

Juniper Networks SRX650 Services Gateway

Security Policy

Document Version: 1.0

Date: April 4, 2012



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

Table of Contents

| | |
|---|----|
| Table of Contents | 2 |
| List of Tables | 2 |
| 1. Module Overview | 4 |
| 2. Security Level | 5 |
| 3. Modes of Operation | 5 |
| Approved Mode of Operation..... | 5 |
| Placing the Module in the Approved Mode of Operation..... | 6 |
| Non-FIPS Mode of Operation | 6 |
| 4. Ports and Interfaces | 6 |
| 5. Identification and Authentication Policy | 6 |
| Assumption of Roles | 6 |
| 6. Access Control Policy..... | 9 |
| Roles and Services..... | 9 |
| Unauthenticated Services..... | 9 |
| Definition of Critical Security Parameters (CSPs) | 10 |
| Definition of Public Keys | 11 |
| Definition of CSP Modes of Access..... | 12 |
| 7. Operational Environment..... | 12 |
| 8. Security Rules..... | 12 |
| 9. Physical Security Policy | 13 |
| Physical Security Mechanisms | 13 |
| Tamper Seal Placement | 14 |
| 10. Cryptographic Algorithm Validation | 16 |
| 10. Mitigation of Other Attacks Policy | 17 |
| 11. Acronyms..... | 18 |
| About Juniper Networks | 18 |

List of Tables

| | |
|--|----|
| Security Level | 5 |
| Hardware Guide | 6 |
| Roles and Required Identification and Authentication | 6 |
| Strengths of Authentication Mechanisms | 8 |
| Services Authorized for Roles | 9 |
| Table of CSPs | 10 |
| Table of Public Keys..... | 11 |
| CSP Access Rights within Roles & Services | 12 |
| Inspection/Testing of Physical Security Mechanisms..... | 14 |
| Cryptographic Algorithm Validation Certificates..... | 16 |

| | |
|-----------------------------------|----|
| Mitigation of Other Attacks | 17 |
|-----------------------------------|----|

1. Module Overview

Juniper Networks SRX650 Services Gateway is a secure router that provides essential capabilities that 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 SRX Series Services Gateways, including products scaled for the branch, campus and data center applications, are powered by Juniper Networks JUNOS —the proven operating system that provides unmatched consistency, better performance with services, and superior infrastructure protection at a lower total cost of ownership.

The Juniper Networks SRX650 runs JUNOS-FIPS, a version of JUNOS created specifically for FIPS compliance. The validated version of JUNOS-FIPS is 11.2S4; the image is `junos-srxsme-11.2S4-fips.tgz`.

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware on the Juniper Networks SRX650 gateway. The cryptographic boundary for the SRX650 is the outer edge of the chassis. The cryptographic module's operational environment is a limited operational environment. The hardware part numbers for the SRX650 are SRX650-BASE-SRE6-645AP and SRX650-BASE-SRE6-645DP.

Figure 1 depicts the SRX650 without tamper seals. For depictions of the units with tamper seals, see section 9.

Figure 1: SRX650



2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Security Level

| Security Requirements Section | Level |
|---|-------|
| Cryptographic Module Specification | 2 |
| Module Ports and Interfaces | 2 |
| Roles, Services and Authentication | 2 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

3. Modes of Operation

Approved Mode of Operation

The cryptographic module supports FIPS-Approved algorithms as follows:

- AES 128, 192, 256 for encryption/decryption
- DSA with 1024-bit keys for digital signature generation and verification
- RSA with 1024 or 2048-bit keys for digital signature generation and verification
- Triple-DES for encryption/decryption
- SHA-1 for hashing
- SHA-2 for hashing (SHA-256)
- HMAC-SHA-1
- HMAC-SHA-256
- FIPS 186-2 RNG (with Change Notice)

The cryptographic module also supports the following non-Approved algorithms which are allowed for use in FIPS mode:

- RSA with 1024-bit keys (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- Diffie-Hellman with 1536-bit keys (key agreement; key establishment methodology provides 96 bits of encryption strength)

The cryptographic module supports the commercially available IKEv1, and SSH protocols for key establishment in accordance with FIPS 140-2 Annex D.

