# Juniper Networks
# MX Series 3D Universal Edge Routers
# with the Multiservices DPC

# Security Policy

**Document Version:** 1.4

**Date:** November 27, 2013

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

## Table of Contents

## List of Tables

## 1. Module Overview

Public sector enterprises are seeking to offer value-added services such as network-based security, tunnel services, and voice services to their network infrastructure.

Juniper Networks MX Series 3D Universal Edge Routers with the Multiservices DPC (the “MX Series”) provides dedicated high-performance processing for flows and sessions, and integrates advanced security capabilities that protect the network infrastructure as well as user data.

The MX Series includes three models: the MX960, MX480, and MX240, each loaded with the MS-DPC, which provides hardware acceleration for an array of packet processing-intensive services such as Session Border Control functions, stateful firewall, NAT, flow monitoring, and anomaly detection. This integration allows customers to eliminate external firewalls that consume router ports and additional management resources.

The MX Series run JUNOS-FIPS, a version of the Junos operating system created specifically for FIPS compliance. The validated version of JUNOS-FIPS is 10.4R11; the image is `junos-juniper-10.4R11-fips.tgz`.

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware on any of the MX Series routers listed below. The cryptographic boundary for the MX Series is defined as follows for the validation:

- the outer edge of the chassis
- includes the Routing Engine (part number RE-S-2000-4096-S) and the MS-DPC (part number 750-024064 ), Switch Control Board (SCB, part number 750-021524), slot cover (part number 760-046576) in the following configurations:
  - For MX240 (2 available RE slots, 2 additional slots): 1 SCB, 1 Routing Engine (RE), at least 1 and up to 2 MS-DPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - MX480 (2 available RE slots, 6 additional slots): 1 SCB, 1 RE, at least 1 and up to 4 MS-DPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For MX960 (2 available RE slots, 12 additional slots): 1 SCB, 1 RE, at least 1 and up to 4 MS-DPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
- includes the inverse three-dimensional space where non-crypto-relevant line cards fit, with the backplane port serving as the physical interface
- excluding the power distribution module on the rear of the device

The cryptographic modules’ operational environment is a limited operational environment.

The image below depicts the physical boundary of the modules, including the Routing Engine, MS-DPC, and excluding the non-crypto relevant line cards.

Images of the Cryptographic Modules

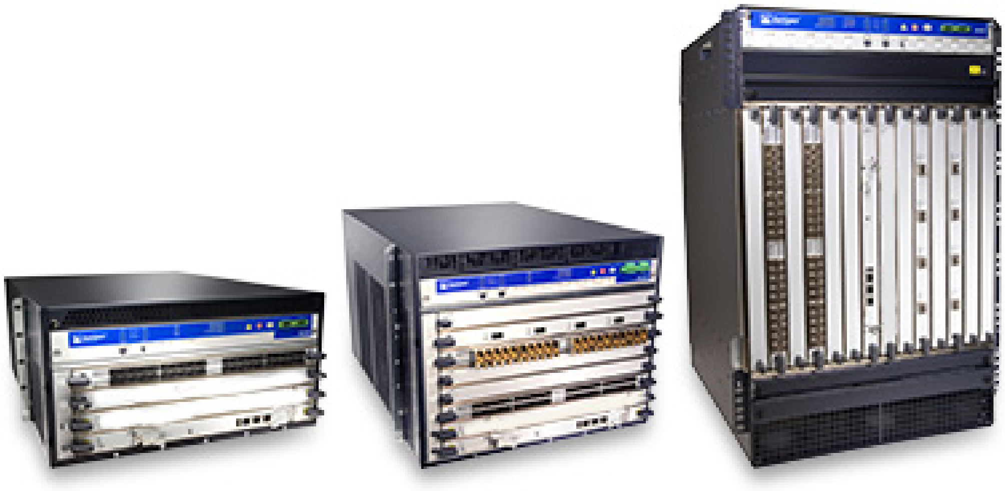


**Figure 1 - Cryptographic Module Images**

## 2. Security Level

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

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** | 1 |

# 3. Modes of Operation

## Approved Mode of Operation

The cryptographic modules support FIPS-Approved algorithms as follows[1]:

- 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 (Three-key)
- 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 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)
- Diffie-Hellman with 1536-bit keys (key agreement; key establishment methodology provides 96 bits of encryption strength)
- The cryptographic modules support the commercially available IKEv1(non-compliant KDF), and SSH (non-compliant KDF) protocols for key establishment in accordance with FIPS 140-2 Annex D which can be used in a FIPS Approved mode under Scenario 4 of FIPS 140-2 IG D.8

The cryptographic module contains the following non-FIPS validated random number generators:

- Non-FIPS validated ANSI x9.62 RNG (used for Initialization Vectors)
- Non-deterministic random number generators that provide suitable entropy for the Approved FIPS 186-2 RNG and the non-FIPS ANSI x9.62 RNG.

