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 5.4.0r4

Revision: Rev 01

Part Number: 093-1876-000

Date: May 3, 2007

Version Summary 4
Documentation Changes 4
New Features and Enhancements 5
- Four-Port Mini-GBIC 5
- Jumbo Frames 5
- DSCP 5
- DSCP Support for Tunnels 6
- NSRD Support 6
- External Antivirus 6
- Internal AV Extended to the SSG Platforms 6
- Integrated Web Filtering and Anti-Spam Extended Support 6
- DI Signature-Pack Selection Enhancement 7
- DHCP Packets Relay Enhancement 7
- Configuring Next-Server-IP 7
- Get Tech Feature 7
- ICMP Unreachable Handling 7
- Source Interface Option for DNS Servers 8
- GPRS 8
- Router Discovery Protocol 9
- IPv6 9
- Password Policy Support 9
- Policy-Based Routing 9
- Service Timeout 9
- SNMP Enhancements 10
- Virtual Systems Enhancements 10
- SCCP Support 10
- Wide Area Network Support 10
- Wireless Enhancements 11
- XAuth with Internet Key Exchange Mode Enhancements 11

Any modification Internal Policy Representation Changes 11
Changes to Default Behavior 11
FIPS 12
Global-Pro command change 12
HTTP Brute-Force attack 12
Interface limit change 12
Log buffer full handling 12
MAC address handling 12
Multicast-route handling 12
Multilink Bundle interface configuration 13
Root/VSYS profile configuration 13
Saved log information handling 13
WAN interface configuration 13
Migration Procedures 13
Requirements for Upgrading and Downgrading Device Firmware 17
Special Boot-ROM or Boot-Loader Requirements 19
NetScreen-500 Boot-ROM 19
ISG 2000 Boot Loader 19
Downloading New Firmware 20
Upgrading to the New Firmware 21
Upgrading Using the WebUI 21
Upgrading Using the CLI 23
Upgrading Using the Boot/OS Loader 24
Saving Multiple Firmware Images with the Boot Loader 25
Downgrading the NetScreen-500 Device 25
Upgrading Devices in an NSRP Configuration 26
Upgrading Devices in an NSRP Active/Passive Configuration 27
Upgrading Devices in an NSRP Active/Active Configuration 30
Upgrading or Migrating the Antivirus Scanner (NetScreen-5GT) 34
Scan Manager Profile 35
AV Pattern Update URL 36
Addressed Issues in ScreenOS 5.4.0r4 36
Administration 37
Antivirus 37
CLI 37
DHCP 38
HA & NSRP 38
Management 38
Other 38
Performance 39
Routing 39
VOIP/H323 40
VPN 40
Web UI 41
Addressed Issues from ScreenOS 5.4.0r3 41
Administration 41

CLI 42
DNS 43
HA & NSRP 43
Management 43
Other 44
Performance 47
Routing 49
Security 49
VOIP/H323 50
VPN 50
Web UI 52
Addressed Issues from ScreenOS 5.4.0r2 53
Known Issues 56
Limitations of Features in ScreenOS 5.4.0 56
Compatibility Issues in ScreenOS 5.4.0 59
Known Issues in ScreenOS 5.4.0r4 60
Administration 60
Antivirus 60
CLI 61
HA & NSRP 61
NAT 61
Other 61
VOIP/H323 62
VPN 62
Web UI 62
Known Issues from ScreenOS 5.4.0r3 62
Administration 62
CLI 63
DHCP 63
HA & NSRP 64
Management 64
Other 64
Routing 65
VOIP/H323 65
VPN 66
Web UI 66
Known Issues from ScreenOS 5.4.0r2 66
Administration 67
HA and NSRP 67
Management 67
Other 67
Performance 68
Routing 68
VoIP/H.323 68
WebUI 68
Known Issues From ScreenOS 5.4.0r1 68

Getting Help 74

Version Summary

ScreenOS 5.4.0 firmware can be installed on 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 5.3r5, 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.

Note: When using an SSG 500 device and an SSG 500M Series device in an NSRP environment, both devices must be running ScreenOS 5.4r2 or later. Both devices must be one of the following clusters: SSG 520 and SSG 520M NSRP cluster or SSG 550 and SSG 550M NSRP cluster.

Note: 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. Refer to the *NetScreen-Security Manager Release Notes* for installation instructions and the features supported with this schema upgrade.

Documentation Changes

- Some device messages text is changed. Refer to the *ScreenOS Messages Log Reference Guide* for ScreenOS 5.4 for details.
- The ScreenOS Concepts & Examples (C&E) Guide volume 5 chapter 2 section “Configuring CRL Settings” incorrectly stated that the “default” system setting on the CRL server URL is used if the setting is not specified in the configuration for the particular CA. The revised documentation now correctly states that the “default” system CRL server URL setting is used only when the (CA) certificate of the CA is not loaded in the device. If a CA certificate is loaded in the device, the device looks for the CRL server URL information in the following order:
  1. The CRL server URL in the CRL Distribution Point (CDP) embedded end-entity certificate

2. The CRL server URL in the particular CA setting

   Note: This document update is related to **cs12624**

New Features and Enhancements

The following sections describe new features and enhancements. These features do not affect migration.

Note: 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, then enter your ID and password.

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

Four-Port Mini-GBIC

The 4-port mini-GBIC (GB4) interface module is supported on the Integrated Services Gateway (ISG) 1000 and ISG 2000 and provides connectivity to fiber-based and copper-based, gigabit Ethernet LANs only. Connect the module using the appropriate cable type depending on the specific media used: single-mode or multimode optical cable for SX and LX, and CAT-5 cable for the copper transceiver.

Jumbo Frames

Jumbo frames are supported on the ISG 2000 supports. To enable jumbo frames, use the **set envar** CLI command and set **max-frame-size** to any value from 1515 through 9830 inclusive; for example, **set envar max-frame-size=7500**. In this release, Jumbo frames are supported only on the 4-port mini-GBIC IO card. When you enable jumbo frames and restart the security device, only interfaces on the 4-port mini-GBIC IO card, plus the management Ethernet interface, become active. Use the **get envar** command to show the **max-frame-size** setting. Use the **unset envar max-frame-size** command to disable jumbo frames support and return the device to the normal maximum frame size (1514 bytes).

DSCP

Differentiated Services Code Point (DSCP) marking is now supported on the Integrated Services Gateway (ISG) 1000 and ISG 2000.

DSCP Support for Tunnels

Differentiated Services Code Point (DSCP) marking is now supported in VPN tunnels on the Integrated Services Gateway (ISG) 1000 and ISG 2000.

NSRD Support

Netscreen Rapid Deployment (NSRD) now supports configuration of T1/E1 interfaces.

External Antivirus

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

External AV scanning including the following features:

- Supports ICAP v1.0 and is fully compliant with RFC 3507
- Supports Symantec scan engine version 5.0 ICAP server

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

Internal AV Extended to the SSG Platforms

The integrated Juniper/Kaspersky antivirus (AV) scan engine is supported on the SSG products with high memory. To activate this feature you must obtain a license, and upgrade your device to high memory if you have purchased a base memory device. The following table lists devices and associated memory capacity

Device	Base Memory	High Memory
SSG-5	128MB	256MB
SSG-20	128MB	256MB
SSG-140	128MB	256MB
SSG-520	256MB	1GB
SSG-550	256MB	1GB

Integrated Web Filtering and Anti-Spam Extended Support

Integrated web filtering and anti-spam support is now available on the following platforms:

- NetScreen-Hardware Security Client
- NetScreen-5GT Series
- NetScreen-25
- NetScreen-50
- ISG 1000

- ISG 2000
- SSG 500 Series

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

DI Signature-Pack Selection Enhancement

A dropdown 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.

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."

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.

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.

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

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."

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.

GPRS

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

- 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).
- GPRS support on the ISG 1000 platform, as well as on the ISG 2000.
- GTP-aware security devices now allow Stream Control Transmission Protocol (SCTP) messages to pass through the firewall.

Combination Support for IE Filtering

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

- 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.

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.”

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*.

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.”

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.”

