# Juniper Networks ScreenOS Release Notes

**Products:** NetScreen Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen-5GT Wireless (ADSL), NetScreen-5GT ADSL, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen500, ISG 1000, ISG 2000, NetScreen-5200, and NetScreen-5400

**Version:** ScreenOS 5.3.0r8

**Release Status:** Rev 01

**Part Number:** 530-021252

**Date:** June 7, 2007

**Contents**

# Version Summary

ScreenOS 5.3.0r8 can be installed on the following products: NetScreen-5XT, NetScreen-5GT Series, NetScreen Hardware Security Client (HSC), NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500, ISG 1000, ISG 2000, and NetScreen-5000 Series security devices.

The ScreenOS 5.3.0r8 release is interoperable with and provides basic support for all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions.

NetScreen-Security Manager, version 2005.2 and earlier, does not support ScreenOS 5.3.0r8.

This release incorporates the following ScreenOS maintenance releases:

- 5.2.0r3b
- 5.1.0r4d
- 5.0.0r11
- 5.0.0-DSLWr10b
- 5.0.0-ISGr10a
- 5.0.0-M2r9b

# Documentation Changes

## *Documentation Changes from 5.3.0r3*

The following information is reflected in ScreenOS 5.3.0r3 documentation.

Changing the route preference with the set vrouter name preference protocol value CLI command does not affect existing routes. This command only affects new corresponding protocol routes. To apply changes to existing routes, you need to delete the routes then add them again. For dynamic routes, you need to disable the protocol and then reenable it or restart the device.

The following correction applies to the Predefined Signature Packs section located in the *Concepts & Examples ScreenOS Reference Guide, Volume 4: Attack Detection and Defense Mechanisms*, Chapter 5: “Deep Inspection.”

**The predefined server-protection signature pack does not include threat coverage for Oracle servers.**

# New Features and Enhancements

The following features and enhancements are new in this release. These features do not affect migration.

**Note:** You must register your product at http://support.juniper.net so that certain ScreenOS features, such as antivirus or deep inspection, can be activated on the device. If you already have an account, enter your user ID and password; if you are a new Juniper Networks customer, create your account first. To register your product, you need the model and serial number of the device. After registering your product, confirm that your device has Internet connectivity. Issue the **exec license-key update** CLI command to make the device connect to the Juniper Networks server to activate the feature.

## *New Features and Enhancements Introduced in ScreenOS 5.3.0r3*

### Service Timeout

To prevent using the wrong service timeout values, the port-based service timeout table lookup is not used when the destination port is overloaded with multiple services with different service timeouts. ScreenOS 5.3.0r3 uses service lookup within the service group based on the destination port to derive the correct service timeout value.

However, to minimize the performance impact due to the costly service lookup within a service group, the port-based service timeout table is still maintained used as a shortcut when service port overlapping is not an issue.

### 5000-M2 Management Module Support

ScreenOS 5.3.0r3 supports the 5000-M2 management module on a NetScreen-5000 Series device.

## *New Features and Enhancements Introduced in ScreenOS 5.3.0r2*

### Antivirus

ScreenOS 5.3.0r2 supports an integrated antivirus (AV) solution on the NetScreen-5GT Series and NetScreen-HSC devices.

In this release of the AV scan engine, you can:

- Configure scanning profiles

  The AV scan engine is enhanced to increase the flexibility and granularity of AV scans. Profile-based scanning allows you to configure a profile to scan traffic and assign the profile to a policy.

- Enable/disable scanning based on application protocol

  The AV scan engine allows you to select the content (FTP, HTTP, IMAP, POP3, or SMTP traffic) to scan. Scan performance can be enhanced due to not scanning certain content.

**Note:** You need to assess the risk and determine the best tradeoff between security and performance.

- Enable/disable scanning based on file extension and content type.

  For example, you can set up a profile that allows scanning of executable files (.exe), but not documentation files (.doc or .pdf).

- Configure decompression layer for specific application protocols.

  In each profile, you can configure different decompression levels for each protocol (HTTP/SMTP/POP3/IMAP/FTP). Based on your network environment, you might specify the number of embedded zips to unpack for each protocol.

- Use the Exclude option to define URL patterns for Webmail scanning

  The internal AV scanner examines specific HTTP webmail patterns only. You can add a pattern for a specific webmail type, so the content is scanned. The patterns for AOL, Yahoo!, and MSN mail services are predefined.

  The optional exclude keyword can be specified if you want to match the pattern other than the specified URL string. For example, use the exclude option to examine for virus patterns in all paths, except in paths containing the matching prefix string.

- Configure e-mail notification to sender/receiver on detected virus and scanning errors

#### *New Juniper-Kaspersky AV Scan Engine*

ScreenOS 5.3.0r2 supports either of two scan engines. In addition to supporting the existing Trend Micro scan engine, ScreenOS 5.3.0 also offers support for a new enhanced scan engine from Kaspersky Lab.

The Juniper-Kaspersky scan engine by default provides the highest level of security. In addition to screening viruses (including polymorphic and other advanced viruses), the new scan engine also provides inbound spyware and phishing protection.

- **Spyware protection.** The new spyware protection feature adds another layer of protection to Juniper Networks anti-spyware and anti-adware solutions by letting you block incoming spyware, adware, keyloggers, and related malware to prevent it from penetrating your enterprise.

  This solution complements Juniper Networks IDP products, which provide spyware phone-home protection (that is, stopping spyware from sending sensitive data from an infected computer workstation or server).

- **Phishing protection.** The phishing protection allows you to block emails that try to entice users to fake (phishing) sites that steal sensitive data from them.

***Default Security Level***

The Standard default security level is the most secure of the three scanning level options. However, you may choose to change the default security level of scanning with the following two options:

- Basic in-the-wild scanning. This level of scanning administers a lower degree of security by scanning the most prevalent viruses. It provides increased performance.
- Extended scanning. This level of scanning traditionally includes more noisy pieces of spyware/adware to the standard scan. It provides more spyware coverage, but potentially can return more false positives.

## Deep Inspection Signature Packs

In ScreenOS 5.3.0r2, Deep Inspection (DI) signatures are optimized into four signature packs for specific threat coverage and desired network deployment. This approach is ideal because of the limited device memory and increased protocol support.

Table 1 describes the four available signature packs in ScreenOS 5.3.0r2.

Table 1. DI Signature Packs

| Signature Pack | Description | Threat Coverage |
|---|---|---|
| Base[1] | A selected set of signatures for client/server and worm protection optimized for remote and branch offices along with small/medium businesses. | Includes a sample of worm, client-to-server, and server-to-client signatures for Internet-facing protocols and services, such as HTTP, DNS, FTP, SMTP, POP3, IMAP, NetBIOS/SMB, MS-RPC, P2P, and IM (AIM, YMSG, MSN, and IRC). |
| Server-protection | For small/medium enterprises and remote and branch offices of large enterprises needing perimeter defense and compliance for server infrastructure, such as IIS and Exchange. | Primarily focuses on protecting a server farm. It includes a comprehensive set of server-oriented protocols, such as HTTP, DNS, FTP, SMTP, IMAP, MS-SQL, and LDAP. Also includes worm signatures that target servers. |
| Client-protection | For small/medium enterprises and remote and branch offices of large enterprises needing perimeter defense and compliance for hosts (desktops, laptops, and so on.). | Primarily focuses on protecting users from getting malware, Trojans, and so on while surfing the Internet. Includes a comprehensive set of client-oriented protocols, such as HTTP, DNS, FTP, IMAP, POP3, P2P, and IM (AIM, YMSG, MSN, and IRC). Also includes worm signatures that target clients. |
| Worm-mitigation | For remote and branch offices of large enterprises along with small/medium businesses to provide the most comprehensive defense against worm attacks. | Includes stream signatures[2] and primarily focuses on providing comprehensive worm protection. Detects server-to-client and client-to-server worm attacks for all protocols. |
| 1. For NetScreen-5XT and NetScreen-5GT Series devices with ScreenOS 5.3.0, only DI | | |

signatures of critical severity are provided due to memory allocation required for new ScreenOS features.

2. All the other DI signature packs support “Stream256,” in which only the first 256 bits of the stream are inspected. The worm mitigation signature pack however, inspects all packets in the stream.

Juniper Networks stores the signature packs on a database server. To use the predefined attack objects, you must have already downloaded the signature pack from this server and loaded it on your security device.

Before you start downloading a signature pack from the URLs listed in (Table 2) “URLs for Predefined Signature Packs”, you must do the following:

1. Register your security device and obtain an authorization code.
2. Purchase a license key and activate a subscription for Deep Inspection.
3. Verify that the system clock and the Domain Name Service (DNS) settings on your security device are accurate.

After you install a DI license key on your security device, you may download any of the four DI signature packs appropriate for your network needs. You can load the desired signature pack one at a time as necessary.

To download one of the four signature packs, you must **set the attack db url** to one of the URLs specified in Table 2 and then execute **exec attack db update**. The signature pack downloaded depends on the URL specified in the **set** command.

Table 2. URLs for Predefined Signature Packs

| To download or update the | Specify this URL |
|---|---|
| Base signature pack (default) | https://services.netscreen.com/restricted/sigupdates |
| Server-protection signature pack | https://services.netscreen.com/restricted/sigupdates/server |
| Client-protection signature pack | https://services.netscreen.com/restricted/sigupdates/client |
| Worm-mitigation signature pack | https://services.netscreen.com/restricted/sigupdates/worm |

Table 3 lists the available DI signature packs on available security platforms.

Table 3. Supported DI Signature Packs for Juniper Networks Firewalls and VPNs

| Platform | Base | Server | Client | Worm Mitigation |
|---|---|---|---|---|
| NetScreen-5XT<br>NetScreen-5GT<br>NetScreen-HSC | ✓* | ✓ | ✓# | ✓ |

| | | | | |
|---|---|---|---|---|
| NetScreen-25/50<br>NetScreen-204/208<br>NetScreen-500<br>ISG 1000/2000<br>NetScreen-5200/5400 | ✓ | ✓ | ✓ | ✓ |

* We recommend using this signature pack for small/medium businesses.

\# We recommend using this signature pack for remote/branch offices.

### Anti-Spam

NetScreen-HSC, NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, and NetScreen-50 devices—The anti-spam feature examines transmitted messages and decides which are spam and which are not. When the device detects a message deemed to be spam, it either tags the message field with a pre-programmed string, or it drops the message. Anti-spam uses a constantly-updated IP-based spam blocking service that uses information gathered worldwide. Because this service is robust and yields few false positives, it is not mandatory to tune or configure blacklists. However, the administrator has the option of adding specific domains and IPs to local whitelists or blacklists, which the device can enforce locally. The ScreenOS 5.3.or2 release supports anti-spam for SMTP protocol only.

### QoS Enhancements

Quality of Service (QoS) enhancements in this release include the following:

- Ingress policing
- Traffic shaping on virtual interfaces
- Use of all 6 bits of DiffServ Codepoint marking (DSCP).

#### *Ingress Policing*

Ingress policing is supported on the following platforms: NetScreen-5XT, NetScreen-5GT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500. Ingress policing enables you to constrain the flow of traffic through the security device by limiting bandwidth on the ingress side. You do this by setting the policing bandwidth (**pbw**) keyword in a firewall policy to a maximum bandwidth value. Traffic exceeding the bandwidth setting is dropped at the ingress side of the security device, thus conserving throughput resources.

#### *Traffic Shaping on Virtual Interfaces*

Traffic shaping is supported on virtual interfaces on the following platforms: NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, and NetScreen500. In the context of traffic shaping, the term *virtual interfaces* refers only to subinterfaces and tunnel interfaces—not to other types of virtual interfaces, such as virtual security interfaces (VSI), or aggregate or redundant interfaces.

Traffic shaping is not supported on loopback interfaces, because no traffic is actually transmitted on a loopback interface. However, a loopback interface is often used as an anchor point in a VPN, to derive the source IP address, while the data is transmitted on an actual egress interface. When using a loopback interface in a VPN, therefore, you configure traffic shaping on the outgoing interface. ScreenOS then associates the session with the real outgoing interface, which it deduces from the routing table, dynamically updating the association as the routing table changes.

#### *DSCP Marking*

DSCP marking is supported on all platforms and can be configured with traffic shaping or independently. Table 4, Table 5, and Table 6 show how DSCP marking works with the various platforms. (See RFC 2401 for specific information about the handling of inner and outer IP headers, extension headers, and options for AH and ESP tunnels.)

Table 4. DSCP Marking for Clear-Text Traffic

| **Description** | **NetScreen-HSC, NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500** | **NetScreen-5000 Series, ISG 1000, ISG 2000** |
|---|---|---|
| Clear packet with no marking on the policy | No marking. | No marking. |
| Clear packet with marking on the policy | The packet is marked based on the policy. | The packet is marked based on the policy. |
| Premarked packet with no marking on the policy | Retain marking in the packet. | Retain marking in the packet. |
| Premarked packet with marking on the policy | Overwrite marking in the packet based on the policy. | Overwrite marking in the packet based on the policy. |

Table 5. DSCP Marking for Policy-Based VPNs

| Description | NetScreen-HSC, NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500 | NetScreen-5000 Series, ISG 1000, ISG 2000 |
|---|---|---|
| Clear packet into policy-based VPN with no marking on the policy | No marking. | No marking. |
| Clear packet into policy-based VPN with marking on the policy | Only the ESP header is marked, based on the policy. | Mark both the inner packet and the ESP header based on the policy. |
| Premarked packet into policy-based VPN with no marking on the policy | The ESP header is not marked; retain marking in the inner packet. | The ESP header is not marked; retain marking in the inner packet. |
| Pre-marked packet into policy-based VPN with marking on the policy | The ESP header is marked; based on the policy, retain marking in the inner packet. | Overwrite the marking in the inner packet based on the policy and copy the inner packet marking to the ESP header. |

Table 6. DSCP Marking for Route-Based VPNs

| Description | NetScreen-HSC, NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500 | NetScreen-5000 Series, ISG 1000, ISG 2000 |
|---|---|---|
| Clear packet into route-based VPN with no marking on the policy | No marking. | No marking. |
| Clear packet into route-based VPN with marking on the policy | The inner packet and ESP header are both marked, based on the policy. | The inner packet is marked, based on the policy. The ESP header is not marked. |

| Description | NetScreen-HSC, NetScreen-5XT, NetScreen-5GT Series, NetScreen-25, NetScreen-50, NetScreen-200 Series, NetScreen-500 | NetScreen-5000 Series, ISG 1000, ISG 2000 |
|---|---|---|
| Pre-marked packet into route-based VPN with no marking on the policy | Copy the inner packet marking to the ESP header; retain marking in the inner packet. | The ESP header is not marked; retain marking in the inner packet. |
| Pre-marked packet into route-based VPN with marking on the policy | Overwrite the marking in the inner packet based on the policy, and copy the inner packet marking to the ESP header. | Overwrite marking in the inner packet, based on the policy. The ESP header is not marked. |

### Media Gateway Control Protocol (MGCP) ALG for VoIP

The MGCP Application Layer Gateway (ALG) is supported on security devices in Route mode, Transparent mode, and Network Address Translation (NAT) mode. The MGCP ALG performs the following procedures:

- Conducts VoIP signaling payload inspection. Conducts VoIP signaling payload inspection. The payload of the incoming VoIP signaling packet is fully inspected based on RFC 3435. Any malformed packet attack is blocked by the MGCP ALG.
- Conducts MGCP signaling payload inspection. The payload of the incoming MGCP signaling packet is fully inspected in accordance with RFC 3435. Any malformed-packet attack is blocked by the ALG.
- Provides stateful processing. The corresponding VoIP protocol-based state machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- Performs Network Address Translation (NAT). Any embedded IP address and port information in the payload is properly translated based on the existing routing information and network topology, and is replaced with the translated IP address and port number, if necessary.
- Manages pinholes for VoIP traffic. To keep the VoIP network secure, the IP address and port information used for media or signaling is identified by the ALG, and any needed pinhole is dynamically created and closed during call setup and subsequent signaling.

