Juniper Networks ScreenOS Release Notes

Release 6.1.0r2
June 2008
Part Number: 530-025799-01
Revision 02

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–MGT3).

Contents

Version Summary

ScreenOS 6.1.0 firmware can be installed on the following products: Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 320M/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 the NS-5000-MGT3 module.

This release incorporates the ScreenOS maintenance releases up to 6.0r4, 5.4r8, and 5.3r10.

NOTE:

- If you are using an SSG 500-series device and an SSG 500M-series device in a NetScreen Redundancy Protocol (NSRP) environment, all devices must be running ScreenOS 6.0r1 or later.
- NSRP clusters require the use of the same hardware products within a cluster. Do not mix different product models in NSRP deployments.

New Features and Enhancements

The sections below describe new features and enhancements available in the ScreenOS 6.1.0 release.

NOTE: You must register your product at http://support.juniper.net to activate licensed features such as antivirus, deep inspection, and virtual systems on the device. To register your product, you need the model and serial numbers 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 your device has Internet connectivity. Use the exec license-key update all command to connect the device to the Juniper Networks server and activate the feature.

NOTE:

- You can use NetScreen-Security Manager (NSM) 2007.3 with the Forward Support Update software to manage devices running ScreenOS 6.1. 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 6.1.0 Release Notes* for installation instructions and the features and platforms supported with this schema upgrade.

New Features and Enhancements Introduced in 6.1.0r2

The section below describes the new features introduced in the ScreenOS 6.1.0r2 release.

ISG-IDP Session Pass Under Heavy Throughput

An option to allow sessions to pass through without inspection under heavy throughput conditions has been introduced in this release. This feature bypasses traffic inspection for some sessions when the Intrusion Detection and Prevention (IDP) Security Module (SM) is unable to stay in lockstep with incoming traffic while continuing to inspect other packets. You might use this feature when you are sensitive to packet drops and want to enable an on/off switch to have packets inspected at the firewall level instead of through the security module. By default, this feature is off; that is, as in previous releases, all traffic is inspected by IDP and under heavy throughput, some packets may be dropped.

To enable this feature, use the following command syntax:

```
exec sm sm_id ksh "scio const set sc_adapt_enable 1"
```

You need to run this command on each IDP SM. The valid sm_id values are 1, 2, 3.

To disable this feature, use the following command syntax:

```
exec sm sm_id ksh "scio const set sc_adapt_enable 0"
```

When enabled, throughput conditions are taken into account and bypassing packet inspection is done using a set of criteria. Traffic conditions will result in IDP operating in the following modes:

- Normal inspection—All traffic is inspected by IDP.
- Basic cut-through mode—All new sessions will be marked as cut-through and will be allowed to pass uninspected. The first packet of the session received by the Security Module triggers the cut-through marking. It is possible for subsequent packets to still be sent to the Security Module before the Management module takes cut-through into effect. All these subsequent packets are sent out without inspection.
- Progressive cut-through mode—All sessions for which packets are being observed by the IDP security module will be bypassed.

Log messages are issued for any IDP bypass state. The six log types for session bypass state changes are:

- Normal to basic cut-through
- Basic cut-through to normal
- Basic cut-through to progressive cut-through
- Progressive cut-through to basic cut-through
- Normal to progressive cut-through
- Progressive cut-through to normal

Here are details of the log messages:

- Category is NS_LOG_CATEGORY_ALARM
- Logtype is NS_LOG_ALARM_OTHERS
- Severity is NS_LOG_SEVERITY_WARNING
- Service is cutthrough_transit. Its values and means are:
  - SC_LOG_CUTTHROUGH_NORM_TO_LOW = 1
  - SC_LOG_CUTTHROUGH_LOW_TO_NORM = 2
  - SC_LOG_CUTTHROUGH_LOW_TO_HIGH = 3
  - SC_LOG_CUTTHROUGH_HIGH_TO_LOW = 4
  - SC_LOG_CUTTHROUGH_NORM_TO_HIGH = 5
  - SC LOG_CUTTHROUGH_HIGH_TO_NORM = 6

Here is a sample log message for status changes:

SM %d IDP (cpu %u) transits from %s. %u sessions was bypassed in the previous state!

The log also includes log version, timestamp, device_domain_id, device_record_id, device_domain_ver2, and policy_id.

You can use counter commands to get information about whether a CPU is in cut-through mode and the number of sessions that were set to cut-through mode. For example:

exec sm 1 ksh "scio counter get kpp

…

sc_kpp_loopback

sc_kpp_norm2low

sc_kpp_low2high

sc_kpp_high2low

sc_kpp_low2norm

…

exec sm 1 ksh "scio counter get flow

…

sc_flow_session_basic_cutthrough 0

sc_flow_session_progress_cutthrugh 0

sc_flow_cur_cutthrough_sessions 0

New Features and Enhancements Introduced in 6.1.0r1

The section below describes the new features introduced in the ScreenOS 6.1.0r1 release.

Hardware Features

- **1X100/1000 SFP Ethernet uPIM**—With ScreenOS 6.1.0, a new 1-port small form-factor pluggable (SFP) Ethernet PIM is now available for the SSG 140, SSG 320M, SSG 350M, SSG 520, SSG 520M, SSG 550, and SSG 550M platforms. This new Ethernet PIM supports the following transceivers: 1000Base-T; Gigabit Ethernet LX, and SX; and 100Base-FX. This 1-port SFP Ethernet PIM does not support spanning tree, Jumbo frames, bridge groups, hot-swapping, or 802.3ad (Link Aggregation).
- **SSG 300M-series 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, and ADSL2 + PIM.
- **New NetScreen-5000 Modules**—The NS-5000-MGT3, NS-5000-8G2-G4, and NS-5000-2XGE-G4 are new modules that you can install in your NetScreen-5000 series device. These modules increase the performance of the device when it is running ScreenOS 6.1 or later software:
  - **NS-5000-MGT3**—Management (MGT) module for NetScreen-5000 series devices with dual 1.4 GHz PowerPC processors. Comes preinstalled with ScreenOS 6.1 software. Use only with either an NS-5000-8G2-G4 or NS-5000-2XGE-G4 Secure Port Module (SPM).
  - **NS-5000-8G2-G4**—SPM for NetScreen-5000 series devices with eight 1-Gigabit SFP sockets for hot-swappable transceivers. Use only with NS-5000-MGT3 modules.

  - **NS-5000-2XGE-G4**—SPM for NetScreen-5000 series devices with two 10-Gigabit XFP sockets for hot-swappable transceivers. Use only with NS-5000-MGT3 modules.

- **1-port 10 Gigabit I/O Module**—The 1-port small form-factor pluggable (XFP) Ethernet I/O module is now available for the ISG 1000, ISG 2000, and ISG 2000 with IDP platforms. This new module supports the following transceivers: 10GBase-SR and LR, and supports jumbo frames (maximum packet size 9830 bytes).

Software Features

Virtual Private Network (VPN)

- **IKEv2**—ScreenOS 6.1.0 adds support for the Internet Key Exchange protocol version 2 (IKEv2). Both IKEv1 and IKEv2 gateways can exist on a ScreenOS device. Note, however, that both ends of a tunnel must use the same IKE version. A tunnel may not be created that uses IKEv1 at one end and IKEv2 at the other.

  The primary advantage of IKEv2 is that it permits different negotiations at both ends of a tunnel. IKEv2 avoids IKE denial of service (DoS) attacks by using a stateless cookie and verifying the peer address before committing IKE negotiation resources for the peer. IKEv2 supports Diffie-Hellman (DH) groups 1, 2, 5, and More Modular Exponential (MODP)14 (RFC 3526).

