

Junos-FIPS 10.4 L1 OS Cryptographic Module

Security Policy

For the M7i and M10i Routers

Document Version: 1.8

Date: June 12, 2012

Table of Contents

Table of Contents..... 2

List of Tables 2

1. Module Overview..... 3

2. Security Level 6

3. Modes of Operation..... 6

 Approved Mode of Operation 6

 Non-FIPS Mode of Operation 7

4. Ports and Interfaces..... 7

5. Identification and Authentication Policy..... 7

 Assumption of Roles 7

6. Access Control Policy 10

 Roles and Services 10

 Unauthenticated Services..... 11

 Definition of Critical Security Parameters (CSPs)..... 12

 Definition of Public Keys..... 14

 Definition of CSP Modes of Access 15

7. Operational Environment 16

8. Security Rules 16

9. Physical Security Policy 17

 Physical Security Mechanisms 17

10. Mitigation of Other Attacks Policy 17

11. Acronyms 17

Appendix A—Cryptographic Algorithm Validation (CAVS) Certificates 19

List of Tables

Table 1. Junos-FIPS 10.4 Series/Platform/RE..... 3

Table 2. Security Level 6

Table 3. Roles and Required Identification and Authentication 8

Table 4. Strengths of Authentication Mechanisms..... 9

Table 5. Services Authorized for Roles..... 10

Table 6. Table of CSPs 12

Table 7. Table of Public Keys..... 14

Table 8. CSP Access Rights within Roles & Services 15

Table 9. Mitigation of Other Attacks 17

1. Module Overview

The Junos-FIPS 10.4 L1 OS Cryptographic Module (Junos-FIPS 10.4) executes on a multiple-chip embedded routing engine in Juniper Networks M Series routers; M7i and M10i. The validated version of Junos-FIPS 10.4 is 10.4R5; the image is `junos-juniper-10.4R5.3-fips.tgz`. See Table 1 below for hardware platform specifics.

Junos-FIPS 10.4 is a release of the Junos operating system, the first routing operating system designed specifically for the Internet. Junos software is currently deployed in the largest and fastest-growing networks worldwide. A full suite of industrial-strength routing protocols, a flexible policy language, and a leading MPLS implementation efficiently scale to large numbers of network interfaces and routes.

Junos-FIPS 10.4 meets the requirements of the FIPS Publication 140-2. Junos-FIPS 10.4 is a firmware-only module designed to operate on Routing Engine (RE) hardware, which is equivalent to PC hardware. The cryptographic module's operational environment is a limited operational environment. The module's cryptographic boundary is the firmware installed on the RE-850-1536 card. The firmware is executed by the processor and the memory devices that contain the executable code and data. The firmware module was tested on the following hardware:

Table 1. Junos-FIPS 10.4 Series/Platform/RE

| Series | Platform | Routing Engine |
|----------|----------|---|
| M Series | M7i | RE-850-1536 - 850MHz processor with 1.5GB of memory |
| | M10i | RE-850-1536 - 850MHz processor with 1.5GB of memory |

