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 300M-series, SSG 500/500M-series, and NetScreen-5000 series (NS 5000– MGT2/SPM2).

Version: ScreenOS 6.0.0r2

Revision: Rev 04

Part Number: 530-021748-01

Date: February 04, 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 320/350M, SSG 520/520M, SSG 550/550M, 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 5.3r8.

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

> **Note:** NSRP clusters require the use of the same hardware products within a cluster. Do not mix different product models in NSRP deployments.

> **Note:** You can use NetScreen-Security Manager (NSM) 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.

New Features and Enhancements

The sections below describe new features and enhancements available in ScreenOS 6.0.0 releases.

> **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.

New Features and Enhancements Introduced in 6.0.0r2

New Features

PIM Support

The following PIMs are now supported on the SSG 300M-series devices: 6-port GE SFP uPIM, 8-port 10/100/1000 uPIM, 16-port 10/100/1000 uPIM, ADSL2+ PIM, G.SHDSL PIM, 2-port T1 PIM, 2-port E1, and 2-port serial PIM.

2M Session Support on NS 5400

The NetScreen 5400-MGT2 Secure Port Module 2 (SPM2) now supports up to two million (2M) sessions.

> **Note:** Since two SPMs are required to support this feature, the NS 5200 will continue to support only 1M sessions.

SSG 320M/350M Devices

There are now two new SSG platforms introduced in conjunction with the 6.0.0r2 ScreenOS release that will support ScreenOS and JUNOS.

Web User Interface for uPIM Statistics

The WebUI now supports uPIM statistics CLI commands that were available in 6.0.0r1. In earlier releases, the standard counters were not enabled for bgroups on the SSG 140, 520, and 550. This feature adds WebUI support for uPIM statistics. All SSG platforms support this WebUI feature.

IPv6 Support for ISG 1000

The ISG 1000 now supports IPv6. ISG-IDP, however, does not yet support IPv6.

Unified Access Control Clustering Enhancements

Auth table entries are now synced from the active device to the backup device and are retained after failover. Auth table cold-sync support was added to support seamless failover. This feature is supported on all platforms. Note that this feature requires Unified Access Control (UAC) 2.1.

Network Time Protocol Server Support

ScreenOS now includes Network Time Protocol (NTP) server support for intranet hosts using the NTP client service. This feature provides Simple Network Time Protocol version 4 (SNTPv4) support to hosts on the internal network requesting network time. NTP server support is available on all platforms and is enabled per-interface on interfaces with their own IP address. Interfaces without a specific IP address cannot use the NTP server feature. Also, NTP server is not supported on tunnel interfaces.

The implementation currently supports only Unicast mode. CLI commands for NTP server are **[set/unset] interface <if_name> ntp-server** and **get interface <if_name> ntp-server**. The feature supports vsys and NSRP. NTP configuration will be synced if NTP server is enabled on a VSI. IPv6 is supported. Transparent mode is not. NTP server support is implemented according to RFC 2030.

Performance Enhancements

Improve Session Age-Out

This feature decreases the amount of communication between the ASIC and CPU by pushing more information to the session stored in hardware and decreasing the DMA time. This change improves session age-out performance on Juniper Networks hardware-accelerated platforms and should increase the sustained session ramp rate. The feature is supported on the ISG 1000, ISG 2000, ISG-IDP, and NetScreen-5000-MGT2/SPM2.

Improve Policy Installation Performance

This feature optimizes policy installation on Application-Specific Integrated Circuit (ASIC) platforms when changes are made to a single policy or when changes are made that affect the entire policy base. This change will decrease symptoms such as packet loss, high-CPU, and system hangs, which are often experienced when a policy, an address object, or a service object is modified while the device is under load. The feature is supported on all platforms.

Resource Manager ALGs Default Changed to Off

Resource manager Application Layer Gateways (ALGs) will be disabled by default on ASIC-based platforms. Affected ALGs include H.323, SIP, MGCP, Skinny, RPC, and SQL. Please note that this feature will only take effect on a new installation (that is, no active configuration is currently in flash). During high CPU utilization situations, it has been noted that the sources of the high CPU utilization are resource manager ALGs, many of which are never in use on ASIC-

based platforms. The feature is supported on the ISG 1000, ISG 2000, ISG-IDP, and NetScreen-5000-MGT2/SPM2.

TCP 3-way-check in ASIC for NetScreen-5000

This feature moves the TCP 3-way-check to the Packet Process Unit (PPU) in the NetScreen-5000 for both single and multi-ASIC sessions. Performance is greatly enhanced when the TCP 3-way-check takes place in the PPU. The feature is implemented in this release on the NetScreen-5000-MGT2/SPM2 and was available on the ISG 2000 in an earlier release.

