDF	SP 800-135	SSHv2	SSH Key Derivation	112, 128, 192, 256[2]	CVL 470
OpenSSL DRBG	SP 800-90A	HMAC-SHA-256	Random Bit Generation	256	752
Kernel TDES	SP 800-20	TCBC	IPsec (ESP) Enc/Dec	112	1879
Kernel SHA	FIPS 180-4	1, 256	Hash for HMAC	128, 256	2734
Kernel HMAC	FIPS 198-1	1, 256	IPsec (ESP) HMAC Gen/Ver	128, 256	2092
MD SHA	FIPS 180-4	1, 256	Hash Generation (Power-Up Integrity)	128, 256	2735

[1] The user of the module should review the Algorithm Transition Tables, available at the CMVP website (http://csrc.nist.gov/groups/STM/cmvp/) to determine the current status of algorithms and key lengths used in the module.
[2] The strength of the SSH KDF is the minimum of the Key Agreement method and the HMAC used.

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

- Non-SP 800-56A Compliant Diffie-Hellman and EC Diffie-Hellman – [IG D.8] Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 192 bits of encryption strength).
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- Non-Deterministic Random Number Generators (NDRNG) used as input for entropy and to seed the Approved HMAC-DRBG
- HMAC-SHA-1-96 (HMAC Certs. #2092 and #2094) – [IG A.8] Hash Message Authentication Code truncated to 96-bits. Allowed for use in FIPS mode when an Approved algorithm is not required.

The cryptographic module supports the commercially available SSHv2 protocol for key establishment in accordance with FIPS 140-2 Annex D.

Placing the Module in the Approved Mode of Operation

The cryptographic officer shall place the module in FIPS Approved mode by following the instruction in the *Junos OS for EX Series Ethernet Switches, Release 14.1R4 FIPS* or *Junos OS for M, MX, PTX, and T Series Routers, Release 14.1R4: FIPS* document.

The operator can verify that the module is in FIPS Approved mode by observing the CLI prompt in Operational Mode and Configuration Modes which will have the format “<user>@<device name>:fips” where the device name is configured in under host-name. The Crypto-Officer can also use the “show system fips level” command to determine if the module is operating in FIPS mode.

Non-FIPS Mode of Operation

The module has a Non-Approved mode of operation. If the module has been in a FIPS Approved mode of operation, the cryptographic officer can configure the module to run in a Non-Approved mode by following the instruction in the *Junos OS for EX Series Ethernet Switches, Release 14.1R4 FIPS* or *Junos OS for M, MX, PTX, and T Series Routers, Release 14.1R4: FIPS.*

The Non-Approved mode of operation supports the same algorithms that are supported in the Approved mode of operation. The Non-Approved mode of operation enables unencrypted methods of communicating with the module (i.e. telnet, Rlogin, FTP, Finger, RSH and TFTP). The module zeroizes all CSPs before transitioning to the Non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module supports the physical ports and corresponding logical interfaces identified below. The flow of the data, control and status through the interfaces is controlled by the cryptographic module. The interfaces can be categorized into following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Out Interface

- Control Input Interface
- Status Output Interface
- Power Interface

The physical ports can be mapped to the logical interfaces. The mapping of the logical interfaces to the physical ports is shown in the following table:

Table 4- FIPS 140-2 Ports/Interfaces

FIPS 140-2 Logical Interface	Physical Port
Data Input	Ethernet, Serial, Backplane
Data Output	Ethernet, Serial, Backplane
Control Input	Ethernet, Serial, Backplane
Status Output	Ethernet, Serial, LED, Backplane
Power Interface	Backplane
N/A Disabled	USB, AUX

The flow of input and output of data, control, and status is managed by the cryptographic module. Details of each model's hardware are available in the guides listed in Table 5.