- **IKEv2 with EAP**—All platforms running ScreenOS 6.1.0 support IKEv2 with Extensible Authentication Protocol (EAP).

- **DSCP Marking per Phase-2 Proposal**—Administrators can now configure the Differentiated Services Code Point (DSCP) marking per phase-2 proposal to interact with Multiprotocol Label Switching (MPLS) traffic engineering. After an administrator has enabled DSCP marking per phase-2 proposal, he or she can configure traffic routing into different tunnels.

- **Session Rerouting Between Tunnels and Physical Interfaces**—ScreenOS 6.1.0 allows the traffic to fail over between route-based VPN tunnels and physical interfaces in the same zone when the security devices are deployed in a fully redundant network design consisting of dynamic routing and route-based VPNs. Without this feature, if a session that originated over an Ethernet link traverses a VPN link (or vice versa) as a result of routing changes, traffic flow will stop, requiring you to restart your applications. This feature reroutes the session and avoids the need to restart applications.

Firewall

- **Customizable Reject Message for Integrated SurfControl**—Administrators can now create a custom reject message when Integrated SurfControl denies access to a URL.

- **Apple iChat ALG**—ScreenOS 6.1.0 provides an Application Layer Gateway (ALG) for Apple iChat applications up to version 3.15 that facilitates text, audio, and video chat.

- **Per-Policy Source-IP Session-Rate Limit**—Administrators can now set session-rate limits for source IPs on a per-policy basis.
- **Traffic Shaping on WAN Interfaces**—Traffic shaping is now supported on Frame Relay and Multilink Frame Relay interfaces on SSG devices. This includes the T1/E1, T3/E3, and 2M-Serial interfaces on the SSG 5/20, SSG 140, SSG 320M/350M, and SSG 520/520M/550/550M devices.

Internet Protocol Version 6 (IPv6) Support

- **IPv6 Support**—IPv6 is now supported on SSG 140, SSG 320M/350M, SSG 520/520M, and SSG 550/550M platforms.
- **ISG 1000 and ISG 2000 with 1GB Memory**—The ISG 1000 and ISG 2000 both support IPv6 with 512K sessions on devices with 1GB of memory.
- **Protection Against SYN-Flood DoS Attacks**—SYN-Proxy and SYN-Cookie mechanisms are now supported for IPv6 to protect against SYN-Flood DoS attacks.
- **IPv6 Support for WAN Interfaces**—IPv6 is now supported on E1/T1, E3/T3, and 2M-Serial interfaces on the SSG 5, SSG 20, SSG 320M/350M, SSG 520/520M, and SSG 550/550M platforms.
- **IPv6 ALGs**—IPv6 support has been added for Sun and MS RPC ALGs, Session Initiation Protocol (SIP), and Real-Time Streaming Protocol (RTSP) ALGs.

NOTE: ScreenOS 6.1.0 includes support for these ALGs in both IPv4 and IPv6 environments. The ALGs are not, however, triggered when doing network address translation-port translation (NAT/PT) or in IPv4 to IPv6 and IPv6 to IPv4 translations.

Universal Threat Management (UTM)

- **AV/DI Pattern Update Proxy**—ScreenOS allows you to specify a proxy server through which the security device can download antivirus (AV) and deep inspection (DI) pattern updates in case your security device is not directly connected to the Internet.
- **AV Maximum File Size Increase**—In this release of ScreenOS, the maximum file size that the AV engine is able to scan has increased from 10MB to 30MB on all SSG devices.

IDP and GPRS

- **IDP IPSec ESP-Null Encryption Inspection**—ScreenOS 6.1.0 now supports inspection of the traffic within IPSec tunnels that use the Null Encryption method. This is supported on ISG 1000 and ISG 2000 with IDP Security Modules.
- **IDP Session Log Correlation**—IDP logs sent to the NetScreen-Security Manager (NSM) server now contain the session ID to aid in correlating attack logs with firewall session logs.

Authentication

- **Captive Portal for WebAuth**—In earlier releases of ScreenOS, if you wanted to access a protected resource behind WebAuth, you had to navigate to the WebAuth address to authenticate and then navigate to the address of the protected resource. Now you can navigate to the protected resource, and if you need to authenticate via WebAuth, you will be redirected to the authentication page. After the credentials are identified, you are forwarded to the original protected resource.

Network Address Translation (NAT)

- **PPTP ALG on ISG 1000/2000 and NS5x00**—High-end devices now support Port Address Translation (PAT) for Point-to-Point Tunneling Protocol (PPTP), allowing multiple remote users to use PPTP through a ScreenOS device.
- **Multiple Non-Contiguous Subnets in a DIP Pool**—ScreenOS 6.1.0 now allows administrators to configure up to three non-contiguous subnets in a single fixed-port DIP pool. It is no longer necessary to have a single large subnet with consecutive IP addresses in order to configure a DIP pool. This will help with situations where users were denied access when the DIP pool was exhausted and no consecutive IP addresses were available. The feature is available on all ScreenOS 6.1.0 platforms.

Virtual Router Redundancy Protocol (VRRP)

- **Virtual Router Redundancy Protocol (VRRP) Support**—ScreenOS 6.1.0 provides support for VRRP (RFC 3768-VRRP version 2.0) on the SSG 5, SSG 20, SSG 140, SSG 320M/350M, and SSG 520/520M/550/550M platforms. This feature allows the security devices to interoperate with other vendors' VRRP implementations. When a device supports VRRP, it cannot support NSRP, as they are mutually exclusive. The current implementation of VRRP does not support stateful failover, nor is VRRP supported through NSM.

Unified Access Control (UAC)

- **Dynamic Discovery of Enforcers**—ScreenOS 6.1.0 allows you to configure the Infranet Enforcer (firewall) to inform the Infranet Controller when a packet is dropped because it originated from an unknown user. When the Infranet Controller authenticates the identity of the user, it will then push the corresponding rules down to the Infranet Enforcer. With earlier releases of ScreenOS, the Infranet Controller would push the entire auth table to the firewall even if the entries were not necessary. This feature will be available with the release of UAC 2.2.
- **Enhanced Range of Roles per Auth Table Entry**—ScreenOS supports a maximum of 200 roles per auth table entry in order to limit the amount of memory occupied by the auth table. The role strings and role name arrays store the first 200 roles configured by the Infranet Controller; any roles beyond that are discarded with a warning message logged to the SSH session that sent the command and to the event log.

Feature Extensions

Application Layer Gateway (ALG)

- **MS-RPC ALG Enhancements**—ScreenOS 6.1.0 adds support for ISystemActivator (IRemoteSCMActivator) bind requests.
- **Avaya H.323 and SIP ALGs**—ScreenOS has extended SIP ALG support for Avaya H.323 and SIP.
- **SIP Trunking ALG**—ScreenOS 6.1.0 has extended the SIP ALG to support SIP trunking from vendors such as Lucent, Broadsoft, and AT&T.
- **PacketCable Extensions for MGCP ALG**—ScreenOS 6.1.0 adds support for the Network-based Call Signaling (NCS) protocol and Trunking Gateway Control Protocol (TGCP). NCS/TGCP is used for delivering advanced, real-time multimedia services over two-way cable deployments.

Network Address Translation (NAT)

ScreenOS 6.1.0 provides a uniform NAT functionality in Layer 3 (L3) among all security devices as follows:

- You can configure the virtual IP (VIP) address as the same as the interface IP address on any device in any zone.
- You can configure the VIP and mapped IP (MIP) address on the same interface using the same IP address. This allows you to selectively redirect traffic for specific applications to designated servers.
- You can configure VIP, MIP, and dynamic IP (DIP) addresses in any combination on any interface.

