Juniper Networks

Release Notes

Product: NetScreen Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen-5GT Wireless, NetScreen-5GT ADSL, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, ISG 1000, ISG 2000, NetScreen-5200, NetScreen-5400

Version: ScreenOS 5.3.0r3

Release Status: Rev A

Part Number: 530-016034-01

Date: 03-27-06

Contents

1. Version Summary

ScreenOS 5.3.0r3 is the latest release version of ScreenOS firmware for the NetScreen-5XT, NetScreen-5GT, NetScreen-5GT Wireless (ADSL), NetScreen-5GT ADSL, NetScreen Hardware Security Client, NetScreen-25, NetScreen-50, NetScreen-204 and NetScreen-208 security appliances, and the NetScreen-500, ISG 1000, ISG 2000, NetScreen-5200 and NetScreen-5400 security systems.

The ScreenOS 5.3.0r3 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 5.3.0r3.

2. Documentation Changes

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 re-add them. For dynamic routes, you need to disable the protocol then re-enable it or restart the device.

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

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

3. New Features and Enhancements

The following features and enhancements are new in this release. These features do not effect 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.*

3.1 New Features and Enhancements for ScreenOS 5.3.0r3

3.1.1 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.

3.1.2 5000-M2 Management Module Support

ScreenOS 5.3.0r3 supports the 5000-M2 management module on the 5000-Series devices.

3.2 New Features and Enhancements from ScreenOS 5.3.0r2

3.2.1 Antivirus

ScreenOS 5.3.0 supports an integrated antivirus (AV) solution on the NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-5GT Wireless, 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 trade-off 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 5.3.0 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.

3.2.2 Deep Inspection Signature Packs

In ScreenOS 5.3.0, 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 5.3.0.

Table 1: DI Signature Packs

Signature Pack	Description	Threat Coverage
Base*	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.

Signature Pack	Description	Threat Coverage
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† and primarily focuses on providing comprehensive worm protection. Detects server-to-client and client-to-server worm attacks for all protocols.

*. For NetScreen-5XT/GT with ScreenOS 5.3.0, only DI signatures of critical severity are provided due to memory allocation required for new ScreenOS features.

†. 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, 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 NetScreen-5GT NetScreen-HSC	✓*	✓	✓#	✓
NetScreen-25/50 NetScreen-204/208 NetScreen-500 ISG 1000/2000 NS-5200/5400	✓	✓	✓	✓

* We recommend using this signature pack for small/medium businesses.
# We recommend using this signature pack for remote/branch offices

3.2.3 Anti-Spam

NetScreen HSC, NetScreen-5XT, NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-5GT Wireless, NetScreen-25, 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. This release supports anti-spam for SMTP protocol only.

3.2.4 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, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500. 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. The following tables show how DSCP marking works with the various platforms. (See RFC2401 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 Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen 25/ 50, NetScreen-204/208, 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.

Description	NetScreen Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen 25/50, NetScreen-204/208, NetScreen 500	NetScreen-5000 series, ISG 1000, ISG 2000
Pre-marked packet with no marking on the policy	Retain marking in the packet.	Retain marking in the packet.
Pre-marked 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 Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen 25/50, NetScreen-204/208, NetScreen 500	NetScreen-5000 series, ISG 1000, ISG 2000
Clear packet into policy-based VPN with no marking on the policy	No marking.	Mark both the inner packet and the ESP header based on the policy.
Clear packet into policy-based VPN with marking on the policy	Only the ESP header is marked, based on the policy.	Overwrite the marking in the inner packet based on the policy and copy the inner packet marking to the ESP header.
Pre-marked 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.	The ESP header is marked, based on the policy, retain marking in the inner packet.

Table 6: DSCP Marking for Route-Based VPNs

Description	NetScreen Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen 25/ 50, NetScreen-204/208, 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.
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.

3.2.5 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 RFC3435. 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 RFC3435. 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 signalling.

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.

3.2.6 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.

