# Juniper Networks ScreenOS Release Notes

**Release 6.2.0r15**
**September 2012**
**Revision 01**

**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 6.1.0r7, 6.0.0r8, and 5.4.0r25.

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 6.2.0r11

### Antivirus (AV)

- **Antispam**—Beginning with ScreenOS 6.2.0, Antispam enhancement inspects the parameters in the received email header.

## New Software Features and Enhancements Introduced in 6.2.0r10

### CLI

- x-in-ip

  **set envar x-in-ip**

| | |
|---|---|
| x-in-ip | In [ISG-1000 and ISG-2000] devices, Protocol 97 forwards traffic through CPU and not hardware, causing high CPU. To allow the unknown protocols like Protocol 97, use the following command: **set envar x-in-ip=yes**<br><br>Use **unset** command to disable envar. |

**Example:** The following command allows the unknown protocols like Protocol 97 on the device:

**set envar x-in-ip=yes**

**reset**

## New Software Features and Enhancements Introduced in 6.2.0r7

### Intrusion Detection and Prevention (IDP)

- **Security Module (SM) Monitor**—Beginning in ScreenOS 6.2.0r7, the IDP security module is enhanced to detect failure in processing packets. An internal heartbeat is implemented to detect failures in the packet processing thread of IDP. In the event of failure, the IDP security module CPU is marked as DOWN, and a log message is generated by the Management Module (MM). The traffic is not forwarded to the security module CPU preventing traffic outage. In case of NSRP cluster deployment, if the SM is marked as DOWN, a failover can be triggered depending on the NSRP SM monitoring configuration. When the SM starts responding to the heartbeats after a failure, a log message is generated. In addition, a log message is also generated if the SM policy is not loaded successfully.

  To enable or disable this feature use the **set** or **unset sm-ctx monitor** command. By default the feature is disabled.

  To configure the monitoring interval for SM use the **set** or **unset sm-ctx monitor-interval <number>** command. The default value is 1 second, which means that the MM sends a heartbeat every second. The range is 1 to 3600 seconds.

  To configure the threshold use the **set** or **unset sm-ctx monitor-threshold <Upcount> <Downcount>** command, where:

- Upcount is the number of continuous heartbeats received to consider the SM as UP state.
- Downcount is the number of continuous heartbeats that are lost to consider the SM as DOWN state.

The range for both <Upcount> and <Downcount> is 1 to 3600. The default for <Upcount> is 1, which means that if the MM receives any heartbeat after a failure, the SM card is marked as UP again. The default for <Downcount> is 30, which means that if MM cannot receive any heartbeat for 30 consecutive times, the SM is marked as DOWN.

To configure the MM to send health notification periodically use the **set** or **unset sm-ctx health-notification-interval <number>** command. The range is 1 to 864000 seconds. The default is 86400 seconds, which means that the MM generates a health notification log each day.

To check the monitoring information and statistics use the **get sm-ctx status** command.

## 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.
- **Sophos Anti-Spam to replace Symantec Anti-Spam**—Beginning mid-September 2009, Sophos Anti-Spam service is made available to the ScreenOS-based products; SSG, and ISG. The Sophos Anti-Spam service will replace the Symantec Anti-Spam.

  There will be no impact to customers running any version of ScreenOS. No configuration changes are required. The redirection to Sophos servers will be automatic and transparent to the end-user. The security devices will be pointed to the Sophos servers.

### 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 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 6.2.0r13

- **Recording event log messages in the right VSYS** — In a multiple VSYS configuration on the firewall, an event that occurred in a specific custom VSYS-A was incorrectly recorded as an event log message in the root VSYS or in a different custom VSYS-B. This behavior is corrected and fixed. As per the behavior change we now log the event log messages under the right VSYS specified for and will avoid logging incorrect event log messages in different VSYS.

### Changes to Default Behavior Introduced in 6.2.0r11

- **Flush rip route learnt from demand circuit**— A new command **clear vr<*vr_name*> protocol rip database** is introduced to flush rip route learnt from demand circuit in the specified VR.

### Changes to Default Behavior Introduced in 6.2.0r7

- **SSL renegotiation**—Beginning with 6.2.0r7 release, ScreenOS rejects SSL renegotiation from the SSL client that does not implement RFC5746.
- **High flow CPU after upgrading ScreenOS**—[NS 5000] Under certain conditions, only software sessions were created when there was no destination MAC address entry of the packet in the MAC learning table. As a result, subsequent packets were flooded and the CPU utilization was high.

## Changes to Default Behavior Introduced in 6.2.0r6

- **Unexpected Low VPN Throughput**—When VPN monitor is configured for VPNs on NetScreen-5200 or NetScreen-5400, the device can define sub-optimal ASIC mapping for processing VPN traffic in the hardware which causes unexpected low VPN throughput. A new command **set flow ipsec-distr-asic** is introduced to include the enhancement that VPN encryption will be distributed into different chips based on the tunnel's SA index per round robin. By default, it is disabled. This is applicable for NetScreen-5000 series only. For NetScreen-5000 series with VPN on IPv6 environment, enabling this command is not recommended as it would yield less than optimal performance.

## Changes to Default Behavior Introduced in 6.2.0r5

- **Unable to telnet to firewall**—The telnet console displays **Can't create telnet-cmd:6 task** error message when the SSG devices are managed through telnet. Hence, the tasks on SSG devices have been increased to allow device management.
- **NAT cookies reach maximum number**—[SSG 140] The maximum number of NAT cookies is increased to 512.
- **Increase in the capacity of number of service objects and address groups**—For ISG Series, the capacity of number of service objects and address groups is increased to 4096. For NS 5000, only the capacity of number of service objects is increased to 4096.

## 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 3.5.139490. For more information on the availability of new releases, see Detector release notes at http://www.juniper.net/techpubs/software/management/idp/de/.

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 ISG-IDP 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 6.2.0r15

#### ALG

- **736470**—H.323 ALG was unable to handle cross vsys H.323 traffic.
- **752103**—ALG is not translating the IP address for "RTSP SET_PARAMETER" request in the RTSP traffic payload when configured for VIP translation.
- **771008**—Communictation failed when H232 ALG may change h245 address in the payload.

### Antivirus (AV)

- **753601**—Sometimes websites failed to open with AV enabled, if the server does not send the FIN ,after sending HTTP body.

### Authentication

- **778720**—Firewall stops authenticating against RADIUS server when the RADIUS server configuration is changed from domain name to IP address.

### Management

- **737433**—The ifIndex value is not the same in standard MIB and Netscreen enterprise MIB while executing SNMP query for interfaces.
- **737747**—While using standard MIB2, indexes or mapping between Indexes of the OID 'ipAdEntIfIndex' and the OID 'ifDescr.x' are incorrect and as a result SNMP poll sends an incorrect result.
- **738116**—SNMP Authentication Failure Trap is generated when a GET-REQUEST with different SNMP version is received.

### NSRP

- **705438**—In asymmetric routing condition, if a session is not prepared and synchronized correctly might result in unexpected packet drop.
- **773841**—Track-ip is unable to change NSRP state from inoperable to backup when monitor setting is deleted.

