Juniper Networks ScreenOS Release Notes

Products: Integrated Security Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 500/500 M Series, and NetScreen-5000 Series (NS 5000 – MGT2/SPM2).

Version: ScreenOS 6.0.0r1

Revision: Rev 03

Part Number: 530-017762-01

Date: January 22, 2008

Contents

Version Summary

ScreenOS 6.0 firmware can be installed on the following products: Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 520/520M, SSG 550/550 M, Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, and NetScreen-5000 series with MGT2/SPM2.

This release incorporates ScreenOS maintenance releases up to 5.4r4 and 5.3r7.

> **Note:** If you are using an SSG 500 series device and an SSG 500 M series device in an NSRP environment, both devices must be running ScreenOS 5.4r2 or later.

> **Note:** You can use NetScreen-Security Manager 2007.1 with the Forward Support Update software to manage devices running ScreenOS 6.0. To do this, install a schema upgrade on the management server and user interface. The upgrade is available at http://www.juniper.net/customers/support/. Refer to the NSM Forward Support for ScreenOS 6.0.0 Release Notes for installation instructions and the features and platforms supported with this schema upgrade.

Documentation Changes

Documentation Changes Introduced in 6.0.0r1

To upgrade existing firmware to ScreenOS 6.0, refer to the ScreenOS *Upgrade Guide* (formerly *Migration Guide*) located at http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/upgrade_guide.pdf. The SSG 500/500M devices require boot loader upgrade. For more information on the upgrade procedure, see the “Upgrade Sequence” in the Compatibility Issues in ScreenOS 6.0 section.

Starting with ScreenOS 6.0.0, we have removed information on configuring Physical Interface Modules (PIMs) and Mini-PIMs from the Installation and Configuration guides for SSG devices. We have moved this information into a new guide called "PIM and Mini-PIM Installation and Configuration Guide." Refer to that guide for information on configuring PIMs and Mini-PIMs.

New Features and Enhancements

New Features and Enhancements Introduced in 6.0.0r1

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

If you already have an account, enter your user ID and password.

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

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

Hardware Features

16-port 10/100/1000 uPIM

The 16-port 10/100/1000 universal Physical Interface Module (uPIM) is supported on the SSG 140, SSG 500 series, and SSG 500M series security devices and provides connectivity to copper-based gigabit Ethernet LANs. This PIM also supports up to eight bridge groups (bgroups), which let you group several Ethernet interfaces together. Connect to the module using CAT-5 cable.

If you are using this module, refer to the "PIM Power and Thermal Requirements," in the Limitations section.

8-port 10/100/1000 uPIM

The 8-port 10/100/1000 universal Physical Interface Module (uPIM) is supported on the SSG 140, SSG 500 series, and SSG 500M series security devices and provides connectivity to copper-based gigabit Ethernet LANs. This PIM also supports up to four bridge groups (bgroups), which let you group several Ethernet interfaces together. Connect to the module using CAT-5 cable.

If you are using this module, refer to the "PIM Power and Thermal Requirements," in the Limitations section.

6-port GE SFP uPIM

The 6-port small form factor pluggable (SFP) universal Physical Interface Module (uPIM) is supported on the SSG 140, SSG 500 series, and SSG 500M series security devices and provides connectivity to fiber-based and copper-based gigabit Ethernet LANs. Non-Juniper SFPs are not supported by JTAC at this

time. This PIM also supports up to three bridge groups (bgroups), which let you group several Ethernet interfaces together. Connect the module using the appropriate cable type depending on the specific media used: single-mode or multimode optical cable for SX and LX, and CAT-5 cable for the copper transceiver.

Synchronous Serial Mini-PIM for SSG 20

The Synchronous Serial Mini-Physical Interface Module (Mini-PIM) is supported on the SSG 20 security device and provides connectivity to Serial network media types. Its dedicated network processor forwards traffic to the SSG 20 CPU where traffic decisions are made based upon the security policy.

