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 5.4.0r12
Revision: Rev 01
Part Number: 530-028951-01
Date: January 2009

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 5.3r10, 5.2r3b, 5.1r4d, and 5.0r11.

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.

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 Introduced in 5.4.0r1

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

Note: You can use NetScreen-Security Manager (NSM) 2006 with the Forward Support Update software to manage devices running ScreenOS 5.4. To do this, install a schema upgrade on the management server and user interface. The

upgrade is available at http://www.juniper.net/customers/support/. Refer to the NSM Forward Support for ScreenOS 5.4 Release Notes for installation instructions and the features and platforms supported with this schema upgrade. NetScreen-Security Manager (NSM) 2007.1 and successive versions support devices running ScreenOS 5.4 without need for Forward Support Update software.

Note: For ISG with IDP platforms the Detector Engine shipped with this ScreenOS version is 3.1.117412.

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.

Changes to Default Behavior

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

Note: If the ScreenOS version is not mentioned in this section, the change in behavior was released with ScreenOS 5.4.0r1.

Changes to Default Behavior Introduced in 5.4.0r11

DNS Port randomization

The ability to enable random port assignment for policy-based DIP pools has been added; both interface-based DIP pools and policy-based DIP pools can now have ports randomly assigned. Interface-based DIP pools have random port assignment by default. Policy-based DIP pools, however, are default set to port translation, so random-port must be manually enabled by an admin.

The random-port keyword has been added to CLI syntax for both DIP pool and extended DIP pool:

set interface*ifname* ext ip*ip/mask* dip *dip_id ip_low ip_high* [random-port]

set interface *ifname* dip *dip_id ip_low ip_high* [random-port]

VPN (285743)

The IKE-ID type with numeric IKE-ID from a third-party VPN device is interpreted correctly during Phase1 negotiations.

WebUI (262490)

In the WebUI, managing a device from an untrust interface using a trustee admin now functions properly.

Changes to Default Behavior Introduced in 5.4.0r6

WLAN

The permitted frequency ranges for wireless devices has been reduced to satisfy FCC requirements. "For more information, please read the JTAC knowledge base number KB 9915"

Changes to Default Behavior Introduced in 5.4.0r1

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. This behavior is only applicable when the “set log audit-loss-mitigation” option is set. By default, this option is unset.

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-down" CLI, link-down option is disabled for wan interfaces

NSM Compatibility

This section provides information about updates required to complementary Juniper Networks products to ensure compatibility with ScreenOS 5.4.

Netscreen-Security Manager (NSM) 2007.1 and successive versions support devices running ScreenOS 5.4 without need for Forward Support Update software.

NSM 2006 requires Forward Support Update software to manage devices running ScreenOS 5.4. To do this, install a schema upgrade on the management server and user interface.

The upgrade is available at http://www.juniper.net/customers/support/. Refer to the NSM Forward Support for ScreenOS 5.4 Release Notes for installation instructions and the features and platforms supported with this schema upgrade.

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 boot loader firmware. Firmware Upgrade Path illustrates the various firmware upgrade paths to ScreenOS 5.4.0.

Figure 1.Firmware Upgrade Path

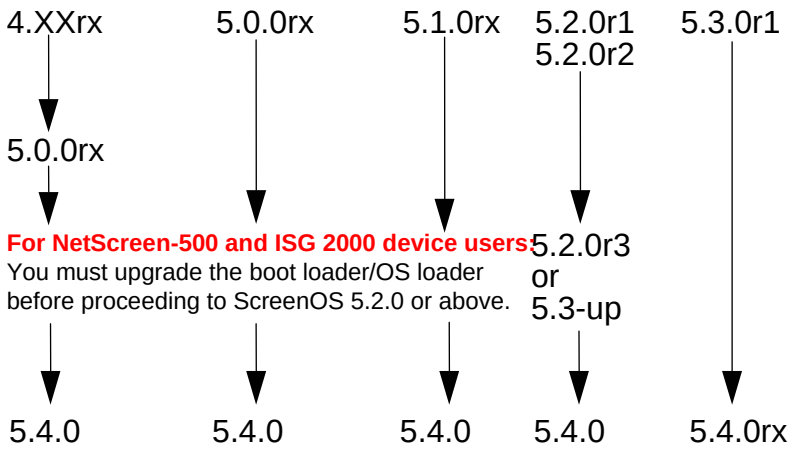


Figure 1 lists the recommended upgrade path to ScreenOS 5.4.0 based on device model and firmware version. For example, if you are running ScreenOS 4.0 on a NetScreen-204, you need to upgrade to ScreenOS 5.0r10 or later before

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	None required	

NS-5000-8G NS-5000-2G24T		
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 NetScreen-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

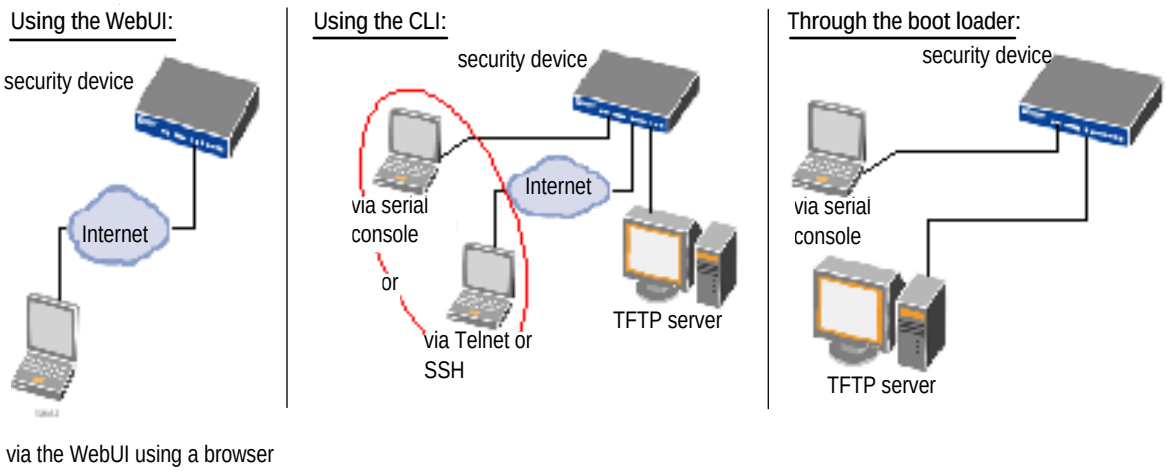
- Console connection or Telnet access to the security device from a computer
- TFTP server installed locally and to which the security device has access
- New ScreenOS firmware (downloaded from the Juniper Networks website and saved to a local TFTP server directory)

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 boot loader upgrade is required, you must upgrade using the boot loader.

To upgrade or downgrade a security device, see the step-by-step procedures in 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 boot loader upgrade before installing ScreenOS 5.4.0. Use either the WebUI or CLI procedure to first install intermediate firmware (if required), then install ScreenOS 5.4.0 firmware.

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:

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

b) Log into security device A.

c) Save the existing configuration:

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

Detector and Attack Objects Update (only for ISG-IDP)

The Detector Engine shipped with this ScreenOS version is 3.1.117412. Refer to the Detector release notes for more information on the availability of new releases.

After you have performed the ScreenOS firmware upgrade, you must update to the latest IDP detector engine and attack object database.

To update the detector and attack objects database:

1. Download the latest detector and attack database to the NSM GUI server. From NSM, select Tools > View/Update NSM attack database and complete the wizard steps.

2. Push the detector update to ISG-IDP devices. From NSM, select Devices > IDP Detector Engine > Load IDP Detector Engine and complete the wizard steps.
3. Push a policy update to ISGIDP devices. From NSM, select Devices > Configuration > Update Device Config and complete the wizard steps.

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 5.4.0r12

The following major bugs have been fixed in this release:

Administration

- **309023**—The device cannot be managed using the OpenSSH 5.1p1.
- **310993**—The Device fails on creating a zone with a name length of 30 or 31 bytes.
- **313447**—Debug flow buffer is populated with "NHTB entry search not found: vpn none tif..." messages.

DHCP

- **263924**—When using a PPPoE interface with a DHCP IP address as the tunnel outgoing interface, the VPN tunnel session still has the old dynamic IP address. This occurs even after the new address has been assigned or the firewall is restarted.

DNS

- **309725**—The WebUI displays incorrect value of DNS cache TTL.

HA & NSRP

- **251157**—The device resets when the NSRP cluster member receives a corrupted HA message.
- **251324**—After the track-ip fails, the primary and backup interface continue to flap until the firewall is rebooted.

