Juniper Networks ScreenOS Release Notes

Products: NetScreen Hardware Security Client (HSC), NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500, Integrated Security Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 500 Series, and NetScreen-5000 Series.

Version: ScreenOS 5.4.0r1

Revision: Rev 05

Part Number: 530-015765-01

Date: 10-24-2006

Contents

1. Version Summary

ScreenOS 5.4.0 is the latest version of ScreenOS firmware for the following products: NetScreen-5GT Series, NetScreen Hardware Security Client (HSC), NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 520, SSG 550, Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, NetScreen-5200, and NetScreen-5400 security devices.

This release incorporates ScreenOS maintenance releases 5.3r3, 5.2r3, 5.1r4b, and 5.0r9.

The ScreenOS 5.4.0 release is interoperable with and provides basic support for all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions.

NetScreen-Security Manager, version 2005.3 and earlier, does not support ScreenOS 5.4.0. You can use NetScreen-Security Manager, version 2006 to manage devices running ScreenOS 5.4.0. To do this, install a schema upgrade on the management server and user interface. The upgrade is available at the ScreenOS Customer Download page at http://www.juniper.net/spgdownloads/. Please refer to the NetScreen-Security Manager release notes for installation instructions and the features supported with this schema upgrade.

---

2. Documentation Changes

Some device messages text has changed. Refer to the *ScreenOS Messages Log Reference Guide* for ScreenOS 5.4 for details.

3. New Features and Enhancements

The following sections describe new features and enhancements.

You must register your product at http://support.juniper.net so that licensed features, such as antivirus, deep inspection, and virtual systems, can be activated on the device. To register your product, you need the model and serial number of the device. At the support page:

- If you already have an account, enter your user ID and password.
- If you are a new Juniper Networks customer, first create an account, and then enter your ID and password.

After registering your product, confirm that the device has Internet connectivity. Use the **exec license-key update all** CLI command to make the device connect to the Juniper Networks server to activate the feature.

3.1 External Antivirus

In ScreenOS 5.4.0, ICAP AV scanning is supported on ISG 1000 and ISG 2000 devices only.

External AV scanning includes the following features:

- Supports ICAP v1.0 and is fully compliant with RFC 3507
- Supports Symantec scan engine version 5.0 ICAP server
- Supports persistent connection to the same ICAP server Persistent connection reduces overhead processing overhead and enhances AV scanning throughput.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 4, Chapter 4, "Content Monitoring and Filtering."

3.2 Internal AV Extended to the SSG Devices

The integrated Juniper/Kaspersky antivirus (AV) scan engine is supported on the SSG products. Maximum memory and a license is required to activate this feature.

3.3 Integrated Web Filtering and Anti-Spam Extended Support

Integrated web filtering and anti-spam support is now available on the following devices: NetScreen-Hardware Security Client, NetScreen-5GT Series, NetScreen-25, NetScreen-50, ISG 1000, ISG 2000, and SSG 500 Series.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 4, Chapter 4, "Content Monitoring and Filtering."

3.4 DI Signature-Pack Selection Enhancement

A drop-down menu in the WebUI indicates the DI signature packs available. Also, the CLI command is simplified to specify the signature pack name instead of typing the URL.

3.5 DHCP Packets Relay Enhancement

You can configure a security device to relay all Dynamic Host Control Protocol (DHCP) responses from multiple servers to a client.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 2, Chapter 8, "System Parameters."

3.6 Configuring Next-Server-IP

The **Next-Server-IP** field is a DHCP configuration parameter that has traditionally been used as the address of the TFTP server in the bootstrap process. This Next-Server-IP information is returned in the **siaddr** field of the DHCP header and is used to chain several bootstrap servers together, with each serving a specific function. ScreenOS 5.4 supports Next-Server-IP to be configured for Option66 (**siaddr=Option66**), which identifies the TFTP server for supporting diskless PCs.

3.7 Get Tech Feature

The Get Tech feature on the Web UI (Help > Ask Support) helps Juniper Networks troubleshoot ScreenOS issues. This feature (available to read-only and read-write admins) allows you to save the complete configuration of your device to a text file on your local drive.

This command produces the same output as the **get tech** CLI command.

3.8 ICMP Unreachable Handling

For different levels of security, the default behavior for Internet Control Message Protocol (ICMP) unreachable errors from downstream routers is as follows:

- Sessions do not close for ICMP type 3 code 4 messages.
- Sessions do not close on receiving any kind of ICMP unreachable message.
- Sessions store ICMP unreachable messages, thereby restricting the number of messages flowing through to 1.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 2, Chapter 5, "Building Blocks for Policies."

3.9 Source Interface Option for DNS Servers

You can now use the **src-interface** option to specify the source interface used when querying each defined Domain Name System (DNS) server. By default, this is set to **none**, which means the device will choose the interface closest to the DNS server.

3.10 General Packet Radio Service

The General Packet Radio Service (GPRS) is enhanced in ScreenOS as follows:

- GPRS support on the ISG 1000 and ISG 2000 devices.
- Support for the following 3GPP R6 Information Elements: Radio Access Technology (RAT), Routing Area Identity (RAI), User Location Information (ULI), Access Point Name (APN) Restriction, International Mobile Equipment ID-Software Version (IMEI-SV)
- GTP-aware security devices now allow Stream Control Transmission Protocol (SCTP) messages to pass through the firewall.

3.10.1 Combination Support for IE Filtering

ScreenOS is enhanced to concurrently support R6 filtering on Information Elements (IEs).

By default, the security device does not perform IE filtering on GTP packets.

In each command line, attributes are *anded* in the following order of precedence:

- RAT

- RAI
- ULI
- IMEI
- MCC-MNC

Whenever you set an attribute restriction, you must also specify an APN.

For example, if you want the security device to pass GTP messages containing RAT 1 *and* RAI 567* *and* MCC-MNC 56789, *or* to pass messages with RAI 123*, but to default to drop packets with any APN value, the following configuration will accomplish this:

```
set rat 1 rai 567* mcc-mnc 56789 apn * pass
set rai 123* apn * pass
set apn * drop
```

The first line of the configuration causes the security device to pass GTP messages containing RAT 1, RAI 567*, MCC-MNC 56789, *and* any APNs. The second line of the configuration causes the device to pass messages containing RAI 123* and any APNS. The third line causes the device to drop any APNs.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide, Volume 13: General Packet Radio Service.*

3.11 Router Discovery Protocol

Internet Control Message Protocol Router Discovery Protocol (IRDP) is an ICMP message exchange between a host and a router (refer to RFC 1256). The security device is the router and advertises the IP address of a specified interface periodically or on demand.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 7, Chapter 10, "Internet Control Message Protocol Router Discovery Protocol."

3.12 IPv6

ScreenOS 5.4.0 introduces dual-stack architecture for Internet Protocol Version 6 (IPv6) on the ISG 2000 device only. IPv6 is not available for the ISG 2000 device with Intrusion Detection and Prevention (IDP).

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide, Volume 14: Dual-Stack Architecture with IPv6*.

3.13 Password Policy Support

The password policy feature allows you to enforce a minimum length and complexity scheme for administrator (admin) and authenticated (auth) user passwords. The password policy feature is intended for use in a local database, and therefore is useful in environments where the Windows directory or RADIUS are not available to provide centralized password policy enforcement.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 3, Chapter 1, "Administration."

3.14 Policy-Based Routing

With Policy-Based Routing (PBR), you can implement policies that selectively cause packets to take different paths. PBR is the first item checked as part of the route lookup process and is transparent to all non-PBR traffic. PBR is configured at the interface level, but you can bind PBR policies to the interface, zone, virtual router (VR) or a combination of interface, zone, or VRs.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 7, Chapter 6, "Policy-Based Routing."

3.15 Service Timeout

To derive the correct service timeout value when the destination port is overloaded with multiple services that have different timeouts values set, the port-based service timeout table lookup is not used; instead, ScreenOS 5.4.0 uses service lookup within the service group based on the destination port.

3.16 SNMP Enhancements

New MIBs are available to permit polling of fault and health status of Security Modules within ISG 1000 and ISG 2000.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 3, Chapter 2, "Monitoring Security Devices."

3.17 Universal Serial Bus Port

Some devices support a universal serial bus (USB) port which allows file transfers, such as device configurations, user certifications, and update version images between an external USB flash key and the internal flash storage located in the security device. The USB host module supports USB 1.1 specification at either low-speed (1.5M) or full-speed (12M) file transfer.

This feature is available only on the SSG 5, SSG 20, and SSG 140 devices.

3.18 Virtual Systems Enhancements

Enhancements have been made to vsys in the following areas:

- Virtual private networking (VPN): You can now view IPSec security associations (SAs) and IKE cookies either at the root level for details from all vsys on a security device or within a vsys context for details from a particular vsys. You can also use the policy scheduler within a vsys.
- Vsys management:
    - Robust vsys profiles to allow for service differentiation.
    - CPU session limits, reserves, and alarms for each vsys.
    - CPU over utilization protection in the form of enforceable quotas for CPU load caused by individual vsys.
- DHCP: DHCP relay for vsys is fully supported. You can configure DHCP relay for a specific vsys and relay all packets from multiple DHCP servers to a client.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 10, Chapter 1, "Virtual Systems," and Volume 2, Chapter 8, "System Parameters."

3.19 SCCP Support

The Skinny Client Control Protocol (SCCP) is supported on security devices in Route, Transparent, and Network Address Translation (NAT) mode.

For more information, refer to the *Concepts & Examples ScreenOS Reference Guide*, Volume 6, Chapter 4, "Skinny Client Control Protocol Application Layer Gateway."