Figure 1. Diagram of the Cryptographic Module

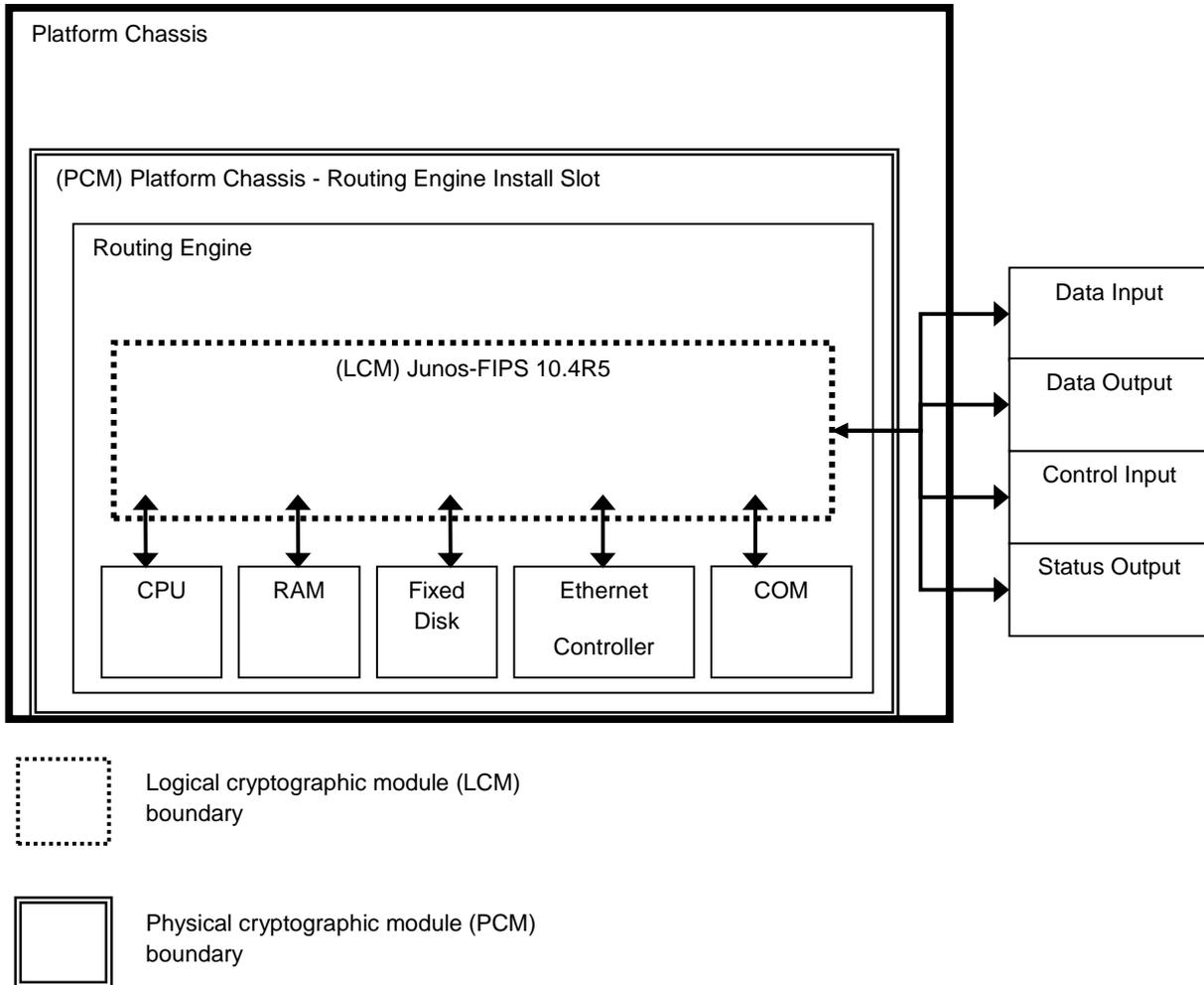
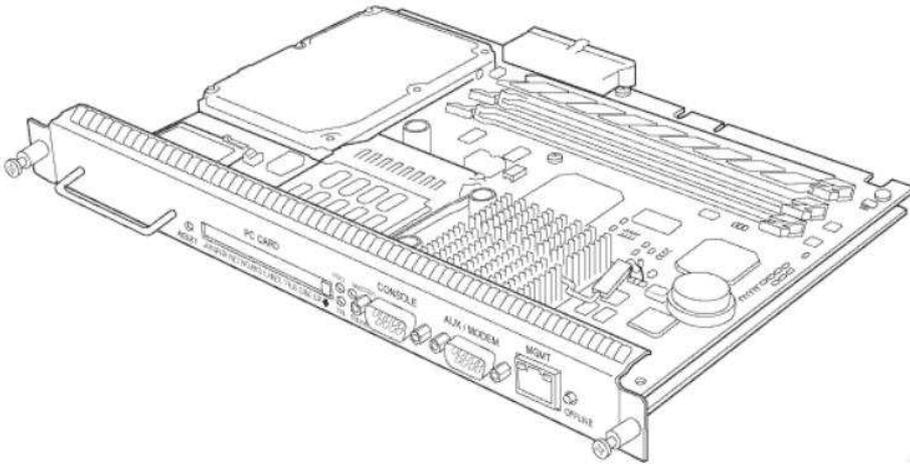