#### *MGCP Security*

The MGCP ALG includes the following security features:

- Denial of Service (DoS) attack protection—The ALG performs stateful inspection at the UDP packet level, the transaction level, and at the call level. MGCP packets matching the RFC3435 message format, transaction state, and call state, are processed. All other messages are dropped.
- Firewall policy enforcement between gateway and gateway controller (signaling policy).
- Firewall policy enforcement between gateways (media policy).
- Per-gateway MGCP message flooding control—Any malfunctioning or hacked gateway will not disrupt the whole VoIP network. Combined with per-gateway flooding control, damage is contained within the impacted gateway.
- Per-gateway MGCP connection flooding control.
- Seamless switch-over/fail-over if calls, including calls in progress, are switched to the standby firewall in case of system failure.

### Gatekeeper Enhancement for H.323

The H.323 protocol ALG is enhanced to support incoming calls in NAT mode, and slow start in Gatekeeper Routed mode. In Gatekeeper Routed mode, all control channel negotiations (Q.931 and H.245) are performed between the gatekeeper and the end points. The media channels, on the other hand, are opened directly between the end points. Support is also provided for video conferences over IP, via Radvision ECS gatekeeper working in conjunction with Polycom video endpoints.

### SIP ALG Enhancements

Several enhancements have been made to the SIP ALG, including the ability to:

- Allow music when the call is put on hold.
- Allow the NOTIFY method beyond dialog termination.
- Handle the OPTIONS method out of dialog.
- Handle the MESSAGE method out of dialog.

### Service Timeout Enhancement

The custom service timeout feature has been enhanced to make service timeout behavior more deterministic and predictable.

### GTP Support

ISG 2000 devices only—ScreenOS provides GTP (GPRS Tunneling Protocol) firewall features that address key security issues on the Gp, Gn, and Gi interfaces in GPRS (General Packet Radio Services) networks.

### Dead Peer Detection

Dead-Peer Detection (DPD) allows an IPSec device to verify the current existence and availability of other IPSec peer devices. The device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to the peers and waiting for DPD acknowledgements (R-U-THERE-ACK).

**Note:** DPD conforms to RFC 3706.

### BGP Route Refresh

The Border Gateway Protocol (BGP) route-refresh feature as defined in RFC 2918 provides a soft reset mechanism that allows the dynamic exchange of route refresh requests and routing information between BGP peers and the subsequent re-advertisement of the outbound or inbound routing table. With this mechanism, it is not necessary to restart the device, and the device does not need to learn all BGP routes again.

### Simple Network Management Protocol Enhancements

On the NetScreen-500, NetScreen-5400, and ISG 2000 devices, ScreenOS supports Simple Network Management Protocol (SNMP) traps for power supply failures and to monitor DIP utilization.

For example, the **set dip alarm-raise *number1*** command sets a DIP utilization alarm threshold, expressed as a percentage of possible DIP utilization. When DIP utilization exceeds this threshold, the device triggers a SNMP trap.

### Source-Based and Source Interface-Based Routing Enhancements

When setting up Source-Based Routing (SBR) and Source Interface-Based Routing (SIBR), ScreenOS accepts a virtual router, such as trust-vr or untrust-vr, as the next hop.

### Dial Enhancements

You can now configure a complete dial disaster recovery system for the NetScreen-5GT or the NetScreen-5XT. You can configure two different types of trustee (limited access) administrative accounts for the monitoring of or changes to the in-band modem connection only. This modem port is used to connect to an external modem or an ISDN terminal adapter (TA) for dialup disaster recovery purposes. You can also specify a priority level for each ISP (up to four) that you configure and specify the trigger mechanism (IP, tunnel, or route tracking).

### Juniper Networks Enterprise Infranet Solution

A Juniper Networks security device and an Infranet Controller (an IC 4000 platform) work together to provide granular, context-specific end-point security and firewall services to connect end users to protected resources. An end user running an Infranet Agent communicates with the Infranet Controller over HTTPS (HyperText Transfer Protocol-Secure) using SSL (Secure Socket Layer) to encrypt the transfer of authentication data. Once authenticated, the user connects to the security device through a policy configured by the Infranet Controller. When the end user logs out the policy is removed from the security device.

### 802.1q VLAN Tag Support on NetScreen-5GT

New supported platforms for VLAN tags are the NetScreen-5GT Series devices.

802.1Q vlan-tagged sub-interfaces are now available on the Trust-Untrust port mode. Juniper Networks security devices support up to a maximum of ten 802.1Q VLAN-tagged subinterfaces.

### Port Modes Support Wireless Interfaces

Juniper Networks NetScreen-5GT Wireless (ADSL) devices support up to four wireless interfaces. The wireless interfaces that are available are dependant on which port mode is configured on your device.

### New Dual/DMZ Port Mode

The NetScreen-5GT Series supports Dual/DMZ port mode. Dual/DMZ mode binds interfaces to the Untrust, Trust, DMZ, and DMZ2 security zones, allowing all security zones to pass incoming and outgoing traffic simultaneously. This port mode requires that you purchase an extended license key.

### Increased Route Redistribution

OSPF and BGP route redistribution capacity has increased on some platforms.

Table 7. Maximum Route Redistribution

| | |
|---|---|
| NetScreen-5200 | 4,096 to 6,000 |
| NetScreen-5400 | 4,096 to 6,000 |
| ISG 2000 | 4,096 to 6,000 |

### Local DNS Resolution Table

All Juniper Networks security devices support a local DNS resolution table (similar to the “host” file on Unix systems).

This feature allows the creation of dynamic policies. You can set a local host name on a security device, add it to the address book, and then use it in policies. Devices under the same administrative domain can use a single policy referring to a local host name; that local host name may have a different IP address depending on the local host name resolution table of each device.

To set a local host name, use the **set dns host name** *host_name ip_address* CLI command.

This feature can be used in conjunction with Proxy-DNS functionality. For instance, multiple security devices from different locations may be resolving the same DNS name, but the resulting IP address may be different based on their respective local host name resolution table.

### Web Filtering

Integrated Web Filtering (with SurfControl) is supported on the following platforms.

**Note:** Web filtering using an external SurfControl server is supported on all platforms.

Table 8. Web-Filtering support

| Device Model | Integrated Web Filtering Support | External Support |
|---|---|---|
| NetScreen HSC<br>NetScreen-5GT Series<br>NetScreen-25<br>NetScreen-50 | YES | YES |
| NetScreen-200 Series<br>NetScreen-500<br>NetScreen-5000 Series<br>ISG 1000,<br>ISG 2000 | NO | YES |

## Changes to Default Behavior

This section lists changes to default behavior between ScreenOS 5.3.0r8 and the previous ScreenOS firmware releases.

**Note:** If the ScreenOS version is not mentioned in this section, the change in behavior was released with ScreenOS 5.3.0r1.

### *Trace Dumps*

Prior to ScreenOS 5.3.0r4, the clear log sys save CLI command did not clear old trace dumps.

### *IKE Attack*

Since ScreenOS 5.3.0r4, the anti-ike-id enumeration attack CLI commands were changed from being available at the vsys level to only available when at the root vsys level.

The following commands are affected:

```
set/unset/get ike ikeid-enumeration
```

### IP Checksum

Since ScreenOS 5.3.0r4, the IP checksum verification was disabled on additional platforms in the NetScreen-5000 series (using 5000-8G and 5000-2G24FE SPM) because the algorithm was not fully RFC compliant and cannot differentiate between 0xffff and 0x0000.

### CPU Calculation

Since ScreenOS 5.3.0r4, CPU utilization calculation could display high CPU cases even though the CPU load is similar to previous ScreenOS version.

### IP Classification

Since ScreenOS 5.3.0r4, after an IP classification returns a new vsys, the device selects the incoming virtual router on the shared interface as the main virtual router instead of the classified vsys.

### Remote Authentication

Since ScreenOS 5.3.0r4, the remote authentication server is queried when an administrator does not appear in the local database.

### TCP Reset

Since ScreenOS 5.3.0r4, TCP reset packets are dropped if they do not match any existing sessions instead of creating a new session.

### Policy Lookup in VoIP ALG

Prior to 5.3.0r4, the VoIP ALG policy lookup module would bypass the Global zone, causing traffic to be classified as MIP instead of non-ALG. 5.3.0r4 has fixed this problem so that ALG correctly emulates a regular traffic policy search.

### SSL Connection Option

Since ScreenOS 5.3.0r4, SSL has an option to connect clients even though the certification path verification failed.

### Password Authentication

Since ScreenOS 5.3.0r4, password authentication attempts are no longer accepted when password authentication is disabled for SSH administrators.

### HA Interface

Since ScreenOS 5.3.0r4, sometimes the HA port will hang. When this port hangs, change the monitoring period to 2 seconds to reset the port.

### *Anti-Spam*

Since ScreenOS 5.3.0r4, after the anti-spam license key expires, only the basic white and black lists are functional.

### *Trend Micro Scan Engine*

Since ScreenOS 5.3.0r4, the Trend Micro scan engine was upgraded to VSAPI 8.0. The Scan-Intelligent scan mode is treated as **scan-all** during a real file scan.

### *Kaspersky AV Scan Engine*

Since ScreenOS 5.3.0r4, when a Kaspersky AV scan engine returns a scan code of password protected file or corrupted file, the device will always pass traffic instead of using the fail mode setting.

ScreenOS has been integrated with the latest Kaspersky AV scan engine and has also been enhanced for AV database file integrity check.

### *ICMP Redirect Packets*

The ICMP redirect packets are dropped without a session match in all modes except Transparent mode. In Transparent mode, the packets will match the existing session, if any.

### *SSH Version 2*

Since ScreenOS 5.3.0r3, administrative users whose accounts were defined in the local (internal) authentication server failed to authenticate when authentication was attempted from an SSHv2 client application.

### *NetScreen-200 Series Virtual Routers*

Prior to ScreenOS 5.3.0r4, devices using the additional virtual router (VR) key had four extra VRs instead of five.

### *SCEP Enrollment*

Since ScreenOS 5.3.0r4, Digital Signature Algorithm (DSA) is unsupported for Simple Certificate Enrollment Protocol (SCEP).

### *Route-Based VPNs*

Prior to 5.3.0r2, if traffic is initiated from the tunnel (encrypted) side, even when there is no reverse route (the route that points to the tunnel interface); traffic would pass through the device. In this release, the reverse route must exist, otherwise packets are dropped.

### *Deep Inspection*

Since ScreenOS 5.3.0, the memory pool on a NetScreen-5GT Series device is reduced to 7 MB. When you upgrade to 5.3.0, you might see the following message during initial restart: (The same message is displayed when you upgrade from ScreenOS 5.1 to 5.3.0 on the NetScreen-5XT device.)

```
Attack DB failed to load. File is too large to load
```

Download the latest DI signature pack by entering the exec attack db update CLI command. You will get a reduced pack containing only critical signatures.

### *AV Scanner File Size Reduced*

The maximum file size, for all email protocols, the AV scanner can examine is 10 megabytes (MB), as opposed to 16 MB in versions prior to ScreenOS 5.3.0. The default file size is also 10 MB.

If the setting on your security device is greater than 10 MB, we recommend that you change the setting to 10 MB before you upgrade the security device to ScreenOS 5.3.0.

### *BGP Peers*

On the NetScreen-5GT Series, NetScreen-5XT, NetScreen-50 devices, the number of BGP peers increased to 10.

### *Interface MTU*

The interface MTU value range changed from 800-1500 bytes to 1280-1500 bytes.

### *XAuth on the NetScreen-Remote*

Previously, a new login window reappeared every time attempts to connect to the Radius server failed (up to 5 times). Currently, only the original login window displays when there is a failed attempt.

## Migration Procedures

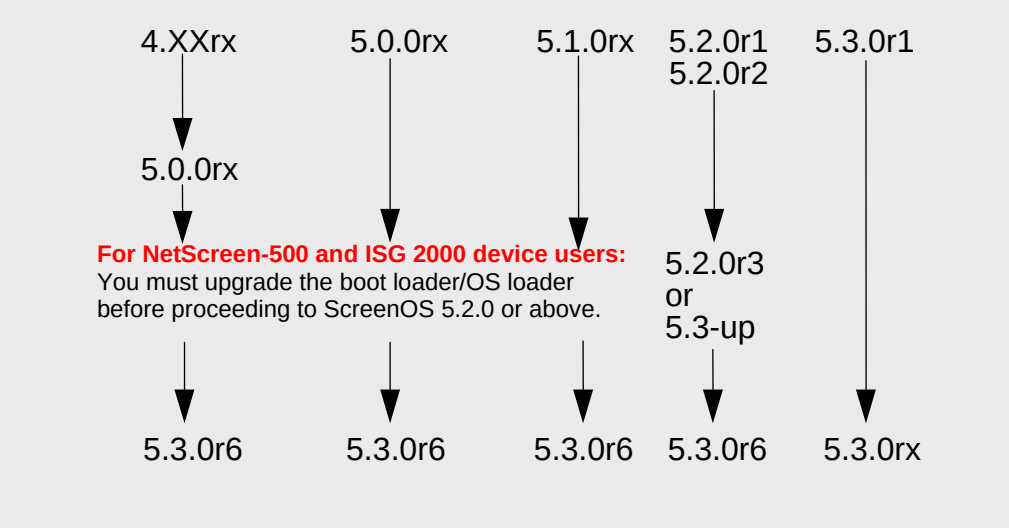
This section includes the migration and upgrade procedures that were part of the Migration Guide in previous releases of ScreenOS. The Migration Guide as a standalone document has been discontinued and its information incorporated in the Release Notes.