- **287173**—The NSRP configuration goes out of sync when a new username and password is added.
- **300517**—The TCP packets for existing sessions are dropped after failover when the "set flow tcp-syn-bit-check" is configured.
- **300760**—When the password hash of the PPPoE username differs on the two devices, the NSRP displays out of sync.
- **306981**—The NSRP configurations go out of sync when the CLI configuration lines are out of order. The CLI configurations lines go out of order when one of the members is reset.

IDP/DI

-
- **301944**—The DI HTTP brute search functionality is incomplete.

Management

- **394878**—The collection of Hardware counters is incorrect.

NAT

- **284672**—When the PPORT is not released, then the DIP allocation fails on the backup device of NSRP cluster.
- **303836**—The device does an incorrect translation of the ICMP sequence number when it receives an ICMP response where both the original ICMP ID and the sequence number are 0.
- **307364**—Interface IP address can be unset even when its MIPs are being used by policies. These MIPs are stored in the configuration and are removed only after the device is reset.
- **308572**—Pinging a DIP IP address results in a routing loop with an upstream device.

Other

- **235297**—The source MAC does not cache in session for PIM traffic.
- **251259**—After a POST request, use of URL filter by some http clients generates extra CRLF might cause an out of memory situation.
- **252037**—Device unexpectedly resets after an 802.1q tagged packet traverses the Security Module.
- **256236**—In transparent mode, tcp-ack forwarded through the firewall causes a checksum error when the VLAN1 IP is unset, and syn-cookie is enabled under syn-flood attack.
- **260307**—Under certain conditions, the firewall corrupts the UDP checksums.
- **267767**—Running "get dbuf stream" prints the message "return due to suspect loop" without any debugs specified.
- **279557**—[SSG Series] The traffic continues to pass even when the WAN serial interface with a backup interface is down.

- **284851**—The firewall authentication might fail when loopback session is invoked.
- **285333**—If a duplex mismatch occurs between the device interface and the switch connected to the device, then the traffic might not pass.
- **286361**—Instead of the primary server, the secondary server receives the external authentication request.
- **290666**—On adding an interface state check in an IPv6 deployment, a null interface might cause the device to fail.
- **298540**—The load-threshold setting for an ISDN interface supports the range 0~100, where a zero value allows for always-up capability.
- **301487**—When using the redundant interface, the snoop functionality is incomplete.
- **301602**—A Linux host is unable to access any web site when the web filtering, anti-virus or the VoIP is enabled.
- **309986**—The event “DHCP server IP address pool changed” is generated when the IP address of the untrust is changed.
- **310435**—When installing the policy tree, access of an illegal memory might cause the firewall to fail.
- **310566**—With SSG5 (Country code of TELEC), the extended channel might be disabled after reset of the device.
- **391368**—The device might reset if the null pointer access prevents the PPPoE control packet being sent out when the PPPoE connection is down.
- **403625**—[NetScreen-5000] The device might reset when redundant interface is configured using the 8G card.

Performance

- **281813**—[NetScreen-5000] Performance on 10Gbps Ethernet is reduced for transit traffic in and out of the same physical port.
- **292576**—When the window scaling factor in SYN ACK packet is not updated in hardware session, an out of sequence error is induced.
- **304334**—The "session scan" task is ineffective when the CPU is high. This is because of constant ARP changes in the network.
- **315217**—[NetScreen-5000 10 Gig] The hardware sessions that are not load balanced in FPGA on backup device cause performance drop after failover.
- **386735**—When adding interface member to aggregate interface in null zone, if aggregate sub-interface is in non-null zone, packet drops are caused due to loops between ASIC and CPU.

Routing

- **223932**—When the ‘set flow path-mtu’ is configured, then the multicast packet with the DF bit set, that are more than 576 bytes in size will get dropped.
- **256473**—Traceroute across an intrazone route based VPN fails.
- **264800**—The route table of the device does not include the default route as advertised via the BGP by the upstream router of the ISP.

- **278718**—After rebooting, the static default route on the PPPoE interface is lost.
- **312042**—An administrator can configure a multicast address on the unicast route table.
- **312623**—Firewall is incorrectly calculating checksum for PIM Register packets.

VoIP

- **230295**—The point to point H.323 traffic fails due to invalid TPKT value.
- **276513**—SIP application error, “Due to stack unable to handle empty display name”.
- **305658**—The RTP packets are lost when NAT-T is enabled.

VPN

- **257708**—The device might reset when subjected to heavy GRE or IPSec traffic.
- **305067**—Device incorrectly decrypts the VPN packet with certain TTL value.
- **305283**—[NetScreen-5000, ISG 1000/2000] ASIC drops the ESP fragment packet.

WebUI

- **289671**—The WebUI fails if there is a change in the tunnel binding.
- **313278**—When connected through SSL VPN proxy, unable to manage the firewall using the WebUI.

Addressed Issues from ScreenOS 5.4.0r11

The following major bugs have been fixed in this release:

Administration

- **259735**—Incorrect information was shown on the multilink and serial interface SNMP report for MTU, link status, operation status and link speed.
- **267997**—Incorrect information was shown in OID ifIndex when link-up/link-down SNMP trap for redundant interfaces occurred.
- **273937**—WebUI to an interface is accessible, although "IP Manageable" is disabled on the interface.
- **278125**—The device resets when there are multiple policies using the same SRC/DST IP and ports, and one is disabled, and one of the address book objects is modified.
- **279094**—Unsetting PPPoE auth-method will erroneously generate the message "Cannot unset idle-interval to default when auto connect is enabled".

- **288632**—Changing service timeout does not take effect if the service is part of a multi-cell policy after a reboot of the device.
- **292227**—[SSG 140] Device could not load OS after a restart.
- **299556**—Modifying service timeout does not get logged as a configuration change in the event log.

Antivirus

- **286714**—In some cases, the Antivirus pattern files are missing and the new file is not downloaded. The scan engine reports a File Not Found message.
- **293490**—In a Web proxy environment, the URL is printed twice in the event log when the AV is enabled.
- **295023**—With the AV enabled, when a non-written memory page was freed up, the device fails.

CLI

- **271297**—The "get perf session detail" command does not display the correct values.

DHCP

- **253304**—Device fails due to multiple DHCP renew.
- **282543**—In certain situations, the device is unable to send a DHCP client request.

DNS

- **215889**—DNS queries are sent to the dynamically-learned DNS servers, even though the DNS servers have been configured with an admin preference of 255.
- **261613**—Proxy DNS does not work when configured to use outgoing-interface loopback.

GPRS

- **260243**—When the rate limit in a GTP object configuration is disabled, the limit is not actually disabled.

HA & NSRP

- **252645**—Gratuitous ARPs for the secondary IP address on an interface is not functional.
- **258242**—In NSRP active/passive mode, the primary device restarts when the pointer has an invalid value.
- **262695**—NSRP failover may cause some VPNs to fail.
- **264768**—Configurations are out-of- sync due to out of order PBR configurations, including the policy-based-routing commands.
- **268708**—Traffic does not pass after failover of a NSRP pair with devices configured in transparent mode.

- **268809**—When no-session-backup is enabled on a policy, traffic through the serial interface does not pass.
- **274997**—The commands "set sm enable" and "set sm disable" were erroneously being synchronized to another member in an NSRP cluster.
- **280217**—[NetScreen-5000, ISG] When the device is in an active/passive NSRP cluster, under a particular circumstance after a preempt primary device is reset, the traffic using VPN is dropped by the VPN peer.
- **282261**—NSRP failover from the backup to the primary is taking more time than the expected.
- **288925**—NSRP configurations are out of sync after unset multiple objects are applied in a multi-cell policy.
- **295846**—The device in an NSRP cluster reset when the device is trying to update and resolve the DNS entry.
- **301156**—Multicast traffic leak occurs on the secondary device in the transparent mode under high traffic load.

IDP

- **258336** —The device restarts when the Deep Inspection Signature Pack is updated.
- **260215**—When profiling smaller networks, the profiler on an ISG-IDP does not detect new events. The profiler does not update old events.
- **264486**—[IDP] Policy installation does not function due to lack of available memory.
- **276587**—[ISG-IDP] VLAN tagged traffic is incorrectly handled and dropped by ISG with IDP modules when IDP and tcp-syn-check is enabled.
- **297722**—IDP may drop sessions in half-connection state if a packet with ACK set is received.
- **298358**—The device resets due to an unspecialized DI attack object in the DI database.

Management

- **252783**—When the command "clear counter interface" is performed, the 64-bit counter on an interface does not show correct information.
- **261465**—Custom web filtering profile is not saved in the config file.
- **266159**—[SSG 140] SNMP MIB walk shows SSG 240, instead of SSG 140.
- **273959**—An object cannot be added to an already existing multi-cell policy.
- **291310**—TTY and socket is not released after telnet service timeout on the device have been reached.