### Other

- **523647**—The "set envar" command used to address the ESP sequence number is not retained permanently after the process of Asic re-init and reboot of the firewall.
- **585488**—Firewall core dumped and rebooted when using tftp get tech > tftp command.
- **587570**—Incorrect calculation of oif in multicast.
- **590160**—Device might crash when route id is a larger number and the NSRP route sync is enabled.
- **689721**—The Random Number Generation for SPI does not work and might overlap between master and backup devices during the HA cluster software upgrade.
- **710595**—When the "Pending Drop Notify" counter fills up the Infranet Controller process on the firewall and does not release regularly, results in Drop queue full message and no Drop notify messages to be forwarded to Infranet Controller.
- **719600**—Device hanged due to ASIC when IDP tried to process IPv6 ESP traffic resulting in split bran situation.
- **721101**—Device might reboot unexpectedly when the firewall received invalid HA messages.

- **728480**—Asymmetric traffic fails when the session is installed in ASIC or Hardware and when IPv6 is enabled.
- **730059**—Firewall might reboot unexpectedly if net-pak contains the wrong flag.
- **731534**—Firewall was spontaneously rebooting due to memory overwrite.
- **732793**—Device might crash when trying to modify an existing policy.
- **735268**—Sometimes device may reboot with core dump due to a logical error in the code.
- **736122**—In IKEv2 VPN, device may reboot with crash dump on receiving illegal or malformed IKEv2 packet.
- **740513**—When SIP ALG fragments the packet, the first fragment is of small-sized which may not include the mandatory SIP headers.
- **740584**—When a sub-interface is created and cancelled an event message "MTU for interface has been changed to 1500." is displayed.
- **742169**—Firewall reboots spontaneously.
- **743309**—Multicast traffic can cause firewall to core dump when there is no mroute or when the route is incorrect.
- **744684**—Sometimes, after OS upgrade, the firewall starts rebooting continuously in loop condition, due to a memory overwrite issue. This is because of smaller buffer size of fat table in flash.
- **744785**—When you send traffic to an IP address that is part of the loopback interface subnet, there is an infinite loop and this might cause high cpu.
- **745791**—In layer2 mode, if a switching loop sending a packet originating from the firewall back to itself on a different interface, then the interface adds the vlan-1 Mac address to the interface Mac table. An additional check is added to prevent the firewall from adding its own vlan.
- **746646**— ARP entries in Hardware and Software may mismatch due to inconsistent ARP update mechanism in the high-end ASIC based firewall.
- **750929**—Device might crash when you delete the interface used by NTP module.
- **751579**—VLAN traffic may be dropped on ASIC based platforms in Layer-2 Transparent Mode if VSYS bound to VLAN Group is deleted, and the same VLAN Group is referenced in an another VSYS.
- **752246**—SCTP natted traffic might stop working when you set the envar x-in-ip.
- **753180**—The check RA message flag does not follow RFC requirement, which makes the test wrong. Change the check for RA message according to RFC.
- **756682**—Internet Explorer 9 pop-up credentials does not appear with SSG firewall Authentication.
- **768558**—Sometimes cross ASIC traffic gets dropped due to incorrect logical check in the code.
- **769297**—Sytem failure occurred during malloc memory leak failure.

- **769737**—When the card is plugged in on slot 5 the information of the card cannot be seen in datafile.
- **771104**—ICMP unreachable traffic does not undergo NAT operation in transparent mode.
- **771666**—When IPv6 and BGP are enabled it caused the firewall to core dump.
- **773293**—Harmless unnecessary debug message has been removed from the console output.
- **775604**—In NSRP cluster, "dhcp server auto" does not work.
- **775844**—In SSG520M and SSG550M devices, fan status sometimes appears as "down".
- **777142**—When performing snoop offset filter on VPN tunnel traffic firewall may core dump.
- **777170**—Backup firewall in a HA cluster with IPv6 enabled experienced high CPU, as the connected switch was forwarding all the packets to the backup device due to a problem with switch losing its MAC table.
- **777402**—Sometimes PPTP fails due to route lookup failure in cross-VR design for child GRE session.
- **778810**—Policy change caused h323 alg hit a null pointer and device failed.
- **779261**—HA resync caused device with large configuration in NSRP failure.
- **780465**—Ctrl+C does not interrupt the output of CLI through get commands.
- **781343**—In a VSD-less cluster, the device will now check to make sure the ingress and egress interfaces match the session. If they do not match, then the device clears the existing session and creates a new session with the correct interfaces.
- **782678**—Device might send multiple traps for a single event causing duplicate entries.
- **789358**—On PIM interfaces, setting "set int <phy link-down>", does not keep the interface down even after a reboot.
- **790842**—Firewall core dumps and reboots when 'set zone trust screen ip-spoofing include-default-route' command is executed.
- **797994**—When the firewall is configured for ALG with loopback interface the firewall may core dump and reboot.

### Routing

- **730018**—BGP IPv6 prefix was not advertised after reboot.
- **783986**—When compatibility with RFC-1583 is set for OSPF and a network change occurs the box have to run several calculation for SPF to get the correct and complete OSPF database.

### Screen

- **743842**—Brute-force attack pop3 detection failed under certain conditions.

### VPN

- **731964**—L2TP IKEv2 VPN might not come up if multiple IKEv1 & IKEv2 VPNs are configured.
- **749931**—Phase 2 rekey failed on IPSec with NAT-Traversal.
- **780247**—Proxy ID mismatch between SA and policy was due to an endian issue.

### WebUI

- **777559**—In WebUI, event log was not showing the correct number of lines.
- **770471**—In WebUI, removing the configuration related to proxy-id was not possible.
- **773466**—In WebUI, special characters in the route map name were discarded when using the "Add Seq No" link. This resulted in the creation of a new route map rather than a new sequence number on the existing route map.

## Addressed Issues from ScreenOS 6.2.0r14

### ALG

- **710227**—SIP ALG was modified to ensure that all SIP data fragments have their call data modified according to any NAT parameters.

### Management

- **687217**—Firewall failed when you run fprofile.
- **696588**—If SCP file transfer was used regularly the firewall experienced high memory utilization.
- **726174**—Firewall might add additional padding to a reply packet.

### NAT

- **700690**—Sometimes the Extended IP x.x.x.x or its range collides with IP y.y.y.y or its range when configuring an ext DIP on unnumbered tunnel interface.

### Other

- **551755**—"IPv6 neighbor gateway [IP6] is reachable" was logged incorrectly when it is unreachable.
- **692085**—Firewall was rebooted and core dumped due to multicast packets accessing the null pointer for a PIM neighbor.
- **700331**—Firewall was rebooted and core dumped after adding VSD-Group.

- **708406**—Firewall rebooted and core dumped due to accessing the invalid memory area.
- **718372**—When a session was taken out of hardware and if the firewall received a FIN then the firewall did not close the session.
- **721988**—There was a memory Leak in Anti-SPAM feature of UTM.
- **722208**—SSG device stopped passing traffic in all directions due to an error in read logic on the interfaces.
- **723404**—During external vulnerability scan, a spontaneous reboot due to a null pointer occurred.
- **724145**—During device reset, the custom NSM management port resets from 7900 to a default port of 7800.
- **726468**—The PKI process might send an incorrectly formatted message to the SSH process, resulting in a core dump.
- **727126**—Firewall spontaneously reboots when FTP server tries to initiate data connection before client sends **RETR** command.
- **727177**—Pass through IPsec sessions are not removed in NSRP VSD-less cluster.
- **728097**—On interface configuration, firewall is accepting network number (1.1.1.0/24) as an IP address.
- **731582**—Debug flow drop, shows the packet information for the dropped packets.
- **733528**—In IGMP proxy, when an admin clears multicast-route (mroute) by executing the CLI **clear vr vr-name mroute** command, it cannot rebuild the mroute even after the new igmp v3 report packet arrived.
- **739175**—Illegal memory access causes spontaneous reboot of the firewall.