Before you begin a security device upgrade, you must have the most recent ScreenOS firmware. If you upgrade from 5.2.0r3 or later to 5.3.0rx, you also require the interim firmware "*xxxx.5.3.0-up*" (where *xxxx* corresponds to the device model). You must upgrade first to the xxx.5.3.0-up firmware then upgrade to 5.3.0rx. See Downloading the New Firmware for more download information.

**Caution:**

- **For NetScreen-5GT Wireless (ADSL) and ISG 1000 device users:** You can go directly to the ScreenOS 5.3.0r6 version because there are no 5.1.0 or 5.2.0 ScreenOS images for these devices.
- **For NetScreen-500 and ISG 2000 device users:** You must upgrade the boot loader/OS loader before proceeding to ScreenOS 5.2.0 or above. Figure 1 shows the firmware upgrade path.

Figure 1. Firmware Upgrade Path




**Caution:** Before upgrading or downgrading a security device, save the existing configuration file to avoid losing any data. When downgrading a security device, the configuration file will be lost.

This section contains the following information:

- Requirements for Upgrading and Downgrading Device Firmware
- Special Boot-ROM or Boot-Loader Requirements
- Downloading the New Firmware
- Upgrading to the New Firmware
- Upgrading and Downgrading the NetScreen-500
- Upgrading the ISG 2000 OS Loader
- Upgrading Security Devices in an NSRP Configuration
- Upgrading or Migrating the AV Scanner

### *Requirements for Upgrading and Downgrading Device Firmware*

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

security device or to downgrade a device from ScreenOS 5.3.0 to ScreenOS 5.2.0: the WebUI, the CLI, or 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 or have remote access to a console server connected to the device.

To use the WebUI, you must have:

- Root or read-write privileges to the security device
- Network access to the security device from a computer that has an Internet browser
- The new ScreenOS firmware (downloaded from the Juniper Networks website and saved locally)

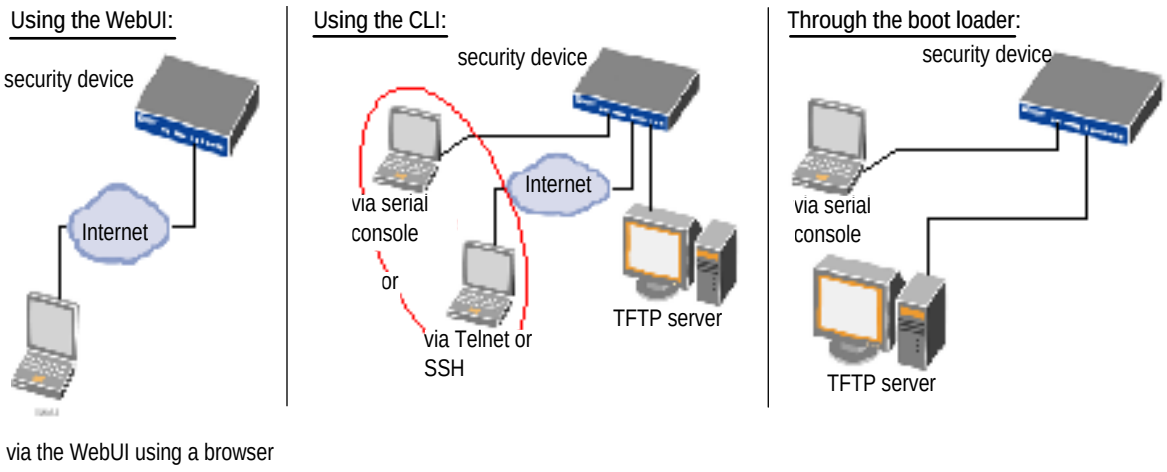
To use the CLI, you must have:

- Root or read-write privileges to the security device
- A console connection or Telnet access to the security device from a computer
- A TFTP server installed locally and to which the security device has access
- The 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:

- Root or read-write privileges to the security device
- A TFTP server installed locally that has an IP address in the same subnet as the security device (255.255.255.0)
- An Ethernet connection from a computer to the security device (to transfer data, namely from a local TFTP server)
- A console connection from the computer to the security device (to manage the security device)
- The new ScreenOS firmware saved to a local TFTP server directory. (Figure 2) illustrates the three different ways by which you can upgrade or downgrade a security device.

Figure 2. ScreenOS Upgrade and Downgrade Methods




via the WebUI using a browser

**Note:** For NetScreen-500 and ISG 2000 devices, you can upgrade or downgrade only through the boot loader.

To upgrade or downgrade a security device, see the step-by-step procedures in Upgrading to the New Firmware or Upgrading Security 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 requires the new boot-ROM (ns500.upgrade6M). To do this, you perform the version upgrade twice. The first time installs the boot-ROM, the second time installs the new ScreenOS image.

### ISG 2000 Boot Loader

Before upgrading an ISG 2000 system to the ScreenOS 5.3.0 release firmware, you must upgrade the OS loader to v1.1.5. You can see the OS loader version scroll by during the startup process or by entering the **get envar** command.

1. Download the OS loader from the Juniper Networks support site to the root directory of your TFTP server.
2. Visit www.juniper.net/customers/support and log in.
3. In the Download Software section, click **ScreenOS Software**.
4. Download the latest OS loader and save it to the root directory of your TFTP server.
5. If necessary, start the TFTP server.

6. Make an Ethernet connection from the device hosting the TFTP server to the MGT port on the ISG 2000 and a serial connection from your workstation to the console port on the ISG 2000.
7. Restart the ISG 2000 by entering the **reset** command. When prompted to confirm the command— System reset, are you sure? y/[n] — press the Y key.
8. When you see the following prompt, press the X key and then the A key:

```
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
```

9. Hit the X and the A keys in sequence to update the OS loader.
10. 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:

```
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]:
```

11. 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.

### *Downloading the New Firmware*

You can obtain the 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. If you upgrade from 5.2.0r2 or later to 5.3.0rx, you also require the interim firmware “xxxx.5.3.0-up” (where xxxx corresponds to the device model). You must upgrade first to the xxx.5.3.0-up firmware then upgrade to 5.3.0rx. The following diagram shows the firmware upgrade path.

1. To get the latest ScreenOS firmware, go to http://www.juniper.net/customers/support, 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 for 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 image, 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, then save the firmware anywhere on the computer.

If you want to upgrade the security devices using the CLI, then 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, then you must use the WebUI to load the new firmware onto the security device.

### *Upgrading to the New Firmware*

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

You can upgrade any device from ScreenOS 5.0.0 and ScreenOS 5.1.0 directly to ScreenOS 5.3.0 using the WebUI or CLI.

You can upgrade any device from ScreenOS 5.2.0 directly to ScreenOS 5.3.0 using the CLI. If you wish to upgrade from ScreenOS 5.2.0 to ScreenOS 5.3.0 using the WebUI, however, you first have to upgrade to an interim firmware. This is due to a buffer size issue.

The following section describes how to perform the upgrade using the WebUI and CLI.

### Using the WebUI

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

1. Log into the security device by opening a browser and then entering the management IP address in the Address field. Log in as the root administrator or an administrator with read-write privileges.
2. Save the existing configuration:
   a) Go to **Configuration > Update > Config File**, then 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 then click **Save**.

#### *Upgrading to the Interim Firmware (for Upgrading from ScreenOS 5.2.0 Only)*

If you are upgrading security devices from ScreenOS 5.0.0 or ScreenOS 5.1.0, skip to step 9.

3. Go to **Configuration > Update > ScreenOS/Keys** and select **Firmware Update**.
4. Click **Browse** to navigate to the location of the interim firmware "xxxx.5.3.0-up' (where *xxxx* corresponds to the device model) or type the path to its location in the Load File field.
5. 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 from step 4.

6. Click **OK** to continue.
7. The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.
8. 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 to the New ScreenOS Firmware*

9. Go to **Configuration > Update > ScreenOS/Keys** and select **Firmware Update**.
10. Click **Browse** to navigate to the location of the new ScreenOS firmware or type the path to its location in the Load File field.
11. Click **Apply**.
12. A message box appears with information on the upgrade time.

13. Click **OK** to continue.

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

14. 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.

### Using the CLI

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

1. Make sure that you have the new ScreenOS firmware. For information on obtaining the new firmware, see Downloading the New Firmware.
2. Run the TFTP server on your computer by double-clicking on the TFTP server application.
3. Log into the security device using an application such as Telnet or Secure Shell (SSH) or Hyper Terminal if directly connected through the console port. Log in as the root administrator or an administrator 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 **save soft from** tftp *ip_addr filename* **to flash** command.

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

6. When the upgrade or downgrade is complete, you must reset the security device. Execute the **reset** command and enter **y** at the prompt to restart 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.
9. Upload the configuration file that you saved in step 3 with the **save config to** {**flash** | **slot1** | **tftp**}... command.

### 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, you cannot use this process to save firmware, ScreenOS 5.1.0 or previous, to flash memory. Use the WebUI or CLI to save ScreenOS 5.1.0 firmware to flash memory

To load firmware with the Boot/OS loader, perform the following steps:

1. Connect your computer to the security device using one of the following methods:
   a) Using a serial cable, connect the serial port on your computer to the console port on the security device. 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 between 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 Downloading the New Firmware.
3. Run the TFTP server on your computer by double-clicking on the TFTP server application. You can minimize its window but it must be active in the background.
4. Log into the security device using a terminal emulator such as Hyper Terminal. Log in as the root administrator or an administrator 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 the keyboard to interrupt the bootup process.

**Note:** If you do not interrupt the security device in time, it proceeds to load 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.

   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.

#### Saving Multiple Firmware Images with Boot Loader

After the firmware is downloaded successfully, the console displays the following:

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

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

On some security devices, you can answer 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 input the name in the TFTP server. If you do not enter a name, then 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.

### *Upgrading and Downgrading the NetScreen-500*

Before the NetScreen-500 platform can support ScreenOS 5.3.0, you must upgrade the OS boot loader and file system to accommodate the larger image size. The previous OS loader and file system supported a smaller image size.

The NetScreen-500 platform has 16 MB of total flash, with 4MB reserved for the OS loader and 12 MB for the file system and system image. In order to load the 5.3.0 image successfully, the file system must not exceed 5.6MB. Do the following to check the size of the file system:

- If you are running ScreenOS 4.X, use the **get file extension** command to list the files and their sizes. You can add up the individual file sizes to get the total size of the file system.
- If you are running ScreenOS 5.x, use the **get file info** command to display the total and available number of bytes.

The file system contains the configuration file, certificates, local logs and other files. If the file system is greater than 5.66M, you can reduce its size by reducing the configuration file size and deleting unnecessary files and logs.

**Caution:** Before you upgrade the OS loader and file system, we strongly recommend that you back up the configuration file.

To upgrade the OS loader and file system, perform the following steps:

1. Download the upgrade image, ns500.upgrade, onto your computer.
2. Visit juniper.net and log in.

3. In the Download Software section, download ns500.upgrade from the ScreenOS 5.2 folder.
4. Load the ns500. upgrade software onto the NetScreen-500 through the WebUI, CLI or boot loader.

   For information on loading the software, see Upgrading to the New Firmware.

   If you used the WebUI to upgrade the NetScreen-500 platform, it automatically restarts. If you used the CLI or the boot loader, use the reset command to restart the device.

The security device restarts, using the ns500.upgrade image. You have completed the upgrade of the OS loader and file system. You can now upgrade the firmware to ScreenOS 5.3.0.

For information on upgrading the firmware, see Upgrading to the New Firmware.

### Downgrading a NetScreen-500 Device

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

If you need to downgrade the device to a version prior to ScreenOS 5.0.0, downgrade using the boot/OS loader (seeUsing the Boot/OS Loader).

To downgrade a NetScreen-500 device from ScreenOS 5.3.0 to ScreenOS 5.0.0 or above, use the CLI or boot loader:

#### *Using the CLI*

To downgrade using the CLI, perform the following steps:

1. Download the firmware from the Juniper Networks website. You must load the firmware on the security device using the CLI. Therefore, save the firmware to the root TFTP server directory on the computer.
2. For information on downloading the firmware, see Downloading the New Firmware.
3. Load the firmware with the CLI. For information on using the CLI to load firmware, see Using the CLI.
4. Enter the **exec downgrade** command.

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. You must load the firmware on the security device using the CLI. Therefore, save the firmware to the root TFTP server directory on the computer.
2. For information on downloading the firmware, see Downloading the New Firmware.
3. Enter the CLI command **exec downgrade**.

The security device automatically restarts.

4. Load the firmware using the boot/OS loader. For information on using the boot/OS loader, see Using the Boot/OS Loader.

### *Upgrading the ISG 2000 OS Loader*

Before the ISG 2000 can support ScreenOS 5.3.0, you must upgrade the OS loader if it is not v1.1.5. You can see the OS loader version scroll by during the bootup process or by entering the get envar CLI command.

1. Download the OS loader from the Juniper Networks support site to the root directory of your TFTP server.
2. Go to http://juniper.net/customers/support and log in using your user credentials.
3. In the Download Software section, download the software from the ScreenOS 5.3.0 folder.
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** CLI command. When prompted to confirm the command—System reset, are you sure? y/[n]—press the Y key.
8. When you see the following prompt, press the X key and then the A key in sequence:

```
NetScreen NS-ISG 2000 BootROM V0.9.0 (Checksum: 8796E2F3)
Copyright (c) 1997-2004 NetScreen Technologies, Inc.
Total physical memory: 1024MB
Test – Pass
Initialization.............. Done
```

9. Hit the X and the A keys in sequence to update the OS loader.
10. 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:

```
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]:
```

11. 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.

## *Upgrading Security 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:** If your security device has a basic configuration, you can upgrade from ScreenOS 5.0.0 or ScreenOS 5.1.0 directly to ScreenOS 5.3.0. However, you risk losing part of the configuration. For NetScreen-500 and ISG 2000 devices, you must follow the version-specific upgrade sequence (see Upgrading to the New Firmware).

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

### Upgrading Devices in an NSRP Active/Passive Configuration

The following illustrates a basic NSRP active/passive configuration where device A is the master and device B is the backup.

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

**Note:** Do not power off your security device while it is upgrading to new firmware. Doing so could result in permanent damage to your device.