Service Timeout

ScreenOS does not use the port-based service timeout table when the destination port is overloaded with multiple services that have different timeout

values set. Instead, to derive the correct service timeout value, ScreenOS does a service lookup within the service group based on the destination port.

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.”

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 overutilization protection in the form of enforceable quotas for CPU load caused by individual vsys
- DHCP: ScreenOS now fully supports DHCP relay for vsys. 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.”

SCCP Support

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

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

Wide Area Network Support

On some security devices, ScreenOS supports wide area network (WAN) interfaces such as Serial, T1, E1, T3, ADSL, ISDN, and V.92.

Refer to the *Concepts & Examples ScreenOS Reference Guide, Volume 12: WAN, ADSL, Dial, and Wireless.*

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

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.

Any modification 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 NSM and re-push the IDP policy to the device.

To obtain the zero day patch, go to the Juniper Support site at http://www.juniper.net/customers/support/ and, after logging in, scroll down to the Download Software section and click on the ScreenOS link. When the Customer Support Center page displays, click on the ScreenOS Software Downloads (including NSM/Global Pro and IDP link, scroll down to the 5.4 section and click the NS-ISG 1000-IDP or NS-ISG 1000-IDP link. The schema updates and instructions for installing them are in the ScreenOS Version 5.4.0r1 Upgrade section, near the bottom.

Changes to Default Behavior

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

File copy admin restriction change **(NSCos67009)**

“save config” to/from tftp server is now restricted to root user only.
“save software” transferring to tftp server is now restricted to root user only.
“save file” is now restricted to root user only.

FIPS

In the past, releases that were not FIPS certified did not allow FIPS mode to be enabled. R3 will allow FIPS mode to be enabled, even though it will not be FIPS certified.

Global-Pro command change

CLI “set global-pro policy-manager primary outgoing-interface” is no longer supported

HTTP Brute-Force attack

S2C HTTP protocol decoding is performed only if you configure server-to-client signature attacks. HTTP:Brute-Force, a server-to-client anomaly attack is detected if you configure a HTTP server-to-client signature attack in the policy. In the following example, HTTP:HIGH:SIGS has server-to-client signature attacks, so add HTTP:HIGH:SIGS along with HTTP:HIGH:ANOM in a policy.

Interface limit change **(NSCos65098)**

Hard limits (enforced in the code) were removed for “max interfaces per area” and “max interfaces per routing-instance” and made them soft limits instead. i.e. they are only recommended values and not enforced in the code. The device may not function correctly if these limits are exceeded.

Log buffer full handling **(NSCos68000/NSCos67431)**

After modification: when the log buffer is full and traffic passing through is stopped, the system will wait until the log buffer is empty before resuming traffic, the result is, wait a longer time to resume the traffic.

MAC address handling **(NSCos65912)**

Previously, for ASIC based platforms, when MAC cache is used, if the peers change their source MAC without sending any gratuitous ARP out, we could not update our hardware L2 table. In this case, when we want to send packets to the peer, the old MAC will be used. With this release, new session will use a new MAC address to send packets to the peer even without gratuitous ARP received. Old session will not be affected.

Multicast-route handling **(NSCos65082)**

Previous behavior: In IGMP proxy, when an admin clears multicast-route(mroute) by CLI(clear vr vr-name mroute), it can’t rebuild the mroute even when the new igmp report packet arrived.
New behavior: Every time the system receives a new IGMP report, the system will update the mroute created by the IGMP proxy. If the admin deletes the mroute by CLI, the system can rebuild it when it receives the next IGMP report packet.

Multilink Bundle interface configuration **(NSCos67022)**
No longer allow adding an ADSL interface into a multilink bundle interface with MLFR encapsulation

Root/VSYS profile configuration **(NSCos66696)**
Previously, the RootProfile can be bound to a nonRoot VSYS, while a non-RootProfile can be bound to Root. Now the RootProfile can only be bound to Root VSYS while non-RootProfile can only be bound to nonRoot VSYS.

Previously, get config always has "set vsys-profile RootProfile xxx" even if the value is the same as the default value; now this line will be shown only when the value is changed, i.e., it is different from the default value.

Saved log information handling **(NSCos62846)**
"Clear log sys saved" was not clearing the saved information on the SSG5 and SSG20 devices in previous versions. The function is now implemented on these devices in 5.4 R3.

WAN interface configuration **(NSCos66426)**
In "set/unset interface serialx/0 phy link-donw" CLI, link-down option is disabled for wan interfaces

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 platform and the firmware your security device is currently running, you also might need intermediate (or step-up) firmware and/or new bootloader firmware. Firmware Upgrade Path illustrates the various firmware upgrade paths to ScreenOS 5.4.0.

Figure 1.Firmware Upgrade Path

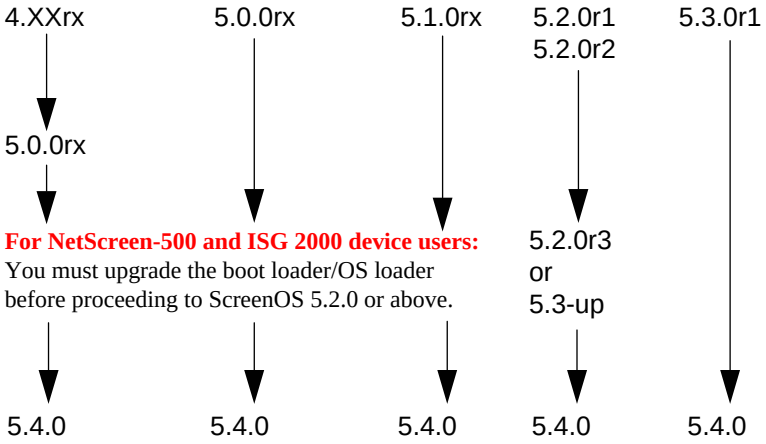


Figure 1 lists the recommended upgrade path to ScreenOS 5.4.0 based on device model and firmware version. For example, if you are running ScreenOS 4.0 on a NetScreen-204, you need to upgrade to ScreenOS 5.0r10 or later before upgrading to ScreenOS 5.4.0. If you are running ScreenOS 5.1 on a NetScreen-204, 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 platform.

Table 1: Upgrade Paths to ScreenOS 5.4.0

Base	Platform 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.
	ISG 1000	5.0r10 or later	
	ISG 1000-IDP	5.0r10 or later	Requires boot loader 1.0.1 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 NS-5000-8G NS-5000-2G24T	5.0r10 or later	
	NetScreen-5000 Series using 5000-M2 NS-5000-8G NS-5000-2G24T	5.0r9 or later	
	NetScreen-5000 Series using 5000-M2 NS-5000-8G2 NS-5000-2XGE	5.0r9 or later	(See Caution 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
	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 NS-5000-8G NS-5000-2G24T	5.2r3 or later	
	NetScreen-5000 Series using 5000-M2 NS-5000-8G NS-5000-2G24T	5.2r3 or later	
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 NS-5000-8G NS-5000-2G24T	None required	
NetScreen-5000 Series using 5000-M2 NS-5000-8G NS-5000-2G24T	None required	(See Caution below)

Caution: 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 NS-5000 modules qualify for a memory upgrade, contact Juniper Networks at 1-866-369-5418 or email mailto:Junipermem@onprocess.com for a memory-upgrade kit. The memory upgrade is free for qualified users.

Caution: 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.