Table 5 –Hardware Guides

Model	Document Title	Download location
MX240	MX240 3D Universal Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx240/index.pdf
MX480	MX480 3D Universal Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx480/index.pdf
MX960	MX960 3D Universal Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx960/index.pdf
MX2010	MX2010 3D Universal Edge Router Hardware	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-

	Guide	series/mx2010/index.pdf
MX2020	MX2020 3D Universal Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx2020/index.pdf
EX9204	Complete Hardware Guide for EX9204 Ethernet Switches	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/topic-collections/hardware/ex-series/ex9200/book-hw-ex9204.pdf
EX9208	Complete Hardware Guide for EX9208 Ethernet Switches	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/topic-collections/hardware/ex-series/ex9200/book-hw-ex9208.pdf
EX9214	Complete Hardware Guide for EX9214 Ethernet Switches	https://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/topic-collections/hardware/ex-series/ex9200/book-hw-ex9214.pdf
T640	T640 Core Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/t-series/t640/index.pdf
T1600	T1600 Core Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/t-series/t1600/index.pdf
T4000	T4000 Core Router Hardware Guide	http://junos.com/techpubs/en_US/release-independent/junos/information-products/pathway-pages/t-series/t4000/index.pdf
M7i	M7i Multiservice Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/m-series/m7i/index.pdf
M10i	M10i Multiservice Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/m-series/m10i/index.pdf
M120	M120 Multiservice Edge Router Hardware Guide	https://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/m-series/m120/index.pdf
M320	M320 Multiservice Edge Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/m-series/m320/index.pdf
PTX3000	PTX3000 Packet Transport Router Hardware Guide	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ptx-series/ptx3000/index.pdf
PTX5000	PTX5000 Packet Transport Router	http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ptx-

	Hardware Guide	series/ptx5000/index.pdf

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports operator roles as follows:

- Cryptographic Officer (CO)
- User
- RE-to-RE

Table 6- Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Via Console: Username and password Via SSH-2: Username and Password or ECDSA signature verification
Cryptographic Officer	Identity-based operator authentication	Via Console: Username and password Via SSH-2: Username and Password or ECDSA signature verification
RE-to-RE	Identity-based operator authentication	Pre-shared keys The RE role uses pre-shared keys for secure communication.

Table 7- Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and password	The module enforces 10-character passwords (at minimum) chosen from the 96 human readable ASCII characters. The module enforces a timed access mechanism as follows: For the first two failed attempts (assuming 0 time to process), no timed access is enforced. Upon the third attempt, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous (e.g. 4^{th} failed attempt = 10-second delay, 5^{th} failed attempt = 15-second delay, 6^{th} failed attempt = 20-second delay, 7^{th} failed attempt = 25-second delay). This leads to a maximum of 7 possible attempts in a one-minute period for each console session (getty). The best approach for the attacker would be to disconnect after 4 failed attempts, and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. Thus the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a one-minute period is $9/(96^{10})$, which is less than 1/100,000.
ECDSA signature	The module supports SSH ECDSA (P-256, P-384, and P-521 curves) which have a minimum equivalent computational resistance to attack of 2^{128}. Thus the probability of a successful random attempt is $1/2^{128}$, which is less than 1/1,000,000. The module can negotiate approximately 5.6e7 SSH connection in one minute; therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{128})$, which is less than 1/100,000.
RE-to-RE pre-shared keys	The module uses 160-bit or 256-bit HMAC keys for RE-to-RE authentication. Thus the probability of a successful random attempt is $1/(2^{160})$, which is less than 1/1,000,000. The module can negotiate approximately 54,347,880 IPsec connections per minute; therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $54,347,880/(2^{160})$, which is less than 1/100,00.

6. Access Control Policy - Roles and Services

Crypto Officer Role

The Crypto-Officer (CO) configures and monitors the module via a console or SSH connection. The cryptographic Officer has permission to view and edit secrets within the module. Descriptions of the services available to the Crypto-Officer role are provided in the Table 8.

User Role

The User role accesses the module's cryptographic services that include monitoring the Routing Engine via the console or SSH. The User Role may not change the configuration. Table 8 lists the services available to the User Role.

RE-to-RE Role

The RE (Routing Engine) role provides for communication with a redundant RE in the switch to enable failover capabilities. Communication between two (2) REs is performed using a secure IPSsec protocol. Note: All REs support the RE-to-RE role; however, the M7i chassis only physically houses a single RE, so the RE-to-RE role cannot be utilized with the M7i chassis.

