Juniper Networks ScreenOS Release Notes

Release 6.2.0r3
August 2009
Revision 02

Products: Integrated Security Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, NetScreen-5GT, Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 300M-series, SSG 500/500M-series, and NetScreen-5000 series (NS 5000–MGT2/SPM2 and NS 5000–MGT3/SPM3).

Contents

Version Summary

ScreenOS 6.2.0 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, NetScreen-5GT, Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, and NetScreen-5000 series with the NS 5000-MGT2/SPM2 and NS 5000-MGT3/SPM3.

This release incorporates bug fixes from ScreenOS maintenance releases up to 6.1r6, 6.0r8, and 5.4r13.

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. The exception to this is SSG 500- and 500m-series devices which can be used together in a cluster.

New Features and Enhancements

The following sections describe new features and enhancements available in the ScreenOS 6.2.0 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.

New Software Features and Enhancements Introduced in 6.2.0

The following section describes the new features introduced in the ScreenOS 6.2.0 release.

Application Layer Gateway (ALG)

- **Traffic Shaping for ALG Sessions**—This enhancement enables traffic shaping on ALG sessions to provide control on the bandwidth available to those sessions (e.g., VoIP).

Antispam

- **Antispam Blacklist Netmask Configuration**—In previous ScreenOS releases, a range of IP addresses in the same subnet needs to be added to the antispam blacklist one at a time. This ScreenOS 6.2.0 enhancement allows a range of IP addresses to be added to the antispam blacklist using both individual network addresses and netmasking.

Antivirus (AV)

- **AV Enhancement: Delete Files in Non-SMTP Sessions**—In releases before 6.2.0, when a virus is detected in an FTP, a POP3, an IMAP, or an HTTP session, ScreenOS will substitute the original content with a virus warning message. In ScreenOS 6.2.0, admins have the option to configure this antivirus feature to either substitute the suspect file with the virus warning message or to just drop the packets silently.
- **AV Enhancement: Send Admin Email Notification After Pattern Update**—In releases before 6.2.0, when an update of the virus pattern file is complete, ScreenOS only generates an event log entry. In ScreenOS 6.2.0, completion of a virus pattern file update will also generate an email notification to the system administrator.
- **AV Enhancement: Send Warning Message to Sender and Allow Editing of a Source Email Address**—In releases before 6.2.0, when a virus is detected in an SMTP, an FTP, a POP3, an IMAP, or an HTTP session, ScreenOS sends a hard-coded warning message to the email sender or HTTP/FTP client, notifying them about the virus scan result. In ScreenOS 6.2.0, the system administrator can configure the content of the warning message as well as specify the source email address.

Authentication

- **Diffie-Hellman Group 14 Support**—ScreenOS 6.2.0 supports Diffie-Hellman (DH) group 14 for IKEv1 and IKEv2 key exchanges. The modulus size of DH group 14 is 2048 bits, thus providing a stronger encryption algorithm.

  This feature is fully handled in hardware on the following devices: SSG 320, SSG 350, SSG 520, SSG 550, ISG 1000, ISG 2000, NS 5200, and NS 5400. For all other devices, this feature is partly handled by hardware and partly by software.
- **Secure Hash Algorithm version 2 (SHA-256) Support** —ScreenOS 6.2.0 supports Secure Hash Algorithm version 2 (SHA-256) authentication. The SHA-256 algorithm produces a 256-bit hash from a message of arbitrary length and a 32-byte key. SHA-256 provides greater cryptographic security than the SHA-1 algorithm.

- **SSH Trusted Path Management Session**—ScreenOS 6.2.0 supports new authentication methods for device and user identification in an SSH management session including host certificates for device identification and PKA certificates for user identification. Host certificates and PKA certificates are mutually exclusive, with host keys and PKA keys, respectively. Note that these new features, and the use of Host/PKA certificates, are supported only with SSHv2, not SSHv1. The device uses only DSA keys for both host certificates and PKA certificates.
- **Enhanced Identification and Authentication**
  - **Admin Role Attributes**—Beginning in ScreenOS 6.2.0, root administrators can assign role attributes (audit, crypto, and security) to non-root read-write and read-only administrators in local databases. For administrators authenticated by external RADIUS servers, please update the dictionary file to assign a role to remote admin users on RADIUS servers. For administrators authenticated by external TACACS+ servers, a new attribute "role" can be used to assign roles to remote admin users. The three values described below can be set for this attribute. ScreenOS does not support a role attribute for admin users authenticated by any other kind of external authentication server.
    - **Crypto**—Gives the admin user the ability to configure and monitor cryptographic data.
    - **Security**—Gives the admin user the ability to configure and monitor security data.
    - **Audit**—Gives the admin user the ability to configure and monitor audit data.

    The role attribute feature is not applicable for root and VSYS administrators.
  - **Cryptographic Policy**—All cryptographic-related configurations, such as encryption algorithm, authentication algorithm, authentication method, Diffie-Hellman (DH) group, and security associations (SAs), can be configured in a cryptographic policy. The feature requires the user to have root or cryptographic administrator privilege.

    You must restart the security device for the cryptographic policy to take affect.
  - **Handling Authentication Failures**—A root or security administrator can configure a limit for the number of unsuccessful login attempts allowed on the security device and lock the unauthorized user account for a specified period if the unsuccessful login attempts exceed this limit. The user account can be locked for a maximum of 1440 minutes. The security device automatically unlocks the user account after the period expires. However, at any given point before the admin lock expires, a root administrator can unlock the user account by clearing this lock.

    This feature also protects the security device against certain types of attacks, such as automated dictionary attacks.
- **Elliptic Curve Digital Signature Algorithm (ECDSA)**—ScreenOS 6.2.0 supports the Elliptic Curve Digital Signature Algorithm (ECDSA) for generating ECDSA key

pairs. As with DSA and RSA certificates, you can use IKEv1 with ECDSA-based certificates.

Border Gateway Protocol (BGP)

- **View BGP Advertised and Received Routes for Neighbors**—Prior ScreenOS releases displayed BGP routes received from all neighbors combined together and did not allow for BGP routes received from each neighbor to be displayed individually. In ScreenOS 6.2.0 it is possible to view BGP advertised and received routes for a specific IPv4 or IPv6 neighbor.

Command Line Interface (CLI)

- **Policy CLI Enhancement**—ScreenOS 6.2.0 includes an enhancement to the syntax of the CLI policy search statements with additional parameters to allow more flexible and powerful policy lookup.
- **Provide Result of** exec nsrp sync **... Commands to Remote Login** —This feature enables the output of an 'exec nsrp sync ... CLI command to be displayed remotely through a Telnet/SSH management session. The output displayed is identical to what would be displayed if the command was entered via the console port.
- **Telnet Client from ScreenOS CLI**—This feature provides support for a Telnet client to make outbound connections from ScreenOS through the CLI.
- **CLI Commands Now Available**—The commands summarized below are now available to customers for us in troubleshooting, debugging, and device management. Details regarding options and syntax for these commands are provided in the *ScreenOS CLI Reference Guide: IPv4 Command Descriptions*.

get commands	
get flow	Displays the flow configuration
get alarm event	Displays alarm events
get log event	Displays event log messages
get session info	Displays a summary of all sessions
get policy disable	Displays disabled policies
get sat *chip_number*	Displays counter information of ASICs used in high-end platforms. This command provides details about ASIC counters such as Q pointers, buffers, and the number of packets forwarded to the CPU

get commands	
get asic	Displays configuration details, functions, counters, and packet flow process data of a packet processing unit (PPU) in the ASICs used in high-end platforms

set commands	
unset flow icmp-ur-session-close	Disables session close when an ICMP unreachable message is received for the existing session
unset flow icmp-ur-msg-filter	Restricts the number of ICMP unreachable messages allowed to flow through a session
set envar max_sip_call_num	Configures the maximum number of concurrent calls possible on the security device
set mac-learn-sticky	Retains the MAC address of an interface for a set interval in the MAC learning table, even when the interface link goes down. The interface must be in transparent mode for the command to work
set ike responder-mode	Enables the security device to act as a responder but not as an initiator when performing IKE negotiation
set arp nat-dst	Configures the security device to respond to ARP requests sent by the host during NAT destination policy configuration
set interface *interface* xg-round-robin	Changes the default FPGA packet distribution algorithm from hash to round-robin
save file *filename* [from | to]	Saves a file from the specified source to the specified destination in the security device, memory card slot, TFTP server, or USB

Firewall

- **Cryptographic Key Protection**—ScreenOS 6.2.0 provides a cryptographic key handling feature for improved data security. When this feature is enabled, the security device protects private keys, preshared keys, VPN manual keys, and keys generated from passwords from unauthorized access and modification.
- **Alarms and Auditing**
  - **Security Alarm and Auditing Enhancements**—Beginning in ScreenOS 6.2.0, root and security administrators can configure a security device to generate an automatic alarm when it detects a security violation. Juniper Networks security devices display security alarm messages on the console accompanied by an audible bell sound. The alarm message is displayed at regular intervals until the alarm is acknowledged by an administrator. The default interval is 10 seconds; the maximum limit is 3600 seconds.
  - **Potential-Violation Security Alarms**—ScreenOS 6.2.0 allows you to configure a set of rules for monitoring events, including thresholds for the following event types:

- Authentication violations
- Policy violations
- Replays of security attributes
- Encryption failures
- Decryption failures
- Key-generation failures
- Cryptographic and non-cryptographic module self-test failures
- Internet Key Exchange (IKE) phase 1 and phase 2 authentication failures

A potential-violation security alarm is triggered if any of the above events exceeds its threshold value. The potential-violation security alarm does not support IPv6 traffic.

- **Exclude Rule**—You can set rules to exclude some audit logs from being generated. By default, no exclude rule is set and the security device generates all logs. You cannot set more than 10 exclude rules.
- **Audit Logs**—ScreenOS 6.2.0 provides an auditable event log for monitoring all security events. An audit log records the following elements for each event: date and time, module, severity level, event type, and a detailed description of each security alarm event. All audit log files can be stored in an external storage device.

- **Admin Inactivity Autolock / Access Schedule**—ScreenOS 6.2.0 provides new features for monitoring access by firewall administrators based on time. These features allow you to restrict intruders from gaining access to unattended admin terminals. To restrict access to unattended terminals, the device autolocks an admin terminal after the specified period of inactivity. Similarly, an admin login can be attached to a predefined access schedule. The device checks the access schedule every 10 seconds, and when the access time expires the admin's access to that security device is terminated.
- **Cryptographic Algorithm Self-Test**—ScreenOS 6.2.0 is compatible with Federal Information Processing Standards (FIPS), which requires that the system provide a cryptograph algorithms self-test function on power-up and under other operational conditions. ScreenOS 6.2.0 meets this requirement by running self-tests under the following conditions:
  - At power-up;
  - On demand by an administrator;
  - After generation of an RSA key;
  - At preconfigured intervals.
- **Configuration File MD5 Checksum**—ScreenOS 6.2.0 enables you to provide an MD5 checksum of the uploaded configuration file. This checksum is compared with the one generated by the device. If the checksums match, the device saves the new configuration file.