Figure 2 Image of RE-850-1536



2. Security Level

The cryptographic module, which is a multiple-chip embedded embodiment, meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2. Security Level

| Security Requirements Section | Level |
|------------------------------------|-------|
| Cryptographic Module Specification | 1 |
| Module Ports and Interfaces | 1 |
| Roles, Services and Authentication | 2 |
| 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

The cryptographic module supports FIPS-Approved algorithms as follows:

- AES 128, 192, 256 for encryption/decryption
- ECDSA with Curve P-192 for digital signature generation and verification
- 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 (three key) for encryption/decryption
- SHA-1 for hashing
- SHA-2 for hashing (SHA-224, SHA-256, SHA-384, SHA-512)
- HMAC-SHA-1
- HMAC-SHA-256
- AES-128-CMAC

- FIPS 186-2 RNG (with Change Notice)

The cryptographic module also supports the following non-Approved algorithms:

- RSA with 1024-bit keys (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- MD5 for message digests (used during authentication, for the purposes of protocol interoperability – see Protocol Peer entries in Tables 3, 4, 5 and 6)
- Diffie-Hellman with 1024-bit keys (key agreement; key establishment methodology provides 80 bits of encryption strength)
- Non-Approved RNG (used to seed Approved FIPS 186-2 RNG)

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

The cryptographic module relies on the implemented deterministic random number generator (RNG) that is compliant with FIPS 186-2 for generation of all cryptographic keys in accordance with FIPS 140-2 Annex C.

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:** Data Input, Data Output, Control Input, Status Outputs
- Power interface: Power Input
- **LEDs:** Status Output

The flow of input and output of data, control, and status is managed by the cryptographic module's defined service interfaces. These physical interfaces are mapped to the logical interfaces, which include SSH-2, TLS (Ethernet) and Console (Serial). The physical cryptographic boundary additionally supports a PC card slot. This port is not supported for use by the logical cryptographic module boundary.

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports six distinct operator roles as follows:

- User
- Cryptographic Officer (CO)
- AS2-FIPS PIC
- RE-to-RE
- IKE Peer
- Protocol Peer

The cryptographic module shall enforce the separation of roles using either identity-based or role-based operator authentication; the cryptographic module meets Level 2 requirements because identity-based authentication is not enforced for all authorized services.

Table 3. Roles and Required Identification and Authentication

| Role | Type of Authentication | Authentication Data |
|------------------------------|--|---|
| User | Identity-based operator authentication | <ul style="list-style-type: none"> • Via Console: Username and password • Via TLS: Username and password • Via SSH-2: Password or RSA signature verification or DSA signature verification |
| | Role-based authentication | <ul style="list-style-type: none"> • Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters |
| Cryptographic Officer | Identity-based operator authentication | <ul style="list-style-type: none"> • Via Console: Username and password • Via TLS: Username and password • Via SSH-2: Password or RSA signature verification or DSA signature verification |
| | Role-based authentication | <ul style="list-style-type: none"> • Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters |
| AS2-FIPS PIC | Identity-based operator authentication | Serial Number (6 bytes) and password (32 bytes) |
| RE-to-RE | Identity-based operator authentication | <p>Pre-shared keys</p> <p>The RE role will use pre-shared keys for secure communication.</p> |
| IKE Peer | Identity-based operator authentication | <p>IKE pre-shared keys</p> <p>Uses IKE to establish keys to be used by the PIC for IPsec communication with IPsec clients.</p> |
| Protocol Peer | Role-based authentication | <p>Will use pre-shared keys to send encrypted traffic. Uses TCP/UDP MD5 MAC only to authenticate operator.</p> <p>Alternatively, a manually configured IPsec SA can be used for authentication.</p> |