1-port GE SFP Mini-PIM for SSG 20

The single port small form factor pluggable (SFP) Mini-Physical Interface Module (Mini-PIM) is supported on the SSG 20 security device and provides connectivity to fiber-based and copper-based gigabit Ethernet LANs. Non-Juniper SFPs are not supported by JTAC at this time. Connect the module using the appropriate cable type depending on the specific media used: single-mode or multimode optical cable for SX, LX, FX, BX, and CAT-5 cable for the copper transceiver.

E-3 Support

ScreenOS now supports E3 PIM on the SSG 500 series platforms.

ADSL2+ PIM

The 1x ADSL2+ PIM (Annex A or Annex B) is now supported on the SSG 140, SSG 520/550, and the SSG 520M/550M platforms. The two new discrete multitone (DTM) standards supported are:

ITU 992.3 (also known as ADSL2), which supports data rates up to 1.2 Mbps upstream and 12 Mbps downstream.
ITU 992.5 (also known as ADSL2+), which supports data rates up to 1.2 Mbps upstream and 24 Mbps downstream.

G.SHDSL PIM

The G.Symmetric High-speed Digital Subscriber Line (G.SHDSL) PIM supports multi-rate, high-speed, symmetrical digital subscriber line technology for data transfer between a single customer premises equipment (CPE) subscriber and a central office (CO). The G.SHDSL PIM is now supported on the SSG 140, SSG 520/550, and the SSG 520M/550M platforms.
ScreenOS 6.0 supports the ITU G.991.2, single-pair High-speed Digital Subscriber Line (SHDSL) Transceiver discrete multitone (DTM) standard.

Virtual Private Network (VPN)

AutoConnect-VPN (AC-VPN)

AutoConnect-Virtual Private Network (AC-VPN) enables spokes in a hub-and-spoke VPN network to dynamically create VPN tunnels directly between each other as-needed. This not only addresses issues of latency between spokes, but reduces processing overhead on the hub and thus improves overall network performance. Because AC-VPN creates dynamic tunnels that time out when traffic ceases to flow through them, network administrators are freed from the time-consuming task of maintaining a complex network of static VPN tunnels. All devices must be running ScreenOS 6.0 or later.

Screen on Tunnel Interface

You can now apply any configured screens to tunnel interfaces. Traffic exiting tunnels is examined before and after encryption. However, screens that currently have limited support on the ASIC-based platforms will continue to have the same limitations.

Firewall

WebUI Enhancements

The Web-based User Interface (WebUI) is improved to optimize work flow, display diagnostic information, enhance the Home page, and categorize the menu options.

FTP Get/Put Service Enhancement

This feature redefines the FTP-Put and FTP-Get service definitions used in firewall policies. In prior ScreenOS releases, FTP-Put and FTP-Get were configured together with different actions in a policy and service groups. In ScreenOS 6.0, the enhancements for FTP Get/Put are as follows:

- FTP / FTP-Get / FTP-Put should not be in a single service group.
- FTP/ FTP-Get /FTP-Put should not be defined for one single policy.
- FTP-Get or FTP-Put is the same as FTP service in policies with deny action.
- Description in WebUI enhanced.

Automated data gathering

This feature is a basic looping script consisting of **get** commands that run as a background process, saving the output to a FIFO file in the flash. You may record any series of get commands to gather information in the background.
Note: Depending on the information gathered, CPU usage is affected.

Universal Threat Management

Antivirus scanning for Instant Messaging (IM) Services

ScreenOS supports antivirus scanning for instant messaging services such as AIM, ICQ, Yahoo! Messenger, and MSN Messenger. AV scanning is supported for text/group chat messages, and file transfer/file sharing.

The following versions of the IM Client and protocol are fully supported. Forward compatibility on later versions of the IM client and protocol are supported on the basis of best effort.

