FIPS 140-2 Non-Proprietary Security Policy

Juniper Networks NSM (Network and Security Manager) Cryptographic Module Version 1.0

Document Version 1.3

February 26, 2010

This document may be reproduced only in its original entirety [without revision]

Prepared For:

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

www.juniper.net

Prepared By:

Apex Assurance Group, LLC

5448 Apex Peakway Drive, Ste. 101

Apex, NC 27502

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the NSM (Network and Security Manager) Cryptographic Module Version 1.0.

This document may be reproduced only in its original entirety [without revision]

Table of Contents

This document may be reproduced only in its original entirety [without revision]

List of Tables

List of Figures

This document may be reproduced only in its original entirety [without revision]

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) owns the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for all products pursuing FIPS 140 validation. *Validation* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the NSM (Network and Security Manager) Cryptographic Module Version 1.0 from Juniper Networks provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The Juniper Networks NSM (Network and Security Manager) Cryptographic Module Version 1.0 may also be referred to as the "module" in this document.

1.3 External Resources

The Juniper Networks website (http://www.juniper.net) contains information on the full line of products from Juniper Networks, including a detailed overview of the NSM solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm) contains links to the FIPS 140-2 certificate and Juniper Networks contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

This document may be reproduced only in its original entirety [without revision]

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
NSM	Network and Security Manager
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

This document may be reproduced only in its original entirety [without revision]

2 Juniper Networks NSM (Network and Security Manager) Cryptographic Module Version 1.0

2.1 NSM Product Overview

Network and Security Manager (NSM) is a centralized management solution that controls the entire device life cycle of firewall/IPSec VPN and IDP devices, including basic setup and network configuration with local and global security policy deployment. Unmatched role-based administration allows IT departments to delegate appropriate levels of administrative access to specific users, thereby minimizing the possibility of a configuration error that may result in a security hole.

2.2 Cryptographic Module Specification

The module is the Juniper Networks NSM (Network and Security Manager) Cryptographic Module Version 1.0. The module is a software-only module installed on a multi-chip standalone device which provides cryptographic services to the Juniper Networks NSM application.

The module is a uniquely identifiable library that is linked into the NSM application. All operations of the module occur via calls from the NSM application, which occur only when an operator is successfully authenticated to the host operating system. As such there are no untrusted services or daemons calling the services of the module. No security functions outside the cryptographic module provide FIPS-relevant functionality to the module.

2.3 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2. The Juniper Networks NSM Cryptographic Module is intended to meet an Overall Security Level 2.

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	N/A
Operational Environment	2
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	2

This document may be reproduced only in its original entirety [without revision]

FIPS 140-2 Section Title	Validation Level
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is not relevant as the module does not implement any countermeasures towards special attacks.

2.4 Algorithm Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificates	Use
Asymmetric Key	RSA	ANSI X9.31	473	Sign / verify operations Key establishment
Hashing	SHA-1	FIPS 180-3	952	Message digest
Keyed Hash	HMAC-SHA-1	FIPS 198	553	Message integrity
Symmetric Key	AES CBC mode with 128, 192, or 256-bit keys	FIPS 197	982	Data encryption
RNG	ANSI X9.31	ANSI X9.31	558	Random Number Generation

Table 3 – Algorithm Certificates (NSM Cryptographic Module for SSP implementation)

Algorithm Type	Algorithm	Standard	CAVP Certificates	Use
Asymmetric Key	RSA	ANSI X9.31	472	Sign / verify operations Key establishment
Hashing	SHA-1, 224, 256, 384, 512	FIPS 180-3	951	Message digest
Keyed Hash	HMAC-SHA-1, 224, 256, 384, 512	FIPS 198	552	Message integrity
Symmetric Key	AES CBC, ECB, OFB, CFB8, CFB128 modes with 128, 192, or 256-bit keys	FIPS 197	981	Data encryption
RNG	ANSI X9.31	ANSI X9.31	557	Random Number Generation

Table 4 – Algorithm Certificates (NSM Cryptographic Module implementation)

The module does not implement any non-approved algorithms.

