Juniper Networks LN1000 Mobile Secure Router Security Policy

Document Version: 1.0

Date: May 1, 2012

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

This page intentionally left blank.

1. Module Overview

The Juniper Networks LN1000 Mobile Secure Router is an edge access router that delivers a high-performance routing firewall and intrusion detection service (IDS). The LN1000 addresses the growing demand for a network access presence in military, first responder and transportation vehicles, mining and exploration equipment, unmanned aircraft, and power grids. It is intended to be installed in a standard VITA 46.0-compliant chassis. Optionally, it may be installed in a VITA 46.0–compliant chassis with a midplane and an LN1000 rear transition module.

The Juniper Networks LN1000 Mobile Secure Router runs JUNOS-FIPS, a version of JUNOS created specifically for FIPS compliance. The validated version of JUNOS-FIPS is 11.2S4; the image is `junos-ln-11.2S4-fips.tgz`. The hardware version of the validated module is LN1000-V.

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware. The cryptographic boundary is defined as the outer edge of the metal case. The cryptographic module's operational environment is a limited operational environment.

Figure 1: Depiction of the Cryptographic Module

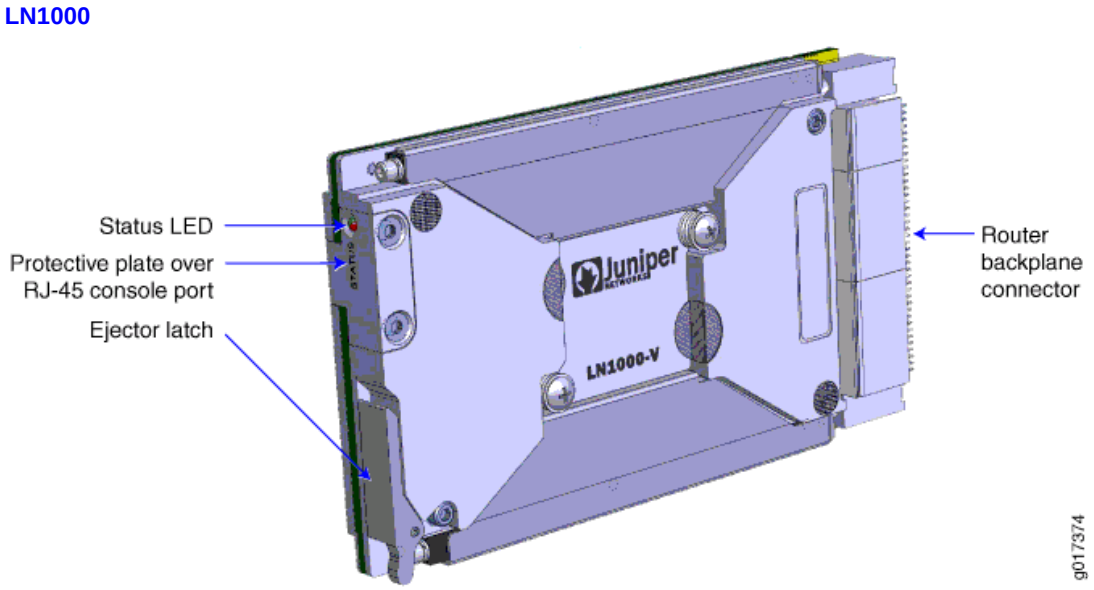

Figure 1 depicts the LN1000 without tamper seal. For depictions of the unit with the tamper seal installed, see section 9.

2. Security Level

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

Security Level

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

3. Modes of Operation

Approved Mode of Operation

The cryptographic modules support FIPS-Approved algorithms as follows:

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

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

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

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

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

Placing the Module in the Approved Mode of Operation

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

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

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

Non-FIPS Mode of Operation

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

4. Ports and Interfaces

The cryptographic module supports the following physical ports:

- **Router backplane connector**. An external interface, located on the back of the LN1000 router, connects the router to the VITA 46.0–compliant chassis. The router's P0, P1, and P2 connectors plugging into the backplane are VITA 46.0–compatible for a 3U peripheral slot with specific key definitions. The P0 and P2 connectors are keyed per the VITA 46.12 specification. Power to the LN1000–V router is provided through the P0 connector.