3.20 Wide Area Network Support

Some security devices support wide area network (WAN) interfaces such as Serial, T1, E1, T3, ADSL, ISDN, and V.92.

Traffic shaping parameters can only be applied to the following WAN interfaces with the following encapsulation types:

- Single T1 or E1 interface that is using PPP or HDLC encapsulation
- ADSL 2+ interface that is using PPP encapsulation
- Single ISDN BRI S/T that is using PPP or MLPPP encapsulation

Frame Relay and Multilink Frame Relay will not work when Quality of Service (QoS) is applied to the encapsulation types mentioned above with the specified WAN interfaces.

ScreenOS 5.4 does not support QoS over a MLPPP link.

For more information about WAN interfaces, refer to the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS 5.4.0.

3.21 Wireless Enhancements

The following wireless enhancements enable you to better manage and secure a wireless local area network (WLAN):

- WPA2
- Wi-Fi Multimedia (WMM) Quality of Service feature
- eXtended Range™
- 802.11a/b/g
- Super A/G

3.22 XAuth with Internet Key Exchange Mode Enhancements

You can now monitor the IP address the security device allocates to the client when a remote user accesses the network through Internet Key Exchange (IKE) mode, ScreenOS authenticates the user with XAuth, and records the event details in the traffic log. Allocated IP addresses can come from the local IP pool or a RADIUS server.

3.23 IDP Internal Policy Representation Changes

After upgrading the ISG 1000 or ISG 2000 with security modules to ScreenOS 5.4.0, users must install the 5.4.0 zero day patch upgrade to Netscreen-Security Manager and re-push the IDP policy to the device.

4. Changes to Default Behavior

This section lists changes to default behavior in ScreenOS 5.4.0 from previous ScreenOS firmware releases.

4.1 DHCP Changes

The Dynamic Host Control Protocol (DHCP) CLI command syntax is modified. Previously, the DHCP command began with **set dhcp**. In ScreenOS 5.4.0, DHCP commands begin with **set interface** *interface* **dhcp**...

4.2 Virtual System Changes

The policy scheduler is now available in the virtual system (vsys) context.

Vsys names must be 10 or fewer characters in length or the device rejects the command and issues an error message. Prior to this release, the device silently truncated the vsys name and performed the requested operation on the truncated name.

4.3 Antivirus Changes

Changed Antivirus (AV) HTTP default values include the following:

- **Connection keep-alive**—the default is now on. Previously, the default was off.
- **Webmail-only mode**—the default is now off. Previously the default was on.

When you upgrade to ScreenOS 5.4,0, the security device retains your settings for **connection keep-alive** and **webmail-only** from your previous software version. CLI output after the upgrade will reflect this. For example, if you are running ScreenOS 5.3 and using the 5.3 default values for **connection keep-alive** and **webmail-only**, and you upgrade to ScreenOS 5.4.0, the ScreenOS detects the values the device was using and reconfigures them. You will see the following two command lines entries logged:

```
unset av http keep-alive
set av http webmail enable
```

4.4 TCP Changes

Upon software upgrade, the Transmission Control Protocol-Request-To-Send (tcp-rst) values for Layer 2 predefined zones (v1-untrust, v1-trust, v1-dmz, v1-null) change from true to false.

4.5 Zone Changes

The maximum allowed number of zones includes only user-defined security zones. Predefined security zones are no longer deducted from the security zone quota/license number. The quota/license number for each security device remains the same, as the previous releases.

4.6 Downgrade Behavior

A downgrade from ScreenOS 5.4.0 to 5.3.0 can cause configuration loss. We recommend that you save a copy of your configuration file before upgrading or downgrading. This issue is caused by new CLI context. When ScreenOS 5.4.0 CLI context is unrecognized by 5.3.0, the subsequent exit will execute and log the user off (or terminate configuration loading).

Any modification (set/unset) to the **proxy-ip** address of the VPN causes the security device to delete the associated active Security Associations (SA).

4.7 Webauth Login

To accommodate the login banner, WebAuth authentication is changed from HTTP basic authentication to HTTP form-based authentication similar to the WebUI admin login page. After entering your username and password you must click the **Login** button. Pressing the **Enter** key will not log you into the device. This change in behavior also applies to WebUI login.

4.8 Anti-Spam Changes

The new anti-spam black/white list sizes for specific security devices are as follows:

- NetScreen-5GT Series: 500
- NetScreen-25/50: 500
- ISG 1000/2000: 1500
- SSG 500 Series: 1500

Use the following command to cause the security device to scan for known spammer IP addresses:

device-> exec anti-spam testscan <*IP addr*>

4.9 TCP Reset Handling

In previous ScreenOS releases, if TCP SYN check is not enabled, the first TCP RST packets arriving at the security device cause sessions to be created and then immediately torn down. During a TCP RST attack, this behavior can lead to high CPU utilization and a high session-creation rate.

In ScreenOS 5.4.0, if TCP SYN check is not enabled, the security device drops the first TCP RST packets without creating new sessions. This behavior change applies only if TCP SYN check is not enabled.

4.10 Snoop ... detail Command

In releases of ScreenOS prior to 5.4.0, administrators with at least read/write privileges can issue the **snoop … detail** command, which allows them to view the sensitive contents of packets. In release 5.4.0, only the root-level administrator can use the **snoop … detail** command and view packet contents. Administrators with read/write privileges can still issue the **snoop** command, but the **detail** option is not available to them.

Note that there is still only a single dbuf buffer for holding the contents of SNOOP. If a root-level administrator defines filter set A and enables **snoop … detail** and then a read/write administrator defines filter set B and also enables **snoop**, the logical OR of these two filters will appear in the **dbuf** buffer. Both administrators will be able to view the contents of the dbuf buffer.

4.11 Login Banner

The size of the login banner is increased to a maximum of 4Kb. This provides space for terms of use statements, which are presented before administrators and authenticated users log into the security device and into protected resources behind the device. The login banner is a clear text ASCII file you create and store on the security device, the file must be called **usrterms.txt**. You activate the banner by restarting of the device. If the banner file is greater than 4Kb, the security device will not accept it and will continue using existing banners entered through the CLI and the WebUI.

When activated, the login banner is used globally by the root device and all virtual systems (vsys). You cannot differentiate or customize between or within a vsys. The login banner pre-empts all individually defined administrative access banners and firewall authentication banners. After entering a username and password, the user must click the **Login** button. Pressing the **Enter** key will not log the user into the device.

Use the SCP utility to securely copy the banner file to the security device. With the following command, an administrator with username **netscreen** copies the banner file **my_large_banner.txt** to a security device at IP address 1.1.1.2. The banner file must be saved on the security device as **usrterms.txt**.

```
linux:~#scp my_large_banner.txt netscreen@1.1.1.2:usrterms.txt
```

You must restart the device to activate the new banner. To modify the banner file, create a new file and overwrite the existing one with the new one.

To remove the banner, issue the following command on the security device:

```
device-> delete file usrterms.txt
```

This disables the login banner feature after you restart the device.

4.12 Shared Zone

For performance reasons, the resource usage of an address group configured in any vsys is charged to the root vsys where the shared zone was created.

4.13 Set and Unset Vsys

When you set and unset vsys using a vsys name exceeding allowed maximum length of 10, it is rejected instead of truncated and set or unset silently.

4.14 IPSec Access Session Hold Time

In an IAS configuration, if hold-time is non-zero Security Associations (SAs) can be deleted even if encryption keys are currently active. This behavior also exists for non-IAS authentication. To disable the hold-time functionality, you must explicitly set the hold-time value to 0, as follows:

```
device-> set ike member-sa-hold-time 0
```

4.15 Boot Up with GBIC Unplugged

On the NetScreen-5000 Series device using the 5000-M2 management module, when you boot the device with a GBIC unplugged, the interface is disabled and remains disabled even after you later plug in a GBIC. This behavior is due to the software skipping port initialization after GBIC detection fails. The solution is to fully initialize the Gigabit Ethernet port whether GBIC is plugged or unplugged.

4.16 Member SA Hold Time

For Dial-up VPNs, if no VPN idle timeout is configured locally or from a RADIUS server for a specific IPSec member security association (SA), member SA hold time is used.

4.17 Maximum Mapped IP

In previous releases of ScreenOS, the maximum number of supported Mapped IP (MIP) addresses for the NetScreen-50 device was 1500. In this release, maximum supported MIPs is reduced to 1000.

4.18 SCEP Polling Interval

SCEP polling interval is now limited to 51800 minutes (360 days).

4.19 Dead Peer Detection

In previous ScreenOS releases, when Dead Peer Detection (DPD) is enabled, a gateway configured as a XAuth server sends out DPD messages by default, even when there is no traffic to the gateway. In ScreenOS 5.4.0, you must set **dpd always-send** to detect a dead peer even when there is no traffic.

4.20 Transition from Transparent mode to L2 VSYS

To transition a security device from transparent mode to L2 VSYS, you must issue the **unset all** CLI command and restart the device. ScreenOS 5.4.0 does not support a mix of L2 ports and L3 ports on the same device.

4.21 Unnumbered Interfaces

When unsetting an unnumbered interface from the CLI, some configuration might remain. To prevent ScreenOS from retaining previous configuration after unsetting an unnumbered interface, restart the device.

4.22 Users in Groups

Previous releases erroneously allowed non-auth users to be members of more than one user group. This configuration is now prohibited and all subsequent assignments of the same non-auth user to a user group are removed from the configuration file.