NSRP Performance Improvements

NSRP messages are now optimized on high-end platforms to improve performance. The performance improvements apply to the ISG 1000, ISG 2000, ISG-IDP, and NetScreen-5000-MGT2/SPM2.

> **Note:** When upgrading NSRP clusters, it is necessary to upgrade both devices as soon as possible. DO NOT run 6.0.0r1 and 6.0.0r2 simultaneously in the same cluster, because messages will get out of sync, which could result in a device crash.

CPU Protection Tools

CPU Enforcement Distribution

This feature allows administration of the firewall during high CPU situations. In prior releases, attacks were enforced by the CPU, which contributes to very high utilization during the attack. This feature moves enforcement to the ASIC and bases dropped traffic on a customizable blacklist. CPU protection is implemented on the ISG 1000, ISG 2000, ISG-IDP, and NetScreen-5000-MGT2/SPM2. Note that this feature is best used in conjunction with CPU utilization profiling.

The following CLI command is used to create a CPU protection blacklist:
set cpu-protection blacklist id<num> <src-ip/mask> <dst-ip/mask> [protocol <num> [src-port <num>] [dst-port <num>]] [timeout <num>]

CPU protection is independent of vsys; it is a per-device configuration. CPU protection is not synced between NSRP peers and is not supported in IPv6. The feature does support Transparent mode.

CPU Utilization Profiling

This feature allows for prioritization of management traffic over noncritical packets during high-CPU situations. In prior releases, when CPU utilization was very high, the device often became unmanageable. Prioritizing management traffic during high-CPU utilization is supported on the ISG 1000, ISG 2000, ISG-IDP, and NetScreen-5000-MGT2/SPM2. Note that this feature is best used in conjunction with the **CPU Protection** feature also provided in the 6.0.0r2 release.

Note that CPU profiling is independent of vsys, is not synced between NSRP peers, and is not supported in IPv6. CPU profiling does support Transparent mode.

The table below indicates how the CPU profiling feature defines critical and noncritical traffic.

Critical	1	Critical traffic includes **Management Traffic** and **Routing Protocol Traffic**
Noncritical	2	Broadcast
	3	Non-first packet
	4	First packet
	5	Other

NSRP Security Module Monitoring

NSRP configuration options in this release include weighted security module monitoring. Security module (sm) monitoring can be set in an NSRP cluster to ensure that security modules are active and to fail the device if a particular security module fails. If your device includes security modules and any module fails, you can set a weight for each module failure. This gives you the flexibility of deciding whether an entire device should fail if a particular security module on that device fails. To set a failure weight for a security module, run **set nsrp monitor sm <x> weight <num>** in the CLI. The default security module monitored weight is 255.

ISG-IDP Flow Enhancements

ISG-IDP device policy implementation has been changed to improve CPU and memory usage. The management module will no longer perform an infinite loop if communication with a security module fails. A timer is used to try to resend the policy for a predetermined period (60 seconds). If communication fails continuously for 60 seconds, the management module will treat this condition as a policy push failure and send the status back to NSM.

ISG-IDP devices do not handle of out-of-memory errors more gracefully. Before compiling a policy, the amount of memory required to compile that policy is estimated. If it is determined that the free memory available is insufficient, the policy compilation will fail immediately, rather than failing to an irrecoverable state later in the process.

Lastly, in the event of a policy-compile failure on at least one security module, the management module will send a compile cleanup message to all security modules. Upon receiving the compile cleanup message, if the current active

policy has previously been unloaded, then IDP will restart on the security module. Otherwise, memory used by the new compiled policy, if any, will be freed up.

New Features and Enhancements Introduced in **6.0.0r1**

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, see "PIM Power and Thermal Requirements" in the Limitations section.

8-port 10/100/1000 uPIM
The 8-port 10/100/1000 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 bgroups, which let you group several Ethernet interfaces together. Connect to the module using CAT-5 cable.

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

6-port GE SFP uPIM
The 6-port small form factor pluggable (SFP) 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 currently supported by Juniper Networks Technical Assistance Center (JTAC). This PIM also supports up to three 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 SFP 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, or BX, and CAT-5 cable for the copper transceiver.

E-3 Support

ScreenOS now supports E3 PIMs 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 SSG 520M/550M platforms. The two new discrete multitone (DMT) standards supported are:

- **ITU 992.3 (also known as ADSL2):** supports data rates up to 1.2 Mbps upstream and 12 Mbps downstream
- **ITU 992.5 (also known as ADSL2+):** 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 DSL 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 SSG 520M/550M platforms.