The cryptographic module contains a non-FIPS validated deterministic random number generator (RNG) that is compliant with the FIPS 186-2.

Placing the Module in the Approved Mode of Operation

To be operating in the approved mode of operation, the following must have occurred:

1. The JUNOS-FIPS firmware image `junos-srxsme-11.2S4-fips.tgz` has been installed on the device and has successfully run its integrity and self-tests.
2. The Crypto-Officer must ensure that the backup image of the firmware is also a JUNOS-FIPS image by issuing the `request system snapshot` command.
3. The tamper evident seals shall be installed for the module to operate in the FIPS Approved mode of operation. See section 9. Physical Security Policy.

No further configuration is necessary for the purpose of placing it in FIPS mode.

Non-FIPS Mode of Operation

The cryptographic module does not provide a non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module supports the following physical ports and corresponding logical interfaces:

- **Ethernet:** Data Input, Data Output, Control Input, Status Outputs
- **Serial:** Control Input, Status Outputs.
- **Power interface:** Power Input
- **Reset:** Control Input
- **LEDs:** Status Output

The flow of input and output of data, control, and status is managed by the cryptographic module. Details of the hardware are available in the guide listed below.

Hardware Guide

| Model | Document Title | Download location |
|--------|-----------------------|---|
| SRX650 | SRX650 Hardware Guide | http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/hardware/SRX650/HW/index.html |

Control input options and status output (not provided by the hardware) are described in the *JUNOS Monitoring and Troubleshooting Guide, Release 11.2* which is available for download at: http://www.juniper.net/techpubs/en_US/junos11.2/information-products/topic-collections/security/software-all/monitoring-and-troubleshooting/index.html.

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports two distinct operator roles as follows:

- Cryptographic Officer (CO)
- User (read-write)
- User (read-only)

The cryptographic module enforces the separation of roles using role and identity-based operator authentication. Identity-based authentication is performed through an authentication database internal to the module; role-based authentication occurs when an external authentication server (e.g. RADIUS or TACACS) is used.

Roles and Required Identification and Authentication

| Role | Type of Authentication | Authentication Data |
|---|--|--|
| Cryptographic Officer | Identity-based operator authentication | Via Console: Username and password Via SSH: Password or RSA/DSA signature verification when using public-key authentication |
| | Role-based authentication | Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters |
| User (read-write) and User (read-only) | Identity-based operator authentication | Via Console: Username and password Via SSH: Password or RSA/DSA signature verification when using public-key authentication |
| | Role-based authentication | Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters |

Strengths of Authentication Mechanisms

| Authentication Mechanism | Strength of Mechanism |
|------------------------------|--|
| Username and password | <p>The module enforces 10-character passwords (at minimum) chosen from the 96+ human readable ASCII characters.</p> <p>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).</p> <p>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.</p> |
| RSA signature | <p>The module supports RSA (1024 or 2048-bit), which has a minimum equivalent computational resistance to attack of either 2^{80} or 2^{112} depending on the modulus size. Thus the probability of a successful random attempt is $1/(2^{80})$ or $1/(2^{112})$, which are both less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{80})$ or $5.6e7/(2^{112})$, which are both less than 1/100,000.</p> |
| DSA signature | <p>The module supports DSA (1024-bit only) which have an equivalent computational resistance to attack of 2^{80}. Thus the probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{80})$, which is less than 1/100,000.</p> |

