Juniper J-Series Services Routers: J2320, J2350, J4350, J6350 Security Policy

Document Version: 1.1

Date: August 31, 2010

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 3

2. Security Level 5

3. Modes of Operation 5

    Approved Mode of Operation 5

    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) 9

    Definition of Public Keys 11

    Definition of CSP Modes of Access 12

7. Operational Environment 12

8. Security Rules 12

9. Physical Security Policy 14

    Physical Security Mechanisms 14

    Tamper Seal Placement 14

10. Mitigation of Other Attacks Policy 17

11. Acronyms 18

About Juniper Networks 19

List of Tables

Table 1. J-Series Configurations 3

Table 2. Security Level 5

Table 3. Roles and Required Identification and Authentication 7

Table 4. Strengths of Authentication Mechanisms 8

Table 5. Services Authorized for Roles 9

Table 6. Table of CSPs 9

Table 7. Table of Public Keys 11

Table 8. CSP Access Rights within Roles & Services 12

Table 9. Inspection/Testing of Physical Security Mechanisms 14

Table 10. Mitigation of Other Attacks 17

1. Module Overview

The Juniper J-Series Services Routers: J2320, J2350, J4350, J6350 are multiple-chip standalone cryptographic modules that execute JUNOS-FIPS firmware on the Juniper Networks J-Series routers. The validated version of JUNOS-FIPS is 9.3R3; the image is `junos-juniper-9.3R3-fips.tgz`. See Table 1 below for hardware specifics. JUNOS-FIPS 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.

The J-Series Services Routers: J2320, J2350, J4350, J6350 meet the requirements of the FIPS Publication 140-2. Each cryptographic module's operational environment is a limited operational environment. The cryptographic boundary is defined as being the outer edge of each module's chassis. Figure 1 below shows the modules.

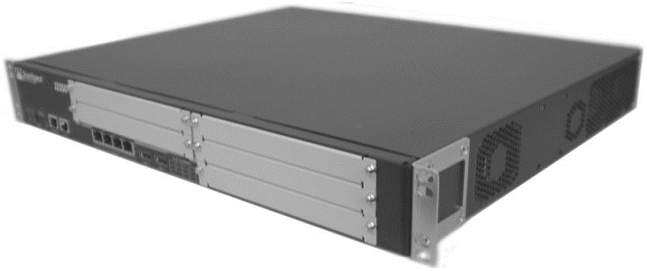
Table 1. J-Series Configurations

Series	Model	HW Part Number
J-Series	J2320	J-2320-JH
	J2350	J-2350-JH
	J4350	J-4350-JB
	J6350	J-6350-JB

Figure 1. Images of the Cryptographic Modules

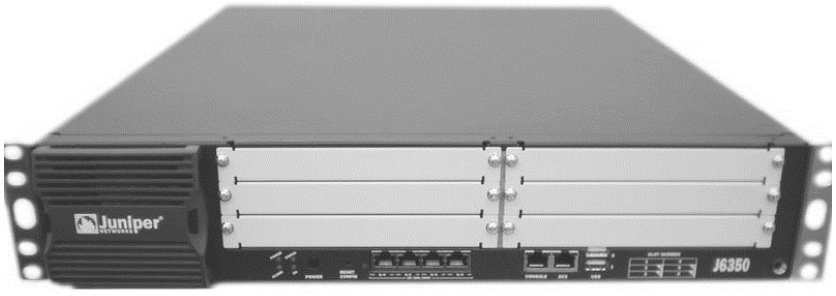
J2320

J2350



J4350

J6350



2. Security Level

The cryptographic modules, which each have a multiple-chip standalone embodiment, meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 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	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved Mode of Operation

The cryptographic modules support 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 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 modules also support 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)
- MD5 and HMAC-MD5

- 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 modules support the commercially available TLS, IKEv1, and SSH protocols for key establishment in accordance with FIPS 140-2 Annex D.

The cryptographic modules rely 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 modules do not provide a non-Approved mode of operation.