To upgrade two devices in an NSRP active/passive configuration, follow these steps (some of these steps are exclusive to the CLI):

- A. Upgrade Device B to ScreenOS 5.3.0
- B. Fail Over Device A to Device B (CLI only)
- C. Upgrade Device A to ScreenOS 5.3.0
- D. Synchronize Device A (CLI only)
- E. Fail Over Device B to Device A (CLI only)

#### *Upgrade Device B to ScreenOS 5.3.0*

##### *WebUI*

If upgrading from 5.2.0r1 or 2 to 5.3.0, make sure that you have the new ScreenOS firmware and the interim firmware "*xxxx.5.3.0-up*" (where *xxxx* corresponds to the device model). For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into device B by opening a browser and entering the management IP address in the Address field. Log in as the root administrator or an administrator with read-write privileges.
2. Save the existing configuration:
   a) Go to **Configuration > Update > Config File**, then 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), then click **Save**.
3. Go to **Configuration > Update > ScreenOS/Keys** and select **Firmware Update**.
4. Click **Browse** to navigate to the location of the ScreenOS 5.3.0 firmware or type the path to its location in the Load File field.
5. Click **Apply**.

   A message box appears with information on the upgrade time.
6. Click **OK** to continue.
7. The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.
8. 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.

##### *CLI*

Make sure that you have the ScreenOS 5.3.0 firmware. For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into device B using an application such as Telnet or Secure Shell (SSH) or HyperTerminal if directly connected through the console port. Log in as the root administrator or an administrator with read-write privileges.
2. Save the existing configuration by executing the following command:

   save config to `{` flash `|` slot1 `|` tftp `}...`
3. Run the TFTP server on your computer by double-clicking on the TFTP server application.

4. On the security device, enter **save soft from tftp** *ip_addr filename* **to flash**, where *ip_addr* is that of your computer and *filename* is that of the ScreenOS 5.3.0 firmware.
5. 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.
6. Wait a few minutes, and then log into the security device again.
7. Use the **get system** command to verify the version of the security device ScreenOS firmware.

#### *Fail Over Device A to Device B (CLI only)*

8. Manually fail over the master device to the backup device.
9. Log into the master device.
10. 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 master device.
    - If preempt is enabled: **exec nsrp vsd-group 0 mode ineligible**
    - If preempt 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 become the primary.

#### *Upgrade Device A to ScreenOS 5.3.0*

##### *WebUI*

Make sure that you have the 5.3.0 ScreenOS firmware and the interim firmware "*xxxx.5.3.0-up*" (where *xxxx* corresponds to the device model). For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into security device A.
2. Save the existing configuration:
    a) Go to **Configuration > Update > Config File**, and then 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 then click **Save**.
3. Go to **Configuration > Update > ScreenOS/Keys** and select **Firmware Update**.
4. Click **Browse** to navigate to the location of the ScreenOS 5.3.0 firmware or type the path to its location in the Load File field.
5. Click **Apply**.

    A message box appears with information on the upgrade time.
6. Click **OK** to continue.

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

7. Log into the security device. You can verify the security device ScreenOS firmware version on the WebUI homepage, in the Device Information section.

#### *CLI*

Make sure that you have the ScreenOS 5.3.0 firmware. For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into security device A.
2. Save the existing configuration by executing the following command:

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

3. Run the TFTP server on your computer by double-clicking on the TFTP server application.
4. On the security device, execute the following command:

   **save soft from tft**p *ip_addr filename* **to flash**

   where $ip\_addr$ is the IP address of your computer and $filename$ is the name of the ScreenOS 5.3.0 firmware file.

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.

5. 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.

#### *Synchronize Device A (CLI only)*

After you complete the upgrade of device A to ScreenOS 5.3.0, manually synchronize the two devices. On device A (backup), issue the **exec nsrp sync rto all** command from peer CLI command to synchronize the RTOs from device B (master).

#### *Fail Over Device B to Device A (CLI only)*

After synchronizing the devices, manually fail over the master device to the backup device. Follow the same steps as in “B. Fail Over Device A to Device B (CLI only)” on page 22, except that you log into device B and fail over device B instead of failing over device A.

### 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 master 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 master of both VSD groups. You then upgrade the backup device first and the master device second.

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

Before you begin, please read the requirements to perform an upgrade (“Requirements to Upgrade and Downgrade Device Firmware” on page 10). Also, make sure that you download the ScreenOS 5.3.0 firmware.

**Warning:** Do not power off your security device while it is upgrading to new firmware. Doing so could result in permanent damage to your device.

To upgrade two devices in an NSRP active/active configuration, follow these steps (note that for some of these steps you can only use the CLI):

A. Fail Over Device B in VSD 1 to Device A in VSD 1 (CLI only)

B. Upgrade Device B to ScreenOS 5.3.0

C. Fail Over Device A to Device B (CLI only)

D. Upgrade Device A to ScreenOS 5.3.0

E. Synchronize Device A (CLI only)

F. Fail Over Device B in VSD 0 to Device A in VSD 0 (CLI only)

#### *Fail Over Device B in VSD 1 to Device A in VSD 1 (CLI only)*

1. Manually fail over the master device B in VSD group 1 to the backup device A in VSD group 1.
2. Log into device B using an application such as Telnet or Secure Shell (SSH) or HyperTerminal if directly connected through the console port. Log in as the root administrator or an administrator with read-write privileges.
3. 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 preempt is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If preempt is not enabled: **exec nsrp vsd-group 1 mode backup**

Either command forces device B to step down and device A to immediately assume mastership of VSD 1. At this point, device A is master of both VSD 0 and 1 and device B is backup for both VSD 0 and 1.

#### *Upgrade Device B to ScreenOS 5.3.0*

##### *WebUI*

Make sure that you have the 5.3.0 ScreenOS firmware and the interim firmware “*xxxx.5.3.0-up*” (where *xxxx* corresponds to the device model). For information on obtaining the firmware, see Downloading the New Firmware.

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

2. Save the existing configuration:
   a) Go to **Configuration > Update > Config File**, and then 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 then click **Save**.
3. Go to **Configuration > Update > ScreenOS/Keys** and select **Firmware Update**.
4. Click **Browse** to navigate to the location of the ScreenOS 5.3.0 firmware or type the path to its location in the Load File field.
5. Click **Apply**.

   A message box appears with information on the upgrade time.
6. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.
7. Log into the security device. You can verify the security device ScreenOS firmware version on the WebUI homepage, in the Device Information section.

*CLI*

Make sure that you have the ScreenOS 5.3.0 firmware. For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into device B.
2. Save the existing configuration by executing the following command:

   save config to {flash | slot1 | tftp}. . .
3. Run the TFTP server on your computer by doubleclicking on the TFTP server application.
4. On the security device, enter **save soft from tftp** *ip_addr filename* **to flash**, where *ip_addr* is that of your computer and *filename* is that of the ScreenOS 5.0.0 firmware.
5. 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.
6. 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.

***Fail Over Device A to Device B (CLI only)***

1. Manually fail over device A completely to device B.
2. Log into device A.

3. Fail over master 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 master device.
   - If **preempt** is enabled: **exec nsrp vsd-group 0 mode ineligible**
   - If **preempt** is not enabled: **exec nsrp vsd-group 0 mode backup**
4. Fail over master device A in VSD 1 to backup device B in VSD 1 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 master device.
   - If **preempt** is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If **preempt** is not enabled: **exec nsrp vsd-group 1 mode backup**

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

#### *Upgrade Device A to ScreenOS 5.3.0*

- **WebUI**

Make sure that you have the 5.3.0 ScreenOS firmware and the interim firmware "*xxxx.5.3.0-up*" (where *xxxx* corresponds to the device model). For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into security device A.
2. Save the existing configuration:
   a) Go to **Configuration > Update > Config File**, and then 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 then click **Save**.
3. Go to Configuration > Update > ScreenOS/Keys and select Firmware Update.
4. Click **Browse** to navigate to the location of the ScreenOS 5.3.0 firmware or type the path to its location in the Load File field.
5. Click **Apply**.

   A message box appears with information on the upgrade time.
6. Click **OK** to continue.

   The security device restarts automatically. The upgrade is complete when the device displays the login page in the browser.
7. Log into the security device. You can verify the security device ScreenOS firmware version on the WebUI homepage, in the Device Information section.

#### *CLI*

Make sure that you have the ScreenOS 5.3.0 firmware. For information on obtaining the firmware, see Downloading the New Firmware.

1. Log into device A.
2. Save the existing configuration by executing the following command:

   save config to {flash | slot1 | tftp}. . .
3. Run the TFTP server on your computer by double-clicking on the TFTP server application.
4. On the security device, use the **save soft from tftp** *ip_addr filename* **to flash** CLI command, where *ip_addr* is the IP address is of your computer. and *filename* is the name of the ScreenOS 5.3.0 firmware file.
5. 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.
6. 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.

#### *Synchronize Device A (CLI only)*

After you complete the upgrade of device A to ScreenOS 5.3.0, manually synchronize the two devices. On device A, issue the exec nsrp sync rto all command from peer CLI command to synchronize the RTOs from device B.

#### *Fail Over Device B in VSD 0 to Device A in VSD 0 (CLI only)*

As the final step, you have to reinstate the two security devices in an NSRP active/active configuration.

1. Log into device A.
2. Fail over master device B in VSD 0 to backup device A 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 master device.

   - If **preempt** is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If **preempt** is not enabled: **exec nsrp vsd-group 1 mode backup**

   At this point, device A is master of VSD 0 and backup for VSD 1, and device B is master of VSD 1 and backup for VSD 0.

### *Upgrading or Migrating the AV Scanner*

Refer to Upgrading to ScreenOS 5.3.0 and follow the procedure below for step-by-step instructions on upgrading your existing antivirus scanner or migrating to a new antivirus scanner:

Table 9. Upgrading to ScreenOS 5.3.0

| If you are upgrading from a previous release of ScreenOS | Follow this procedure |
|---|---|
| With antivirus<br>(AV license installed) | Save your current configuration.<br>Install the AV license.<br>Upgrade to ScreenOS 5.3.0[1]. |
| Without antivirus<br>(without AV license installed) | Upgrade to ScreenOS 5.3.0.<br>Install the AV license. |

1. Save your current configuration.
2. Install your AV license key.

   To access your AV license key, refer to the *Concepts & Examples ScreenOS Reference Guide*. You must install the license key before you upgrade to ScreenOS 5.3.0, or you might lose some of your current configuration.

   ScreenOS 5.3.0 supports 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.

Table 10. AV Scan Engines

| AV Scan Engine | License Key | ScreenOS version |
|---|---|---|
| Trend Micro | av_key | *<device_name>tmav.5.3.0r6* |
| Juniper-Kaspersky | av_v2_key | *<device_name>.5.3.0r6* |
| where <device_name> refers to the hardware security device and xx refers to the letters identifying the build. | | |

3. Upgrade to ScreenOS 5.3.0.

   There are two versions of ScreenOS 5.3.0 as shown in (Table 10). A single version of ScreenOS does not support both scan engines.

   Make sure you select the ScreenOS version which supports the AV scan engine that was installed in Step 2. For example, the file names for NetScreen-5GT are of the format:

   - Trend Micro image: ns5gttmav.5.3.0r6
   - Juniper-Kaspersky image: ns5gt.5.3.0r6

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

### Scan Manager Profile

The global scan-mgr CLI command controls the embedded scan manage, 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, some of the previously global settings are now configured from within a profile context as shown in Command Updates. 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 set using the set av scan-mgr CLI command.