6. Access Control Policy

Roles and Services

Services Authorized for Roles

| Role | Authorized Services |
|--|---|
| Cryptographic Officer: 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 | <p><u>Configuration Mode:</u> Allows the CO to configure the gateway.</p> <p><u>Operational Mode:</u> Allows the user to modify the state of the gateway. (Example: shutdown, reboot)</p> <p><u>Status Checks:</u> Allows the user to get the current status of the gateway, including logs and statistics.</p> <p><u>Zeroize:</u> Allows the user to zeroize the configuration (all CSPs) within the module.</p> <p><u>SSH:</u> Provides encrypted login via the SSH protocol.</p> <p><u>Console Access:</u> Provides direct login access via the console.</p> <p><u>Self-tests:</u> Allows the user to perform cryptographic self-tests by restarting the module.</p> <p><u>Account Management:</u> Allows the user to create other administrative accounts.</p> <p><u>Tamper Seals:</u> Ordering, installing, maintaining, storing and examining tamper-evident seals.</p> |
| User (read-only): Configures and monitors the gateway via console or SSH. May not change the configuration. | <p><u>Configuration Mode:</u> Allows the user to view the gateway configuration.</p> <p><u>Operational Mode:</u> Allows the user to modify the state of the gateway. (Example: shutdown, reboot)</p> <p><u>Status Checks:</u> Allows the user to get the current status of the gateway, including logs and statistics.</p> <p><u>SSH:</u> Provides encrypted login via the SSH protocol.</p> <p><u>Console Access:</u> Provides direct login access via the console.</p> <p><u>Self-tests:</u> Allows the user to perform cryptographic self-tests by restarting the module.</p> |
| User (read-write): Configures and monitors the gateway via console or SSH. May change the configuration. | <p><u>Configuration Mode:</u> Allows the user to configure the gateway.</p> <p><u>Operational Mode:</u> Allows the user to modify the state of the gateway. (Example: shutdown, reboot)</p> <p><u>Status Checks:</u> Allows the user to get the current status of the gateway, including logs and statistics.</p> <p><u>Zeroize:</u> Allows the user to zeroize the configuration (all CSPs) within the module.</p> <p><u>SSH:</u> Provides encrypted login via the SSH protocol.</p> <p><u>Console Access:</u> Provides direct login access via the console.</p> <p><u>Self-tests:</u> Allows the user to perform cryptographic self-tests by restarting the module.</p> |

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module
- Routing Protocols: Unauthenticated routing protocols (e.g., TCP, UDP)
- SNMP Traps (Status)

Definition of Critical Security Parameters (CSPs)

Table of CSPs

| CSP | Description |
|--------------------------------|---|
| SSH Private Host Key | The first time SSH is configured, the key is generated. RSA, DSA. Used to Identify the host. 1024-bit or 2048-bit length. |
| SSH Session Key | Session keys used with SSH, TDES (3 key), AES 128, 192, 256, HMAC-SHA-1 key (160), DH Private Key 1024 |
| User Authentication Key | HMAC-SHA-1 Key SHA-1 hash of user password with hard-coded salt value. Used to authenticate the user to the module. |
| CO Authentication Key | HMAC-SHA-1 Key SHA-1 hash of user password with hard-coded salt value. Used to authenticate the CO to the module. |
| IPsec SAs | Session keys used within IPsec. TDES (3 key), HMAC-SHA-1 |
| DH Private Key | Diffie-Hellman 1536-bit private key used in IKE and SSH protocol exchange |
| Approved RNG State | RNG seed and seed key |
| SNMPv3 security key | Key used for privacy and/or authentication by SNMPv3 (AES, DES, 3DES, HMAC SHA-1) |
| RADIUS shared secret | Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block |
| TACACS+ shared secret | Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block |

Definition of Public Keys

Table of Public Keys

| Key | Description/Usage |
|--|--|
| SSH Public Host Key | First time SSH is configured, the key is generated. RSA (1024 or 2048-bit), DSA. Identifies the host. |
| User Authentication Public Keys | Used to authenticate a user to the module via SSH. RSA (1024 or 2048-bit) or DSA |
| CO Authentication Public Keys | Used to authenticate the CO to the module via SSH. RSA (1024 or 2048-bit) or DSA |
| JuniperRootCA | RSA 2048-bit X.509 certificate Used to verify the validity of the Juniper image at software load and also at runtime for integrity. |
| PackageCA | RSA 2048-bit X.509 certificate Used to verify the validity of the Juniper image at software load and also at runtime for integrity. |
| DH Public Keys | Used within IKE and SSH for key establishment. |