GPRS Tunneling Protocol (GTP)

- **Increase GTP Tunnels on ISG 1000 and ISG 2000**—ScreenOS 6.2.0 increases the maximum GTP tunnel capacity to 450,000 for ISG 2000 and 250,000 for ISG 1000.

Intrusion Detection and Prevention (IDP)

- **IPv6 Support on ISG-IDP Devices**—Beginning in ScreenOS 6.2.0, ISG 1000-IDP and ISG 2000-IDP devices support IPv6 traffic. This feature requires additional Packet Processor Unit (PPU) support. There is also a change in the flow behavior of the packets in the security device.

  These features have the following limitations:

  - When both IDP and IPv6 traffic is supported, the throughput of the security device is affected.
  - Profiler and packet capture are not supported, because NSM does not support IPv6 addresses.
  - Only "any-any" IPv6 IDP policies are supported.

- **Flow Filters for IDP Traffic**—ScreenOS 6.2.0 provides an option for creating debug flow filters for IDP traffic. Because security modules do not support flow filters, any ScreenOS debug flow filter that is turned on filters all traffic through the security modules, making it difficult to isolate specific debug information. To avoid this, you can create debug flow filters for IDP traffic with the attributes of source address, destination address, source port, destination port, and protocol. This debug flow filter for IDP traffic is equivalent to the ScreenOS flow filter.
- **Application Identification for ISG Security Modules**—Application Identification (AI) identifies TCP/UDP applications running on non-standard ports by looking for specific patterns in the first few data packets of a session. AI thus helps the ISG security module apply layer 7 protocol decoders to handle traffic on non-standard ports. It also helps narrow the scope of stream- and packet-based attack signatures for applications without decoders and thereby improves performance.

Internet Protocol Security (IPsec)

- **IPsec Transport Mode Support**—ScreenOS 6.2.0 provides IPsec transport mode support in the following configurations: Transport mode IPsec packet pass through; L2TP over a transport mode IPsec VPN; GRE over a transport mode IPsec VPN; From-/To- self transport mode IPsec traffic.
- **NATed Transport Mode IPsec VPNs**—ScreenOS 6.2.0 provides ISG 1000 and 2000 devices with support for transport mode IPsec VPNs to secure traffic initiated and terminated by servers behind Juniper security gateways. In order to support transport mode IPsec for traffic between gateways, each security gateway must meet the RFC standard requiring the source address of outgoing packets and the destination address of the incoming packets be addresses belonging to a security gateway.

This feature has the following limitations:

- It is necessary to set a proxy-id for policy-based VPNs since transport mode IPsec VPN always works with NAT and the IP peer views this as a NATed IP.
- This feature does not support the following ALGs: SIP, SCCP, MGCP, H.323, RTSP, SQL, PPTP, P2P, and Apple iChat.

Internet Protocol Version 6 (IPv6)

- **BGP for IPv6**—ScreenOS 6.2.0 supports multiprotocol Border Gateway Protocol (BGP) for IPv6.
- **Transparent Mode for IPv6**—ScreenOS now supports IPv6 addressing and functionality on security devices in transparent mode. This feature adds support for three new kinds of VPNs: IPv4 over IPv6 IPsec, IPv6 over IPv4 IPsec and IPv6 over IPv6 IPsec. Device management is also permitted in IPv6 mode.
- **NSRP for IPv6 (Active/Passive and Active/Active)**—Previous ScreenOS releases supported NSRP clusters in IPv4 only. ScreenOS 6.2.0 supports NSRP high-availability (HA) clusters using IPv6.
- **DHCPv6 Relay**—For IPv6-enabled ScreenOS, DHCPv6 relay support is available in ScreenOS 6.2.0. This feature allows a Dynamic Host Configuration Protocol version 6 (DHCPv6) client to send a message to a DHCPv6 server that is not connected on the same subnet.
- **Multicast Listener Discovery (IPv6) - MLDv1**—The Multicast Listener Discovery (MLD) protocol is used by an IPv6 router to discover the presence of multicast listeners on directly attached links and to discover specifically which multicast addresses are of interest to those neighboring nodes. MLD is now a supported protocol on ScreenOS devices.

Network Address Translation (NAT)

- **NAT Support in Transparent Mode**—ScreenOS 6.2.0 supports source IP translation in transparent mode. Note that only policy-based DIP pools are supported.

NetScreen Gateway Protocol (NSGP)

- **NetScreen Gateway Protocol (NSGP) Hold-off Timer**—ScreenOS 6.2.0 provides a hold-off timer option. The primary advantage of this timer is that it directs the Gi firewall to deny unintended traffic from the server that arrives within the hold-off time. Additionally, the IP address used by a previous mobile station (MS) will be assigned to a new MS only after the hold-off timer expires. In this way, the new MS will not be charged for traffic that traverses the Gi firewall even after the GTP tunnel is deleted.

Network and Security Manager (NSM)

- **Application Volume Tracking (AVT)**—ScreenOS 6.2.0 supports Application Volume Tracking (AVT), a feature that enables Network and Security Manager

(NSM) to track network bandwidth usage on a per-application basis. The security device sends the NSM server periodic update messages containing details about port activity. NSM listens for and processes these periodic update messages and maintains a cumulative count for each port. NSM displays this count on the console.

The AVT feature has the following limitations:

- The periodic updates maintained per port for each active session can slightly affect CPU performance.
- The accuracy of AVT data is dependent on communication with the NSM server. NSM, however, lacks a mechanism to ensure that periodic updates sent by AVT from ScreenOS are received, which may result in a lag between traffic instances and reporting of those instances. NSM maintains a cumulative count for all traffic on each port regardless of session, node, or protocol. The count displayed is thus a total across all sessions; and because updates are periodic, the currently displayed number of bytes in NSM may be inaccurate until the next update.

NetScreen Redundancy Protocol (NSRP)

- **Extended Support for DHCP in NSRP Clusters**—Prior ScreenOS releases implemented some basic functions to support DHCP functionalities in NSRP cluster deployments; these functions include configuration sync and RTO sync for both DHCP client and DHCP server. ScreenOS 6.2.0 included additional enhancements to fully support DHCP functionalities in complex NSRP cluster environments. Starting with this release, admins can enable the DHCP client on VSI interfaces, use a configurable client ID to support multiple NSRP clusters in the same DHCP realm, and enable the DHCP server on VSI subinterfaces.

Open Shortest Path First (OSPF)

- **Increase the Number of LSAs in ISGs and NetScreen 5000-series devices**—ScreenOS 6.2.0 has doubled the limit of LSAs in OSPF to 4096. Previous releases had an LSA limit of 2048.

Other

- **TCP-RST in Layer 2 Zones**—ScreenOS 6.2.0 adds support for enabling TCP-RST in Layer 2 zones. The advantage of this support is that it will permit fast application convergence for sites running in transparent mode in Layer 2 zones. The option to send TCP-RST on tcp-syn-bit-check failure is an attribute that is configured per zone. L2 zones in previous ScreenOS releases do not have this option, but with this ScreenOS 6.2.0 feature, admins will be able to configure the TCP-RST option in L2 zones.
- **Route Descriptions Option for Routes in ScreenOS**—ScreenOS 6.2.0 includes the option to add descriptive labels to static routes. The ability to apply labels to static routes makes managing routing tables easier when a given deployment includes a very large number of static routes.

- **Counter for Interface Bounces**—This new counter provides a way to track how many times an interface has bounced (soft or hard reset) since the last reboot.
- **Option to Send Debug Output to a USB Flash Drive**—In prior releases, all debug information is saved only to system memory. The maximum size allowed for this is 4MB. When the debug record reaches the maximum size, the oldest debug information will be overwritten with new data and irretrievably lost. ScreenOS 6.2.0 supports sending debug output to a USB flash drive (on devices that include a USB port).

  When new debug data is produced, the system saves it to USB as well as to the system memory. Since USB flash drives are hot-swappable, essentially any amount of debug information can be saved indefinitely. When the size of the debug data file on the connected USB flash drive approaches the remaining available space on the drive, the device will prompt the system administrator.
- **SNMPv3 Views ScreenOS**—A limited subset of the SNMPv3 View Access Control Model has been implemented within the SNMP v1/v2c agent in ScreenOS 6.2.0. Configurable MIB filters may be defined to include or exclude an IP address and netmask from being included in responses to queries against specific tables. These MIB filters are then applied to SNMP communities. The following tables and entries are affected by these MIB filters:

Table Name	MIB Entry	OID
atTable	atNetAddress	1.3.6.1.2.1.3.1.1.3
ipRouteTable	ipRouteDest	1.3.6.1.2.1.4.21.1.1
ipNetToMediaTable	ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3

- **1 million sessions per ASIC on NetScreen 5200**—This new session maximum applies to NS 5000-8G2-G4 and NS 5000-2XGE-G4 devices only.
- **ISG 1000 and ISG 2000 Protocol Statistic Session Counters**—ISG platforms (ISG 1000/2000 with SM) running ScreenOS 6.2.0 add support to session counters for protocol statistics in the security module. This feature initiates a session counter and displays protocol statistics in sessions (with current session number, total sessions, and ignored sessions) for the SM. This feature is enabled by default.
- **MAC Address Checking During SYN Flood Attacks**—In some environments, SYN cookie-based SYN flood protection may cause a MAC learning error in adjacent equipment when ScreenOS sends a SYN cookie using its own MAC address. Beginning in ScreenOS 6.2.0, high-end devices can check the destination MAC address during a SYN flood attack and only issue SYN cookies for frames whose destination MAC address is their own MAC address. This feature is disabled by default. To enable this feature with the CLI:
  set asic ppu dest-mac-check

  On high-end devices, IPv4 SYN flood attack detection is done in the ASIC (PPU), and the destination MAC address check is performed in the CPU.

- **Session-based Hash Mode Support for 8G2 Aggregate Interfaces**—Beginning in ScreenOS 6.2.0, session-based hash mode support is enabled for the following devices and interfaces:
  - SG 1000, ISG 2000
  - Aggregate interface on NS-5000-series 8G2 card
  - NS-5000-series 10G card

  Session-based hashing is enabled by default on 8G2 and 10G cards. You can disable session-based hash mode on these cards using the CLI to force them to operate in per-packet round-robin use of the aggregate members. Note that in session-based hash mode the maximum bandwidth available for any individual session traversing the aggregate link is the bandwidth of one link member. For ISG 1000 and ISG 2000 devices, session-based hash mode cannot be disabled.
- **Forced Packet Fragment Reassembly Enhancement**—Beginning in ScreenOS 6.2.0, all packet fragments entering a security device can be queued and reassembled before being forwarded. When enabled, this feature executes the following:
  - Discards incomplete or overlapping packet fragments;
  - Refragments reassembled packets according to the MTU of the actual egress interface.