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

Note: 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:

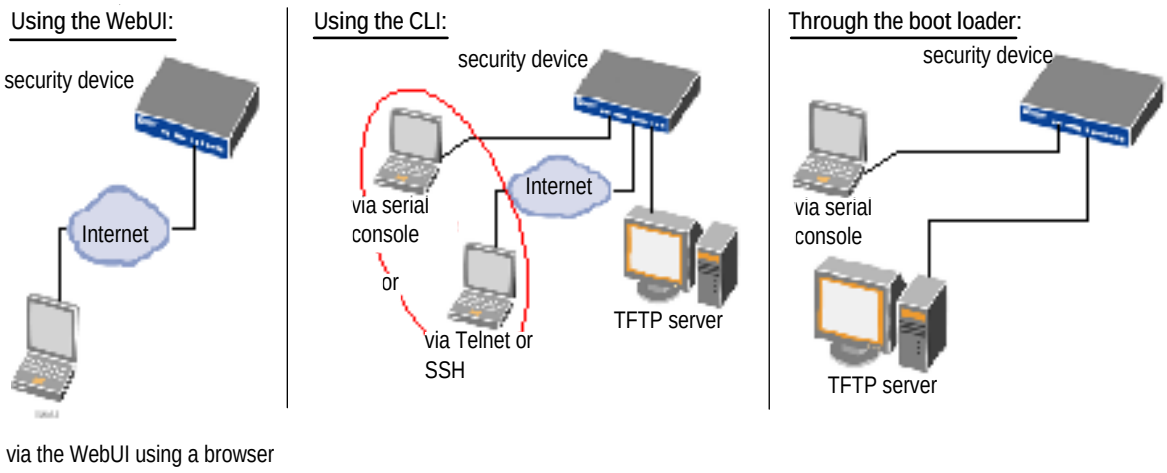
- Root or read-write privileges to the security device
- Console connection or Telnet access to the security device from a computer
- TFTP server installed locally and to which the security device has access
- New ScreenOS firmware (downloaded from the Juniper Networks website and saved to a local TFTP 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 illustrates the three different ways by which you can upgrade or downgrade a security device.

Figure 2. ScreenOS Upgrade and Downgrade Methods



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

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

Special Boot-ROM or Boot-Loader Requirements

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

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. See Upgrade Paths to ScreenOS 5.4.0.

Note: 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.

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** 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. Log into http://www.juniper.net/support.
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 by entering the **reset** 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.
```

You have completed the upgrade of the OS loader, and can now proceed to section, Downloading New Firmware.

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.

Note: 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.

Note: 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.

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.

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

Check Upgrade Paths to ScreenOS 5.4.0 to determine whether you need to install intermediate firmware or a bootloader 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.

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.

   See 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**.

Note: 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.

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 the 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 }...
   ```

5. 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**

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

6. When the upgrade is complete, you must reset the security device. Execute the **reset** command and enter **y** at the prompt to reset the device.
7. Wait a few minutes, and then log into the security device again.
8. Use the **get system** command to verify the version of the security device ScreenOS firmware.

   If you upgraded to intermediate firmware in step 1, on the security device enter the following command and specify the filename of the firmware, repeat steps 5 through 8 to install the ScreenOS 5.4.0 firmware.
9. 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 }...
```

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.

Note: 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.
   a) 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.
   b) 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.
2. 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.
3. 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.
4. 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.
5. Restart the security device.
6. 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.

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

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

Note: If Upgrade Paths to ScreenOS 5.4.0 lists an intermediate firmware requirement, enter that filename at this step.

If you enter **slot1:** before the specified filename, 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.

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

Note: 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.

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.

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

Downgrading the NetScreen-500 Device

Caution: 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** 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"...
```

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.

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

Caution: 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.

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

Caution: 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:

   1. Go to Configuration->Update->Config File, and then click Save to File.
   2. In the File Download dialog box, click **Save**.
   3. 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 homepage.

CLI

a) Make 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) Run 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 reset the device.

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

h) Enter the **get system** 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 Firmeware.

b) Log into security device A.

c) Save the existing configuration:

1. **Configuration->Update->Config File**, and then click **Save to File**.
2. In the File Download dialog box, click **Save**.
3. 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. For information on obtaining the firmware, see section Downloading New 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 reset the security device. Execute the **reset** command and enter **y** at the prompt to reset 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 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.

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).

Warning: 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
```

Either 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). Check 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:

      1. Go to **Configuration >Update >Config File**, and then click **Save to File**.
      2. In the File Download dialog box, click **Save**.
      3. 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 homepage.

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 reset the security device. Execute the **reset** command and enter **y** at the prompt to reset 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
```

c) 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). Check 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:

   1. Go to **Configuration->Update->Config File**, and then click **Save to File**.
   2. In the File Download dialog box, click **Save**.
   3. 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 homepage.

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 reset the security device. Execute the **reset** command, then enter **y** at the prompt to reset 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.

h) 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.

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

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

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

Note: 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.

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.