Definition of CSP Modes of Access

Table 8 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

CSP Access Rights within Roles & Services

| Role | | | Service | Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete |
|------|-----------|-----------|--------------------|--|
| CO | User (RO) | User (RW) | | |
| X | | | Configuration Mode | All CSPs (R, W, D) |
| | X | | Configuration Mode | Read access to CSPs (R) |
| | | X | Configuration Mode | All CSPs except changing other account passwords (R, W, D) |
| X | | | Account Management | Creates or removes passwords (W, D) |
| X | X | X | Operational Mode | No access to CSPs |
| X | X | X | Status Checks | No access to CSPs |
| X | | X | Zeroize | All CSPs (D) |
| X | X | X | SSH | SSH session key (R) |
| X | X | X | Console Access | CO Authentication Key, User Authentication Key (R) |
| X | X | X | Self-tests | No access to CSPs |
| X | | | Tamper Seals | No access to CSPs |

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module has a limited operational environment.

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 2 module.

The cryptographic module provides three distinct operator roles. These are the User (read-write) role, User (read-only) role and the Cryptographic Officer role.

The cryptographic module supports both role-based and identity-based authentication mechanisms.

Authentication of identity to an authorized role is required for all services that modify, disclose, or substitute CSPs, use Approved security functions, or otherwise affect the security of the cryptographic modules.

The cryptographic module performs the following tests:

- Power up tests

- Cryptographic algorithm tests
 - Hardware (IPSec acceleration):
 - TDES KAT
 - AES KAT
 - SHA-1 KAT
 - SHA-256 KAT
 - HMAC-SHA-1 KAT
 - HMAC-SHA-256 KAT
 - Software (general purpose):
 - TDES KAT
 - AES KAT
 - SHA-1 KAT
 - SHA-256 KAT
 - HMAC-SHA-1 KAT
 - HMAC-SHA-256 KAT
 - RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
 - DSA pairwise consistency test (sign/verify) and KAT
 - FIPS 186-2 RNG KAT
 - KDF KATs
- Firmware integrity test:
 - RSA digital signature verification (PKCS1.5, 2048-bit key, SHA-1) and SHA-1 hash verification
- Conditional tests
 - Pairwise consistency tests
 - RSA pairwise consistency test (sign/verify and encrypt/decrypt)
 - DSA pairwise consistency test (sign/verify)
 - Firmware load test: RSA digital signature verification (2048-bit key)
 - Manual key entry test: Duplicate key entries test
 - Continuous random number generator test: performed on the Approved FIPS 186-2, Appendix 3.1 RNG, and on a non-Approved RNG that is used to seed the Approved RNG.
 - Bypass test is not applicable.

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.

Prior to each use, the internal RNG is tested using the continuous random number generation conditional test.

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 supports concurrent operators.

9. Physical Security Policy

Physical Security Mechanisms

The modules physical embodiment is that of a multi-chip standalone device that meets Level 2 Physical Security requirements. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow observation of any kind to any component contained within the physically contiguous cryptographic boundary. Tamper evident seals are used to provide evidence in

case the modules are physically tampered with. Tamper evident seals must be applied by the Cryptographic Officer to operate as FIPS 140-2 Approved modules. Seals are available for order from Juniper using part number JNPR-FIPS-TAMPER-LBLS.

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.

Tamper seals are applied in the same fashion regardless of the part number of the device.

Inspection/Testing of Physical Security Mechanisms

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|--|--|---|
| Tamper labels, opaque metal enclosure. | Upon receipt of the module and per security policy by the Cryptographic Officer. | Labels should be free of any tamper evidence. |

Tamper Seal Placement

Seal 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.
- All surfaces to which the seals are to be applied must be prepared by sanding lightly with 200 grit sandpaper to roughen the surface. Use an alcohol wipe to ensure that all surfaces are clean and clear of any residue.
- Apply with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

If a tamper seal is to be replaced, the Crypto Officer must follow the above instructions to prepare the surface prior to applying the new seal.