When you upgrade to ScreenOS 5.3.0, a scan manager profile named scan-mgr is automatically generated to migrate the global scan-mgr CLI 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
```

Table 6 shows the updated commands in ScreenOS 5.3.0. The following commands are now invoked from within a profile context:

Table 11. Command Updates

| Commands previous to ScreenOS 5.3.0 | ScreenOS 5.3.0 commands invoked from within a profile context |
|---|---|
| set av http skipmime | set av profile scan-mgr<br>set http skipmime mime-list ns-skip-mime-list<br>set http skipmime enable<br>exit |
| unset av http skipmime | set av profile scan-mgr<br>unset http skipmime enable<br>exit |
| set av scan-mgr content { FTP \| HTTP \| IMAP \| POP3 \| SMTP } [timeout number] } | set av profile scan-mgr<br>set { FTP \| HTTP \| IMAP \| POP3 \| SMTP<br>{ enable \| timeout *number* } }<br>exit |
| unset av scan-mgr content { FTP \| HTTP \| IMAP \| POP3 \| SMTP } | set av profile scan-mgr<br>unset { FTP \| HTTP \| IMAP \| POP3 \| SMTP }<br>enable<br>exit |

**Antivirus Pattern Update URL**

Trend Micro Inc. will stop hosting AV pattern file updates at

http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini.

The new pattern update URL location is

http://5gt-p.activeupdate.trendmicro.com/activeupdate/server.ini.

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

Upgrade to a newer release or manually change the AV pattern update URL to the new location. To verify if the pattern update URL is modified during the upgrade process, enter 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

The following sections identify which major bugs have been fixed in each release of ScreenOS 5.3.0.

## *Addressed Issues in ScreenOS 5.3.0r8*

**Admin**

- **cs11896—**In some cases, during an IKE P1 initiation event, a log/syslog is not generated.
- **cs12493—**The "get service syslog" command displayed the same information twice.
- **cs12613—**SNMP counter does not update until "get count stat" is issued from the CLI.

**CLI**

- **cs10066—**When configuring a static route through the CLI, a metric of zero cannot be configured when the next-hop is a virtual router.
- **cs12128—**ISG 2000 NSRP cluster primary unit core-dumped when pasting commands via CLI.

**HA & NSRP**

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

**Management**

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

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

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

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

- **cs11794—**Some WebTrend log entries are not formatted properly.

- **cs12068—**An SNMP query to a NetScreen policy MIB failed if no policy was configured in Root vsys.

- **cs12251—**Under certain circumstances, syslog entries will contain invalid send/receive value.

- **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.

**Other**

- **cs12738—**ISG 2000 crashed because of an invalid sess idx from the chip.

- **cs11099—**Firewall was upgraded to 5.4r1 and NTP task is causing high CPU (~80%) with no traffic going through the device.

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

- **cs10558—**A new ALG connection failed if the total number of existing ALG connections was greater than 1024.

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

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

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

- **cs12637—**Under high session utilization on lower-end firewalls such as the NetScreen-5GT, session creation failure may lead to a device failure.

**Performance**

- **cs10867—**An interface set to 100mb/full fixed was found to be operating in half-duplex mode.

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

**Routing**

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

- **cs12818—**Primary firewall stops 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.

- **cs12164—**Under certain conditions, static routes using the gateway tracking function may change/disappear if the interface goes down then back up. W/A: Specify the outgoing interface in a static route.

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

- **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.

**VOIP/H323**

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

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

**VPN**

- **cs12434—**VPN dial-up using ike-id asn1-dn wildcard failed.

- **cs12419—**UDP fragments could get dropped across a site to site VPN on a NetScreen-5200-II, where the routed interface is a sub-interface. W/A: Set the max-frame-size=1514 bytes or smaller.

- **cs10624—**Packets are not sent out when the dial-up VPN is configured on the loopback interface in a vsys.

**Web UI**

- **cs10838—**Not able to configure MIP grouping policy thru the WebUI.

- **cs12067—**When using NAT or Route mode, the outgoing interface options for an IKE Gateway configuration incorrectly included Transparent Mode options.

- **cs12558—**The eBGP and iBGP route preference would swap when saving VR settings in the WebUI.

- **cs12452—**Policies with more than 55 address objects did not display correctly in the WebUI.

- **cs10281—**The device failed when two simultaneous and incomplete logins via the WebUI occurred.

## *Addressed Issues from ScreenOS 5.3.0r7*

### *Administration*

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

- **cs10996—**The save config to tftp CLI command did not save the set alarm threshold cpu CLI command to the config file.

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

- **cs11548—**When setting an administrator password through the WebUI it could not contain the quotation character (") **W/A:** Use the CLI if using quotations (") in the administrator 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.

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

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

- **cs11106—**[NetScreen 5000 series] The "clear count all" CLI command did not clear the interface counters on a 5000-24FE SPM configured with aggregate interfaces.

- **cs11347—**If the system limitation for address groups is reached, a Multi-cell address could not be added.

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

### *Antivirus*

- **cs09939—**[NetScreen-5GT] AV was failing on some occasions with the following messages posted to the log: ‘SCAN-MGR: Check AV pattern file failed with error code: -3’ and ‘AV:…scan-engine error or constraint with code 10 for Internal Error 800’.

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

- **cs10938—**In some cases, the antivirus service intermittently blocked mail clients.

***CLI***

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

- **cs11617—**[NetScreen-5GT] In the default configuration, a blank line could have appeared after the 'set hostname' CLI command.

- **cs11536—**An incorrect interface was used when redirecting some CLI "get" commands output information to the TFTP server.

- **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.

***DNS***

- **cs10969—**On some occasions the device would restart due to incorrect handling of a DNS server response.

- **cs09540—**Issuing the "exec dns refresh" command may have caused MIP traffic to stop passing through the device. **W/A:** Disabling and enabling any MIP policy resolved the situation.

***HA & NSRP***

- **cs10020—**In an NSRP environment, the backup device failed due to a loop in the code caused by the "HA_MSG_RPC_INSERT_MAP" message.

- **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.--

- **cs11993—**In an NSRP environment, the device would fail on occasion when the pre-allocated resource group was used up.

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

***Management***

- **cs11631—**In a single ARM VPN configuration, telnet was allowed on the interface, even when telnet was disabled.

- **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.-

- **cs11222—**[NetScreen-200] Under certain conditions, the “Flash” LED did not illuminate after a reboot.

- **cs11688—**[ISG 2000] The interface statistics displayed the “out ucast” as a value of 2^64; this value does not increase or change.

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

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

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

- **cs10021—**The ifAdminStatus OID was UP regardless of the state of the interface. In the case of interface down in the firewall, "ifAdminStatus" showed UP and "ifOperStatus" showed DOWN. This combination indicated a fault in SNMP management systems which triggered an alarm.

- **cs10111—**NSM's active sessions tab did not provide a consistent list of sessions.

- **cs07702—**[ISG 1000, ISG 2000] Electrical noise caused the MGT interface to report up and down status changes even though there was no physical connection. **W/A:** Physically connect the MGT interface.

- **cs10425—**Configuring an SNMP host address of x.x.x.255 produced an “invalid IP address” error.

- **cs11274—**In some cases pushing a large configuration to a device with NetScreen-Security Manager caused the device to restart.

***NAT***

- **cs11198—**The device did not respond to an ARP request for a destination NAT policy with a specific source address specified under the source address field.

***Other***

- **cs11280—**Xauth for a user in MS Active Directory Server configured as an LDAP server did not work. The same server when configured for admin auth worked for the same user.

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

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

- **cs10621—**FTP transfers were failing on occasion when "reassembly-for-alg" was enabled.

- **cs10610—**A large number of TTL packets with value zero caused high CPU on the device.

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

- **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.

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

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

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

- **cs11840—**Active FTP data session failed if syn-flood was triggered in an ECMP zone.

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

- **cs11232—**When viewing a VSYS configuration, the first VSYS listed in the configuration file had vrouter information while subsequent VSYS entries did not.

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

***Performance***

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

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

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

***Routing***

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

- **cs09033—**The debug message was improperly showing the OSPF nexthop.

- **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.

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

***Security***

- **cs11204—**Some standard traffic was incorrectly identified and dropped when syn-cookie was enabled in Transparent (L2) mode.

- **cs11423—**The device would reset when DI was enabled and a certain type of server message block (SMB) protocol was going through the device.

- **cs09995—**A triggered UDP flood with a specific DST-IP configured did not record in the event log, even though the UDP counter continued to increase.

- **cs11469—**In some cases with URL filtering using Websense, slowness occurred due to the URL request queue filling up on the device.

***VOIP/H323***

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

- **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.

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

- **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:** manually disable alg sip using the command “unset alg sip enable"

***VPN***

- **cs11294—**In the case where the serial backup interface took over while the DSL interfaces had gone down, and the option Dead Peer Detection was enabled, when the DSL interface was restored, retransmission messages from the serial backup interface were posted in the log, even though it was down.

- **cs04993—**After a device was 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.--

- **cs11700—**An IKE user with Distinguished Name and Xauth were disabled after a device reset.

- **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 is incorrectly set to 0.0.0.0. **W/A:** Change the policy to another service, such as udp500 or ANY.

***Web UI***

- **cs11918—**The WebUI displayed an error when adding/editing VSYS interface.

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

- **cs11716—**An SIBR route could not be removed through 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:** Use the CLI to delete the categories.

- **cs07951—**In the WebUI menu Screening>Anti-virus>Scan-Manager, checking "HTTP Webmail Enable" will only scan Webmail and not the rest of the HTTP traffic. For clarity, the button now shows "Webmail Only"

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

## *Addressed Issues from ScreenOS 5.3.0r6*

#### *Administration*

- **cs09142**—Within a policy, GTP names that contained spaces were stored incorrectly.
- **cs09197**—When **log session-init** is enabled in a policy, the initialization traffic was displayed to the local log but did not send the information to a syslog server. The device only sent session logs to a syslog server upon termination.
- **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.
- **os66650**—Update internal Daylight Savings Time (DST) tables for the new USA 2007 schedule.

#### *Antivirus*

- **cs10644**—With AV enabled, e-mails failed when they were sent to an e-mail address that contained equity (example: equity@anydomain).

#### *DHCP*

- **cs10427**—When DHCP relay was used, the device incorrectly sent broadcast instead of unicast even though the broadcast flag was set to 0.

#### *HA & NSRP*

- **cs09586**—The **unset vr trust nsrp-sync-config** CLI command could prevent the backup device from loading an NSRP saved configuration after the **exec nsrp sync global save** CLI command was executed.
- **cs08853**—Configuring the RADIUS auth-server from the CLI, WebUI, or NetScreen-Security Manager and executing the **exec nsrp sync global config check-sum** CLI command resulted in the error **Warning: configuration out of sync**.
- **cs10761**—In an NSRP configuration in which the aggregate interfaces were configured for specific duplex sets, executing the configuration sync CLI commands on the backup device could cause the duplex settings to be modified.

- **cs05194**—An NSRP backup failed when clear ARP was issued on the primary device.

***Management***

- **cs09306**—When upgrading a device, if a CLI command failed while the device was restarting, any extraneous exit commands following the failed command could cause the remaining configuration to be lost.
- **cs10475**—With SSH v1 enabled, SSH or WebUI management of the device could fail after several days. This was due to the resources being released incorrectly.
- **cs08466**—When using a Sun Solaris device to log in through SSH using PKA-DSA and SCP, the authentication was successful but the prompt to connect to the device did not display. Using SSH to log in with a password worked correctly.
- **cs09589**—In an NSRP Active-Active environment, the device did not send WebTrend logs when it was configured with the **Use Trust Zone Interface as Source IP for VPN** option.
- **cs11149**—After a device was upgraded to 5.3r4 and later, NetScreen-Security Manager would take approximately 10 times longer to complete the upgrade.

***Other***

- **cs10163, cs10407**—(ISG 2000 and ISG 1000) With subinterfaces and DI enabled, traffic would be blocked and DNS lookups could failed.
- **cs10459**—Real Time Streaming Protocol (RTSP) application connections intermittently failed.
- **cs08855**—With web filtering enabled, the device could restart if the session information became invalid prior to receiving a response from a Content Portal Authority (CPA).
- **cs09166**—The Auth Server Source Interface feature was not working as expected in a wireless environment.
- **cs09572**—Oracle communication between the client and server could fail if using a policy configured with the predefined service of SQL*NET v2 and ALG was enabled.
- **cs11116**—Traffic loss was experienced when an interface was remove, because the device mistakenly removed the ARP entry.
- **cs11066**—When reassembly-for-alg was enabled on a zone, and TCP traffic needed to be reassembled, sometimes causing the device to restart.
- **cs10157**—The device would restart when the wrong internal memory address was accessed.

- **cs11249**—When using Transparent (L2) mode ARP entries were incorrectly stored in the table.

***Performance***

- **cs11014**—In some configurations, in which there were many policies, the device would encounter high memory usage. User would have to restart the device to recover from the situation.
- **cs10042**—The traffic-shaping current bandwidth calculation was inaccurate.

***Routing***

- **cs09324**—(NetScreen-5400 using 5000-M2 management modules) After UDP traffic passing through the device created a single session, clearing the ARP table could cause the source MAC address in the session detail to display as zeros.
- **cs10749**—(ISG 2000) For interfaces with VLAN tagged, the device was not passing traffic when DI was enabled on the policy.
- **cs10713**—Unable to reconnect to PPPoE when the ISP provided a new IP address and an incoming DIP was configured in a policy for SIP.
- **cs11254**—The device incorrectly handled a multicast command if the access-list contained a deny item.

***Security***

- **cs10424**—In a vsys, URL protocol type SurfControl (SCFP) was not retained after a device was restarted.

***VOIP/H323***

- **cs09619**—With SIP ALG enabled, the device incorrectly handled an asterisk (*) in the Contact SIP header field.

***VPN***

- **cs09812**—The device was unable to run a trace route through a route-based VPN tunnel when the tunnel interface was configured as an unnumbered interface. Additionally, the ICMP packet type/code returned was not the expected **type 11 code 0**.
- **cs09486**—In some cases, L2TP over IPSec communication failed after a phase 2 rekey.
- **cs11236**—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**.**
- **cs10869**—In some cases, parts of a VPN remote user configuration were removed when the device restarted, causing connection problems.
- **cs11027**—PPPoE with serial dial backup did not work when VPN failover was used.

- **cs11086**—In some cases, when an existing dynamic VPN policy was deleted, the device would restart.
- **cs10929**—If a dialup IPSec session was established with XAuth enabled, the accounting stop packet was not immediately sent upon session termination.

#### *WebUI*

- **cs09551**—Route-map names created through the WebUI are truncated at 19 characters; unlike the CLI where the max limit of 30 characters can be used.
- **cs09690**—(NetScreen-5GT) The WebUI Reports for active users was calculated incorrectly for NAT users.

### *Addressed Issues from ScreenOS 5.3.0r5*

#### *Administration*

- **cs10884**—By default, the V1-Null zone was shared, whereas all other Layer-2 zones were not shared.
- **cs09436**—(NetScreen-5000 Series using 5000-2G24FE SPM) The device would have up to 100 screen options configured. Exceeding this limit could cause network interruptions.
- **cs10605**—The **set interface** *interface* **protocol igmp accept router** *acl number* CLI command was not retained after the device was restarted.

#### *CLI*

- **cs08380**—A DIP configured on the loopback interface was invisible in the CLI.

#### *DNS*

- **cs10278**—The device would restart if the proxy DNS was set in a vsys. The feature proxy DNS was unsupported in a vsys, therefore it was unable to be set.

#### *HA & NSRP*

- **cs10582**—After upgrading from ScreenOS 5.0, the **set nsrp monitor int mgt** CLI command became invalid.
- **cs09760**—When the **save config all** CLI command was issued from an NSRP peer device, it saved only a global configuration. Non-global configuration commands, such as **manage-ip**, were lost.
- **cs08526** — Read and Write administrator privileges were functioning incorrectly for the **set nsrp** CLI commands.
- **cs09404**—(ISG 2000 and ISG 1000) When a lot of sessions were synchronized between the active and backup NSRP devices, sometimes performance would drop and the device restarted.

- **cs05206**—Running in Transparent mode with an NSRP Active-Passive configuration, sometimes incorrectly handled VPN decrypted packets, which then caused an error when the device restarted.
- **cs10465**—A backup device would not be 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.
- **cs04112**—In an NSRP environment, sometimes the interfaces used the physical MAC address instead of the virtual MAC address.
- **cs04430**—In an NSRP Active-Passive environment, with tcp-syn-check and holddown time configured, FTP traffic might stop when traffic was reverted from a backup to a primary device.

***Management***

- **cs10113**—When multiple interfaces were bound to the Trust security zone, the device would send the Webtrends log to the last source interface created.
- **cs10454**—(ISG 2000) The SNMP MIB **iftype** returned a value of **other** for the Gigabit interface.

***Other***

- **cs08570**—SQLv2 traffic did not pass through the device when ALG was enabled.
- **cs08897**—(ISG 2000) GTP version 0 functioned incorrectly.
- **os58621**—(ISG 1000 and ISG 2000) The device handled packets with TTL=1 incorrectly. Initially it returned TTL exceeded packets, but if it received the same packet again, it decremented the TTL to 0 and passed the packet the device. This issue was specific to pass IPSec packets.
- **cs09139**—In some configurations, PPPoA connection failed to automatically re-connect after a device was restarted. Manual re-connection through the WebUI was required.
- **cs09683**—In some cases, multicast prune messages were sent incorrectly during a switch over from Shared Tree to Shortest Path Tree (SPT).
- **cs10224**—Enabling some memory debugs caused the devices to be inaccessible.
- **os58124**—(ISG 1000 and ISG 2000) Packets were handled incorrectly when DF bit was set. For example, if the device received a packet that was larger than the MTU and the packet also had DF bit enabled, the device would send a Fragment Needed message to the client. The device also created a session for this rejected packet. The device would continue to receive packets on this session and would continue to pass the packets.
- **cs09979**—(NetScreen-5000 Series) Running in Transparent mode, when aggregate interfaces were configured, pings greater than 1419 bytes failed.

- **cs09570**—(ISG 2000 and ISG 1000) The device experienced a period of high CPU usage when a new multi-cell policy was added through the WebUI.
- **os60115**—(ISG 1000 and ISG 2000) With IPv6 enabled, due to an internal memory error, the device would restart when a policy was configured through the WebUI.

***Performance***

- **cs09795**—Traffic failed to pass through the device after the ISP central office restarted the PPPoA connection.

***Routing***

- **cs08940**—The **get vr mroute** CLI command would sometimes incorrectly display the same source for multiple interfaces.
- **cs09553**—(ISG 1000) The device did not forward PIM-BSR messages over a tunnel.
- **cs08884**—Due to an incomplete internal GTP tunnel deletion process, the device would intermittently restart.