3.2.7 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.

3.2.8 Service Timeout Enhancement

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

3.2.9 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.

3.2.10 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.*

3.2.11 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.

3.2.12 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.

3.2.13 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.

3.2.14 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).

3.2.15 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.

3.2.16 802.1q VLAN Tag Support on NetScreen-5GT

New supported platforms for VLAN tags are NetScreen-5GT, NetScreen-5GT Wireless, NetScreen-5GT Wireless ADSL, and NetScreen-5GT ADSL.

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 (10) 802.1Q vlan-tagged sub-interfaces.

3.2.17 Port Modes Support Wireless Interfaces

Juniper Networks NetScreen-5GT Wireless and 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.

3.2.18 New Dual/DMZ Port Mode

The NetScreen-5GT and NetScreen-5GT Wireless support 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.

3.2.19 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

3.2.20 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.

The CLI command to set a local host name is: **set dns host name** *< host_name >* *< ip_address >*

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.

3.2.21 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.

Device Model	Integrated Web Filtering Support	External Support
NetScreen HSC NetScreen-5GT NetScreen-5GT ADSL NetScreen-5GT Wireless NetScreen-25/50	YES	YES
NetScreen-204/208 NetScreen-500 NetScreen-5000 Series ISG 1000/2000	NO	YES

4. Changes to Default Behavior

This section lists changes to default behavior between ScreenOS 5.3.0r3 and the previous ScreenOS firmware releases.

4.1 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.

4.2 Deep Inspection

In ScreenOS 5.3.0, the memory pool on the NetScreen-5GT 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 CLI command, **exec attack db update**. You will get a reduced pack containing only critical signatures.

4.3 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 previous versions of ScreenOS. 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.

4.4 BGP Peers

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

4.5 Interface MTU

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

4.6 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.

5. 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.

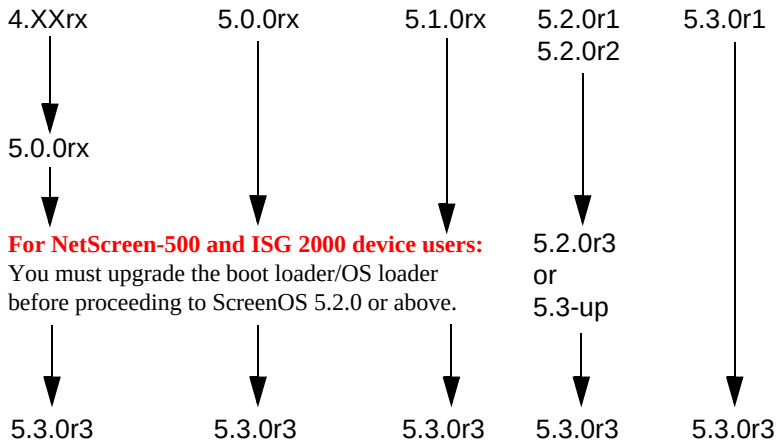
Before you begin a security device upgrade, you must have the most recent ScreenOS firmware. If you upgrade from 5.2.0r3 or later to 5.3.0rx, you also require the interim firmware "*xxxx.5.3.0-up*" (where *xxxx* corresponds to the device model). You must upgrade first to the xxx.5.3.0-up firmware then upgrade to 5.3.0rx. Refer to 5.3 Downloading the New Firmware on page 18 for more download information.

Caution:

- For NetScreen-5GT Wireless and ISG 1000 device users: You can go directly to the ScreenOS 5.3.0r2 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.

The following diagram shows the firmware upgrade path.