4.23 VPN Policies

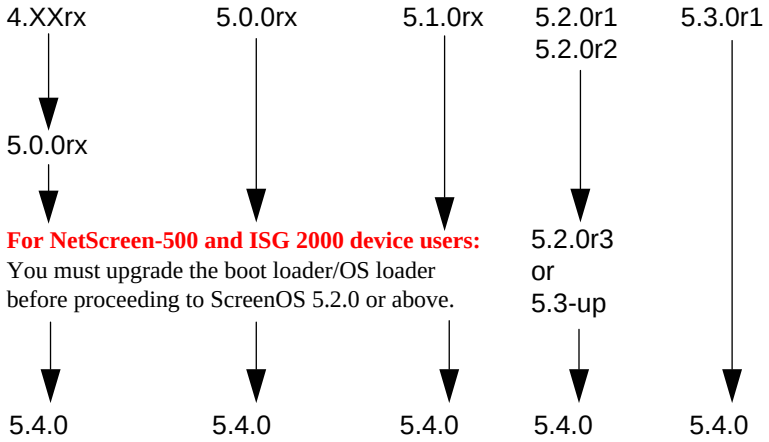
Configurations using multiple VPN policies with the same proxy-ids are no longer valid. During initial startup of ScreenOS 5.4.0, the second defined VPN policy and any subsequent VPN policy with the same proxy-id will be removed from the configuration.

5. Migration Procedures

This section contains procedures to upgrade existing firmware to ScreenOS 5.4.0.

Before you upgrade a security device, you must have the most recent ScreenOS firmware stored on your local drive. Depending on the device and the firmware your security device is currently running, you also might need intermediate (or step-up) firmware and/or new boot loader firmware. Firmware Upgrade Path illustrates the various firmware upgrade paths to ScreenOS 5.4.0.

Firmware Upgrade Path



Upgrade Paths to ScreenOS 5.4.0 lists the recommended upgrade path to ScreenOS 5.4.0 based on device model and firmware version. For example, if you are running ScreenOS 4.0 on a NetScreen-204, you need to upgrade to ScreenOS 5.0r10 or later before upgrading to ScreenOS 5.4.0. If you are running ScreenOS 5.1 on a NetScreen-204, however, you can upgrade directly to 5.4.0. Upgrade Paths to ScreenOS 5.4.0 also lists memory and boot loader upgrade requirements for each ScreenOS version and device.

Upgrade Paths to ScreenOS 5.4.0

Base	Device Name	Intermediate Firmware Name	Upgrade Requirement
4.0	NetScreen-200 Series	5.0r10 or later	Boot loader upgrade not required
	NetScreen-25	5.0r10 or later	Boot loader upgrade not required
	NetScreen-50	5.0r10 or later	Boot loader upgrade not required
	NetScreen-5000 Series using 5000-M	5.0r10 or later	
5.0	NetScreen-HSC	5.0r10 or later	
	NetScreen-5GT Series	5.0r10 or later	
	NetScreen-25	5.0r10 or later	
	NetScreen-50	5.0r10 or later	
	NetScreen-200 Series	5.0r10 or later	
	NetScreen-500	5.0r10 or later	Requires boot loader upgrade. See section 5.2.1 NetScreen-500 Boot-R
	ISG 1000	5.0r10 or later	
	ISG 1000-IDP	5.0r10 or later	Requires boot loader 1.1.5 upgrade.
	ISG 2000	5.0r10 or later	Requires boot loader 1.1.5 upgrade.
	ISG 2000-IDP	5.0r10 or later	Requires boot loader 1.1.5 upgrade.
	NetScreen-5000 Series using 5000-M	5.0r10 or later	Requires SIMM DRAM upgrade to 1GB (see note below)
	NetScreen-5000 Series using 5000-M2	5.0r9 or later	Requires SIMM DRAM upgrade to 1GB (see note below)
5.1	NetScreen-HSC	None required	
	NetScreen-5GT	None required	
	NetScreen-25	None required	
	NetScreen-50	None required	
	NetScreen-200 Series	None required	
	SSG 500 Series	Factory installed with 5.1r4	

	NetScreen-500	None required	Requires boot loader upgrade. See section 5.2.1 “NetScreen-500 Boot-ROM”.
	NetScreen-5000 Series using 5000-M	None required	
5.2	NetScreen-HSC	5.2r3 or later	
	NetScreen-5GT	5.2r3 or later	
	NetScreen-5GT ADSL	5.2r3 or later	
	NetScreen-25	5.2r3 or later	
	NetScreen-50	5.2r3 or later	
	NetScreen-200 Series	5.2r3 or later	
	NetScreen-500	5.2r3 or later	
	ISG 2000	5.2r3 or later	Requires boot loader 1.1.5 upgrade
	NetScreen-5000 Series using 5000-M	5.2r3 or later	Requires SIMM DRAM upgrade to 1GB (see note below)
	NetScreen-5000 Series using 5000-M2	5.2r3 or later	Requires memory upgrade Requires SIMM DRAM upgrade to 1GB (see note below)
5.3	NetScreen-HSC	None required	
	NetScreen-5GT Series	None required	
	NetScreen-25	None required	
	NetScreen-50	None required	
	NetScreen-200 Series	None required	
	NetScreen-500	None required	
	ISG 1000	None required	
	ISG 2000	None required	Requires boot loader 1.1.5 upgrade
	NetScreen-5000 Series using 5000-M	None required	Requires SIMM DRAM upgrade to 1 GB (see note below).
	NetScreen-5000 Series using 5000-M2	None required	Requires SIMM DRAM upgrade to 1 GB (see note below).

This release requires the SIMM DRAM upgrade to 1GB on the NetScreen-5000 Series devices. Secure Port Modules (SPMs) affected are 5000-8G2 and 5000-2XGE manufactured before 2/1/2006. If your SPMS qualify for a memory upgrade, please contact Juniper Networks at 1-866-369-5418 or email Junipermem@onprocess.com for a memory-upgrade kit. The memory upgrade is free for qualified users.

Before upgrading or downgrading a security device, save the existing configuration file to avoid losing any data. During the upgrade/downgrade process, the device might remove part or all of the configuration file.

5.1 Requirements for Upgrading and Downgrading Device Firmware

This section lists what is required to perform the upgrade or downgrade of security device firmware. You can use any of the following methods to upgrade or downgrade a security device:

- WebUI
- CLI
- Through the boot loader or ScreenOS Loader

You can upgrade or downgrade some security devices locally or remotely, but we recommend that you perform the upgrade or downgrade of a security device at the device location. For NetScreen-500 and ISG 2000 devices, both of these operations require console access, therefore you must be at the device location.

To use the WebUI, you must have the following:

- Root privilege to the security device
- Network access to the security device from a computer that has a browser
- New ScreenOS firmware (downloaded from the Juniper Networks website and saved locally)

To use the CLI, you must have the following:

- Root or read-write privileges to the security device
- Console connection or Telnet access to the security device from a computer
- TFTP server installed locally and to which the security device has access
- New ScreenOS firmware (downloaded from the Juniper Networks website and saved to a local TFTP server directory)

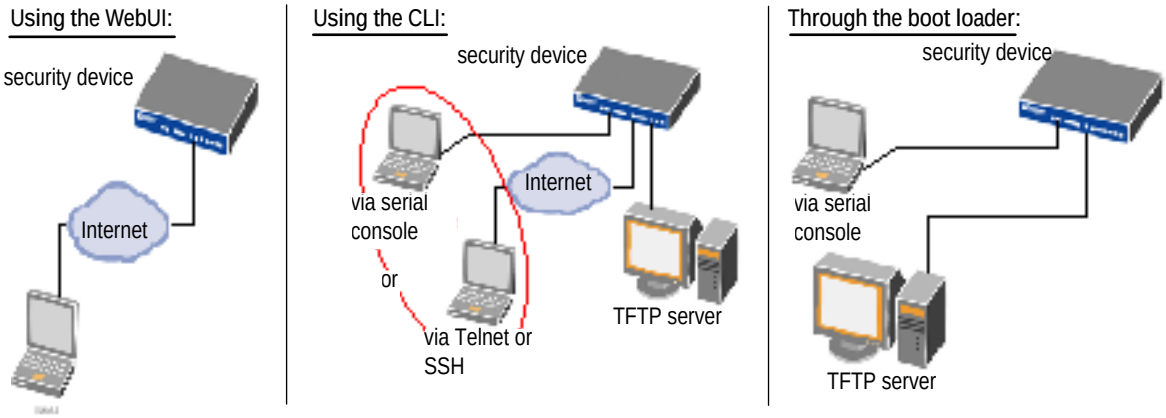
To upgrade or downgrade through the boot loader, you must have the following:

- Root or read-write privileges to the security device

- TFTP server installed locally that has an IP address in the same subnet as the security device (255.255.255.0)
- Ethernet connection from a computer to the security device (to transfer data, namely from a local TFTP server)
- Console connection from the computer to the security device (to manage the security device)
- New ScreenOS firmware saved to a local TFTP server directory

ScreenOS Upgrade and Downgrade Methods shows the three different ways by which you can upgrade or downgrade a security device.

ScreenOS Upgrade and Downgrade Methods



For NetScreen-500 and ISG 2000 devices, if a boot loader upgrade is required, you must upgrade using the boot loader.

To upgrade or downgrade a security device, see the step-by-step procedures in section Upgrading to the New Firmware, or section Upgrading Devices in an NSRP Configuration.

5.2 Special Boot-ROM or Boot Loader Requirements

Some devices require upgrade of the boot-ROM or boot loader before or during upgrade.

5.2.1 NetScreen-500 Boot-ROM

Installation of this release on a NetScreen-500 device running ScreenOS 5.0 or 5.1 requires the new boot-ROM (ns500.upgrade6M). This makes the upgrade a two-step process. In the first step you install the boot ROM, in the second step you actually install the new image.