Instant Messaging Service	Supported Protocol Versions	Supported IM Client Versions
AIM and ICQ	OSCAR generic service version 4	AIM 5.9.3861 to 5.9.6089 ICQ 5.04 to 5.1
Yahoo! Messenger	Yahoo Messenger Service Gateway Protocol (YMSG) version 8, 9, 10	Yahoo! Messenger 5.5.1228 (v8.0.0.506 is supported as best efforts)
MSN Messenger (Windows XP)	Mobile Status Notification Protocol (MSNP) version 11, 12, 13	MSN Messenger 7.5

All platforms require high-memory option to run AV scanning. Platforms supported: SSG 5, SSG 20, SSG 140, SSG 520/550, and SSG 520M/550M.

AV HTTP Trickling Enhancement

This feature enhancement is important for low-speed links. It allows you to configure time-based thresholds to send bits through the firewall to prevent browser timeouts when the device is receiving data or while the data is being scanned by the internal AV engine.

IDP and GPRS

IDP Enhancements

IDP Recommended Action: You can now allow recommended actions in IDP rules. If you specify “recommended” as the action in a rule, the recommended action will be applied in cases where you do not specify an action within a policy rule. If you specify an action within a policy rule, it will take precedence over the recommended action.

VLAN Groups for L2 VSYS: VLAN Groups for L2 VSYS is now supported on the ISG 1000, ISG 1000-IDP, ISG 2000-IDP, and the NetScreen-5400 devices.

IDP inspection of GTP and GRE-encapsulated traffic: The ISG 1000 and ISG 2000 with IDP Security Modules can now inspect traffic that is encapsulated in GPRS Tunneling Protocol (GTP) and Generic Routing Encapsulation (GRE).

IMSI information in NSM logs: NSM IDP logs now contain International Mobile Subscriber Identity (IMSI) data on the IDP security devices. This information allows you to specifically identify the end user for threats and attacks that are detected during forensic evaluation using the provided subscriber-level identifiers.

IDP Detector.so has been updated to IDP 4.0: The IDP 4.0 engine has been synced to ScreenOS 6.0. You will now have the same detection capabilities on ISG1000/ISG2000 with IDP as you do on the standalone IDP 4.0 devices.

DSCP Marking based on IDP action: You can now change the DSCP marking of a packet based on IDP actions performed on the ISG 1000/2000 with IDP. This will allow upstream and downstream devices to prioritize traffic based on IDP rules.

Troubleshooting IDP: You can use the "get sm tech-support" command to gather IDP configuration and statistics to troubleshoot IDP security modules.

Authentication Service Enhancements

ScreenOS authentication service provides the following enhancements:

Add user IP address to authentication logs

Support TACACS+ authentication servers

Prioritize authentication between external server and local database

Increase number of permitted administrator IP addresses

Enhance RADIUS features

“Framed-pool” support (IP pool supplied by RADIUS server, not local device)

Customizable interface description

Called-Station-ID attributes for differentiated billing purposes

VSYS

Virtual System Enhancements

Increased Virtual System Support on ISG 1000 and ISG 2000 Devices: The ISG 1000 and ISG 2000 security devices now support additional virtual systems. The ISG 1000 now supports up to 50 virtual systems (increased from 10 virtual systems). The ISG 2000 now supports up to 250 virtual systems (increased from 50 virtual systems). To take advantage of these increases in virtual system support, you must install a new license key.

Virtual System Names: Virtual System names can contain up to 20 characters. Previously, virtual system names could contain up to 10 characters.

NAT

DIP Pool Enhancement

The number of Dynamic IP (DIP) pool addresses per Vsys and per interface is increased to 1020. The maximum global DIP pool size limit is 64K.

NSRP

NSRP Dynamic Route Synchronization

ScreenOS 6.0 now supports dynamic route synchronization. You can sync Dynamic Routing Protocol (DRP) routes in an Active/Passive NSRP cluster. In the event of a failover, the new active device can use the backup routes while it establishes peering relationships.