Table 4. 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 has 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> |
| AS2-FIPS PIC password | <p>The module supports 32 byte passwords to authenticate the PIC. Thus the probability of a successful random attempt is $1/(256^{32})$, which is less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one minute period is $5,084,005/(256^{32})$, which is less than 1/100,000.</p> |
| RE-to-RE pre-shared keys | <p>The module uses 160-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 probability of a success with multiple consecutive attempts in a one-minute period is $54,347,880/(2^{160})$, which is less than 1/100,000.</p> |

| Authentication Mechanism | Strength of Mechanism |
|--------------------------------------|--|
| IKE pre-shared keys | The module uses 160-bit HMAC keys for the PIC to use for IPsec communication with IPsec clients. Thus the probability of a successful random attempt is $1/(2^{160})$, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a one minute period is $54,347,880/(2^{160})$, which is less than 1/100,000. |
| Protocol peer pre-shared keys | The module supports TCP-MD5 with a 128-bit pre-shared key. Thus the probability of a successful random attempt is $1/(2^{128})$, which is less than 1/1,000,000. The probability of a success with multiple consecutive attempts in a one minute period is $54,347,880/(2^{128})$, which is less than 1/100,000. |

6. Access Control Policy

Roles and Services

Table 5. Services Authorized for Roles

| Role | Authorized Services |
|---|--|
| <p>User:</p> <p>Configures and monitors the router via the console, SSH-2, or TLS.</p> | <ul style="list-style-type: none"> • Configuration Management: Allows the user to configure the router. • Router Control: Allows the user to modify the state of the router. (Example: shutdown, reboot) • Status Checks: Allows the user to get the current status of the router. • SSH-2: Provides encrypted login via the SSH-2 protocol. • TLS: Provides encrypted login via the TLS protocol. • Console Access: Provides direct login access via the console. |
| <p>Cryptographic Officer:</p> <p>Configures and monitors the RE via the console, SSH-2, or TLS. Also has permissions to view and edit secrets within the RE.</p> | <ul style="list-style-type: none"> • Configuration Management: Allows the CO to configure the router. • Router Control: Allows the user to modify the state of the router. (Example: shutdown, reboot) • Status Checks: Allows the user to get the current status of the router. • Zeroize: Allows the user to zeroize the configuration (all CSPs) within the module. • Load New Software: Allows the verification and loading of new software into the router. Note: Loading of software invalidates the module’s FIPS 140-2 validation. • SSH-2: Provides encrypted login via the SSH-2 protocol. • TLS: Provides encrypted login via the TLS protocol. • Console Access: Provides direct login access via the console. |
| AS2-FIPS PIC | <ul style="list-style-type: none"> • Receives SAs: Allows the PIC to receive the SAs associated with a particular IPsec tunnel. • Secure IPC Tunnel: Allows the PIC to communicate with the RE using a secure tunnel. |