4. Ports and Interfaces

The cryptographic modules support 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
- **Reset:** Control Input
- **LEDs:** Status Output

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic modules support two distinct operator roles as follows:

- FIPS User
- Cryptographic Officer (CO)

The cryptographic modules shall enforce the separation of roles using either identity-based or role-based operator authentication; the cryptographic modules meet 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
FIPS User	Identity-based operator authentication	• Via Console: Username and password • Via SSH-2: Password or RSA signature verification or DSA signature verification
	Role-based authentication	• Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters
Cryptographic Officer	Identity-based operator authentication	• Via Console: Username and password • Via SSH-2: Password or RSA signature verification or DSA signature verification
	Role-based authentication	• Via RADIUS or TACACS+: Pre-shared secret, minimum 10 characters

Table 4. 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 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.
RSA signature	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.
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 1/1,000,000. 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.

6. Access Control Policy

Roles and Services

Table 5. Services Authorized for Roles

Role	Authorized Services
User: **Configures and monitors the router via the console or SSH-2**	• 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. • JUNOScript: Provides script handling service for module via SSH-2 or TLS session. • 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 RE via the console or SSH-2. Also has permissions to view and edit secrets within the module.**	• 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. • JUNOScript: Provides script handling service for module via SSH-2 or TLS session. • SSH-2: Provides encrypted login via the SSH-2 protocol. • Console Access: Provides direct login access via the console.

Unauthenticated Services

The cryptographic modules support the following unauthenticated services:

- 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. RSA, DSA. Used to Identify the host. 1024-bit or 2048-bit length.
SSH-2 Session Key	Session keys used with SSH, 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,

CSP	Description
	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
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
Approved RNG State	RNG seed and seed key

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. RSA (1024 or 2048-bit), DSA. 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.
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**		
X		Configuration Management	All CSPs (**R, W, D**)
	X	Configuration Management	No access to CSPs
X	**X**	Router Control	No access to CSPs
X	**X**	Status Checks	No access to CSPs
X		Zeroize	All CSPs (**D**)
X		Load New Software	No access to CSPs
X		JUNOScript	All CSPs (**R, W, D**)
	X	JUNOScript	No access to CSPs
X	**X**	SSH-2	SSH-2 session key (**R**)
X	**X**	Console Access	CO Authentication Key, User Authentication Key (**R**)

7. Operational Environment

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

8. Security Rules

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

1. The cryptographic modules shall provide two distinct operator roles. These are the FIPS User role and the Cryptographic Officer role,.
2. The cryptographic modules 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 modules.
4. The cryptographic modules shall perform the following tests:
    - Power up tests
        A. Cryptographic algorithm tests
            i. TDES KAT

ii. AES KAT
iii. AES CMAC KAT
iv. SHA-1 KAT
v. SHA-224, 256, 384, 512 KAT
vi. HMAC-SHA-1 KAT
vii. HMAC-SHA-256 KAT
viii. ECDH KAT
ix. ECDSA pairwise consistency test (sign/verify) and KAT
x. RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
xi. DSA pairwise consistency test (sign/verify) and KAT
xii. FIPS 186-2 RNG KAT
xiii. KDF KATs

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

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 modules are in an idle state, the operator shall be capable of commanding the modules 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 key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the modules.
9. The modules shall support concurrent operators.

9. Physical Security Policy

Physical Security Mechanisms

Each module's physical embodiment is that of a multi-chip standalone device that meets Level 2 Physical Security requirements. The modules are completely enclosed in a nickel or clear zinc coated cold rolled steel and plated steel and brushed aluminum. 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 to operate as FIPS 140-2 Approved modules.

Table 9. Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper labels, opaque metal enclosure.	The Crypto-Officer must inspect all tamper label locations for the assembled chassis components to verify proper configuration throughout the lifespan of the module; it is recommended this is done on regular intervals.	Labels should be free of any tamper evidence.

Tamper Seal Placement

Seal Application Instructions

For all seal applications, observe the following instructions.

- Handle the seals with care. Do not touch the adhesive side.
- All surfaces to which the seals will be applied must be clean and dry. Ensure 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.