(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

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
```

Addressed Issues in ScreenOS 5.4.0r4

The following major bugs have been fixed in this release:

Administration

- **cs12008—**In transparent mode, the CLI/WebUI incorrectly displayed the option to configure Route/NAT mode for a VLAN1 interface.

- **cs11548—**When setting an admin password through the WebUI, it could not contain the quotation character (") **W/A:** In previous releases use the CLI if using quotations (") in the admin password.

- **cs12112—**The firewall device did not send Node-Type P-Node (Peer-to-Peer) as a DHCP custom option; instead, the default type of Hybrid was always sent.

- **cs11769—**When using NSM and importing a NetScreen-5000 device with a 2xGE line module, the following error message is displayed: "Invalid enum value".

- **cs12230—**If the "get config" command does not match the "get config datafile" command, an NSM verify failure occurred.

- **cs10932—**If the HTTPS port is changed to a port number other than 443, the HTTP redirect is sent to the wrong port.

- **cs12284—**[SSG 500] The predefined service for RADIUS is set to dst port 5127-5383, which was incorrect.

- **cs12493—**The "get service syslog" command displayed the same information twice.

- **cs11980—**In some cases, while using NSM, the NSM agent part of ScreenOS was updating its datafile incorrectly.

Antivirus

- **cs12117—**With AV enabled, POP3 mail failed if the POP3 username contains “capa” (example: capa@test.com).

CLI

- **cs12571—**The "get config" command failed under certain circumstances with the console message: "Config generation failed due to writing config conflict."

- **cs11379—**[SSG] The device was unable to configure a serial interface with unframed E-1 options.

- **cs11925—**The CLI command "get route ip", incorrectly displayed some routes twice. This is a display issue only and did not affect functionality.

DHCP

- **cs12061—**An ISG device with an IDP module configured for transparent mode, dropped DHCP discovery packets.

HA & NSRP

- **cs11838—**In an Active/Active NSRP configuration, the packet forward received count was not correct.

- **cs11872—**In an NSRP configuration, when creating a sub-interface on a physical interface in the null zone, the MAC assigned to the sub-interface was that of the physical interface and not the virtual MAC.

- **cs12180—**In an NSRP configuration, the command "set nsrp rto-mirror session ageout-ack" did not work properly.

- **cs11566—**The secure ID node secret was not being copied to the secondary device correctly, thus causing problems with authentication after NSRP failover.

Management

- **cs12371—**In some cases, SSH from a Linux machine to a firewall device failed.

- **cs11890—**Inconsistency between config-file and datafile on NSM agent of the firewall caused errors on the NSM station.

- **cs11485—**The traffic syslog records contained an incorrect character in the leading digit for the send/recv byte count when reporting multi-megabyte sessions.---

- **cs07434—**The counter statistics returned from an SNMP query displayed incorrect values for the Ethernet2 interface.

Other

- **cs11804—**When “seq-number-validation” was enabled for GTP, the following error would occur: “sourceIP is not valid GSN”.

- **cs12239—**In some cases, LDAP CRL download caused the device to reset.

- **cs11920—**Management traffic from a trust subnet failed when used with source-based routing.

- **cs11422—**When NTP was enabled and set to an IP address, rather than a FQDN, the device was performing unnecessary DNS lookups for the IP.

- **cs12046—**When SQLNETv2 traffic passes through an IPSec tunnel in a NetScreen?-25, the session create for SQLNETv2 data channel was incorrect.

- **cs12259—**[NetScreen-5000] The device dropped protocol 253 packets even though the screen option “unknown-protocol” was disabled.--

- **cs12119—**The state of the interface is taken at the wrong time during bootup, which caused interface monitoring to not work properly.

- **cs11876—**[SSG 500] When in transparent mode the device incorrectly identified particular MAC addresses as multicast only, thus dropping the packet.

- **cs11585—**When using 802.1X on the trust interface and a radius server is on the untrust side, the negotiation between the NetScreen device and the radius server did not complete because of a radius malformed packet.

Performance

- **cs11909—**CPU usage was higher when adding ICMP-ANY as a multi-cell service in the policy.

- **cs11897—**On occasion, high CPU or packet loss would occur for a period of time after modifying a service timeout or the service name.

- **cs12409—**In a high traffic environment with "in overrun" counter increasing, the ISG exhibited packet loss.

Routing

- **cs11806—**Creating more than four Equal Cost Multipath (ECMP) routes would result in the error: “exceeds ecmp limit (4)”.

- **cs12391—**After a route failure, the aggregate BGP route did not populate the route table after the network is restored.

- **cs11312—**Internal marking of a host route timestamp would sometimes cause a stale route, resulting in the CPU utilization to increase.

- **cs11285—**In some cases, the device was not sending RIP updates even though a route-map was assigned to the protocol instance.

- **cs12376—**In some cases, multicast traffic may have problems going to specific groups. This happens when the incoming-interface of multicast route-entry added in the out-interface list.-

- **cs11614—**In some cases, RIP would clean stale routes incorrectly in the routing table.

VOIP/H323

- **cs12874—**In some cases, specific MGCP traffic would cause the device to reset.

- **cs11662—**An [SSG] device configured with MLPPP did not pass voice traffic.

- **cs11165—**In rare cases, timing and sequencing of hanging up and answering a VOIP call would cause the device to reset.

- **cs11984—**Under certain conditions, unsetting the Media Gateway Control Protocol (MGCP) ALG would cause the device to reset.

- **cs11911—**In some environments, a Media Gateway Control Protocol (MGCP) connection may have failed to pass through a firewall device.

- **cs11845—**During an upgrade to 5.3, the “unset alg sip” command was not recognized. **W/A:** In previous releases you can manually disable alg sip using the command “unset alg sip enable"

VPN

- **cs11409—**PKI SCEP enrollment was not working with some certificate authorities.

- **cs11837—**The tunnel interface goes into ready state when the VPN is down.

- **cs11217—**In some situations, enabling SurfControl web filtering in a VPN environment would result in permitted web sites displaying a blank page.

- **cs12272—**When IKE-NAT service was referenced in a policy and the traffic matching the policy required DST-IP translation, the source IP in the packet was incorrectly set to 0.0.0.0. **W/A:** In previous releases you can change the policy to another service, such as udp500 or ANY.

Web UI

- **cs12894—**On occasion, logging into the WebUI interface would fail. The user could see the login screen but when entering the user name and password the screen would freeze after clicking the login button.

- **cs11357—**[ISG 2000] Bandwidth of aggregate interfaces were reported incorrectly in the WebUI.

- **cs11961—**If the custom SurfControl URL profile name contained a space, the administrator was unable to delete categories through the WebUI. **W/A:** In previous releases you can use the CLI to delete the categories.

- **cs11969—**After configuring a custom SSL port, the SSG device randomly changes the SSL port. **W/A:** In previous releases you can upload and replace a saved configuration file without the custom SSL port specified.

Addressed Issues from ScreenOS 5.4.0r3

The following major bugs have been fixed in this release:

Administration

- **cs11171—**If using the commands set/unset global-pro policy-manager prima outgoing-interface and/or set/unset global-pro policy-manager sec outgoing-interface, upon reboot they are always changed to the set configuration, even if manually unset.

- **cs09504, cs07271—** When using RADIUS Authentication, after the third firewall login try, an error occurred when the device was reset.

- **cs10141—**[NetScreen-5GT] In some cases setting a VIP via the WebUI could cause the device to reset.

- **cs10349—**The NTP maximum adjustment incorrectly calculated the difference between the local clock and the time received through the NTP update, which resulted in an inaccurate clock reading.

- **cs10889—**The number of MIPs on a NetScreen-200 was incorrectly set to 100; the limit has now been corrected.

- **cs10884—**By default, the V1-Null zone is shared, whereas all other Layer-2 zones are not shared.

- **cs11484—**[NetScreen-5GT] Device only allows 3 secondary IP's to be configured, although it should allow 4. -

- **cs11297—**[NetScreen ISG 1000] There are invalid characters included at the end of the output when issuing the get log system save CLI command.

- **cs09635—**When using NSM, adding an aggregate interface in some cases caused the NSRP primary to reset.

- **cs07098—**Message guide error (00034) Message: SSH: Maximum number of SSH sessions () exceeded is incorrectly documented. The error “SSH: Max number () of session reached” is posted to the system log.

- **cs10950—**NetScreen-5GT was added to the 5.4.0 MIB files and duplicate entries were removed.

- **cs11009—**The NS Device did not send an accounting start message out for L2TP.

- **cs11457—**In some cases SNMP query of OID nsPlyMonPackPerMin is incorrect.

- **cs11095—**Syslog logging incorrectly duplicated source and destination port.

- **cs08725—**The non-vsys traffic log shows [No Name] on the syslog message.

- **cs10061—**Modifying the timeout value for a pre-defined service used in an ANY policy and configuring a timeout value for a custom service that includes the same pre-defined service could reset the timeout value to the default.

CLI

- **cs11400—**[NetScreen-5x00] In some cases, it can take more than 10 minutes to load a large configuration file.

DNS

- **cs10969—**The device sometimes restarts due to incorrectly handling a DNS server response.

HA & NSRP

- **cs08488—**A serial failover can cause the ISP's DNS to be injected into the devices internal DHCP scope.
- **cs12182—**Radius shared secret does not synchronize between the primary and secondary in an NSRP cluster.
- **cs11184—**In some cases in an NSRP environment, both device were recognized as primary, causing traffic to be affected.
- **cs10761—**In an NSRP configuration in which the aggregate interfaces were configured for specific duplex setting, executing the configuration sync CLI command on the secondary device could cause the duplex settings to be modified.
- **cs10590—**The command "set interface phy full 100mb" is changed "set interface phy full* 100mb" after NSRP configuration is synced. As a result, this command is removed after reboot.
- **cs04112—**In an NSRP environment, sometimes the interfaces used the physical MAC address instead of the virtual MAC address.
- **cs08853—**In an NSRP environment, configuring Radius auth-server from CLI, WebUI, or NSM and executing "exec nsrp sync global config check-sum" results in the error "Warning: configuration out of sync".