NetScreen Redundancy Protocol (NSRP)

- **Enhanced Range of Cluster IDs and VSD IDs**—ScreenOS now supports up to 64 cluster IDs or 64 VSD IDs or some combination equal to 64. In addition, ScreenOS 6.1.0 provides increased cluster session ramp-up performance and limited asymmetric routing support through an NSRP cluster. All devices in a cluster must be set to the same value.

Cluster ID:	0	8	16	32	64
VSD ID:					
0	default	default	supported*	supported*	supported*
8	default	default	supported*	supported*	supported*
16	supported*	supported*	supported*	supported*	unsupported
32	supported*	supported*	supported*	unsupported	unsupported
64	supported*	supported*	unsupported	unsupported	unsupported

* Using the environment variable to set the values. This is an example of how to set the environment variables:

```
ssg5-serial-wlan-> set envar nsrp-max-cluster=32
nsrp cluster is set to 32
The system must be rebooted for new setting to take effect!
ssg5-serial-wlan-> set envar nsrp-max-vsd=16
nsrp vsd is set to 16
The system must be rebooted for new setting to take effect!
```

- **Active-Active Support for Transparent Mode**—ScreenOS 6.1.0 adds support for Active-Active configurations in Transparent mode on the ISG 1000/2000 and NS5x00 platforms.

Other

- **SCTP Stateful Inspection**—ScreenOS 6.1.0 supports stateful inspection of Stream Control Transport Protocol (SCTP) traffic on all platforms. Supported maximum concurrent SCTP sessions is 2000.
- **NSRD Support via USB**—With the current release of ScreenOS, the NetScreen Rapid Deployment (NSRD) feature allows you to load a configuration on a security device with factory default configuration from a configlet file stored on a USB storage device. Please see SSG 300-Series NSRD Support in the Limitations section for more information about this feature on SSG 300-series devices.
- **Ability to Keep Session Flow in CPU on ASIC-Based Platforms**—On ISG 1000/2000 and NS5x00 platforms, you can retain the session flow in the CPU itself based on a policy that you define, facilitating packet capture for debugging purposes. In earlier releases, the CPU handled only the first packet of a session with the subsequent packets of the flow sent to the ASIC.
- **WebUI Enhancements for Opening a JTAC Case**—The enhancements to the WebUI allow you to open a Juniper Technical Assistance Center (JTAC) case for technical support where the WebUI automatically populates fields with device-specific information.
- **Secondary Login Banner Acknowledgement**—This version of ScreenOS allows the creation of a secondary banner which requires users attempting to access a device to positively acknowledge a banner before displaying a prompt for credentials (such as a username/password or username/public key). If the user does not acknowledge the banner, the device will not give them a login prompt and will close the connection. This feature is consistent on various types of management sessions including those created via console, telnet, and SSH.

  To enable the feature, run the following command:

  set admin auth banner ack-secondary

NOTE: This feature cannot be used on firewalls that are acting as an Infranet Enforcer working in conjunction with UAC. This is because UAC communicates with the firewall via SSH and does not have a method to accept the banner.

- **Ability to Use the Option 'deny' in Access Lists for Multicast**—You can now specify the option 'deny' in access lists to simplify access list configuration instead of having to create permit-only lists.
- **Environment and Temperature MIBs**—All platforms now support environmental and temperature MIBs.
- **Ability to Accept/Discard Gratuitous ARP Requests and Responses**—You can now accept/discard gratuitous ARPs on a per interface basis in Layer 3 and on a per VLAN basis in Transparent mode.
- **Wildcard Mask Support in Policies**—ScreenOS 6.1.0 allows you to configure wildcard masks in policy entries, such as 10.10.10.10/0.0.255.0. There is a potential session ramp rate impact when enabling this feature.
- **Dynamic DNS Service Enhancements**—ScreenOS 6.1.0 adds support for Static DNS and Custom DNS from the Dynamic DNS from dyndns.com.
- **ICSA Compliance Updates to CLI**—The set firewall log-self command now includes four additional logging options: NSM, SSH, telnet, and web.
- **Dial-in Console Access Security Enhancements for SSG 5/20**—The following security enhancements have been added for dial-in console access on the SSG 5 and SSG 20 platforms:
  - Log all dial-in attempts (success and failure) and include the caller numbers;
  - Support for whitelists and blacklists for caller numbers;
  - Deny access for a particular caller number after a configurable number of failed login attempts;
  - Disconnect the call after a configurable number of failed login attempts;
  - Disconnect the call after a configurable length of time without successful authentication;
  - Specify whether to allow or deny calls from unknown caller numbers.

Changes to Default Behavior

This section lists changes to default behavior in ScreenOS 6.1.0r1 from earlier ScreenOS firmware releases.

- **[SSG 140] Maximum Number of Supported Zones**—In previous releases, the administrator was able to create more than the maximum amount of user-defined zones (30). With 6.1.0r1, this limit is now enforced on the SSG 140.
- **NSRP Active-Active Configuration in Transparent Mode**—The virtual security device (VSD) is determined by the VLAN tag in Transparent mode instead of the VMAC in Route/NAT mode.
- **Consistent NAT Behavior Across Platforms**—ScreenOS now provides a consistent NAT behavior across all platforms. This includes the following:
  - Allows VIP and MIP to be the same as interface on any Layer 3 zone instead of only the Untrust zone
  - Allows VIP and MIP to be on the same interface with the same IP

  - Adds new CLI set interface interface-num vip interface-ip and change set interface interface-num vip untrust-ip to a hidden command.

- **SA IDs Displayed Consistently in the Same Base**—With this release of ScreenOS, Security Association (SA) IDs are displayed in Hex both when using the get sa command and in the displayed configuration.
- **Performance Enhancement**—The ISG 1000 platform supports enhanced performance to 2Gbps.
- **Increase in Limit of Entries in Routing Tables**—With ScreenOS 6.1.0, running on the SSG 520/520M/550/550M platforms, routing and forwarding tables can have 250,000 entries, which is increased from the earlier limit of 20,000. The routing tables accept 250,000 total routes including connected, static, imported, and those learned from the routing protocols.
- **Wildcard Masks**—ScreenOS 6.1.0 provides an option to use wildcard masks in IP addresses. If you configure a policy that uses wildcard masks, the system prompts that a wildcard address or wildcard policy is configured because using wildcard address/wildcard policy causes a performance penalty.
- **"Deny" Option in Access Lists in Multicast Policies**—ScreenOS provides an option to include a deny option in access lists in the multicast policy. This might appear as an increase in the number of multicast access lists.
- **Session Capacity Increases**—Session capacity increases as listed below.