ScreenOS 6.0 supports the ITU G.991.2, Single-pair High-speed Digital Subscriber Line (SHDSL) Transceiver discrete multitone (DMT) standard.

Virtual Private Network (VPN)

AutoConnect-Virtual Private Network (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 also reduces processing overhead on the hub and thus improves overall network performance. Because AC-VPN creates dynamic tunnels that time out when traffic stops flowing 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 Scontinue to have the same limitations.

Firewall

WebUI Enhancements

The Web user interface (WebUI) is improved to optimize work flow, display diagnostic information, enhance the homepage, 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 earlier 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:

- o FTP / FTP-Get / FTP-Put should not be in a single service group.
- o FTP/ FTP-Get /FTP-Put should not be defined for one single policy.
- o FTP-Get or FTP-Put is the same as FTP service in policies with deny action.
- o 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 a series of **get** commands to gather information in the background, but not all **get** commands are supported.

Note: Depending on the information gathered, CPU usage is affected.

Universal Threat Management

AV Scanning for IM Services

ScreenOS supports antivirus (AV) scanning for instant messaging (IM) services such as AIM, ICQ, Yahoo! Messenger, and MSN Messenger. AV scanning is supported for text/group chat messages and for 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 a best-effort basis.

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 the high-memory option to run AV scanning. Supported platforms are the 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 actions:** 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 are now supported on the ISG 1000, ISG 1000-IDP, ISG 2000-IDP, and NetScreen-5400 devices.

- **IDP inspection of GTP-encapsulated and GRE-encapsulated traffic:** The ISG 1000 and ISG 2000 with IDP 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 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 application marking:** 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:
- Added user IP address to authentication logs

- Support for TACACS+ authentication servers

- Prioritized authentication between external server and local database

- Increased number of permitted administrator IP addresses

- Enhanced 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

Virtual Systems

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 (vsys). The ISG 1000 now supports up to 50 vsys (increased from 10). The ISG 2000 now supports up to 250 vsys (increased from 50). To take advantage of these increases in vsys support, you must install a new license key.

- **Virtual system names:** Vsys names can contain up to 20 characters. Previously,vsys names could contain up to 10 characters.

Network Address Translation

DIP Pool Enhancement

The number of dynamic Internet Protocols (DIP) pools per vsys is increased to 1020 on all platforms. For low-end platforms, the maximum number of DIP pools is 1000; and for some high-end platforms supporting vsys, 51K for ISG 1000 and 64K for NetScreen 500, NetScreen-5000, NetScreen 5400, and ISG 2000.

NetScreen Redundancy Protocol

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 devices.

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 antispam) on a per-role basis. This allows you to make policy decisions such as activating AV for partners or untrusted machines, or turning on Web filtering for specific roles.

- Increased number of auth table entries

Devices	Auth Table Entries
SSG	10,000
ISG	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. 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 bgroups 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 ISG 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, and NetScreen-5000 series devices.

Management IP Address Limit Increased

The total number of IP addresses from which a security device can be managed is increased to 50 plus 1 times the number of virtual systems. 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 ISG 1000 and ISG 2000 with IDP and on the NetScreen 5200/5400.

Universal Serial Bus Support

Universal Serial Bus (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. USB functionality is available on SSG devices.

The following USB flash drives have been tested and found to work properly with SSG devices:

- Lexar JumpDrive Firefly 1GB

- Kingston Datatraveler 2GB

- PNY attaché 256M

- SanDisk Cruzer Micro 512M

Some other USB flash drives have been found to not work properly with 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 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.)

Changes to Default Behavior

Changes to Default Behavior Introduced in <u>6.0.0r2</u>

This section lists changes to default behavior in ScreenOS 6.0.0r2 from previous ScreenOS firmware releases.

Max Dialing Interval Default

The maximum dialing interval has changed from 60 to 600 seconds. This resolves an issue in previous releases regarding the dialing interval in that sometimes dialing failed but the device did not wait long enough and instead redialed almost immediately.

CPU Protection and Utilization Profiling

As a result of implementation of CPU protection and utilization profiling features in this release, the **set firewall ppu** command is now hidden and nonfunctioning. Systems that currently have the command set will lose the setting when upgrading to this release.

TCP-SYN-Check Packet Flow

In previous ScreenOS releases, all three handshake packets (SYN, SYN-ACK, and ACK) were sent to the CPU when you set **TCP-SYN-Check**. This was the case for single-ASIC, dual-ASIC, and multi-ASIC platforms. With the 6.0.0r2 release, only the first packet (SYN) will be sent to the CPU with the following two packets (SYN-ACK and ACK) processed by the PPU (ASIC) when you set **TCP-SYN-Check**.