## Placing the Module in the Approved Mode of Operation

Once the JUNOS-FIPS firmware image `junos-juniper-10.4R11-fips.tgz` is installed on the router, and the router has successfully run its integrity and self-tests, the router is operating in the approved mode. 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. No further firmware configuration is necessary for the purpose of placing it in FIPS mode. The Crypto Officer must apply the tamper evident label over the USB port as described in section 12.

[1] The user of the module should review the Algorithm Transition Tables, available at the CMVP website (http://csrc.nist.gov/groups/STM/cmvp/) and in the SP 800-131A to determine the current status/risks of algorithms and key lengths used in the module.

### 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
- **Line Card Backplane Interface:** Data Input, Data Output, Control Input, Status Outputs
- **Serial Console:** Control Input, Status Outputs
- **Auxiliary Port:** Control Input, Status Outputs
- **Power interface:** Power Input
- **Reset:** Control Input
- **LEDs:** Status Output
- **Craft Indication Interface:** Status Output

The USB port on the routing engine is not used in FIPS mode of operation.

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

Hardware Guides

| Model | Doc Title | URL |
|---|---|---|
| **MX960** | MX960 Hardware Guide | http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx960/index.html |
| **MX480** | MX480 Hardware Guide | http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx480/index.html |
| **MX240** | MX240 Hardware Guide | http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/mx-series/mx240/index.html |

Control input options and status outputs (not provided by the hardware) are described in the *Junos® OS - Basic System Configuration, Release 10.4*, which is available for download at: http://www.juniper.net/techpubs/en_US/junos10.4/information-products/pathway-pages/system-basics/index.html

# 5. Identification and Authentication Policy

## Assumption of Roles

The cryptographic module supports operator roles as follows:

- Cryptographic Officer (CO)
- User

The cryptographic module enforces the separation of roles using either identity-based or role-based operator authentication. Identity-based authentication occurs when authentication is performed via local authentication database; 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<br>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** | Identity-based operator authentication | Via Console: Username and password<br>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** | The module enforces 10-character passwords (at minimum) chosen from the 96+ human readable ASCII characters.<br>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).<br>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

### Services Authorized for Roles

| Role | Authorized Services |
|---|---|
| **Cryptographic Officer:**<br>**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** | Configuration Mode: Allows the CO to configure the router.<br>Operational Mode: Allows the user to modify the state of the router. (Example: shutdown, reboot)<br>Status Checks: Allows the user to get the current status of the router, including logs and statistics.<br>Zeroize: Allows the user to zeroize the configuration (all CSPs) within the module.[2]<br>SSH: Provides encrypted login via the SSH protocol.<br>Console Access: Provides direct login access via the console.<br>Self-tests: Allows the user to perform cryptographic self-tests by restarting the module.<br>Account Management: Allows the user to create other administrative accounts.<br>Tamper Seals: Ordering, installing, maintaining, storing and examining tamper-evident seals. |
| **User:**<br>**Configures and monitors the router via the console or SSH. May not change the configuration.** | Status Checks: Allows the user to get the current status of the router, including statistics.<br>SSH: Provides encrypted login via the SSH protocol.<br>Console Access: Provides direct login access via the console. |

## Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module

[2] Note that keys and CSPs residing in the MS DPC are zeroized during power cycle.

## 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 1596 |
| **User Authentication Key** | HMAC-SHA-1 Key<br>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<br>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.<br>AES, TDES (3 key), HMAC-SHA-1 |
| **DH Private Key** | Diffie-Hellman 1596-bit private key used in IKE and SSH protocol exchange |
| **RADIUS shared secret** | Used to authenticate COs and Users (10 chars minimum)<br>This includes the Authentication Data Block |
| **TACACS+ shared secret** | Used to authenticate COs and Users (10 chars minimum)<br>This includes the Authentication Data Block |
| **Approved RNG State** | RNG seed and seed key |
| **SNMPv3 security key** | Key used for privacy and/or authentication by SNMPv3 (AES, DES, TDES, HMAC SHA-1) |

## 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<br>Used to verify the validity of the Juniper image at firmware load and also at runtime for integrity. |
| **PackageCA** | RSA 2048-bit X.509 certificate<br>Used to verify the validity of the Juniper image at firmware load and also at runtime for integrity. |
| **DH Public Keys** | Used within IKE and SSH for key establishment. |

### Definition of CSP Modes of Access

The table below 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<br>R=Read, W=Write, D=Delete |
|---|---|---|---|
| CO | User | | |
| X | | Configuration Mode | All CSPs (**R, W, D**) |
| X | | Account Management | Creates or removes passwords (**W**, **D**) |
| X | | Operational Mode | No access to CSPs |
| X | X | Status Checks | No access to CSPs |
| X | | Zeroize | All CSPs (**D**) |
| X | X | SSH | SSH session key (**R**) |
| X | X | Console Access | CO Authentication Key, User Authentication Key (**R**) |
| X | | Self-tests | No access to CSPs |
| X | | Tamper Seals | No access to CSPs |

## 7. Operational Environment

The FIPS 140-2 Operational Environment is a limited operational environment. The module’s operating system is JUNOS OS version 10.4R11.

