Juniper Networks ScreenOS Release Notes

Release 6.2.0
January 2009
Part Number: 530-023778-01
Revision 03

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 6.1r3, 6.0r7, 5.4r10, and 5.3r10.

NOTE:

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

NOTE: 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/.

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.

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.

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*

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.

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.

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.

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.

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.
  - NSM 2008.2r1 is required to view the enhanced logging this feature provides.

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.

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 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.

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.

  This feature has the following limitations:

  - When both IDP and IPv6 traffic are 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.
  - IPv6 IDP logging requires the use of a syslog server.
  - NSM 2008.2r1 is required to use IPv6 support on IDP devices.
- **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.

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.

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.

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.

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.

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 ScreeenOS**—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]

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).

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.

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).

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.

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.

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 congfigurations 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.

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.

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.

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.

Changes to Default Behavior

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

- **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 reseting 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.

Addressed Issues in ScreenOS 6.2.0

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

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/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.

Dynamic Host Configuration Protocol (DHCP)

- **302116**—The DHCP server service mis-handles custom options 78 and 79 by truncating the first character of the text entered after "string" in the set interface bgroup *number* dhcp server option custom *number* string “*string*” command. The issue has been resolved; custom options 78 and 79 are now correctly supported.

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 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**—[NS-5000, ISG] When the device is in Active/Passive NSRP cluster, under a particular circumstance after a preempt primary device is reset, traffic via VPN is dropped by its VPN peer.
- **282261**—NSRP failover from the backup to the primary taking longer than expected.
- **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 config 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 dialup 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 in ScreenOS 6.2.0

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

Administration

- **282562**—When upgrading from ScreenOS 6.1.0 to 6.2.0 in an NSRP deployment, IPv6 sessions cannot be synchronized from the 6.1.0 device because IPv6 session sync is not a supported feature in 6.1. This issue will cause IPv6 sessions to be lost during an upgrade to 6.2.0.
- **309759**—Reloading configurations while the device is experiencing heavy traffic may 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.

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.

- **Zone screen alarm-without-drop does not drop packets when Session Limiting is enabled**—Session Limiting always takes effect regardless of whether or not alarm-without-drop has been enabled.
- **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 devices 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 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.

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.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.