Infranet Auth Object Cleanup

In releases prior to 6.0.0r2, infranet auth table entries were removed as soon as connectivity with the Infranet Controller was lost. In this release, infranet auth table entries remain for two minutes while the device attempts to reestablish a connection to the Infranet Controller.

When combined with Infranet Controller changes scheduled for release in UAC 2.1, the delay in removing auth table entries allows for better failover in Infranet Enforcer and Infranet Controller clusters.

Infranet Auth Cold Start NSRP Synchronization

In releases prior to 6.0.0r2, infranet auth table entries were synchronized between nodes in an NSRP cluster as long as both nodes were up and communicating with each other. Any infranet auth table changes that occurred while one node was down, however, would not be seen by the other node.

In this release, the infranet auth table entries are synchronized between the two nodes of an NSRP cluster when they start communicating with each other.

Infranet Controller and Management IP

In releases prior to 6.0.0r2, it was not possible to use an interface with a management IP configured to communicate with the Infranet Controller. This was because the NACN message was sent from the non-management IP, and the Infranet Controller would attempt to ssh back to the Infranet Enforcer using the non-management IP, resulting in a failed connection.

In this release, the management IP (if configured) is used to send NACN messages to the Infranet Controller.

Removing Denied Sessions on Auth Table Change

In releases prior to 6.0.0r2, upon removal of an infranet auth table entry, all associated sessions were terminated. However, other changes to the infranet auth table or infranet auth policies had no effect on existing sessions. In this release, when an infranet auth table entry changes, all of its associated sessions are reevaluated. Any that are no longer allowed are terminated.

Changes to Default Behavior Introduced in 6.0.0r1

This section lists changes to default behavior in ScreenOS 6.0.0r1 from previous ScreenOS firmware releases.

TCP-SYN-Check Default

The default for NS-5200/5400 devices is **set flow tcp-syn-check,** which includes both SYN-bit check and a three-way handshake. In ScreenOS 6.0.0r1, the default is **set tcp-syn-bit-check**.

RADIUS Attributes

In ScreenOS 6.0.0r1, both calling-station and called-station IDs are supported as default behavior.

IP Option Packets

The IP option packets (record-route and timestamp) in ScreenOS 6.0.0r1 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.

Addressed Issues

This section describes addressed issues with the current release and includes the following sections:

Addressed Issues in ScreenOS 6.0.0r2

> **Note:** Due to an update in the ScreenOS problem tracking system, some issues listed here have two bug numbers. The six-digit numeric code shown first is for the new system; the "**os**" and "**cs**" numbers included in the listing for some issues are provided as a reference to older Known Issues. Eventually the older reference numbers will be phased out.

The following operational issues were resolved in this release:

Antivirus

- **224994 [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."

- **218326 [os66700]—**Yahoo! Messenger IM file transfer from the Internet does not get scanned when "set av http skipmime" is enabled.

- **225910 [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**.

- **225920 [os70207]—**Under high stress conditions with AV, it is possible to see FTP traffic blocked.

  W/A: Restart or reduce traffic through the device.

HA and NSRP

- **224248 [os69429]—**"Unset interface <name> ip manageable" is not propagated from master to slave.

IDP

- **224257 [os69438]—**Under heavy traffic conditions, if the IDP Profiler is enabled, the CLI may respond slowly.

- **224759 [os69720]—**If you see this event log, "dma_transmit failed to 1," then you've reached the maximum capacity of your device.

Other

- **226119 [os70287]—**Global DIP pool limit is 1K on SSG devices.

- **224307 [os69468]—**There is no option to clear the newly introduced bgroup interface counters on the SSG140.

- **224500 [os69570]—**On the SSG 20 devices, operating mode configured for ADSL2 or ADSL2+ is always incorrectly seen as **auto** in the WebUI.

- **221408 [cs12430]—**Some MGCP protocol extension traffic was being dropped by the MGCP ALG.

  W/A: Turn off MGCP ALG.

- **229379—**After upgrading from ScreenOS 5.4 to 6.0.0r1, SQL traffic may fail to pass through the device.

Routing

- **223879 [os69272]—**ISG 1000 with IDP may fail when passing SunRPC traffic through a security module.

WebUI

- **225485 [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.

- **222724, 121948 [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.

- **227317 [cs13945]—**On SSG20-wireless devices, it is not possible to use the WebUI to bind a wireless interface to an SSID. Attempting to do so will result in a Web error page.