NAT

- **267994**—CPU utilization is high after the Virtual IP (VIP) is configured.
- **298064**—Device may reset under certain environment when using the DIP pool.

Other

- **214346**—When obtaining details of an unmapped memory address, the device resets.
- **219085**—When an unsafe procedure call is made while running debug mgcp, the device resets.
- **229408**—When the display information is too large, other tasks will modify the current display content, which may cause a failure.
- **235777**—The command "unset admin hw-reset" is not saved to the config file after a reset.
- **240577**—The device may reset under certain traffic pattern conditions.
- **240625**—Memory utilization is high due to DI session leak when SYN protection is enabled.
- **252082**—The FTP session for an IPv4 to IPv6 session connects, but the client's FTP session freezes when FTP get, put, and ls commands are entered.
- **254140**—NFS mount fails due to rpcbind service erroneously being added to the RPC mapping table.
- **255301**—Task CPU becomes high when a TCP socket leak causes loss of SSH management and BGP peering.
- **261379**—[ISG] Session may not age normally if the first fin packet is sent quickly after syn-ack packet.
- **265647**—[NetScreen-50] Device failed due to the maximum task number being too low.
- **266875**—Interface MAC did not change correctly when the VSI interface was assigned to the management zone.
- **269121**—GRE keep alive is dropped when the recursion control bit is set.
- **269922**—With IPv6, an incorrect ICMP message is generated when the policy is configured with action reject.
- **270600**—[UAC] Device failed due to policy push from IC without role name.
- **271025**—Memory allocated while checking the Certificate Revocation List (CRL) is not released properly once the check is complete.
- **271349**—With a low-quality connection, PPPoE may stop responding during negotiation.
- **273021**—The connection between the firewall and the external Surfcontrol server was lost randomly several times a day.
- **273879**—Authentication entries in a pending or fail state are not cleared.
- **276077**—Non-RPC MS Exchange traffic is dropped due to incorrect timeout.
- **281722**—A device reset occurred when running "debug ike" and "unset console dbuf".
- **282781**—High task CPU utilization occurs when CTRL+C is typed while displaying traffic logs in a CLI session.
- **283348**—A device running Antivirus, URL Filtering, or VoIP does not function due to an unexpected packet type.
- **283355**—The "Unsupported command - set interface vlan1 nat" message is displayed during startup.

- **285252**—When the traffic shaping is enabled, the MAC address is shifted on the sub interfaces.
- **288625**—A policy modification via Network Security Manager may cause a device reset.
- **288649**—[ISG, NetScreen-5000] Internal buffer leak causes some traffic drop.
- **288938**—The backup interface in a redundant interface setup is erroneously forwarding packets and causes duplicate packets to be sent.
- **289413**—WLAN LEDs are turned off when all wireless interfaces are shut down.
- **289435**—[SSG 140] In transparent mode, the device may not pass through traffic when a host moves from one interface to another interface in the same zone.
- **289724**—SIP calls are not cleaned up properly when the transaction timer expires and results in operation failure.
- **290478**—[NetScreen-5000, ISG 1000/2000] Packet is dropped due to internal congestion control mechanism.
- **296079**—The firewall drops TALK packets (UDP: 517/518) with an application error.
- **296850**—RTSP media flow is disconnected after about a minute.
- **299424**—With FTP-pathname user-defined signatures, the device does not check the filename in FTP out and get commands.
- **302271**—Failed to create multicast session once it timed out due to a down interface.
- **302382**—In certain conditions, the firewall may reset if a session incorrectly references a MAC address without route information.

Performance

- **219454**—Packet drops occurred when the traffic shaping is enabled on policies between the custom L2 zone and a pre-defined L2 zone.
- **259126**—Packet loss and TCP retransmissions occur when performing file transfers across the T1 WAN interface.
- **266111**—Slow performance with the Web traffic when the URL filtering and the SYN Proxy is enabled.
- **268006**—When the VPN is bound to a loopback interface, and traffic shaping is enabled, the VPN traffic drops.
- **283200**—In certain situations, the device tags packet incorrectly and does not allow the traffic to pass.
- **284276**—VPN performance degrades when the DI is enabled on a policy.

Routing

- **225133**—In some scenarios, the device does not check the group address in a bootstrap packet. As a result, the device does not forward the BSR packets. At the same time, the BSR priority is assigned to invalid value (displayed 255 as -1).

- **235311**—Transmission of the multicast data stream might stop for a while when handling a PIM fragment packet.
- **262604**—The first multicast packets in the flow are dropped.
- **274600**—Multicast group does not join due to a corruption in the multicast policy.
- **274788**—Multicast route through GRE tunnel fails after the GRE routers do a failover.

VPN

- **204717**—Main mode IKE negotiations may fail when peer is identified by DNS address instead of IP address.
- **235321**—IKE Phase 2 renegotiates before the Phase 2 lifetime expires.
- **254631**—VPN fails after concurrent rekeys.
- **279789**—In some network topologies, VPN monitoring may bring the VPN tunnel down.
- **280101**—Dial-Up VPN traffic was dropped due to a change to the IP address on the dialup client.
- **285748**—[NetScreen-5000] IPSec pass-through packets are being dropped when the device is in transparent mode.
- **286723**—VPN negotiation with enabled Xauth the Phase 2 SA is removed incorrectly.
- **287368**—IP configuration from RADIUS such as the DNS server setting may not be configured properly to the Xauth client.

VOIP/H323

- **229190**—The device may fail when the SIP "content-length" parsing is not properly handled.
- **274300** —The event log contains the message, "Can't allocate memory for SCCP call context" due to the timing between session age-out and call completion.
- **281460**—Video does not work properly when using MIP or VIP.
- **288193**—Under certain conditions, the device may reset when processing pinhole for SIP traffic.

WebUI

- **227316**—Unable to configure DHCP on an interface from a trustee admin user via the WebUI.
- **266100**—WebUI displays the message, "More than one physical interface in zone V1-Trust". WebUI error appears when binding multiple interfaces to a Layer 2 zone.
- **272946**—Using the WebUI, an IKE gateway on a device in transparent mode cannot be created.
- **276288**—When using the WebUI, configuring an NSRP cluster ID with a value over 63 displays an incorrect error message.

- **281160**—Editing or cloning a policy with traffic shaping enabled generates an error.
- **299090**—In the WebUI, the PCMCIA option for log settings is incorrectly shown as option USB. The PCMCIA option for log setting configured by the CLI (Command Line Interface) is not displayed correctly in the WebUI.

Addressed Issues from ScreenOS 5.4.0r10

The following major bugs have been fixed in this release:

Administration

- **215340**—Some log entries are not formatted properly in the WebTrend output.
- **223139**—Task CPU becomes high when executing some CLI commands with a large configuration, which triggers high overall CPU utilization, and reaches the alarm threshold.
- **224423**—If a timeout is configured in one GTP object, this timeout is used for all GTP objects.

Antivirus

- **226520**—Login banner was not being displayed when logging in via Putty.
- **237473**—Large iso files cannot be downloaded from certain Web sites when the AV keep-alive option is set.
- **237639**—Admin authentication to the device WebUI via Radius fails if the username is 31 characters.
- **237846**—A POP3 connection to a POP3 server was reset after enabling AV.
- **241401**—Device failed after deleting a VSYS.
- **261597**—[NetScreen-5GT] Unable to set interface ethernet2 to the Null zone.
- **267372**—The SNMP trap (OID) of the interface status is not correct.

DHCP

- **236408**—Device does not send DHCPREQUEST message via broadcast on T2 time when acting as DHCP client.

DNS

- **240535**—PPPoA learned DNS values overwrite the local DNS settings of the firewall, regardless of preference setting.

GPRS

- **259128**—With GTP inspection enabled, CreatePdpRequest packets could be dropped because the firewall ran out of available GTP paths.