  This feature is a requirement of the U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments.

  To enable this feature with the CLI:

  ```
  set flow force-ip-reassembly
  ```
- **IPv4 Address Support for EPRT/EPSV/229 Commands**—ScreenOS 6.2.0 supports IPv4 addressing for RFC 2428 EPRT/EPSV/229 commands. These commands can now be executed with both IPv4 and IPv6 addresses.
- **DHCPv4 Support**—All devices running ScreenOS 6.2.0 support DHCP. ScreenOS 6.2.0 fully supports DHCP client/server/relay for virtual systems, but only on Ethernet-related interfaces.
- **Specify Source Interface in Trace-route**—A new keyword option has been added to the trace-route CLI command to allow system administrators to specify a source interface. This enhancement allows system administrators to do a trace route from virtual routers (VRs) other than the one they are currently logged into and is particularly useful for troubleshooting route-based VPNs.

  When working in route mode, trace-route uses the route tables to determine the "closest" interface to the destination address, and uses that interface IP address as the source IP address (note that the interface should have an IP address set); if the command is initiated in transparent mode, trace-route uses the default VLAN1 IP address as the source IP address. If, after attempting to execute the command, the device cannot route the packet, an error message will be displayed.

  Note that the specified from interface should be active and it cannot be loopback, null, HA, or a tunnel interface. Also, it cannot be in a null zone and cannot be a

bgroup member. The specified interface should be either a pure L2 interface or a pure L3 interface.

The new *from* interface command line interface (CLI) option is as follows:

trace-route { *ip_addr* | *name_str* } [hop *number* [time-out *number*]] [from *interface*]

- **Redirect Web Filtering of HTTPS Traffic**—ScreenOS 6.2.0 includes the ability to redirect and filter HTTPS traffic using Websense URL filtering. Prior releases only allowed redirect of HTTP traffic. As with the earlier HTTP-only implementation, this enhancement allows the device to intercept the first HTTPS request for each new TCP connection and then sends a request to Websense to determine whether or not the request should be blocked.
- **DNS Port Randomization**—The ability to enable random port assignment for policy-based DIP pools has been added; both interface-based DIP pools and policy-based DIP pools can now have ports randomly assigned. Interface-based DIP pools have random port assignment by default. Policy-based DIP pools, however, are default set to port translation, so random-port must be manually enabled by an admin.

  The random-port keyword has been added to CLI syntax for both DIP pool and extended DIP pool:

  set interface *ifname* ext ip *ip/mask* dip *dip_id ip_low ip_high* [random-port]

  set interface *ifname* dip *dip_id ip_low ip_high* [random-port]

Performance

- **FCB Pool Enhancement**—Beginning in ScreenOS 6.2.0, administrators can change the default fragment control block (FCB) pool size. Administrators can use an environmental variable, fcb_pool_multiple, to increase the FCB pool size to as much as five times the default. A larger FCB pool size improves system throughput when the system must handle a large number of fragments. The new command is:
  set envar fcb_pool_multiple *number*

  This feature is not supported on high-end platforms such as the ISG 1000, ISG 2000, and NS-5000 series devices.
- **Gate Search Performance Enhancement**—ScreenOS 6.2.0 improves gate search performance by storing gate items with source port ranges in a hash table. When an incoming packet does not match any sessions, a gate search is invoked. In earlier releases, the gate items with accurate source addresses, destination addresses, source ports, and destination ports were stored in a hash table, and those items with any of the values in a range were stored in a list. Most ALGs have a range of source port addresses, so in previous releases they were stored in a list. Because it is more time-consuming to search a list instead of a hash table, ScreenOS 6.2.0 stores the gate items with source port ranges in a hash table, thus improving search performance.
- **Software Rule Search Default Policy Lookup**—In previous releases of ScreenOS, ASIC-based devices (ISG 1000, ISG 2000, and NS-5000 series) use a hardware

policy lookup search algorithm by default. ScreenOS 6.2.0 eliminates the session setup rate bottleneck this causes by implementing software rule search as the default policy lookup on all platforms. Hardware rule search works well for deployments with small numbers of both policies and security zones because it increases session setup rates without significantly increasing CPU load.

Operational experience has shown that most customers using the platforms listed above have relatively large numbers of policies and/or security zones, so the default has been changed to software rule search to optimize operation in these environments.

It still may be more effective in some deployments to use hardware policy lookup to reduce CPU load demands. Customers who wish to use hardware policy lookup on ASIC-based devices must run unset policy swrs to change back to the earlier method.

To turn software rule searching back on, run set policy swrs to reset the device to the default.

RADIUS

- **Decouple RADIUS Authentication and Accounting**—In prior ScreenOS releases, RADIUS Accounting is coupled with RADIUS Authentication when using XAUTH and L2TP authentication. In ScreenOS 6.2.0, an option has been added to enable/disable the accounting function and to separate the configuration of accounting and authentication servers that are designated to XAUTH and L2TP.

Transmission Control Protocol/User Datagram Protocol (TCP/UDP)

- **TCP Sweep Screen**—This feature is a new control that will focus on behavior where a fixed IP sweeps across many destinations (IPs) in a short time period. This feature is a TCP/UDP sweep with functionality similar to the existing IP sweep for ICMP.

Unified Access Control (UAC)

- **UAC Captive Portal Redirect per URL Policy**—When UAC is deployed through a ScreenOS firewall, the firewall acts as the Infranet Enforcer (IE) and will redirect unauthorized access to a configured URL (captive portal). Previous ScreenOS releases permitted only one redirect URL per Infranet Controller (IC). ScreenOS 6.2.0 configures the redirect URL through a policy which means that more than one redirect URL can be configured for the same IC.
- **Messages Return for Unauthorized Access in UAC**—This feature adds a notification sent from ScreenOS to the IC. Notification is sent when traffic is rejected from an endpoint that has an infranet auth table entry if the denial is due to an infranet policy.
- **UAC / ISG-IDP Coordinated Threat Control**—Beginning in ScreenOS 6.2.0, you can configure ScreenOS to notify the Infranet Controller (IC) about attacks the IDP module detects. To enable this notification with the CLI:
  exec infranet controller notify idp-attack [*auth-only*]

ScreenOS notifies the IC of an attack by writing to the SSH connection between the ScreenOS device and the IC. When the IC receives the notification, it applies policies to the endpoint where the attack originated.

- **UAC Infranet Enforcer Redirect on Port 3128**—As part of the captive-portal enhancement to UAC deployments available in ScreenOS 6.2.0, the predefined HTTP-EXT service has been redefined to add the well-known default SQUID proxy server port (port 3128).

Virtual LAN (VLAN)

- **VLAN Retagging for ISG 1000 and 2000 Devices**—Beginning in ScreenOS 6.2.0, VLAN retagging support is available on the ISG 1000 and ISG 2000 devices. On these devices, VLAN retagging is done in the FPGA. To enable this feature with the CLI: set vlan retag name*retag-name* { untag | *vlan* } { untag | *vlan*}

Virtual Router (VR)

- **Management VR**—The ability to change the default Virtual Router (VR) to an existing VR has been added in ScreenOS 6.2.0. On high-end platforms, the VR for the management zone can be changed to an existing VR and is no longer bound to the trust-vr. The management VR will support out-of-band management and segregate firewall management traffic away from production traffic.
- **Trace-route Option**—In this release, you can specify an optional source interface when issuing a trace-route command. This option is useful for troubleshooting route-based VPNs and allows you to initiate a trace-route from a different Virtual Router (VR) than the one where you are currently logged in.

Virtual Security Interface (VSI)

- **Tunnel Interfaces as VSIs**—In ScreenOS 6.2.0, an 'inactive' link state has been added for all tunnel interfaces on non-primary virtual security devices (VSDs). A check has also been added to determine if a tunnel interface is or is not a virtual security interface (VSI). All configurations with a tunnel interface except virtual private networks (VPNs) should sync to an NSRP peer if the tunnel interface is a VSI. All other configurations will not sync. VPN configurations will sync to an NSRP peer regardless of whether the tunnel or carrier interface is a VSI.
- **VSI state reflects packet-forwarding and VSD status**—ScreenOS 6.2.0 will change the link status of VSIs belonging to a non-primary VSD to "down" instead of just "inactive" when packet forwarding fails. Inactive status signals routers not to send traffic to these interfaces and the route entries related to the interface will be removed from the Forwarding Information Base (FIB) table.

Virtual Systems (Vsys)

- **Inter-Vsys Communication over Shared-DMZ Zone**—A new shared zone called shared-DMZ has been introduced to allow inter-Vsys communications. NAT is also available for traffic from Vsys-to-Vsys based on the shared-DMZ zone to solve overlapping address issues.
- **Session Clearing in a Vsys**—The CLI can be used to clear sessions in a Vsys. In previous releases, session clearing was permitted only at the root.
- **Use Identical Zone Names on Different Vsys**—Previous ScreenOS releases do not allow for the use of the same zone name within the same device even if the zones are in different Vsys. This enhancement in ScreenOS 6.2.0 allows for identical zone names to be used in different Vsys on the same device. So, for example, a single firewall can have multiple "Accounting" zones as long as each accounting zone is in another Vsys.
- **Virtual System Support on Security Devices**—Beginning in ScreenOS 6.2.0, Virtual System (Vsys) support is now available for firewall devices, such as an Infranet Enforcer (IE) connection to an Infranet Controller (IC). A single IC can monitor multiple Vsys on one firewall.

  To enable this feature with the CLI: exec bulkcli vsys *vsys_name bulkcli_string*

Web User Interface (WebUI)

- **WebUI Policy Search Enhancement**—This new policy search feature permits admins to quickly find the policy or policies they are looking for in specific source or destination zones. The feature adds wildcard (*) support for services when searching for source and destination addresses.
- **Firefox Browser Support**—The ScreenOS 6.2.0 WebUI supports the use of the Firefox web browser version 2.0 and above for device administration. Firefox 2.0.0.16 for Windows and 2.0 for Linux are confirmed to work with the ScreenOS WebUI.

Changes to Default Behavior

This section lists changes to default behavior in ScreenOS 6.2.0 from earlier ScreenOS firmware releases.

