JUNOS-FIPS Firmware Module
Security Policy

Document *Version 1.8*

Juniper Networks

April 27, 2006

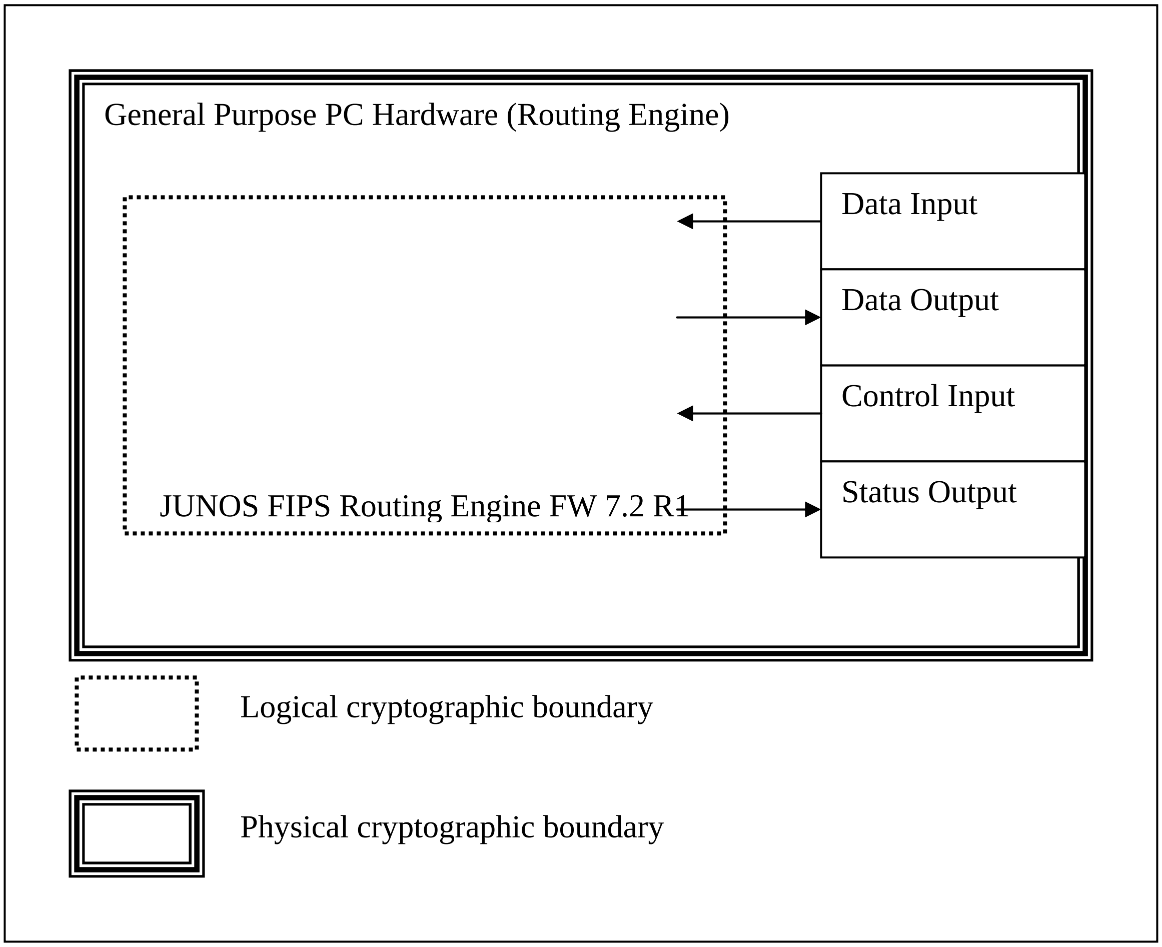
Table of Contents

1. Module Overview

JUNOS Firmware is the first routing operating system designed specifically for the Internet. It runs on all Juniper Networks T-series, M-series, and J-series routers, and is currently deployed in the largest and fastest-growing networks worldwide. Its full suite of industrial-strength routing protocols, flexible policy language, and leading MPLS implementation efficiently scale to large numbers of network interfaces and routes. As well, JUNOS software supports the industry's first production-ready GMPLS implementation.