HA & NSRP

- **220773**—After merging configurations via TFTP to the primary device, some of the configuration fails to synchronize to the backup device, resulting in partial configuration loss.
- **236524**—The NSRP backup device in transparent mode incorrectly forwards SNMP requests sent to its manage-ip, and treats traffic as through-traffic instead of self-traffic, which causes the corresponding switch MAC address to flap.
- **238578**—Non-VSD sessions in an Active/Active NSRP configuration incorrectly synchronize between cluster members if the session's egress subinterface differs between cluster members.
- **239624**—Ping packets with a large packets size may be dropped in an NSRP failover.
- **251797**—In certain conditions, when a policy is deleted from the primary device, it does not sync to the backup device.
- **258684**—The tcp/udp/icmp sessions were not cleared on the backup device in transparent mode. Also, the "set nsrp rto-mirror session ageout-ack" command was not functioning correctly, resulting in sessions on the backup not being cleared.
- **259736**—When an AES algorithm or AH protocol is used, the backup firewall fails to read the correct SA sequence number from the primary firewall, causing a VPN issue after a device failover.
- **260760**—[SSG 5] NSRP failover not working properly when both NSRP interfaces and a secondary path are enabled.
- **262533**—[SSG 140] Alarm LED on the device was not displaying correctly when an NSRP failover event occurred.
- **267734**—The primary ISG does not read the sequence number correctly from the ASIC for AES after failover.

IDP

- **234254**—L2TP negotiation packets could not pass while enabling IDP in a policy.
- **236437**—[ISG 1000/2000] In certain situations, the traffic passing through an inline mode IDP rule may experience excessive delay when other rules are configured for TAP mode IDP.
- **237769**—[ISG 1000/2000] High CPU utilization occurred on a single SM (Security Module) due to uneven session distribution.
- **256820**—QuickTime RTSP streaming video failed when IDP was enabled.

Management

- **203409**—When an SSH or SCP session disconnects from the firewall device, a non-zero value is returned, which causes scripts to fail.
- **212870**—Device may fail due to memory corruption when trying to establish communication to an NSM server.

- **217312**—Updating devices from NSM using supplemental CLIs may cause cluster members to show incorrect status.
- **224382**—Task CPU spikes when the authentication result from the RADIUS server does not arrive on time.
- **226236**—A device was not able to re-establish connection to NSM after a service disruption.
- **227370**—NSM config update failed due to bulk-cli flag not being set.
- **232175**—The device failed when updating the configuration via TFTP.
- **235506**—Device failed when loading NSM configlet.
- **241576**—After an ISRAU, only one GTP tunnel is deleted while the other stays active.
- **252781**—64-bit hardware counters for aggregate interface exceed the 32-bit limit, causing inaccurate results.
- **254755**—Unable to upgrade device via Secure Copy (SCP) using PSCP (Putty SCP).
- **258148**—SNMP reports incorrect ifspeed on the serial interface.
- **258279**—Under certain circumstances, when using duplicated DIP IDs among different virtual systems, the existing mapping entries may be removed from both virtual systems when the DIP pool is removed from one virtual system.
- **259773**—[SSG 140] When doing an SNMP get to the device, an incorrect sysObjectId is returned.
- **260188**—The device is only able to send 400 to 500 logs per second to NSM.
- **264713**—Tunnel ID and hardware SA in an existing session do not update properly after VPN change, which causes traffic to stop.
- **266873**—In the event log, when the number of telnet and ssh connections to a device are higher than its display limitation, the log entries of the telnet-cmd number and ssh-cmd number are incorrectly displayed.
- **269298**—Some invalid commands are removed from the CLI command tree.
- **275106**—New policy may not take effect if managed using NSM and CLI.

NAT

- **250756**—In certain cases, NAT translation for ICMP/ICMPv6 causes the device to restart.
- **255984**—Policy-based NAT is unable to perform NAT to pass through ESP packets.

Other

- **221831**—Debug output using debug tag is not being filtered by 'set ffilter'.
- **223845**—An interface assignment to a zone could not be changed when traffic-shaping was enabled.
- **224782**—The transmit and receive counters on an HA interface between two NSRP peers shows a mismatch, due to an incorrect byte count.
- **226075**—[ISG 1000/2000, NetScreen-5000-8G2] Device sending two ESP packets with the same sequence number.

- **226345**—Configuration of service timeout may affect the corresponding port timeout.
- **226997**—An invalid L2 pointer caused the device to fail.
- **227438**—CTS traffic incorrectly detected as "HTTP:Overflow:Content-Overflow" and dropped.
- **228235**—Spam emails were not tagged properly when the source used the DomainKey Signature.
- **228288**—[ISG 2000] TTL of the first fragmented packets were changed from 254 to 6 when it passed through the device.
- **229924**—Passive FTP fails if FTP client is not RFC compliant.
- **229985**—[SSG 140] In unframe mode, the device sent an idle flag that conflicted with an M7i router.
- **231278**—The device failed when the SNMP zone ID and address object were mismatched.
- **233850**—[NetScreen-5000-MGT2 Series using 5000-2G24FE SPM] In some cases when a device is in transparent mode, packets from 5000-2G24FE SPM are dropped incorrectly.
- **233972**—Excessive ICMP packets causing high CPU.
- **234140**—Debug causes device failure because of malformed TCP packets.
- **234715**—The device may fail under certain conditions when receiving MGCP traffic.
- **234773**—When a cable is not connected to an interface with track-ip configured, the device may restart periodically.
- **236565**—L2TP configured in a VSYS would not work after a restart.
- **236694**—In rare cases, the device may restart due to an invalid interface reference.
- **238369**—A failure could occur in the GTP function when referencing deleted GTP tunnels, which in some circumstances were not deleted by the system.
- **239575**—When both tcp-syn-check is set and IDP is enabled in the policy, the ACK packet of a 3-way handshake is dropped.
- **241107**—When sending RST to tear down the connection, the reason is logged as Close - AGE OUT.
- **241343**—When a user in the Radius system belongs to multiple groups, and the user is authenticated via the firewall to the Radius server, the firewall may restart.
- **251463**—Device failed when a packet with an invalid ALG port number address was being forwarded.
- **252613**—When a second user attempts to authenticate via WebAuth while the first user is still active from the same IP address and the same authentication group, the device keeps sending authentication requests to the RADIUS server.
- **252624**—NSRP DIP debugging messages are being printed to the console even with no debugs enabled.

- **253020**—On occasion, a device failure occurs when the function to match sessions from IPv6 embedded packets tries to access an incorrect memory location.
- **254619**—A MIB file issue occurred when high-availability(15) was removed from the MIB files.
- **256010**—The device outputs a WebTrends log with an improper format.
- **256071**—TCP sessions established through a tunnel interface with GRE are not removed from the session table, even after application termination.
- **256783**—Device failed due to mishandling of null pointer.
- **257095**—The Antispam list would not display in alphabetical order due to a sorting issue.
- **261134**—With 'set arp nat dst' enabled, the device responds to an ARP request, even though the policy is disabled.
- **262448**—The 'exec policy verify' command was not working when empty address groups are used in the policies.
- **262666**—When NTP is enabled, and "set ntp server src-interface" is used, NTP communication cannot be checked in the policy when the traffic is sent out to an interface other than the one specified in the command.
- **263019**—ARP entry to a non NSRP management zone causes track IP failure after failover in transparent mode.
- **265230**—[SSG 140] The alarm LED on the device incorrectly displays as amber, instead of red, when an attack was detected.
- **265446**—SQL data session times out incorrectly; only half of the service timeout is used.
- **266244**—The IPv6 network advertisement solicitation flag was set incorrectly.
- **267370**—When generating a syslog message, the source port and destination port are incorrectly interpreted from the event log.
- **279652**—In certain conditions, the incorrect policy may be applied to the flow when configured via NSM.

Performance

- **221953**—Access to web sites with multimedia (flash, movie trailers) is slow when Websense is enabled.
- **224073**—[ISG 1000] Packets with 1514 bytes were being fragmented after passing through the device in transparent mode.
- **234153**—High flow CPU utilization caused by packet looping between CPU and ASIC.
- **252920**—The device may experience high CPU utilization in certain conditions.

Routing

- **225134**—When gateway tracking routes are configured, the device may restart while processing traffic that uses the gateway tracked route.

- **228200**—An alternate route could not be added to the routing table and be active after a tunnel failure. This issue will occur when using the "set interface tunnel_name protocol rip demand-circuit" command.
- **235160**—IPv6 routing suddenly fails due to an exception on one of the PPUs.
- **240158**—The device may fail when one IGMP router interface proxies more than one host interface.
- **269341**—IGMP Join occurs 10 seconds after a unicast route has changed.
- **227948**—When OSPF is configured with Reduce flooding, a rare condition of network changes can cause an incorrect value of "LSAs with no DC-option" counter, resulting in continuous purging of OSPF LSAs.

Security

- **250519**—In some environments, packets are dropped due to the behavior of MAC lookup in a flow process.

VPN

- **255512**—The command ‘unset ike policy-checking’ only applied per device, not per VPN.

VOIP/H323

- **226994**—If both the IDP module and the SCCP ALG are active, IP phones were unable to register using SCCP.
- **256706**—The device was not doing routing and policy lookup for IP addresses with unknown contact bindings from the SIP server.
- **264625**—[ISG 1000/2000] SCCP ALG logging messages in the event log, after the ALG was disabled.