Changes to Default Behavior Introduced in 6.2.0r3

- **NAT cookies and H.323 calls**—For the SSG-300 and SSG-500 devices, the value of max_nat_cookies_num and max_h323_call_num is increased to 1024.
- **SecurID Authentication**—SecurID Authentication with RSA Authentication Manager 7.1 is now supported.
- **"Too many loopback, maybe caused by misconfiguration", message in debug flow basic**—Packets with destination IP 0.0.0.0 are dropped silently instead of being looped in the firewall.
- **Confirm behavior of remote authentication**—Local authentication is tried only if the remote server is **"down"** and no response is received in time when the remote authentication is primary. Remote authentication is tried only if the user name does not exist in the local server when the local authentication is primary.
- **SNMP reports the wrong information for Serial and ML interface**—In previous ScreenOS versions, trunked interfaces being polled using SNMP RFC MIBS for the ifOper status was showed as UP. After the upgrade, the ifOper status was showed as DOWN. For more information, see the JTAC knowledge base number KB 13962 located at http://kb.juniper.net

Changes to Default Behavior Introduced in 6.2.0r1

- **Trustee admins untrust interface visibility on WebUI**—In prior releases, admins only had visibility to the default untrust interface when using the WebUI. With the implementation of this change, all ethernet and bgroup interfaces in the untrust zone will be visible to admins logged in to the WebUI. A new HTML page has been created to display this interface list.
- **Update set common-criteria command CLI**—The set common-criteria command keyword no-internal-command is obsolete and has been removed from the CLI.
- **[NS 5000-series] The get interface command now shows DHCP client information**—In previous releases, the get interface command failed to show DHCP client enabled on NS 5000-series devices when DHCP client was in fact enabled. The command will now show DHCP client on NS 5000-series devices.
- **NSRP link-hold-time description updated**—The set nsrp link-hold-time command is used to set a monitoring time for NSRP interfaces. Previous releases provide a misleading CLI description for this command. The description has now been updated. For systems in transparent mode, when the backup system has not set the link-up-on-backup feature and has set NSRP to monitor the interface, at times the link cannot be brought up right away. This delay might cause the system to fail-over again. To avoid an erroneous fail-over, the set link-hold-time command will hold the NSRP monitor for that set period of time, if after that period of time the monitored link is still not up, then it will fail-over. The default setting for link-hold-time is 5 seconds.

- **System reset persistence for set console disable command**—In previous releases, the set console disable command could be saved, but the setting would be lost after a system reset. The command now persists after a system reset.
- **Command unset console disable in FIPS mode resets device to factory defaults**—Previously when a device was running in FIPS mode, the unset console disable command would enable the console without resetting the device. FIPS mode, however, requires that enabling the console will cause the device to reset to the factory default configuration. Starting with ScreenOS 6.2.0, running unset console disable while the device is in FIPS mode will reset the device to its factory default configuration.
- **H.323 ALG support for dial-up VPN**—Ordinarily, the unset ike policy-checking command is not supposed to be used with a dial-up VPN tunnel. With this command, however, the device will not add a next hop tunnel binding (NHTB) for the H.323 session and the appropriate RTP/RCTP port will not be opened. In ScreenOS 6.2.0, the unset ike policy-checking command has been added to IKE gateways instead of as global configuration which permits the creation of the NHTB and the H.323 session.
- **Change NSM support for displaying chassis information**—In previous ScreenOS releases when checking chassis information using NSM, the system board was not displayed. Running the get chassis CLI command would, however, show it. From this release of ScreenOS, NSM will include the system board when displaying the chassis information and otherwise display chassis information in a manner consistent with that displayed by the get chassis CLI command.

NSM Compatibility

This section provides information about updates required to complementary Juniper Networks products to ensure compatibility with ScreenOS 6.2.

You must use Network and Security Manager (NSM) 2008.2r1 or later to manage devices running ScreenOS 6.2.0. Navigate to the support web page for more information http://www.juniper.net/support/.

Detector and Attack Objects Update (only for ISG-IDP)

The Detector Engine shipped with this ScreenOS version is 3.5.126103. Refer to the Detector release notes for more information on the availability of new releases.

After you have performed the ScreenOS firmware upgrade, you must update to the latest IDP detector engine and attack object database.

To update the detector and attack objects database:

1. Download the latest detector and attack database to the NSM GUI server. From NSM, select Tools > View/Update NSM attack database and complete the wizard steps.
2. Push the detector update to ISG-IDP devices. From NSM, select Devices > IDP Detector Engine > Load IDP Detector Engine and complete the wizard steps.

3. Push a policy update to ISGIDP devices. From NSM, select Devices > Configuration > Update Device Config and complete the wizard steps.

Addressed Issues

The following operational issues from ScreenOS 6.1, 6.0, and 5.4 release branches were resolved in this release:

Addressed Issues in ScreenOS 6.2.0r3

Administration

- **202421**—After a reboot, the unset admin hw-reset command was not saved.
- **412072**—After the "**Ctrl + C**" and "**Ctrl + Z**" actions, some event log entries were blank.
- **414839**—The policy logs in the syslog did not show the correct statistics data of the FTP traffic that was sent or received.
- **416563**—The snoop did not collect data when the filter was applied to the serial interface.
- **416873**—After a reboot, some event log entries were not recorded in the syslog file, when the syslog was configured using UDP.
- **416915**—Incorrect metric were returned when queried for the SNMP MIB variable NsVrOspfIfMetricEntry.
- **418197**—Traffic logs sent using e-mail reported an incorrect port number.
- **420873**—The set interface *name* phy commands did not generate the configuration level logs.
- **421033**—The forbidden command unset int tun.1 zone could not be executed. The command is removed from the CLI
- **428631**—In transparent mode, bandwidth option for interfaces in layer 2 zones were missing.
- **428795**—The ADSL interface showed incorrect physical downstream bandwidth.
- **429883**—The MSS-based sockets were changed on the new accepted socket.
- **432014**—An authorized user with read and write privileges was able to issue the set admin password command due to which some user privileges were lost.
- **448230**—Trustee administrator did not have correct privileges to access.

Antivirus

- **402935**—The system failed when the Antivirus (AV) module issues floating point instruction.

DHCP

- **411167**—[NetScreen 5GT-WAN] The DHCP server option for the Trust or Ethernet1 interface was missing after unset when it was in the dual-untrust mode.
- **422196**—The device was unable to obtain the DHCP address as the device used the wrong option in the offer packet.

DI

- **408269**—The Deep Inspection (DI) database failed to update due to a memory leakage introduced in the DI update process.
- **426280**—The attack db rollback command did not work on some platforms. For the other platforms, the result of the command was logged as either successful or failed in event log.

GPRS

- **417630**—When GTP inspection was enabled, the CrPdpResponse packet was not inspected when SGSN used a high source port and the GGSN used GTP pooling.
- **420613**—When GTP inspection was enabled, ICMP Destination Unreachable packets of the GTP session were dropped.
- **422979**—When GTP inspection was enabled, occasionally a DeletePdpResponse or EchoResponse dropped and the message "**non-existent gsn**" appeared in the log.
- **426075**—With GTP inspection enabled, a CreatePdpRequest that contained a duplicate TEID for the control or data plane was dropped.
- **432267**—The MS-timezone GTP Information Element was not removed when set remove-r6 was configured.

HA and NSRP

- **404981**—When the DHCP server mode was set to "**auto**" in the NSRP cluster, the standby box transmitted DHCP discover when a corresponding interface was active. This packet caused a traffic interruption by confusing the MAC table connection to the L2 switch.
- **422747**—In Active/Active mode, Fin packet in NSRP data path was not correctly processed when SYN-CHECK was enabled.

- **424242**—When performing an NSRP failover, the route pointed to a different tunnel interface. However, the synchronized session continued to point to the old SA tunnel.
- **402911**—When the device was in transparent mode, with a high traffic load, a multicast traffic leaked on the secondary device.
- **437756**—IPv6 Manual configured interface-id changed with virtual mac when NSRP was enabled.

IDP

- **415094**—[ISG-IDP] IDP engine core dump occurred due to buffer overrun condition.
- **427754**—IDP engine core dump occurred when invalid memory resources were accessed.

Management

- **411075**—If the hash value for the SSL certificate used for https management starts with a zero, the delta configuration from the NSM would occasionally report configuration difference between the device and the NSM.
- **411209**—NSM get config datafile was not in synchronization with the firewall get config saved due to the route table next hop.
- **411862**—The get config datafile that included radius attribute "**calling-station-id**", caused NSM synchronization problem with the firewall configuration.
- **414778**—[SSG-5, SSG-20] The access to a bgroup0 interface manage-IP failed when bgroup0 interface had a new port binding.
- **415871**—When the get config datafile command was issued, a trace dump appeared on the console preventing NSM import.
- **432393**—IPv6 policies were not verified correctly using the "exec policy verify".
- **438684**—The set flow mac-cache-mgt command was not working for management of the backup firewall using the Master firewall.

NAT

- **412278**—The internal algorithm used to allocate resources for interface NAT (Pport) did not allocate the resources evenly.
- **414357**—After a certain time, TCP socket leak caused loss to the management access as a result, the CLI output for the get tcp socket command showed sockets in "**close**" or "**closing**" state.
- **419638**—The RTSP ALG failed to allocate an RTSP cookie due to a memory leak.
- **427480**—NAT DST failed when IP was included in an existing DIP pool.

Other

- **257164**—URL filtering using Websense failed as the source and destination addresses in the Websense packet were reversed on the SSG platform.
- **392208**—The flow CPU value increased as a result of packet looping.
- **393301**—During Web authentication, when an ACK packet was received, the firewall mistakenly sent out a FIN packet to end the session.
- **395341**—The device would occasionally fail when RPC traffic was handled.
- **401773**—ISG chassis might have problems detecting some of the mini-GBIC interface status when under heavy traffic.
- **402919**—Under a high traffic load, the interface counter on the ASIC platform was not accurate.
- **403509**—DIP leaks when a loopback interface for cross-Vsys is used simultaneously with a loopback group in the destination Vsys for outgoing DIP NAT.
- **404582**—The RTCP packets did not prevent the RTSP session from timing out.
- **406495**—Invalid entries related to the "**bgp snmp**" were logged and displayed by the get log sys command.
- **408134**—The device reset unexpectedly when an HTTP session was released while receiving a response from the Websense server.
- **410010**—Removing a VSI or subinterface from a bridge group removed the entire bridge group configuration.
- **411673**—DH keys triggered a firewall crash.
- **412160**—[NetScreen-5000] VPN fragmented traffic for cross-ASIC sessions was dropped.
- **413421**—The URL filtering of the hosts in white list failed because the DNS resolution in white list failed.
- **413443**—When the firewall issued multiple pings, there was a delay in response.
- **413449**—In certain situations, an edit duplicated the VPN policy caused a system crash.
- **413775**—[ISG] The set sat sess-close [0|1] command did not function as expected.
- **416573**—When the debug command was run, the redundant debug information was removed.
- **420541**—The number of spaces in the syslog message was inconsistent.
- **421293**—[SSG-5, SSG-20] An interface failover or fallback did not occur when multi-link interfaces were used.
- **422068**—Clearing the authentication table entry based on the IP cleared the entire authentication table.
- **422340**—The Web authentication redirection failed when the HTTP request HOST-LINE was split to two packets.