Platform	Sessions
SSG 5/SSG 20	8,000
SSG 5/SSG 20 - Adv	16,000
SSG 140	48,000
SSG 320M	-
SSG 350M	-
SSG 520/SSG 520M	128,000
SSG 550/SSG 550M	256,000
ISG 1000	512,000
ISG 1000-IDP	-
ISG 2000	1,000,000
ISG 2000-IDP	-
NS5200/MGT2	-
NS5400/MGT2	2,000,000

- **Increase in GTP Tunnels**—ScreenOS 6.1.0 increases the maximum number of active GTP tunnels supported to 400,000 for the ISG 2000 platform and to 200,000 for the ISG 1000 platform.
- **Increase in Roles per Auth Table Entry**—ScreenOS 6.1.0 increases the number of roles per auth table entry from 26 to 200.
- **Session Rerouting Between Tunnels and Physical Interfaces**—ScreenOS 6.1.0 allows the traffic to fail over between route-based VPN tunnels and physical interfaces in the same zone when the security devices are deployed in a fully redundant network design consisting of dynamic routing and route-based VPNs. To restore the original behavior, use the set envar no-reroute-tunnel-physical=yes command.
- **Increase in Maximum Tunnel Interfaces**—On the NS-5000 w/MGT2 platform, ScreenOS 6.1.0 increases the maximum number of tunnel interfaces per device from 4096 to 8192.
- **ETSI Standards Support**—Currently, Juniper Networks security devices do not support the new wireless standard from European Telecommunications Standards Institute (ETSI), DFS2. This will result in the disabling of the frequency ranges 5250-5350 MHz and 5470-5725 MHz for all SSG 5/20 wireless systems (region ETSI) after March 2008.
- **UDP Flood Screen**—Juniper Networks ASIC-based security devices (NS5400, NS5200, ISG 1000, and ISG 2000) enforce configured screen options for a subinterface even when the physical interface of this subinterface is in a null security zone.
- **Packet Distribution Mode Setting**—On an NS5200 MGT2 with 10GE blade, you can now configure the packet distribution mode for ingress traffic as either hash or round-robin mode using the CLI command set interface interface-name mode. Default is hash mode.
- **Virtual IP on Loopback Interfaces**—With ScreenOS 6.1.0, you can configure the virtual IP (VIP) and Track IP addresses for a loopback interface. Earlier releases of ScreenOS did not provide this option.
- **Configurable Wait Time to Confirm NSM Connection**—If you manage your security device with Juniper Networks NetScreen-Security Manager (NSM), you can load the security device with a configuration from NSM. If a configuration upload fails for some reason, the security device may lose communication with the NSM server. The device can reestablish the connection with NSM by rebooting and loading the previous configuration. The device, however, is unable to immediately detect that the connection is broken, so it is necessary to wait for a specified interval and then check the connection status. The new CLI to configure the wait interval to check the connection status is set nsm bulkcli reboot-wait [seconds]. If the connection is broken, the device can be configured to wait for another specified interval and then reboot.
- **Addition of HA and MGT Zones**—ScreenOS 6.1.0 adds support for high availability (HA) and management (MGT) zones on the SSG 5 and SSG 20 devices. When you start these devices for the first time, the device adds the HA and MGT zones by default.
- **Option to Configure Email Virus Scanning Action**—ScreenOS 6.1.0 provides an option to configure the action that the security device should take if a virus is found in an email. You can choose to have the security device drop the infected

email or send a notification mail to the intended recipient with the infected email replaced with an alert message.

- **Firmware Information**—ScreenOS 6.1.0 adds information about the firmware and its components to the output of the get system CLI command on an ISG 1000 or ISG 2000 device.
- **Bgroup PPS Counters**—ScreenOS 6.1.0 now displays packet-per second counters on bgroup interfaces.
- **VLAN Capacity Increase**—ScreenOS 6.1.0 now supports up to 4094 VLAN interfaces on ISG 1000/2000, ISG 1000/2000-IDP, and NS5x00 series devices when operating in Transparent mode.
- **TCP MSS Modified for Bidirectional VPN Traffic**—The TCP Maximum Segment Size (MSS) value for bidirectional VPN traffic can now be modified in the CLI. The new CLI command set flow vpn-tcp-mss number sets the same MSS for both inbound and outbound traffic. In prior ScreenOS releases, the CLI set flow tcp-mss command worked only for outbound VPN traffic.

NOTE: The older command still works, but any value set using it will be overlaid if the new command is run. Running unset flow vpn-tcp-mss will cause the device to once again use the earlier value and permit use of the older command. When no MSS value is given, the default setting is 1350; when the new command is used, an MSS value configured by set flow tcp-mss will not be valid even if set flow tcp-mss is run again. [261891]

Addressed Issues in ScreenOS 6.1.0r2

The following operational issues were resolved in this release:

Administration

- **215340, 256010**—Some log entries are not formatted properly in the WebTrend output.
- **223139**—Task CPU becomes high when executing some CLI commands with a large configuration, which triggers high overall CPU utilization, and reaches the alarm threshold.
- **258225**—The admin-preferences of the local DNS defined via the CLI gets reset when any changes are made to DNS setting via the WebUI.
- **258522**—Policy list in the root vsys may be blank when viewed from the WebUI.
- **259735**—Incorrect information shown on the multilink and serial interface SNMP report for MTU, link status, operation status, and link speed.
- **261597**—[NetScreen-5GT] Unable to set interface ethernet2 to the Null zone.
- **262685, 267506**—Bridge Group interfaces would not go to full duplex, even when the bgroup members are hard-coded to full duplex.
- **262912**—Sync Serial card shows up as JXMBRI-ST in get chassis.
- **267997**—Incorrect ifIndex in link-up/link-down SNMP trap for redundant interfaces occurred.
- **275288**—Device restarts when MIP configured with incorrect mapping from IPv4 to IPv6.
- **276003**—The "sess-limit" option is getting lost after a restart.

Antivirus

- **225931**—ICAP AV may fail with error code 3 for running out of connection objects due to incorrect freeing of ICAP connection.
- **266736**—With Antivirus enabled, an email containing certain characters may cause the POP3 or SMTP session to freeze.

DHCP

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

HA and NSRP

- **226031**—Only the first IP Pool gets synchronized to the backup device.
- **227665**—The NSRP vsd-group track-ip method CLI command is lost after a reset.
- **238578**—Non-VSD sessions in an Active/Active NSRP configuration incorrectly synchronize between cluster members if the session's egress subinterface differs between cluster members.
- **251157**—An NSRP cluster member received a corrupted HA message, causing the device to reset.
- **252645**—Gratuitous ARPs for the secondary IP address on an interface did not work.
- **258989**—[NetScreen-5000] Traffic is not forwarded when the packets are received on an aggregate interface of the backup VSD in an NSRP Active/Active cluster due to the TCP SYN check failing incorrectly.
- **260760**—[SSG 5] NSRP failover not working properly when both NSRP interfaces and a secondary path are enabled.
- **262533**—[SSG 140] Alarm LED on the device was not displaying correctly when an NSRP failover event occurred.
- **264768**—Configurations are out of sync due PBR out of order set match-group commands.
- **267734**—The primary ISG does not read the sequence number correctly from the ASIC for AES after failover.
- **268708**—Traffic fails to pass after failover of a NSRP pair with devices configured in transparent mode.
- **268809**—When no-session-backup is enabled on a policy, traffic through the serial interface stops passing.
- **274997**—The commands set sm enable and set sm disable were erroneously being synchronized to the other member in an NSRP cluster.

Management

- **224382**—Task CPU spikes when the authentication result from the RADIUS server does not arrive on time.
- **252700**—Unsupported "Far End" OIDs were modified so that they return a "no such object" response to an SNMP query.
- **252783**—The 64-bit counter on an interface was showing incorrect information after the "clear counter" command was performed.
- **258148**—SNMP reports incorrect ifspeed on the serial interface.
- **260188**—The device is only able to send 400 to 500 logs per second to NSM.