WebUI

- **220659**—The WebUI Java menu had an incorrect link for the ALG Configuration page causing a "404 page not found" error.
- **228482**—Multicast Routing menu is not displayed inside vsys.
- **235599**—It is possible to erroneously configure a VIP that is the same as Untrust for http (port 80).
- **239316**—When editing an aggregate interface (next to Traffic Bandwidth), "Memmbers" is used instead of "Members."
- **239748**—[NetScreen-5200-MTG2] Counting configured on a policy incorrectly shows a drastic drop in the bytes/sec counter in the WebUI.
- **256041**—In a particular circumstance, the device may fail when an admin edits a VPN configuration using the WebUI.
- **259582**—When adding Antispam to an existing Antivirus Profile via the WebUI, FTP session disconnects occur and result in abnormal behavior of FTP commands (ls, dir).
- **262652**—Retrieve subscription did not work via the GUI.

- **265334**—From the WebUI, if a RIP summary route is set to a metric of 1, it does not get written to the config.
- **266871**—Custom RPC service is deleted from the policy when that policy is edited.
- **268659**—Adding redundant interface or redundant subinterface through the WebUI succeeds, but the WebUI incorrectly produces an error.

Addressed Issues from ScreenOS 5.4.0r9

The following major bugs have been fixed in this release:

Administration

- **233016**—Dropped traffic from the Self MGT zone was not being logged for IPv6 packets.
- **234164**—[SSG 500] The "clear counter all" command did not clear the 64-bit hardware counters.
- **229935**—The "set pak-poll" command appears and disappears frequently in the configuration file.

DHCP

- **257662**—User cannot set a negative integer value for DHCP custom option 2.

HA & NSRP

- **227050**—In an NSRP failover, the state of the XFP gigabit interface is DOWN, but the software shows it as UP.
- **229480**—Unable to manage backup device in NSRP cluster via manage-ip.
- **235941**—NSRP configurations out of sync due to the different ordering of AV parameters between primary and backup devices.
- **251044**—The CLI incorrectly displays the supported NSRP cluster ID range of 1 - 63.
- **237697**—An NSRP cluster is out of sync due to the udp-flood dest-ip setting.
- **253075**—FTP traffic stopped when an NSRP failover occurred.
- **255920**—Sessions on the backup device in an NSRP cluster could not be closed properly when 'nsrp session ageout-ack' was enabled.

IDP

- **252958**—Login attempts with FTP brute force signatures were erroneously being logged as accepted.

Management

- **232075**—Time binding attacks are not reporting logs to the NSM server.
- **233109**—User auth sessions are not being cleared, despite being logged off for an extended time.
- **235853**—Some NSM configurations may cause the device to fail, due to task mismatch.
- **226808**—Under a high-traffic volume condition, the traffic log is not sent to NSM.
- **237505**—The ASIC sector memory space has been increased to allow more policies to be configured.
- **239362**—The BGP Established Time was not shown correctly using SNMP walk.
- **239747**—The syslog message incorrectly shows that the action is deny, but traffic is permitted.
- **240098**—The traffic to a VIP address that is the same as the interface IP gets dropped.
- **250913**—In certain conditions, the firewall incorrectly replaces a global policy with zones other than global.
- **253762**—The NSM agent sends an incorrect MS-RPC UUID service value back to NSM, causing a configuration update issue.
- **252700**—Unsupported "Far End" OIDs were modified so that they return a "no such object" response to an SNMP query.

Other

- **219624**—Window scaling factor not taken into account if TCP sequence checking is enabled.
- **225017**—[SSG 5/20] The device may stop passing traffic due to a link-layer buffer problem.
- **225211**—The ISDN Basic Rate Interface (BRI) does not work correctly with certain ISDN vendors.
- **234233**—Xauth server config is lost after reboot if auth-server name contains a space.
- **234503**—When using 802.1x authentication, the NAS-IP-ADDRESS field becomes 0.0.0.0 when the RADIUS server is on the remote side of a route-based VPN using an unnumbered tunnel interface IP.
- **235560**—[Netscreen-5000-MG2-8G2/2XGE] TCP traffic fails due to improper behavior of syn-cookie (after syn-cookie has been triggered).
- **236768**—Device may issue an ACK in response to a RST packet.
- **252224**—The wireless client reports a different link speed than what the device reports.

- **257753**—SQL connection fails due to RM group created too early.

Performance

- **221019**—SYN cookie doesn't work properly on aggregate interfaces, which causes a high CPU condition
- **233167**—[ISG, NetScreen-5000] High CPU utilization in flow occurs when L2TP traffic passes through the ASIC device.
- **254924**—In some cases, when a packet loops between two devices, the TTL is not decreased accordingly, which causes high CPU utilization.

Routing

- **229973** —Under some conditions, the device fails due to an inconsistency between the routing table and the IP Classification table, resulting in an invalid route.
- **238162**—When using src-interface for some services, the route lookup is done in the default virtual router (VR) instead of the src-interface VR.
- **239971**—[ISG 1000, ISG 2000, NetScreen-5000] IPv6 traffic does not pass on ASIC platforms when in transparent mode.
- **239997**—Deleting an access list entry using the CLI does not check if there is an address and netmask match.
- **240429**—In some cases, multiple multicast routes for the same group are added to the routing table, causing the multicast-route limit to be reached, and no more multicast routes can be added.
- **255472**—In transparent mode, OSPF pass-through sessions time out after 1 minute.

Security

- **230716**—The source and destination session limit drops packets when "generate alarms without dropping packet" is enabled.
- **233964**—A critical parsing vulnerability (CVE-2003-0543 and CVE-2003-0544) was reported in OpenSSL ASN.1.
- **241420**—Using MS-RPC-EPM or SUN-RPC-PORTMAPPER in a service group on a deny policy caused the firewall to not install the ASIC rule properly.

VOIP/H323

- **227486**—In transparent mode, h.323 communication failed due to inability to execute the MAC cache operation.
- **231134**—The system failed in the SIP ALG functions.
- **255168**—With the ALG enabled, the pre-marked DSCP values for H.323 traffic is not retained when passing through the device.

VPN

- **221350**—[NetScreen-5000-MGT2] UDP fragmented packets are dropped in a site-to-site VPN tunnel.
- **226681**—A memory allocation error occurred when trying to establish a dial-up VPN using certificates.

WebUI

- **232471**—The DSCP settings on a policy are lost when the policy is modified.
- **235245**—The configuration shows route preference when configuring via WebUI, but no route preference appears after configuring via the CLI.
- **250313**—When using the WebUI for MIP grouping in a policy, the MIP object can be deleted.

Addressed Issue from ScreenOS 5.4.0r8a

The following major bug has been fixed in this release:

IDP

- **265110—**[ISG 1000/2000 with IDP] The IDP detector released with ScreenOS 5.4.0r8 may cause issues with the IDP Security Module. To resolve this issue, and to improve coverage and accuracy for HTTP, SIP, NFS, and SNMP protocols, upgrade to 5.4.0r8a, and update to the latest detector version.

  Note: If you are upgrading to 5.4.0r8a from 5.4.0r8 firmware, perform the following steps:

  1. Check the detector version on 5.4.0r8 to see if it is 3.1.101390. To check the detector version run the command **get system** and check the value of **detector.so**.

  2. If the detector is version 3.1.101390 after upgrading the firmware to r8a, run the command **del file flash:detector.so** to delete the existing detector from flash memory.

  3. Run the command **reset** to reset the firewall.

  4. After the firewall restarts, immediately push the latest detector from NSM.

If you are already running detector version 3.1.103797 on r8 then simply upgrade the firewall to r8a and restart.

Addressed Issues from ScreenOS 5.4.0r8

The following major bugs have been fixed in this release:

Administration

- **227374—**[SSG 500] Firewall may fail to start with the correct serial number, resulting in the license keys not being properly loaded.

Antivirus

- **226847—**AV drops SMTP traffic when the SMTP server uses the BDAT command.

HA & NSRP

- **190653—**Local management options on the backup device in an NSRP Active/Passive cluster are overwritten by the primary device after NSRP sync.
- **226959—**[SSG 520M] The ALARM LED always shows RED when NSRP is configured on the firewall. There is no effect on the firewall's performance.
- **223728—**Packet drops occurred after an NSRP failover and failback.
- **227366—**FTP traffic is lost after an NSRP failover occurs.
- **231510—**Enabling NSRP secondary path via the WebUI does not get saved to flash.
- **234080—**NSRP configuration was out of sync because the command lines in the config were in a different order.