- **422710**—In transparent mode, when the manage-IP address differs from that of the VLAN1 IP address, only the VLAN1-IP address was pinged. The ping did not include the manage-IP address.
- **423471**—[NetScreen-5000, ISG]In certain situations, session never age out in transparent mode.
- **423540**—When loopback function was checked, the device rebooted due to incorrect status of outgoing interface.
- **424182**—The CPU did not decrement the TCP RST packet's TTL, resulting in an infinite loop.
- **424649**—Multicast fragmented traffic was unnecessarily merged and dropped on the firewall.
- **425461**—When Webauth was enabled on the firewall and the user was redirected to a framed Web page, Internet Explorer (IE) 7.0 went into a loop if pop-ups were disabled.
- **425564**—The second ISDN channel status was not set to UP.
- **425765**—The device hung due to a FIPS IKE DH test.
- **427094**—Occasionally, the connection between the Catalyst switch and the Copper Gigabit Interface with Manual duplex setting was down.
- **427463**—New SQL, RTSP, H.323, SIP, SCCP connections failed due to an RM group leak.
- **427730**—[NetScreen-5000 MGT3] In transparent mode, cross-ASIC TCP traffic using a VLAN tag was dropped.
- **431675**—Defragmentation limit changed to support up to 65535 bytes of IP packet.
- **431762**—During an upgrade to Release 6.1.0r5, MGCP-related messages appeared on the console.
- **431944**—In transparent mode, MPLS pass-through traffic was dropped.
- **431994**—The DHCP server ignored the **"broadcast"** bit in DHCPDISCOVER.
- **433456**—The original source and destination addresses were missing from the USB flash log.
- **434988**—The device rebooted due to IPSec pass-through traffic.
- **436214**—The device rebooted when run into high memory condition.
- **437164**—Interface flapping occurred on some versions of NS-ISG-SX2 card.
- **441838**—After reset, when the wireless interface was disabled, the set int wireless0/0 shutdown command was added to the configuration.
- **452297**—Due to a problem, the telnet client settings could not be saved in the configuration file.

Performance

- **394094**—On an ISG platform with Jumbo frame support enabled, only one FIFO channel was enabled instead of two FIFO channels.
- **417766**—Interface bandwidth to multiple tunnel interfaces could not be configured.
- **417872**—Traffic did not pass due to a problem in handling the ESP-Null packet in ASIC.
- **419654**—[NetScreen-5000] Fragmented packets of cross-chip ASIC VPN traffic were dropped.

Routing

- **310021**—The IGMPv3 report packet was delayed when the state of the host interface changed.
- **398277**—OSPF adjacencies were lost due to an FPGA error.
- **416416**—The access list was enforced in the Policy-based routing after it was deleted.
- **417320**—When an attempt was made to initialize a type 7 LSA, some OSPF routes were lost.
- **425573**—When the device restarted, the OSPF demand-circuit or reduce flooding caused partial loss of the routing table.
- **427872**—When "**OSPF demand**" was enabled or disabled, the SPF database was not in synchronization.
- **429461**—For the default route, access-list 0.0.0.0/32 could be configured incorrectly instead of 0.0.0.0/0.
- **430932**—Secondary VPN Tunnel configured with point to multi-point OSPF stopped in ExStart.

Security

- **410696**—For the account-type 802.1X, the auth-server src-interface traffic was originated as "**self**" instead of the specified interface.
- **413037**—The firewall considered the link-local IPv6 address of the peer as IP spoofing.
- **433848**—Synchronization of flood source and destination threshold failed with IPv6 traffic.
- **464534**—CVE-2008-5077 OpenSSL incorrect checks for malformed signatures were addressed.

VoIP

- **297158**—The device was reset unexpectedly as the endpoint deletion was not handled properly with MGCP.
- **393140**—When the SIP ALG was disabled, the device reset unexpectedly with heavy SIP traffic.
- **410097**—When a SIP register request was processed, the device rebooted due to an internal error.
- **420306**—H.323 Avaya VoIP calls failed due to an ASN.1 decoding error.
- **421768**—When the H323 ALG was enabled, the H323 RAS admissionConfirm packets were dropped.
- **431830**—SIP communications failed because RPORT parameter was not considered in the ALG.

VPN

- **304277**—If there was heavy IPSec traffic, the ISG firewall would drop packets incorrectly.
- **395312**—When Baltimore Unitrust CA was used, the PKI negotiation using the SCEP failed.
- **422327**—[SSG] The IPv4 address was set incorrectly in an IPv6-in-IPv4 tunnel.
- **429634**—Fragmented packets entering the VPN were dropped when the "**ipsec-dscp-mark**" environment variable was set to "**yes**".
- **430028**—The device rebooted on its own when SCEP auto renewal of the same key was performed.
- **433589**—Global settings for IKE timers were not propagated to individual IKE gateways.

WebUI

- **411492**—When users saved the traffic log of the policy using WebUI, the "**Close Reason**" did not appear in the log data.
- **413447**—The proxy settings for a DI Attack Signature update was not displayed as expected.
- **414310**—In event log entries, for "**logged out**" of Web (http, https) management, both the src.port and dst.port were incorrect.
- **416971**—[SSG-5, SSG-20] The output for the get chassis command was missing when the get tech command was issued from the WebUI.
- **424074**—The DNS Proxy checkbox on the loopback interface was removed from the WebUI.

- **425929**—The ScreenOS CLI allowed the creation of a policy with DSCP-marking enabled and no DSCP value defined. However, when the policy was created using WebUI, a DSCP value had to be set.
- **440445**—[SSG] WebUI included reports setting for PCMCIA that were not supported.

Addressed Issues from ScreenOS 6.2.0r2

Administration

- **255412**—[SSG 500] Unable to upgrade bootloader remotely. The save boot from tftp <*ipaddress*> <*filename*> to <*filename*> command allows the administrator to upgrade the bootloader remotely using tftp.
- **303181**—The SSH PKA authentication failed when the password policy complexity was enabled.
- **303555**—Some configuration changes were not logged to the event log.
- **308262**—Device erroneously allowed to set up the reserved policy IDs between 320000 and 320002.
- **314252**—[SSG] Onboard interfaces on a SSG firewall randomly showed half-duplex, even after it was manually configured as 100 MB/Full.
- **388689**—TACACS authentication did not send auth-server connect_origin field.
- **390305**—Intrazone blocking configuration was allowed for VLAN functional zone.

NOTE: For devices managed by NSM, refer to KB13250 located at http://kb.juniper.net/KB13250

- **392254**—The WebUI idle timeout cannot be changed using external auth-server with auth-admin users.
- **395477**—The device did not authenticate to support external authentication server.
- **398432**—The TACACS type, **"auth-server scr-interface"** did not work and it took the IP address of the outgoing interface instead of the configured scr-interface.
- **403134**—RFC MIB for ifAliasm FW returned an empty space character (“ “), instead of a null string.
- **403310**—Unable to remove a URL category name with string "BL".

Antivirus

- **299978**—Antivirus scanning of MSN Instant Messaging led to high CPU utilization.

CLI

- **392417**—The set tag <*number*> command under Vsys is not configured correctly.

DNS

- **308106**—The device resets when the DNSA task was not processed on time.
- **391177**—When an address book entry was modified from one domain name to another domain name due to DNS, the CPU utilization remains high.
- **403429**—When DNS proxy is used, the event log was flooded with messages.

HA and NSRP

- **251324**—After the track-ip fails, the primary and backup interface continue to flap until the firewall is rebooted.
- **295846**—The device in an NSRP cluster resets when the device tries to update and resolve the DNS entry.
- **302374**—The CLI command unset admin hw-rese caused out of synchronization state between the NSRP cluster members.
- **310384**—In transparent mode, NSM is unable to manage the backup device in a NSRP cluster.
- **312711**—The device resets due to malformed IKE P1 NSRP RTO object.
- **389495**—In transparent mode, the management traffic to backup firewall, that passes through the master firewall caused packet loop.
- **401403**—A change in the NSRP VSD group init hold time was not saved to the flash and the configuration was not retained after rebooting.
- **408567**—With method "arp", Track IP failure time is longer than the configured "interval" and "threshold" .
- **412942**—IPv6 session in backup device was not ageing correctly when the set nsrp rto-mirror session ageout-ack command was enabled.

IDP/DI

- **297722**—When a packet with ACK set was received, the IDP dropped sessions that were in half-connected state.
- **301944**—The DI HTTP brute search functionality was incomplete.

Management

- **266093**—The custom URL category within the custom Vsys were not manageable.
- **308356**—Webtrends traffic log did not display Vsys name.
- **309253**—When the interface IP and manage-IP are different, were not able to ping the interface IP within the device.
- **309587**—When the SSH is enabled in a large number of Vsys in a short time, the CPU utilization remains high for a long time and the management of the device is lost.
- **310298**—When an interface inside a Virtual System is configured to be NTP server, the NTP server configuration line was not correctly placed in the root Vsys configuration.
- **313417**—When the command exec policy verify was executed on any SSG devices, the policy verification failed.
- **387338**—When the SSH from an HP-UX client to the firewall failed, the CPU utilization remains high.
- **391304**—The duration of time reported by policy traffic logs was shorter than the actual time duration.
- **391755**—The device lost connectivity to NSM due to an incorrect internal buffer size allocation.
- **392249**—SNMP queries on read-only also returned read-write strings.
- **394878**—Hardware counters were not collected correctly.
- **397119**—The Interface description for a sub-interface inside a Vsys does not appears correctly in the root Vsys.
- **400183**—When unnumbered tunnel interface were used in a route based VPN, unable to query *nsVrOspfIfIpAddress* .

NAT

- **307364**—Interface IP address could be unset even when the MIPs were used by policies. These MIPs are stored in the configuration and are removed only after the device is reset.
- **308572**—Pinging a DIP IP address resulted in a routing loop with an upstream device.
- **311682**—When the policy is modified from fix-port to non fix-port, packet drops due to DIP allocation failure.
- **311907**—When the CCRQ message was sent from server side, the PPTP session closes and the child GRE sessions were not cleared.
- **407396**—The DIP table erroneously showed 100% utilization, even though there were DIP resources available.