Boot-ROM is referred to as *intermediate firmware* in Step 3 in section Upgrading Using the WebUI, and section Upgrading Using the CLI.

5.2.2 ISG 2000 Boot Loader

Before upgrading an ISG 2000 device from ScreenOS 5.0 to ScreenOS 5.4.0 firmware, you must upgrade the OS loader to v1.1.5. You can view the OS loader version during the startup process or by entering the **get envar** CLI command. To upgrade the OS loader, perform the following steps:

1. Download the OS loader from the Juniper Networks support site to the root directory of your TFTP server.

2. Visit http://www.juniper.net/support and log in.

3. In the Download Software section, click **ScreenOS Software**.

4. Download the latest OS loader and save it to the root directory of your TFTP server.

5. If necessary, start the TFTP server.

6. Make an Ethernet connection from the device hosting the TFTP server to the MGT port on the ISG 2000 and a serial connection from your workstation to the console port on the ISG 2000.

7. Restart the ISG 2000 with the **reset** CLI command. When prompted to confirm the command—System reset, are you sure? y/[n] — press the Y key.

   The following device output appears:

   ```
   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
   ```

8. Press the X and A keys sequentially to update the OS loader.

9. Enter the filename for the OS loader software you want to load (for example, load2000v115.d.S), the IP address of the ISG 2000, and the IP address of your TFTP server. The following system output appears:

   ```
   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.S
   Self IP Address [10.150.65.152]:
   TFTP IP Address [10.150.65.151]:
   Press the Enter key, and the file loads.
   Save loader config (112 bytes)... Done
   Loading file "load2000v115.d.S"...
   rtatatatatata ...
   Loaded successfully! (size = 383,222 bytes)
   Ignore image authentication!
   Program OS Loader to on-board flash memory... ++++++++++++++++++++++++Done!
   Start loading...
   ......................
   Done.
   ```

10. The OS loader upgrade is now completed.

5.3 Downloading New Firmware

You can obtain the ScreenOS firmware from the Juniper Networks website. To access firmware downloads, you must be a registered customer with an active user ID and password. If you have not yet registered your Juniper Networks product, then you must do so at the Juniper Networks website before proceeding.

Before you begin a security device upgrade, you must have the most recent ScreenOS firmware. Check Upgrade Paths to ScreenOS 5.4.0 to make sure you have the required intermediate software, if any.

1. To get the latest ScreenOS firmware, enter http://www.juniper.net/support in your browser. Click Support > Customer Support Center, then perform the following steps:

   a. Log in by entering your user ID and password, then click **LOGIN**.

   b. Select **Download Software** or pick the actual product you want to download from the Quicklink picker.

      A list of available downloads appears.

   c. Click **Continue**.

      The File Download page appears.

   d. Click the product link for the firmware you want to download.

      The Upgrades page appears.

   e. Click the link for the ScreenOS version you want to download.

      The Upgrades page appears.

   f. Click the upgrade link.

      The Download File dialog box appears.

2. Click **Save** and then navigate to the location where you want to save the firmware zip file.

Before loading the firmware, you must unzip the file.

You must save the firmware onto the computer from which you want to perform the upgrade.

If you want to upgrade the security device using the WebUI, save the firmware anywhere on the computer.

If you want to upgrade the security devices using the CLI, save the firmware to the root TFTP server directory on the computer. If you do not have a TFTP server installed on your computer, then you can download one from the Internet. If no TFTP server is available, you must use the WebUI to load the new firmware onto the security device.

5.4 Upgrading to the New Firmware

This section provides instructions on how to upgrade firmware on the security device using the WebUI, the CLI, and the Boot/OS loader. This section also describes how to save multiple firmware images with the boot loader.

Before upgrading a security device, save the existing configuration file to avoid losing any data.

Upgrade Paths to ScreenOS 5.4.0 to determine whether you need to install intermediate firmware or a boot loader upgrade before installing ScreenOS 5.4.0. Use either the WebUI or CLI procedure to first install intermediate firmware (if required), then install ScreenOS 5.4.0 firmware.

5.4.1 Upgrading Using the WebUI

This section describes how to upgrade the firmware on the security device using the WebUI. Instructions include upgrading to an intermediate version of firmware, if required, and upgrading to ScreenOS 5.4.0.

To upgrade firmware using the WebUI, perform the following steps:

1. Log into the security device by opening a browser:
   a. Enter the Management IP address in the *Address* field.
   b. Log in as the root admin or an admin with read-write privileges.
2. Save the existing configuration:
   a. Go to Configuration > Update > Config File, and click **Save to File**.
   b. In the File Download dialog box, click **Save**.
   c. Navigate to the location where you want to save the configuration file (cfg.txt), and click **Save**.
3. Upgrade to intermediate firmware, if required.

   Upgrade Paths to ScreenOS 5.4.0 to determine if intermediate firmware is required. If intermediate firmware is required, follow this procedure. Otherwise, proceed to Step Upgrade to the new ScreenOS firmware

   a. Go to Configuration > Update > ScreenOS/Keys and select **Firmware Update**.
   b. Click **Browse** to navigate to the location of the intermediate firmware.
      For example, if you upgrade a NetScreen-5GT running ScreenOS 5.2r1, you must upgrade to ScreenOS 5.2r3 or later, then continue this procedure.
   c. Click **Apply**.

   This process takes some time. DO NOT click **Cancel** or the upgrade will fail. If you click **Cancel** and the upgrade fails, power off the device and then power it on again. Restart the upgrade procedure beginning with step 3.

   ---

   d. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

   e. Log into the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI homepage.
4. Upgrade to the new ScreenOS firmware

a. Go to Configuration > Update > ScreenOS/Keys and select **Firmware Update**.

b. Click **Browse** to navigate to the location of the new ScreenOS firmware or enter the path to its location in the Load File field.

c. Click **Apply**.

A message box appears with information on the upgrade time.

d. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

5. Log into the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI homepage.

5.4.2 Upgrading Using the CLI

This section describes how to upgrade the firmware on the security device using the CLI. Instructions include upgrading to an intermediate version of the firmware, if required, and upgrading to ScreenOS 5.4.0.

To upgrade firmware using the CLI, perform the following steps:

1. Make sure you have the new ScreenOS firmware, or the intermediate firmware if required, in the TFTP root directory. For information on obtaining the new firmware, see section Downloading New Firmware.

2. Run the TFTP server on your computer by double clicking on the TFTP server application. You can minimize this window, but it must be active in the background.

3. Log into the security device using an application such as Telnet or SSH, (or HyperTerminal if connected directly through the console port). Log in as the root admin or an admin with read-write privileges.

4. Save the existing configuration by executing the command:

   save config to { **flash** | **slot1** | **tftp** }...

   On the security device, enter the following command and specify the filename of the firmware (if you are installing intermediate firmware, specify the filename of the intermediate firmware):

   save soft from tftp *ip_addr_your_computer screenos_filename* **to flash**

   If this upgrade requires intermediate firmware and you have not already upgraded to that firmware, enter the intermediate firmware filename when entering this command.

   ---

5. When the upgrade is complete, you must restart the security device. Execute the **reset** command and enter **y** at the prompt to restart the device.

6. Wait a few minutes, and then log into the security device again.

7. Use the **get system** command to verify the version of the security device ScreenOS firmware.

If you upgraded to intermediate firmware in step On the security device, enter the following command and specify the filename of, repeat steps 5 through 8 to install the ScreenOS 5.4.0 firmware.

8. If necessary, upload the configuration file that you saved in step 4 by executing the following command:

   save config from tftp to { **flash** | **slot1** | **tftp** }...

5.4.3 Upgrading Using the Boot/OS Loader

The Boot/OS Loader brings up the hardware system, performs basic and sometimes critical hardware configurations, and loads system software used to run a security device.

On the NetScreen-500 device, you cannot use this process to save ScreenOS 5.1.0 or previous versions of firmware to flash memory. You must use the WebUI or CLI to save ScreenOS 5.1.0 firmware to flash memory.

To upgrade firmware using the Boot/OS Loader, perform the following steps:

1. Connect your computer to the security device.
2. Using a serial cable, connect the serial port on your computer to the console port on the security device (refer to your hardware manual for console settings). This connection, in combination with a terminal application, enables you to manage the security device.
3. Using an Ethernet cable, connect the network port on your computer to port 1 or to the management port on the security device. This connection enables the transfer of data among the computer, the TFTP server, and the security device.
4. Make sure that you have the new ScreenOS firmware stored in the TFTP server directory on your computer. For information on obtaining the new firmware, see section Downloading New Firmware.
5. Run the TFTP server on your computer by double clicking on the TFTP server application. You can minimize this window but it must be active in the background.
6. Log into the security device using a terminal emulator such as HyperTerminal. Log in as the root admin or an admin with read-write privileges.
7. Restart the security device.
8. When you see “Hit any key to run loader” or “Hit any key to load new firmware” on the console display, press any key on your computer keyboard to interrupt the startup process.

   If you do not interrupt the security device in time, it loads the firmware saved in flash memory.

   ---

9. At the Boot File Name prompt, enter the filename of the ScreenOS firmware that you want to load.

If the Upgrade Paths to ScreenOS 5.4 section lists an intermediate firmware requirement, enter that filename at this step.

If you enter **slot1:** before the specified file name, then the loader reads the specified file from the external compact flash or memory card. If you do not enter **slot1:** before the filename, then the file is instead downloaded from the TFTP server. If the security device does not support a compact flash card, then an error message is displayed and the console prompts you to reenter the filename.