| Role | Authorized Services |
|--|--|
| <p>RE-to-RE</p> <p>The RE role is able to communicate with other REs to enable failover capabilities.</p> | <ul style="list-style-type: none"> • <u>Configuration Management</u>: Allows propagation of configuration database to the backup RE. • <u>Router Control</u>: Allows the master RE to control the state of the backup RE. • <u>Status Checks</u>: This service will allow the user to get the current status of the router (ports, number of packets, uptime, and so forth) • <u>Secure Transport</u>: Allows the master RE to communicate with the backup RE using a secure IPsec connection. • <u>Secure IPC Tunnel</u>: Allows the PIC to communicate with the RE using a secure tunnel. |
| <p>IKE Peer</p> <p>This role performs IKE negotiation with the RE.</p> <p>The IKE peer will create SAs for the AS2-FIPS PIC to use when using IPsec with a VPN client in cyberspace.</p> | <ul style="list-style-type: none"> • <u>Key Agreement</u>: Allows the negotiation of keys for use with an IPsec tunnel. |
| <p>Protocol Peer</p> <p>This role allows remote router to communicate with the RE via standard networking protocols. The supported routing protocols (BGP, ISIS, LDP, MSDP, OSPF, RIP2, RSVP, VRRP, and NTP) authenticate peers to each other for purpose of updating routing tables.</p> | <ul style="list-style-type: none"> • <u>Mutual Authentication</u>: Allows validating a known protocol peer. • <u>Protocol Exchange</u>: Allows the peers to communicate using an agreed-upon protocol. • <u>Secure Protocol Transport</u>: Allows IPsec connection between protocol peer and router. |

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- PIC Software Image Load: Downloads PIC software image to PIC.
- Receive Service Set Configuration: Allows the PIC to receive service set configuration database.
- Show Status: Provides the current status of the cryptographic module.
- Self-tests: Executes the suite of self-tests required by FIPS 140-2.
- Routing Protocols: Unauthenticated routing protocols (e.g., TCP, UDP)
- SNMP Traps (Status)

Definition of Critical Security Parameters (CSPs)

Table 6. Table of CSPs

| CSP | Description |
|--|--|
| SSH-2 Private Host Key | The first time SSH-2 is configured, the key is generated. DSA. Used to identify the host. |
| SSH-2 Session Key | Session keys used with SSH-2, TDES (3 key), AES 128, 192, 256, HMAC-SHA-1 key (160), DH Private Key 1024 |
| TLS Host Certificate, Private Portion | X.509 certificates for TLS for authentication. RSA or DSA |
| TLS Session Parameters | Session keys used with TLS, TDES (2 or 3 key), AES 128, 192, 256, HMAC-SHA-1; Pre-master Secret |
| User Authentication Key | HMAC-SHA-1 Key Used to authenticate users to the module. |
| CO Authentication Key | HMAC-SHA-1 Key Used to authenticate COs to the module. |
| IPsec SAs | Session keys used within IPsec. TDES (3 key), HMAC-SHA-1 |
| IKE Session Parameters | Nonces, DH Private Key 1024-bit keys, TDES, HMAC-SHA-1, used within IKE |
| Secure IPC (Internal) Session Key | TDES (3 Key) Used to communicate securely between the RE and the PIC |
| RE-to-RE Authentication Key | HMAC Key (Manual IPsec SA) 160 bit key with 96 bit truncated MAC. |
| RE-to-RE Encryption Key | TDES key (Manual IPsec SA) |
| Protocol Peer Authentication Keys | TCP-MD5 key to authenticate the routing peer role for the following protocols: BGP, ISIS, LDP, MSDP, OSPF, RIP2, RSVP, VRRP, NTP, APSCP |
| ASPIC password | 32 byte password |
| RADIUS shared secret | Used to authenticate COs and Users (10 chars minimum) |

| CSP | Description |
|------------------------------|--|
| | This includes the Authentication Data Block |
| TACACS+ shared secret | Used to authenticate COs and Users (10 chars minimum) This includes the Authentication Data Block |
| Manual SA for PIC | Entered into the RE, which is then passed over to the PIC for use by PIC with IPSEC |
| RNG Seed | Optional user input (XSEED) |
| RNG Seed-Key | Seed-key for RNG (XKEY) |