JUNOS-FIPS (Versions 7.2R1.7 and 7.4R1.7) is a version of JUNOS designed to meet the requirements of the FIPS Publication 140-2. JUNOS-FIPS is targeted at security sensitive customers, and provides a limited operational environment. JUNOS-FIPS is a firmware only module capable of operating on a general purpose computing platform comprised of general purpose production grade components (e.g. Intel x86 CPU, RAM, printed circuit board, hard drive, etc.).

Figure 1 – Diagram of the Cryptographic Module


General Purpose PC Hardware (Routing Engine)
Data Input
Data Output
Control Input
Status Output
JUNOS FIPS Routing Engine FW 7.2 R1
Logical cryptographic boundary
Physical cryptographic boundary

2. Security Level

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

Table 1 - Module Security Level Specification

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

In FIPS mode, the cryptographic module supports FIPS Approved algorithms as follows:

- DSA with 1024 bit keys for digital signature generation and verification
- RSA with 2048 bit keys for digital signature generation and verification
- Triple-DES (three key) for encryption/decryption
- DES for encryption/decryption (transitional phase only – valid until May 19, 2007; for use with legacy systems only)
- AES 128, 192, 256 for encryption/decryption
- SHA-1 for hashing
- HMAC-SHA-1
- RNG

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

- RSA with at least 1024 bits keys for key wrapping (key wrapping, key establishment methodology provides 80 bits of encryption strength)

- MD5 for hashing (used during authentication)
- Diffie-Hellman (key agreement, key establishment methodology provides 80 bits of encryption)
- Non-Approved RNG (used to seed Approved FIPS 186-2 RNG)

The cryptographic module supports the commercially available TLS, IKE, and SSH protocols for key establishment.

The cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with FIPS 186-2 for generation of all cryptographic keys.

Non-FIPS mode of operation

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

4. Ports and Interfaces

The cryptographic module supports physical ports provided by the general purpose PC with the following mapping of logical interfaces:

- Ethernet: Data input, Data output, Control Input, Status Outputs
- Serial: Data input, Data output, Control Input, Status Outputs
- Power interface: Power Input

The flow of input and output of data, control and status is managed by the cryptographic module's API.

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports six distinct operator roles as follows:

- Crypto-Officer
- FIPS User
- 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 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
FIPS User	Identity-based operator authentication Role Based authentication	• Via Console: Username and Password • Via TLS: Username and Password • Via SSH: Password or RSA signature verification or DSA signature verification • Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters.
Crypto-Officer	Identity-based operator authentication Role Based authentication	• Via Console: Username and Password • Via TLS: Username and Password • Via SSH: Password or RSA signature verification or DSA signature verification • Via RADIUS or TACACS+: pre-shared secret, minimum 10 characters.
AS2-FIPS PIC	Identity-based operator	Serial Number (6 bytes)

	authentication	and Password (32 bytes)
RE to RE	Identity-based operator authentication	Pre-shared keys The RE role will use pre-shared keys for secure communication.
IKE Peer	Identity-based operator authentication	Uses IKE Pre-shared keys. Uses IKE to establish keys to be used by the PIC for IPSec communication with IPSec clients.
Protocol PEER	Role Based authentication	Will use pre-shared keys to send encrypted traffic. Uses TCP/UDP MD5 MAC to only authenticate operator. Alternatively, a manually configured IPSec SA can be used for authentication.