Other

- **279557**—[SSG Series] The traffic continued to pass even when the WAN serial interface with a backup interface was down.
- **288649**—[ISG, NetScreen-5000] Internal buffer leak caused some traffic drop.
- **292941**—The Counter Statistics for the bgroup interface did not correctly reflect the amount of traffic passing through the interface.
- **301623**—The integrated URL filtering did not work if the HTTP request header "hostname" included port number.
- **303202**—The device is reset due to long loop in one of the RTSP ALG's internal buffer.
- **304208**—The device is reset when the illegal memory is accessed.
- **304276**—The wireless interface remained enabled after reset and the configuration of the set int wireless0/0 shutdown command was not saved.
- **305815**—The fragmented ICMP packets were dropped for being out of order.
- **306168**—After the Web Authentication with a "&" in the URL, the "&" character was removed by the firewall.
- **306864**—The SMTP header is RFC2822 compliant and includes the timestamp.
- **307357**—[SSG 300M-Series] The status of the fan in get chassis was not accurate.
- **307814**—The HTTP 302 was not sent when the UAC authentication is stuck in pending status.
- **308408**—The ICMP flood protection option in the Screen feature allowed one packet more than the configured threshold.
- **309001**—[SSG 500] The interface link goes down intermittently causing some packet drop.
- **309168**—The device displayed the erroneous messages regarding the connectivity status of the Juniper 1GE LX Optics SFP transceiver.
- **309986**—The event "**DHCP server IP address pool changed**" was generated when the IP address of the untrust was changed.
- **310391**—[ISG] In certain situations, packets dropped when the session “inactivity age out” timer expires.
- **310435**—Accessing an illegal memory caused firewall failure while installing the policy tree.
- **310566**—With SSG 5 (Country code of TELEC), the Extended Channel is disabled after the device was reset.
- **311743**—A duplicate message was displayed when the configuration was saved in the WebUI.
- **312442**—In certain conditions, the packet for RSG traffic dropped, as the child session aged out when its parent was closed.
- **313379**—The firewall did not accept an infranet authorization table entry when it contains '\o' as a part of the user name.

- **314353**—[NetScreen 5000–M3] IPv6 did not pass through in transparent mode unless the IPv6 envar was enabled.
- **314402**—The transceivers JX-SFP-1GE-T with the part number 740-013111 always show the status as **link up** even when the cable is disconnected.
- **314819**—The device failed if VPN traffic was asymmetrically routed using a self interface.
- **315248**—The wireless interface could not be initialized when scheduler was enabled in the configuration.
- **387143**—The alarm LED cleared automatically without issuing the clear led alarm command.
- **387902**—When the UAC changes the MTU, the SSL task accesses a closed null socket pointer and the device resets.
- **389098**—Unexpected results were displayed when the AIM module treated IPv6 addresses as IPv4 addresses.
- **389786**—The counter *no arp entry* was not displayed in the get counter stat output.
- **392208**—The flow CPU becomes high due to packet looping.
- **392411**—The BRI interface configured as backup was not enabled when primary interface was disabled.
- **392767**—The device might reset when SYN attack was sent using either subinterface in route mode or VLAN trunk configured in transparent mode.
- **394959**—The device rebooted unexpectedly due to failure in memory allocation.
- **395279**—Execution of the command exec policy verify held on to the CPU for long time and caused the device to reboot.
- **395323**—A malformed VPN packet with multicast as its destination address unexpectedly went through HA interface, causing device to reset.
- **396878**—The "auth-server src-interface" traffic was originated as "self" instead of the specified interface.
- **397423**—The traffic failed when there was a duplex mismatch between the firewall and some switches.
- **398117**—HTTP Redirect to an Infranet Controller failed when the client is also using a HTTP proxy.
- **399247**—The set alarm snapshot CPU trigger command did not produce an output in the get alarm snapshot CPU all command.
- **402228**—When UDP flood protection hit the threshold, the firewall leaked one extra UDP packet.
- **405788**—The PPTP ALG caused the firewall to reset.
- **406336**—The device rebooted due to an internal error when a NTP task was processed.
- **407881**—When connected to an odd numbered RTP port, some RTSP traffic failed.
- **408158**—The device resets due to corrupted ASIC session pointer.

- **408184**—Script using CLI commands with more stack space caused the device to reboot on its own.
- **411721**—IPv6 stopped passing the traffic after 8 to 10 hours due to an IPv6 resource leak.
- **412156**—The firewall did not honor Gratuitous ARP requests when the "arp nat-dst" option was set.
- **417286**—[NetScreen-5000, ISG series] Data corruption caused the ASIC chip to get stuck and stop forwarding traffic.

Performance

- **297405**—Inter-Vsys traffic dropped unless it went through an ALG or ICMP.
- **299621**—CPU utilization runs high once for every other second.
- **304334**—The **"session scan"** task is ineffective when the CPU is high, because of constant ARP changes in the network.
- **313904**—[NetScreen 5000–MGT3, ISG] The packets dropped due to internal congestion control mechanism.
- **314096**—When accessed a null pointer, heavy H.323 traffic caused the device to reset.
- **315217**—[NetScreen 5000-2XGE/2XGE-G4] The hardware sessions that were not load balanced in FPGA on backup device caused performance drop after failover.
- **386698**—The syslog caused more miscellaneous error and discard packets that caused packet drops.
- **386735**—When an interface member was added to an aggregate interface in null zone and the aggregate sub-interface was in non-null zone, the packet dropped due to loops between ASIC and CPU.
- **405001**—[NetScreen–5000, ISG] UDP fragments are dropped because of stuck condition in ASIC chip (PPUC).
- **409538**—[NetScreen–5000, ISG series] Peer-to-Peer ALG was incorrectly enabled by default and therefore MSN, Yahoo Messenger and AIM traffic was not processed by ASIC in hardware sessions. This situation could cause high CPU utilization if the traffic load for these services was high. This ALG is not applicable to these platforms and was disabled.
  W/A: Use unset alg p2p enable command to disable it manually.

Routing

- **256473**—Traceroute across an intra-zone route based VPN failed.
- **268031**—The number of OSPF routes unexpectedly reduces due to an internal function failure.
- **302011**—The router did not determine the OSPF routes from the peer even when the router did not attain maximum routes.

- **312513**—When the RIP demand-circuit was used on a tunnel interface, the RIP neighbors were lost after NSRP failover.
- **312623**—The firewall calculated incorrect checksum for PIM register packets.
- **389669**—The firewall failed to announce BGP network prefix when the same was configured as BGP aggregate route.
- **390553**—OSPF MD5 authentication password is shown as clear text in the event logs.
- **394777**—The device incorrectly allowed the configuration of PBR next-hop of 0.0.0.0 with no interface specified.
- **395594**—The PBR entry ID greater than 128 was not considered.
- **398075**—When connected networks were redistributed into RIPng, the advertised address contained the host part instead of the subnet.
- **398950**—End of DST (Daylight Savings Time) caused OSPF to flap.
- **400333**—The device reboots due to an invalid pointer when clearing mroute object.
- **402531**—The IGMP session was refreshed unexpectedly when the IGMP proxy shared the same mroute with a static mroute.
- **404458**—The device might reboot when receiving an invalid BGP origin attribute.

VoIP

- **302418**—A buffer overflow in SIP module caused the device to reset.
- **305658**—The RTP packets were lost when NAT-T was enabled.
- **309859**—The PPORT paired ports were not released completely after an Avaya H.323 phone call was completed.
- **310081**—Changing the remote IP address within SCCP payload of the device caused a silent listener of an agent's call to fail.
- **313085**—In some scenarios, SIP cancel messages failed through the firewall.
- **393342**—The CPU rate was high due to "policy not found" error in SIP ALG.
- **394454**—The device resets due to SIP ALG error on "policy not found".
- **405078**—The device resets when SIP ALG performed an extra NAT translation.
- **406871**—MGCP ALG call transfer does not work as expected.

VPN

- **305067**—The device incorrectly decrypts the VPN packet with certain TTL value.
- **308251**—Failure to remove SPI entry caused memory leak.
- **309216**—In some scenarios, CRL renewal process failed when the CRL was renewed on the last or first day of the month.
- **389414**—In a certain condition, decryption for incoming VPN packets failed due to incomplete incoming key installation when the commit bit was enabled.

- **395216**—The fragmented packets of cross-chip ASIC VPN traffic are dropped.
- **397917**—The device in transparent mode reset when a tunnel packet with wrong destination MAC address was received.
- **399759**—The VPN configurations were being synchronized for non-VSI interface situations. A new set/unset CLI is introduced to enable or disable this feature:
  set nsrp config sync [vpn-non-vsi]
  unset nsrp config sync [vpn-non-vsi]
- **403260**—Proxy ID in dial-up VPN failed to match with multiple VPN policies.

WebUI

- **306796**—An incorrect "**Anti-spam was detached from the policy**" message was generated when the policy was created or edited using the WebUI.
- **307314**—The WebUI did not accept zero as a value for ISDN interface "load-threshold" setting.
- **309725**—The WebUI displayed incorrect DNS cache TTL value.
- **311759**—The traffic shaping parameters, PBW, and GBW could not be configured using the WebUI.
- **313278**—The firewall could not be managed using the WebUI when connected through SSL VPN proxy.
- **400895**—The outgoing-interface of Proxy DNS could not be modified.
- **403443**—Unable to configure Gateway Tracking in the WebUI.
- **405079**—Unsetting an object from multi-cell policy using software policy search causes high CPU and packet loss.
- **408978**—Address in a multi-cell policy could not be unset from the WebUI.
- **409068**—The IP address port field in proxy settings could not be unset in Security menu.

Addressed Issues from ScreenOS 6.2.0r1

Administration

- **257485**—In certain situations, the administrator was unable to add an address book item to a multi-cell policy.
- **260995**—The debug buffer might intermittently log messages even though no debug commands are running.
- **278125**—When there are multiple policies using the same src or dst IP and ports and one is disabled, and one of the address book objects is modified, the device might 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 the loopback interface fails.

- **292669**—Running the unset static igmp group command will not clear the IGMP group until that IGMP group times out.
- **302783**—When event log entries exceed the maximum number that can be stored, older entries will be overwritten without notification. The issue has been resolved by the inclusion of an event log entry to record the overwrite event.

Antivirus (AV) / Antispam

- **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.
- **297944**—When using the latest antivirus database update, a zipped EICAR test file is not always detected by the scan engine when the file is sent by an HTTP server.
- **304781**—When multiple IP addresses are entered in the antispam blacklist in netmask form, the different entries may result in the same hash key. In such a circumstance, removing an entry may make it impossible to remove one or more other specific entries. It may be necessary to run unset blacklist to remove all entries and start over.

Border Gateway Protocol (BGP)

- **303929**—A BGP peer connection cannot be established if neighbors are configured using a loopback interface as the source interface. This issue has been resolved.

Documentation

- **307763**—ScreenOS 6.2.0 documentation does not clearly explain that telnet client functionality is not available from a Vsys.

Domain Name System (DNS)

- **215889**—DNS queries are sent to the dynamically-learned DNS servers, even though the DNS servers have been configured with an admin preference of 255.

General Packet Radio Service (GPRS)

- **270890**—If the GTP Sequence Number Validation was enabled, GTP traffic was dropped due to 'bad sequence number' after two NSRP failovers.

High Availability (HA) and NSRP

- **262695**—NSRP failover might cause some VPNs to fail.
- **274948**—In NSRP, when adding an interface to an L2 zone, it does not become a VSI.

- **277859**—Session close message from primary to backup might be lost when traffic is very heavy. Disable "set nsrp rto-mirror session ageout-ack" could help reduce traffic and resolve this.
- **280217**—[NetScreen–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.
- **281729**—In Active-Active NSRP mode, some VSIs in a master VSD configured as IGMP proxy and static IGMP groups are unable to correctly send IGMP query packets. This issue will result in the interface configured IGMP host being unable to report these sorts of IGMP groups.