Layer 2 Transparent Mode

VLAN Retagging

VLAN retagging provides a way to selectively screen VLAN traffic. You place a security device in parallel with your Layer 2 switch, and configure the switch to direct to the security device only traffic from VLANs you want screened. Traffic to and from your other VLANs continues to pass directly through the switch, thus avoiding any impact to throughput that might be caused by passing all VLAN traffic through the security device. This is currently only supported on NetScreen 5000-series.

UAC

Infranet Authentication

The Infranet authentication includes the following enhancements:

Visual display of Auth Table entries in the WebUI

This feature allows you to view the users with active auth table entries (displays the User, Source IP, and Roles).

Additional actions field for Infranet Auth policies.

This feature available with UAC 2.1 permits the Infranet Controller to control additional policy actions (AV, DI, logging, web filtering, and anti-spam) on a per-role basis. This allows you to make policy decisions such as activating AV for partners or untrusted machines, or turning on URL filtering for specific roles.

Increased number of auth table entries

Devices	Auth Table entries
SSG devices	10,000
ISG devices	50,000
NS-5000 series	50,000

Feature Extensions

Jumbo Frames

Jumbo frames are supported on the ISG 1000 and ISG 2000 devices without IDP security modules. To enable jumbo frames, use the **set envar** CLI command and set **max-frame-size** to any value from 1515 through 9830 inclusive; for example, **set envar max-frame-size=7500**. When you enable jumbo frames and restart the security device, only interfaces on the 4-port SFP IO card, plus the management Ethernet interface, become active. Use the **get envar** command to show the **max-frame-size** setting. Use the **unset envar max-frame-size** command to disable jumbo frames support and return the device to the normal maximum frame size (1514 bytes).

Jumbo frames are also supported on the NS-5000 series running MGT2 and SPM2 cards. Limitation: DI and IPv6 are not supported in Jumbo Frames mode.

Bridge Groups for Ethernet ports on SSG Devices

Bridge groups (bgroups) let you group several Ethernet interfaces together. Starting with ScreenOS 6.0, the SSG 140 security device is preconfigured with three bgroups to which you can add the built-in Ethernet ports. New uPIMs support bridge groups on all SSG devices. Limitation: SSG500/500M series do not support bridge groups on the built-in Ethernet ports.

DHCP Relay Flow

No DHCP Relay: By default, ScreenOS relays DHCP request packets from all zones except the V1-Untrust zone and V1-DMZ zone. Enable this feature to prevent relay of DHCP request packets from a specified zone.

Layer 2 Vsys

Layer 2 Vsys is now supported on the Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, the ISG 2000, ISG 2000-IDP, and the NetScreen-5000 series.

Management IP Address limit increased

The total number of IP addresses from which a security device can be managed is increased to 50 plus one times the number of Vsys. By making the number of manager IPs a function of the number of Vsys, memory is not wasted on low-end devices that require relatively few manager IPs, while high-end devices are not restricted to an artificially selected number.

PPU Enhancement

To increase throughput, tcp-syn-bit checking is now done in the Programmable Processing Unit (the ASIC), and supported on the NetScreen 5200 and NetScreen 5400.

DSCP Enhancement

Differentiated services code point (DSCP) marking is now supported on the Integrated Services Gateway (ISG) 1000 and ISG 2000 with IDP Security Modules and NetScreen 5200/5400.

Universal Serial Bus (USB) Support

USB ports allow file transfers such as device configurations, user certificates, and update version images between an external USB storage device and the internal flash storage. The USB functionality is available on the SSG devices.

Coredump and Logs to USB Port

ScreenOS supports full coredump file, logs and full memory dump file transfers to the USB port on the SSG 5 Series and SSG 20 and USB ports/compact flash cards on the SSG 140, SSG 500 series, and SSG 500M series security devices.

IPv6 Support

IPv6 is now supported on the following security devices:

NS-5000 Series using 5000-M2 management module

SSG 5/SSG 20: IPv6 support is available on Ethernet interfaces. (IPv6 is not supported on wireless or WAN interfaces.)