Definition of Public Keys

Table 7. Table of Public Keys

| Key | Description/Usage |
|--|---|
| SSH-2 Public Host Key | First time SSH-2 is configured, the key is generated. DSA. Used to identify the host. |
| TLS Host Certificate, Public Portion | X.509 certificates for TLS for authentication. RSA (1024 or 2048-bit) or DSA |
| User Authentication Public Keys | Used to authenticate users to the module. RSA (1024 or 2048-bit) or DSA |
| CO Authentication Public Keys | Used to authenticate CO to the module. 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. |
| EngineeringCA | 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. |
| PackageProduction | RSA 2048-bit X.509 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. |
| RE RSA Verify Key (Public Authentication key) | RSA 1024-bit key sent to the PIC to sign data to allow the PIC to authenticate to the RE by having the PIC sign data that is verified by the RE. |
| PIC RSA Verify (Public Authentication) Key | RSA 1024-bit key to allow the RE to authenticate to the PIC by signing data and having the PIC verify the signature. |
| PIC RSA Encrypt Key | RSA 1024-bit key used to encrypt the TDES session key. |
| RE RSA Encrypt Key | RSA 1024-bit key sent to the PIC; note that the PIC never uses this key. |
| DH Public Keys | Used within IKE and SSH-2 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:

Table 8. CSP Access Rights within Roles & Services

| Role | | | | | | Service | Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete |
|------|------|----------|--------------|----------|------------|-------------------------------------|--|
| CO | User | RE-to-RE | AS2-FIPS PIC | IKE Peer | Prot. Peer | | |
| X | | | | | | Configuration Management | All CSPs (R, W, D) |
| | X | | | | | Configuration Management | No access to CSPs |
| | | X | | | | Configuration Management | All CSPs (R, W) |
| X | X | X | | | | Router Control | No access to CSPs |
| X | X | X | | | | Status Checks | No access to CSPs |
| X | | | | | | Zeroize | All CSPs (D) |
| | | | X | | | Receives SAs | Relevant IPsec SAs (R) |
| | | | | X | | Key Agreement | IPsec SAs (R) |
| | | | | | X | Mutual Authentication | Relevant Authentication data: (R) |
| | | | | | X | Protocol Exchange (OSPF, VRRP, etc) | No access to CSPs |
| X | | | | | | Load New Software | No access to CSPs |
| X | X | | | | | SSH-2 | SSH-2 session key (R) |
| X | X | | | | | TLS | TLS session parameters (R) |
| X | X | | | | | Console Access | CO Authentication Key, User Authentication Key (R) |
| | | X | X | | | Secure IPC Tunnel | Secure IPC (Internal) Session Key (R) |

| Role | | | | | | Service | Cryptographic Keys and CSP Access Operation R=Read, W=Write, D=Delete |
|------|------|----------|--------------|----------|------------|---------------------------|--|
| CO | User | RE-to-RE | AS2-FIPS PIC | IKE Peer | Prot. Peer | | |
| | | X | | | | Secure transport | RE-to-RE Encryption Key, RE-to-RE Authentication Key (R) |
| | | | | | X | Secure Protocol transport | Protocol Peer Authentication Keys (R) |

7. Operational Environment

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

8. Security Rules

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

1. The cryptographic module shall provide six distinct operator roles. These are the User role, the Cryptographic Officer role, RE-to-RE role, AS2-FIPS PIC role, IKE Peer role, and Protocol Peer role.
2. The cryptographic module shall support both role-based and identity-based authentication mechanisms.
3. 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 module.
4. The cryptographic module shall perform the following tests:
 - Power up tests
 - A. Cryptographic algorithm tests
 - i. DES - KAT¹
 - ii. TDES - KAT
 - iii. AES - KAT
 - iv. AES - CMAC KAT
 - v. SHA-1 KAT
 - vi. SHA-224, 256, 384, 512 KAT
 - vii. HMAC-SHA-1 KAT
 - viii. HMAC-SHA-256 KAT
 - ix. ECDH KAT
 - x. ECDSA pairwise consistency test (sign/verify) and KAT
 - xi. RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
 - xii. DSA pairwise consistency test (sign/verify) and KAT
 - xiii. FIPS 186-2 RNG KAT
 - xiv. KDF-IKEv1 KAT
 - B. Firmware integrity test:
 - i. RSA digital signature verification (PKCS1.5, 2048-bit key, SHA-1) and SHA-1 hash verification

¹The DES function is used to implement TDES and is not otherwise available for use in the cryptomodule.