  The LN1000 router supports up to eight ports of gigabit Ethernet traffic with up to 1024 logical interfaces. The eight gigabit Ethernet ports on the LN1000 router are 1000Base-X interfaces with autonegotiation on by default. The Ethernet ports are on the router interface with the chassis in which it is installed or with the LN1000 rear transition module, if installed in a chassis.
- **RJ-45 console port**. The router's RS-232 console port has a baud rate of 9600 8N1 and is located on the left side of the LN1000 router's front panel. It is covered by a protective aluminum plate that prevents access to the port. When the LN1000 router is operational and installed in a chassis, even though you can remove the protective aluminum plate to access the console port on the router, typically you access the console port using one of the following methods:
  - On the chassis backplane when the router is installed in VITA 46.0-compliant chassis.
  - On the front panel of the rear transition module when the router is installed in a VITA 46.0-compliant chassis with a LN1000 rear transition module.
- **Status LED.** Displays the following status indications:
  - No color: power off
  - Steady red: error condition
  - Steady green: Ready for operation. The router is powered on and has successfully booted and run SPOST and POST diagnostics.
  - Blinking green: Powering on and then running SPOST and POST diagnostics, or running individual diagnostics, or performing an upgrade.

The physical interfaces map to the following logical interfaces:

- **Router backplane:** Data Input, Data Output, Control Input, Status Outputs, Power Input
- **Console port:** Control Input, Status Outputs
- **LED:** Status Output

The flow of input and output of data, control, and status is managed by the cryptographic module. More detailed hardware documentation is available at http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ln1000-series/router-ln1000v.html.

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

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports two distinct operator roles as follows:

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

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

Roles and Required Identification and Authentication

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

Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and password	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

Services Authorized for Roles

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

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

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

Definition of Critical Security Parameters (CSPs)

Table of CSPs

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

Definition of Public Keys

Table of Public Keys

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

Definition of CSP Modes of Access

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

CSP Access Rights within Roles & Services

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

7. Operational Environment

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

8. Security Rules

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

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

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

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

The cryptographic module performs the following tests:

- Power up tests

- Cryptographic algorithm tests
  - Hardware (IPSec acceleration):
    - TDES KAT
    - AES KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
  - Software (general purpose):
    - TDES KAT
    - AES KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - RSA pairwise consistency test (sign/verify and encrypt/decrypt) and KAT
    - DSA pairwise consistency test (sign/verify) and KAT
    - FIPS 186-2 RNG KAT
    - KDF KATs
- Firmware integrity test:
  - RSA digital signature verification (PKCS1.5, 2048-bit key, SHA-1) and SHA-1 hash verification

- Conditional tests
  - Pairwise consistency tests
    - RSA pairwise consistency test (sign/verify and encrypt/decrypt)
    - DSA pairwise consistency test (sign/verify)
  - Firmware load test: RSA digital signature verification (2048-bit key)
  - Manual key entry test: Duplicate key entries test
  - Continuous random number generator test: performed on the Approved FIPS 186-2, Appendix 3.1 RNG, and on a non-Approved RNG that is used to seed the Approved RNG.
  - Bypass test is not applicable.

Any time the cryptographic module is in an idle state, the operator is capable of commanding the modules to perform the power-up self-test by power-cycling the module.

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

Data output is inhibited during key generation, self-tests, zeroization, and error states.

Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the modules.

The module supports concurrent operators.

9. Physical Security Policy

Physical Security Mechanisms

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

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

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seal 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.

Note that the device has two factory-installed circular stickers. These are not security relevant and are not intended to provide tamper evidence.

Inspection/Testing of Physical Security Mechanisms

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

Tamper Seal Placement

Seal Application Instructions

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

- Handle the seal with care. Do not touch the adhesive side.
- All surfaces to which the seal is to be applied must be prepared by sanding lightly with 200 grit sandpaper to roughen the surface. Use an alcohol wipe to ensure that all surfaces are clean and clear of any residue.
- Apply with firm pressure across the seal to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

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

LN1000 (1 seal)

A tamper evident seal shall be applied to the following location (see highlighted pointer):

- Label #1 across the edge of the metal cover opposite the router backplane connector, extending across the console port cover plate and wrapping around to the other side of the metal cover.

Figure 2. LN1000 Tamper Evident Seal Location (Top)

10. Cryptographic Algorithm Validation

Cryptographic Algorithm Validation Certificates

Algorithm	Software (General purpose)	Hardware (IPSec)
AES-CBC 128/192/256	1957	1956
3DES-CBC	1270	1269
SHA-1, SHA-256	1716	1715
HMAC SHA-1, HMAC SHA-256	1179	1178
FIPS 186-2 RNG	1028	N/A
DSA 1024/2048	624	N/A
RSA 1024/2048	1013	N/A

10. Mitigation of Other Attacks Policy

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

Mitigation of Other Attacks

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

11. Acronyms

ACRONYM	DESCRIPTION
AES	Advanced Encryption Standard
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
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
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.