- **260243**—When disabling the rate limit in a GTP object configuration, the limit was not actually disabled.
- **261714**—The NSRP failover event log is not sent to the syslog server.
- **262697**—In certain conditions, the device may reset when a policy is pushed from NSM.
- **266873**—In the event log, when the number of telnet and ssh connections to a device are higher than its display limitation, the log entries of the telnet-cmd number and ssh-cmd number are incorrectly displayed.
- **267372**—The SNMP trap (OID) of the interface status is not correct.
- **269298**—An invalid command appeared in the CLI: "exec admin".
- **270999**—Hardware counter for out bytes always shows zero on the management interface.
- **271297**—The get perf session detail command did not display the correct values.
- **273424**—Under certain condition, device update after the creation of a new custom vsys using NSM would result in the error: "unknown keyword unset".

Other

- **224161**—HDLC debug output was being sent to the dbuf buffer when any debug flow was enabled, making troubleshooting difficult.
- **224423**—If a timeout is configured in one GTP object, this timeout is used for all GTP objects.
- **224782**—The transmit and receive counters on an HA interface between two NSRP peers shows a mismatch, due to an incorrect byte count.
- **226075**—[ISG 1000/2000, NetScreen-5000-8G2/8G2-G4] Device sending two ESP packets with the same sequence number.
- **227438**—CTS traffic incorrectly detected as "HTTP:Overflow:Content-Overflow" and dropped.
- **231670**—In certain environments, if only URL filtering is enabled in the policy, the HTTP response might fail to be parsed.
- **233490**—RTSP ALG does not translate addresses properly when in NAT mode.
- **235311**—Transmission of the multicast data stream might stop for a while when handling a PIM fragment packet
- **236768**—Device may issue an ACK in response to a RST packet.
- **239594**—The device may fail when AV is enabled and AIM traffic is passing through.

- **240625**—Memory utilization is high due to DI session leak when SYN protection is enabled.
- **250504**—A conflict over multiple tracked gateway routes caused the device to fail.
- **252082**—FTP session IPv4 to IPv6 session connects, but the client's FTP session hangs when FTP commands are entered.
- **252224**—The wireless client reports a different link speed than what the device reports.
- **253965**—Frame Relay clocking mode did not initialize properly.
- **254619**—A MIB file issue occurred when high-availability(15) was removed from the MIB files.
- **256589**—When a large number of VPN policies are configured, the device may fail to create a VPN policy when the tunnel ID is not specified.
- **256783**—Device failed due to mishandling of null pointer.
- **257095**—The Antispam list would not display in alphabetical order due to a sorting issue.
- **258336**—The device restarts on its own when the Deep Inspection Signature Pack is updated.
- **260087**—PPTP traffic not working properly when source nat policy is enabled.
- **260626**—[SSG 300] Device unable to pass packets greater than 1,468 bytes across an 802.1q tagged subinterface.
- **261543**—[NS-5000-MGT2]Issuing the command get bridge word 0 may cause the firewall to reset.
- **262448**—The 'exec policy verify' command was not working when empty address groups are used in the policies.
- **262450**—The WebAuth login page contained a script error after entering a user name.
- **262666**—When NTP is enabled, and set ntp server src-interface is used, NTP communication cannot be checked in the policy when the traffic is sent out to an interface other than the one specified in the command
- **262894**—Device fails to connect to Websense server after the Websense server IP address has changed.
- **263585**—In certain situations, traffic that is NAT'd and uses the H.323 ALG caused the device to reset.
- **263850**—FTP ALG did not correctly create child sessions for cross-vsys flows, causing data packets to be dropped.

- **264263**—Device failed due to Null pointer access in sunrpc.
- **265230**—[SSG 140] The alarm LED on the device incorrectly displays as amber, instead of red, when an attack was detected.
- **266875**—Interface MAC did not change correctly when the VSI interface was assigned to the mgt zone.
- **267114**—When URL filtering is enabled, permitted URLs are logged twice in the firewall event log.
- **267255**—Unset ALG not saved after reset.
- **267370**—When generating a syslog message, the source port and destination port are incorrectly interpreted from the event log.
- **267767**—Running get dbuf stream prints out the message return due to suspect loop" with any debugs specified.
- **267994**—CPU utilization is high after Virtual IP (VIP) is configured.
- **269121**—GRE keepalive is dropped when the recursion control bit is set.
- **269668**—Deleting multiple virtual systems at one time may prevent traffic from passing through other virtual systems.
- **269922**—With IPv6, an incorrect ICMP message is generated when the policy is configured with action reject.
- **273021**—The connection between the firewall and the external Surfcontrol server was lost randomly several times a day.
- **274187**—Under certain circumstances, the first SYN packet is not matching the policy.
- **274973**—When get vr trust protocol pim rp proxy is executed, an exception dump may occur.
- **278559**—In certain conditions, clearing the auth table via IP address may cause the device to reset.
- **280532**—Websense is not working and displays the following error: "Unknown message type: 8e".
- **289248**—FTP failed if there was a NO PASSV response and then the client tried to use PORT mode.

Performance

- **234153**—High flow CPU utilization caused by packet looping between CPU and ASIC.

- **266111**—Slow performance with Web traffic when URL filtering and the SYN Proxy is enabled.

Routing

- **223180**—Multicast traffic was not forwarded to both spokes in a hub-and-spoke VPN.
- **225874**—Creating a default route from one VR to the other VR caused the firewall to reset.
- **259054**—The BGP neighbor goes to idle after the BGP connection is reset.
- **260646**—The device would not become the PIM designated router (DR) after increasing the DR-priority.
- **262604**—The first multicast packets in the flow get dropped.
- **263665**—Routes learned via OSPF are not propagated to NSSA LSA after NSRP failover is done.
- **264800**—The default route advertised via BGP by the ISP's upstream router was not propagating into the device's route table.
- **268471**—BGP stops advertising the tunnel's static route after a reset.
- **269341**—IGMP Join occurs 10 seconds after a unicast route has changed.
- **274788**—Multicast route through GRE tunnel fails after the GRE routers do a failover.
- **282293**—Routes are stuck in the RIP database in multiple custom VR configurations.

VoIP/H323

- **256706**—The device was not doing routing and policy lookup for IP addresses with unknown contact bindings from the SIP server.
- **264625**—[ISG 1000/2000] SCCP ALG logging messages in the event log, after the ALG was disabled.
- **271315**—SIP ALG did not support LWS.
- **274300**—The "Can't allocate memory for SCCP call context" message appears in event logs due to the timing between session age-out and call completion.

VPN

- **254357**—Pings through VPN are dropped when IPSec SA is 0.

- **255512**—The command unset ike policy-checking only applied per device, and not per VPN.
- **257708**—When subjected to heavy GRE/IPSec traffic, the device may reset.
- **263126**—The device did not send an Account-Stop message for the old Phase1 SA.
- **264713**—Tunnel ID and hardware SA in an existing session do not update properly after VPN change, which causes traffic to stop.
- **275108**—NSP-tunnel (used in IPSec environments) was erroneously deleted but still referenced by another module, and caused device to reset.
- **282310**—The device may reset when a NetScreen Remote VPN connection is made.
- **282564**—Multiple dial-up VPN users could not login if the name in the certificate is similar to the previous user.

WebUI

- **222872**—Access to the WebUI is very slow when opening the main home page.
- **256041**—In a particular circumstance, the device may fail when an admin edits a VPN configuration using the WebUI.
- **259582**—When adding Antispam to an existing Antivirus profile via the WebUI, FTP session disconnects occurs and result in abnormal behavior of FTP commands (ls, dir).
- **262479**—Read-Write admin account was incorrectly offered "Enable Web Management Idle Timeout" option in the Admin Management page, causing the page's Apply function to fail.
- **262827**—WebUI: Deleting an aggregate sub-interface erroneously gives you a warning that you are about to remove one aggregate interface.
- **264300**—Config Merge from the WebUI fails.
- **265334**—From the WebUI, if a RIP summary route is set to a metric of 1, it does not get written to the config.
- **265413**—Unable to specify u-fqdn IKE-ID type when creating a Dial-Up VPN User.
- **266871**—Custom RPC service is deleted from the policy when that policy is edited.
- **267496**—The WebUI reports that the gbw value is out of range when editing on a subinterface.