- **cs04844—**When passing heavy VPN traffic in Active/Active mode, the device dropped all fragmented packets.

Management

- **cs11631—**In a single ARM VPN configuration, telnet is allowed on the interface, even when telnet is disabled.
- **cs05878—**When using NSM, importing a deny policy will fail.
- **cs10475—**With SSH v1 enabled, SSH or WebUI management of the device could fail after several days. This is to due to the resources not getting released correctly. Workaround: Enable SSH v2 instead of v1.

- **cs07029—**The device had high CPU usage when syslog and policy logging were enabled.

- **cs11960—**After an upgrade, loss of communication between the firewall and NSM server could occur.

- **cs10985—**If a policy has the service MS-RPC-ANY, no other services can be added to the policy.

- **cs10113—**When multiple interfaces were bound to the Trust security zone, the device would send the Webtrends log to the last source interface created.

- **cs12260—**[SSG 550] In 5.4.0r2, when using the "get chassis" command, all the fans are reported incorrectly as being down.

- **cs12091—**Secondary SSG 5/20 devices using bgroup in NSRP loses configuration after sync and reset.

- **cs08870—**In some cases the NSM agent would fail to upgrade a device to 5.2r3.

- **cs10111—**NSM Active Sessions tab does not provide a consistent list of sessions.

- **cs11015—**When pushing a config to create a new VPN on a vsys, NSM sends an unknown 'exec password' CLI to the vsys, causing config push failure.

- **cs09856—**Memory resources were not being reclaimed when administration was closed before an internal process was finished.

- **cs11875—**[NetScreen-5200 M2 Management board] The out-of-band modem port does not function correctly.

- **cs10454—**(ISG 2000) The SNMP MIB iftype returned a value of other for the gigabit interface.

- **cs07702—**(ISG 1000 and ISG 2000) The MGT interface reports up and down status changes even though there is no physical connection, which is caused by noise. W/A: Physically connect the MGT interface.

Other

- **cs07232—**Incorrect handling of MSRPC messages occasionally caused a bootloop and the device to reset.

- **cs11681, cs11358—**In some cases Xauth was not working when using LDAP due to a cookie matching issue.

- **cs07062, cs07122—** In some cases telnet administration to the device will disconnect when an operation takes a long time(such as a paste of a config).

- **cs11329—**Application ignore is not available for SUN-RPC ALGs. W/A: Run the command “unset alg sunrpc” or “unset alg msrpc”.

- **cs11262—**When using a 10/100/1000 card there is no option for hard setting the physical interface to 1000mb.

- **cs10555—**When using multicast, intermittently, mroute is not formed, however the PIM join is being sent from the device to the RP.

- **cs11543—**When upgrading from 5.0.0 to 5.3.0 and above, service groups with multi cell policies may not be recognized upon reboot. This will cause the configuration of the device to be lost.

- **cs07583—**Incorrect handling of MSRPC messages occasionally caused a bootloop and the device to reset.

- **cs11320—**In some cases, multicast resources are reclaimed incorrectly.

- **cs09841—**[NetScreen-5GT Series] The device incorrectly interpreted the 802.1q tag of the incoming packet and placed the packets into the wrong interface buffer queue, therefore ARP works incorrectly.

- **cs10803—**In some cases sun-rpc-mountd service was not working properly.

- **cs08779—**Event log does not show the IP address of the Radius Server.

- **cs11336—**When issuing the get vsys CLI command, the output is aligned incorrectly with the column header.

- **cs10839—**Customer upgrade to 5.4.0r1.0 code, Syslog truncates "Dst=" IP in traffic log.

- **cs09474—**An issue in the dlog process (process that controls syslog and logging on policies) caused a failure on the primary firewall.

- **cs07816—**In some cases, CPU utilization may show a spike due to ARP not aging out correctly.

- **cs07800—**Incorrect handling of MSRPC messages occasionally caused a bootloop and the device to reset.

- **cs07466—**[NetScreen-500] In some cases when passing specific GPRS traffic the device would reset.

- **cs08697—**In some cases FTP was opening to many pports.

- **cs11643—**In some cases custom L2 zones could cause login errors due to unwanted fragmentation.

- **cs10100—**Interface counter for fragmented packets is not updated correctly.

- **cs11166—**Traffic is interrupted when a vsys element is removed, even though the element which is changed has nothing to do with the traffic other than using the same physical interface

- **cs10853—**In some cases when using Transparent mode with custom L2 zones, packets would be dropped.

- **cs10630—**Embedded ICMP packets dropped due to unnecessary and incorrect parsing for tcp seq checking.

- **cs10907—**After a restart, the source interface for Websense reverts back to default interface.

- **cs10407, cs10163—**[ISG 2000 and ISG 1000] With subinterfaces and DI enabled, traffic can be blocked and DNS lookups could fail.

- **cs09683—**In some cases, multicast prune messages were sent incorrectly during a switchover from Shared Tree to Shortest Path Tree (SPT).

- **cs09478—**Random high task CPU occurred after GPRS Tunneling Protocol (GTP) was configured.

- **cs09431—**[NS-5000 Series using an 8G or 24FE SPM] In some cases, both devices in an NSRP environment tried to become the primary device. This action occurred because an internal queue was incorrectly re-initialized.

- **cs09399, cs08119—** With MSRPC ALG enabled, a device reset with an error when very large actual_count MSRPC messages occurred.

- **cs11249—**When using transparent (L2) mode, arp entries were not correctly stored in the table.

- **cs08570—**SQLv2 traffic did not pass through the device when ALG was enabled.

- **cs07887—**NetScreen-25 sometimes fails to ping to local interface. It might also cause a failure in getting ICMP response from local subnets.

- **cs06741—**When using a NetScreen-5000 with a 24FE line interface module, in some cases MSRPC traffic could cause traffic to stop.

- **cs08760—**Outbound hardware counters stay at zero in DMZ-Dual Untrust port mode.

- **cs10912—**When using a NetScreen-5000 with aggregate interfaces the first UDP packet is lost.

- **cs07003—**In some configurations, sessions could be dropped if there is no policy in the direction of the session.

- **cs11189—**Firewall is restarting because of URL filtering.

- **cs10921—**When upgrading to 5.4r1 and 5.3r4, the session table is maxing out with very little traffic change. Some of the sessions which are across two different Interfaces are not closed even after receiving a FIN.

- **cs07588—**Incorrect handling of MSRPC messages occasionally caused a bootloop and the device to reset.

- **cs05474—**Manually setting the GE copper interface to 1000/full did not save.

- **os66651—**Update internal Daylight Savings Time (DST) tables for the new USA 2007 schedule.

Performance

- **cs11014—**In some configurations, in which there are many policies, the device could encounter high memory usage. Restart the device to recover from the situation.

- **cs08157, cs07605—**[NetScreen-5200 using 5000-M management module] Sometimes, the device gradually ran out of memory.

- **cs09453—**Due to an error in internal software session link list, high CPU occurred on ISG.

- **cs06223—**With TCP_SYN_Check disabled, and a large number of TCP RST packets received the device experienced periods of high CPU and telnet access was unavailable.

- **cs11948—**When using an NetScreen-5000 MGT2 w/2XGE interface modules in transparent (L2) mode, the CPU usage would increase due to UDP fragmented packets.

- **cs11091—**Due to a packet matching multiple signatures, multiple times, processing was not unique. This resulted in a packet loss on the IDP module and the CPU utilization to increase.

- **cs09795—**Traffic failed to pass through the device after the ISP central office reset the PPPoA connection. W/A: Manually disconnect and reconnect the PPPoA connection on the firewall.

- **cs11787—**[NetScreen-5000, ISG 2000] Task CPU could temporarily increase while waiting for an administrator to respond to a CLI prompted question (such as “Configuration modified, save [y]/n”).

- **cs08614—**Under certain conditions, policy push through NSM would cause performance problems.

- **cs12109—**Load sharing when using aggregate interfaces was not properly working.

- **cs11155—**[NetScreen 5x00] IP-over-IP fragmented traffic across two different device modules is handled incorrectly affecting performance and causing the CPU utilization to increase.

- **cs08776—**Slow performance occurs when media files are transferred using HTTP from an Apple Mac client.

- **cs08494—**ISG with a Security Module could encounter performance problems when a policy is pushed. This happens when CPU0 is made unavailable while a policy is being installed. Device performance remains stable if the Security Module is disabled. **W/A:** Contact JTAC for a patch.

Routing

- **cs08940—**The "get vr mroute" CLI command would sometimes incorrectly display the same source for multiple interfaces.
- **cs07627—**In a route based VPN multi-VR environment, the security device incorrectly performed a route lookup in the wrong VR.
- **cs10859—**Upstream router was not receiving ARP reply when an interface was in a logical down state.
- **cs10713—**Unable to re-connect to PPPoE when the ISP has provided a new IP address and an incoming DIP is configured in a policy for SIP.
- **cs08109—**The firewall accepts the default route on the serial interface through the PPP connection and might result in leaking of data through this default route if no other route is available to traffic on the firewall.
- **cs09820—**In a VSYS configuration using IP-classification, the device incorrectly handled a VSYS route lookup.
- **cs10883—**In a Win2003 environment, TFTP through the firewall would fail due to the ALG handling.
- **cs10822—**RIP routes show default metric of 10 no matter what it was configured as.
- **cs10749—**[ISG 2000] For VLAN tagged interfaces, the device is not passing traffic when DI is enabled on the policy.
- **cs06031—**PPPoE does not insert default routes into the routing table.

Security

- **cs11204—**Some standard traffic is incorrectly identified and dropped when Syn-cookie is enabled in Transparent (L2) mode.
- **cs11423—**The device resets when DI is enabled and a certain type of server message block (SMB) protocol is going through the device.
- **cs07048—**Syn-flood protection double counts the number of proxy sessions causing false alarms at times.
- **cs10976—**Security module failed while doing an update due to a bad internal pointer.

- **cs04592—**The ip-spoof feature "drop-no-rpf-route" was not working correctly.--

- **cs08754—**In Transparent mode, the Syn Cookie feature did not work correctly.

- **cs11469—**In some cases with url filtering using Websense, slowness may be caused due to URL request queue getting full on the firewall.

VOIP/H323

- **cs10962—**When sending a SIP message, the device is adding an extra ">" to the end of the header.

- **cs10556—**The firewall does not correctly NAT an H.245 IP Address.

- **cs11150—**Packets with a destination port of 2000 were inadvertently being dropped.