10. At the Self IP Address prompt, enter an IP address that is on the same subnet as the TFTP server.
11. At the TFTP IP Address prompt, enter the IP address of the TFTP server.

The Self IP address and TFTP IP address must be in the same subnet; otherwise, the TFTP loader rejects the Self IP address and then prompts you to re-enter it.

An indication that the firmware is loading successfully is the display of a series of "rtatatatatatata..." running on the terminal emulator screen and a series of symbols running on the TFTP server window. When the firmware installation is complete, a message informs you that the installation was successful. Repeat these steps if your first firmware upgrade was to an intermediate version.

5.4.4 Saving Multiple Firmware Images with the Boot Loader

After the firmware is downloaded successfully, the console prompts you:

```
Save to on-board flash disk? (y/[n]/m)
```

Entering **y** (yes) saves the file as the default firmware. This image runs automatically if you do not interrupt the startup process.

On some security devices, you can enter **m** (multiple) to save multiple firmware. You must select a filename at the following prompt:

```
Please input multiple firmware file name [BIMINITE.D]: test.d
```

The name in brackets is the recommended name automatically generated after you enter the name in the TFTP server. If you do not enter a name, the recommended name is used.

You must enter a name that is DOS 8.3 compatible. The maximum length of the boot file name used by the Loader cannot exceed 63 characters.

5.5 Downgrading the NetScreen-500 Device

Before downgrading a security device, back up the existing configuration file. The current configuration file will be lost when downgrading the device.

Perform the following steps to downgrade the NetScreen-500 device from ScreenOS 5.4.0 to ScreenOS 5.0.0 or later. If you need to downgrade the device to a version prior to ScreenOS 5.0.0, downgrade using the boot/OS loader (see Using the Boot/OS Loader).

Using the CLI

To downgrade using the CLI, perform the following steps:

1. Download the firmware from the Juniper Networks website and save it to the root TFTP server directory on the computer.

   For information on downloading the firmware, see section Downloading New Firmware.

2. Load the firmware with the CLI. For information on using the CLI to load firmware, see section Upgrading Using the CLI.

3. Enter the **exec downgrade** CLI command if you are downgraded to 4.x releases.

   The security device automatically restarts with the firmware you loaded.

Using the Boot/OS Loader

To downgrade using the boot/OS loader, perform the following steps

1. Download the firmware from the Juniper Networks website, and save it to the root TFTP server directory on the computer.

   For information on downloading the firmware, see section Downloading New Firmware.

2. Enter the **exec downgrade** command.

   The security device automatically restarts.

3. Load the firmware using the boot/OS loader. For information on using the boot/OS loader, see section Upgrading Using the Boot/OS Loader. The following system output appears:

```
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.S
Self IP Address [10.150.65.152]:
TFTP IP Address [10.150.65.151]:
```

4. Press the Enter key to load the file. The following system output appears:

```
Save loader config (112 bytes)... Done
    Loading file "load2000v115.d.S"...
```

5.6 Upgrading Devices in an NSRP Configuration

For security devices in a NetScreen Redundancy Protocol (NSRP) configuration, you must upgrade each device individually. This section describes two different upgrade procedures addressing two different NSRP configurations: NSRP active/passive and NSRP active/active.

For upgrading NetScreen-500 and ISG 2000 devices, you must follow the version-specific upgrade sequence (see section Upgrading to the New Firmware).

When upgrading, you risk losing part of the configuration that existed before the upgrade. Before upgrading a security device, we strongly recommend that you back up the existing configuration file to avoid losing any data.

5.6.1 Upgrading Devices in an NSRP Active/Passive Configuration

The following explains the steps to upgrade a basic NSRP active/passive configuration where device A is the primary and device B is the backup.

Before you begin, read section Requirements for Upgrading and Downgrading Device Firmware. Also, make sure that you download the ScreenOS firmware to which you are upgrading each device.

Do not power off your security device while it is upgrading to new firmware. Doing so could result in permanently damaging the device.

To upgrade two devices in an NSRP active/passive configuration, perform the following steps (some steps require CLI use).

1. Upgrade device B to ScreenOS 5.4.0.

WebUI

a. Make sure that you have the new ScreenOS firmware (and the intermediate firmware if required). For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into device B by opening a browser and entering the management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.

c. Save the existing configuration:

   i. Go to Configuration > Update > Config File, and then click **Save to File**.

   ii. In the File Download dialog box, click **Save**.

   iii. Navigate to the location where you want to save the configuration file (cfg.txt), then click **Save**.

d. Go to Configuration > Update > ScreenOS/Keys and select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 5.4.0 firmware, or enter the path to its location in the Load File field.

f. Click **Apply**.

   A message box appears with information on the upgrade time.

g. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. To verify the version of the ScreenOS firmware, log into the security device and go to the Device Information section of the WebUI Home page.

CLI

a. sure you have the ScreenOS 5.4.0 firmware (and the intermediate firmware, if required). For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into device B using an application such as Telnet, or SSH (or Hyper Terminal if directly connected through the console port). Log in as the root admin or an admin with read-write privileges.

c. Save the existing configuration by executing the following command:

save config to { **flash** | **slot1** | **tftp** }...

d. Start the TFTP server on your computer by doubleclicking on the TFTP server application.

e. On the security device, enter the following command:

save soft from tftp *ip_addr* **filename to flash**

where *ip_addr* is the IP address of your computer and **filename is** the filename of the ScreenOS 5.4.0 firmware

f. When the upgrade is complete, enter the **reset** command and then enter **y** at the prompt to restart the device.

g. Wait a few minutes, then log into the security device.

h. Enter the **get system** CLI command to verify the version of the security device ScreenOS firmware.

2. Manually fail over the primary device to the backup device (CLI only).

a. Log into the primary device (device A).

b. Issue one of the following CLI commands. The command that you need to execute depends on whether or not the preempt option is enabled on the primary device.

- If the preempt option is enabled:

  exec nsrp vsd-group 0 mode ineligible

- If the preempt option is not enabled:

  exec nsrp vsd-group 0 mode backup

Either command forces the primary device to step down and the backup device to immediately assume the primary device role.

3. Upgrade the primary device (device A) to ScreenOS 5.4.0.

WebUI

a. Make sure that you have the ScreenOS 5.4.0 firmware. For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into security device A.

c. Save the existing configuration:

   i. Go to Configuration > Update > Config File, and then click **Save to File**.

   ii. In the File Download dialog box, click **Save**.

   iii. Navigate to the location where you want to save the configuration file (cfg.txt), then click **Save**.

d. Go to Configuration > Update > ScreenOS/Keys and select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 5.4.0 firmware or enter the path to its location in the Load File field.

f. Click **Apply**.

   A message box appears with information on the upgrade time.

g. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. To verify the version of the ScreenOS firmware, log into the security device and go to the Device Information section of the WebUI Home page.

CLI

a. Make sure you have the ScreenOS 5.4.0 firmware.

b. Log into security device A.

c. Save the existing configuration by executing the following command:

   save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double clicking on the TFTP server application.

e. On the security device, execute the following command:

   save soft from tftp *ip_addr_your_computer screenos_filename* **to flash**

f. When the upgrade is complete, you must restart the security device. Execute the **reset** command and enter **y** at the prompt to restart the device.

g. Wait a few minutes, and then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

4. Synchronize device A (CLI only).

   After you complete the upgrade of device A to ScreenOS 5.4.0, manually synchronize the two devices. On device A (backup), issue the **exec nsrp sync rto all** command from the peer CLI to synchronize the RTOs from device B (primary device).

5. Manually fail over the primary device to the backup device (CLI only).

a. Log into the primary device (device B).

b. If pre-empt is enabled on device A, no action is needed. If pre-empt is not enabled on device A, issue the following CLI command:

exec nsrp vsd-group 0 mode backup

Either command forces the primary device to step down and the backup device to immediately assume the primary device role.

5.7 Upgrading Devices in an NSRP Active/Active Configuration

This upgrade section applies to an NSRP configuration where you paired two security devices into two virtual security devices (VSD) groups, with each physical device being the primary in one group and the backup in the other. To upgrade, you first have to fail over one of the devices so that only one physical device is the primary of both VSD groups. You then upgrade the backup device first and the primary device second.

The following illustrates a typical NSRP active/active configuration where device A is the primary device for VSD 0 and the backup for VSD 1, and device B is the primary device for VSD 1 and the backup for VSD 0.

Before you begin, see section Requirements for Upgrading and Downgrading Device Firmware. Also, make sure you download the ScreenOS 5.4.0 firmware (and intermediate firmware, if required).

Do not power off your security device while it is upgrading to new firmware. Doing so could permanently damage the device.

To upgrade two devices in an NSRP active/active configuration, perform the following steps (some steps require CLI use).

1. Manually fail over the master device B in VSD group 1 to the backup device A in VSD group 1. (CLI only)

a. Log into device B using an application such as Telnet or SSH (or Hyper Terminal if directly connected through the console port). Log in as the root admin or an admin with read-write privileges.

b. Issue one of the following CLI commands. The command you need to execute depends on whether or not the preempt option is enabled on the master device.

- If the preempt option is enabled:

exec nsrp vsd-group 1 mode ineligible

- If the preempt option is not enabled:

exec nsrp vsd-group 1 mode backup

Both command forces device B to step down and device A to immediately assume the primary role of VSD 1. At this point, device A is the primary of both VSD 0 and 1 and device B is the backup for both VSD 0 and 1.