Known Issues

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

- **Limitations of Features in ScreenOS 6.0.0r1**—identifies features that are not fully functional at the present time and that will be unsupported for this release.

- **Compatibility Issues in ScreenOS 6.0.0r1**—describes known compatibility issues with other products, including, but not limited to, specific Juniper Networks appliances, other versions of ScreenOS, Web 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 6.0.0r2**—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.

- **Known Issues from ScreenOS 6.0.0r1**—describes deviations from intended product behavior discovered in 6.0.0r1 that may still exist in 6.0.0r2 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 of various features in ScreenOS. They apply to all platforms unless otherwise noted.

- **SSG 500-series**—Bridge groups (bgroups) are supported on Ethernet switch PIMs (uPIMs), including 16-port GE, 8-port GE, and 6-port SFP. Bgroups are not supported on 1-port SFP, old enhanced PIMs (ePIMs), and on-board GE ports. Bgroup interfaces can be dynamically created and deleted. The maximum number of bgroup interfaces on each PIM is half the number of ports.

- **SSG 140**—Bgroups are supported on both on-board Ethernet ports and Ethernet switch PIMs (uPIMs). Bgroup interfaces can be dynamically created and deleted. The maximum number of bgroup interfaces on each PIM is half the number of ports. For the on-board ports, three bgroup

interfaces are precreated. Bgroup interfaces can be configured on the same PIM or the system board only.

- **IPv6 ASIC support in NetScreen-5000 systems**—Because NetScreen-5000 systems now support IPv6, per-ASIC session support has been decreased from 1M to 512K. This is caused by the increase in the session size in the session table. This limitation should have minimal impact on most customers. Note that to achieve maximum session count on the NS-5000 series firewalls, it would be best to design the network to utilize multiple ports on the SPMs. This type of network architecture would distribute the sessions to multiple ASICs. For example, if only two ports on an 8G2 SPM card are used, the max session count value will be 512K.

- **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 the CPU instead of the 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 frames. All other I/O cards in the device are disabled automatically (including the ISG 1000 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 browser or apply the default Help Link Path button in the WebUI under **Configuration>Admin>Management.** Because of the cookies Juniper Networks sets 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 AV 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, the values are represented as nondimensional tokens.

Device	Available Tokens	
	Power	Heat
SSG 140	67	67
SSG 320M	50	50
SSG 350M	84	84
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* (formerly *Migration 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.

Use 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]:

3. 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 "Upgrading to the New Firmware" in the ScreenOS *Upgrade Guide* for instructions on performing the upgrade.

Known Issues in ScreenOS 6.0.0r2

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**.

> **Note:** Due to an update in the ScreenOS problem tracking system, some issues listed here have two bug numbers. The six-digit numeric code shown first is for the new system; the "**os**" and "**cs**" numbers included in the listing for some issues are provided as a reference to older Known Issues. Eventually the older reference numbers will be phased out.

Antivirus

- **233302**—Under unusual circumstances, when AV is enabled and there is heavy traffic through the device, an SSG 20 may fail and restart without warning or any other indication that there is a problem.

- **226198 [os70325]**—Under some conditions, AV supplemental CLIs cannot be pushed to the device because NSM erroneously reports that the AV license is not installed.

- **227591 [os70991]—**When enabling AV and updating the AV database (either manually or automatically), CPU utilization may reach 90% after a short time.

HA and NSRP

- **234401—**Under certain long-term heavy traffic circumstances, if VPN traffic is running through an ISG 2000-IDP in an active-passive NSRP cluster, the active device may reset.

- **227728 [cs14043]—**ScreenOS does not currently support redundant or aggregate interfaces in an active-active HA pair of ISG 2000 systems. Packets received on the backup device cannot pass through the cluster in an active-active ISG 2000 pair.

   W/A: Avoid using the redundant interface to forward traffic.

- **227073 [os70785]—**Under certain circumstances, an NSRP cold sync may require half an hour to complete when processed under heavy traffic conditions.

- **228679—**The command "set syslog src-interface XXX" is synced to the backup device in an NSRP cluster even when the src-interface is a local interface.

- **226337 [cs13767]—**In an NSRP environment, if a policy has passed infranet auth, when the session permitted by the policy is synced to the backup device, the timeout of sessions on the backup is set to 10 seconds and will quickly age out, terminating the connection.

IDP

- **226383 [os70393]—**When major and minor attacks are configured in the IDP rulebase, FTP attacks are not detected within a GTP tunnel.