Figure 1: Firmware Upgrade Path



This section contains the following information:

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.*

5.1 Requirements to Upgrade and Downgrade 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.*

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)

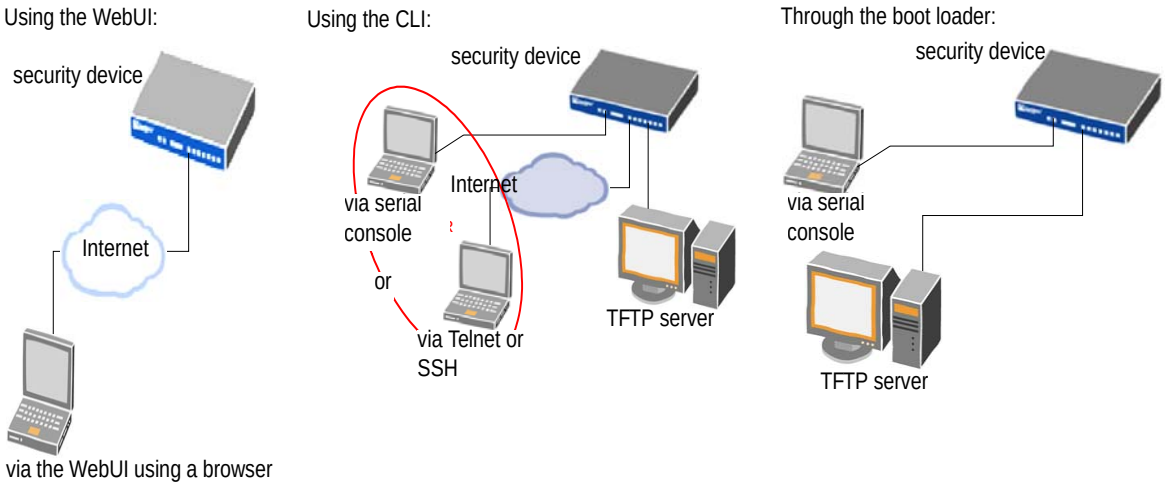
To use the CLI, you must have:

- 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

The illustrations below show the three different ways by which you can upgrade or downgrade a security device.



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 the following sections: “Upgrading to the New Firmware” on page 19 or “Upgrading Security Devices in an NSRP Configuration” on page 26.

5.2 Special Boot-ROM or Boot-Loader Requirements

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

5.2.1 NetScreen-500 Boot-ROM

Installation of this release on a NetScreen-500 device 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.

5.2.2 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 bootup 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/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 key 'X' and 'A' sequentially to update 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.

5.3 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, enter http://www.juniper.net/support in your Web browser. Click Support > Customer Support Center, and then follow these steps:
   a. Log in by entering your user ID and password, and 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.

5.4 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 via the WebUI and CLI.

5.4.1 Using the WebUI

Perform the following steps to upgrade the firmware using the WebUI:

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

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

7. Log in to the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI Home page.

Upgrading to the New ScreenOS Firmware

8. Go to Configuration > Update > ScreenOS/Keys and select Firmware Update.
9. Click **Browse** to navigate to the location of the new ScreenOS firmware or type the path to its location in the Load File field.
10. Click **Apply**.

    A message box appears with information on the upgrade time.

11. Click **OK** to continue.

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

12. Log in to the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI Home page.

5.4.2 Using the CLI

Perform the following steps to upgrade the firmware using the CLI:

1. 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 new firmware, see "Downloading the New Firmware" on page 18.
2. Run the TFTP server on your computer by double-clicking on the TFTP server application.
3. Log in to 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 admin or an admin with read-write privileges.
4. Save the existing configuration by executing the command:

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

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

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

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 reset the device.
7. Wait a few minutes, and then log in to 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 by executing the command:

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

5.4.3 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.*

Perform the following steps to load firmware with the Boot/OS Loader:

1. Connect your computer to the security device:
2. Using a serial cable, connect the serial port on your computer to the console port on the security device. This connection, in combination with a terminal application, enables you to manage the security device.
3. Using an Ethernet cable, connect the network port on your computer to port 1 or to the management port on the security device. This connection enables the transfer of data between the computer, the TFTP server, and the security device.
4. Make sure that you have the new ScreenOS firmware stored in the TFTP server directory on your computer. For information on obtaining the new firmware, see “Downloading the New Firmware” on page 18.
5. 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.
6. Log in to the security device using a terminal emulator such as Hyper Terminal. Log in as the root admin or an admin with read-write privileges.
7. Restart the security device.
8. When you see “Hit any key to run loader” or “Hit any key to load new firmware” on the console display, press any key on your computer keyboard to interrupt the bootup process.