IDP

- **260215**—When profiling smaller networks, the profiler on an ISG-IDP is not detecting new events and is not updating old ones.
- **270319**—[ISG with IDP] The device restarts when updating a policy with no attacks that was previously configured with attacks.

IKE

- **302790**—The CLI command get ike cookie incorrectly displays the IKEv2 authentication method as "RSA-REV." The authentication method should be EAP.
- **303184**—ScreenOS will now distinguish between the src_port and dst_port from a service instead of always only using dst_port when setting IKE proxy ID ports.

Management

- **255035**—Redundant subinterfaces could not be imported properly from NSM.
- **271129**—In some cases, all management access might be lost except through the console.
- **290562**—Unable to determine BGP aggregate status within NSM.

Other

- **235777**—The command unset admin hw-reset was not saved to the configuration file after a reset.
- **252398**—Wireless connection instability occurs 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-8021" 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 might 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 might stop responding during negotiation.
- **272184**—In a deployment where one Gn firewall (NSGP client) intentionally connects with two Gi (NSGP servers), the NSGP servers might not reliably receive all management traffic sent to them by the NSGP client firewall.
- **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 was 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 subinterfaces.
- **285333**—Traffic might not pass if there is a duplex mismatch between the device interface and the switch connected to the device.
- **294702**—Load balancing among aggregate interfaces on 4-port mini GBIC cards is uneven when the interfaces are in hash mode.
- **294716**—Load balancing among aggregate interfaces on 4- and 8-port Fast Ethernet cards is uneven if the aggregate interfaces are in hash mode and the number of interfaces is three. There is also packet loss when traffic is heavy.
- **294946**—Load balancing among aggregate interfaces on 2-port mini GBIC (0x2), 4-port mini GBIC (0x3), 2-port 10/100/1000 Gigabit Ethernet, and 4-port 10/100/1000 Gigabit Ethernet cards is uneven when the interfaces are in hash mode.

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 flooding is detected and packets are dropped, even when the pps rate is less than the specified 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.
- **300444**—If a static route which has next-hop information is redistributed into RIPng, the redistributed route is not withdrawn by an unset redistribute command.

VoIP

- **278563**—Child session for SIP could not be created correctly.
- **278773**—If an Avaya 96xx phone is used in the network, the ScreenOS H.323 ALG is unable to decode Q.931 messages due to insufficient OLC support.

Virtual Private Network (VPN)

- **280101**—Dial-Up VPN traffic was dropped due to a change to the IP address on the dial-up client.
- **285748**—[NetScreen-5000] IPsec pass-through packets are being dropped when the device is in transparent mode.
- **285935**—VPN packet drop occurs due to traffic looping when aggregate interfaces are used on the device.
- **304201**—When configuring an AutoConnect-virtual private network (AC-VPN) using the Wizard, if an IP address is input as a netmask the Wizard will generate a null webpage. Once the null webpage is closed and another item is clicked or selected, an error message will be generated. The error message should now appear at the correct point of the AC-VPN Wizard configuration flow.
- **304250**—When a Virtual Private Network (VPN) connection is configured in aggressive mode and the peer is behind a device in NAT mode, negotiation will fail. This issue has been resolved and negotiation will now succeed.

WebUI

- **227316**—Unable to configure DHCP on an interface from a trustee admin user via the WebUI.
- **262490**—Unable to manage a device from an untrust interface via a trustee admin via the WebUI.
- **277867**—The RP Proxy setting is not removed when its corresponding RP 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.
- **301952**—When using the WebUI to configure static routes, admins might encounter errors when metric values are deleted. To avoid this problem, it is recommended that metric values either be left at their default settings or clearly assigned a desired value and not simply left at 0.
- **303201**—Under some conditions, the WebUI button used to create a new Virtual System (Vsys) may disappear. This problem should no longer occur.
- **303662**—An erroneous character string was appearing in the Certificate New Request WebUI page near the RSA checkbox. It has been removed.
- **304207**—The WebUI alarm log list displays inaccurate entries. This issue has been resolved.
- **290035**—When accessing a device through the WebUI, if some background GIF files fail to load properly at login, the WebUI response might appear slow and subsequent attempts to login my fail. It might be necessary to close all browser windows and clear the browser cache before attempting to login to the device again.
- **304541**—The WebUI has been enhanced to include configuration of Antivirus Warning Messages and Antivirus Notify E-mail, but this enhancement only works on SSG series devices and not on ISG or NetScreen devices.

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**.

Known Issues in ScreenOS 6.2.0r3

Administration

- **445491**—When displaying BGP, route advertised without specifying a neighbor address, the error **"bgp neighbor 0.0.0.0 does not exist"** is displayed.

ALG

- **446420**—The Microsoft windows management interface (WMI) control service fails in some scenario.

Authentication

- **429374**—Re-authentication for dot1x is not being handled correctly.

CLI

- **435979**—[SSG 500] The output of the get chassis command does not include PIM name.

DNS

- **439044**—If syslog server is referenced using DNS hostname, syslog messages are still sent to the original IP address even after the IP address of the hostname is changed.

HA and NSRP

- **437661**—The RIP and OSPF MD5 authentication results in the NSRP configuration are not in synchronization.
- **438794**—Backup NSRP firewall loses synchronized OSPF routes.

IDP/DI

- **410393**—When updating offline from the Local Server, the automatic DI signature update fails.

Other

- **435348**—[SSG5/20, SSG140/SSG500] The firewall could reset due to an exception before the boot up process. The device shows the exception dump.
- **441723**—Firewall does not send TCP RST for traffic matched by IPv6 REJECT policies.
- **427467**—[SSG 140] The device reboots unexpectedly due to ARP traffic across bgroup interfaces.

Routing

- **416966**—When a route is displayed by get route command some of the flags are not freed, causing a reboot of the firewall. But the route is frequently added and deleted by making changes in dynamic routing.

Known Issues from ScreenOS 6.2.0r2

None

Known Issues from ScreenOS 6.2.0r1

Administration

- **282562**—When upgrading from ScreenOS 6.1.0 to ScreenOS 6.2.0 in an NSRP deployment, IPv6 sessions cannot be synchronized from the ScreenOS 6.1.0 device because IPv6 session synchronization is not a supported feature in ScreenOS 6.10. This issue will cause IPv6 sessions to be lost during an upgrade to ScreenOS 6.2.0.
- **309759**—Reloading configurations while the device is experiencing heavy traffic might cause the device to fail.
- **388700**—It is currently possible to configure a VIP from a subnet other than the unnumbered tunnel interface IP. This, however, is not a supported configuration; admins should not be allowed to configure a VIP from a subnet other than the unnumbered tunnel interface IP.

Antivirus / Antispam

- **299960**—Using the new Kaspersky Labs antivirus scan engine, the antivirus database takes a relatively long time (1 to 5 minutes) to load from a flash disk to system memory. While the database is loading, CPU usage might go extremely high and device performance will drop.
- **307808**—When antivirus scanning attempts to inspect a large file (more than 30MB) during periods of heavy HTTP traffic, the device may stop passing traffic and will need to be reset.
- **388885**—The extended antivirus (AV) pattern file is too large for device flash memory for devices that support this function. Note that the standard antivirus pattern file works as expected; only the extended pattern is too large. Note also that there is no impact on ISG 1000/2000 and NS 5000-series as they do not support the extended AV pattern setting.
  W/A: Do not attempt to enable extended antivirus pattern file support.

HA and NSRP

- **273267**—In an NSRP deployment, the configuration setting for the local interface's zone (that is, set interface zone) is synced by the NSRP peers. Under NSRP, the zone configuration is synced by the NSRP peers even though the interface is a local interface. Since there is no check for zone CLIs, they are treated as global configurations. Note that this issue exists in all ScreenOS versions.
- **280659**—If an admin sets up an NSGP connection between two Vsys in the same device via an external physical link, the device might duplicate sessions when accomplishing an NSRP failover.
- **283360**—Clearing the DNS cache on the master device in an NSRP cluster will not cause the cache to be cleared on the backup device.
  W/A: Clear the the DNS cache in the backup device manually.
- **303714**—For NSRP cluster deployments, when upgrading from ScreenOS 5.4 (or any earlier release), the following ALGs will not sync correctly until both devices in the pair are upgraded: SIP, SCCP, MGCP, RTSP, SQL, PPTP, P2P, Apple iChat, and H.323.

IDP

- **263654**—On ISG 2000, when IDP enables the C2S + S2C policy instead of the C2S policy, then up to 50 % UDP throughput drop is observed.
- **269464**—For each session creation, when syn-check is enabled, then syn, syn ack, and ack arrive at flow CPU. However, when syn-check is disabled, only syn arrives at flow CPU for each session creation.

  Therefore, with syn-check enabled, the performance can drop to 8000 connections per second.
- **300443**—IDP does not support inspection of traffic or detection of attacks in nested tunnels (such as a GTP tunnel nested inside an IPsec tunnel) and thus only inspects traffic in the first level of nested tunnels for attacks.
- **305128**—If only a destination port (dst-port) is specified in IDP flow filter, the filter will not capture traffic in both directions. Traffic is correctly captured in both directions if a destination IP (dst-ip) is specified in IDP flow filter.
- **305295**—If an IDP rule is configured with the attack value NONE, then diffserv will not work. Also, when the IDP rule attack value is NONE, if a TCP packet that matches the drop packet action passes through the device, IDP will not be able to escalate the response and drop the connection.

Management

- **272925**—When the console timeout is set to 0, telnet client applications have no way to determine when a session has timed out. If the telnet client has not sent data for a significant length of time and the session should timeout, the TCP socket for the telnet session might not be correctly released.

- **298795**—Configuration of the constant specific service differs in the NSM GUI and in ScreenOS. The constant number of specific service with NSM GUI is less than in ScreenOS.

Other

- **263480**—When a small second packet follows a jumbo frame (more than 8500 bytes) on 10G card within a minute, then it might be dropped.
- **274425**—The drop of to-self IKE packets is not logged when no IKE is configured.
- **290823**—ASIC-based platforms handle byte counts differently from software-based platforms resulting in slightly different behaviors when running IKE. First, on software platforms the byte count includes both incoming and outgoing traffic. ASIC platforms, however, count incoming and outgoing traffic (bytes) independently. Also, on software platforms the byte count includes the ESP padding part of the traffic. On ASIC platforms ESP padding bytes are not counted.
- **291999**—The system might either become unstable or reboot if large debug information is printed directly on the console.
- **294425**—The CPU rate is high when the FIPS self-test runs on high-end platforms.
- **312046**—On some devices, an attempt to negotiate the maximum transmission unit (MTU) using the ICMP "packet too big" packet may fail. Failure to negotiate the MTU may, for example, cause an FTP session failure. The failure is caused in part because the ICMP packet is sent only once.
- **312724**—Sometimes a device real-time clock (RTC) will stop, causing issues with all RTC-dependent processes. For example, if the RTC stops, ICMP sessions will not age out.
- **388378**—When available system memory is very low (for example when a large number of EBGP peers are configured), if OSPF sends link state update (LSU) packets, the device may stop responding and need to be reset.