Table 3 – 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: 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 per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing a 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.
RSA Signature	The module supports RSA (2048 bit) which have a minimum equivalent computational resistance to attack of 2^112. Thus the probability of a successful random attempt is 1/ 2^112, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a one minute period is 5.6e7 / 2^112 which is less than 1/100,000.
DSA Signature	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 million. 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.
AS2-FIPS PIC Password	The module supports 32 byte passwords to authenticate the PIC. Thus the probability of a successful random attempt is 1/ 255^32, which is less than 1/1 million. The probability of a success with multiple consecutive attempts in a one minute period is 4,940,716 /255^32 which is less than 1/100,000.
RE to RE Pre-shared keys	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 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.
IKE Pre-shared keys	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 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 million. 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 4 – Services Authorized for Roles

Role	Authorized Services
User: Configures and monitors the router via the console, SSH, or TLS.	• Configuration Management: This service allows the User to configure the router. • Router Control: This service allows the user to modify the state of the router. (Example: Shutdown, reboot) • Status Checks: This service will allow the user to get the current status of the router. • SSH: This service provides encrypted login via the SSH protocol. • TLS: This service provides encrypted login via the TLS protocol. • Console Access: This service provides direct login access via the console.
Cryptographic-Officer: Configures and monitors the RE via the console, SSH, or TLS. Also has permissions to view and edit secrets within the RE.	• Configuration Management: This service allows the CO to configure the router. • Router Control: This service allows the user to modify the state of the router. (Example: Shutdown, reboot) • Status Checks: This service will allow the user to get the current status of the router. • Zeroize: This service allows the user to zeroize the configuration (all CSPs) within the module. • Load New Software: This service allows the verification and loading of new software into the router. • SSH: This service provides encrypted login via the SSH protocol. • TLS: This service provides encrypted login via the TLS

	protocol. • Console Access: This service provides direct login access via the console.
AS2-FIPS PIC	• 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.
RE to RE The RE role is able to communicate with other RE's to enable failover capabilities.	• Configuration Management: Allows propagation of configuration database to the backup RE. • Router Control: Allows the Master RE to control the state of the backup RE. • Status Checks: This service will allow the user to get the current status of the router (Ports, Number of Packet, Up Time, etc) • Secure Transport: Allows the Master RE to communicate with the Backup RE using a secure IPSEC connection.
IKE Peer This role performs IKE negotiation with the RE. The IKE peer will create SAs for the AS2-FIPS PIC to use when using IPSec with a VPN client in cyberspace.	• Key Agreement: Allows the negotiation of keys for use with an IPSec tunnel.
Protocol PEER 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, NTP) authenticate peers to each other for purpose of updating routing	• Mutual Authentication: Allows validating a known protocol peer. • Protocol Exchange: Allows the peers to communicate using an agreed upon protocol. • Secure Protocol Transport: Allows IPSec connection between Protocol Peer and router. • SNMPv3: Allows the Protocol peer to use SNMPv3 on the router. Note that the cryptography supported by SNMPV3 has only been implemented to support the underlying

tables.	protocol; no security attributes are attributed to the SNMPV3 functionality.

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: This service provides the current status of the cryptographic module.
- Self-tests: This service 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 5 – Table of CSPs

CSP	**Description**
SSH Private Host Key	*1st time SSH is configured the key is generated. RSA, DSA. Used to Identify the host.*
SSH Session Key	*Session keys used with SSH, TDES (3key), AES 128, 192, 256, HMAC-SHA-1 key (160), DH Private Key 1024 min.*
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-1Key* *Used to authenticate COs to the module.*

CSP	**Description**
IPSec SAs	*Session keys used within IPSec.* *TDES (3 key), HMAC-SHA-1*
IKE Session Parameters	*Nonces, DH Private Key 1024 bit minimum, TDES, HMAC-SHA-1, used within IKE*
Secure IPC (Internal) Session Key	*TDES (3Key)* *Used to communicate securely between the RE and the PIC*
RE to RE Authentication Key	*HMAC Key (Manual IPSecSA)* *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)*
TACACS+ shared secret	*Used to authenticate COs and Users (10 chars minimum)*
Manual SA for PIC	*Entered into the RE, which is then passed over to the PIC for use by PIC with IPSEC*