- C. Critical functions tests
 - i. Verification of Limited Environment
 - ii. Verification of Integrity of Optional Packages
- Conditional tests
 - D. Pairwise consistency tests
 - i. ECDSA Pairwise Consistency test
 - ii. RSA pairwise consistency test (sign/verify and encrypt/decrypt)
 - iii. DSA pairwise consistency test (sign/verify)
 - E. Firmware load test: RSA digital signature verification (2048-bit key)
 - F. Manual key entry test: duplicate key entries test
 - G. 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.
 - H. Bypass test is not applicable.
- 5. Any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test by power-cycling the module.
- 6. Prior to each use, the internal RNG shall be tested using the continuous random number generation conditional test.
- 7. Data output shall be inhibited during self-tests and error states.
- 8. Key generation, manual key entry and zeroization processes shall be logically isolated from data output.
- 9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- 10. The module shall support concurrent operators.
- 11. The Routing Engine hardware implements a PC card slot. The slot is not supported as an interface for use with the module's logical cryptographic boundary.
- 12. The Routing Engine must be installed in one of the approved platforms as listed in Table 1, per Juniper installation guidance.

9. Physical Security Policy

Physical Security Mechanisms

The Junos-FIPS 10.4 firmware module's physical embodiment, as represented by the tested platform, is a multi-chip embedded routing engine that meets Level 1 physical security requirements. The module implements production grade components.

10. Mitigation of Other Attacks Policy

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

Table 9. Mitigation of Other Attacks

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

11. Acronyms

| ACRONYM | DESCRIPTION |
|---------|-------------|
|---------|-------------|

| ACRONYM | DESCRIPTION |
|-------------------|---|
| AES | Advanced Encryption Standard |
| DES | Data Encryption Standard |
| DSA | Digital Signature Algorithm |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Standard |
| GMPLS | General Multiprotocol Label Switching |
| HMAC-SHA-1 | Keyed-Hash Message Authentication Code |
| IKE | Internet Key Exchange Protocol |
| IPsec | Internet Protocol Security |
| MD5 | Message Digest 5 |
| MPLS | Multiprotocol Label Switching |
| PIC | Physical Interface Card |
| RADIUS | Remote Authentication Dial-In User Service |
| RE | Routing Engine |
| RSA | Public-key encryption technology developed by RSA Data Security, Inc. The acronym stands for Rivest, Shamir, and Adelman. |
| SA | Security Association |
| SHA-1 | Secure Hash Algorithms |
| SSH-2 | Secure Shell |
| SSL | Secure Sockets Layer |
| TACACS | Terminal Access Controller Access Control System |
| TCP | Transmission Control Protocol |

| ACRONYM | DESCRIPTION |
|-------------|-----------------------------------|
| TDES | Triple - Data Encryption Standard |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |

Appendix A—Cryptographic Algorithm Validation (CAVS) Certificates

| | ALGORITHM | CAVS VALIDATION # |
|------------------|-----------|-------------------|
| RNG | RNG | 909 |
| SSH-IPSEC | AES | 1727 |
| | TDES | 1113 |
| | SHA | 1510 |
| | HMAC | 1002 |
| | AES | 1726 |
| Kernel | TDES | 1112 |
| | SHA | 1509 |
| | HMAC | 1001 |
| MD | SHA | 1508 |
| | HMAC | 1000 |
| OpenSSL | AES | 1719 |
| | TDES | 1106 |
| | DSA | 531 |
| | SHA | 1502 |
| | RSA | 847 |
| | HMAC | 994 |
| | ECDSA | 225 |

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

Copyright 2010 Juniper Networks, Inc. May be reproduced only in its 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 marks, 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.

Mon 2010