   W/A: 1. Configure a rule in the IDP rulebase with GTP service selected and no attacks and action. Configure another rule with attacks selected (major and minor) and action. 2. Now, when FTP root attacks are triggered, they will be detected in either direction.

- **228623—**With FTP attacks configured in the IDP rulebase, the GTP tunnel goes into the Ignored state, meaning that FTP attacks are not detected within the GTP tunnel.

   W/A: 1. Configure a rule in the IDP rulebase with GTP service selected and no attacks and action. Configure another rule with attacks selected (FTP attacks category) and action. 2. Now, when FTP root attacks are triggered, they will be detected in either direction.

- **232420—**An ISG 2000 device running ScreenOS 6.0.0r1 with IDP in Inline mode causes packets to be dropped for return traffic if NAT and a

mirror port are both configured. Note that this is not a recommended configuration.

- **229680—**When running an ISG 1000 appliance in Transparent mode with IDP in Tap mode, packet sizes larger than 1500 bytes cannot be fragmented into the proper size. Some applications may fail under these circumstances.

- **229975—**An ISG 2000-IDP may intermittently stop advertising prefixes to eBGP peers after BGP peer refreshes from other devices.

   W/A: Run the **unset enable** and **set enable** commands inside the BGP protocol configuration.

- **232805—**In Transparent mode on an ISG 1000 with IDP enabled, if both Web filtering and IDP are enable in one policy, all Web browsing that uses the policy will hang.

Management
- **233428—**In Transparent mode, the management feature on a v1-Untrust zone is not added to the configuration, so it becomes disabled after a device reset.

- **234025—**On the SSG 140 platform, DNS settings cannot be accepted through a PPPoE connection.

- **226201 [os70328]—**It is possible that during a configuration save, a "Read of flash block 193 failed before write" message will appear on the console. If this happens, please try to save the configuration again.

Other
- **226637 [os70613]—**The ICMP signature with time-binding enabled is not triggered when the number of attacks found is equal to the count specified in the time-binding settings. For ICMP packets, there is no concept of a session. Therefore, on ISG platforms, the packets are distributed between the two CPUs on the security module. As a result, the number of attacks for ICMP packets is tracked separately on each CPU. Only if the number of attacks found is equal to the count specified in the time-binding settings will the signature be triggered. This is unavoidable on an ISG device because the memory is not shared between the processes.

   W/A: One solution is to set the count in the time-binding settings to be half the value of the number of attacks that need to be seen.

- **233385**—Packets may get dropped with the message "dip with port translate allocation fail" if an interface-based DIP (NAT-Src from the egress interface IP address) is applied.

- **226595 [os70571]**—When a voice call is invoked from v1-trust to v1-untrust under Transparent mode, it is possible that one session with timer at 0 will be stuck in the register and unremovable.

- **226115 [os70283]**—Sometimes after a blacklist is unset, traffic may be blocked.

  W/A: Please restart the device and try again.

- **226377 [os70387]**—When creating a cpu-protection blacklist during heavy traffic, it may take up to six seconds to make the blacklist work. During this period, it is not possible to execute **cpu-protection** CLI commands. Under normal traffic circumstances, this process should take less than one second.

- **233140**—Under some circumstances when the RADIUS auth server is configured, the device will fail to execute the **set auth-server xxxx** command after a restart.

- **226582 [os70558]**—Under extreme circumstances, the device may crash if a blacklist is set or unset repeatedly during heavy traffic.

- **230155**—The **get fprofile** command may cause a device crash when packet profiling is enabled.

- **231754**—In Transparent mode, SIP traffic may cause a device crash.

- **228479**—When an SSG 550 is working between client and proxy servers in Transparent mode with DI enabled, the device interprets the traffic from client to server on port 80 as an "HTTP:Overflow:Content-Overflow" attack and drops it.

- **227782 [os71064]**—Under some narrow circumstances when deploying NTP server on ISG 1000 appliances, a hardware session is refreshed by a packet but will still be aged out immediately.

- **233872**—After a restart followed by many hours of heavy traffic, an SSG 5 may stop forwarding all traffic.

- **227641 [os71009]**—Sometimes invalid session information will be read from the ASIC chip while executing "get db s" on the console and the packet will be dropped. This happens very infrequently.

- **226193 [os70320]**—Under some conditions, it may take up to 30 minutes to load 8191 tunnel interfaces on NetScreen-5000 series platforms during startup.

- **233516**—After a large number of configuration changes (policy and VR changes particularly), an ISG 2000 may stop receiving IPv6 packets.

- **229234**—When setting a Web filtering profile name that includes a space, after reset the profile cannot be saved.