## 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 two distinct operator roles: the User role and the Cryptographic Officer role.

The cryptographic modules support a role-based or identity based authentication mechanism. Once successfully authenticated, the operator can perform actions respective to the role assigned to that operator.

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
    - MS DPC Hardware (IPsec acceleration):
      - TDES KAT
      - AES KAT
      - SHA-1 KAT
      - SHA-256 KAT
      - HMAC-SHA-1 KAT
      - HMAC-SHA-256 KAT
    - JUNOS Firmware (general purpose):
      - TDES KAT
      - AES KAT
      - SHA-1 KAT
      - SHA-256 KAT
      - SHA-512 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 for the Junos implementation
  - Critical functions tests
    - Verification of Limited Environment
    - Verification of Integrity of Optional Packages

- 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 in Routing Engine
    - Performed on the NDRNG in the Routing Engine.
    - Performed on the non-Approved ANSI x9.62 in the MSDPC
  - Bypass test is not applicable since bypass mode is not supported in FIPS mode.

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.

## 9. Physical Security Policy

The modules' physical embodiment is that of a multi-chip standalone device that meets Level 1 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.

## 10. Cryptographic Algorithm Validation

Cryptographic Algorithm Validation Certificates

| Algorithm | Junos Firmware | Hardware (IPsec) |
|---|---|---|
| **AES-CBC 128/192/256** | 2218<br>2222<br>2221 | 762 |
| **TDES-CBC** | 1388<br>1391<br>1390 | 667 |
| **SHA-1, SHA-256** | 1908<br>1909<br>1913<br>1912 | 769 |
| **HMAC SHA-1, HMAC SHA-256** | 1348<br>1349<br>1352<br>1351 | 417 |
| **FIPS 186-2 RNG** | 1112 | N/A |
| **DSA 1024** | 688 | N/A |
| **RSA 1024/ 2048** | 1137 | N/A |

## 11. Mitigation of Other Attacks Policy

A tamper evident label shall be installed over the USB port on the Routing Engine. The tamper evident label will show evidence if the USB port is used. See Crypto Officer Guidance for placement and instructions on applying the tamper evident label over the USB port.

## 12. Crypto Officer Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the firmware version of the module is Junos 10.4R11FIPS Edition. No other version can be loaded or used in FIPS mode of operation.

- Ensure that the tamper evidence label is applied to the USB port. The tamper evident label shall be installed for the module to operate in a FIPS Approved mode of operation.

- Inspect the tamper evident label periodically to verify it is intact and the serial numbers on the applied tamper evident labels match the records in the security log.

- Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
- When configuring RADIUS and TACACS+ ensure that pre-shared secrets are a minimum 10 characters.

### 12.1 Tamper Evidence Label Placement

The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. The Crypto Officer is responsible for applying the labels; Juniper Networks does not apply the labels at time of manufacture. Once applied, the Crypto Officer shall not remove or replace the labels unless the USB port has shown signs of tampering, in which case the Crypto Officer shall reimage the module and follow all Guidance to place the module in FIPS mode.

Please note that if additional labels need to be ordered, the Crypto Officer shall contact Juniper Networks support and request part number 520-027949.

The Crypto Officer is responsible for:

- securing and having control at all times of any unused seals, and
- maintaining 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.