Management

- **218452—**Certificate fails to renew CRL if the CA server's publication interval is less than 12 hours.
- **224163—**The SNMP packet 64-bit counter values are not reporting correctly.
- **224421—**The 'set ike p1-max-dialgrp-session' command does not work properly because the concurrent p1 dialgrp sessions number is counted incorrectly.
- **227364—**Traffic log information is changed when adding or removing more specific policies.
- **227488—**Issuing the "get tech" command via telnet or SSH causes task CPU to spin in a loop, creating high task CPU.
- **229295—**If GTP inspection was used, GTP UpdPdpRequest packets failed the sanity check and were dropped if the TEID was zero.
- **234363—**[ISG 1000/2000, NetScreen-5000] Large policy installs via NSM to ASIC platforms may cause OSPF adjacencies to drop.

- **234463—**With certain protocols, e.g. telnet and ftp, the first pass through connection could stop responding when using the policy pass-through auth and external auth server.
- **234662—**Device failed when trying to update a policy configuration using NSM.
- **234722—**In NSM, Active Sessions statistics showed IP addresses being reversed.
- **235630—**High CPU load during NSM policy update might cause other processes to fail temporarily.
- **235940—**Unsetting a custom syn-flood destination threshold did not go back to the default value.
- **236281—**When downgrading from 6.0 to 5.4, the following console message occurs: "The device is storing the firmware into reserved flash sectors". It is important to not power off the device during this operation; doing so could result in a loss of firmware.
- **238777—**When deleting 2000 policies from an ISG 2000 using NSM, the update will fail after about 130 policies are removed.

Other

- **225869—**[ISG 2000] A failure occurred because of an array error in a route table lookup.
- **232036—**64-bit out bytes and out ucast counters are incorrect for the serial interface.
- **235905—**When using MLPPP or T3, the serial interface encounters timing slips.
- **237811—**Traffic fails to pass when using the NAT interface, due to DIP allocation failure.
- **238612—**Packet drop occurs due to a DIP allocation failure.

Routing

- **214163—**ASIC is overburdened with processing RIP packets when a large number of RIP tunnels are being built up during the failover.
- **231865—**TCP traffic cannot pass when there are no ARP entries in the ARP table. The TCP traffic will succeed when ARP entries exist.
- **235835—**Static routes redistributed into RIP updates with the wrong next-hop.
- **236497—**In some cases, the device was not clearing out redistributed routes from the RIP database, even though the sending routing protocol has been disabled.

VOIP/H323

- **223896—**A SIP auth request is dropped when MIP is configured on a SIP Proxy.
- **230195—**The firewall failed unattended, due to SIP ALG.

VPN

- **230340—**A VPN with a VLAN tag configured in a vsys, after a VPN rekey, caused problems with VPN traffic from a remote peer that used an old key, which fails to match the correct hardware session.

WebUI

- **225149—**WebUI management via HTTPS (SSL) fails unexpectedly.

Addressed Issues from ScreenOS 5.4.0r7

The following major bugs have been fixed in this release:

Administration

- **225013—**The types filed in the traffic log, byte_recv and byte_sent, should be displayed as an unsigned value in the log, but when something larger than 2147483647 occurred it printed as a negative value.
- **226764—**When configuring an authentication server for SSID, the name of the authentication server is saved without quotes. If the name contains spaces, the corresponding command line fails after the device is reset.
- **227726—**Time stamp in event log/traffic log changes to Year 2035 incorrectly.

Antivirus

- **227667—**Tagged VLAN traffic may be dropped when AV is enabled.

DNS

- **224598—**In DNS, the policy doesn't refresh the Address Book entry with the domain name when the IP changes so the policy still uses the old IP address.
- **231728—**[SSG 140] DNS information from PPPoE does not update to firewall's DNS host setting.

HA & NSRP

- **218161—**It was not possible to use an aggregate interface as a secondary-path for NSRP and the interface was not available as a choice when using the CLI.

- **222057—**[NetScreen 5000] A memory leak can cause an NSRP Split Brain.

- **223776—**The backup firewall sends frames with a Virtual MAC address after restart.

- **223900—**The RTSP ALG generated many sess_ch messages on the primary device in a cluster, which gets synced to backup. This caused high CPU on the backup firewall.

- **224084—**When an administrator is authenticated via Radius in a clustered environment, some commands may not be synchronized via NSRP.

- **224721—**The primary config will be overridden by the config of the backup, including manage-ip and hostname.

- **225274—**The console on the backup device in an NSRP cluster showed the message “###Port-xlate dip out", which was due to a failure of session sync.

IDP

- **225502—**[ISG with IDP] The IDP drops legitimate HTTP traffic for very large HTTP downloads.

Management

- **223336—**Event log entries get lost when NSM connectivity is lost then restored.

- **208408—**WebUI shows "Deny" when FTP-PUT/GET in the service group, however traffic is still passing.

- **222603—**When a root system administrator is authenticated via RADIUS, it's not possible to set the admin password for a vsys.

- **224786—**The scio subs status command does not display CPU usage.

- **225131—**The device may reset while running L2tp debug.

- **225140—**With a specific deny policy in place for syslog traffic, syslog traffic can still be allowed through the firewall at times.

- **226998—**WebTrends traffic log message is missing double quote for the firewall name.

- **227315—**After adding 10/100/1000TX interfaces to an aggregate interface, the counter of the aggregate interface is wrong.

- **227607—**Include Session ID to be displayed in the policy log.

- **227963—**Black/White list entries cannot be displayed/edited using the WebUI.

Other

- **216913—**High task CPU causes transmits being dropped.

- **221755 (cs12527)—**IP spoofing is incorrectly detected when an interface bound to an IP spoofing enabled zone is still initializing due to firewall restart or interface flap.

- **226344—**The device incorrectly identifies DHCP relay packets as IP Spoofing and drops the packets.

- **226765—**[ISG 2000] The default value of max number for TCP ooo segment is set to 256.

- **227229—**The devices maintaining hardware sessions may drop packets for UDP based applications, if the frequency of the traffic and the time-out is configured to be the same.

- **227670—**The FTP connection fails under rare circumstance when an FTP retransmission packet is received.

- **228350—**Some resources were going into a dead loop, causing the device to fail.

- **231303—**Service timeout may become incorrect when predefined service is overloaded by custom service.

Performance

- **225627—**With URL filtering enabled, firewall randomly generates high amounts of TCP keep alive traffic to hosts browsing the internet behind the trust interface. This causes high CPU on the intermediate router.
- **225930—**On lower-end devices with certain configurations, such as those with multiple AV policies, the device could experience high CPU.

Routing

- **224949—**OSPF neighbor may get stuck in Ex-start state when Opaque LSA’s are received.
- **226284—**Certain BGP prefix routes were lost when advertising.

VOIP/H323

- **217205—**The SIP stack was not able to properly handle messages that contained the "#" character in the user name part of the URI or phone extension.
- **222866—**Certain MGCP traffic types can cause the device to reset.
- **223138—**The device would reset with certain MGCP configuration changes.
- **226740—**Timed out sessions were not being cleared from the session table since RTSP ALG returned an incorrect value.
- **233533—**RTSP ALG sessions timed out, but did not get removed from the session table.

VPN

- **223729—**PPP always referenced the L2TP Tunnel auth setting for query config. This resulted in "set l2tp auth server query-config" as a valid command; however "set l2tp default auth server query-config" fails to work.
- **225567—**[NetScreen 50] Cannot establish L2tp tunnel with a Juniper E320.

WebUI

- **221670—**When saving traffic logs using the WebUI, the saved file is empty.
- **224461—**In the WebUI there was an issue with the configuration of serial interfaces. The error message "unknown keyword" would appear. W/A: Configure using the CLI.
- **227556—**The device may restart when upgrading software via the WebUI.
- **227729—**System may fail when doing a save self log from the WebUI.

Addressed Issues from ScreenOS 5.4.0r6

The following major bugs have been fixed in this release:

Administration

- **222606 (cs12730)—**When entering a vsys via telnet, an incorrect log entry is generated.
- **223571 (cs13036)—**[NetScreen 5000] Device may show strange interface counter values.
- **225871 (cs13677)—**A duplicate redundant interface status changes reported when a member of a redundant interface was changed to up. ScreenOS updated the redundant interface status again, which caused the duplicate message.
- **226225 (cs13738)—**Due to incorrect internal indexing, deletion of a multicast policy may fail with the error message: "unset multicast policy error, entry not found!". W/A: Reset the device and delete the multicast policy.

Antivirus

- **225135 (cs13488)—**Sometimes HTTP traffic via the proxy server will be slowed down or dropped when AV is enable.