- **267521**—"Bypass authentication option" for XAuth can not be configured via WebUI.
- **268659**—Adding redundant interface or redundant subinterface through the WebUI succeeds, but the WebUI incorrectly produces an error.
- **270630**—Can not disable SSH2 management from the WebUI.
- **272946**—Unable to create an IKE gateway on a device in transparent mode from the WebUI.
- **276288**—When configuring an NSRP cluster ID with a value over 63 using the WebUI, an incorrect error message is displayed.

Addressed Issues in ScreenOS 6.1.0r1

NOTE: Due to an update in the ScreenOS problem tracking system, some issues listed here may 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:

VPN

- **220334** (os70336)—When the IP address of a remote peer changed, IKE phase 1 failed to update correctly. This issue has been resolved.

Firewall

- **236113**—When you enabled TCP-SYN-Check on the NetScreen-5000 platform, the device failed to establish a cross-chip TCP connection in Transparent mode. This issue has been resolved.

IDP

- **225502**—[ISG with IDP] The IDP drops legitimate HTTP traffic for very large HTTP downloads.
- **226284**—An ISG 2000-IDP intermittently stopped advertising prefixes to eBGP peers after BGP peer refreshed from other devices. This issue has been resolved.
- **229742**—In Transparent mode on an ISG 1000 with IDP enabled, if both Web filtering and IDP were enabled in one policy, all Web browsing that used the policy stopped responding. This issue has been resolved.
- **232075**—[ISG 1000/2000] Time binding attacks are not reporting logs to the NSM server.
- **232420**—An ISG 2000 device running ScreenOS 6.0.0r1 with IDP in Inline mode caused packets to be dropped for return traffic if NAT and a mirror port were both configured. This issue has been resolved.
- **236437**—[ISG 1000/2000] In certain situations, the traffic passing through an inline mode IDP rule may experience excessive delay when other rules are configured for TAP mode IDP.
- **237769**—[ISG 1000/2000] There is high CPU utilization on a single SM (Security Module) due to uneven session distribution.
- **239575**—When both tcp-syn-check is set and IDP is enabled in the policy, the ACK packet of a 3-way handshake is dropped when ISG is in transparent mode.
- **252958**—[ISG 1000/2000] Login attempts with FTP brute force signature were erroneously being logged as accepted.

Other

- **225017**—If you restarted an SSG 5 appliance after many hours of heavy traffic, the device stopped forwarding all traffic. This issue has been resolved.
- **226651** (os70627)—When traffic reached 1Gbps (in each direction) through two uPIMs, traffic was blocked in both directions after approximately one hour. This issue has been resolved.
- **233516**—If you made a large number of configuration changes (especially in policies and virtual routers), an ISG 2000 stopped receiving IPv6 packets. This issue has been resolved.
- **231754**—In Transparent mode, SIP traffic caused a device to fail. This issue has been resolved.
- **227229** (os71064)—When you deployed NTP Server on ISG 1000 appliances, the device aged out a packet even if the hardware session was refreshed by the packet. This issue has been resolved.

Routing

- **228200**—Adding an alternate route to the routing table and making it as active after a tunnel failure was not possible. This issue occurred when you used the set interface tunnel_name protocol rip demand-circuit command. This issue has been resolved.

Management

- **231728**—On the SSG 140 platform, DNS settings were not accepted through a PPPoE connection. This issue has been resolved.
- **233428**—In Transparent mode, the management feature on a v1-Untrust zone was not added to the configuration, so it was disabled after a device reset. This issue has been resolved.

Known Issues

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.

Known Issues in ScreenOS 6.1.0r2

Administration

- **257485**—In certain situations the administrator was unable to add an address book item to a multi-cell policy.
- **260995**—debug buffer showed messages even though no debug commands were running.
- **270319**—Device restarts when updating a policy with no attacks, which was previously configured with attacks.
- **278125**—When there are multiple policies using the same src/dst IP and ports, one is disabled, and one of the address book object is modified, the device may reset.
- **279094**—Unsetting PPPoE auth-method will erroneously generate the message "Cannot unset idle-interval to default when auto connect is enabled".
- **282163**—TFTP traffic sourced from loopback interface fails.

Antivirus

- **282592**—Enabling AV as an http proxy in transparent mode causes the packets to use the MAC address of the VLAN interface as the source MAC address.

DNS

- **215889**—DNS queries are sent to the Dynamically-learned DNS servers even though an Administered defined DNS server has been configured with an admin-preference of 255.

HA and NSRP

- **262695**—NSRP failover may cause some VPNs to fail.
- **270890**—If GTP Sequence Number Validation was enabled, GTP traffic would be dropped due to 'bad sequence number' after two NSRP failovers.
- **274948**—In NSRP, when adding an interface to a L2 zone, it does not become a VSI.
- **280217**—[NS-5000, ISG] When the device is in Active/Passive NSRP cluster, under a particular circumstance after a preempt primary device is reset, traffic via VPN is dropped by its VPN peer.
- **282261**—NSRP failover from the backup to the primary taking longer than expected.

IDP

- **260215**— When profiling smaller networks, the profiler on an ISG-IDP is not detecting new events and is not updating old ones.

Management

- **255035**—Redundant sub-interfaces could not be imported properly from NSM.
- **271129**—Unable to manage device after the interface received many TCP out of order packets.
- **290562**— Unable to determine BGP aggregate status within NSM.

Other

- **235777**—The command unset admin hw-reset was not saved to the config file after a reset.
- **252398**—Wireless connection instability when using 802.1x with Intel Pro/Wireless NIC with 802.1x auth.
- **255301**—TCP socket leak causes lost SSH management and BGP peering, resulting in high task CPU utilization.
- **257812**—NAS-Port-Type was "Wireless-Other" instead of "Wireless-IEEE-802-11" for example when authenticating wireless clients via radius.
- **260307**—Under certain conditions, the firewall seems to be corrupting UDP checksums.
- **267891**—URL filtering did not have a null pointer which caused the device to reset.
- **269018**—After enabling DI, when a syn-flood is detected, the device may restart.
- **269488**—In transparent mode, unauthenticated users are not being redirected to the Infranet Controller (IC).
- **270342**—In a vsys environment, ping traffic from the other vsys to the local interface failed.
- **271349**—With a low quality connection, PPPoE may stop responding during negotiation.
- **273879**—Authentication entries in a pending or fail state, fails to be cleared.
- **276282**—Device reset due to problem with hardware session pointer.
- **279407**—Memory leak occurred when a second user from the same user group is authenticated.
- **280079**—DSCP TOS bit were not being set correctly on the device.

- **281722**—A device reset occurred when running debug ike and unset console dbuf.
- **283182**—Traffic through the SSG-500 stops intermittently.
- **285252**—When traffic shaping is enabled, the MAC address is shifted on the sub interfaces.
- **285333**—Traffic may not pass if there is a duplex mismatch between the device interface and the switch connected to the device.

Performance

- **221537**—FTP downloads from dial up or slow links are failing when AV enabled.
- **254058**—Bandwidth testing site via web shows lower bandwidth than actual upload speed.
- **264366**—UDP flood is detected and packets are dropped even when pps rate is less than threshold.