VoIP/H.323

- **300723**—According to RFC 3261, a calling party shall use "a = sendonly" to hold a call and "a = sendrecv" to un-hold it. The observed behavior of the SIP phone used in our testing is that it does not include the "a = sendrecv" command when it tries to un-hold a call. This lack causes the SIP server to return a "500 internal error" response because it is unable to determine the state of the transaction. This problem is actually a telephony system bug that cannot be resolved by ALG, so there is no work around for this issue available through a firewall.
- **310928, 314481**—SSG 140 and NS-5400 devices running in NAT mode may stop responding under heavy Media Gateway Control Protocol (MGCP) traffic.
- **311192**—Under some heavy H.323 traffic circumstances, the backup device in an Active/Passive NSRP cluster may fail.
- **311726**—Under some heavy H.323 traffic circumstances, a device in NAT mode may have inaccurate session timeout values.

VPN

- **292971**—The supported character set for IKE Distinguished Names is: A-Z, a-z, 0-9, ,) (+ , - . / : = ? Use of any other character might cause problems with the generation of key pairs. Note that this issue exists in all ScreenOS versions.
- **292975**—IPv6 traffic is incorrectly dropped by policy on a dial-up VPN.
- **293515**—The SSG 140 does not communicate with the NS Remote VPN version 10.8.1 if the encapsulating type is ESP[null/sha1]. However, the SSG 140 continues to communicate with the Microsoft IPsec VPN.
- **295494**—On modifying the destination address of transport mode VPN policy from 32-bits netmask to non-32-bits netmask, the policy-action changes to deny.
- **296270**—VPN configuration using a local interface might fail to be synced across peers in an NSRP cluster.
  W/A: Configure the local interface to a VSI interface or configure the local interfaces on both devices before configuring the VPN. Either of these approaches will permit the VPN configuration to be synced across devices in a cluster.
- **296314**—When processing GRE over IPsec traffic, sometimes the ASIC engine of ASIC-based devices will hang and traffic might be blocked.
- **298269**—At times, the RFC2544 throughput test results on NS 5000 and NS 5000M3 platforms might be zeroes. This is observed when packet size is about 9000 bytes in aes192-sha1 VPN mode.
- **301446**—Sometimes NetScreen devices cannot negotiate with NS-Remote when using ESP authentication (AES256/SHA-1).
- **314152**—If a NAT device is active between two endpoints of a transport mode VPN tunnel, any IP addresses enclosed within the VPN packets are protected and will not be translated by NAT. The NAT device thus interferes with the FTP signaling packet and the FTP ALG cannot support this configuration.
- **398018**—DNS proxy across a VPN tunnel may not work if the traffic from the IP address of the tunnel interface is not permitted by the remote firewall; for example if the tunnel interface is bound to the untrust zone.
  W/A: Set the tunnel interface's IP address using the IP address of an interface on the peer firewall that will permit the traffic.

WebUI

- **268279**—When interface information is displayed by CLI while a simultaneous WebUI session on the same device unsets any interface these overlapping actions might cause a device reset. Note that this issue exists in all ScreenOS versions.
- **298584**—On WebUI, the value of admin manager-ip cannot be set to 0.0.0.0/0.
- **313191**—For ISG-IDP devices (IDP-enhanced ISG 1000 or 2000), when running the get tech command from the WebUI (Help > Ask Support > Get Tech), security module (SM) related information is not included in the output even though the information is available.
- **393022**—ECDSA signature authentication is missing from the authentication methods list in the IKE phase 1-proposal editing WebUI page.

W/A: Use the CLI to enable ECDSA signature authentication for IKE instances.

Errata

This section lists outstanding issues with the documentation.

Deep Inspection (DI)

DI for peer-to-peer (P2P) networking application is not supported. The Concepts & Examples ScreenOS Reference Guide erroneously states DI supports the P2P networking application.

Limitations and Compatibility

This section describes limitations and compatibility issues with the current release.

Limitations of Features in ScreenOS 6.2.0

This section describes the limitations of some features in the ScreenOS 6.2.0 release. They apply to all platforms unless otherwise noted.

NOTE: Transceiver Compatibility—Juniper Networks strongly recommends that only Juniper-provided transceivers be used on interface modules. Different transceiver types (long-range, short-range, copper, and so on) can be used together on multi-port SFP interface modules as long as they are Juniper-provided transceivers.

Juniper Networks cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

- **Admin login sessions not cleared automatically**—If the admin timeout value is set to zero using the set console time 0 command, any accidental network disconnection (e.g., a cable is unplugged or the client is not closed normally) will leave the associated sessions open and leave an active entry in the admin table. The entries will not be cleared until the device is reset. [281310].
- **Telnet client not available from a Virtual System (Vsys)**—The new telnet client from the CLI interface enhancement is not available at the Vsys level. [307763]
- **Fast Ethernet port trunking on ISG 1000/2000 requires consecutively numbered ports**—Fast Ethernet port trunking on ISG 1000 and ISG 2000 devices has a limitation. If an aggregate interface has more than two ports defined, the ports must be numbered consecutively without interruption when they are added to the interface.

  For example, ethernet2/2, ethernet2/1, and ethernet2/3 ports can be configured even in the order given because they are numbered consecutively. If ports

ethernet2/1, ethernet2/2, and ethernet2/4 are configured, however, then sessions on this interface will experience load balancing issues. This second example is not a supported or recommended configuration.

- **IP Authentication Header not supported over IPsec VPNs**—Use of IP Authentication Headers (AH) over a transport IPsec VPN is not supported and will result in dropped traffic. Encapsulating Security Protocol (ESP) over transport IPsec VPN is a confirmed, viable alternative to IP AH. [283618].
- **Use of DIPs and SCTP multi-homing**—There are several Stream Control Transmission Protocol (SCTP) limitations when the ScreenOS device uses DIPs.

  When SCTP multi-homing is used with DIPs, there is source port translation error that results in erroneous source port translation and ultimately dropped traffic.

  When DIPs are used in an SCTP multi-homing deployment, sessions cannot be immediately cleared when a shutdown message is received and will only be freed after a timeout.

  When SCTP multi-homing is employed on a device using DIPs, not all sessions will be synched by devices in an NSRP cluster.

  When DIPs are used with SCTP multi-homing, SCTP heartbeat traffic will be dropped by the device, thus the SCTP heartbeat function is not supported.

  In general, ScreenOS 6.2.0 does not support SCTP multi-homing when DIPs are used by the ScreenOS device. [285236, 285672, 285722, 285988]
- **8G2-G4 card throughput stability**— Running repetitive maximum throughput tests at certain small frame sizes, can cause a variance of up to about 14% difference in throughput between two test cycles. The behavior is restricted to the 8 port G4 card. This does not jeopardize customer traffic in any way.
- **NS 5000-series throughput stability**—For NS 5000 8G2-G4, a hardware limitation might result in degraded throughput stability. This limitation is also present in ScreenOS 6.0.0 and 6.1.0. [287811]
- **TCP and UDP sweep screen attack monitoring**—The TCP and UDP sweep screen check is insufficiently accurate. Under extended testing, it will sometimes report benign traffic or below-threshold attacks as valid sweep attacks. [293313]
- **Virtual MAC Address duplication**—Because ScreenOS derives VMACs based on information taken from cluster ID, interface ID, and VSD, it is not permitted to use the same clusters and VSDs on the same broadcast domain. If cluster IDs and VSDs are duplicated on a broadcast domain, it might result in the same VMAC being assigned to more than one interface or device. [300933]
- **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.

- **NSRP**—NSRP is not supported on WAN interfaces. Devices with WAN interfaces can use NSRP, but the WAN ports do not automatically failover as the Ethernet ports do.
- **Flood Screens**—On ISG 1000, ISG 2000, NetScreen-5000 Series devices, the UDP and ICMP flood screens apply to the physical interface and therefore require that the zone be bound to a physical interface. The following limitations apply:
  - When zones are bound to a sub-interface, the ICMP and UDP flood screens are not enforced unless the zone is also bound to a physical interface.
  - When ICMP and UDP flood screen options are configured for different zones and on the same physical interface, the flood threshold is applied based on the last configured zone threshold.
  - When ICMP and UDP flood screen options are applied to a zone tied to multiple physical interfaces, the entire threshold value is applied to each of the physical interfaces.
  - For reference, the High Availability (HA) zone does not allow any screen features to be configured.
- **Configuration file downloads through WebUI without authentication**—Using the WebUI firewall downloads the configuration file without authentication. For more information, see the JTAC knowledge base number KB 12943 located at http://kb.juniper.net.

NetScreen-5GT Support Errata

While a majority of the new features and enhancements included in ScreenOS 6.2.0 are available for use on NetScreen-5GT devices, due primarily to memory constraints, some 6.2.0 features are not available on the NS-5GT. The section below notes which common features and enhancements in ScreenOS 6.2.0 are not available for NS-5GT customers.

- Transparent Mode for IPv6
- DHCPv4 service improvements
- NSGP Enhancements (GPRS)
- Deep Inspection (DI)
- Universal Threat Management (UTM)
  - Anti-spam
  - Antivirus
- Increase FCB buffer for Multicast Fragmented Packet Support
- Make software rule search (set env swrs=yes) the default behavior

NS-5GT Limitations

- ScreenOS 6.0.0 and 6.1.0 do not support NS-5GT devices. When upgrading from ScreenOS 5.4.0, it is not necessary (or even possible) to upgrade to an interim release.
- 5GT devices are unable to upload new device images using a script. This is actually a precaution to maintain a viable image at all times and prevent a system failure. When uploading a new image, until the entire image block is written to the flash, the device will not permit any other flash operations. [301162]
- 5GT devices have insufficient flash memory to support the current antivirus (AV) key and database. When an NS-5GT device is upgraded from an early release to ScreenOS 6.2.0, the AV license and database will be removed. [306084]

Compatibility Issues in ScreenOS 6.2.0

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 6.2.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, Firefox version 2.0.0.16 and above for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS X.
- **Upgrade Support**—We recommend that you follow the upgrade instructions described in the ScreenOS 6.2.0 *Upgrade Guide* located at http://www.juniper.net/techpubs/software/screenos/screenos6.2.0/upgrade_guide.pdf.

Documentation Changes

- The document called ScreenOS *Migration Guide* in some earlier releases has been renamed ScreenOS *Upgrade Guide*. The content is updated for 6.2.0.
- 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 a searchable index to and made some changes to the appearance of the online Help system.

Getting Help for ScreenOS 6.2.0 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.