J2320 (7 seals), J2350 (9 seals)

Tamper evident seals shall be applied to the following locations highlighted in red (Figures 2, 3 and 4):

- The front of the chassis, across the ends of each of the PIM blanking/filler plates, extending onto the chassis of the module (Figures 2 and 3)
- The front of the chassis, horizontally, covering the two USB ports (Figure 2 and 3)
- The rear of the modules, over the center of the cover plate, extending to the bottom of the chassis (Figure 4)
- The rear of the J2350, across the edge of the ventilation screen, extending around to the side of the chassis (Figure 4)

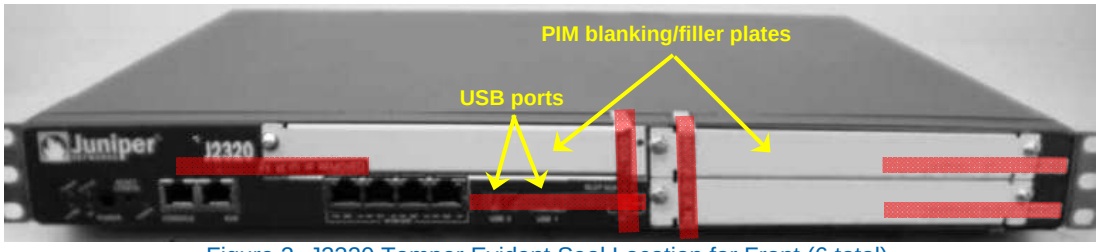


Figure 2. J2320 Tamper Evident Seal Location for Front (6 total)

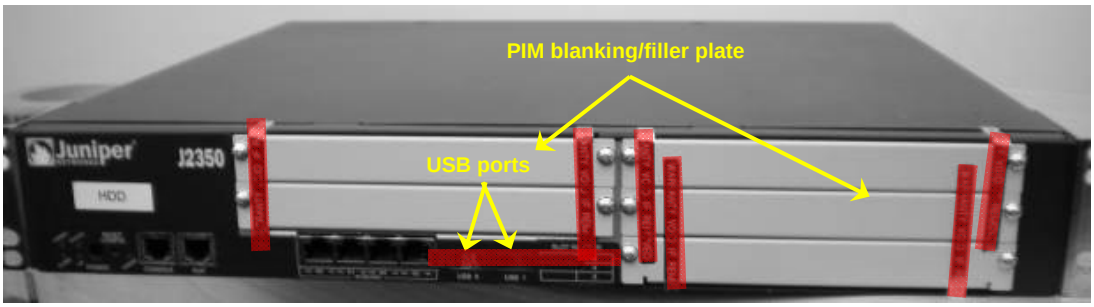


Figure 3. J2350 Tamper Evident Seal Location for Front (7 total)

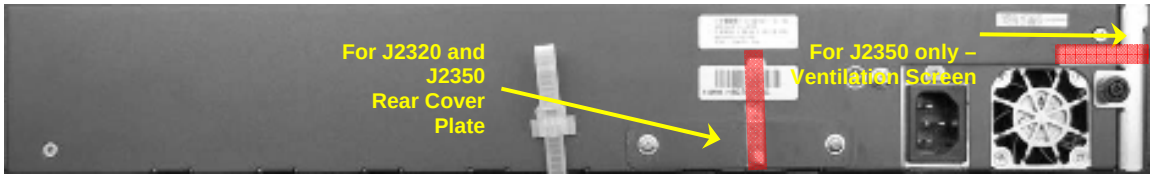


Figure 4. J2320 and J2350 Tamper Evident Seal Location for Rear (J2320 - 1 total, J2350 - 2 total)

J4350 (13 seals), J6350 (13 seals)

Tamper evident seals shall be applied to the following locations highlighted in red (Figures 5, 6, 7 and 8):