2.5 Module Interfaces

The figure below shows the module's physical and logical block diagram:

This document may be reproduced only in its original entirety [without revision]

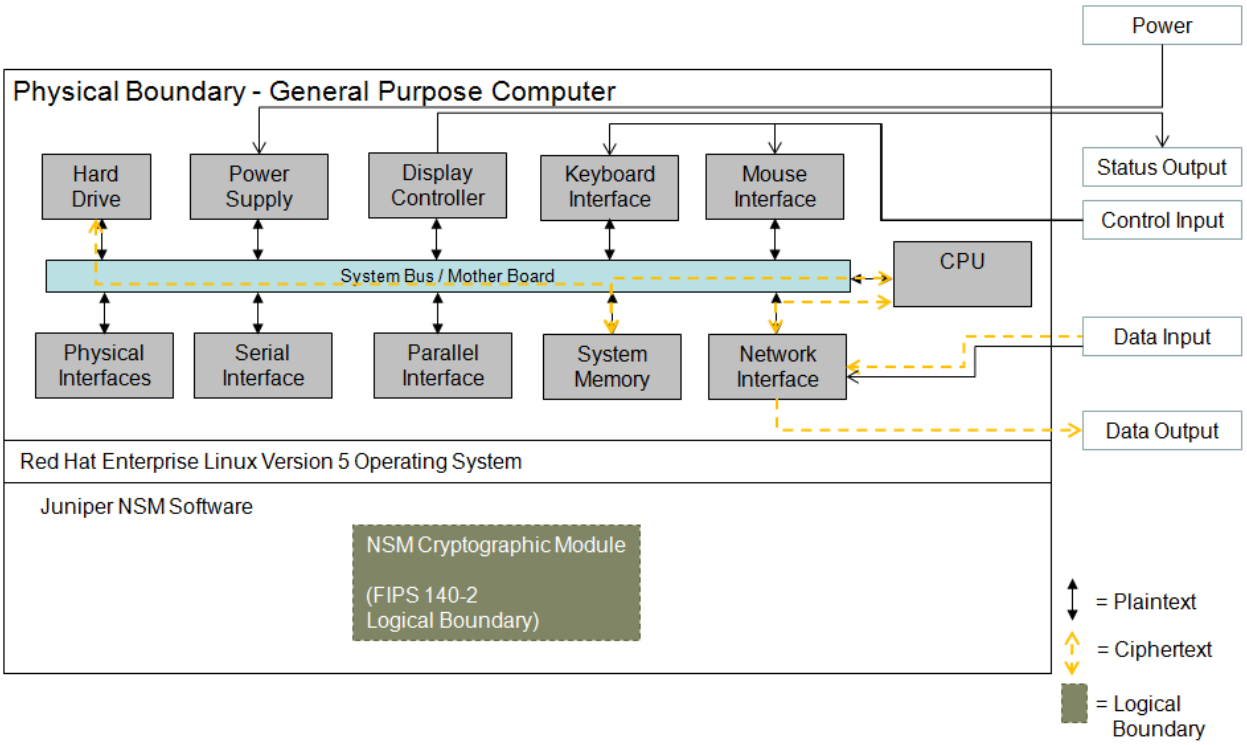

Figure 1 – Module Interfaces Diagram

The interfaces (ports) for the physical boundary include the computer keyboard port, CDROM drive, floppy disk, mouse, network port, parallel port, USB ports, monitor port and power plug. When operational, the module does not transmit any information across these physical ports because it is a software cryptographic module. Therefore, the module's interfaces are purely logical and are provided through the Application Programming Interface (API) that a calling daemon can operate. The logical interfaces expose services that applications directly call, and the API provides functions that may be called by a referencing application (see Section 2.6 – Roles, Services, and Authentication for the list of available functions).

The API provided by the module is mapped onto the FIPS 140- 2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140- 2 logical interfaces relates to the module's callable interface, as follows:

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Data Input	Input parameters of API function calls	Ethernet/Network port
Data Output	Output parameters of API function calls	Ethernet/Network port
Control Input	API function calls	Keyboard and mouse

This document may be reproduced only in its original entirety [without revision]

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Status Output	Function calls returning status information and return codes provided by API function calls	Monitor
Power	None	Power supply/connector

Table 5 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role. The Crypto Officer can access all services in the module and perform initialization while the User role can only access the services of the module. The module does not support a Maintenance role.

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Roles
Initialize	Initializes the module for FIPS mode of operation	Crypto Officer
Decrypt	Decrypts a block of data using AES	Crypto Officer User
Encrypt	Encrypts a block of data using AES	Crypto Officer User
Generate Keys	Generates cryptographic keys	Crypto Officer User
Self-Test	Performs self-tests on critical functions of the module	Crypto Officer User
Key Establishment	Provides a protected session for establishment of AES keys with peers	Crypto Officer User
Message Digest	Hash data with approved function	Crypto Officer User
Status	Status of the module	Crypto Officer User

Table 6 – Operator Services and Descriptions

The module does not support multiple concurrent operators.