Table 8- Services Authorized for Roles in Approved FIPS mode

Role	Authorized Services
User: Monitors the Routing Engine via the console, SSH.	Status Checks: Allows the user to get the current status of the Routing Engine. SSH-2: Provides encrypted login via the SSH-2 protocol. Console Access: Provides direct login access via the console.
Cryptographic Officer: Configures and monitors the Routing Engine via the console, SSH.	Configuration Management: Allows the CO to configure the Routing Engine. Routing Engine Control: Allows the CO to modify the state of the Routing Engine. (Example: shutdown, reboot) Status Checks: Allows the CO to get the current status of the Routing Engine. Zeroize: Allows the CO to zeroize the configuration (all CSPs) within the module. Load Juniper image: Allows the verification and loading of a new validated firmware image into the Routing Engine. Note: Loading of non-validated firmware invalidates the module's FIPS 140-2 validation. SSH-2: Provides encrypted login via the SSH-2 protocol. Console Access: Provides direct login access via the console. Account Management: Allows the crypto-officer to create other administrative accounts. Self-tests: Allows the crypto-officer to perform cryptographic self-tests by restarting the module. Change Mode: Configure the module to run in a non-Approved mode.
RE-to-RE Role	Configuration Management: Allows propagation of configuration database to the backup RE Routing Engine Control: Allows the master RE to control the state of the backup RE. Status Checks: Allows the user to get the current status of the Routing Engine Secure Transport: Allows the master RE to communicate with the backup RE using secure a IPSec connection

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module (LEDs).

Non-FIPS Mode Services

The cryptographic module supports the following services in a non-FIPS Approved mode of operation in addition to all the services that are listed above as available in the FIPS Approved mode of operation:

- Change Mode- Configure the module to run in a FIPS Approved mode: Enabled by crypto-officer
- Telnet and Rlogin, FTP, Finger, RSH, TFTP: configurable by crypto-officer

Table 9 - Definition of Critical Security Parameters (CSPs)

CSP	Description	Zeroizaton	Use
SSH-2 Private Host Key	The first time SSH-2 is configured, the key is generated according to FIPS 186-4 using the SP800-90A HMAC DRBG. Used to identify the host. ECDSA (P-256)	Zeroize command	Used to identify the host.
SSH-2 Session Keys	Session keys used with SSH-2. Encryption: TDES (3key), AES 128, 192, 256 generated by the SSHv2 KDF MACs: HMAC SHA-2-256, HMAC-SHA1, HMAC SHA2-512, HMAC SHA1-96 generated by the SSHv2 KDF Key Exchange: DH Group exchange (2048 ≤ key ≤ 8192), ECDH Prime curve NID_secp521r1 (NIST Curve P-521) generated according to FIPS 186-4 using the SP800-90A HMAC DRBG	Power Cycle & Session Termination	Symmetric key used to encrypt data between host and client HMAC keys used to for data integrity DH keys used to establish symmetric and HMAC keys
User Authentication Key	Hash of the User's password. SHA-1, SHA-256, SHA-512	Zeroize command	Used to authenticate user to the module
CO Authentication Key	Hash of the CO's password. SHA-1, SHA-256, SHA-512	Zeroize command	Used to authenticate CO to the module
RE-to-RE Authentication Key	HMAC Key (Manual IPsec SA) 160-bit key with 96 bit truncated MAC or 256-bit key	Zeroize/Explicit Delete command	Used to authenticate the RE-to-RE

CSP	Description	Zeroizaton	Use
	This key can be output in in plaintext over the console port.		connection
RE-to-RE Encryption Key	TDES key (Manual IPsec SA). This key can be output in plaintext over the console port.	Zeroize/Explicit Delete command	Used in IPSec connection between RE's
HMAC DRBG Seed	Seed for DRBG generated by the NDRNG.	Seed is not stored by the module	For seeding DRBG
HMAC DRBG V value	The value *V* of *outlen* bits, which is updated each time another *outlen* bits of output are produced	Power Cycle	A critical value of the internal state of DRBG
HMAC DRBG Key value	The current value of key. The *outlen*-bit *Key*, which is updated at least once each time that the DRBG mechanism generates pseudorandom bits	Power Cycle	A critical value of the internal state of DRBG
NDRNG entropy	Internal state of the NDRNG. Used to generate the HMAC DRBG Seed	Power Cycle	Entropy input to HMAC DRBG