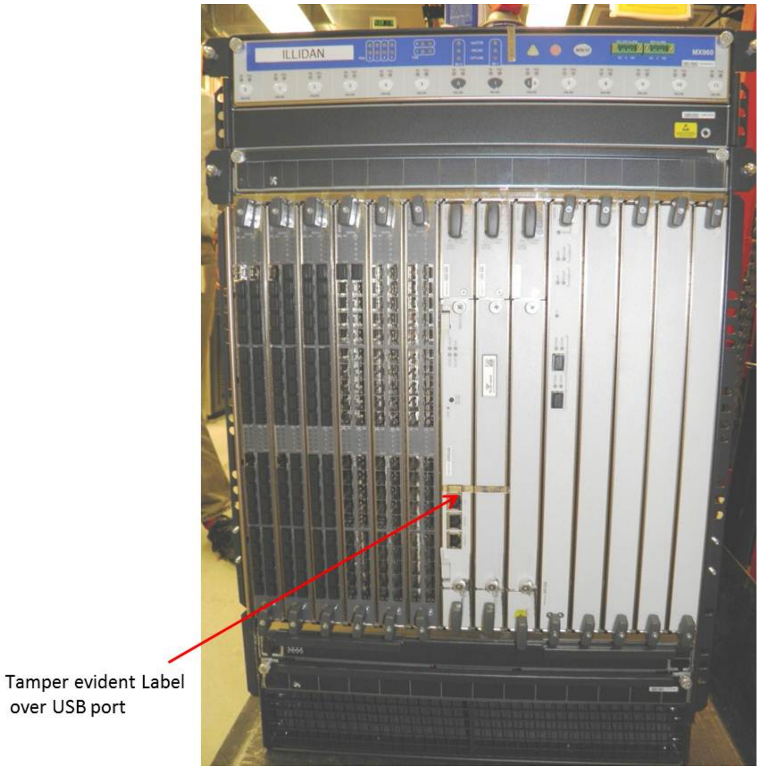
For all seal applications, the Cryptographic Officer should observe the following instructions.

- MX960 and MX480
  1. Handle the seals with care. Do not touch the adhesive side.
  2. Use an alcohol wipe to ensure that all surfaces are clean and clear of any residue.
  3. Apply with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

- MX240
  1. Handle the seals with care. Do not touch the adhesive side.
  2. All chassis surfaces, which contain the black surface finish, to which the seals are to be applied must be prepared by sanding lightly with 200 grit sandpaper to roughen the surface.
  3. Use an alcohol wipe to ensure that all surfaces are clean and clear of any residue.
  4. 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.

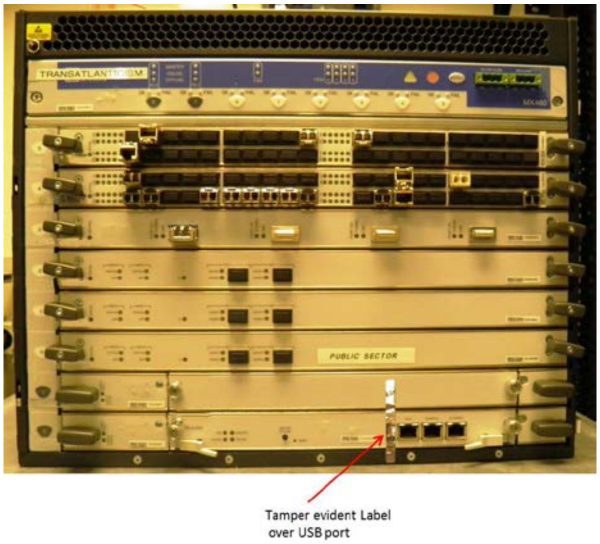
### 12.1.1 Tamper Evidence Label Placement: MX960



Tamper evident Label
over USB port

Figure 2 - MX960 Label Placement

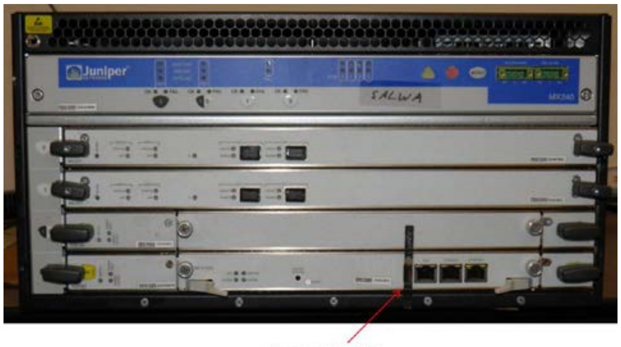
### 12.1.2 Tamper Evidence Label Placement: MX480



Tamper evident Label
over USB port

Figure 3 – MX480 Label Placement

### 12.1.3 Tamper Evidence Label Placement: MX240



Tamper evident label over the USB port

**Figure 4 – MX240 Label Placement**

## 11. Acronyms

| ACRONYM | DESCRIPTION |
|---|---|
| **AES** | Advanced Encryption Standard |
| **DSA** | Digital Signature Algorithm |
| **EMC** | Electromagnetic Compatibility |
| **EMI** | Electromagnetic Interference |
| **FIPS** | Federal Information Processing Standard |
| **HMAC-SHA-1** | Keyed-Hash Message Authentication Code |
| **IKE** | Internet Key Exchange Protocol |
| **IPsec** | Internet Protocol Security |
| **KDF** | Key Derivation Function |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **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 |
| **UDP** | User Datagram Protocol |

## About Juniper Networks

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

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