2.6.2 Operator Authentication

Operators authenticate to the module via the General Purpose Operating System, which implements a username/password authentication mechanism and enforces operator authentication prior to the operator utilizing any system services. Further, the GPOS authentication mechanism distinguishes

This document may be reproduced only in its original entirety [without revision]

operators that have administrator rights on a computer system. The modules rely on this mechanism to distinguish an operator between the two supported roles.

Passwords must be a minimum of 8 characters (see Secure Operation section of this document). The password can consist of alphanumeric values, **a-z A-Z 0-9**, yielding 62 choices per character. The probability of a successful random attempt is $1/62^8$, which is less than 1/1,000,000.

The GPOS module will lock an account after 5 consecutive failed authentication attempts; thus, the maximum number of attempts in one minute is 5. Therefore, the probability of a success with multiple consecutive attempts in a one minute period is $5/62^8$ which is less than 1/100,000.

2.7 Physical Security

This section of requirements does not apply to this module. The module is a software-only module and does not implement any physical security mechanisms.

2.8 Operational Environment

The cryptographic module was tested and validated on a HP Proliant DL365 G5 Server platform running an AMD Opteron processor. The module runs on Red Hat Enterprise Linux Version 5, which has met Common Criteria EAL 4+ certification. The module's software is entirely encapsulated by the cryptographic boundary shown in Figure 1. The Common Criteria Security Target, which specifies the evaluated configuration and GPC system information for the Red Hat Operating System, can be found at http://www.niap-ccevs.org/cc-scheme/st/st_vid10165-st.pdf

The GPC used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B, Class A.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Session Key	AES-CBC 128-bit key for encryption / decryption of session traffic	Internal generation by X9.31 RNG	Storage: RAM plaintext Association: The system is	Agreement: NA Entry: NA Output: Key handle from API request is	See paragraph below	Crypto Officer R W D

This document may be reproduced only in its original entirety [without revision]

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
			the one and only owner. Relationship is maintained by the operating system via protected memory.	output only to the NSM application		User R
RNG Seed	System Entropy seed the X9.31 RNG	External	Storage: RAM plaintext Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: NA Entry: NA Output: NA	See paragraph below	Crypto Officer RWD User None
Asymmetric Key	RSA 1024-bit for sign / verify operations and key establishment[1]	Internal generation by X9.31 RNG	Storage: RAM plaintext Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: NA Entry: NA Output: Key handle from API request is output only to the NSM application	See paragraph below	Crypto Officer R W D User R
HMAC Key	160-bit HMAC-SHA1 for message verification	Internal generation by X9.31 RNG Key	Storage: RAM plaintext Association:	Agreement: NA Entry: NA Output: Key handle from API	See paragraph below	Crypto Officer R W D

[1] Key establishment methodology provides 80 bits of encryption strength

This document may be reproduced only in its original entirety [without revision]

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
			The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	request is output only to the NSM application		User R
HMAC Software Integrity Key	160-bit HMAC-SHA1 for Software integrity	Hardcoded for integrity check.	Persistent storage as plaintext. Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: NA Entry: NA Output: NA	Not zeroized; persistent per IG 7.4	Crypto Officer None User None
Operator passwords	Alphanumeric passwords externally generated by a human user for authentication to the operating system.	Not generated by the module; defined by the human user of the workstation	Storage: on disk Association: controlled by the operating system	Agreement: NA Entry: Manual entry via operating system Output: NA	Handled by operating system	Crypto Officer R W D User R W D

Table 7 – Key/CSP Management Details

R = Read W = Write D = Delete

The NSM application ensures that no keys or CSPs leave the physical boundary of the module in plaintext.

The module employs RSA public key components. These public components shall be protected from unauthorized modification and substitution.

This document may be reproduced only in its original entirety [without revision]

All keys and CSPs are stored in memory, and zeroization has been implemented to ensure no traces are left of any CSPs upon termination of the service using the CSP. For the CSPs related to the SSP implementation, zeroization has been implemented by overwriting the allocated memory buffer with zeros before freeing the memory to other uses. Any service using a CSP will zeroize the CSP upon normal termination and when transitioning into error states. Zeroization is initiated by terminating the process and powering off the module. For other CSPs related to the implementation, the end user is responsible for zeroizing CSPs via wipe/secure delete procedures.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module/NSM application will output an error to the audit log and will shutdown. To access status of self-tests, success or failure, the application provides access to the audit log. Status is viewable via operating environment's audit mechanism and by verifying proper loading and operation of the NSM application.