### Routing

- **703677**—In redundant VPN configuration, OSPF did not come up during VPN failback from secondary to primary.
- **718144**—During route failover some sessions are not getting cleared.
- **728946**—BGP router cannot be established between two loopback interfaces belonging to different Virtual routers on the same device.
- **734361**—BGP neighbor parameter rejection command is deleted after BGP instance flap or upon reconnect.

### WebUI

- **687935**—In WebUI, the policy search feature was unable to display the selected service if it belonged to multi-cell service.
- **688016**—WebUI was unable to display NHTB table entries if the list of NHTB entries was more than 582.
- **717325**—Monitor Zone and Monitor Interface configuration was not available in WebUI.

## Addressed Issues from ScreenOS 6.2.0r13

### ALG

- **604887**—With SIP ALG enabled, the device might sometimes send TCP packets with window size zero which might stall the SIP session.
- **666641**—RM resources are released incorrectly causing RTSP traffic to drop subsequently.
- **678300**—Failure to translate IP on SET-PARAMETER within RTSP by ALG causes the video streaming to stop intermittently.

### Antivirus

- **690029**—Downloading large file (if the content-length of HTTP request was too large) failed with ASP error when AV was enabled.

### IDP

- **670441**—Security Module in the ISG platform stopped passing traffic due to a memory leak condition.
- **716838**—A potential memory leakage occurred when IDP engine checked compound signature.

### Management

- **703695**—Unable to add MIP configuration to a multi-cell policy through WebUI.

### NAT

- **611751**—MIP for GRE over IPsec does not work, if the MIP is not in the same IP subnet as the tunnel interface.

### NSRP

- **568133**—IPv6 RA messages are processed on VSD 0 interfaces and are not processed on VSI interfaces which are part of VSD 1 and VSD 2.
- **672901**—After failback due to preempt, the new master (with preempt) sometimes lost connection to IC4500 (Infranet Controller).
- **703949**—The expired tunnel sessions were not removed properly in a backup device.

### Other

- **574244**—Even after no preempt option was enabled, sometimes the device rebooted as master.
- **578204**—Firewall forwarded duplicate log information to NSM due to an error in the session byte count.

- **599686**—FTP ALG did not work correctly when receiving unexpected ack from server, after the EPASV request from client.
- **599808**—Ability to log UDP floods on ASIC based systems was added.
- **600543**—With NSM enabled, the device management was very slow and the device was resetting frequently.
- **660288**—In non-HA mode, IPv6 multicast packet was dropped by the interface when ipv6 configuration is disabled. Do not consider VSI.
- **660420**—The backup device in an Active or Passive NSRP cluster sometimes failed to create the session.
- **662330**—Asic classifier bug caused IGMP Query messages to trigger Source Route IP alert on ISG's.
- **662589**—Firewall experienced core dump and rebooted the system when accessing the Dlog process.
- **664502**—H323 messages are still flooding in ISG2000 even after disabling h323 app-screen message-flood.
- **665008**—TCP connection was not established for MSRCP traffic in certain conditions, due to an endian issue.
- **665355**—NSM does not support the firewall "unset nsrp config sync vpn-non-vsi" command.
- **671719**—NSM was unable to update policy to device because sme_bulkcli was stuck.
- **674245**—"Packet Too Big" message from ICMPv6 was dropped due to no session.
- **674637**—The firewall crashes sometimes when a long URL was described in custom category of sc-cpa.
- **674736**—GTP IDreq packets are incorrectly dropped by sanity check due to unknown IE.
- **675296**—In L2 mode, the vsdless session must have time sync mechanism.
- **675550**—When upgrading through tftp, the device might reboot with core dump.
- **676289**—The device crashes while running certain commands through SSH or telnet.
- **676354**—SSG140 dlog queue fullness causes session leak and results in traffic drop with message "packet dropped,the dlog queue is full".
- **676984**—Authentication in NSRP from an Infranet Controller can sometimes lead to duplicate authentication entry and caused crash dump and rebooted unexpectedly.
- **677385**—Transparent or L2 mode firewalls sends a SYN+ACK response packet to client with an all-zero MAC address.
- **677467**—Open SSH 5.8 client with pty-req greater than 256 bytes fails with "PTY allocation request failed" error.
- **679138**—Data link was unavailable when there was only one link in HA zone connected to 16 port uPIM.

- **680365**—Firewall crashes and reboots when AV was enabled.
- **681955**—Syn-cookie might not get triggered sometimes for the traffic that traverses custom L2 zones.
- **683501**—The MSS option and length are incorrectly built when using SYN proxy.
- **686087**—Unable to bind an unnumbered tunnel interface within a VSYS if the VSYS name contains parenthesis.
- **686165**—If the IP of egress interface changes then existing sessions never gets updated with the new IP.
- **687653**—Sometimes tftp fails due to save configuration (from device).
- **688228**—When layer 2 broadcast packet was received, it was incorrectly interpreted as Winnuke attack.
- **688938**—In a multiple VSYS environment, event Log messages on the Syslog server was showing a wrong VSYS as the origin of the message, as the message belongs to a different VSYS.
- **690786**—Unable to change the maximum number of sessions with envar command on ISG2000 box with advanced license and less than 2GB memory.
- **692124**—NHRP feature resulted in a memory leak condition.
- **692497**—When "set envar x-in-ip=yes" on ISG1000, get error "x-in-ip not supported".
- **699131**— ISDN primary number and alternative number length fields changed from 15 to 16.
- **699200**—Due to URL filter and DNS the firewall caused core dump and rebooted the system.
- **700352**—DNS server cache snooping remote information disclosure detected.
- **700481**—With SNMP and more than 8 VSD groups configured, the device might cause core dump and rebooted during SNMP polling.
- **701519**—Pass through VPN traffic breaks source session limit set on zone screening.
- **701968**—Session are not updated with the new VPN with better route and packet dropped.
- **707116**—Backup firewall in the NSRP cluster was not able to close all the eligible sessions when it received a session close message from the master.
- **709646**—Under a certain condition, Serial interface accepted traffic whereas Ethernet interface did not accept traffic.

### Routing

- **683325**—OSPF neighbour ship gets affected in loading while the OSPF messages fragment size is bigger than 1668 bytes.
- **686224**—BGP neighbor flapped at irregular intervals.

### VoIP

- **705648**—SIP ALG was unable to parse the multipart or mixed MIME type in SIP INVITE packet, when it had values within quotes, but spaces in between words.

### VPN

- **592160**—After HA failover, the tunnel route pointing to the VPN stayed inactive for long time by causing traffic loss on the new master.
- **592488**—Connection to VPN failed when the external IP changes on the NAT device that resides in-between VPN end points.
- **661016**—Device experienced memory leak if ACVPN was configured.
- **673075**—IKE DPD messages are generated from the NSRP backup device even after NSRP failover occurred.