The next release of ScreenOS (6.0r2) will support IPv6 on the ISG 1000 device.

Changes to Default Behavior

Changes to Default Behavior Introduced in 6.0.0r1

This section lists changes to default behavior in ScreenOS 6.0 from previous ScreenOS firmware releases.

TCP-SYN-Check Default

The default for NS-5200/5400 is **set flow tcp-syn-check** which includes both SYN-bit check and a 3-way handshake. In ScreenOS 6.0, the default is **set tcp-syn-bit-check**.

RADIUS Attributes

In ScreenOS 6.0, both calling- and called-station IDs are supported as default behavior.

IP Option Packets

The IP-option packets (record-route and timestamp) in ScreenOS 6.0 are not dropped. All four IP-option packets (record-route, timestamp, security and stream) behave consistently.

Coredump to USB

The maximum file size limitation for the coredump file is removed. The maximum USB size supported is 1GB.

Known Issues

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

Limitations of Features in ScreenOS 6.0—identifies features that are not fully functional at the present time, and will be unsupported for this release.
Compatibility Issues in ScreenOS 6.0—describes known compatibility issues with other products, including but not limited to specific Juniper Networks appliances, other versions of ScreenOS, Internet browsers, Juniper Networks management software and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.
Known Issues in ScreenOS 6.0—describes deviations from intended product behavior as identified by Juniper Networks Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

Limitations

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

SSG 500 Series—Bridge groups are supported on ethernet switch PIMs (uPIM), including 16-port GE, 8-port GE and 6-port SFP. Bridge group is not supported on 1-port SFP, old Enhanced PIMs (ePIM), and on-board GE ports. Bgroup interface can be dynamically created and deleted. The maximum number of bgroup interfaces on each PIM is half the number of ports.

SSG 140— Bridge groups are supported on both on-board ethernet ports and ethernet switch PIMs (uPIM). Bgroup interface can be dynamically created and deleted for the PIMs. The maximum number of bgroup interfaces on each PIM is half the number of ports. For the on-board ports, 3 bgroup interfaces are pre-created. Bgroup interfaces can be configured on the same PIM or the system board only.

Screens on traffic exiting tunnels—has the following limitations:

- This feature is not compatible with the new Syn-bit check in PPU feature. Screens for traffic exiting tunnels are performed by CPU instead of PPU.

- This feature will only apply if the Screen is activated on the physical interface where the tunnel is terminated if the Screen is hardware accelerated.

AC-VPN—DPD does not work on the spoke when set on AC VPN profile with global IKE heartbeat enabled.

Jumbo frame support on the ISGs —Only the 4-port SFP modules on the ISGs support jumbo frame. All other i/o cards in the device are disabled automatically (including the ISG1000 built-in i/o card), when **max-frame-size** is set in the jumbo range (1515~9830).

Online Help—After upgrading to ScreenOS 6.0, you may have to either clear your cookies in your Web browser or apply the default Help Link Path button in the WebUI under **Configuration>Admin>Management.** Due to the cookies we set when managing a device, you may receive the prior version's help files when selecting the online help from within the WebUI.

Device Specific Values for AV Scanning

The following table specifies device-specific values for Antivirus scanning:

AV Command/Device	SSG 5/20	SSG 140	SSG 500
The **Decompress Layer*** CLI option (set <protocol> decompress-layer <number>) specifies the number of layers of nested compressed files the internal AV scanner can decompress before it executes the virus scan.	1 to 4	1 to 6	1 to 8
The **Maximum Content Size#** CLI option (set av scan-mgr max-content-size <number>) specifies the maximum size of content for a single message that the internal AV scanner scans for virus patterns.	20-10000 KB	20-16000 KB	20-24000 KB
Total number of messages scanned concurrently.	256	512	1024

* The default value on the device is dependent on the selected protocol.

The default value for all devices is 10,000KB.

PIM Power and Thermal Requirements

If you install either 8-port or 16-port Ethernet Universal Physical Interface Modules (uPIMs) in your SSG 140, SSG 500-Series, or SSG 500M-Series device, you must observe the following +power and thermal guidelines.