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

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

   If you type slot1: before the specified file name, then the loader reads the specified file from the external Compact Flash or memory card. If you do not type 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 retype the filename.

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

    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.

5.4.4 Saving Multiple Firmware Images with Boot Loader

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

```
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 file name 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 file name used by the Loader cannot exceed 63 characters.*

5.5 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 16M of total flash, with 4M reserved for the OS loader and 12M 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.*

Perform the following steps to upgrade the OS loader and file system:

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” on page 19.

   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” on page 19.

5.5.1 Downgrading the 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.*

Perform the following steps to downgrade the NetScreen-500 device from ScreenOS 5.3.0 to ScreenOS 5.0.0 or above. If you need to downgrade the device to a version prior to ScreenOS 5.0.0, downgrade using the boot/OS loader (see Using the Boot/OS Loader on page 24).

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.

   For information on downloading the firmware, see "Downloading the New Firmware" on page 18.

2. Load the firmware with the CLI. For information on using the CLI to load firmware, see "Using the CLI" on page 20.
3. Enter the CLI command, **exec downgrade**.

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.

   For information on downloading the firmware, see "Downloading the New Firmware" on page 18.

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

   The security device automatically restarts.

3. Load the firmware using the boot/OS loader. For information on using the boot/OS loader, see "Using the Boot/OS Loader" on page 21.

5.6 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** command.

1. Download the OS loader from the Juniper Networks support site to the root directory of your TFTP server.
2. Visit juniper.net and log in.
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** 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 key 'X' and 'A' sequentially to update 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.

5.7 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" on page 19).*

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

5.7.1 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 to Upgrade and Downgrade Device Firmware" on page 15. 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" on page 26

B. "Fail Over Device A to Device B (CLI only)" on page 27

C. "Upgrade Device A to ScreenOS 5.3.0" on page 28

D. "Synchronize Device A (CLI only)" on page 29

E. "Fail Over Device B to Device A (CLI only)" on page 29

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" on page 18.

1. Log in to device B by opening a Web browser (for example Internet Explorer or Netscape) and entering the Management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.
2. Save the existing configuration:
   a. Go to Configuration > Update > Config File, and 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 in to the security device. You can verify the version of the security device ScreenOS firmware in the Device Information section of the WebUI Home page.

CLI

Make sure that you have the ScreenOS 5.3.0 firmware. For information on obtaining the firmware, see "Downloading the New Firmware" on page 18.

1. Log in to device B 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 admin or an admin 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 the IP address is that of your computer and the 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 in to 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)

1. Manually fail over the master device to the backup device.
2. Log in to the master device.
3. 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 the preempt feature is enabled: **exec nsrp vsd-group 0 mode ineligible**
   – If the preempt option is not enabled: **exec nsrp vsd-group 0 mode backup**

Either command forces the master device to step down and the backup device to immediately assume mastership.

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" on page 18.

1. Log in to 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 in to the security device. You can verify the security device ScreenOS firmware version on the WebUI Home page, 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" on page 18.

1. Log in to 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 tftp *ip_addr filename* **to flash**

   where:

   ip_addr is the IP address of your computer.
   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 in to 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 in to device B and fail over device B instead of failing over device A.

5.7.2 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)” on page 30

B. “Upgrade Device B to ScreenOS 5.3.0” on page 30

C. “Fail Over Device A to Device B (CLI only)” on page 31

