

# ScreenOS 5.0.0r9-FIPS With NSM Reference Note

12 August 2005

Part No.

093-1735-000

Revision A

## Before You Begin

---

Before carrying out any step to secure a Juniper Networks security appliance, check that the product has not been tampered with. You should also confirm that the product received matches the version that is certified as FIPS 104-2 compliant.

Verify the product security with these observations:

- The outside packaging does not show damage or evidence that it has been opened. If the cardboard shows damage that would allow the device to be removed or exchanged, this may be evidence of tampering.
- Each box is packaged with custom tape to indicate that the device was packaged by Juniper Networks or an authorized manufacturer. The tape is unique, with the word **NetScreen** printed repeatedly along the tape. If the tape is not present, your device may have been tampered with.
- The internal packaging does not show damage or evidence of tampering. The plastic bag should not have a large hole and the label that seals the plastic bag should not be detached or missing. If the bag or seal are damaged in any way, your device may have been tampered with.

## About This Document

---

This document describes the Federal Information Processing Standards (FIPS) certified release of ScreenOS 5.0.0.r9-FIPS. There are no new features in this release; however, certain behaviors and options vary from the 5.0 release. These variations were developed in order to comply with FIPS requirements.

This document contains the following information:

- FIPS Supported Platforms
- Restrictions
- Changing the Device Mode
- Managing FIPS Mode Devices
- Deployment Tips

For more information on FIPS, please refer to the National Institute of Standards and Technology FIPS page at <http://csrc.nist.gov/publications/fips/index.html>.

## FIPS Supported Platforms

---

The 5.0.0r9-FIPS release supports the following platforms:

- NS-5XT
- NS-204/208
- NS-500
- NS-5200/5400

Following is a summary of FIPS 5.0.0r9 firmware images:

<b>Platform</b>	<b>NSM and SNMP support</b>
NS-5XT	ns5xt.500-FIPS.r9.h
NS-200	ns200.500-FIPS.r9.h
NS-500	ns500.500-FIPS.r9.h
NS-5200/5400	ns5000.500-FIPS.r9.h

## Restrictions

---

When ScreenOS 5.0.0r9-FIPS is not operating in FIPS mode, its behavior is identical to that of ScreenOS 5.0.

ScreenOS images that run in FIPS mode must be authenticated before loading. To perform the authentication, the NetScreen DSA public key must be present. The public key can be downloaded from the Juniper Networks support site at <http://www.juniper.net/support>. To load the key on to the NetScreen device, use the **save image-key** CLI command.

FIPS mode restricts the following on a NetScreen device:

- Management via Telnet, HTTP (WebUI), or NetScreen-Security Manager is available only through a VPN using 256-bit AES encryption.
- Management via SSH is available only with Triple-DES encryption.
- High Availability (HA) traffic must be 256-bit AES encrypted.
- If a VPN is configured using Triple-DES encryption, Internet Key Exchange (IKE) must be configured to use Diffie-Hellman Group 5.

FIPS mode disables the following on a NetScreen device:

- The modem port is disabled.
- Administration via SNMP Read-Write community is disabled. Monitoring via the Read-Only community remains available.
- The debug service is disabled.
- The Global-Pro reporting agent is disabled.
- Loading and output configuration files to a TFTP server is disabled.
- Administration via SSL is disabled.
- Use of the MD5 algorithm is disabled.
- All hidden commands are disabled.

**NOTE:** The Data Encryption Standard (DES) protocol is supported but not recommended for use. It will not be supported in future releases.

## Changing the Device Mode

---

To place the device in FIPS mode, enter the following CLI command:

```
ns-> set fips-mode enable
```

At the following prompt, press **Enter** to reset the device:

```
Fips_mode is set! Reset dev? [y]/n
```

## Verifying the Device Mode

To check whether the device is in FIPS mode, enter the following CLI command:

```
ns-> get system
Product Name: NS208
Serial Number: 0099122004000991, Control Number: 00000000, Mode: FIPS
Hardware Version: 0110(0)-(12), FPGA checksum: 00000000, VLAN1 IP (0.0.0.0)
Software Version: 5.0.Or9.h, Type: Firewall+VPN
Feature: FIPS
Base Mac: 0010.db90.f770
File Name: ns200.500-FIPS.r9.h, Checksum: 48e3d429
```

The current mode appears on the second line of the output.

## Disabling FIPS Mode

To disable FIPS mode on a NetScreen device, enter the following CLI command:

```
unset fips-mode enable
```

At the following prompt press **Enter** to reset the device:

```
Fips_mode is set! Reset dev? [y]/n
```

## Managing FIPS Mode Devices

---

A NetScreen device that is operating in FIPS mode requires all NetScreen-Security Manager traffic to be protected by a VPN with 256-bit AES encryption. This requires a manually configured VPN tunnel between the remote device that is to be managed and a local VPN device. The local VPN device should be on the same local network as the NetScreen-Security Manager server. After the VPN has been successfully configured, the managed device can be imported into NetScreen-Security Manager.

To ensure that NetScreen-Security Manager traffic is routed solely through the VPN, use the following CLI command:

```
set nsmgmt server primary a.b.c.d src-interface tunnel_int
```

Variable	meaning
<b>a.b.c.d</b>	The IP address of the NetScreen-Security Manager server.
<b>tunnel_int</b>	The tunnel interface that is associated with the AES VPN.

The VPN endpoint that is local to NetScreen-Security Manager Device Server cannot be in FIPS mode if the device is managed with NetScreen-Security Manager.

[ a graphic would be useful here to illustrate the network architecture]

### **Configuring High Availability options in FIPS mode**

NSRP traffic between member devices in an NSRP cluster must be encrypted using a 256-bit key. The password option to the **set nsrp encrypt** command is not available in FIPS mode. Following is an example of how a 256-bit key is specified in four groups of 16 hexadecimal characters.

```
set nsrp encrypt  
0123456789abcdef,0123456789abcdef,01234567890abcdef,0123456789abc  
def
```

### **Managing Virtual Security Device (VSD) clusters in FIPS mode**

We recommend that FIPS mode devices are placed in an Active-Active cluster, rather than an Active-Passive cluster if they are going to be managed using NSM.

## **Deployment Tips**

---

Because the debug service is not available in FIPS mode, Juniper Networks recommends that you do not place the device in FIPS mode until after the configuration is debugged. In a multi-device deployment, you should enable FIPS mode on each device sequentially, confirming that each configuration is still functioning as expected before enabling the next device.

If an error occurs when the configuration is loaded, refer to the Restrictions on page 3 and edit your configuration as necessary to use only the supported options.