- **226044 [os70254]**—Under some circumstances, the warning message "st_demux_bad_sess_id_from_SM_proc is not support in this build" may display on the console. This message is for debug purposes and can be safely ignored.

- **227592 [os70992]**—The environment variables **nsrp-max-vsd** and **nsrp-max-cluster** must be a power of 2 value from this release. Although the function still works, the current value may not be a power of 2 if it was set using an earlier release.

  W/A: Reset the environment variables after upgrading to this release.

- **228675**—When configuring a track-ip object using ARP and binding it to a special VSD group, the track-ip object will be lost after reset. In other words, the CLI command **set nsrp vsd x track-ip ip x.x.x.x method arp** setting will be lost after a reset. The impact is limited to this track-ip object and does not affect any other function.

- **226651 [os70627]**—When traffic reaches 1Gbps (in each direction) through two uPIMs, traffic will be blocked in both directions after approximately one hour.

- **231513**—When configuring a policy with multi-cell service or a service group that includes predefined services in the multi-cell or service group, traffic that matches this policy may have an incorrect timeout value.

- **231101**—After heavy HTTP/FTP/UDP mixed traffic, several sessions could not be aged out. The sessions will only be cleaned up following a device reset. The issue is caused by a PCI problem that causes the device to read a bad session index from the hardware.

- **226217 [os70336]—**When the IP address of a remote peer changes, IKE phase 1 may fail to update correctly.

  W/A: Clear the IKE cookies, SA, or DNS cache to force VPN to use the correct IP address.

- **234058—**If an IKE gateway peer address is configured to be IPv4 but the local address is an IPv6 address, the device will fail and need to be reset.

- **236113—**On the NetScreen-5000 platform, if TCP-SYN-Check is enabled, a cross-chip TCP connection cannot be established in Transparent mode.

  W/A: Disable TCP-SYN-Check.

- **238795**— On SSG 300M-series devices, you cannot upgrade the bootloader v3.0.5 or upload firmware via the bootloader when the SSG 300M-series device is connected to the TFTP server via an HP 1800-24G switch.

  W/A: Connect the TFTP server directly to the SSG 300M-series device.

Performance
- **234168—**When deleting a policy, there are many tasks that need to be accomplished. For example, sessions must be scanned for policy rematching and policies must be deleted from hardware. These operations are CPU intensive, so CPU usage is very high when many policies are simultaneously deleted.

Routing
- **228200—**An alternate route cannot be added to the routing table and be active after a tunnel failure. This issue will occur when using the **set interface tunnel_name protocol rip demand-circuit** command.

VPN
- **231887—**When running a policy-based VPN together with Web filtering configured on an SSG140, the device may crash under heavy traffic.

- **230357—**When multiple users who belong to the same VPN group try to connect via dialup VPN simultaneously, some connections will fail because of concurrent IKE negotiation limits. An event log entry will be made. Here is an example log entry:

  ```
  Discarded peer's P1 request because there are
  currently <089> sessions--max is <075>. (2007-02-18
  12:28:49)<000>
  ```

- **233217—**In some situations, for example when an IPsec tunnel is configured, NetScreen-5000 devices cannot fragment 1500 byte VPN packets to the proper size and will instead drop the traffic.

WebUI

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

- **230134—**After creating an aggregation interface on an ISG 1000, the WebUI shows all interfaces as one member of this aggregation interface. This is only a Web display issue. The device will function properly.

- **232569—**If quality of service (QoS) is configured on a Voice-over-IP (VoIP) policy via the WebUI, the setting cannot be saved.

- **234071—**Under some circumstances, the ADSL PPPoE interface service option cannot be changed via the WebUI. It can, however, be changed via the CLI or NSM even if configuration fails using the WebUI.

Known Issues from ScreenOS 6.0.0r1

The following are known deficiencies in features at the time of release of ScreenOS 6.0.0r1. Whenever possible, a workaround is suggested following the problem description, preceded by **W/A**.

> **Note:** Due to an update in the ScreenOS problem tracking system, some issues listed here have two bug numbers. The six-digit numeric code shown first is for the new system; the "**os**" and "**cs**" numbers included in the listing for some issues are provided as a reference to older Known Issues. Eventually the older reference numbers will be phased out.

Antivirus

- **225186 [os69903]—**Running heavy IM traffic for over a day on SSG5/20 may cause memory issues.

- **220962 [os67933]—**You may experience a lost or delayed file transfer request if a MSN IM session is idle for more than 20 minutes.

- **225915 [os70202]—**When Yahoo! Messenger instant messaging antivirus 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 **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.