CLI

- **221902 (cs12566)—**Read-only admin could not issue "get" commands.

HA & NSRP

- **221071 (cs12353)—**Local config is missing in the NSRP backup after NSRP synchronizes configuration and the device resets.
- **223996 (cs13176)—**The get nsrp track-ip show command displays incorrect information if track-ip with arp and with a non-default interval.
- **224082 (cs13209)—**With NSRP track IP, if the interface is brought down then up, the NSRP member cannot fall back to the master or backup mode.

- **224714 (cs13395)—**Using the command 'exec nsrp vsd-group 0 mode backup' caused the upgraded cluster member to fail.

- **226514 (cs13786)—**[ISG 2000] The primary device in a cluster failed because of the Watch Dog timer.

IDP

- **222054 (cs12603)—**[ISG 1000/2000] Devices with an IDP blade and with an IDP policy, CRC errors appeared in the switch interface that directly connects to the ISG 1000/2000 device when traffic passed through.

Management

- **208197 (cs09776)—**The firewall stopped sending mail alerts for traffic and event alarms because it has referred the wrong record.
- **224086 (cs13213)—**[SSG 550M] Power failure events are not reported from the event log or from the chassis status.
- **224385 (cs13306)—**When TCP Sequence check is enabled on the firewall, certain traffic patterns may cause a device failure.
- **225405 (cs13556)—**Policy push fails on VSYS device when schedule attack DB is enabled.
- **225811 (cs13659)—**High CPU occurred after a policy push from NSM.
- **226338 (cs13768)—**A device failure occurred under certain circumstances when managing the box using SSHv1 and abruptly interrupting the connection.

Other

- **223635 (cs13058)—**Firewall may reset due to the creation of invalid software session ID.
- **223998 (cs13178)—**The device may fail during debugs if an invalid URL request is made.
- **224099 (cs13226)—**Firewall may reset due to ARP processing in the flow.
- **224456 (cs13328)—**The DIP resource is not released if the session is initiated from the server side.
- **224565 (cs13350)—**After adding a UAC device in the network, the firewall reset.
- **225068 (cs13473)—**EAP users not authenticated through Wireless using 802.1x.
- **226296 (cs13765)—**GTP MMS traffic was dropped because the create_PDP request/response was not expected to modify the exiting tunnel with a new SGSN address for the GTP-U plane.
- **230858—**[NetScreen 5000] Device failed to start with 5.4r5 if a CF card was inserted.

Routing

- **225067 (cs13472)—**Rapid OSPF Adjacency changes caused a memory leak and caused a device reset.

Security

- **221225 (cs12388)—**When DI is enabled on a policy and there is asynchronous traffic flow through an Active/Active cluster, NSRP data-forwarding traffic is denied.
- **225457 (cs13574)—**An FTP connection was not completing the login phase when AV was enabled.
- **225926 (cs13684)—**The device may reset when using URL filtering causing an out of memory situation.

VOIP/H323

- **225066 (cs13471)—**H.323 was not working in a MIP policy based NAT.

VPN

- **220344 (cs12203)—**IKE P1 continued to use the old IP address after dynamic-dns, NAT-T peer had changed IP.
- **221601 (cs12484)—**In a hub and spoke VPN, ping with size 1704 bytes from spoke to spoke sites, after decryption in a NetScreen 5200 (Hub site), NS fails to send 2nd IP Fragment with IP length equal to 1500 bytes but is okay with 1499bytes.
- **222721 (cs12752)—**Under certain circumstances, for example, when editing VPN policies, the proxy-id of dial-up VPNs could be incorrectly reset to a non proper value. This caused the IKE key renewal to fail then VPN clients, such as NetScreen-Remote, would prompt indefinitely for new authentication.

WebUI

- **220039 (cs12131)—**When configuring HTTP options from the WebUI in "Screening > DI Service Limits > HTTP" many duplicate entries in the configuration file are being added. The new changes are not taking effect and will not alert or block.
- **225076 (cs13483)—**Enabling authentication on a policy does not display the auth icon if server type is "default". The policy works as configured and is shown properly in the CLI. Only the display of the icon on the policy GUI is incorrect.
- **229794—**[NetScreen-5GT-WiFi] Wireless SSID settings could not be viewed or edited in the WebUI. **W/A:** Use the CLI to edit SSID settings.

Addressed Issues from ScreenOS 5.4.0r5

The following major bugs have been fixed in this release:

Administration

- **cs10996—**The save config to tftp CLI command did not save the set alarm threshold CPU CLI command to the config file.
- **cs13187—**On SSG platforms, the syslog traffic log may report a wrong port number.
- **cs11896—**In some cases, during an IKE P1 initiation event, a log/syslog is not generated.
- **cs12613—**The SNMP counter does not update until "get count stat" is issued from the CLI.

Antivirus

- **cs12445—**In certain situations, POP3 AV inspection may drop traffic.

CLI

- **cs12128—**[ISG 2000] NSRP cluster primary device failed when pasting commands via the CLI.
- **cs11617—**[NetScreen-5GT] In the default configuration, a blank line could have appeared after the 'set hostname' CLI command.

DHCP

- **cs12646—**Device changes the DHCP relay agent IP when it is configured as a DHCP relay.
- **cs12385—**When using bgroups and DHCP, an update of DNS does not always work properly.
- **cs13154—**In certain environments where DHCP packets need to traverse the firewall in transparent mode, the device may fail.

HA & NSRP

- **cs12605—**In an NSRP configuration, GTP messages could be misinterpreted, causing the device to reset.
- **cs12550—**On the ISG platform, the backup firewall in NSRP cluster may restart.

- **cs12186—**The backup firewall in a transparent (L2) NSRP cluster is unable to ping the HSRP VIP address.

IDP

- **cs12584—**[SSG 520/550] The wrong attack-db version may be reported.
- **cs12722—**Under certain conditions, "invalid ip action mode 1" is seen in the event log and console.
- **cs12223—**On SSG platforms, updates to attacks.sig on the primary are not updated on the backup via NSRP HA.

Management

- **cs12055—**Unable to manage the device via http using the tunnel interface manage-ip.
- **cs12364—**In the WebUI, "Reports > System Log > Self" showed the wrong port numbers.
- **cs11688—**[ISG 2000] The interface statistics displayed the “out ucast” as a value of 2^64; this value does not increase or change.
- **cs13114—**Using SSH V2 to the firewall times out, even when admin authentication timeout has been set to 0.
- **cs11794—**Some WebTrend log entries were not formatted properly.
- **cs12287—**[ISG 1000/2000] Device reports very high number of CRC, overrun, and out bytes.
- **cs12684—**Under certain conditions, management to the backup ISG firewall in NSRP cluster fails, except for console access.
- **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.
- **cs09589—**In an NSRP Active-Active environment, the device does not send WebTrend logs when it is configured with the "Use Trust Zone Interface" as the source IP for the VPN option.
- **cs13221—**Could not configure a wireless interface from NSM. Exception on NSM reports "unset interface wireless0/0 shutdown did not get updated to the device."

Other

- **cs11222—**Under certain conditions, the "FLASH" LED is not illuminated.
- **cs12949—**Device failure occurred on the primary firewall in an HA environment within a minute of upgrading both firewalls to 5.4r3. Disabling the HA link stops the failure.
- **cs12567—**When using SecurID, if a user inputs the wrong passcode 3 times, SecurID will prompt for the next code; however, even after entering the correct code on the SecurID token, it fails.

- **cs11061—**Unable to configure PPPoE or PPPoA if the firewall is in transparent (L2) mode.
- **cs12050—**Changing the interface duplex setting did not take effect until there was a change in link status.
- **cs12715—**When using IPV6, passive FTP does not work correctly.
- **cs12682—**When modifying a multi-cell policy, with custom timeout service object, all of the matching sessions were removed from the session table.
- **cs12983—**An ISG firewall stopped passing traffic when URL-filter and IDP were used.
- **cs12183—**When configuring NTP through the WebUI, if the NTP backup1 and backup2 IP addresses were not configured, an IP address value of 0.0.0.0 was automatically entered when “apply” was selected.
- **cs11840—**Active FTP data session failed if syn-flood was triggered in a zone with ECMP routing.
- **cs12231—**Some pages did not load when Web Filtering was enabled.
- **cs12332—**When in transparent mode (L2), IPv6 did not pass through the device.
- **cs12440—**Traffic shaping on MLPPP dropped all traffic.
- **cs13083—**When using the GTP feature in ScreenOS, the PDP Request filtering checks the Access Point Name in the Information Element, which is sometimes not supplied.