### WebUI

- **610921**—WebUI had limitations on ipv6 client-duid length.
- **671222**—The WebUI login might not accept an username of 31 or greater characters even though the username was valid through CLI.
- **676776**—WebUI was unable to display vrouter name, if the length was more than 15 characters.
- **678280**—Unable to modify WEB filter custom message on ScreenOS firewall through NSM GUI for integrated SurfControl CPA.

## Addressed Issues from ScreenOS 6.2.0r12

### ALG

- **539589**—Return NIS packets might be dropped on the firewall due to non-existence of ALG pinhole. This is specifically with design where NIS server resorts to DNS lookup when host is not found in NIS database.

### Antivirus / Antispam

- **604069**—When Antispam or Antivirus was enabled, under certain conditions during TCP establishment, the TCP traffic did not flow properly.

### DHCP

- **658763**—-The maximum number of DHCP relay agents supported was increased from 3 to 4.

### HA&NSRP

- **609184**—HA LED status was incorrect when **unset VSD-group** id was configured as 0.

### IDP

- **662378**—After restarting the security module the policies are not compiled and loaded in to the IDP module.
- **670888**—IDP module core dumps when the security module is restarted.

### Management

- **556535**—PBR configuration was lost after the firewall was rebooted.
- **575680**—SNMP walk on 10-gig interfaces shows incorrect interface speed.

### Other

- **487640**—Hardware counters did not work on NS-5000-2XGE-G4 [2 x 10GigE Secure Port Module (SPM)].
- **544795**— "Unset http skipmime mime-list" command appears during config.
- **558343**—Memory utilization of "sys pool" increases as some of the memory allocated in SMTP parser are not freed when the SMTP sessions are released.
- **561641**—Packet loss under heavy traffic with NS5400 and 2XGE cards.
- **578457**—SCP was not working on Ubuntu 10.10.
- **581190**—The device failed when memory was allocated.
- **585768**—SSH connections drop after 45 seconds of inactivity.
- **587433**—Sometimes after OS upgrade, the firewall did not start up because of a certain condition in flash writing mechanism.

- **593583**—The device failed while processing SMTP traffic for Antispam.
- **596169**—SSG device running PPPoe core dumps when there was no DNS option defined in PPP control packet.
- **598630**—Event log displays "route is invalid" even though there are no route changes.
- **598836**—ASIC resets when FTP service is configured with a never timeout.
- **599609**—The "in packet" and "in ucast" counter increased, though the physical interface was down.
- **610023**— [SSG300/500]Byte count for log-self shows wrong value.
- **601092**—Device name was missing in the syslog message forwarded from the firewall.
- **601364**—Interface physical link is brought up after reboot even after it is down.
- **601173**—Shared memory corruption caused by CPU enqueuing caused incorrect packets to free buffer queue.
- **602147**— "set arp" command was not supported in Transparent mode.
- **606118**—Internal duplicate policy log entries caused the send mail task on the firewall to loop that subsequently caused high CPU usage.
- **607350**—Unable to retrieve the chassis slot information with snmp walk.
- **610271**—While logging multicast traffic, the policy based traffic log was incorrect.
- **612248**—During high traffic, frequently pressing Crtl+C on console caused wrong output in the event log and subsequently the device failed.
- **613108**—After deleting a policy, the "traffic logs" for that policy was not removed and are not cleared manually.
- **614521**—Policy scheduler cannot cover one minute between 23:59 and 00:00
- **660950**—In NSRP Active or Active environment, PPTP might get disconnected unexpectedly.
- **660958**—[SSG550/SSG320] IPv6 log self shows wrong source and destination port numbers.
- **661003**—[SSG500/SSG300] destination ports are shown different in the self log saved from WEBUI.
- **662392**—Duplicate MAC addresses are returned in reports for the mac-tables of SSG bgroup interfaces.
- **664485**—Policy did not compile exactly, when "negate" was used.
- **666370**—Incorrect destination port was displayed 20480(0x5000) in the event log for the web management connection when the system configuration is saved through web-UI.
- **673295**—The command "set chassis audible-alarm all" was modified on the SSG platform to remove the "battery" option as the SSG platform does not support this option.

- **685029**—For IPv4 traffic with IP Protocol 58, traffic log displayed ICMPv6 in the service field.
- **687205**—"Config datafile" for NSM might not include routes from shared DMZ VR (for vsys) to other vrouters.

### Performance

- **598073**—FPGA performance limitation dropped HTTP packets and caused latency during performance testing.

### Routing

- **577347**—After double NSRP failover, the routes redistributed into OSPF failed.
- **610108**—IPv6 Auto-Discovered route was inactive when IPv6 over PPPoE is connected.

### VoIP

- **662790**—SIP registration packet was larger than the allowed registration packet size for Avaya 9600 series phone.

### VPN

- **584827**—The backup firewall might not get all IPSec SA synchronized from system restart due to large number of VPN connections on NSRP setup.
- **590496**—Firewall does not respond to notification message when phase 2 proposals mismatch in IkeV2.
- **591501**—After reboot, the configuration pertaining to IKEv2 for EAP authentication was not preserved if the definition of the IKEv2 gateway name contained spaces.

### Vsys

- **604785**—While creating VSYS with VR in the same line an incorrect and mandatory VR id number syntax is required as an optional field.

### WebUI

- **614616**—The 6 to 4 tunnel end point IP address from WebUI will be rolled out by clicking Ok button.
- **665076**—The maximum number of DHCP relay agents increased from 3 to 4.

## Addressed Issues from ScreenOS 6.2.0r11

### Administration

- **562438**— In WebUI, the "dialup user group" for IKEv2 is disabled and cannot be configured.
- **582678**— Creating admin user with special characters resulted in creating an invalid user.

### ALG

- **586961**— Application with large MSRPC payload did not work with ALG enabled.

### Authentication

- **580534**— Auth table entries for the Infranet-auth policies was not maintained correctly for the VPN tunnel sessions.
- **587578**— 802.1x authentication is not supported on a bgroup interface.

### IDP

- **560339**— ISG IDP signature did not detect the Telnet attack pattern when configured in the policy.

### Other

- **537064**— Corrected the tunnel policy search logic, after opening a pinhole in the firewall because sometimes the tunnel policy search failed.
- **554007**— The device sometimes failed because of a particular type of packet.
- **554716**— Memory leak was triggered in system memory pool upon SSH login to SSG.
- **555070**— SCTP traffic failed when it was moved to ASIC using the command set envar x-in-ip=yes.
- **561219**— Firewall experienced high CPU while receiving ICMP ECHO request with fixed sequential ID.
- **563425**— Firewall failed sometimes when there was a communication error, such as duplex mismatch with the Infranet Controller.
- **563494**— Syslog messages contained the character 'T' between date and time that caused parsing errors.
- **568377**— ASIC goes into non-responsive state with IPSEC-DSCP marking enabled.
- **572707**— Firewall failed because of malfunction while running SPF in the OSPF task.
- **578196**— Hardware version displayed 0(0) on the WebUI.
- **579899**— In transparent mode, the traffic destined to vlan1 through policy based vpn could not reply back to the same tunnel. Eventually management traffic such as ping did not work.
- **580933**— High task CPU triggered flow CPU utilization alarm.
- **585139**— Sometimes device might reboot unexpectedly when certain TCP-based SIP traffic passes through the firewall.
- **585314**— SCP to the firewall failed from an UNIX machine and displayed the error "unknown file '--ns_sys_config."
- **590147**— Members of aggregate interface set as down were up after reboot.