- **225916 [os70203]—**MSN users 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.

HA and NSRP

- **221391 [os68106]**—FTP sometimes fails to complete in an NSRP active-passive setup. The data transfer fails when failover and fallback happen frequently during the FTP transfer.

- **224082 [cs13209]**—A backup device does not handle ARP requests when the interface is in Inactive mode or when the interface is disconnected and then reconnected.

- **217312 [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.

- **220335 [cs12194]**—In some cases on the ISG 2000, FTP data transfers do not complete in an active-passive NSRP failover.

IDP

- **225442 [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.

- **223283 [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 is not supported.

- **225124 [os69887]**—On 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 module. For example, for security module 1, the command is **#exec sm 1 ksh "scio policy unload s0"**

Management

- **222914 [cs12801]**—In some cases, when you update the certificate for one vsys using NSM, another unrelated vsys certificate may be removed.

- **221467 [os68130]**—This is an NSM only issue. Import Configuration in NSM may fail if your device has a backslash (\) in the parameter string. The problem stems a from lack of escape sequence for commands, such as 'set av mime-list' where NSM considers backslash as a control character.

Other

- **214251 [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.

- **223155 [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.

- **219115 [cs11922]**—If a very small fragmented packet is sent to the FPGA, it is possible that it will be delayed until a larger packet is received to trigger the FPGA hashing functionality.

- **223996 [cs13176]**—In scenarios using the ARP method for track-ip, changing the track-ip interval may cause track-ip failure.

- **222710 [os68704]**—SSG 520, SSG 550, SSG 520M, and SSG 550M 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.

- **223684 [cs13083]**—When using the GTP feature in ScreenOS, the PDP Request filtering checks the Access Point Name (APN) in the Information Element (IE), which is sometimes not supplied.

- **222850 [os68781]**—On the SSG 5 device, if the **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.

- **224249 [os69430]**—An SSG 20 device fails if you insert a write-protected USB device followed by a **get file** command.

- **223776 [cs13119]—**After the backup firewall is started and if the NSM server sends a FIN packet to it, the backup firewall, when sending resets, uses virtual MAC rather than physical MAC. This causes traffic disruption for short periods (~ 30 seconds) if this packet passes through a switch.

- **224099 [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
- **222946 [os68825]—**After long durations of heavy attack traffic conditions, the device may display "bad session id" messages incorrectly.

- **224845 [os69772]—**Memory issues may occur on the ISG 1000 with IDP running in Transparent mode with all attacks installed.

- **223070 [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
- **215642 [cs11355]—**ISG 1000 and ISG 2000 devices do not terminate a TCP session immediately when a client sends an RST packet with an incorrect sequence number and with **set flow check tcp-rst-sequence** and **set flow tcp-rst-invalid-session** commands enabled.

- **224606 [cs13366]—**eBGP neighbor is displayed as an iBGP peer in the "**get vr <vr_name> protocol bgp neighbor**" command.

VLAN
- **223634 [cs13057]—**Cannot create subinterfaces in two different zones and VRs with the same IP address.

VPN
- **223339 [cs12969]—**Cannot FTP large files through a VPN to Cisco devices, because the ISG devices change sequence numbers randomly, causing issues with the VPN tunnel on the Cisco end.

WebUI
- **222963 [cs12816]—**NS-5200 systems with M2/8G2 modules drops NAT-T UDP packets due to bad UDP checksum.

- **222872 [cs12797]—**In some situations, when accessing the firewall's WebUI interface, the WebUI homepage takes a long time to load.

Documentation Changes

The sections below describe changes that pertain to the ScreenOS documentation.

Documentation Changes Introduced in 6.0.0r2

ScreenOS 6.0.0r2 includes minimal changes to the provided documentation. Online help files have been updated to reflect Web user interface (WebUI) modifications, and this release note document describes new features offered in 6.0.0r2. No other changes have been made to other volumes of ScreenOS documentation for release 6.0.0r2. All new features available in 6.0.0r2 will be fully documented in the next ScreenOS release.

Documentation Changes Introduced in 6.0.0r1

To upgrade existing firmware to ScreenOS 6.0, refer to the ScreenOS *Upgrade Guide* located at http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/upgrade_guide .pdf. The SSG 500/500M-series devices require boot loader upgrade. For more information on the upgrade procedure, see "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 Physical Interface Modules (Mini-PIMs) from the installation and configuration guides for SSG devices. We have moved this information into a new guide, the *PIM and Mini-PIM Installation and Configuration Guide*. Refer to that guide for information on configuring PIMs and Mini-PIMs.

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.