Table 10 - Definition of Public Keys

Key	Description/Usage
SSH-2 Public Host Key	First time SSH-2 is configured, the key is generated. ECDSA (P-256). Identifies the host.
User Authentication Public Keys	Used to authenticate users to the module. ECDSA (P-224, P-256, P-384, P-521)
CO Authentication Public Keys	Used to authenticate CO to the module. ECDSA (P-224, P-256, P-384, P-521)
Juniper Root CA	RSA 2048-bit X.509 certificate or ECDSA prime256v1 X.509 V3 Certificate Used to verify the validity of the Engineering CA.
Engineering CA	RSA 2048-bit X.509 certificate or ECDSA prime256v1 X.509 V3 Certificate Used to verify the validity of the Package CA.
Package CA	RSA 2048-bit X.509 certificate or ECDSA prime256v1 X.509 V3 Certificate Used to verify the validity of the PackageProduction Certificate.

PackageProduction Certificate	RSA 2048-bit X.509 certificate or ECDSA prime256v1 X.509 V3 Certificate Certificate that holds the public key of the signing key that was used to generate all the signatures used on the packages and signature lists.
DH and ECDH Public Keys	Used within SSH-2 for key establishment.

Definition of CSP Modes of Access

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 11- CSP Access Rights within Roles & Services

Role			Service	Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete, G=Generate
CO	User	RE-to-RE		
X			Configuration Management	All CSPs (**R, W, D**) SSH-2 Private Host Key (**W, D, G**)
		X	Configuration Management	All CSPs(R,W)
X		X	Routing Engine Control	No access to CSPs
X	X	X	Status Checks	No access to CSPs
X			Zeroize	All CSPs (**D**)
X			Load Juniper Image	No access to CSPs
X	X		SSH-2	SSH-2 session key (**R, G**)
X	X		Console Access	CO Authentication Key, User Authentication Key (**R**)
X			Account Management	Creates or removes passwords (**W, D**)
X			Self-tests	No access to CSPs
X			Change Mode	All CSPs (**D**)
		X	Secure Transport	RE-to-RE Encryption Key, RE-to-RE Authentication Key (R)

7. Operational Environment

The FIPS 140-2 Operational Environment is a limited operational environment. The module's operating system is Junos OS version 14.1R4.

8. Security Rules

The cryptographic module design corresponds to the cryptographic module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of a FIPS 140-2 Level 1 module.

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The cryptographic module performs the following self-tests:

- Power-Up Self-Tests:
  - Cryptographic Algorithm Tests
    - OpenSSL TDES Encrypt Known Answer Tests (KAT)
    - OpenSSL TDES Decrypt KAT
    - OpenSSL AES Encrypt KAT
    - OpenSSL AES Decrypt KAT
    - OpenSSL HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 KATs
    - OpenSSL ECDSA Sign KAT
    - OpenSSL ECDSA Verify KAT
    - OpenSSL RSA Verify KAT
    - OpenSSL SSHv2 KDF KAT
    - OpenSSL FIPS SP 800-90A HMAC DRBG KAT
    - Kernel TDES Encrypt/Decrypt KATs
    - Kernel HMAC-SHA-1, HMAC-SHA-256 KATs
    - MD SHA-1 KAT
  - Firmware integrity test:
    - ECDSA signature verification (P-256, SHA-256)
    - Critical functions tests
    - Verification of Limited Environment

- Conditional self-tests:
  - Pairwise consistency tests
    - ECDSA pairwise consistency test (sign/verify)
  - Firmware load test: ECDSA signature verification (P-256, SHA-256) or RSA digital signature verification (2048-bit key)
  - Key entry test: Duplicate key entries test
  - Continuous random number generator test: performed on the Approved FIPS SP800-90A DRBG and the NDRNG before each use.

Any time the cryptographic module is in an idle state, the operator is capable of commanding the modules to perform the power-up self-test by power-cycling the module. Upon successful completion of self-tests, the module displays a solid “online LED” and displays “FIPS Self-tests Passed” on the console.

Data output is inhibited during key generation, self-tests, zeroization, and error states.

Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the modules.

The module requires two (2) independent internal actions to be performed prior to outputting plaintext CSPs.

The module does not support bypass.

The module supports concurrent operators.