Routing

- **267357**—Permanent route attributes are not being exported from one VR to the other.
- **276971**—Tunnel interfaces were being counted as an outgoing interface, which exceeds the maximum number of interfaces allowed for multicast traffic.

VOIP/H323

- **278563**—Child session for SIP could not be created correctly.
- **278773**—H323 ALG was unable to decode Q.931 using Avaya phones, due to not enough OLC support.

VPN

- **280101**—Dial-Up VPN traffic dropped due to IP address on Dial Up client changed.
- **285748**—[NS-5000] IPSec pass-through packets are being dropped when the device is in transparent mode.
- **285935**—VPN packet drop occurred under traffic looping.

WebUI

- **227316**—Unable to configure DHCP on an interface from a trustee admin user via WebUI.

- **262490**—Unable to manage device from untrust interface via trustee admin via WebUI.
- **277589**—When editing a subinterface, WebUI responds with an erroneous traffic bandwidth message "0 is not within the valid range (1 - 1000000)".
- **277867**—PIM RP Proxy setting is not removed when PR Candidate is deleted via WebUI.
- **279141**—VPN policies created with the WebUI paired up incorrectly.
- **281505**—In an NSRP environment, a fault error message "IP conflict" is shown in the WebUI when accessing a backup device to configure an interface.

Known Issues in ScreenOS 6.1.0r1

This section describes known issues with the listed release.

Flow

- **235781**—Using Transparent mode, under high traffic conditions, sometimes a small number of sessions cannot be cleared. The sessions appear to be "time 0" but will remain in the session table. Running set sat session-clean will clear these sessions from the table after one round of session cleaning.
- **239631**—If you configure the initial session timeout below the valid range (20—300 seconds), the system interprets these values as minutes instead of seconds.

HA and NSRP

- **235303**—Delay in the peripheral devices updating the forwarding table when a failover occurs in an NSRP cluster in Transparent mode. When the devices have no gratuitous ARP mechanism as in NAT or Route mode, peripheral devices update the forwarding table only when the active physical interface is restarted. The update happens after five seconds by default.

  W/A: Use the CLI command set nsrp link-hold-time to modify the link downtime.
- **236275**—If the VSD group is not bound to a VLAN group, the security device incorrectly reports the VSD as being in Active-Passive mode.
- **236634**—In an Active-Passive configuration, if the active security device handles a large number of FTP connections, the CPU utilization of the backup device remains high even when the rate of the FTP connections per second on the backup is low.
- **253467**—If a device's SIP traffic is very heavy in an NSRP deployment, although the master box works well, there will be some delays when resources on the backup box are removed. Operational impact on the cluster is minimal, and the backup box will automatically recover.

IPv6

- **227934**—SSG platforms incorrectly process the ICMPv6 error packet that they receive in response to a non-first fragment packet that exceeds the outgoing interface MTU.

  W/A: Set the interface MTU at a value that accommodates all packets for all links through a path.

- **236085**—In Transparent mode, you cannot manage a zone that is on a vsys using the zone nsrp manage CLI command, because it is a global setting based on vlan1 interface. In root mode, you can manage only the related vsys.

- **236087**—On SSG 320/350 devices, a 4-byte PVE tag is used to identify which interface the packet came from, limiting the maximum supported packet length to 1514 bytes.

- **236549**—When deployed in Transparent mode, some high-end platforms such as ISG 1000-IDP do not support more than 20 reassembled segments. If you try to ping another device with data that requires more than 20 reassembled segments (for example, 30,000 bytes), the ping request fails.

- **239285**—ScreenOS does not verify the IP address that you enter when you configure the security device.

  W/A: You should verify the IP address that you enter for an interface. For example, you must not assign a multicast or broadcast IP address as an interface's IP address.

- **239598**—On some high-end platforms, after you have enabled IPv6, the CLI incorrectly allows you to enable parameters such as DSCP marking, IDP, and NSRP Data Forwarding that are not supported in IPv6 mode.

- **267239**—When modifying an IPv6 or a wildcard policy through the WebUI, all existing sessions for the policy will be removed. However, existing sessions will not be removed if you only modify some minor features—such as session-limit or alarm-without-drop—of an ordinary IPv4 policy through the WebUI.

Other

- **236210**—In an IDP deployment, when a policy incorporating diffserv is created the security module does not mark the first attack packet. This is by design, and all subsequent packets are correctly marked.

- **255774**—The debug command unset console dbuf might make the box unstable, especially under heavy traffic. Administrators are advised to use care when running this command.

- **258931**—Due to a memory limitation, NS 5000 devices are currently unable to support 500 vsys when an advanced license key—such as for virtual router or Layer 2 Active-Active support—is part of the deployment.

- **263512**—ScreenOS 6.1.0 includes a new SSHv2 secondary login banner feature. However, unless the feature is enabled, if the secondary banner is displayed before a login prompt on a console or via a Telnet connection, no positive acknowledgment to the secondary banner is required (applicable to console, Telnet, SSHv1, and SSHv2 connections).

- **266022**—Because the NS 5400 supports 2 million sessions by default in 6.1 (and 6.0r2 and later), you must make sure that the device has a minimum of 450MB of free memory when upgrading from 5.4 or 6.0r1 to 6.1 or 6.0r2. One million sessions will require approximately 340MB of memory.
- **278668**—[SSG 550/550M] An error in the boot-loader code caused the interface references to be switched and the motherboard version to be incorrectly reported while upgrading from boot mode.

Routing

- **251874**—ScreenOS does not limit the number of routing entries that are distributed through Routing Information Protocol (RIP). This incorrectly allows you to configure more static routing entries than are supported.
- **251875**—ScreenOS does not limit the number of Open Shortest Path First (OSPF) areas and virtual links. This incorrectly allows you to configure more OSPF areas and virtual links than are supported.
- **251879**—ScreenOS does not limit the number of Open Shortest Path First (OSPF) interfaces. This incorrectly allows you to configure more OSPF interfaces than are supported.
- **251883**—ScreenOS does not limit the number of static routing entries that are redistributed through OSPF. This incorrectly allows you to configure more static routing entries than are supported.
- **255815**—The device does not check the destination MAC address for packets when the SYN-cookie is triggered and responds with SYN-ACK whether the destination MAC belongs to itself or not.
- **258978**—For the SSG 320M and 350M, the supported maximum number of Border Gateway Protocol (BGP) redistributed routes is 4096. However, if a large number of routes are added with an automated script, it is possible to exceed the supported limit. Routes entered or redistributed manually should not be able to exceed 4096.
- **258979**—For the SSG 320M and 350M, the supported maximum number of Open Shortest Path First (OSPF) redistributed routes is 4096, but it may be possible to exceed the maximum. OSPF redistributed routes are handled in two parts: route task and OSPF task. The route task will add redistributed routes to OSPF continuously during one CPU time slice. The redistributed routes counter will not, however, be updated until the OSPF task is processed by the CPU, so more routes may be added in OSPF when the routes are added using an automated script. Routes entered or redistributed manually should not be able to exceed 4096.

VoIP

- **239517**—During a VoIP call that uses the H.323 protocol, if you change the mapped IP or virtual IP address assignments, subsequent calls lose the audio. Child sessions that are required to provide audio are not established because the security device does not recognize a matching policy with the changed MIP or VIP assignments.

  W/A: Create a policy similar to the one you had configured and add it to the global zone.

- **240574**—In standalone mode, if an alternative gatekeeper is initiated during a VoIP call, sessions do not age out immediately after the call ends. In HA mode, if an alternative gatekeeper is initiated during a VoIP call and there is a firewall HA recycle, sessions only age out after a long time.

