

# ScreenOS 5.4.0r4 FIPS Reference Note

31 January 2008

Part No.

093-1649-000

Revision 02

## 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 5.4.0.r4 for FIPS.

This document contains the following information:

- FIPS Certified Platforms
- Restrictions
- Changing the Device Mode
- Managing FIPS Mode Devices
- Upgrading the OS Loader

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 Certified Platforms

---

ScreenOS 5.4.0r4 is FIPS certified on the following platforms:

- NS-5GT
- NS-204/208
- NS-500
- ISG-1000
- ISG-2000
- NS-5200/5400
- SSG 5/20
- SSG 520M/550M

## Restrictions

---

ScreenOS images that run in FIPS mode must be authenticated before loading. To perform the authentication, the NetScreen DSA public key must be present. You must contact technical support to retrieve a key. To load the key on to the security device, use the **save image-key** CLI command.

FIPS mode restricts the following on a security 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 SSHv2 and 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 security device:

- The modem port is disabled.
- Administration via SNMP Read-Write community is disabled. Monitoring via the Read-Only community remains available.
- The Global-Pro reporting agent is disabled.
- Loading and output configuration files to a TFTP server is disabled.
- Administration via SSL is disabled.
- The DES and MD5 algorithms are disabled.

## 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:



**CAUTION:** Switching the device to FIPS mode causes the device configuration to revert back to factory defaults. The device automatically resets.

---

```
Enable FIPS mode? [y]/n y
```

## 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: 5.4.0r4.0, Type: Firewall+VPN
Base Mac: 0010.db90.f770
File Name: ns200.5.4.0r4.0, Checksum: 48e3d429
```

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

## Disabling FIPS Mode

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

```
unset fips-mode enable
```

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

```
unset fips-mode enable
```



**CAUTION:** Switching the device to FIPS mode causes the device configuration to revert back to factory defaults. The device automatically resets.

---

```
Disable FIPS mode? [y]/n y
```

## Managing FIPS Mode Devices

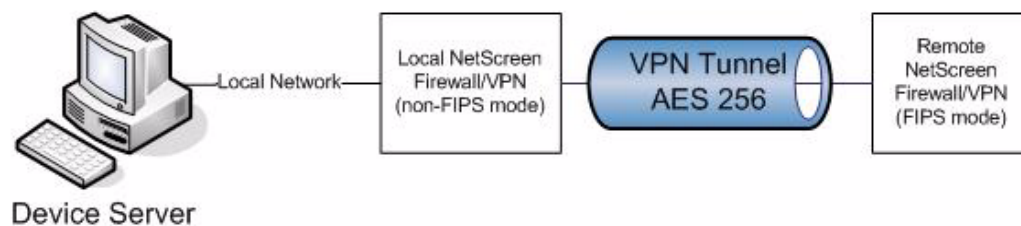
A security device that is operating in FIPS mode requires Telnet, WebUI, and all NetScreen-Security Manager traffic to be protected by a VPN with 256-bit AES encryption. This requires a manually configured VPN tunnel between the remote device that is to be managed and a local VPN device. The local VPN 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.



All management traffic should be directed to the interface that terminates the VPN on the managed FIPS device.

### 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,0123456789abcdef,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.

## Upgrading the OS Loader

FIPS mode requires both the firmware and OS loader to be digitally signed. Before the ISG 1000, ISG 2000, NS-5200-M2 and NS-5400-M2 devices can support ScreenOS 5.4.0r4 in FIPS mode, you might need to upgrade the OS loader if it is not a signed version. You can see the OS loader version number scroll by during the boot process or by entering the `get envar` CLI command.

If the OS loader on the device is not signed, when you enable FIPS mode on the device the following error message appears:

```
*****Invalid DSA signature
*****Bogus image - not authenticated
```

The following OS loaders are required for operation in FIPS mode:

**Table 1: Required OS Loaders for FIPS**

Device	OS Loader Version	OS Loader File Name
ISG 1000	1.0.1	load1000v101.d
ISG 2000	1.1.5	load2000v115.d
NS-5200/5400	1.0.0	load5000v100.d

To upgrade the OS loader on the device, you need to download the appropriate OS loader from the Juniper Networks support site to the root directory of a TFTP server.

1. Go to <http://juniper.net/customers/support> and log in using your user credentials.
2. In the Download Software section, download the software from the ScreenOS 5.4.0r4 folder.
3. Download the latest OS loader and save it to the root directory of your TFTP server.
4. If necessary, start the TFTP server.
5. Establish an Ethernet connection from the device hosting the TFTP server to the MGT port on the device, and a serial connection from your workstation to the console port on the device.
6. Restart the device by entering the `reset` CLI command. When prompted to confirm the command—`System reset, are you sure? y/[n]`—press the Y key.
7. When you see a prompt similar to the following, press the X key and then the A key in sequence:
 

```
NetScreen NS-ISG 2000 BootROM V0.9.0 (Checksum: 8796E2F3) Copyright (c)
1997-2004 NetScreen Technologies, Inc. Total physical memory: 1024MB Test -
Pass Initialization..... Done
Hit key 'X' and 'A' sequentially to update OS Loader....
```
8. A set of prompts similar to those shown below will be displayed. Enter the filename for the OS loader software you want to load (for example, `load2000v115.d.`), the IP address of the device, and the IP address of your TFTP server:

Serial Number [0079112003000031]: READ ONLY  
BOM Version [C06]: READ ONLY  
Self MAC Address [0010-db58-c900]: READ ONLY  
OS Loader File Name [boot2000v090.ld.S]: load2000v115.d  
Self IP Address [10.150.65.152]: TFTP IP Address [10.150.65.151]:

9. After entering the name of the OS loader file and the IP addresses of the device and TFTP server, the device will attempt to download the OS loader from the TFTP server.

```
Save loader config (112 bytes)...  
Done Loading file "load2000v115.d" ...  
rtatatatata ...  
Loaded successfully! (size = 383,222 bytes)  
Image authenticated!  
Program OS Loader to on-board flash memory...  
+++++Done!  
Start loading..... Done.
```

You have completed the upgrade of the OS loader.

## Copyright Notice

---

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

## FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.



**CAUTION:** Changes or modifications to this product could void the user's warranty and authority to operate this device.

---

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.