2. Upgrade Device B to the ScreenOS 5.4.0 firmware.

WebUI

a. Make sure that you have the 5.4.0 ScreenOS firmware (and the intermediate firmware, if required). Upgrade Paths to ScreenOS 5.4.0 for details. For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into security device B by opening a browser and entering the management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.

c. Save the existing configuration:

   i. Go to Configuration > Update > Config File, and then click **Save to File**.

   ii. In the File Download dialog box, click **Save**.

   iii. Navigate to the location where you want to save the configuration file (cfg.txt), then click **Save**.

d. Go to Configuration > Update > ScreenOS/Keys, and select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 5.4.0 firmware or enter the path to its location in the Load File field.

f. Click **Apply**.

   A message box appears with information on the upgrade time.

g. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

   To verify the version of the ScreenOS firmware, log into the security device and go to the Device Information section of the WebUI Home page.

CLI

a. Make sure that you have the ScreenOS 5.4.0 firmware. For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into device B.

c. Save the existing configuration by executing the following command:

   save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double-clicking on the TFTP server application.

e. On the security device, enter the following command:

   save soft from tftp *ip_addr_your_computer screenos_filename* **to flash**

   where *ip_addr* is the IP address of your computer and *screenos_filename* is the ScreenOS 5.4.0 firmware.

f. When the upgrade is complete, you must restart the security device. Execute the **reset** command and enter **y** at the prompt to restart the device.

g. Wait a few minutes, and then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

3. Manually fail over device A completely to device B (CLI only).

a. Log into device A.

b. Fail over primary device A in VSD 0 to backup device B in VSD 0 by issuing one of the following CLI commands. The command you need to execute depends on whether or not the preempt option is enabled on the primary device.

- If the preempt option is enabled:

exec nsrp vsd-group 0 mode ineligible

- If the preempt option is not enabled:

exec nsrp vsd-group 0 mode backup

If pre-empt is enabled on device A, no action is needed. If pre-empt is not enabled on device A, issue the following command

exec nsrp vsd-group 1 mode backup

At this point, device B is the primary device for both VSD 0 and 1, and device A is backup for both VSD 0 and 1.

4. Upgrade device A to ScreenOS 5.4.0.

WebUI

a. Make sure that you have the 5.4.0 ScreenOS firmware (and the intermediate firmware, if required). Upgrade Paths to ScreenOS 5.4.0 for software details. For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into security device A.

c. Save the existing configuration:

i. Go to Configuration > Update > Config File, and then click **Save to File**.

ii. In the File Download dialog box, click **Save**.

iii. Navigate to the location where you want to save the configuration file (cfg.txt), then click **Save**.

d. Go to Configuration > Update > ScreenOS/Keys, and select **Firmware Update**.

e. Click **Browse** to navigate to the location of the ScreenOS 5.4.0 firmware, or enter the path to its location in the Load File field.

f. Click **Apply**.

A message box appears with information on the upgrade time.

g. Click **OK** to continue.

The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.

h. To verify the version of the ScreenOS firmware, log into the security device and go to the Device Information section of the WebUI Home page.

CLI

a. Make sure that you have the ScreenOS 5.4.0 firmware. For information on obtaining the firmware, see section Downloading New Firmware.

b. Log into device A.

c. Save the existing configuration by executing the following command:

save config to { **flash** | **slot1** | **tftp** }...

d. Run the TFTP server on your computer by double clicking on the TFTP server application.

e. On the security device, enter the following command:

save soft from tftp *ip_addr_your_computer screenos_filename* **to flash**

f. When the upgrade is complete, you must restart the security device. Execute the **reset** command, then enter **y** at the prompt to restart the device.

g. Wait a few minutes, then log into the security device again. You can verify the security device ScreenOS firmware version by using the **get system** command.

5. Synchronize device A (CLI only).

   After you complete the upgrade of device A to ScreenOS 5.4.0, manually synchronize the two devices. On device A, issue the **exec nsrp sync rto all** command from peer CLI to synchronize the RTOs from device B.

6. Fail over Device B in VSD 0 to Device A in VSD 0 (CLI only).

   As the final step, return the devices to an active/active configuration.

   Log into device A.

   If pre-empt is enabled on device A, no action is needed. If pre-empt is not enabled on device A, issue the following command:

   exec nsrp vsd-group 1 mode backup

   Now device A is the primary device for VSD 0 and the backup for VSD 1, and device B is the primary device for VSD 1 and the backup for VSD 0.

5.8 Upgrading or Migrating the Antivirus Scanner (NetScreen-5GT)

For the NetScreen-5GT device only, two antivirus scan engines are available, as shown in AV Scan Engines.

To migrate to a new antivirus (AV) scanner, follow this procedure:

For a new AV installation, you can first upgrade the security device to run ScreenOS 5.4.0, and then install the AV license, or you can install the AV license first and then upgrade the security device to ScreenOS 5.4.0.

---

1. Save your current configuration.

2. Install your AV license key.

To access an AV license key, refer to the *Concepts & Examples ScreenOS Reference Guide*. You must install the license key before you upgrade to ScreenOS 5.4.0, or you might lose some of your current configuration.

ScreenOS 5.3.0 and later support two scan engines, Juniper-Kaspersky and Trend Micro. Make sure you have the correct AV license key for your scan engine. The two license keys, however, can coexist on your security device.

AV Scan Engines

AV Scan Engine	License Key	ScreenOS version
Trend Micro	av_key	ns5gttmav.5.4.0x
Juniper-Kaspersky	av_v2_key	ns5gt.5.4.0x

3. Upgrade to ScreenOS 5.4.0.

   There are two versions of ScreenOS 5.4.0, as shown in AV Scan Engines. A single version of ScreenOS does not support both scan engines, however.

   Make sure you select the ScreenOS version that supports the AV scan engine that was installed in Step 2.

4. Check the configuration file (especially policies) to ensure it is intact.

5.8.1 Scan Manager Profile

The global **scan-mgr** command controls the embedded scan manager, which is the AV component that interacts with the scan engine. For example, the **set** or **get av scan-mgr** CLI command sets the global commands that control parameters, such as max-content-size, max-msgs, pattern-type, pattern-update, and queue-size.

In ScreenOS 5.3.0 and later, some of the previously global settings are now configured from within a profile context. For example, global commands such as **timeout** and **max-decompress-layer** are no longer global; they are now set within the profile for each protocol. Commands such as **max-content-size** and **max-msgs**, which configure the embedded scan manager, are global and are now set using the **set av scan-mgr** command.

When you upgrade to ScreenOS 5.3.0 or later, a scan manager profile named **scan-mgr** is automatically generated to migrate the global **scan-mgr** commands. The **scan-mgr** profile executes the following commands:

```
set ftp decompress-layer 2
set http decompress-layer 2
set imap decompress-layer 2
set pop3 decompress-layer 2
set smtp decompress-layer 2
set http skipmime enable
set http skipmime mime-list ns-skip-mime-list
```

Command Updates shows the updated commands in ScreenOS 5.4.0. Updated commands are now entered from within a policy context.

Table 3: Command Updates

Commands previous to ScreenOS 5.3.0	Commands for ScreenOS 5.3.0 and Later Within a Profile Context
set av http skipmime	set av profile scan-mgr set http skipmime mime-list ns-skip-mime-list set http skipmime enable exit
unset av http skipmime	set av profile scan-mgr unset http skipmime enable exit
set av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP } [timeout *number*] }	set av profile scan-mgr set { FTP | HTTP | IMAP | POP3 | SMTP { enable | timeout *number* } } exit
unset av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP }	set av profile scan-mgr unset { FTP | HTTP | IMAP | POP3 | SMTP } enable exit

5.8.2 AV Pattern Update URL

Trend Micro Inc. no longer hosts AV pattern file updates at *http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini*.

The new pattern update can be found at *http://5gt-p.activeupdate.trendmicro.com/activeupdate/server.ini*.

After you upgrade the ScreenOS image, the new image automatically uses the new server URL for AV pattern-update operations; however, the URL in the saved configuration will not change unless you explicitly issued the **save** command.

When you upgrade to a newer release or manually change the AV pattern update URL to the new location, you can verify the pattern update URL is modified during the upgrade process by entering the following command:

5gt1-> **get av scan-mgr**

```
Embedded AV Management Info:
Pattern Management:
AV Key Expire Date: 12/31/2005 00:00:00
Update Server: http://5gt-p.activeupdate.trendmicro.com/activeupdate/server.ini
```

6. Known Issues

This section describes known issues with the current release and includes the following sections.

Limitations of Features in ScreenOS 5.4.0 — identifies features that are not fully functional at the present time, and will be unsupported for this release.

Compatibility Issues in ScreenOS 5.4.0 — describes known compatibility issues with other products, including but not limited to specific Juniper Networks appliances, other versions of ScreenOS, Internet browsers, Juniper Networks management software and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

Known Issues in ScreenOS 5.4.0 — describes deviations from intended product behavior as identified by Juniper Networks Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

6.1 Limitations of Features in ScreenOS 5.4.0

This section describes the limitations in various features in ScreenOS. They apply to all devices, unless otherwise noted.

- **500 NSM with DI enabled**—Users might experience issues when downloading configuration files larger than 1.7 M.
- **5000 Series vsys capacity**—Virtual Systems Capacity for NetScreen 5000 Series Device describes the number of virtual systems ScreenOS supports for each 5000 Series device.

Table 4: Virtual Systems Capacity for NetScreen 5000 Series Device

ScreenOS	NetScreen-5200 using 5000-M	NetScreen-5200 using 5000-M2	NetScreen-5400 using 5000-M	NetScreen-5400 using 5000-M2
4.0x	500	N/A	500	N/A
5.0x	500	500	500	500
5.1x	500	N/A	500	N/A
5.2x	500	500	500	500
5.3x	500	500	100	500
5.4.x	500	500	100	500

- **`Limitations of WAN interface traffic shaping`** — Traffic shaping parameters can only be applied to the following WAN interfaces with the following encapsulation types:
  - Single T1 or E1 interface that is using PPP or HDLC encapsulation
  - ADSL 2+ interface that is using PPP encapsulation
  - Single ISDN BRI S/T that is using PPP or MLPPP encapsulation

  Frame Relay and Multilink Frame Relay will not work when Quality of Service (QoS) is applied to the encapsulation types mentioned above with the specified WAN interfaces.