No keys or CSPs will be output when the module is in an error state. Additionally, the module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the process will be halted and the module will not initialize. In this error state, no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check[2] via HMAC-SHA1
- RSA pairwise consistency
- AES KAT (encryption and decryption)
- SHA-1 KAT
- RNG KAT

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests can be run on demand by reinitializing the module in FIPS-Approved Mode of Operation.

[2] The integrity of the FIPS object code (i.e., all files within the Cryptographic Boundary) is protected by a HMAC-SHA1 digest that is calculated over the files at the time they are created. The digest is verified when the module is initialized.

This document may be reproduced only in its original entirety [without revision]

2.10.2 Conditional Self-Tests

Conditional self-tests are on-demand tests and tests run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Pairwise consistency tests for RSA
- Continuous RNG test run on output of ANSI X9.31 RNG implementations

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

This document may be reproduced only in its original entirety [without revision]

3 Guidance and Secure Operation

This section describes how to configure and initialize the module for FIPS-Approved mode of operation. When configured and initialized per this Security Policy, the module will only operate in the FIPS Approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Software Installation

The module is included with the NSM Server Application Version 2008.2 r2 and is not available for direct download. The NSM Server Application Version 2008.2 r2 has not been evaluated and is outside the scope of this FIPS 140-2 validation. The NSM Server application (and subsequently the module) is to be installed on a Red Hat Enterprise Linux Version 5 operating system.

Please note that this operating system must meet installation and configuration requirements specified in the operating system's Common Criteria Security Target (http://www.niap-ccevs.org/cc-scheme/st/st_vid10165-st.pdf). See Section 2.4 Configurations of the Security Target for evaluated GPC systems, installation and configuration details. The cryptographic module was tested and validated on a HP ProLiant DL365 G5 server.

3.1.2 Enabling FIPS Module within the NSM application.

The FIPS Mode setting in NSM 2008.2 r2 is initially configured by the installer[3]. The NSM application is configured to use the module as follows:

- When using the NSM 2008.2 r2 installer to either upgrade an existing NSM installation or install a new one, the installer will prompt:

  "Do you want to enable FIPS Mode?" (n)

  Valid responses are **Y**, **y**, **N**, **n**, and **RETURN**, which will default option **n**.

- When using NSM 2008.2 r2, the FIPS Mode may be modified by toggling the **enableFIPS** flags value between **yes** and **no** in both the **/usr/netscreen/GuiSvr/var/guiSvr.cfg** and **/usr/netscreen/DevSvr/var/devSvr.cfg** files and restarting the system, in order for the change to take effect. For instance:

  ```
  # vi /usr/netscreen/GuiSvr/var/guiSvr.cfg

  # vi /usr/netscreen/DevSvr/var/devSvr.cfg
  ```

[3] Note that if FIPS mode is not enabled, the NSM application may use algorithms that are not provided by the validated cryptographic module and are not FIPS-Approved, additionally FIPS-required self-tests will not be run.

This document may be reproduced only in its original entirety [without revision]

```
# /etc/init.d/guisvr.sh restart

# /etc/init.d/devsvr.sh restart
```

- The NSM development team is responsible for ensuring the source files that comprise the NSM (Network and Security Manager) Cryptographic Module Version 1.0 are built into the NSM application. These files are listed with the Juniper NSM Configuration Management Overview document available internally.

3.1.3 Additional Rules of Operation

1. All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.

2. The writable memory areas of the Module (data and stack segments) are accessible only by the NSM application so that the Module is in "single user" mode, i.e. only the NSM application has access to that instance of the Module.

3. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.

4. The key generation service allows the crypto-officer and user to ensure that the seed material for the module's RNG provides at least 128 bits of entropy prior to the use of the RNG for the generation of cryptographic key components. The crypto-officer must ensure the entropy source provides at least 128 bits. This may be done via statistical analysis of the seed source, such as calculation of the minimum entropy per Appendix C, NIST SP 800-90.

5. The end user of the operating system is responsible for zeroizing CSPs via wipe/secure delete procedures.

3.2 User Guidance

3.2.1 General Guidance

The module is not distributed as a standalone library and is only used in conjunction with the NSM solution. As such, there is no direct User Guidance.

This document may be reproduced only in its original entirety [without revision]