Performance

- **cs10867—**[NetScreen-5GT] An interface set to 10mb/full fixed was found to be operating in half-duplex mode.
- **cs12838—**During heavy traffic, SSG devices showed high CPU (99%) usage and the following warning message was displayed on the console: "WARNING: insertion in tree failed when free a port. It's Possible that the Node Pool was exhausted!"

Routing

- **cs12505—**Configuring PBR Action-Group for 'next-hop only' option does not work from the WebUI.
- **cs12307—**When configured for OSPF, routes across a GRE tunnel appeared inactive in the route table.
- **cs12818—**The primary firewall stopped advertising BGP routes after a physical interface was found to be going up and down continuously.
- **cs12501—**When OSPF cost value was above the limit, the route was incorrect in the route table.
- **cs11355—**[ISG 1000/2000] The devices did not terminate a TCP session immediately when a client sends an RST packet with an incorrect sequence number, and 'set flow check tcp-rst-sequence' and 'set flow tcp-rst-invalid-session' commands are enabled.

Security

- **cs11679—**[SSG 500] DI attack detection stopped after several days.
- **cs12630—**Default SCREEN options for custom zones starting with "untrust" is not consistent.

VLAN

- **cs12453—**Traffic shaping fails to forward packets on redundant sub-interfaces.
- **cs13057—**Cannot create sub-interfaces in two different zones and VR’s with the same IP address.

VOIP/H323

- **cs12427—**The firewall did not correctly NAT an H.245 IP address.
- **cs11767—**In some cases, RTSP packets are dropped inadvertently.
- **cs12737—**CallProceeding messages are not decoded correctly, causing H.323 VoIP calls to fail.

VPN

- **cs12441—**In some cases when using NSRP, the modem password is not synchronized properly.
- **cs12817—**Under certain situations, VPN monitoring with source interface and destination IP would fail to bring up the VPN tunnel.
- **cs12433—**When a device is added to NSM and the connection from the device to the NSM server is over a VPN, the device fails to connect the first time. On the NSM server, the status is "Waiting for first connect" and on the device "get nsm" displays the status as "Connected & UP".
- **cs11413—**A memory leak occurred on an SSG 500 due to PKI online CRL.
- **cs12636—**VPN monitor status in the event log did not appear upon the first successful connection.
- **cs12156—**[SSG 5] VPN to a third party VPN device had problems with Phase 1 re-key.
- **cs12968—**The 'get sa' command shows A/I on the backup firewall in NSRP lite, I/I expected.

Web UI

- **cs12643—**Custom URL for Web Filtering via WebUI had a 50 character limit.
- **cs12558—**The eBGP and iBGP route preference would swap when saving VR settings in the WebUI.

- **cs12755—**In an NSRP environment, you could not use the WebUI to assign priority when you create a second redundant interface.
- **cs12766—**Traffic log on SSG platforms showed random ports in the WebUI.
- **cs13184—**In some cases, the firewall restarts when a sub-interface is being created on a redundant interface via the WebUI.
- **cs12792—**When clicking on a policy with DI configured via the WebUI, then clicking cancel, the DI configuration is erased.
- **cs12804—**Creating a new address object in the WebUI resulted in a subnet mask set to "/0", which is not valid.
- **cs12937—**When a single quote (') is used in the user group name the remove key is not available from the WebUI.

Addressed Issues from 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 startup, 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 restart 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 restart.
- **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 boot loop 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 restart. This will cause the configuration of the device to be lost.

- **cs07583—**Incorrect handling of MSRPC messages occasionally caused a boot loop 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 boot loop 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 sub interfaces 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—**[NetScreen-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 boot loop 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 restart.
- **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.

WebUI

- **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 restarts 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.

- **ISG and NetScreen 5000 series Multicast Hardware Support**—Multicast sessions can be handled by the ASIC only if there is a single output interface per virtual router. The mcast group address can be pushed to ASIC so frames are forwarded in hardware. To use this feature run the set/unset flow multicast install-hw-session command.
- **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 5000-M	NetScreen-5200 using 5000-M2	NetScreen-5400 using 5000-M	NetScreen-5400 using 5000-M2
4.0x	500	N/A	500	N/A
5.0x	500	500	500	500
5.1x	500	N/A	500	N/A
5.2x	500	500	500	500
5.3x	500	500	100	500
5.4.x	500	500	100	500

- **Limitations of 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.
- **DI Subscription Service**—For customers that have purchased the Deep Inspection (DI) subscription service on NetScreen-5XT and NetScreen-5GT devices with ScreenOS 5.3 or later, we provide signature updates which include “critical” level signatures only.
- **AV Subscription Service**—For customers that have purchased the Antivirus (AV) subscription service on NetScreen-5GT devices, we do not support extended-scanning with Kaspersky. Customers using Trend Micro on

NetScreen-5GT receive only “in-the-wild” signatures via the pattern file update.

- **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 5.4.0r12

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

- **255412**—Unable to upgrade bootloader remotely.
- **387163**—Admin login fails when crossing vsys.
- **403134**—RFC MIB for ifAliasm FW returns a " " (empty space character), instead of a NULL string.

Management

- **234379**—In Transparent mode, cross VSYS management traffic is allowed, even though there is no policy to allow this traffic.
- **391755**—Device loses connectivity to NSM for every 8 minutes.

Other

- **263850**—The data packets are lost when the FTP ALG did not create the child sessions correctly for the cross-vsys flows.
- **285992**—The output of the "exec nsrp sync global-config save" command is not sent to the debug buffer (get db stream).
- **290501**—The “set core-dump” command freeze if there is no enough space on the Compact Flash (CF) when the CF card is formatted.
- **387143**—The alarm LED is cleared automatically without issuing the "clear led alarm" command.
- **401773**—ISG chassis might have problems detecting some of the mini-GBIC interface status when under heavy traffic.

Performance

- **405001**—UDP fragments are dropped when the PPU is stuck.

Routing

- **268031**—When an internal functions fails, the number of OSPF routes reduces unexpectedly.
- **300214**—When OSPF LSA database is large and firewall CPU is fairly busy, OSPF adjacency might flap.

VoIP

- **310081**—Device changes remote IP address within SCCP payload, causes a silent listener of an agent's call to fail**.**

VPN

- **303538**—When the physical and tunnel interface are in different zones, VPN monitor reply packets might get dropped across a route-based VPN.

WebUI

- **403443**—Unable to configure Gateway Tracking in the WebUI.

- **405079**—When the software policy search is used, unsetting an object from multi-cell policy causes high CPU and packet loss.

Known Issues from ScreenOS 5.4.0r11

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.

WebUI

- **222872**—Access to the WebUI is very slow when opening the main home page.

Known Issues from ScreenOS 5.4.0r10

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.

Other

- **270342**—In a VSYS environment, ping traffic from the other VSYS to the local interface failed.

Performance

- **267324**—[ISG, NetScreen-5000] Packets are being sent out of order when using aggregate interfaces on ASIC platforms.

Known Issues from ScreenOS 5.4.0r9

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.

Management

- **229923—**The device may inadvertently reset if you direct a browser to the management IP address via WebUI.

Other

- **226768—**The limit-session screen option is enforced even if the alarm-without-drop option is enabled.

Known Issues from ScreenOS 5.4.0r8

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.

None

Known Issues from ScreenOS 5.4.0r7

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.

None

Known Issues from ScreenOS 5.4.0r6

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**.

VOIP/H323

- **217205, 232541 (cs11592)—**The SIP stack was not able to properly handle messages that contained the "#" character in the user name part of the URI or phone extension.

Known Issues from ScreenOS 5.4.0r5

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**.

None

Known Issues from 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

- **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.

HA & NSRP

- **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".

Other

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

- **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.

VOIP/H323

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

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.

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

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

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

HA & NSRP

- **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.

Other

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

Security

- **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.

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

WebUI

- **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.

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.

Management

- **cs11121**—The following system log message is put into the event log, at start up.

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

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

Other

- **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.

Performance

- **cs10105, cs10471**—The bandwidth option on WAN interfaces does not work properly.

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.

WebUI

- **cs11046**—(NetScreen-5000) There is no **Asynchronous VPN** button 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.
- **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.
- **cs08773**—An existing SSH session pauses while a new SSH session is authenticated.
- **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.
- **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.
- **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.

- **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.
- **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.
- **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.
- **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.
- **os62720**—In some cases, the device fails while editing a policy.
- **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 2000) For a device with a high number of policies configured, an optimized tree search must be enabled to avoid performance issues.

  W/A: Use the **set policy swrs** CLI command then restart the device.
- **os63290**—In Transparent mode vsys, when a VLAN interface is unset, the ARP table is not flushed.

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

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

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