- **595078**— The system crashed while calculating ike_id_hash when local id is an IP address in ACVPN.
- **596093**— Java Script WebUI display error was corrected in Internet Explorer 9.
- **596585**— If IPv6 is not enabled on incoming interface, the multicast link local packet such as NA was not considered as a to-self packet, and the device forwarded these packets.
- **600426**— Removing an old NHTB entry causes incorrect VPN removal resulting in trace errors or crash dump causing the device to reboot unexpectedly.
- **610123**— ASIC stopped forwarding traffic due to shared memory corruption problem.

### Routing

- **543025**— OSPF summary's are not checked when a new OSPF area joins the backbone area subsequently causing inconsistency in routing table.

### VPN

- **573906**— Firewall uses old xauth-ip for p2sa rekey though the xauth-ip has changed. This resulted in repeatedly requesting the user for Xauth authentication.
- **587809**— Negotiation event log was not generated when IKE phase one was initiated.

## Addressed Issues from ScreenOS 6.2.0r10

### ALG

- **524042**—SIP ALG was unable to handle the RTP data session properly in a DIP/VIP environment.

### Antivirus

- **529357**—Management traffic was dropped by the firewall while the antivirus database was getting updated.

### Authentication

- **448478**—RSA SecureID authentication stopped working after few hours of operation.
- **557646**—WebAuth failed to provide the correct login page to the client for connecting through a VPN tunnel.

### CLI

- **568937**—The tunnel interface description command was not displayed in the **get configuration** output, and the configuration was lost after the firewall was rebooted.
- **574045**—A command was introduced to permit IGMP packets with TTL greater than 1 and to provide compatibility with other interoperability devices.

### DHCP

- **586766**—DHCP TCP/IP settings were not propagated from untrust to trust intermittently.

### DNS

- **580838**—Fragmented DNS packets failed to pass through device if Jumbo frame support was enabled.

### IDP

- **530282**—sme_image caused high task CPU and NSM failed to update ISG-IDP.
- **546621**—IDP AVT timeout parameters caused high task CPU. This problem was seen more in NSRP cluster.

### Management

- **428710**—Deleting the source interface bound to NSM module resulted in trace errors or crash dump causing the device to reboot unexpectedly.
- **548025**—NHRP configuration was not supported in the config data file when managing through NSM.
- **569631**—The admin name and password could not be changed or edited using NSM.

### Other

- **522601**—Firewall failed while processing the packet for Ichat ALG.
- **524318**—The null zone was renamed to an unknown name in the VSYS environment when renaming the vsys.
- **539351**—MS-RPC sessions failed because of a cold start sync failure caused by RPC process.
- **548257**—Traffic stopped passing because of session allocation failure in certain condition.
- **548464**—Sometimes the tcp traffic was delayed by 1 ms, when the tcp traffic passed through the 10G IO card.
- **558859**—Firewall experienced a high memory usage and memory leak in the SSL and certificate modules.
- **558980**—Firewall failed when executing **get route ip** command in a multicast environment.
- **562919**—Firewall failed when the command was executed and redirected to tftp **get igmp group > tftp x.x.x.x get_igmp.log from ethernet2/1.1:1**.
- **564557**—Firewall incorrectly handled the POP3 RSET command.

- **567152**—Firewall stopped passing traffic on the bgroup interface with two interfaces in the bgroup connected to the same switch and when one of the member interface state changed to down.
- **567976**—Firewall failed when collecting the debug data for a split-brain condition because of an ASIC problem.
- **569540**—Incorrect time stamp was displayed in the event log message during the last day of a month of DST, when the DST was enabled.
- **569979**—Firewall failed to download a file from Adobe website when the reassembly-for-alg was enabled in the zone with DI.
- **570868**—The firewall rebooted unexpectedly because of an unexceptional read error in an incorrect packet buffer.
- **570432**—Incorrect log with IPv4 address was generated while editing an IPv6 address book entry.
- **570628**—Debug messages were displayed in the buffer even when no debugs were running on the firewall.
- **570948**—Firewall failed when it received a last fragment packet size of 64 bytes.
- **571584**—NSM reported an error in delta config when the command **set interface bgroup0 dhcp server config updatable src-interface ethernet0/0** was set on the SSG5 device.
- **576128**—Could not obtain security module information with error "sm_get_cmd transmit timeout" because of memory leak on SM.
- **576768**—Firewall rebooted after removing CA and CRL certificate through the WebUI.
- **582278**—Firewall dropped the pass through PIM multicast traffic because of an error in a policy lookup process.
- **584381**—Firewall failed unexpectedly because of an unexceptional error while processing the traffic.

### Routing

- **564997**—Firewall sent invalid triggered-RIP updates on the interface which was not configured to send the update.

### VPN

- **550440**—With IKEv2, NetScreen firewall responded to the **create_child_sa** message from peer successfully but showed VPN status as inactive.
- **579094**—IKEv2 with AES encryption in proposal failed because of incorrect attributes.
- **581469**—When running IKEv2, clients located behind some NAT devices were disconnected.

### WebUI

- **519824**—The device failed when a reject message was configured for integrated surf control using WebUI containing more than 500 double byte characters.
- **552566**—With HTTP redirect enabled, the device failed to redirect to HTTPs while accessing IPv6 address using WebUI.
- **567094**—Sometimes the firewall policy with multiple address/service objects change to a single object, if the "too many counting policies" error was encountered when the policy was configured using WebUI.
- **573637**—WebUI did not display all the list of interfaces when there was a long list of interfaces with subinterfaces.

## Addressed Issues from ScreenOS 6.2.0r9

### Authentication

- **536931**—Cross-vsys authentication did not bind to the correct session in both vsys which resulted in a session that was created in the ingress vsys but not in the egress vsys. This resulted in denial of traffic.

### AV

- **548601**—Sometimes the ASP did not send back ACK packets until all the out-of-seq TCP packets were received in sequence.
- **559335**—File download stopped intermittently when AV was enabled because of an error in the TCP proxy connection.

### CLI

- **541186**—The set log exclude-id command did not work for some of the event-types.
- **559694**—When concurrent session was large, there was intermittent high task CPU for a second, when an interface was added or removed.

### DI

- **538459**—Memory leak in sys memory pool occurred when generating an alarm for some of the signatures.

### GPRS

- **544157**—GTP events produced multiple log entries.

### HA & NSRP

- **524021**—NSRP backup session installation error occurred because of route look up failure that caused packet drop after failover.

- **538250**—Communication through the master node sometimes failed when exchanging the backup device through NSM performing the RMA procedure.

### IDP

- **536048**—Repeated pushing of AppSig Db to security modules from NSM in the absence of IDP policy caused memory leak on the security modules leading to update failures on NSM.