D. “Upgrade Device A to ScreenOS 5.3.0” on page 31

E. “Synchronize Device A (CLI only)” on page 32

F. “Fail Over Device B in VSD 0 to Device A in VSD 0 (CLI only)” on page 33

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 in to device B 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 admin or an admin 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 the preempt feature is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If the preempt option is not enabled: **exec nsrp vsd-group 1 mode backup**

Either command forces device B to step down and device A to immediately assume 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” on page 18.

1. Log in to security device B by opening a Web browser (for example Internet Explorer or Netscape) and entering the Management IP address in the Address field. Log in as the root admin or an admin with read-write privileges.
2. Save the existing configuration:
   a. Go to Configuration > Update > Config File, and 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 in to the security device. You can verify the security device ScreenOS firmware version on the WebUI Home page, 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" on page 18.

1. Log in to 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 double-clicking on the TFTP server application.
4. On the security device, enter save soft from tftp ip_addr filename to flash. Where the IP address is that of your computer and the 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 in to 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 in to 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 the preempt feature is enabled: **exec nsrp vsd-group 0 mode ineligible**
   - If the preempt option 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 the preempt feature is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If the preempt option 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" on page 18.

1. Log in to 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 in to the security device. You can verify the security device ScreenOS firmware version on the WebUI Home page, 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" on page 18.

1. Log in to 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, enter the following command:

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

   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 in to 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 in to 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 the preempt feature is enabled: **exec nsrp vsd-group 1 mode ineligible**
   - If the preempt option 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.

5.8 Upgrading or Migrating the AV Scanner

Refer to Table 8 and follow the procedure below for step-by-step instructions on upgrading your existing antivirus scanner or migrating to a new antivirus scanner:

Table 8: Upgrading to ScreenOS 5.3.0

If you are upgrading from a previous release of ScreenOS	Follow this procedure
With antivirus (AV license installed)	Save your current configuration. Install the AV license. Upgrade to ScreenOS 5.3.0*.
Without antivirus (without AV license installed)	Upgrade to ScreenOS 5.3.0. Install the AV license.

*. Select the ScreenOS version which supports the AV scan engine as shown in Table 5.

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 9: AV Scan Engines

AV Scan Engine	License Key	ScreenOS version
Trend Micro	av_key	*ns5gttmav.5.3.0r1*
Juniper-Kaspersky	av_v2_key	*ns5gt.5.3.0r1*

   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 9. 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.5.3.0r1
   – Juniper-Kaspersky image: ns5gt.5.3.0r1
4. Check config file (especially policies) to ensure it is intact.

5.8.1 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 Table 10. 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 10: 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 set http skipmime mime-list ns-skip-mime-list set http skipmime enable exit
unset av http skipmime	set av profile scan-mgr unset http skipmime enable exit

Commands previous to ScreenOS 5.3.0	ScreenOS 5.3.0 commands invoked from within a profile context
set av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP } [timeout number] }	set av profile scan-mgr set { FTP | HTTP | IMAP | POP3 | SMTP { enable | timeout *number* } } exit
unset av scan-mgr content { FTP | HTTP | IMAP | POP3 | SMTP }	set av profile scan-mgr unset { FTP | HTTP | IMAP | POP3 | SMTP } enable exit

5.8.2 AV Pattern Update URL

Trend Micro Inc. will stop hosting AV pattern file updates at URL http://5gt-t.activeupdate.trendmicro.com/activeupdate/server.ini and 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
```

6. Addressed Issues

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

6.1 Addressed Issues in ScreenOS 5.3.0r3

- 04092 – 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.
- 04221 – (WebUI) The **remove** option did not remove a CA certificate.
- 04334 – Setting traffic to a vsys had problems. Debugging the device would show traffic that was going to the vsys was incorrectly classified to the root vsys.
- 04457 – A disabled IKE user could successfully connect through the VPN.
- 04522 – Incoming mail did not pass through a MIP when AV was enabled.
- 04553 – Occasionally, packets were not routed correctly even though they matched the session.