- **cs09708—**In some cases and configurations, specific VOIP and H323 traffic would cause the device to fail.

VPN

- **cs12168—**Certificate renewal does not propagate to the secondary device in an NSRP cluster.

- **cs12620—**When using the Infranet Controller the redirect URL field was not working correctly. The client was redirected by the enforcer but the redirect URL field is left blank.

- **cs11699—**Infranet Auth Controller with ISG 1000 redirect not working.

- **cs09081—**Changing the tunnel binding for multiple tunnels through the WebUI may cause the device to reset with an error.

- **cs11117—**The device will not allow the setup of a user group VPN within a VSYS with shared interfaces.

- **cs10155—**[NetScreen-5GT WLAN] In some environments, policy-based VPN tunnels using certificates would not connect. W/A: Configure the VPN tunnel to use pre-shared keys.

- **cs08518—**Rekey option incorrectly tries to initiate VPN through an interface that is down.

- **cs09981—**SA lifetime was incorrectly interpreted causing the VPN tunnels to rekeying around every 6 minutes.

- **cs08733—**In some cases using PKI for VPN tunnel negotiation caused the device to reset after about 30 days.

- **cs08905—**Memory resources were improperly reclaimed after VPN phase2 negotiations.

- **cs09123—**Dial-up VPN peers with Source Interface-Based Routing (SIBR) and Src-NAT were unable to communicate with each other.

- **cs11700—**IKE user with Distinguished Name and Xauth are disabled after reboot.

- **cs06358—**Large packets going into a policy based VPN tunnel were first fragmented and then encapsulated.

- **cs11358—**In some cases Xauth was not working when using LDAP due to a cookie matching issue.

- **cs11772—**In some cases when a MIP is configured on a tunnel interface associated with a VPN, the VPN will fail to negotiate Phase 2 correctly.

- **cs11761—**When using DHCP on the outgoing interface, VPN traffic stops, if the outgoing interface is assigned a new IP address.

- **cs05200—**When configured as route based VPN hub and spoke, packets from NetScreen device contained incorrect ESP sequence numbers.

- **cs04801—**The device could fail when a VPN tunnel is removed in an NSRP environment.

- **cs11236, cs11483—**After a device was upgraded to 5.3r4 and later, XAuth with RADIUS did not work. The following message could be posted to the event log: Phase 1: Aborted negotiations because the time limit has elapsed.

- **cs11294—**In the case where the serial backup interface took over while the DSL interfaces had gone down, and the option Dead Peer

Detection is enabled, when the DSL interface is restored retransmission messages are posted in the log.

- **cs04993—**After a device is restarted, the OCSP configuration for a CA-certificate could change to use CRL; resulting in the VPN failing to establish. When this happens, the error message PKI object store not correctly loaded <-1> is posted to the console display.

- **cs11086—**In some cases, when an existing dynamic VPN policy was deleted, the device would reset.

Web UI

- **cs10817—**With every update, NSM tries to set the interface physical parameters resulting in the following failure:
  Error Code:
  Error Text: Exception caught during Update Device:
  The following parameters did not get updated to the device: “set int ethernet2/1 phy manual’.

- **cs10736—**When the Policy Verification is performed on an IDP policy, this verification fails with the following error:

  Error Code:
  Error Text: Error in IDP validation:
  Error Details:
  error(s) found during validation.
  Invocation compiler error

  NOTE: This is only a validation error, the update to the device works fine.

- **cs10411—**Unable to bind ethernet0/3 to a zone other than HA.

- **cs10825—**ISG 2000 reboots when URL Filtering is enabled. **W/A:** Contact JTAC for a patch.

- **cs07175—**When using NSM, an unknown command sent to the vsys during a config push would cause a config push failure.

- **cs11356—**Disabling or enabling logging on a policy, using the WebUI, resets the sessions using that policy.

- **cs11029—**[ISG 2000]-Device would not change redundant vsi sub-interface settings via WebUI

- **cs09690—**[NetScreen-5GT] The WebUI Report for active users was calculated incorrectly for NAT users.

Addressed Issues from ScreenOS 5.4.0r2

The following major bugs have been fixed in this release:

- **os55174—**Not all error messages visible from CLI are available through the NSM interface. **W/A:** None.
- **os57620—**When an interface had both IPv4 and IPv6 address configured, if either address was used, the other IP address could not be unset from the interface.
- **os59154—**The VoIP ALG with HA under a very high load could experience a resource leak.
- **os63007—**For ISRAU with multiple GTP tunnels, not all tunnels were properly created.
- **os63351—**Enabling or disabling SIP ALG with outstanding calls could cause the device to restart.
- **os63487—**(WebUI) The allowed MTU range for VSIs was incorrect.
- **os63498—**ScreenOS did not block the configuration of and interface in the MGT zone even though the interface also had VSI configured.
- **os63513—**Unsetting the sub-interface could cause device failure if there was heavy traffic through a sub-interface with traffic shaping enabled.
- **os63523—**(NetScreenS-5400 using 5000-M2 and 5000-8G2 and 5000-2XGE) TCP traffic on the device did not always pass if the traffic crossed the ASIC chip and was through a VPN tunnel.
- **os63532—**A device with high AV traffic for a long time, the AV subsystem could run out of memory and continuously restart the AV process which could cause device failure.
- **os63543—**A GTP session could be incorrectly aged out after NSRP failover if the **teid-id** was configured.
- **os63612—**Repeated login from the same XAUTH user could cause the device to retransmit the account start message to the RADIUS server.
- **os63626—**RTO sync of GTP tunnel objects created new tunnels instead of replacing them.
- **os63632—**Unsetting the custom L2 zone, while there was still a VLAN port associated with it, could cause system failure.

- **os63638—**Internal BIOS changes on the SSG-140 before public release did not properly initialize onboard interfaces with ScreenOS 5.4.0r1.
- **os63861—**(SSG 20 ADSL mini-PIM with PPPoA enabled) Some websites could not be displayed.
- **os63911—**(SSG 20) For ISDN interface set as primary interface, track-ip could not dial up when the interface is down.
- **os64355—**(SSG 5 and SSG 20) Asymmetrical VPN performance was impacted by decryption and encryption.
- **cs07991—**The NSM Logviewer incorrectly displayed sessions with multiple attacks as accepted even though they were dropped.
- **cs09404—**(ISG 2000 and ISG 1000) When many sessions were synchronized between the active and backup NSRP devices, sometimes performance dropped and the device restarted
- **cs09764—**When using the mtrace command, replies were not correctly reporting.
- **cs09777—**After an NSRP failover, in some cases the primary device had problems reconnecting with the NSM server.
- **cs09849—**Sessions on an NSRP backup device were not being properly removed.
- **cs09968—**(ISG-1000) After the IDP was enabled via a policy push, the device stopped forwarding packets. This was caused by a combination of fragmented packets (TCP & UDP) with a TTL value of 1.
- **cs09981—**SA lifetime was incorrectly interpreted, causing the VPN tunnels to re-key approximately every 6 minutes.
- **cs10163, cs10407—**(ISG 2000 and ISG 1000) With subinterfaces and DI enabled, traffic could be blocked and DNS lookups could fail.
- **cs10180—**The DNS refresh schedule was unreliable.
- **cs10310, os62872—**After entering the unset alg sip enable CLI command, when viewing the system configuration, the command unset sip alg enable is displayed twice.
- **cs10378—**Configuring custom group services with multiple MS-RPC service types could cause the device to restart.
  W/A: Use the ms-rpc-any service in a custom group service or create individual policies.
- **cs10425—**No SNMP traps are sent to x.x.x.255 even though the host address could be configured.
- **cs10427—**(DHCP relay) The broadcast flag was always set to 0 regardless of the original request.

- **cs10446—**In some cases, the device intermittently blocked spanning tree frames.
- **cs10454—**(ISG 2000) When using a standard SNMP walk, the value other was returned for the Gigabit interfaces.
- **cs10462—**In some cases, the SIP B2BUA feature did not work consistently.
- **cs10465—**A backup device was not synchronized when the **unset vr trust-vr nsrp-config-sync** CLI command was configured on a shared virtual router (VR); the **exec nsrp sync global save** CLI command was issued, and the device was restarted.
- **cs10505—**(IPv6) The device reset if the wrong buffer was retrieved.
- **cs10582—**After upgrading from ScreenOS 5.0, the set nsrp monitor int mgt CLI command became invalid.
- **cs10610—**Large numbers of TTL packets with value zero caused high CPU usage on the security device.
- **cs10621—**FTP transfers could fail when reassembly-for-alg was enabled.
- **cs10624—**Packets were not sent out when the dial-up VPN was configured on the loopback interface in a vsys.
- **cs10658—**In some configurations, retrieval of Certificate Revocation List (CRL) information through an LDAP server failed.
- **cs10662—**(SSG-520/550) WebUI was showing discrepancy for serial interface counters compared to CLI output.
- **cs10702—**When using a GRE tunnel, fragmented traffic was sometimes dropped.
- **cs10802—**Inconsistency configuring static route (with tag) redistributed into OSPF, using match tag route-map. For example, with tag 1 in the static route configuration, the command line allowed input only of the number 1, not 0.0.0.1; but when applying or using the tag (in route-map), the command line allowed both 1 and 0.0.0.1 when defining the route-map.
- **cs10809—**(SSG devices) Anti-Spam service did not work.
- **cs10817—**With every update, NSM tried to set the interface physical parameters, resulting in the following failure:

  Error Code: Error Text: Exception caught during Update Device: The parameters in the following CLI command were not updated to the device: set int ethernet2/1 physical manual.
- **cs10839—**When customer upgrade to 5.4.0r1.0 code, Syslog truncated Dst= IP in the traffic log.
- **cs10869—**In some cases, parts of a VPN remote user configuration was removed upon restart, causing connection problems.

- **cs10879—**When using the WebUI—with a GRE tunnel configured—clicking the apply button without entering any information removed the GRE next-hop tunnel association.
- **cs10920—**In some cases, UAC using 802.1x to connect caused the device to reset.
- **cs10968—**A configuration save took much longer than in previous releases.
- **cs11099—**With upgrade to ScreenOS 5.4.0r1, NTP task caused high CPU usage (~80%) when there was no traffic on the device.
- **cs11358—**In some cases, due to a cookie matching issue, Xauth did not work when using LDAP.

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.

Limitations of Features in ScreenOS 5.4.0

This section describes the limitations in various features in ScreenOS. They apply to all platforms, 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 1. Virtual Systems Capacity for NetScreen 5000 Series Device