Definition of Public Keys

Table 6 – Table of Public Keys

Key	Description/Usage
SSH Public Host Key	*1st time SSH is configured the key is generated. RSA(>=1024 bit), DSA. Idenitfy the host.*
TLS Host Certificate, Public Portion	*X.509 Certificates for TLS for authentication. RSA (>=1024 bit) or DSA*
User Authentication Public Keys	*Used to authenticate users to the module. RSA (>=1024 bit) or DSA*
CO Authentication Public Keys	*Used to authenticate CO to the module. RSA (>=1024 bit) or DSA*
JuniperRootCA	*RSA 2048 bit X.509 Certificate* *Used to verify the validaty of the Juniper Image at software load and also at runtime for integrity.*
EngineeringCA	*RSA 2048 bit X.509 Certificate* *Used to verify the validaty of the Juniper Image at software load and also at runtime for integrity.*
PackageCA	*RSA 2048 bit X.509 Certificate* *Used to verify the validaty 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 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 sent to the PIC to sign data to allow the PIC authenticate to RE by have the PIC sign data that is verified by the RE*

Key	**Description/Usage**
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 used to encrypt the TDES session key.*
RE RSA Encrypt Key	*RSA 1024 bit sent to the PIC; note that the PIC never uses this key*
DH Public Keys	*Used within IKE and SSH for key establishment*

Definition of CSPs Modes of Access

Table 7 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 7 – CSP Access Rights within Roles & Services

Role						**Service**	**Cryptographic Keys and CSPs Access Operation** **R=Read, W=Write, D=Delete**
C.O.	**User**	**RE**	**ASPIC**	**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	SSH 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**)
		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 FIPS User role, the Cryptographic-Officer role, RE Role, PIC Role, IKE Peer Role, and Protocol Peer.
2. The cryptographic module shall support both role-based and identity based authentication mechanisms.
3. Authentication 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 - CBC KAT
        ii. TDES - CBC KAT
        iii. AES - CBC KAT
        iv. AES - CFB KAT
        v. SHA-1 KAT

vi. HMAC-SHA-1 KAT
vii. RSA pairwise consistency test (sign/verify & encrypt/decrypt)
viii. DSA pairwise consistency test (sign/verify)
ix. FIPS 186-2 DRNG KAT

B. Firmware integrity test:

i. RSA digital signature verification (PKCS1.5, 2048 bit key, SHA-1) and SHA-1 hash verification

C. Critical functions tests

i. Verification Of Limited Environment

ii. Verification of Integrity of Optional Packages

- Conditional tests

A. Pairwise consistency tests

i. RSA pairwise consistency test (sign/verify & encrypt/decrypt)

ii. DSA pairwise consistency test (sign/verify)

B. Firmware load test: RSA digital signature verification (2048 bit key)

C. Manual key entry test: duplicate key entries test

D. Continuous random number generator test: performed on the Approved FIPS 186-2, Appendix 3.1 DRNG, and on a non-Approved RNG that is used to seed the Approved DRNG.

E. Bypass test is not applicable.

6. At 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.
7. Prior to each use, the internal RNG shall be tested using the continuous random number generation conditional test.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
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.

9. Physical Security Policy

Physical Security Mechanisms

JUNOS-FIPS is a firmware only module and is defined as running on a multi-chip standalone device that is equivalent to general purpose production grade PC hardware.

Table 8 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
General purpose production grade PC hardware	N/A	N/A

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks, which are outside of 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. Definitions and Acronyms

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator (aka. Pseudo Random Number Generator)
DSA	Digital Signature Algorithm

ACRONYM	**DESCRIPTION**
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
FIPS	Federal Information Processing Standard
GMPLS	General Multi-protocol Label Switching
HMAC-SHA-1	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IPSEC	Internet Protocol Security
MD5	Message Digest 5
MPLS	Multi-protocol 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.
SHA-1	Secure Hash Algorithms
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TDES	Triple - Data Encryption Standard
TLS	Transport Layer Security
UDP	User Datagram Protocols