- 04819 – An IGMP proxy to multiple host interfaces for the same group was disallowed.
- 04978 – (WebUI) Antivirus information was incorrectly contained as **Recent Event** information.
- 05284 – After a reboot, policy-based VPN tunnel, with SRC-NAT and DIP configured, was inactivate due to an incorrectly set proxy-ID.
- 05471 – The discard counter did not increment properly.
- 05515 – The **get service any** CLI command displayed the default timeout value as one minute.
- 05733 – In some cases, a track-ip ping response was lost.
- 05738 – (WebUI) The Local Auth server timeout field was incorrectly limited to a three digit value when the value should have been four digits.
- 05903 – A session failed when DI was enabled and the DI was unable to handle half-close state.
- 05981 – (WebUI) An error occurred when deleting an aggregate interface or subinterface.
- 06161 – (ISG-2000) In transparent mode, configuring a large number of policies resulted in a policy look up timeout and dropped packets.
- 06240 – Source-based NAT did not occur on traffic from Trust to DMZ security zones.
- 06295 – There was intermittent device failure due to policy database failure.
- 06297 – In some cases, the RADIUS authentication over policy based tunnels stopped working.
- 06441 – The antivirus option was unavailable when a policy was configured for multi-cell context.
- 06990 – Corrupt mis-interpreted and mis-directed HA message caused the backup device to coredump and loose connectivity with the primary device.
- 06991 – (NetScreen-50) Coredump and reboot occurred in an active/passive NSRP configuration, when secure-ID user inserted a long user name and password.
- 07059 – DHCP requests from clients on untrust side of any NS device in X-mode acting as VPN initiator will be relayed to DHCP server behind the VPN responder through the VPN tunnel.
- 07101 – DSCP marking for IPSec pass through traffic in route mode did not work properly on some platforms.
- 07132 – Dial backup did not work (modem does not return dial) due to PPPLCP keepalives not being sent.
- 07133 – Sometimes there were a few differences on SA's SPI between Master's SA and Backup's SA when running the NSRP hot-sync.
- 07177 – After an IGMP configured subinterface had participated in multicast, it could no longer be deleted or assigned to the null zone.
- 07178 – In some cases, IPSec sessions were not cleaned up in the session table resulting in VPN failure.
- 07217 – Modifying or adding an L2TP policy corrupted the system configuration.
- 07218 – (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.

- 07259 – (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 not protected.
- 07279 – A message, indicating that there was a corrupted session, was displayed on the console every 5 to 10 minutes on a backup device in an active/passive NSRP configuration.
- 07295 – The **exec policy verify** CLI command returned incorrect results.
- 07301 – (NetScreen 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.
- 07354 – (NetScreen-5XT) Issues occurred when a device was upgraded from 4.0 to 5.3.
- 07402 – (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.
- 07425 – 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.
- 07462 – SSL based FTP server was inaccessible when AV was enabled on the policy.
- 07488 – NetScreen-Security Manager returned a error when trying to set physical link-down of any interface on an ISG device.
- 07508 – In some cases, during IKE negotiation, device failure occurred when the IP ID was generated
- 07519 – 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.
- 07562 – In some situations, when processing BGP updates, a second withdrawn message was sent 30s after the first withdrawn message.
- 07614 – 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.
- 07623 – Inter vsys routing was handled improperly.
- 07627 – In a route based VPN multi-VR environment, the security device incorrectly performed a route lookup in the wrong VR.
- 07633 – 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.
- 07637 – 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.
- 07660 – Passive FTP traffic was translated incorrectly.
- 07661 – Interface last_change attribute was sometimes displayed incorrectly and did not get updated when the interface state was changed to up.