Warning: Exceeding the power or heat capacity of your device may cause the device to overheat, resulting in equipment damage and network outage.

The following table shows the power and heat dissipation capacity of all available SSG series devices. In order to simplify this information, we represent these values as non-dimensional tokens.

Device	Available Tokens	
	Power	Heat
SSG 140	67	67
SSG 520	86	100
SSG 550	67	100
SSG 520M	100	100
SSG 550M	100	100

The following table shows the power and heat dissipation requirements of all available PIMs for SSG-series devices.

Model	Description	Tokens Required	
		Power	Heat
JXU-16GE-TX-S	16xGE uPIM	38	36
JXU-8GE-TX-S	8xGE uPIM	21	27
JX-1ADSL-A-S JX-1ADSL-B-S	1xADSL2+	16	16
JX-2SHDSL-S	2xG.SHDSL	9	10
JXE-4FE-TX-S	4xFE ePIM	9	9
JXU-6GE-SFP-S	6xSFP uPIM	13	13
JXE-1GE-SFP-S	1xSFP ePIM	8	8
JX-1DS3-S	1xDS3	7	7
JX-1E3-S	1xE3	7	7
JX-2E1-RJ48-S	2xE1	6	6
JX-2T1-RJ48-S	2xT1	6	5
JXE-1GE-TX-S	1xGE ePIM	6	7
JX-2Serial-S	2xSerial	5	6

The total number of power tokens required by all of the installed PIMs must be less than the number of power tokens available from the device in which the PIMs are installed. Likewise, the number of heat tokens required by the PIMs must be less than the number available from the device.

For example, if you have three 8-port uPIMs and one Serial PIM installed in an SSG 520 device, the power and heat consumption is as shown in the following table:

Description	Tokens Required		Extended	
	Power	Heat	Power	Heat
JXU-8GE-TX-S 8xGE uPIM	21	27	63	81
JX-2Serial-S 2xSerial PIM	5	6	5	6
Total Required			68	87
Available from SSG 520			86	100
Tokens Remaining			**18**	**13**

Since the SSG 520 has 18 power tokens and 13 heat tokens remaining beyond those required by the installed PIMs, this configuration falls within the heat and power capacity of the SSG 520.

Compatibility Issues in ScreenOS 6.0

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

Compatible Web browsers—The WebUI for ScreenOS 6.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, and Netscape Navigator 6.X for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS X. Other versions of these and other browsers were reported to display erroneous behavior.

Upgrade sequence—Juniper Networks recommends that you follow the upgrade instructions described in the ScreenOS *Upgrade Guide* located at http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/upgrade_guide.pdf. If you upgrade directly from ScreenOS 5.0.0 or ScreenOS 5.1.0 to ScreenOS 6.0, you risk losing part of any existing configuration. For ISG 2000 devices, you must upgrade to an intermediate firmware and upgrade the boot loader before upgrading to the ScreenOS 6.0 firmware. Refer to Upgrade Paths to ScreenOS 6.0 in the ScreenOS *Upgrade Guide* for intermediate software and boot loader upgrade information.

Refer to the following procedure to upgrade the SSG 500/SSG500M boot loader:

1. Download the boot loader image (v.1.0.3) from the Juniper Networks support site to the root directory of your TFTP server.
2. Log into http://www.juniper.net/customers/support/.
3. In the Download Software section, click ***ScreenOS Software***.
4. Download the latest SSG 500/SSG 500M boot 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 SSG 500 and a serial connection from your workstation to the console port on the SSG 500.
7. Restart the SSG 500 by entering the ***reset*** command. When prompted to confirm the command--System reset, are you sure? y/[n]--press the Y key.