  ScreenOS 5.4 does not support QoS over a MLPPP link.

- **Limitations of the AV scanner**—The following lists basic troubleshooting items and limitations of the AV scanner:
  - The AV scanner sometimes aborts a session. Refer to AV Scanner Symptoms and Solutions for symptoms and solutions.

Table 5: AV Scanner Symptoms and Solutions

Symptom	Solution
Device runs out of packets	Change the max content size option to a smaller value. For example, set av scan-mgr max-content-size <*number in KB*>
Excessive use of av resources	Increase user resource limit. For example, set av all resource <*number in percent*>
Memory allocation failure when processing an AV session	Restart your device

  - Default route is required for AV to function in transparent mode.
  - If a virus is found in an element on an HTML page, the contents of the element is replaced by white space.
  - The maximum size file inspected by the integrated AV feature defaults to 10MB. If AV and Deep Inspection (DI) are enabled, we recommend reducing the maximum size file to 6 MB. If AV, DI, and Web filtering are all enabled, it is advisable to reduce the maximum size file to 4MB.
- **Dead Peer Detection (DPD)**—When DPD detects a dead peer, the device should deactivate any existing VPN with that peer. However, if a tunnel interface is bound to the VPN, the device does not make any state changes on that interface, or on any Phase 2 tunnel associated with the interface. Consequently, DPD only works correctly when the VPN is not bound to a tunnel interface.
- **NSRP cluster synchronization**—Under very special circumstances it is possible for two members of an NSRP cluster to be out of synchrony regarding sessions and state. If a session for which an ALG exists (for example, H.323) starts and immediately terminates, and a failover of the NSRP cluster occurs before the session state synchronization completes, a session might exist on one member of the cluster and not the other. The extraneous session will age out on the device at the normal scheduled interval.
- **Transparent mode vsys**—When implementing transparent mode vsys, or if changing device configuration from one using transparent mode vsys to one using Layer3 interfaces and security zones, the administrator must issue the CLI command **unset all** and restart the device, then create or import the desired configuration.
- **IPv6 Functionality**—IPv6 functionality is modified as follows:
  - MIP on policy-based VPN is not supported; include MIP on physical or tunnel interface.
  - Policy-based traffic count is not supported.
  - Screen component-block is not supported.

- Screen syn-ack-ack proxy is not supported.

- **NSRP** —NSRP is not supported on WAN interfaces. Devices with WAN interfaces can use NSRP, but the WAN ports do not automatically failover as the Ethernet ports do.

- **Fragmentation support on multilink frame relay** —Frame Relay fragmentation (FRF.12) is not supported in this release.

- **Frame Relay and Cisco HDLC encapsulation** —With this type of encapsulation, ScreenOS devices can only be a spoke in a hub and spoke environment. With industry standard encapsulations, such as IETF, there are no restrictions.

- **Flood Screens** —On ISG 1000, ISG 2000, NetScreen-5000 Series devices, the UDP and ICMP flood screens apply to the physical interface and therefore require that the zone be bound to a physical interface. The following limitations apply:

  - When zones are bound to a sub-interface, the ICMP and UDP flood screens are not enforced unless the zone is also bound to a physical interface.

  - When ICMP and UDP flood screen options are configured for different zones and on the same physical interface, the flood threshold is applied based on the last configured zone threshold.

  - When ICMP and UDP flood screen options are applied to a zone tied to multiple physical interfaces, the entire threshold value is applied to each of the physical interfaces.

  - For reference, the High Availability (HA) zone does not allow any screen features to be configured.

6.2 Compatibility Issues in ScreenOS 5.4.0

Below are the known compatibility issues at the time of this release. Whenever possible, a work-around (starting with “W/A:”) has been provided for your convenience.

Compatible web browsers —The WebUI for ScreenOS 5.4.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, and Netscape Navigator 6.X for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS 10.x. Other versions of these and other browsers were reported to display erroneous behavior.

Upgrade sequence —Juniper Networks recommends that you follow the upgrade instructions described in section 5 Migration Procedures. If you upgrade directly from ScreenOS 5.0.0 or ScreenOS 5.1.0 to ScreenOS 5.4.0, you risk losing part of any existing configuration. For NetScreen-500 and ISG 2000 devices, you must upgrade to an intermediate firmware and upgrade the boot loader before upgrading to the ScreenOS 5.4.0 firmware.

WebUI upgrade —When upgrading from ScreenOS 5.2.0 to ScreenOS 5.4.0 using the WebUI, you must upgrade the device to ScreenOS 5.2r3 and then upgrade the device directly to ScreenOS 5.4.0. Refer to section Upgrading to the New Firmware for instructions on how to perform the upgrade.

6.3 Known Issues In ScreenOS 5.4.0

The following are known deficiencies in features at the time of this release. Whenever possible, a workaround is suggested following the problem description, preceded by: **W/A**.

- **cs11603** — (NetScreen-5GT) The extended scanning option for the Kaspersky antivirus is not available. Therefore, setting the device for extended scanning causes errors when updating signatures.

W/A: Revert to the standard antivirus scanning setting (the default setting).

- **os66190** — Attempting to load AV signature files larger than 10mb results in the error “AV pattern file size is too large.”

  W/A: Revert to the standard antivirus scanning setting (the default setting).

- **cs11257** — On the WebUI Network>Interfaces screen, the New Interface menu near the upper right corner contains the invalid option "VLAN." This option should not appear in the list, as all ScreenOS devices are preconfigured with a VLAN interface (VLAN1) and only one such interface is allowed.

  W/A: Do not use the VLAN option on the New Interface menu.

- **os59409** — (SSG 140, SSG-520, SSG-550) In multi-link frame relay, if the traffic volume is very close to the maximum bandwidth available on the aggregated links, Frame Relay LIP/LMI packets may get dropped and the multilink may go down. This issue is most likely to occur on relatively low-speed interfaces such as serial interfaces.

- **os62852** — If you perform the following configuration sequence, the device reports "Unsupported Command" errors during startup:

  1. Create a logical interface.

  2. Create an NSRP configuration that depends on the logical interface.

  3. Delete the logical interface upon which the NSRP configuration depends.

  4. Restart the device.

  W/A: Delete all dependant NSRP configurations before deleting logical interfaces.

- **os65695** — (SSG 140) The device does not reconnect with NetScreen-Security Manager after restarting.

  W/A: Manually reconnect NetScreen-Security Manager after restarting the device by using the CLI commands "unset nsmgmt enable" and then "set nsmgmt enable" to disable and reenable the NSM agent.

- **os64055** — When the device is in NAT mode, and subjected to high volumes of H.323 traffic, the device may report NAT errors.

- **os63861** — (SSG 20 ADSL mini-PIM with PPPoA enabled) Some websites cannot be displayed.

  W/A: Set IP MTU on interface to 1500.

- **os63870** — (SSG 5 and SSG 20) A print message is continuously displayed when the NSRP state is changed from M to B.

  W/A: In Transparent mode, HA interface is only supported in Null security zone.

- **os63911** — (SSG 20) When the ISDN interface is set as primary interface, track-ip cannot dial up when the interface is down.

  W/A: Use manual dialup.

- **os63952** — (SSG 5 and SSG 20) After using the set/unset CLI commands for the ADSL sub-interface, ADSL PPPoA connection is unsuccessful.

- **os64355** — (SSG 5 and SSG 20) Asymmetrical VPN performance on decryption and encryption.

- **os64122** — (SSG 5 and SSG 20) When the v.92 modem dials out to a different ISP with the same primary-number/user/password, the device prompt displays an error message stating that the latest modem state is inactive, because the device did not have a clear prompt for the dialer connection.
- **os64434** — (SSG 5 and SSG 20) The set interface ml1 and set interface ml00001 CLI commands will create two ml1 interfaces, and the user can only delete one of them.
- **os64464** — (SSG 5 and SSG 20) When the length of a sent packet is larger than the member link MTU, the device could fail.
- **os64466** — (SSG 5 and SSG 20) The line speed data transfer through PPP or MLPPP link connection will flap.
- **os64490** — (SSG 5 and SSG 20) When the length of a sent packet is larger than the Multilink Frame Relay MTU, the device could fail.
- **cs06894** — At times the status for the NetScreen-Security Manager VPN monitor might be inaccurate.
- **cs07098** — The error (00034) message documented in the Messages Guide will not appear when SSH reaches max sessions.
- **cs08159** — Error message **IP address conflict** is displayed when changing the Managed IP on an untrust interface.
- **cs08252** — Boot-Rom TFTP will use source port 0 when upgrading. This operation will fail if only allowing the predefined TFTP service because it is defined as ports 1-65535.
- **cs08760** — (DMZ-Dual Untrust port mode) The hardware counters are improperly incremented.
- **cs08773** — An existing SSH session pauses while a new SSH session is authenticated.
- **cs09147**—(Trend Micro integrated AV) The extension exclude list does not work.
- **cs09394** — The DNS settings on a device do not appear if the device obtained an Untrust IP address with DHCP.
- **cs09534** — (ISG 1000 and ISG 2000 acting as GPRS gateway**)** Version 1 Update PDP context requests are unchecked, and the firewall passes them even if there is no active context or tunnel.
- **cs10407** — SMTP, DNS traffic is dropped when using sub-interfaces in a vsys with DI enabled.
- **cs10425** — No SNMP traps are sent to x.x.x.255 even though the host address can be configured.
- **cs10427** — (DHCP relay) The broadcast flag is always set to 0 regardless of the original request.
- **cs10444** — (NetScreen-5000 Series using 5000-M2) The device erroneously reports a high number of sessions (1,000,000) through SNMP.
- **cs10454** — (ISG 2000) When using a standard SNMP walk, the value **other** is returned for the Gigabit interfaces.
- **cs10505** — (IPv6) The device restarts if the wrong buffer is retrieved.
- **cs10702** — Fragmented packets fail to pass through a GRE tunnel.
- **os55631**— In the scenario of SIP Proxy in a different zone from the endpoints, the **get sip call** CLI command might display two entries when they are in fact for the same call.