- 07729 – An ARP packet buffer was increased to improve performance.
- 07760 – (WebUI) Having the same IP address for interface track IP & NSRP track-IP was not permitted.
- 07772 – Internal mishandling of H.323 traffic caused device failure.
- 07803 – While using Web Authentication, the vsys pointer for a secure-id path was set improperly, causing the response failure. This action resulted in a Web Auth failure inside a vsys.
- 07814 – A device failure occurred when user configured the ninth DHCP server.
- 07816 – In some cases, CPU utilization displayed a spike due to ARP aging out incorrectly.
- 07871 – The device failed while handling ISAKMP packets with invalid and/or abnormal contents.
- 07884 – (NetScreen-5200) The **get log sys saved** CLI command sometimes displayed trace dump on the device console.
- 07887 – (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.
- 07888 – In some cases, outbound SIP calls caused device failure.
- 07931 – The device passed traffic incorrectly when using address groups.
- 07964 – In some cases, the device failed when issuing the **debug flow** CLI command.
- 07995 – 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.
- 08032 – Internal mishandling of RADIUS traffic caused device failure.
- 08053 – (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 management zone.
- 08066 – Unresolved unicast route had a missing null ptr check which caused device failure.
- 08073 – An internal task incorrectly increased the CPU usage.
- 08077 – large number of VPN tunnels and traffic caused the device to fail.
- 08079 – Dial Line remained open even though there was no interesting traffic as idle timer was reset every few seconds.
- 08080 – (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.
- 08085 – (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.
- 08109 – 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.
- 08113 – In some cases, the device management was delayed after about an hour.
- 08161 – Syn cookie mechanism was working incorrectly on logical interfaces.
- 08164 – Due to incorrect storage of buffer packet for reassembly, a device reset and displayed the console error "### No DIMM found on board ###".

- 08256 – (NetScreen-5000 Series) The **get flow** CLI command incorrectly displayed that the rcp-rst-invalid session was unsupported.
- 08257 – (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.
- 08265 – Overlapping UDP customer service port range with IKE port (UDP port 500) caused incorrect session timeout for IKE sessions.
- 08279 – (WebUI) After configuring an Xauth local authentication user group, the **CHAP Only** was automatically selected and it was impossible to disable it.
- 08293 – 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.

6.2 Addressed Issues in ScreenOS 5.3.0r2

- 07871 – A check was added to address vulnerability issue with implementation of the ISAKMP protocol.
- 07979 – When generating a P1 gateway, it was impossible to select dynamic mode VPN and a distinguished name from the WebUI.
- 53319 – When using a Linux FTP client/server, FTP timeout occurred when sending files larger than 5 MB.
- 53388 – Established VPN UDP sessions kept using the old route even after the route was changed.

7. Known Issues

This section describes known issues with the current release.

- section 7.1 “Limitations of Features in ScreenOS 5.3.0r3 on page 40 identifies features that are not fully functional at the present time, and will be unsupported for this release.
- section 7.2 “Compatibility Issues in ScreenOS 5.3.0r3 on page 41 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.
- section 7.3 “Known Issues In ScreenOS 5.3.0r3 on page 42 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.

7.1 Limitations of Features in ScreenOS 5.3.0r3

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

7.1.1 Limitations in ScreenOS 5.3.0r3

- The FTP extended passive mode is not supported.

7.1.2 Limitations in 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-MGT1	NetScreen-5200-MGT2	NetScreen-5400-MGT1	NetScreen-5400-MGT2
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:
  - AV session is aborted.

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

  - Default route is required for AV to function in transparent mode.
  - 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.

7.2 Compatibility Issues in ScreenOS 5.3.0r3

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

- **Compatible web browsers** – The WebUI for ScreenOS 5.3.0r3 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.

7.2.1 Upgrade Paths from Previous Releases

Upgrade sequence – We recommend that you follow the upgrade instructions described in section 5. "Migration Procedures on page 14. 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. Refer to section 5.4 "Upgrading to the New Firmware on page 19 for instructions on how to perform the upgrade.

7.3 Known Issues In ScreenOS 5.3.0r3

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 starts with "W/A:" If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

7.3.1 Known Issues in ScreenOS 5.3.0r3

- 07833 – (NetScreen-5GT) A device with Trend Micro Antivirus enabled does not properly handle the Active X screen option.