ScreenOS				
	NetScreen-5200 using	NetScreen-5200 using	NetScreen-5400 using	NetScreen-5400 using

	5000-M	5000-M2	5000-M	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 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 2. 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.

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 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. Refer to Upgrade Paths to ScreenOS 5.4.0 for intermediate software and boot loader upgrade information.

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.

Known Issues in ScreenOS 5.4.0r4

The following, organized by category, 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**.

Administration

- **cs13306—**When trying to manage the firewall, the firewall restarted because it accessed a corrupted net-pak buffer.

- **cs10664—**When adding an interface to a security zone, then adding a second interface, the default interface for the zone changes to the newly added one. If you then remove and re add the first interface the default interface follows the latest one added (first interface) until a reset; in which case it will then revert back to the second interface.

Antivirus

- **cs13618—**A memory leak occurs with the Trend Micro AV feature enabled in ScreenOS.

- **cs13488—**Web traffic passing through a proxy server that is behind a firewall can experience delays or dropped packets. This particularly applies to traffic passing through a policy that has the antivirus feature enabled and the proxy server configured on port 8080 (as opposed to tcp/3128, the default).

CLI

- **cs13213—**[SSG] The command "get chassis" does not show whether any of the power supply units have failed.

HA & NSRP

- **cs12388—**When DI is enabled for a policy in an active/active NSRP setup with asymmetric routing, NSRP data-forwarding traffic is denied causing traffic to be dropped. **W/A:** Use symmetric routing or source-based routing to ensure that traffic in both directions goes through a single firewall.

- **cs13103—**With TCP sequence check enabled in a VSD-less configuration (vsd 0 unset and local interfaces) after fail-over and fail-back, the sessions will not sync, causing traffic for existing sessions to be dropped. W/A: Disable TCP sequence check using "set flow no-tcp-seq-check".

- **cs13209—**A backup device does not do ARP requests when the interface is in inactive mode or when the interface is disconnected and then reconnected.

NAT

- **cs13328—**You may see dip allocations failure for FTP data connection when using an interface based nat source.

Other

- **cs12459—**Issue with FTP downloads when AV is enabled.

- **cs13350—**Active firewall crashes after adding UAC IC6000 cluster.

- **cs13486—**The firewall is unable to forward PIM BSR message under PIM-Sparse Mode since the firewall treats it as a unicast message. The command "debug pim all" shows a message showing "PIMSM Received unicast bsr message hence no need to FWD"

- **cs13409—**HA interface counter mismatch occurs. If you look at the counters on both HA interfaces they do not match. You would expect to see the master data channel count transmit information to be equal to the backup data channel count for receive. This is also observed for both control links.

- **cs13226—**Some times during the flow processing, after a packet's arp entry is determined and before packet is being sent, the arp entry is freed, which caused the device to fail.

- **cs13176—**In scenarios using the ARP method for track-ip, changing the track-ip interval may cause track-ip failure.

VOIP/H323

- **cs12791—**With MGCP ALG enabled, the firewall may reset while processing a call.

VPN

- **cs12752—**The proxy ID for a dial-up VPN may be set back to 255.255.255.255 when some other policy is edited. NetScreen-Remote clients may see the login/password prompt popping up on the screen, even if the connection is not made. This is applicable when multiple policies are referring to the same DIALUP VPM. **W/A:** With a reset the problem disappears temporarily.

Web UI

- **cs12797—**In some situations, when accessing the firewall's WebUI interface, the home page in WebUI takes a long time to load.

- **cs13255—**When enabling RIP on a tunnel interface through the WebUI and then clicking apply, the entry looks fine, but once you click OK, the tunnel interface's RIP information is removed.

Known Issues from ScreenOS 5.4.0r3

The following, organized by category, 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**.

Administration

- **cs12503—**In ScreenOS 5.4, when saving the policies report using the WebGUI the saved file is empty. The WebUI will prompt for a filename, the device creates the file, but there is no information in it.

- **cs11896—**In some cases during an IKE P1 initiation event log/syslog is not generated.

- **cs11301—**[SSG 550] Webtrend output log is not consistent with other devices.

- **cs12015—**The NSM heart-beat interval is not changing even if the command "set nsmgmt hb-interval" is set.

- **cs11725—**When configuring a device using NSM, in some cases the VPN peer ID is not populated correctly.

- **cs12527—**Device incorrectly sends IP Spoofing alarm log messages from legitimate IP addresses at bootup.

- **Cs11106—**[NetScreen 5000 series] The “clear count all” CLI command does not clear the interface counters on a 5000-24FE SPM configured with aggregate interfaces.

- **cs12498—**The device will generate an IP Spoof alarm if the traffic is going to the device when booting up.

- **cs11458—**When using NSM, the maximum number of VIPs configured for ScreenOS 5.1 and above is incorrect.

- **cs12238—**In some cases the device is keeping vlink info in a datafile even though it is not in the config which causes errors with NSM.

- **cs12230, cs11890—**If the "get config" does not match the "get config datafile" this causes an NSM verify failure.

- **cs12613—**SNMP counter does not update until "get count stat" is issued from CLI.

CLI

- **cs12128—**ISG 2000 NSRP cluster primary unit core-dumped when pasting commands via CLI.

DHCP

- **cs12646—**Device changes the DHCP relay agent IP when it is configured as a DHCP relay.

- **cs12385—**When using bgroups and DHCP, update of the DNS does not always work properly.

HA & NSRP

- **cs12605—**When in a NSRP configuration, GTP messages could be misinterpreted causing the device to reset.

- **cs11602—**After issuing an update, the NSM UI displays one of the NSRP cluster devices as "Managed, Device Changed". The status change occurs when using supplemental CLI to set commands that are un-managed from NSM.

Management

- **cs12055—**Unable to manage the device via http using tunnel interface manage-ip.

- **cs12566—**Read-only admin cannot Issue 'get' commands.

- **cs12364—**In the WebUI, "Reports > System Log > Self" shows the wrong port numbers. W/A: use the CLI command "get log self".

- **cs10111—**NSM Active Sessions tab does not provide a consistent list of sessions.

Other

- **cs11183—**Dial-Up VPN users connected to an SSG device may experience slowness with Outlook after some period of time. W/A: Modify the MS-Exchange service timeouts to 30 minutes.

- **cs12715—**When using IPV6 passive FTP does not work correctly.

- **cs12194—**[ISG 2000] In an A/P NSRP environment, in some cases FTP data transfer fails after failover.

- **cs12691—**In an extreme condition, large auth table and high number of sessions would cause the device to reset.

- **cs12567—**When using SecurID, if a user inputs the wrong passcode 3 times, SecurID will prompt for next code. However, even after entering the correct code on the SecurID token, it fails.

- **cs11464—**[SSG 550] The option to set the physical interface to full 1000 is not available.

- **cs11128—**When using aggregate ports, SNA traffic did not traverse the device.

- **cs12332—**When in transparent mode (L2) IPv6 does not pass through the device.

- **cs12440—**Traffic shaping on MLPPP drops all traffic.

Routing

- **cs12307—**When configured for OSPF, routes across a GRE tunnel appear inactive in the route table.

- **cs12501—**When OSPF cost value is above the limit, the route is incorrect in the route table.

- **cs10252—**In some cases, disabling OSPF process once it has been established could cause the device to reset.

Security

- **cs11679—**[SSG 500] DI attack detection stops after several days.

- **cs12665—**[NetScreen-5000] In some cases the syn-cookie feature did not work properly on a 10G interface.

VOIP/H323

- **cs06688—**Transmitting H323 from a Tandberg device through an ISG 2000 may fail due to a packet size limitation; the current limit is 1400. [Reported in 5.2]

- **cs11592—**The SIP error packet is not processed by stack. The SIP stack of 5.4 needs to be enhanced to handle messages that contains "#" character in the user name part of URI.

- **cs11767—**In some cases RTSP packets are dropped inadvertently.

- **cs11375—**When establishing a NetMeeting voice (H323) session from a client behind a NetScreen-5GT in NAT mode could fail.

VPN

- **cs12434—**VPN Dialup using ike-id asn1-dn wildcard fails
- **cs11409—**PKI SCEP enrollment was not working with some certificate authorities
- **cs12441—**In some cases when using NSRP, the modem password is not synced properly.
- **cs12484—**When using a VPN, packet fragments with size equal or greater than 1500 bytes are dropped.
- **cs12156—**SSG5 VPN to third party VPN device - problems with Phase 1 rekey
- **cs11413—**Memory leak on SSG-500 due to PKI online CRL

Web UI

- **cs10589—**Portions of IGMP configuration was lost after the device was rebooted.
- **cs08811—**The WebUI incorrectly creates an RP-candidate after enabling PIM instance on an interface. If using NSM this also affects NSM pushing of a configuration.
- **cs11918—**The WebUI displayed an error prompt when adding/editing VSYS interface.
- **cs11716—**A SIBR route cannot be removed through the WebUI.
- **cs12231—**When using the WebUI, some pages do not load when web filtering is enabled.
- **cs12792—**By clicking on a policy with DI configured via the WebUI, then clicking cancel, the DI configuration is erased.

Known Issues from ScreenOS 5.4.0r2

The following, organized by category, 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**.

Administration

- **cs03723**—It is not possible to create a configlet for a device in transparent mode.
- **cs11232**—When viewing a vsys configuration, the first vsys listed in the configuration file has vrouter information while subsequent vsys entries do not.
- **cs11548**—When setting an Admin password via the webUI, the password can not contain the double quotes character (").

  W/A: Use the CLI.

HA and NSRP

- **cs11566**—The Secure ID node secret is not correctly copied to the backup device, causing problems with authentication after an NSRP failover.
- **cs11200**—While in a NSRP configuration, when adding or removing address or service objects, in some cases the information is not being synchronized to the backup device.

Management

- **cs10475**—With SSH v1 enabled, SSH or WebUI, management of the device can fail after several days because the resources are not correctly released.
- **cs11121**—The following system log message is put into the event log, at boot up.