- **cs10766**—After a device was restarted, some information in an IGMP configuration was lost.
- **cs10029**—(ISG1000 and ISG 2000) A Contivity device is unable to establish a BGP peer because the unsupported optional parameters response was handled incorrectly.

***Security***

- **os64441**—Modifications were made to allow for future attack db updates. The attack URL has changed from https://services.netscreen.com/restricted/sigupdates/5.3/attacks.bin to https://services.netscreen.com/restricted/sigupdates/5.3u/attacks.bin.

***VOIP/H323***

- **cs07333**—A device might fail due to a Q931 session being setup incorrectly.
- **cs09655**—An internal error caused the device to fail when processing VoIP traffic.
- **cs08143**—A device failed with the error **###SIP callinfo dead loop** when H.323 ALG was enabled.
- **cs10757**—In rare circumstances, SIP traffic caused device failure due to a failed null pointer check.
- **cs08480**—In some cases, H.323 audio does not work when calls are received and placed from the same interface or zone.

***VPN***

- **cs10155, cs10550**—(NetScreen-5GT WLAN) In some environments, policy-based VPN tunnels using certificates did not connect.

- **cs09064**—In a hub and spoke route-based VPN environment, where AV was enabled on the hub, AV scanned spoke-to-spoke traffic was dropped.

#### *Web UI*

- **cs10931, cs10589**—Portions of an IGMP configuration were lost after the device was restarted.
- **cs11200**—In an NSRP environment, adding and removing addresses or services in a multicell policy and/or enabling or disabling a policy did not synchronize with the NSPR peer.

### *Addressed Issues from ScreenOS 5.3.0r4*

#### *Administration*

- **cs07271, cs09504**—When using RADIUS Authentication, after the third device login try, an error occurred when the device was restarted.
- **cs07855**—Unable to unset a user when a user was in use. This restriction was due to the user entry being improperly removed if the user group was deleted before deleting the user.
- **cs08084**—(ISG 2000) In an NSRP environment, excessive NSRP session messages sometimes caused an error on the backup device when it was restarted.
- **cs08188**—In some cases the device may reset processing particular Real Media streams.
- **cs08222**—The system clock lost time.
- **cs08507**—The error message **system error 00556 UF-MGR: UF key expired** was posted to the event log every 20 minutes after the default Web-Filtering key expired.
- **cs08670**—The **unset admin hw-rest** CLI command was not saved after a device was restarted.
- **cs09055**—The error **too many entries** was received when a new service group was created and the error **set service failed** was received when a new policy with multiple services was created.
- **cs09174**—When an administrator hung up a dial connection through the WebUI, the pop-up message **You do not have the privilege** was incorrectly displayed.
- **cs09468**—When a member was added to a group and the ASIC rules were exhausted, an error or warning was not returned. This addition would cause some policy ASIC rules to not be installed and packets to be dropped from the configuration.
- **cs09803, cs08337, cs07883, cs10381**—Zone names containing spaces stored incorrectly.

- **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.

***Antivirus***

- **cs08993**—The device was unable to download AV signatures using HTTPS in FIPS mode. This action caused an update failure with a non-specific error (-11).
- **cs09559**—(NetScreen-5GT Series) A new Kaspersky AV pattern file would not download if an existing pattern file of greater than 10 MB existed in flash memory.

***HA & NSRP***

- **cs10340**—Internal resources were release incorrectly, causing devices in an NSRP environment to failover.
- **cs04991**—An NSRP cluster did not recover from failover when a Run Time Objects (RTO) sync was used.
- **cs07086**—An administrator user with the **all** privilege could not configure NSRP.
- **cs07279**—In an NSRP Active-Passive configuration, a message was displayed on the console every 5 to 10 minutes indicating a session corruption pointer on the backup device.
- **cs07737, cs04359**—In a dual-untrust NSRP VPN configuration, unplugging one of the untrust interfaces could generate high CPU usage until the next rekey occurred.
- **cs08937**—(ISG 2000) In an NSRP cluster, unsetting a subinterface could change the MAC address from the virtual MAC to the physical MAC.
- **cs09523**—In an NSRP environment, Real Time Streaming Protocol (RTSP) packets sometimes caused an error when the device was reset.
- **cs10187**—When subdirectories existed, the data when using the **exec vfs ls flash:** CLI command was displayed incorrectly.

***Management***

- **cs03147**—In some cases, when a device was in Transparent mode, clicking on the policy screen caused device failure.
- **cs07029**—The device had high CPU usage when syslog and policy logging were enabled.
- **cs07107**—The devices would not connect to the NetScreen-Security Manager Server after the DevSvr MIP IP was changed.
- **cs07433**—(NetScreen-HSC) The **get log sys save** CLI command improperly displayed trace dumps.

- **cs07863**—Issuing the **bulkcli** CLI command to change a device configuration sometimes broke the NSM connection.
- **cs08183**—An SSH login attempt stopped the debug process.
- **cs08237**—The untrust interface did not return to the original state after failover when track-ip was enabled.
- **cs08408**—The user could not connect to a device using SSH when RADIUS authentication was enabled.
- **cs08878**—An internal NSM configuration error caused device failure.
- **cs08978**—Time stamp was incorrect in the Websense log report.
- **cs09825**—After a device was upgraded from firmware version 5.1.0 to 5.3.0, the VLAN zone changed to a shared resource. The zone could be changed back to non-shared, but if the device was managed using NSM, the administrator should ignore the **validation error**.
- **os55569—**Event log entries were inadvertently emitted for every successful SNMP get command.
- **os60977**—Severity information for deep inspection (DI) was categorized incorrectly.

***Other***

- **cs02529**—The VLAN capacity increased to 128 VLANs when an extended license key was used.
- **cs05221**—Issuing the **delete ssh device all** CLI command when troubleshooting an SSH issue could cause the device to restart.
- **cs05461**—(NetScreen-5000 Series using the 5000-M2 management module) Sessions with Time To Live (TTL) of 0 would not age out.
- **cs06917**—In some cases, specific fragmented traffic caused device failure.
- **cs07724**—Traffic was dropped if designated for a multi-cell policy that followed an Remote Procedure Call (RPC) deny policy.
- **cs08087**—In a PPPoE environment, the device could occasionally restart with an error when receiving large packets of IPv6, IPX, etc.
- **cs08119, cs09399**—With MSRPC ALG enabled, a device would restart with an error when very large actual_count MSRPC messages occurred.
- **cs08427**—(NetScreen-5XT) In a dial-backup configuration, connection using the modem port was not always successful when the modem idle time was set to 0.
- **cs08439**—Network Time Protocol (NTP) on the device would be incorrectly updated if an NTP server replied twice to a single NTP update request.

- **cs08554**—(NetScreen-5200 using 5000-M2) Sometimes, an active FTP connection intermittently stopped.
- **cs08722**—RTSP traffic passing through a device could cause the device to hang and the error **wrong rms buf len, Trace** to be displayed on the console.
- **cs08787**—In rare cases, having sequence checking enabled caused device failure.
- **cs08804**—A PPPoE interface failed to establish connection when there were two PPPoE instances configured on different physical interfaces. For example, one interface was bound to ethernet3 (Untrust zone), and the other was bound to ethernet2 (DMZ zone). Under this configuration, once the PPPoE connection on the ethernet2 was terminated, it could never be re-established when the error message **failed to set PPPoE interface gateway** occurred.
- **cs07418, cs07754, cs07921**—SQLnet V2 traffic was dropped when a specific SQL policy was configured.
- **cs09036**—The device reset with an error when SecurID was used with the New PIN Mode.
- **cs09108**—The **create PDP context** response packet was incorrectly dropped.
- **cs09431**—(NetScreen-5000 Series using 5000-8G or 5000-2G24FE SPMs) 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.
- **cs09478**—Random high task CPU occurred after GPRS Tunneling Protocol (GTP) was configured.
- **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.
- **cs10146**—While a PPP issue was being debugged, the device reset with an error if the PPP access profile contained characters that could not be displayed in the debug output. For example, Chinese characters.

***Performance***

- **cs02916**—A device would have poor performance when URL scanning and AV were running simultaneously.
- **cs07605, cs08157**—(NetScreen-5200 using 5000-M management module) Sometimes, the device gradually ran out of memory.
- **cs07944**—In some cases, certain traffic delayed the device until it was restarted.

- **cs09025**—(NetScreen-5200) Some traffic configurations could lead to a mismatch between sessions maintained in the software and in the ASIC, which then resulted in device failure.

***Routing***

- **cs02991**—A static route, which was configured as the preferred route, did not take precedence over a connected route.
- **cs08681**—With Internet Group Membership Protocol (IGMP) Proxy configured, multicast connections would timeout after 10 seconds.
- **cs08895**—Routes were improperly removed from vsys sub-interfaces, until the device was restarted.
- **cs09290**—Changes to an access-list that was used for route-export, resulted in a flap for each route exported. Therefore, the Link State (LS) update was sent with LS age set to 3600 before another update was sent with the age set to 1. This led to a brief disruption in traffic flow.
- **cs09820**—In a vsys configuration using IP-classification, the device incorrectly handled a vsys route lookup.

***Security***

- **cs05561**—Patch to provide support for latest version of Verisign OSCP certificate.
- **cs07747**—The RADIUS authentication failed if the Access Accept authentication string exceeded approximately 700 bytes.
- **cs08510**—A device might restart with an error when the initial NSM configuration push included web filtering.
- **cs08754**—In Transparent mode, the Syn Cookie feature worked incorrectly.

***VOIP/H323***

- **cs06575**—In some cases, fax communication with H.323 failed but voice worked.
- **cs08370**—In some VoIP environments, the device stopped passing traffic after approximately 2 to 3 days, then the ARP table might only contain a few entries.
- **cs08922**—In some cases, H.323 sessions were not cleared in the session table.

***VPN***

- **cs07903**—VPN traffic failed to pass when a route-based VPN had the loopback interface configured as the outgoing interface and put a sub-interface as part of the loopback group.
- **cs08074**—A device might drop VPN traffic when replay protection was enabled.

- **cs08221**—A NetMeeting session might not connect across a policy-based VPN between a security device and a PIX device.
- **cs08786**—A device might fail if a VPN tunnel was removed while other tunnels were using the same Security Association (SA).
- **cs08792**—(NetScreen-5000 Series) In a GPRS environment, the device restarted with an error when a new VPN gateway was configured.
- **cs08905**—Memory resources were improperly reclaimed after VPN phase2 negotiations.
- **cs08913**—For configurations with a large number of IKE ID users, the device might restart with an error when a CLI command was entered.
- **cs08975**—Memory resources were improperly reclaimed when using PKI certificates.
- **cs09123**—Dial-up VPN peers with Source Interface-Based Routing (SIBR) and Src-NAT were unable to communicate with each other.

***Web UI***

- **cs06422**—Editing an SNMP community host configured with a non /32 subnet mask resulted in an **Invalid Address** error.
- **cs06889**—A device failed when the policy counter graph was viewed using the WebUI.
- **cs07859**—HTTP requests decreased and sometimes failed when surfcontrol was enabled because there was not enough sockets being allocated on the device.
- **cs08169**—Only the first 20 multicast routes were displayed even though the number of entries to be displayed had changed.
- **cs08856**—With DI enabled, after device startup, the device cannot be managed using the WebUI.
- **cs08894**—Configuring a VPN policy with a pre-defined service group (for example, H.323 or SIP) conflicted with a VPN policy using ANY as the service. The following error message might occur during configuration, **The new policy id<14> has identical IKE ID as that of policy <12>**.
- **cs10145**—In some cases, when configuring the device using HTTPS WebUI, an ISP account password became corrupt.
- **cs10239**—If an alternate telephone number is used in a dial-up connection to the ISP, the WebUI incorrectly indicated that the primary number was used.

## *Addressed Issues from ScreenOS 5.3.0r3*

- **cs04092**—When converting a policy to a set of rules, the ASIC sometimes used a conversion algorithm that created a different number of rules than had previously been generated for the same policy.

- **cs04221**—(WebUI) The **remove** option did not remove a CA certificate.
- **cs04334**—Setting traffic to a vsys had problems. Debugging the device indicated that traffic going to the vsys was incorrectly classified to the root vsys.
- **cs04457**—A disabled IKE user could successfully connect through the VPN.
- **cs04522**—Incoming mail did not pass through a MIP when AV was enabled.
- **cs04553**—Occasionally, packets were routed incorrectly even though they matched the session.
- **cs04819**—An IGMP proxy to multiple host interfaces for the same group was disallowed.
- **cs04978**—(WebUI) Antivirus information was incorrectly contained as **Recent Event** information.
- **cs05284**—Sometimes, after a device was restarted, policy-based VPN tunnel, with SRC-NAT and DIP configured, was inactivate due to an incorrectly set proxy-ID.
- **cs05471**—The discard counter would increment improperly.
- **cs05515**—The **get service any** CLI command displayed the default timeout value as one minute.
- **cs05733**—In some cases, a track-ip ping response was lost.
- **cs05738**—(WebUI) The Local Auth server timeout field was incorrectly limited to a three digit value when the value should have been four digits.
- **cs05903**—A session failed when DI was enabled and the DI was unable to handle half-close state.
- **cs05981**—(WebUI) An error occurred when deleting an aggregate interface or sub-interface.
- **cs06161**—(ISG 2000) In Transparent mode, configuring a large number of policies resulted in a policy look up timeout and dropped packets.
- **cs06240**—Source-based NAT did not occur on traffic from Trust to DMZ security zones.
- **cs06295**—There device intermittently failed due to policy database failure.
- **cs06297**—In some cases, the RADIUS authentication over policy based tunnels stopped working.
- **cs06441**—The antivirus option was unavailable when a policy was configured for multi-cell context.
- **cs06990**—Corrupt mis-interpreted and mis-directed HA messages caused the backup device to coredump and lose connectivity with the primary device.

- **cs06991**—(NetScreen-50) A device coredump and restart occurred in an NSRP Active-Passive configuration, when a secure-ID user inserted a long user name and password.
- **cs07059**—DHCP requests from clients on untrust side of any device in Transparent mode acting as VPN initiator was relayed to a DHCP server behind the VPN responder through the VPN tunnel.
- **cs07101**—DSCP marking for IPSec pass through traffic in route mode worked improperly.
- **cs07132**—Dial backup did not work (modem does not return dial) due to PPPLCP keepalives not being sent.
- **cs07133**—Sometimes there were a few differences on SA's SPI between Master's SA and Backup's SA when running the NSRP hot-sync.
- **cs07177**—After an IGMP configured sub-interface had participated in multicast, it could no longer be deleted or assigned to the null zone.
- **cs07178**—In some cases, IPSec sessions were not cleaned in the session table resulting in VPN failure.
- **cs07217**—Modifying or adding an L2TP policy corrupted the system configuration.
- **cs07218**—(WebUI) When modifying a policy ID and adding a service of ICMP-any to the Untrust to Trust policy, the device reloaded with a software forced error.
- **cs07259**—(NetScreen-200 Series) Sometimes a device failed due to an ALG cookie between MSRPC and H.323 because the NAT cookie allocation and free process were unprotected.
- **cs07295**—The **exec policy verify** CLI command returned incorrect results.
- **cs07301**—(ISG 2000) When using slow speed links, latency caused fragmented packets to be re-assembled incorrectly in the device because small fragments arrived fast but large fragment takes too long.
- **cs07354**—(NetScreen-5XT) Issues occurred when a device was upgraded from 4.0 to 5.3.
- **cs07402**—(NetScreen-5GT) When a device was configured as a DHCP client and connected to DHCP Server A but was disconnected from DHCP server A and connected to DHCP server B on a different network, the system continued to try to renew its IP address with the older network to which it was previously connected.
- **cs07425**—Under certain circumstances in an NSRP configuration, the device suddenly stopped forwarding traffic, and the ARP table was empty. The device was unable to ping other hosts. This problem also caused the NSRP configuration to not failover to the backup device.

- **cs07462**—SSL based FTP server was inaccessible when AV was enabled on the policy.
- **cs07488**—(ISG 1000 and ISG 2000) NSM returned a error when trying to set physical link-down of any interface.
- **cs07508**—In some cases, during IKE negotiation, device failure occurred when the IP ID was generated.
- **cs07519**—In an ECMP configuration, when devices were connected through more than one point-to-point physical link, OSPF advertised next-hop as 0.0.0.0 instead of the actual IP address.
- **cs07562**—In some situations, when processing BGP updates, a second withdrawn message was sent 30s after the first withdrawn message.
- **cs07614**—When multiple services were added to a policy, a hidden service group was created, members of which were the services attached to the policy. When a user removed the custom defined service, a hidden service group without a member was left. Under this circumstance, when a user tried to access a member, the device failed.
- **cs07623**—Inter vsys routing was handled improperly.
- **cs07627**—In a route based VPN multi-VR environment, the security device incorrectly performed a route lookup in the wrong VR.
- **cs07633**—Out of order TCP packets caused a lot of TCP Seq check failed error messages. These messages led the debug buffer to fill up because the debugging capability was hindered.
- **cs07637**—When an FTP client established the connection with an FTP server through the device, the device created a stand-alone FTP data session, but did not create FTP control sessions for the child session.
- **cs07660**—Passive FTP traffic was translated incorrectly.
- **cs07661**—Interface last_change attribute was sometimes displayed incorrectly and was not updated when the interface state changed to up.
- **cs07729**—An ARP packet buffer was increased to improve performance.
- **cs07760**—(WebUI) Having the same IP address for interface Track IP and NSRP Track-IP was not permitted.
- **cs07772**—Internal mishandling of H.323 traffic caused device failure.
- **cs07803**—While using Web Authentication, the vsys pointer for a secure-id path was set improperly, causing response failure. This action resulted in a Web Auth failure inside a vsys.
- **cs07814**—A device failure occurred when user configured the ninth DHCP server.

- **cs07816**—In some cases, CPU utilization displayed a spike due to ARP aging out incorrectly.
- **cs07839, cs54021**—In some cases, invalid or malformed VLAN packets caused device failure.
- **cs07871**—The device failed while handling ISAKMP packets with invalid and/or abnormal contents.
- **cs07880**—A device could fail when viewing the log entries with the WebUI.
- **cs07884**—(NetScreen-5200) The **get log sys saved** CLI command sometimes displayed trace dump on the device console.
- **cs07887**—(NetScreen-25) The device failed to ping to a local interface due to failure in freeing the allocated net-pak and caused failure in getting ICMP response from local subnets.
- **cs07888**—In some cases, outbound SIP calls caused device failure.
- **cs07931**—The device passed traffic incorrectly when using address groups.
- **cs07964**—In some cases, the device failed when issuing the **debug flow** CLI command.
- **cs07995**—When a user upgraded from 5.1.0pw7.0 to 5.3, there were problems passing traffic to a VPN site behind a NAT firewall.
- **cs08032**—Internal mishandling of RADIUS traffic caused device failure.
- **cs08053**—(NetScreen-204) The **unset nsrp vsd-group id 0** CLI command required that the device be reset if there was any interface assigned to the MGT zone.
- **cs08066**—Unresolved unicast route had a missing null pointer check which caused device failure.
- **cs08073**—An internal task incorrectly increased the CPU usage.
- **cs08077**—A high amount of VPN tunnels and traffic caused device failure.
- **cs08079**—Dial Line remained open even though there was no interesting traffic as idle timer was reset every few seconds.
- **cs08080**—(WebUI) When a user clicked the **hangup** button on the Modem-Trustee page, the serial interface was brought down. This button should only disconnect the modem, not bring down the interface.
- **cs08085**—(WebUI) While entering a TCP port with a trailing blank into the custom service page, the firewall set the port to 0 without providing errors.
- **cs08109**—The device accepted the default route on the serial interface through the PPP connection made which resulted in the leakage of data through the default route if no other route was available to send traffic.

- **cs08113**—In some cases, the device management was delayed after about an hour.
- **cs08161**—Syn cookie mechanism was working incorrectly on logical interfaces.
- **cs08164**—Due to incorrect storage of buffer packet for reassembly, a device would restart and display the console error: ### No DIMM found on board ###
- **cs08256**—(NetScreen-5000 Series) The **get flow** CLI command incorrectly displayed that the rcp-rst-invalid session was unsupported.
- **cs08257**—(NetScreen-5GT) Due to possible zero length option or EOL which processing TCP header options, the device performed a coredump on the console after downloading an image/file from any TFTP server.
- **cs08265**—Overlapping UDP customer service port range with IKE port (UDP port 500) caused incorrect session timeout for IKE sessions.
- **cs08279**—(WebUI) After configuring an Xauth local authentication user group, the **CHAP Only** was automatically selected and it was impossible to disable it.
- **cs08293**—Sometimes an internal error page was displayed when a page was browsed with a zero byte content length and the connection was closed by the server.