- **os56461** — Source-based routing is unsupported by all VoIP ALGs.
- **os56484** — The ARP table is not updated when changing a zone for a SIP phone in Transparent mode.
- **os57066** — (External AV) When the ICAP AV scanner is used in the presence of virtual systems, the ICAP status can be viewed from the vsys context but not the virus status. All statistics including virus status are only visible from the root level.
- **os57612** — (AV) The HTTP Upload layer is sometimes processed as one layer of compression.
- **os57620** — When an interface has both IPv4 and IPv6 address configured, if either address is used, the other IP address cannot be unset from the interface.

  W/A: Make sure neither IP address is used before unsetting them.
- **os57729** — SIP ALG for inter vsys traffic is unsupported.
- **os57762** — H.323 ALG for inter vsys traffic is unsupported.
- **os57899** — (External AV) When 10 or more viruses affect a single transaction, the device reports only the first 10. The **get event** CLI command reports a maximum of 10 viruses and the counter associated with the transaction increments by 1.
- **os58138** — (External AV) Certain compressed file types are unscanned.
- **os58177** — (Embedded AV) RAR files might not be scanned because the scanner tries to allocate large amounts of memory when trying to scan this type of files.
- **os58369** — (AV) Internet Explorer issue exists. The browser might freeze when uploading large (64MB) text files.
- **os58552** — (Embedded AV) WebUI connection, you cannot select **standard**, **extended**, or **in the wild** when configuring scanning.

  WA: Use the CLI.
- **os58602** — The device returns a non-zero value when exiting from an SSH or SCP session.
- **os58624** — In some cases, the device does not send the accounting-ON message for RADIUS Authentication.
- **os58754** — SCCP ALG for inter vsys traffic is unsupported.
- **os58785** — Calls will fail if the caller is using a custom service instead of the SIP service. The ALG cannot find a matching policy because it is searching for port 5060 in a service definition.

  WA: Include port 5060 in the destination port range when defining a custom service for SIP.
- **os58845** — (NetScreen-5000 Series using 5000-M2 and 5000-8G2 or 5000-2XGE) The device could experience a 20-to-25% performance drop in TCP-connection rate compared to the 5.0 release.
- **os58915** — VPN wizard support for IPv6 is unavailable.
- **os59154** — The VoIP ALG with HA under a very high load can experience a resource leak.
- **os59351** — There is no support for using the same user group in both an IPv4 and an IPv6 IKE gateway.

- **os59450** — Because an ISDN interface is a slow link and AV requires the files to be buffered for scanning, for files larger than 1MB, it takes a long time to buffer the file. As a result, files greater than 1MB sent over an ISDN link might be unscanned.

- **os59754** — SIP calls will fail if placed across a policy-based VPN that performs NAT.

  WA: Re-architect to avoid NAT in tunnels or use route-based VPNs in NAT mode.

- **os60122**— (IPv6) The DNS lookup table is unsupported.

- **os60181**— (NetScreen-5000 Series using 5000-M2) The management module incorrectly reports bandwidth of 0Mbps for the HA link.

- **os60233**— (NetScreen-5000 Series using 5000-M2 and 5000-8G or 5000-2G24FE) The device could experience a session setup rate up to 30% lower than ScreenOS 5.3.

- **os60360** — While in TrendMicro AV scan-extension mode, the exclude list is currently ignored, but the files will still be scanned for viruses.

- **os60365** — Under stressful conditions, trying to bring up multiple VPNs simultaneously can cause some SAs to not display.

  WA: Unset/reset the policy or tunnel interface binding for these SAs.

- **os60674** — (ISG 1000/ISG 2000 with GTP license) Version 1 Update PDP context requests are not strictly checked.

- **os60680** — When sending an unnamed file with container violation, the email notification and event log displays the file name as **TRAFFIC**.

  W/A: Name the file to avoid further confusion.

- **os61042** — (WebUI) The bandwidth for redundant interfaces is displayed incorrectly.

- **os61326** — In some cases, the CPU utilization is high (about 30% or higher) even though there is no traffic. The WebUI is consuming too many resources in this release.

- **os61446**— Due to changes in zone accounting, the user could configure more zones than in previous releases.

- **os61462** — (WebUI) If an error is encountered when generating a key pair, no error is reported.

  WA: Use the CLI to generate a key pair which will display a detailed error message.

- **os61536** — In an Active-Passive NSRP pair, changing the duplex and speed could cause the primary device to fail.

- **os61541** — When free space on the flash is small and a new image needs to be saved, other flash activity can cause the upgrade to fail.

- **os61716** — (SSG devices) Removal of a serial interface from a Multilink Frame Relay (MLFR) bundle can cause the device to freeze if the device has queued traffic for transmission and is still waiting for the Frame Relay task to be processed.

  W/A: Administratively disable the bundle interface before removing members, and then re-enable it after membership is correct.

- **os61980** — In H.323 NSRP stress testing, with session age out ACK enabled, some sessions do not age out if the primary device is operating correctly.

  W/A: Clear the session to recover. Turn off session age out ACK with the **unset nsrp rto sync ageout-ack** CLI command.

- **os62075** — The maximum number of management VLAN interfaces that can be configured on a device is 128.

- **os62477** — SSHv2 sessions time out after 25 minutes.

- **os62697** — A device restart is required in order for changes to BGP route-maps to take effect.

- **os62720** — In some cases, the device fails while editing a policy.

- **os62737** — The SIP and H323 ALGs do not support incoming DIPs in a VPN scenario.

  W/A: Perform NAT at the other VPN peer.

- **os62756** — In some cases, a NetScreen-Security Manager policy push caused one of the security modules to fail. Traffic throughput was affected until a **clear session all** was performed.

- **os62872** — The **unset alg enable** CLI command might be displayed in the configuration file.

- **os63007** — For ISRAU with multiple GTP tunnels, not all tunnels are properly created.

- **os63287** — When switching between Transparent mode and Route mode, some error messages might be displayed upon restart for commands that are unsupported.

- **os63138** — (ISG 2000) For a device with a high number of policies configured, an optimized tree search must be enabled to avoid performance issues.

  W/A: Use the **set policy swrs** CLI command then restart the device.

- **os63290** — In Transparent mode vsys, when a VLAN interface is unset, the ARP table is not flushed.

  W/A: Use the **clear arp all** command to manually clean the ARP table.

- **os63351**— Enabling or disabling SIP ALG with outstanding calls can cause the device to restart.

  WA: Stop all calls before enabling or disabling SIP ALG.

- **os63487** — (WebUI) The allowed MTU range for VSIs is incorrect.

  WA: Use the CLI to set MTU size.

- **os63498** — ScreenOS does not block the configuration of and interface in the MGT zone even though the interface also has VSI configured.

- **os63513** — Unsetting the sub-interface could cause device failure if there is heavy traffic through a sub-interface with traffic shaping enabled.

  WA: Stop the traffic before unsetting a sub-interface.

- **os63523** — (NetScreenS-5400 using 5000-M2 and 5000-8G2 and 5000-2XGE) TCP traffic on the device might not pass if the traffic crosses the ASIC chip and is through a VPN tunnel.

W/A: Turn off TCP sequence number check.

- **os63527** — During internal H.323 stress testing, NSRP failover issues occurred.
- **os63532** — A device with high AV traffic for a long time, the AV subsystem might run out of memory and continuously restart the AV process which can cause device failure.
- **os63538** — An NDP entry will not be cleared from NDP cache if the associated interface is being used.

  W/A: Unset other objects that use this interface first.
- **os63543** — A GTP session might be incorrectly aged out after NSRP failover if the **teid-id** is configured.
- **os63554** — NSRP failover of VOIP calls involving non-root vsys is unsupported.
- **os63576** — Firewall authentication does not work in Transparent mode vsys.
- **os63610** — Power or device failure during a write operation can cause a file system to be corrupt.
- **os63612** — Repeated login from the same XAUTH user can cause the device to retransmit the account start message to the RADIUS server.
- **os63626** — RTO sync of GTP tunnel objects will create new tunnels instead of replacing them.

  W/A: Clear the GTP tunnel objects on the backup prior to RTO sync.
- **os63627** — The **clear gtp** CLI command does not clear GTP objects on the NSRP peer.

  W/A: Initiate the **clear gtp** CLI command on the peer NSRP device.
- **os63632** — Unsetting the custom L2 zone, while there is still a VLAN port associated with it, can cause system failure.

  W/A: Unset the VLAN port before unsetting the L2 zone.
- **os63974**— Multilink PPP (MLPPP) does not accept frames with compressed headers.

  W/A: If possible, disable header compression on the peer MLPPP device.

7. Getting Help

For further assistance with Juniper Networks products, visit

```
www.juniper.net/support
```

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your security device with Juniper Networks at the above address.