- **241465**—If a phone tries to register while SIP is disabled, SIP sessions must be cleared once SIP is enabled. After SIP is enabled and SIP sessions have been cleared, all phones that tried to register prior to SIP being enabled will need to be reset. Failure to reset a SIP phone that attempted to register before SIP was enabled will result in that SIP phone being unable to place or receive calls.

- **250319**—The SIP functionality does not support a customized port, so a SIP call that uses custom ports might fail.

  W/A: Use the default SIP port (5060).

- **261464**—On NS 5400 devices, Media Gateway Control Protocol (MGCP) traffic performance drops significantly when the number of active calls exceeds 8000. The issue is the result of having sessions installed on both ASICs in the device rather than on only one as is the case with single-ASIC platforms.

VPN

- **240108**—The security device does not allow a static DNS host entry to be removed if the hostname has been used in an IKE gateway configuration, even if the entry was entered in error or incorrectly and even if the IKE gateways had since been removed.

  W/A: Reboot the device to clear the DNS entry. Because the DNS entry is erroneous, rebooting will maintain the IKE configuration while clearing the mistaken DNS entry.

- **241207**—During IPSec SA rekeying, some packets may be dropped on the initiator side because the packet is received before the SA table is created. Packets will only be dropped for a very short time. There should not be any packets dropped after the SA table is installed.

- **253238**—ScreenOS does not limit the number of GRE tunnels you can create. This incorrectly allows you to create more GRE tunnels than are supported.

Limitations and Compatibility

Limitations of Features in ScreenOS 6.1.0

This section describes the limitations of some features in the ScreenOS 6.1.0 release. They apply to all platforms unless otherwise noted.

- **ISG 1000, ISG 1000-IDP, ISG 2000, ISG 200-IDP, NetScreen-5000 series**—Some environments require that firewalls be able to log all dropped packets. The ScreenOS command set flow log-dropped-packetswill enable this function and get log flow-deny will display the dropped packet logs. Hardware limitations, however, prevent the devices listed above from logging packets without data and with the protocol field set to 0, 1, 6, or 17 sent either to or through the device. Packets that have data and where the protocol field is set to 0 or 6 sent to or through the device from any host are also not logged by these devices. [300152].
- **SSG 300-Series NSRD Support**—Without running a slot configuration, NSM is unable to locate the source interface list when using NSRD on SSG 300-series devices, and without the source interface list NSRD is unable to select a configlet file. To use NSRD on an SSG 300-series device, do a slot config through NSM, which will make it possible for the device to see the interface list and then configure with NSRD. [259596].
- **SSG 300-Series and 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. Administrators can dynamically create or delete bgroup interfaces. The maximum number of bgroup interfaces on each PIM is half the number of ports. You can configure bgroup interfaces only on the same PIM or on the system board.
- **SSG 140**—Bgroups are supported on both on-board Ethernet ports and Ethernet switch PIMs (uPIMs). You can dynamically create or delete bgroup interfaces. The maximum number of bgroup interfaces on each PIM is half the number of ports. On-board ports have three preset bgroup interfaces. You can configure bgroup interfaces only on the same PIM or on the system board.
- **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.

  To achieve maximum session count on the NS-5000 series security devices, you should design the network traffic 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 the 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**—Dead peer detection (DPD) does not work on the spoke when set on an 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 you enable Jumbo frames by setting the max-frame-size setting in the range 1515–9830.
- **VRRP with NSM**—ScreenOS 6.1.0 does not support VRRP with NSM. [262624]
- **PIM Power and Thermal Requirements**—If you install either 8-port or 16-port uPIMs in your SSG 140, SSG 500-series, or SSG 500M-series device, you must observe the power and thermal guidelines. Please refer to the PIM and Mini-PIM Installation and Configuration Guide for the power and thermal guidelines for all supported platforms, available at:

  http://www.juniper.net/techpubs/hardware/pim_guide/pim_guide.pdf

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

Compatibility Issues in ScreenOS 6.1.0

This section lists 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 at the time of this release.

- **Compatible Web Browsers**—The WebUI for ScreenOS 6.1.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, Netscape Navigator 6.X for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS X.
- **Upgrade Sequence**—We recommend that you follow the upgrade instructions described in the ScreenOS Upgrade Guide located at http://www.juniper.net/techpubs/software/screenos/screenos6.1.0/upgrade_guide.pdf. If you upgrade directly from ScreenOS 5.0.0 or ScreenOS 5.1.0 to ScreenOS 6.1.0, 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 6.1 firmware. Refer to "Upgrade Paths to ScreenOS 6.1" in the ScreenOS *Upgrade Guide* for intermediate software and boot loader upgrade information.

  Use the following procedure to upgrade the SSG 500/500M boot loader:

  1. Download the boot loader (v.1.0.5) from the Juniper Networks Support site.
     a. Navigate your browser to http://www.juniper.net/customers/support/. The Support page appears.
     b. Locate the DOWNLOAD SOFTWARE section, and click ScreenOS. Enter your user ID and password in the LOGIN page that appears, and then click the LOGIN button. The ScreenOS page appears.

c. In the table of software download versions, locate SSG-500 and click version 6.1.

d. In the Software tab (under Package), click SSG-500_Boot_loader.

2. Save and extract the boot loader zip file and put it in the root directory of your TFTP server.

3. Start the TFTP server, if necessary.

4. 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.

5. Restart the SSG 500 by entering the reset command. When prompted to confirm the system reset, press y. 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
```

6. Press the X and A keys sequentially to update the boot loader.

7. Enter the filename for the boot loader software you want to load (for example, loadssg500v105) and the IP addresses of the SSG 500 device and TFTP server. The following system output appears:

```
File Name [boot2.1.0.2]: loadssg500v105
Self IP Address [10.150.65.152]:
TFTP IP Address [10.150.65.151]:
```

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

```
Save loader config (112 bytes)... Done
Loading file " loadssg500v105"...
/
Loaded successfully! (size = 125,512 bytes)
Ignore image authentication!
...
.....................
Done.
```

- **WebUI Upgrade**—When upgrading from ScreenOS 5.2.0 to ScreenOS 6.1.0 using the WebUI, you must upgrade the device to ScreenOS 5.4rX and then upgrade the device directly to ScreenOS 6.1.0. Refer to "Upgrading to the New Firmware" in the ScreenOS *Upgrade Guide* for instructions on performing the upgrade.

Documentation Changes

- To upgrade existing firmware to ScreenOS 6.1.0, refer to the ScreenOS *Upgrade Guide* located at ScreenOS 6.1.0 Upgrade Guide. You may need to upgrade the boot loader of the SSG 300-series and SSG 500/500M-series devices. For more information on the upgrade procedure, see "Upgrade Sequence" in the Compatibility Issues in ScreenOS 6.1.0 section of this document.
- The document formerly called ScreenOS *Migration Guide* has been renamed ScreenOS *Upgrade Guide*. The content is updated for 6.1.0 but is otherwise unchanged.
- We have added a new document, *JUNOS Software with Enhanced Services Migration Guide*, to support users who would like to migrate from ScreenOS firmware to JUNOS software with enhanced services firmware for supported platforms.
- 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. This information is now in a new guide, the *PIM and Mini-PIM Installation and Configuration Guide*. Refer to that guide for information on configuring PIMs and Mini-PIMs.
- We have added search capability to the online Help system for the WebUI and have made some changes to the appearance of the online Help system.

Getting Help for ScreenOS 6.1.0 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.