### Management

- **544149**—[SSG350]Status of I/O fan 2 was reported incorrect through SNMP on SSG350.
- **551538**—Sometimes, the **set envar config=flash** command did not load the existing configuration file upon reboot.
- **552547**—When there were primary and secondary NSM servers configured with source interface, the device did not try to connect to the primary, and tried connecting only to the secondary NSM server.

### NAT

- **533403**—While translating from IPv6 to IPv4, NAT-PT process on the firewall was adding additional fragment header without doing fragmentation, which caused the packets to drop.

### NSRP

- **524381**—Firewall in the active/active cluster displayed the message "backup session cannot find its related auth table" in the debug buffer with no debugs enabled.

### Other

- **453396**—Under certain conditions the L2TP packets timed out, and the tunnel was not deactivated and removed properly, which caused new packets to use an existing tunnel and was black holed.
- **499157**—High-end platforms reported high task CPU utilization if there were huge number of phase 2 SAs configured.
- **504136**—The firewall sometimes resets when SIP packets with invalid header were received.
- **511497**—Traffic was stuck because packet was sent with wrong vlan tag in PIM chip.
- **524232**—RTSP ALG erroneously treated two different packets as a pair of translated packet and then dropped the packet.
- **527319**—[SSG20]No link was present for Copper SFP running JXM-1SFP-S module.
- **527721**—ASIC stopped passing traffic under certain condition due to a problem with the PDMA.

- **535584**—Firewall was not able to learn the new MAC address in the IPV6 environment when the upstream device NIC card or MAC address was changed.
- **540038**—Sometimes, in NSRP active/active mode, asymmetric traffic was dropped.
- **540193**—Firewall failed when the tunnel session was considered as a normal session during packet processing.
- **541647**—The error message "FTP, FTP-Get and FTP-Put should not be put in the same group" was displayed when adding FTP service to a multi-cell policy.
- **542028**—When the firewall failed, coredump information was not saved in the buffer for an unknown reason.
- **547040**—ASIC dropped multicast packet when the last hop PIM router with SPT disabled packet was received.
- **547117**—Packets were dropped by anti-spoofing screening option on the backup NSRP firewall.
- **547750**—[IPv6] UDP checksum was zero.
- **547943**—[NS5000] The increasing CPU4 drop counters affected the MGT3 platform only.
- **548054**—ISG and NS5000 platforms dropped pass-through ESP fragmented packets with total size around 1700 bytes.
- **548294**—When the **set flow reverse-route clear always** command was configured, the packet did not get arp resolved and was queued twice.
- **549614**—Firewall failed when details for a peer gateway in a manual VPN configuration were accessed.
- **549816**—Under certain circumstances, the firewall core dumped and rebooted unexpectedly.
- **552417**—Incorrect calculation of string length caused the device to reboot unexpectedly.
- **555254**—Implemented the support for UDP based fragment on data session when the session was a part of the ALG such as SIP protocol.
- **559330**—NSRP backup device failed and rebooted unexpectedly when accessing an invalid pointer in the flow.

### Routing

- **409691**—OSPF did not form adjacency on vpn tunnel interface over dialer interface.
- **441711**—RIPv2 failed to advertise routes to the neighbors after few hours of operation in a hub-and-spoke VPN setup.
- **535615**—OSPF neighbor on the VPN tunnel went down when the OSPF neighbor session was incorrectly formed on the loopback interface rather than the tunnel interface.
- **543671**—BGP peering failed when force-reconnect option was enabled under certain configuration conditions.

- **544754**—Inter-area route was not removed from routing table even though an intra-area route was learnt and existed in the OSPF database.
- **547702**—Asterisk(*) for active route disappeared for host route in NSRP backup.

#### Security

- **540983**—SYN packet sent to the server by the firewall after triggering the SYN-proxy had an incorrect checksum.

#### VoIP

- **530047**—SIP ALG was unable to handle the SIP calls that needed cross vsys policy search.
- **539819**—An H.323 IP phone registration failed because a packet that matched a session on the ASIC was forwarded to an incorrect session queue.

#### VPN

- **533635**—Route-based VPN failover did not work because of an error in the route look up process.
- **537411**—Firewall rebooted unexpectedly when service in the policy for AutoKey IKE VPN was added, when single Phase 1 and multiple Phase 2 VPNs existed.
- **548117**—In IKEv2, firewall did not send the IDi and IDr messages with payload information to the peer when the Phase 2 VPN failed with a proposal mismatch.

### Addressed Issues from ScreenOS 6.2.0r8

#### Administration

- **511835**—Sometimes, the configuration got deleted while configuring the administration setting for custom L2-zone.
- **526215**—"Policy:Not Found" error was displayed when the user tried to add a new policy with "before id" and "DSCP enable value" keywords together.
- **536897**—Under certain circumstances, the message **command rejected due to writing config conflict** was printed on the telnet, ssh or console of the device.

#### Antivirus

- **523759**—The firewall rebooted unexpectedly with **Exception Dump** message when AV was enabled on the policy.
- **535728**—While scanning the FTP session, the APP session was aborted because the device ran out of packets with code 0 resulting in low memory. Delete unused license to free memory space.

### Authentication

- **528252**—The firewall sent multiple WebAuth requests to the user when a single HTTP request was split into multiple packets.

### DI

- **528641**—Under certain conditions, after DI attack signature update, the configured "action" in attack policies became incorrect.

### HA & NSRP

- **509803**—Software sessions on backup firewall did not ageout properly because of its inability to synchronize time with its master unit.
- **529696**—Under certain circumstances, with the HA link probe configured, the device sometimes rebooted unexpectedly when the status of the HA link changed.

### Management

- **522075**—TCP sweep and UDP sweep screen options could not be configured using NSM because these options were missing in the ScreenOS config datafile.
- **526797**—When DNS response was fragmented, the reason for session close in the traffic log became age-out.

### NAT

- **532937**—The firewall incorrectly allowed the user to configure an IPv6 MIP and a DIP with the same address.

### Other

- **478573**—[SSG300]The device sent corrupted IP packets on reboot.
- **500993**—Issue with RSH when the application reused source port while closing control connection. The data traffic still existed.
- **503307**—Application-Specific Integrated Circuit (ASIC) hung and stopped passing traffic due to incorrect session pointer.
- **504566**—The device sometimes rebooted unexpectedly if a tunnel session was treated as a normal session.
- **513394**—A problem with the generation of counter statistics caused the firewall to reboot unexpectedly.
- **519557**—Firewall sometimes dropped packets in transparent mode if syn-flood was enabled.
- **526243**—The device rebooted unexpectedly due to CPU deadlock.
- **529690**—ESP pass-through traffic did not consider custom service timeout when the custom ESP service was part of a service group.

- **529736**—The policy scheduling options "Recurring" and "Once" did not work together.
- **533822**—When using SQL redirect, the ALG did not open the pinhole correctly.
- **536064**—The device rebooted unexpectedly when the hash table index got corrupted during cache aging-out phase.
- **536700**—Under certain circumstances, syn-flood generated false alarm because the IP protocol was interpreted incorrectly.
- **537316**—The device rebooted unexpectedly during DNS refresh.
- **538766**—The device rebooted unexpectedly due to IPv6 address double free issue.

### Routing

- **533910**—RIP updates with more than 825 routes were dropped.

### VPN

- **508798**—Firewall utilized very high memory when VPN was configured.