The following system output appears:

```
NetScreen SSG500 BootROM V1.0.2 (Checksum: 8796E2F3)
Copyright (c) 1997-2004 NetScreen Technologies, Inc.
Total physical memory: 512MB
Test - Pass
Initialization..... Done
```

1. Press the X and A keys sequentially to update the boot loader.
2. Enter the filename for the boot loader software you want to load (for example, Boot2.1.0.3), the IP address of the SSG 500, and the IP address of your TFTP server. The following system output appears:

```
File Name [boot2.1.0.2]: boot2.1.0.3
Self IP Address [10.150.65.152]:
TFTP IP Address [10.150.65.151]:
```

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

```
Save loader config (112 bytes)... Done
Loading file "boot2.1.0.3"...
/
Loaded successfully! (size = 125,512 bytes)
Ignore image authentication!
...
.....................
Done.
```

WebUI upgrade—When upgrading from ScreenOS 5.2.0 to ScreenOS 6.0 using the WebUI, you must upgrade the device to ScreenOS 5.2r3 and then upgrade the device directly to ScreenOS 6.0. Refer to section Upgrading to the New Firmware in the ScreenOS *Upgrade Guide* for instructions on how to perform the upgrade.

Known Issues in ScreenOS 6.0

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

Antivirus

os69903—Running heavy IM traffic for over a day on SSG5/20 may cause memory issues.

os69848—When the device is under heavy HTTP traffic and memory is running low, an incorrect debug message is displayed: "Fail to allocate new data area for buf."

os66700—Yahoo Messenger IM file transfer from the Internet does not get scanned when "set av http skipmime" is enabled.

os67933—You may experience a lost or delayed file transfer request, if MSN IM session is idle for over 20 minutes.

os70197—When HTTP AV is enabled and Yahoo Messenger (YMSG) IM AV is disabled, file transfers over YMSG (that use the HTTP protocol) may occasionally cause the file transfer to fail on reaching the maximum configured limits. For example, a file transfer may fail if the file is larger than the configured max-content-size.

os70202—When Yahoo Messenger IM AV is enabled and the action is set to pass if the file being examined is larger than the configured value, then the event notifying that the max-content-size was exceeded is sent twice. The corresponding error counter is also incremented by 2 instead of 1. The actual handling of the file transfer is correct and no packets are retransmitted.

os70203—MSN user may experience apparent delay during chatting if MSN network traffic load is low; for example, if there is no on-going file transfer and not many users are chatting through the firewall.

os70207—Under high stress conditions with AV, it is possible to see FTP traffic blocked.
W/A: Reboot or reduce traffic through the device.

HA & NSRP

os68106—FTP sometimes failed to complete in an NSRP Active/Passive setup. The data transfer fails when failover and fallback happens frequently during the FTP transfer.

os69429—"Unset IP managable" is not propagated from master to slave.

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

cs11602—After issuing an update, the NSM UI displays one of the NSRP cluster devices as “Managed, device changed.” The status change occurs when using supplemental CLI to set commands that are not managed from NSM.

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

IDP

os69994—On an ISG 1000 device, pushing 'all attacks' using NSM might fail after upgrading to ScreenOS 6.0.
W/A: Delete the policy.gz.v from the flash prior to upgrading to ScreenOS 6.0. To delete the policy prior to upgrading, enter the following command from the CLI, # del file flash:policy.gz.v. After you upgrade, push the new policy to the device.

cs12951—The command 'exec policy verify' is used when DI is enabled on your device. On the ISG 2000/1000 IDP, the DI command is available, but it is not supported.

os69887—On the ISG 1000/2000 devices, memory issues occur and policy push fails if you continuously push IDP policies.
W/A: Unload the policy on the IDP security module prior to pushing a new policy. Enter the command, # exec sm <sm#> ksh "scio policy unload s0" on all the security modules. Replace "sm#" with the number of the security modules. For example, for security module 1, the command is #exec sm 1 ksh "scio policy unload s0"

os69438—Under heavy traffic conditions, if the IDP Profiler is enabled, the CLI may respond slowly.

os69720—If you see this event log, “dma_transmit failed to 1,” then you’ve reached the maximum capacity of your device.