7.3.2 Known Issues from ScreenOS 5.3.0r2

- 07523 – (NetScreen-5GT) 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.
- 07816 – In some cases, CPU utilization may show a spike due to ARP not aging out correctly.
- 07833 – (NetScreen-5GT) A device with Trend Micro Antivirus enabled does not properly handle the Active X screen option.
- 07839 – In some cases, invalid or malformed VLAN packets caused device failure.
- 07866 – Web-filtering does not work correctly with the **set flow no-tcp-seq check** CLI command enabled.
- 07880 – A device could fail when viewing the log entries with the WebUI.
- 07893 – (NetScreen-HSC) The device may stop passing traffic when AV is enabled.
- 07931 – The device may not pass traffic correctly when using address groups.
- 07964 – In some cases, the device may fail when the debug flow command is issued.
- 08014 – The device cannot establish a VPN due to port 4500 being incorrectly interpreted.

7.3.3 Known Issues From ScreenOS 5.3.0r1

- 07663 – 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 an NetScreen-25 platform you need to enter: *https://services.netscreen.com/restricted/sigupdates/5.3/ns25/attacks.bin?sn=<serial>*
- 48563 – 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.
- 48581 – With a device that has a large VSYS configuration, if a user changes the configuration in the vsys, it might disrupt traffic.
- 48603 – 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.
- 48642 – The Multitech CDMA wireless modem does not work properly with NetScreen-5GT devices due to inter-operability issues.
- 49670 – If a security device passes frames larger than 1518 bytes while connected to a Cisco switch, it may increase the "Out Discard" (internal) counter.
- 51841 – 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.
- 51953 – Video Conference calls across the firewall system using Tandberg Equipment fail.
- 52798 – 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.
- 53100 – 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.
- 53675 – 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.
- 53727 – In an NSRP active/passive scenario with a large volume of SIP calls, SIP call numbers in the primary and secondary devices may not be in sync.
- 53904 – A user cannot configure the OSPF Neighbor List using the WebUI.
  W/A: Use the CLI.
- 53927 – When setting up a BGP peer group using the WebUI, the device needlessly requests for a EBGP Multihop value.
  W/A: Use the CLI to configure a BGP peer group.
- 53928 – 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.
- 53930 – A user cannot configure a BGP network command using the WebUI.
  W/A: Use the CLI.
- 53932 – On a device configured with BGP aggregate address, an attempt to access the aggregate address WebUI page causes the device to fail.
- 53991 – A slow speed WAN connection causes fragmented packets to be re-assembled incorrectly because small fragments arrive faster than large fragments.
- 54013 – In a stressful NSRP active/passive scenario in NAT mode, after a failover, if a user terminates all SIP calls and executes the "clear sip all" command on both devices, the devices might not release sip calls, gates, and resources.

- 54021 – When using the WebUI Policy page: if a user clicks Edit, makes no modifications, and then clicks OK, the event log incorrectly shows that AV is detached and incorrectly generates unnecessary events.
- 54036 – Incorrectly adding a proxy-id in a VPN policy may cause the device to fail.
- 54064 – In a stressful NSRP active/passive scenario with VPNs, there might be differences with the security parameter indexes (SPI) for the security associations (SAs) on the primary and secondary devices.
- 54181 – The AV scan engine may restart when browsing certain Web sites.
- 54221 – When using an Avaya IP Phone, the device may fail when the Avaya phone restarts.
- 54223 – The AV scanner currently drops SMTP emails over 7 MB.
- 54373 – The device may experience a slowing down of SMTP traffic, which may cause a timeout when sending files larger than 7MB.
- 54689 – Configuring a MIP through the WebUI does not allow subnet definition W/A: Use the command line interface.

8. Getting Help

For further assistance with Juniper Networks products, visit

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

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