The CO must maintain control of the module until the zeroization process completes successfully.

9. Physical Security Policy

The modules physical embodiment is that of a multi-chip embedded device that meets the FIPS 140-2 Level 1 physically security requirements. The module is composed of commercial grade components.

A tamper evident seal must be installed over the USB port. The tamper evident seal will show evidence if the USB port is used. See Crypto Officer Guidance for placement and instructions on applying the tamper evident seal. The tamper seal has not been tested to FIPS 140-2 requirements.

10. Mitigation of Other Attacks Policy

The module does not implement mitigations for any other attacks.

11. Guidance

Crypto-Officer Guidance

Enabling FIPS Approved Mode of Operation

The crypto-officer is responsible for initializing the module in a FIPS Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The crypto-officer should follow the steps found in the *Junos OS for EX Series Ethernet Switches, Release 14.1R4 FIPS* or *Junos OS for M, MX, PTX, and T Series Routers, Release 14.1R4: FIPS* document Chapter 2. The crypto-officer must apply the tamper evident label(s) on the module for a FIPS Approved mode of operation.

Placing the Module in a Non-Approved Mode of Operation

As Crypto Officer, the operator may need to disable FIPS mode of operation on the routing engine to return it to non-FIPS operation. To disable FIPS mode on the routing engine follow the steps found in the *Junos OS for EX*

Series Ethernet Switches, Release 14.1R4 FIPS or *Junos OS for M, MX, PTX, and T Series Routers, Release 14.1R4: FIPS* document Chapter 2 in the section titled Disabling FIPS Mode.

Tamper Evident Labels

The Routing Engine requires one (1) tamper evident seal over the USB port to operate in a FIPS Approved mode of operation. The crypto-officer can obtain tamper evident seals from Juniper Networks using the part number **520-052564**.

The crypto-officer is responsible for applying and checking the seal on the routing engine periodically to verify the security of the module is maintained.

Tamper Evident Seal Instructions
Each routing engine platform requires a tamper-evident seal on its USB port. For all seal applications, follow these general instructions:

1. Handle the seal with care. Do not touch the adhesive side. Do not cut a seal to make it fit.
2. Make sure all surfaces to which the seal are applied are clean and dry and clear of any residue.
3. Apply the seal with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

Routing Engine Tamper-Evident Seal Application

Apply one tamper-evident seal to the USB port to secure routing engine cryptographic module.

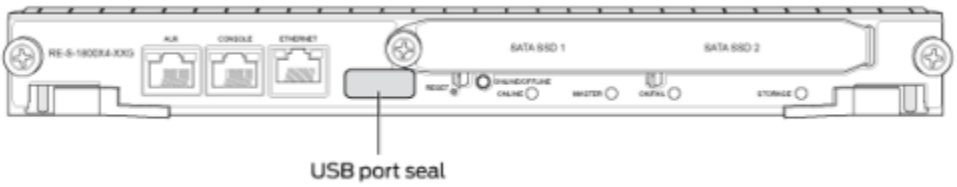

Figure 6: Example Tamper-Evident Seal Location on a RE-S-1800X4-XXG

User Guidance

The user should verify that the module is operating in the desired mode of operation (FIPS Approved mode or Non-Approved mode) by displaying the FIPS level currently on the switch. A switch enabled in FIPS Approved mode is at level 1 or 2 (there is no difference between 1 and 2). A switch in the Non-Approved mode is at level 0.

Display the FIPS level currently on the switch

```
[edit]
root@switch:fips# show system fips level
```

12. Acronyms

Table 12- Acronyms

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
CLI	Command-Line Interface
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
RSA	Public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman.
SHA-1	Secure Hash Algorithms
SSH	Secure Shell
TCP	Transmission Control Protocol
TDES	Triple - Data Encryption Standard
UDP	User Datagram Protocol

About Juniper Networks

Juniper Networks was founded on a simple but incredibly powerful vision for the future of the network: "Connect everything. Empower everyone."

We believe the network is the single greatest vehicle for knowledge, understanding, and human advancement the world has ever known. We are dedicated to uncovering new ideas and creating the innovations that will serve the exponential demands of the networked world. To do this, we're leading the charge to architecting the new network, built on simplicity, security, openness and scale.