### WebUI

- **535613**—In the WebUI, editing a VIP using a service name with an ampersand (&) resulted in "400 Bad Request" error.
- **536474**—Replacing the NSRP configuration using the WebUI including certain specific CLI sometimes caused unexpected behavior after reset.

## Addressed Issues from ScreenOS 6.2.0r7

### Administration

- **467398**—Local root user sometimes lost root privilege when the remote admin used the same user name.
- **504196**—SSH management sometimes disconnected abruptly when large output commands were executed.
- **509654**—[SSG 140] TX/RX LED remained ON even after set interface ethernet0/X phy link-down command was executed.

### Authentication

- **499421**—With edipi enabled, XAUTH user could not inherit the IP information from old XAUTH session when new SA leading to memory leak was rekeyed.
- **511019**—802.1X authentication failed after PC hibernation.

### CLI

- **484141**—The system rebooted unexpectedly when the **get sip transactions** command was executed.

- **510473**—Typo in **infranet enforcer mode test** command resulted in syntax error after reboot.
- **517043**—The output displayed the null interface with zero MAC address.

### DHCP

- **510653**—Unable to configure DHCP option string with a length greater than 128 bytes.

### HA & NSRP

- **515159**—The backup device used virtual MAC for ip tracking in a PPPoE environment using interface redundancy.
- **519838**—Both firewalls in NSRP cluster sometimes became master.

### IDP

- **507318**—IDP Engine failed on security module and created core file.
- **513071**—With application identification enabled, invalid pointers to destructed flows had created an issue. This problem has been resolved.
- **522728**—Under certain conditions, the traffic dropped because the inline-tap mode was changed to inline mode.

### Management

- **471425**—The event log displayed interface flapping messages within the same second on the firewall, but the other end of the connection did not record interface flapping messages within the same second on the firewall.
- **488614**—The **set zone <zone name> tcp-rst** command did not work on ISG and NS5000 platforms.
- **494629**—SNMP trap was not sent to indicate that the CPU utilization had returned to normal level.
- **501026**—The **exec policy verify** command did not work for the group service.
- **501343**—Even though there was no incoming traffic, alarm traffic for policy increased, because the self traffic was denied by the deny policy.
- **502845**—The firewall rebooted unexpectedly when the L2TP policy was removed through NSM.
- **503139**—Under certain conditions, during an SNMP walk, the firewall sometimes rebooted unexpectedly.
- **503323**—After deleting a VSYS, the system log erroneously displayed error messages related to deleting a tunnel zone, and SSH PKI key associated with that VSYS.
- **505106**—Under certain conditions, the policies were marked as "invalid" because of NSM policy push operation.
- **505456**—Event log displayed "system temperature severely high" message even when the temperature of the device was appropriate and the hardware was in good condition.

- **505554**—Traffic log for large PING over MTU size was displayed as close-ageout instead of close-resp.
- **520991**—After reboot, the **unset http skipmime mime-list** command was added to the configuration.
- **522349**—Signatures with 30 or more characters were truncated when passed through the syslog output.

### NAT

- **512224**—MIP translation between IPv6 addresses failed to translate.

### Other

- **419637**—Many drop notification messages between IC and IE caused instability in the SSH connections.
- **494617**—ScreenOS devices managed by NSM version 2009 or above sometimes encountered memory leak issue.
- **495554**—Firewall rebooted unexpectedly when the policies were changed and read at the same time.
- **498562**—IPv6 did not work on PPPoE ADSL interface.
- **498869**—Fragmented MSRPC packets were not supported in the ALG.
- **506282**—Whitelist URL was blocked by URL filtering because the code did not identify the port number (non 80) in the hostname header.
- **506473**—Radius server was not reachable when the source interface was not the Virtual Security Interface (VSI).
- **506543**—Parsing a folder with the name "quit" abruptly closed the FTP session.
- **508319**—The device sometimes rebooted unexpectedly when the memory got overwritten by the EAP task.
- **509166**—SSG5 wireless device was not able to locate the best channel under certain conditions.
- **512752**—In certain conditions, failure of the infranet controller connection caused high CPU condition on the device.
- **515064**—In certain conditions, it was possible to define a custom service object for protocol 0.

### Routing

- **501996**—In case of multiple virtual routers (VRs), sometimes, deleting a multicast route from one VR did not update information in the other VR caused the device to reboot unexpectedly.
- **511812**—When a BGP neighbor was configured and an outgoing route map was applied, the firewall did not apply the local preference correctly as specified in the policy terms.

- **528011**—In specific circumstances, BGP did not send updates on routes that were unreachable.
- **505962**—The RIP packets were constructed twice with the same RTE, but with different metrics.

### Security

- **511026**—Implementation of IKEv2 DoS attack prevention was incorrect.

### VoIP

- **511469**—Limitation on the maximum h245 channel number was 10. This limitation caused problem with certain VoIP applications.
- **517439**—URI of SIP message was modified incorrectly when NAT with SIP ALG was used.
- **529845**—With SIP ALG enabled, the firewall sometimes experienced high CPU.

### VPN

- **500203**—ASIC based firewall sometimes stopped passing traffic when ESP packets with invalid SA value were received.
- **508886**—Netscreen Remote Client for dial up VPN did not failover to redundant gateway when track-ip failed.

### WebUI

- **507172**—Sometimes, the firewall rebooted unexpectedly when WebUI was accessed.
- **513085**—In the WebUI, under certain conditions, MIP configuration for IPv6 address was not available.
- **515172**—Alarm events for DI detection were missing in an exported report from the WebUI.

## Addressed Issues from ScreenOS 6.2.0r6

### Administration

- **417686**—Socket leak might occur when Internet Explorer (IE) with HTTPS was used for WebAuth management.
- **480480**—Under certain conditions, memory leak in the event log module caused high memory utilization.
- **493627**—Under certain conditions, device might reboot unexpectedly when RPC (MS-RPC or SUN-RPC) traffic passed through the device and **show rpc map** command was executed.

- **496029**—While managing the firewall using SSH Secure Shell v.3.2.9, firewall reported "Potential replay attack detected on SSH connection initiated from x.x.x.x."
- **501075**—The VeriSign CA certificate had expired and was invalid. It could be removed from the system as the system already contained a valid VeriSign CA certificate. The valid certificate could be seen with **get pki x list cert** command.

### ALG

- **498113**—In certain conditions, with RTSP ALG enabled, the RTSP traffic fails through the firewall.

### Antivirus

- **498121**—In certain scenarios, with AV enabled, the HTTP slows down due to TCP retransmission.

### Authentication

- **503196**—The source interface option for authentication (auth) did not work when LDAP was configured as the AUTH server.

### DHCP

- **484087**—The destination IP was incorrectly set to 0.0.0.0 when DHCP relay agent received a DHCP ACK in response to a DHCP INFORM.
- **495244**—DHCP custom option 43 was sent with an invalid length.

### GPRS

- **485578**—The GTP remove-r6 feature removed the mandatory RAI IE from SGSN Context Request and Identification Request messages.
- **485911**—Support had been added for removing Information Element '184 - Bearer Control Mode' using the GTP remove-R6 feature.
- **486613**—When GTP traffic dropped, the bad system status message appeared in the log.