### *Addressed Issues from ScreenOS 5.3.0r2*

- **cs07871**—A check was added to address vulnerability issue with implementation of the ISAKMP protocol.
- **cs07979**—When generating a P1 gateway, it was impossible to select dynamic mode VPN and a distinguished name from the WebUI.
- **cs53319**—When using a Linux FTP client/server, FTP timeout occurred when sending files larger than 5 MB.
- **cs53388**—Established VPN UDP sessions kept using the old route even after the route was changed.

## Known Issues

This section describes known issues with the current release.

- Limitations of Features in ScreenOS 5.3.0 identifies features that are not fully functional at the present time, and will be unsupported for this release.
- Compatibility Issues in ScreenOS 5.3.0 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 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 5.3.0*

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

### Limitations in ScreenOS 5.3.0r6

Custom Dynamic DNS is not supported.

### Limitations from ScreenOS 5.3.0r3

The FTP extended passive mode is not supported.

### Limitations from ScreenOS 5.3.0r2

- 500 NSM with DI enabled—Users may experience issues when downloading configuration files larger than 1.7 M.
- 5000 Series Vsys Capacity—The following table describes the number of virtual systems ScreenOS supports for each 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 |

- Limitations of the AV Scanner—The following lists basic troubleshooting items and limitations of the AV scanner:

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

  - AV session is aborted.
  - Default route is required for AV to function in transparent mode.
  - The av scan engine may not be able to detect a virus if the virus is fragmented and transferred into multiple network objects.
  - 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, it is advisable to reduce the maximum size file to 6 MB. If AV, DI, and Web filtering are all enabled, it is advisable to reduce the maximum size file to 4MB.

- **Dead Peer Protection**—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.
- **(NetScreen-200 Series) Deep Inspection**—Installing the Deep Inspection (DI) license key on the NetScreen-200 in advanced mode decreases the maximum number of sessions to 64,000 sessions. To restore the number of sessions supported to 128,000 sessions, remove the DI license key and reboot the security device.

### *Compatibility Issues in ScreenOS 5.3.0*

Below are the known compatibility issues at the time of this release. Whenever possible, a workaround (indicated with **W/A**) has been provided for your convenience.

Compatible browsers—The WebUI for ScreenOS 5.3.0 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 Paths from Previous Releases

**Upgrade sequence**—We recommend that you follow the upgrade instructions described in Migration Procedures. If you upgrade directly from ScreenOS 5.0.0 or ScreenOS 5.1.0 to ScreenOS 5.3.0, you risk losing part of any existing configuration. For NetScreen-500 and ISG 2000 devices, you must upgrade to an interim firmware image before upgrading to the 5.3.0 firmware image.

**WebUI upgrade**—Due to a buffer size issue when upgrading from ScreenOS 5.2.0 to ScreenOS 5.3.0 using the WebUI, you must upgrade to an interim firmware image before upgrading to the 5.3.0 release image. See Upgrading to the New Firmware for instructions on how to perform the upgrade.

## *Known Issues in ScreenOS 5.3.0r8*

The following are known deficiencies in features at the time of this release. Whenever possible, a workaround is suggested following the problem description. Workaround information is indicated by **W/A**. If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

### Admin

- **cs09826—**When a global deny policy is created, with a service group and an FTP-GET or FTP-PUT is added, the policy behavior changes. FTP-GET and FTP-PUT must be used in individual policies. For additional information, refer to the Knowledge base article KB3692.

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

- **cs12498, cs12527—**The device generates an IP spoof alarm if traffic is going to the device when starting up after a reset.

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

- **cs10664—**When adding an interface to a security zone, then adding a second interface, the default interface for the zone changes to the newly added one. If you then remove and re-add the first interface the default

interface follows the latest one added (first interface) until a reset; in which case it will then revert back to the second interface.

### Antivirus

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

### HA & NSRP

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

- **cs13153—**The secondary firewall in an NSRP configuration shows high CPU caused by RTSP traffic on the primary device. This creates many Sess_ch messages to the secondary.

- **cs13586—**In a VSD-less high availability configuration, sessions are not aged-out when "ageout-ack" option is enabled for RTO session synchronization.

### Management

- **cs10231—**When using NSM, vsys update fails due to a command NSM sends to the device which does not exist at the vsys level.

- **cs09777—**Device cannot connect back to the NSM Primary server after an NSM failover, if the device was originally added to the active NSM secondary server.

### Other

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

- **cs08452—**In some cases certificates may fail due to CDP parsing.

- **cs12194—**In some cases on the ISG 2000, FTP data transfers do not complete in an A/P NSRP failover.

- **cs11207—**The character "!", is not supported as a negative policy delimiter.

- **cs11001—**[NetScreen-25/50, 200, 500] Under isolated circumstances, most often associated with the use of MIPs, traffic may drop even when a policy is set to allow it.

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

**Performance**

- **cs12606—**[NetScreen-5000 and ISG] An internal error on these high end platforms caused net-pak buffer leak (get net-pak s shows missed / failed counter increasing at a high rate) causing the split-brain issue.

- **cs12583—**In some cases, browsing may be slower when using Websense URL filtering.

**Routing**

- **cs13160—**Large multicast packets were not sent through the tunnel when path-mtu is enabled.

**VPN**

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

- **cs12968—**Get SA shows A/I on the backup firewall in NSRP lite, I/I expected.

- **cs09155—**VPN monitor status not correct due to a small period where a notification event gets lost. This results in the tunnel interface state not getting updated correctly.

## *Known Issues from ScreenOS 5.3.0r7*

### *Administration*

- **cs09826—**When a global deny policy is created, with a service group and a FTP-GET or FTP-PUT is added, the policy behavior changes. FTP-GET and FTP-PUT must be used in individual policies. For additional information, refer to the Knowledge base article KB3692.

- **cs06320—**Self-originated NTP and RADIUS authentication traffic is not treated as through traffic; thus no policy checking will be performed. Change to this behavior is considered as an enhancement request.

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

- **cs09803, cs08337—**Zone names containing spaces are not correctly stored. **W/A:** Do not use spaces when creating zone names. Example: "Test Zone" will not be saved correctly, use "Test_Zone" instead.

- **cs07471—**WebUI does not display the first custom attack group that is configured; it is only displayed via the CLI.

- **cs12013—**When executing an SNMP walk of the device, the vlan interface is reported incorrectly. The administrator status shows up even though the true status is down.

- **cs09740—**When upgrading from 5.2 to 5.3, a two-step upgrade process is required. Customers upgrading from 5.2r2 to 5.3r3 may encounter an exception error when performing the second step of the upgrade process; upgrading from 5.3.0 up to 5.3r3. **W/A:** Upgrade to 5.3r2 first then upgrade to 5.3r3.

- **cs07360—**Using OpenSSH with ServerAliveInterval enabled causes disconnects.

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

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

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

- **cs12498—**The device generates an IP spoof alarm if traffic is going to the device when starting up after a reset.

- **cs08493—**Incorrectly receiving "VIP server down" event alarm messages.

- **cs07352—**Running the command "set firewall log-self exclude" without any options does not stop logging of the packet types for which logging is enabled. To disable it, specify the type of packet as well.

  **Example:** set firewall log-self exclude <packet type>

  | | |
  |---|---|
  | icmp | log icmp packets to self |
  | ike | log ike packets to self |
  | multicast | log multicast packets to self |
  | snmp | log snmp packets to self |

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

- **cs07760—**The WebUI does not permit use of the same IP address for the interface Track-IP and the NSRP Track-IP.

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

- **cs07454—**PPTP with PAT causing authentication errors when the ALG is enabled.

- **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.

- **cs07783—**After removing a DNS cache host table, you cannot create a new entry until the device is restarted.

***Antivirus***

- **cs08677—**In some cases, with AV enabled, the message "Wrong etype in netpak" would be printed to the console. Eventually the device would fail and must be power cycled.

- **cs09804—**Please refer to cs09559 from “Addressed Issues From 5.3.0r4”.

- **cs05947—**Downloading large files, in some cases, leads to a system failure.

***DHCP***

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

***DNS***

- **cs07687—**Special characters are not allowed in the domain name string command. In the following example, the "*" is not allowed: set address "Untrust" "*.DTDS.ZXCWWW.COM" *.DTDS.ZXCWWW.COM "DTDS Service".

***HA & NSRP***

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

- **cs05475—**In some cases an NSRP master device will fail when a policy accesses the wrong memory location.

- **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.

- **cs05447—**During a cold start sync of a secondary NSRP A/P device, a portion of the sessions were dropped if there was more than 30,000 sessions.

- **cs12605—**In an NSRP configuration, GTP messages could be misinterpreted, causing the device to reset.

- **cs11011—**In an NSRP configuration the primary device could reset if the device incorrectly interprets the wrong session.

- **cs09777—**After an NSRP failover, in some cases, the new primary device had issues reconnecting to the NSM server.

- **cs06410—**A firewall device configured for NSRP in transparent mode may experience high CPU and/or reset with an error due to an incorrect session handling.

***Management***

- **cs09681—**When an update from NSM is performed, if the interface goes down, the device fails.

- **cs10231—**When using NSM, vsys update fails due to a command NSM sends to the device which does not exist at the vsys level.

- **cs12566—**Read-only administrator cannot issue 'get' commands.

- **cs10475—**With SSH v1 enabled, SSH or WebUI management of the device could fail after several days. This is to due to resources not getting released correctly. **W/A:** Enable SSH v2 instead of v1.

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

- **cs12281—**In some cases, subinterfaces are not imported into NSM correctly.

- **cs05615—**Overuse of administration leads to manageability issues.

- **cs09825—**After a device was upgraded from firmware version 5.1.0 to 5.3.0, the VLAN zone changed to a shared resource. The zone could be changed back to non-shared, but if the device was managed using NetScreen-Security Manager, the administrator should ignore the "validation error".

- **cs08434—**After upgrading ScreenOS from 5.2.0r3.0 to 5.3.0r2.0, NSM update fails while sending "set di service" commands.

- **cs07753—**Authentication resources were not being freed correctly and was affecting remote administration.

- **cs10425—**Configuring an SNMP host address of x.x.x.255 produced an “invalid IP address” error.

- **cs12801—**In some cases, when updating the certificate for one vsys using NSM, another unrelated vsys certificate may be removed.

- **cs09895, cs06275—**In some cases, an internal memory pointer causes the device to fail.

***Other***

- **cs07979—**When generating a P1 gateway, it is not possible to select dynamic mode VPN and a distinguished name from the WebUI. **W/A:** Use the CLI.

- **cs03910—**Some CDMA wireless modems are unable to dial out as a dial backup.

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

- **cs08452—**In some cases certificates may fail due to CDP parsing.

- **cs10159—**RTSP traffic is dropped when using a MIP. W/A Disable the RTSP ALG.

- **cs11750—**In some cases, with URL filtering enabled, the CPU usage may increase when syn-check is enabled. **W/A:** Unset tcp-syn-check---

- **cs06959—**If traffic is being sent through a policy and the policy settings are modified, the firewall will permit traffic through using the original setting until the device is reset. Example: Original policy "set pol id 2 from untrust to trust any mip(2.2.2.1) any tun vpn vpn pair-policy" modified to "set pol id 2 from untrust to trust any mip(2.2.2.1) any tun vpn vpn pair-policy" will permit traffic through to the MIP until the device is reset.

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

- **cs12037—**The device does not take window scaling into account when sequence checking is enabled.

- **cs10064—**In some cases, the device would stop passing traffic due to an internal buffer being stuck.

- **cs07492—**The firewall may stop responding for a period of time when a custom service timeout that is referenced in a policy is changed.

- **cs07726—**If a NetScreen-5x00 in transparent mode is receiving high numbers of fragmentation errors, it may occasionally reset with the error "Illegal Data Access Address".

- **cs12194—**[ISG 2000]In some cases, in an A/P NSRP environment failover, FTP data transfers do not complete.

- **cs09764—**When using the mtrace command, replies were not reporting correctly.

- **cs07819—**TCP sessions take 10 seconds to clear the session table upon receipt of the FIN packet.

- **cs11207—**The character "!", is not supported as a negative policy delimiter.

- **cs04937—**Ping is enhanced to handle duplicated ICMP echo responses.

- **cs10982—**After exicuting the "unset all" command (clearing the confiuration) the device has issues setting the URL cache size back to 1000.

- **cs12755—**When using the WebUI in and NSRP environment, after creating one redundant interface and creating a second redundant interface, it is not possible to assign priority using the WebUI. **W/A:** Use the CLI to configure the priority.

- **cs03880—**If "save" and "unset" operations are performed on a vsys by different users, traffic will stop flowing.

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

- **cs07071—**In some cases, an internal pointer error caused the device to fail.

- **cs08064—**Slow responding HTTP packets dropped with DI enabled.

- **cs10180—**DNS refresh schedule time was unreliable.

- **cs11001—**On legacy NetScreen-25/50, NetScreen-200 & NetScreen-500 series devices, under isolated circumstances most often associated with the use of MIPs, traffic may drop even when a policy is set to allow it.---

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

- **cs09713—**In some situations, a GTP PDP content response could be dropped.

- **cs09895, cs06275—**An inconsistency existed in counting total address and service groups when used in a multi-cell policy.

***Performance***

- **cs12583—**In some cases, browsing may be slower when using Websense URL filtering.

- **cs02161—**The "set flow max-frag-pkt-size" CLI command is not applicable for high-end firewall devices.

***Routing***

- **cs10883—**In a Windows Server 2003 environment, TFTP through the firewall would fail due to the ALG handling.

- **cs09563—**Packets traversing a route-based VPN to a MIP in the trust zone are not correctly redirected to the MIP IP if that IP is mapped to a device in the DMZ zone.

- **cs03616—**BGP peering is changing states from down to established, due to the keep-alive timer expiring. When in this state the device will eventually fail.

- **cs09642—**When using RIP, if the connected network address matches up to the 4th octet, even when subneted, the packets are dropped.

- **cs09968—**[ISG 1000] After the IDP is enabled by an NSM policy push, the device stops forwarding packets. This is caused by a combination of fragmented packets (TCP & UDP) with a TTL value of 1.

- **cs10240—**In some situations, a GTP PDP content response could be dropped if an EchoRequest message initiates the GTP session.

**Security**

- **cs09658—**If the RADIUS accounting port is closed, an XAuth authentication will fail. Currently authentication only of an XAuth user is unsupported. Authentication also requires accounting.

- **cs07048—**On occasion, syn-flood protection double counts the number of proxy sessions and causes false alarms.

***VOIP/H323***

- **cs12427—**Same as NSCcs10556

- **cs08777—**Microsoft Live Communications Server will not work properly with the SIP ALG enabled.

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

- **cs08683—**In some cases, not all SIP traffic is passed through the device.

- **cs09113—**SIP publish messages are dropped with the following errors posted: "Cannot parse SIP message" and "application error". The pubilsh message function is not yet supported in ScreenOS 5.3.

- **cs10905—**In some cases, incoming SIP calls have about a 10 second delay, then a busy signal occurs.

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

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

***VPN***

- **cs10658—**In some configurations, retrieval of Certificate Revocation List (CRL) information through a Lightweight Directory Access Protocol (LDAP) server fails.

- **cs07020—**Pass-through VPN tunnels may fail, due to the device sending the packets to the wrong MAC.

- **cs08903—**The second SA of a policy-based VPN sharing the same profile does not establish when using PPPoE to connect.

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

- **cs07473—**Removal of a VPN phase2 binding to a tunnel interface may cause the FW to reset with an error.

- **cs09045—**LAN to LAN VPN fails when the name resolution of one gateway (via DDNS) expires.

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

- **cs08105—**Fragmented IKE negotiation packets are dropped.

- **cs07325—**Device may fail if a VPN is already set up and then overwritten with a different VPN policy.

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

- **cs07651—**When setting up a VPN with a failover-weight, the VPN name can not have spaces. If the VPN name has spaces, upon restart the command is considered an unsupported command and is removed from the configuration.

- **cs09594—**Memory resources are not released and reclaimed correctly when GRE tunnels are used in conjunction with VPN tunnels.

- **cs10702—**When using a GRE tunnel, fragmented traffic is sometimes dropped.

- **cs09155—**VPN monitor status not correct due to small period where a notification event gets lost. This results in the tunnel interface state not getting updated correctly.

**Web UI**

- **cs08811—**The WebUI incorrectly creates a RP-candidate after enabling PIM instance on an interface. If using NSM this also affects the NSM push of a configuration.

- **cs10234—**Virtualization key only added an extra 32 vlans, not 64 vlans.

- **cs09392—**[NS-50] Not able to configure the VSI interface when using the WebUI.

## *Known Issues from ScreenOS 5.3.0r6*

### *Administration*

- cs09826—When a global deny policy is created, with a service group and a FTP-GET or FTP-PUT is added, the policy behavior changes. FTP-GET and FTP-PUT must be used in individual policies. For additional information, refer to the Knowledge base article **KB3692**.

### *Management*

- cs05462—In the NetScreen-Security Manager User Interface, the NSRP state is incorrectly displayed on the NSRP Monitor after device failover.
- cs06832—SNMP works correctly if it is sent to the manage-ip of the interface. However, if the request is sent to the interface IP, the response uses the interface manage-ip as the reply packet source address.

### *Security*

- cs09658—If the RADIUS accounting port is closed, an XAuth authentication will fail. Currently authentication only of an XAuth user is unsupported. Authentication also requires accounting.

### *VPN*

- cs10948, cs10374—In some cases an invalid or corrupt VPN session might cause the device to reset.

- cs09045—LAN to LAN VPN fails when the name resolution of one gateway (via DDNS) expires.

## *Known Issues from ScreenOS 5.3.0r5*

### *Other*

- cs10621—FTP transfers could fail when reassembly-for-alg is enabled.

### *VPN*

- cs10624—Packets are not sent out when the dial-up VPN is configured on the loopback interface in a vsys.
- cs10702—When using a GRE tunnel, fragmented traffic is sometimes dropped.

### *VoIP/H323*

- cs09113—SIP Publish messages are dropped with the following errors posted: Cannot parse SIP message and application error.

## *Known Issues from ScreenOS 5.3.0r4*

### *Management*

- cs01627—Traffic using src-port 1503 is not logged.
- os60968—(WebUI) Radio button, **Enable NSM**, works incorrectly.

  **W/A:** Use the CLI to configure NSM.

### *Performance*

- cs08776—Slow performance occurs when media files are transferred using HTTP from an Apple Mac client.
- cs09062—An incorrect route lookup occurs for traffic destined for Trust sub-interface.

### *Routing*

- cs09553—(ISG 1000) The device does not forward PIM-BSR messages over a tunnel.

### *Security*

- cs08136—For a device in Transparent mode, the Drop If No Reverse Path Route Found screen option is incorrectly listed.

### *VPN*

- cs09518—In some route based VPN configurations, packets destined for a MIP are dropped, requiring the device to be restarted.

### Known Issues from ScreenOS 5.3.0r3

- cs07833—(NetScreen-5GT Series) A device with Trend Micro Antivirus enabled does not properly handle the Active X screen option.

### Known Issues from ScreenOS 5.3.0r2

- cs07523—(NetScreen-5GT Series) The Guaranteed bandwidth feature on the device does not work properly, and causes traffic shaping failure. Low priority traffic may starve without even getting their allocated gbw in case traffic starts a little later after the device boots up.
- cs07816—In some cases, CPU utilization may show a spike due to ARP not aging out correctly.
- cs07866—Web-filtering does not work correctly with the **set flow no-tcp-seq check** CLI command enabled.
- cs07893—(NetScreen-HSC) The device may stop passing traffic when AV is enabled.
- cs08014—The device cannot establish a VPN due to port 4500 being incorrectly interpreted.

### Known Issues From ScreenOS 5.3.0r1

- cs07663—Unable to download attack db for NetScreen-25 or NetScreen-50 platforms.

  **W/A:** Replace NetScreen25-50 with NetScreen25 or NetScreen50 in the database server path. For example, with a NetScreen-25 platform, you need to enter:

  ```
  https://services.netscreen.com/restricted/sigupdates/5.3/ns25/attacks.binsn=<serial>
  ```

- cs48563—With devices that have DI enabled and experience prolonged periods of high traffic, it may occur that some sessions are not removed from the session table.
- cs48581—With a device that has a large vsys configuration, if a user changes the configuration in the vsys, it might disrupt traffic.
- cs48603—In an NSRP Active-Passive configuration with route-based VPN and UDP traffic, the traffic flow could stop after a failover to the secondary device.
- cs48642—(NetScreen-5GT WLAN) The Multitech CDMA wireless modem works improperly due to inter-operability issues.
- cs49670—If a security device passes frames larger than 1518 bytes while connected to a Cisco switch, it might increase the Out Discard (internal) counter.

- cs51841—In Transparent mode, DHCP Relay Agent works even though the server resides in the v1-trust zone and the client resides in the v1-untrust zone.
- cs51953—Video Conference calls across the firewall system using Tandberg Equipment fail.
- cs52798—In a policy-based VPN setup, if a user configures a MIP on a Tunnel interface, a device located at the other end of the VPN tunnel will not be able to ping that MIP.
- cs53100—In a scenario where the device is operating normally, when the VPN monitor detects a failure to connect, the device may use existing sessions with the wrong dest-mac resulting in failed IKE negotiation.
- cs53675—A security device generates an alarm even though the packet rate is lower than the alarm threshold, because the attack counter (syn threshold count) increases by 2 every time a syn packet is proxied.
- cs53727—In an NSRP Active-Passive configuration with a large volume of SIP calls, SIP call numbers in the primary and secondary devices might not be in sync.
- cs53904—A user cannot configure the OSPF Neighbor List using the WebUI.

  **W/A:** Use the CLI.
- cs53927—When setting up a BGP peer group using the WebUI, the device needlessly requests for a EBGP Multi-hop value.

  **W/A:** Use the CLI to configure a BGP peer group.
- cs53928—Juniper Networks does not recommend adding a new BGP peer to a BGP peer group using the WebUI. The operation might fail.

  **W/A:** Use the CLI to configure BGP peers.
- cs53930—A user cannot configure a BGP network command using the WebUI.

  **W/A:** Use the CLI.
- cs53932—On a device configured with BGP aggregate address, an attempt to access the aggregate address WebUI page causes the device to fail.
- cs54013—In a stressful NSRP Active-Passive configuration in NAT mode, after a failover, if a user terminates all SIP calls and executes the **clear sip all** CLI command on both devices, the devices might not release SIP calls, gates, and resources.
- cs54181—The AV scan engine might restart when browsing certain websites.
- cs54221—When using an Avaya IP Phone, the device might fail when the Avaya phone restarts.
- cs54223—The AV scanner currently drops SMTP emails over 7 MB.

- cs54689—Configuring a MIP through the WebUI does not allow subnet definitions.

  **W/A:** Use the CLI.

## 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 have access to these releases, you must register your security device with Juniper Networks at the above address.