Management

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

os68130—This is an NSM only issue. Import Configuration in NSM may fail if your device has a backslash (\) in the parameter string. This is rooted

from lack of escape sequence for commands, such as 'set av mime-list' where NSM considers backslash as a control character.

Other

os64521—It is possible to create a subinterface for PPP and HDLC connections even though it is not supported in ScreenOS. ScreenOS supports subinterfaces for Frame Relay and Multi-Link Frame Relay only.

os68925—SSG 20 devices cannot resolve IPv6 domain names for the IKE gateway.
W/A: Specify an IPv6 address instead of a domain name for the IKE gateway.

os70287—Global DIP pool limit is 1K on the SSG devices.

os69468—There is no option to clear the newly introduced bgroup interface counters on the SSG140.

cs11922—If a very small fragmented packet is sent to the FPGA, it is possible that it is delayed until a larger packet is received to trigger the FPGA hashing functionality.

os69570—On the SSG 20 devices, operating mode configured for ADSL2 or ADSL2+ is always incorrectly seen as auto in the WebUI.

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

os68704—SSG520, SSG550, SSG520M, and SSG550M devices have incorrect AUX port settings. The correct values are 9600, 8, N, and 1. Currently, the default values are 115200, 8, N, and 1.

cs13083—When using the GTP feature in ScreenOS, the PDP Request filtering checks the Access Point Name in the Information Element, which is sometimes not supplied.

os68781—On the SSG5 device, if "debug modem all" and "unset console db" commands are both enabled, the CPU utilization is too high to allow for modem dialout from the v.92 interface.

os69430—A SSG 20 device fails if you insert a write-protected USB device followed by a "get file" command.

cs12430—Some MGCP protocol extension traffic was being dropped by the MGCP ALG.
W/A: Turn off MGCP ALG.

cs13119—After the backup firewall is booted and if the NSM server sends a FIN packet to it, the backup firewall when sending reset uses virtual MAC rather than physical MAC causing traffic disruption for short period (~ 30 seconds) if this packet passes through a switch.

cs13226—Sometimes during flow processing, after the packet's ARP entry is determined and before the packet is sent, the ARP entry is freed, which causes the device to fail.

Performance

os68825—After long durations of heavy attack traffic conditions, the device may display 'bad session id' messages incorrectly.

os69772—Memory issues may occur on the ISG1000 with IDP running in transparent mode with all attacks installed.

cs12838—During heavy traffic, SSG devices show high CPU (99%) usage and a warning message is displayed on the console, "WARNING: insertion in tree failed when free a port. Possibly Node Pool exhausted!"

Routing

cs11355—ISG 1000 and ISG 2000 devices do not terminate a TCP session immediately when a client sends an RST packet with incorrect sequence number and 'set flow check tcp-rst-sequence' and 'set flow tcp-rst-invalid-session' commands are enabled.

os69272—ISG 1000 with IDP may fail when passing SunRPC traffic through a security module.

cs13366—eBGP neighbor is displayed as an iBGP peer in the “get vr <vr_name> protocol bgp neighbor” command.

VLAN

cs13057—Cannot create sub interfaces in 2 different zones and VRs with the same IP address.

VPN

cs12969—Cannot FTP large files through a VPN to Cisco devices, because the ISG devices change Sequence # randomly causing issues with the VPN tunnel on the Cisco end.

Web UI

cs12816—NS-5200 systems with M2/8G2 modules drops NAT-T UDP packets due to bad UDP checksum.

os70000—If you delete a VSYS using the CLI, the VSYS is still displayed in the WebUI. Selecting this incorrectly displayed VSYS on WebUI will cause the device to fail.

cs12755—In an NSRP environment, you cannot use the WebUI to assign priority when you create a second redundant interface.
W/A: Use the CLI to configure the priority.

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

Getting Help for ScreenOS 6.0 Software

For further assistance with Juniper Networks products, visit http://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.