  ```
  system alert 00062 SCCP ALG enabled on the device.
  ```

  ```
  system alert 00062 SCCP ALG registered line break to tcp-proxy.
  ```

- **cs11274**—In some cases pushing a large configuration to a device using NSM might cause the device to reset.

Other

- **cs09711**—An ISG device with an IDP module produces a false positive of SMTP: MIME filename directory traversal for ISO-2022-JP encoded files.
- **Cs10159**—RTSP traffic is dropped when using a MIP.

  W/A: Disable the RTSP ALG.
- **cs11001**—Traffic is dropped even when a policy is set to allow it.
- **cs11207**—The exclamation point character (!) is not supported as a negative policy delimiter.
- **cs11422**—When NTP is enabled and set to an IP address rather than a FQDN, the device does an unnecessary DNS lookup for the IP.

Performance

- **cs10105, cs10471**—The bandwith option on WAN interfaces does not work properly.
- **cs11091**—Due to a packet matching multiple signatures multiple times, processing was not unique. This resulted in packet loss on the IDP module and an increase in CPU usage.
- **cs11116**—Traffic loss is experienced when an interface is removed, This is due to the device removing the ARP entry by mistake.

Routing

- **cs10252**—In some cases, disabling an OSPF process once it has been established causes the device to reset.

  W/A: Enable SSH v2 instead of v1.
- **cs10821**—RIP redistributes static routes pointing to a VSI interface regardless of the VSI interface state.
- **cs11285**—In some cases the device does not send RIP updates even though a route-map is assigned to the protocol instance.
- **cs11312**—Internal marking of a host route timestamp can create a stale route, thus causing CPU utilization to increase.
- **cs11614**—In some cases RIP does not correctly clean up stale routes in the routing table.

VoIP/H.323

- **cs11165**—In rare cases, the timing and sequence of hanging up and answering a VOIP call can cause the device to reset.

WebUI

- **cs11046**—(NS-5000) There is no **Asynchronous VPN** button in the WebUI.
- **cs11357**—(ISG-2000) The bandwidth of aggregate interfaces is incorrectly reported in the WebUI.

Known Issues From ScreenOS 5.4.0r1

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**.

- **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.

- **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 inproperly 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.
- **cs10444**—(NetScreen-5000 Series using 5000-M2) The device erroneously reports a high number of sessions (1,000,000) through SNMP.
- **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.
- **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.

  W/A: Use the CLI.
- **os58602**—The device returns a non-zero value when exiting from an SSH or SCP session.
- **os58624**—In some cases, an accounting-ON message is unsent.
- **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.

  W/A: 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.
- **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.

  W/A: 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.

  W/A: 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 filename 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.

  W/A: 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.

- **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 session 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 reset 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.
- **os63287**—When switching between Transparent mode and Route mode, some error messages might be displayed upon restart for commands that are unsupported.
- **os63138**—(ISG 200) 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.

- **os63527**—During internal H.323 stress testing, NSRP failover issues occurred.
- **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.

- **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.
- **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.

- **os63974**—Multilink PPP (MLPPP) does not accept frames with compressed headers.

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

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.