- The front of the modules, vertically, across each of the installed interface cards, or slot covers, extending onto the chassis of the modules (Figure 5)
- The front of the modules, horizontally, across both sides of the removable ventilation cover (Figure 5)
- The front of the modules, vertically, across the USB ports (Figure 5)
- (For the J4350 only) Covering the power supply covers at the back of the module and extending onto the removable cover (Figure 6)
- (For the J4350 only) Covering the screw to the left of the power supply fan (Figure 6)
- (For the J6350 only) Covering the power supply cover at the rear of the module and extending onto the module's removable cover (Figure 7)
- (For the J6350 only) Covering the power supply and extending onto the underside of the chassis (Figure 7)
- The top of the module's removable cover and extending onto the side of the chassis opposite the power supply (Figure 8)

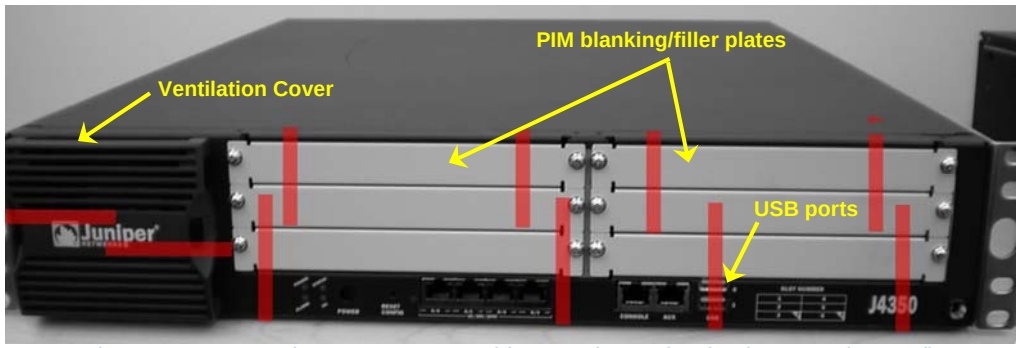


Figure 5. J4350 and J6350 Tamper Evident Seal Location for the Front (10 total)

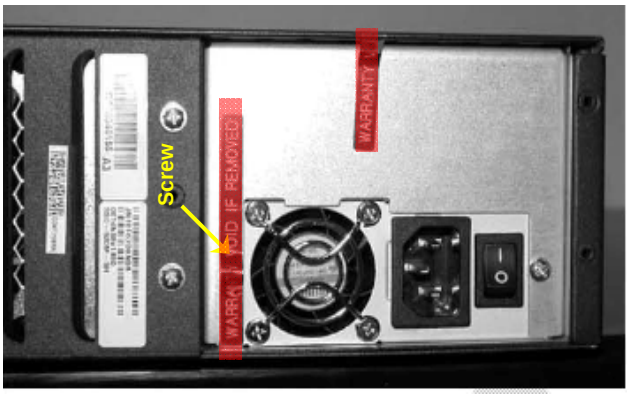


Figure 6. J4350 Tamper Evident Seal Location for Rear (2 total)

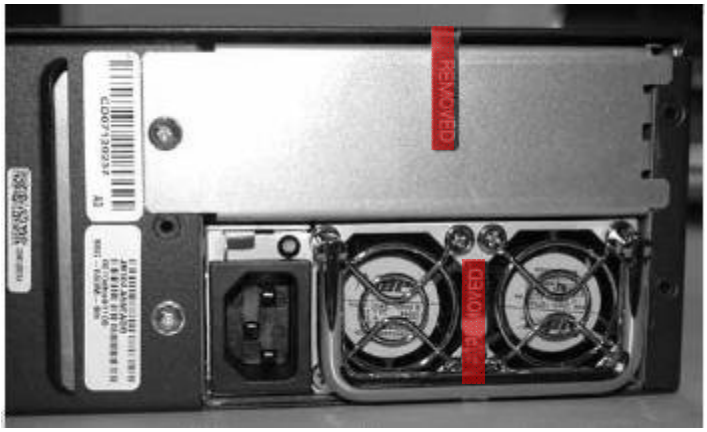


Figure 7. J6350 Tamper Evident Seal Location for Rear (2 total)

Figure 8. J4350 and J6350 Tamper Evident Seal Location for Rear Corner- Opposite Power Supply (1 total)

10. Mitigation of Other Attacks Policy

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

Table 10. Mitigation of Other Attacks

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

11. Acronyms

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	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 Protocol

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.