SRX650 (19 seals)

Tamper evident seals shall be applied to the following locations (see highlighted pointers):

- The front of the module:
 - Label #1 horizontally across the left edge of slot cover plate #1, extending on to the front of the chassis.
 - Label #2 horizontally across the left edge of slot cover plate #2, extending on to the front of the chassis.
 - Label #3 vertically across the left edge of slot cover plates #3 and #4, extending on to the bottom of the chassis.
 - Label #4 vertically across the right edge of slot cover plates #1 and #2, extending on to the top of the chassis.
 - Label #5 vertically from the bottom of the chassis across the right edges of slot cover plates #3 and #4, overlapping with the bottom of label #4.
 - Label #6 vertically across the left edges of slot cover plates #5 and #6, extending on to the top of the chassis.
 - Label #7 vertically from the bottom of the chassis across the left edge of slot cover plates #7 and #8, overlapping with the bottom of label #6.
 - Label #8 horizontally across the right edge of slot cover plate #5, extending on to the right side of the chassis.
 - Label #9 horizontally across the right edge of slot cover plate #6, extending on to the right side of the chassis.
 - Label #10 horizontally across the right edge of slot cover plate #7, extending on to the right side of the chassis.

- Label #11 horizontally across the right edge of slot cover plate #8, extending on to the right side of the chassis.
- The left side of the module:
 - Label #12 vertically from the side of the chassis on to the bottom of the chassis.
- The right side of the module:
 - Label #13 vertically from the side of the chassis on to the bottom of the chassis.
- The rear of the module:
 - Label #14 vertically from the top of the chassis, extending on to the top power supply or cover plate.
 - Label #15 vertically from the bottom of the chassis, extending across the bottom power supply, overlapping with label #14.
 - Label #16 vertically from the top of the chassis, extending on to the central part of the top slot cover plate.
 - Label #17 vertically from the bottom of the chassis, extending on to the central part of the installed card and overlapping with label #16.
 - Label #18 vertically from the top of the chassis, extending on to the air filter cover plate.
 - Label #19 vertically from the bottom of the chassis, extending on to the air filter cover plate and overlapping with label #18.



Figure 1. SRX650 Tamper Evident Seal Locations (Front)



Figure 2. SRX650 Tamper Evident Seal Location (Left Side)



Figure 3. SRX650 Tamper Evident Seal Location (Right Side)



Figure 4. SRX650 Tamper Evident Seal Location (Rear)

10. Cryptographic Algorithm Validation

Cryptographic Algorithm Validation Certificates

| Algorithm | Software (General purpose) | Hardware (IPSec) |
|-------------------------------------|----------------------------|------------------|
| AES-CBC 128/192/256 | 1960 | 1959 |
| 3DES-CBC | 1272 | 1271 |
| SHA-1, SHA-256 | 1719 | 1718 |
| HMAC SHA-1, HMAC SHA-256 | 1181 | 1180 |
| FIPS 186-2 RNG | 1029 | N/A |
| DSA 1024/2048 | 625 | N/A |
| RSA 1024/2048 | 1014 | N/A |

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks that are outside the scope of FIPS 140-2.

Mitigation of Other Attacks

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---------------|----------------------|----------------------|
| N/A | N/A | N/A |

11. Acronyms

| ACRONYM | DESCRIPTION |
|-------------------|---|
| AES | Advanced Encryption Standard |
| DSA | Digital Signature Algorithm |
| EMC | Electromagnetic Compatibility |
| FIPS | Federal Information Processing Standard |
| HMAC-SHA-1 | 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. The acronym stands for Rivest, Shamir, and Adelman. |
| SHA-1 | Secure Hash Algorithms |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| TACACS | Terminal Access Controller Access Control System |
| TDES | Triple - Data Encryption Standard |

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Copyright ©2012 Juniper Networks, Inc. May be reproduced only in its original entirety [without revision]

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.