### HA & NSRP

- **472083**—When NSRP track-ip monitoring was configured within vsys, configdata file had incorrect track-ip information.
- **504713**—NSRP config was out of sync due to **set tftp source-interface <interface name>** command.

### IDP

- **485928**—[ISG-IDP] The IDP engine resets due to application identification.
- **493618**—[ISG-IDP] The IDP engine core dumped frequently due to DFA cache memory corruption.

### Management

- **455186**—Firewall running OSPF rebooted unexpectedly after a delta configuration through NSM was performed.
- **470754**—[NetScreen-5000] The redundant interface reported overflow errors when it was not initialized correctly after a system restart.
- **485725**—Firewall socket issue caused higher task CPU than expected which caused the management through web and SSL to fail.
- **485946, 470729**—Event log message displayed <username> turn off debug switch for all when admin exited the CLI.
- **491026**—SNMP walk for certain MIBs did not return any value.
- **491132**—ICMP packets to the management interface experienced delay at regular intervals.

### NAT

- **480667**—The firewall allocated vsys limit for configuring MIPs to a shared interface in root-vsys instead of global limit.

### Other

- **456690**—The traffic log did not display IPv6 addresses correctly.
- **463515**—MAC entries in the bgroup mac-table were not cleared after an interface went down.
- **472690**—ICMP flood screening option incorrectly dropped packet and generated alarm even when the packet rate was lower than the configured threshold.
- **479300**—In some scenarios, non-impacting messages such as "TR installing ready reverse wing" were logged to the debug buffer.
- **479752**—Under certain conditions, the device might reboot unexpectedly when running **get config datafile** command.
- **480179**—When the SC-CPA server was inaccessible, the device displayed **UF-MGR: Internal error: Failed to allocate uf_record event**.
- **481805**—The bandwidth settings configured on the gigabit subinterfaces were not loaded after reboot.
- **484133**—With unknown protocol protection disabled, the traffic with protocol number greater than 137 was dropped erroneously.
- **484839**—In some scenarios, firewall might reboot unexpectedly if **get alg pptp xlate** command was executed.
- **485192**—GRE packets of PPTP session might be dropped if PPTP server CALLID was set to 0.
- **485332**—The PIM register message was dropped when the inner packets were fragments.

- **486445**—The device might reboot unexpectedly due to its access to a NULL pointer.
- **486896**—Event log timestamp was changed because of the NTP update.
- **489167**—The session was torn down while changing multi-cell policy if RPC was one of the service cell.
- **489205**—In IPv6, the MTU was not changed according to an ICMP6 "Packet Too Big" error message.
- **490158**—[Netscreen-5000] In some scenarios, the firewall stopped forwarding traffic and was also not accessible through in-band access.
- **490176**—An upgrade for SSG140 running a dual boot image using SCP (secure copy) required the device to reboot twice.
- **491466**—The SQL connections might fail when SQL ALG was enabled.
- **491531**—TCP session might be broken when failover occurs from one tunnel to the other due to wrong TCP Window Scaling Factor in hardware session.
- **491555, 492544**—In certain situations, TCP-based SIP traffic in the environment could cause the firewall to reboot unexpectedly.
- **494276**—A URL blocked by Websense might not display the corresponding blocked message in the browser in an asymmetric routing environment.
- **494946**—[SSG300] The alarm LED did not turn red when large ICMP packets were detected.
- **498529**—Executing the SNMP get query for BGP related OID might provide an incorrect output.
- **500495**—With antispam enabled, e-mail with attachments greater than 3 to 4 MB might drop due to out of memory error.
- **500843**—Output of SNMP walk might display wrong interface for ARP table entries.
- **501256**—While saving traffic logs using WebUI, the Translated Dest column was empty.
- **502419**—Traffic shaping statistics were not displayed on the NSRP VSI interfaces on the firewall.
- **504084**—The track IP might fail when interface was inactive.

### Performance

- **478205**—When large amount of WebAuth transaction takes place at a time, some HTTP SYN packets might drop during TCP 3-way handshake without returning SYN and ACK packets.
- **494910**—[SSG140] In certain circumstances when there is heavy traffic through the interface, all the traffic passing through the interface e0/9 is blocked.

### Routing

- **468697**—Under certain circumstances, with BGP enabled, the firewall rebooted unexpectedly.
- **473625**—Under certain conditions, multicast traffic did not match the longest matching multicast group policy.
- **480470**—BGP anti-flap processing was removed from the backup NSRP node.
- **482372**—In some scenarios, IBGP did not send updates to some of the BGP peers.
- **483854**—OSPF neighbor relationship was lost on active primary connection when the backup link flapped.
- **485608**—Firewall failure dump was caused by the BGP route updates.
- **490020**—In specific circumstances OSPF converged incorrectly.
- **504708**—With NSRP sync route enabled, the redistribution of routes from BGP to OSPF was delayed.

### Security

- **519131**—CVE-2010-0740 "Record of Death" vulnerability in OpenSSL was addressed.

### VoIP

- **484227**—SIP MIME and Multipart messages were modified on the firewall that caused the SIP packets to drop.

### VPN

- **441805**—The ikmpd task caused periodic high task CPU peaks.
- **475831**—Quotation marks (" ") were removed from configuration when the **set vpn vpn_name bind zone "zone_name"** command was used.
- **480642**—User could not pair a VPN policy when multiple MIPs were used as destination.
- **480691**—The VPN tunnel down message (for example,VPN <vpn-name> from <IP-address> is down) was not generated in the event log when the NSRP backup device became the master.
- **482399**—AC-VPN failed to connect from one Spoke to another Spoke VPN site in the NAT-T scenario.
- **485001, 505065**—The VPN policy with domain name did not update the right proxy-id after reboot.
- **486043**—Firewall might reboot unexpectedly when IKE/CLI and flow module accessed the NHTB table at the same time.
- **492884**—Tunnel interface might remain in down state after NSRP failback, as a result the traffic stops flowing through the VPN tunnel.

- **494667**—Incorrect proxy-id with VPN Policy having MIP and overlapping source and destination address.
- **502729**—VPN failed to come up when the outgoing interface was a loopback interface.
- **504014**—In some scenarios, VPN policy with MIP failed to translate Proxy ID.

### WebUI

- **291948**—When the device had many event log entries, refreshing the main WebUI page or the report page using Report > System Log > Event action caused high CPU utilization.
- **450974**—Enabling or disabling the Java or ActiveX component also unsets IP Spoofing.
- **479440**—"unknown keyword ipv6" error was displayed when using VPN wizard for vpn setup with IPv6 disabled on the firewall.
- **493414**—In the WebUI, when the user clicked **Go** or **New** button to open a policies menu, the device rebooted unexpectedly.
- **495940**—WebUI incorrectly displayed the tunnel interface status as inactive.
- **496267**—The tunnel interface erroneously appeared inactive in the WebUI and ready in the CLI when the VPN monitor was disabled.
- **496418**—WebUI configured as a web bookmark did not open in a new window on a SA Series page.
- **502098**—At times, the device might reboot unexpectedly when changing the vpn name.

## Addressed Issues from ScreenOS 6.2.0r5

### Administration

- **472816**—Sometimes the **clear socket <socket id>** command could not clear the tcp socket when it was in a certain state.
- **481730**—The **get system** command displayed the hardware version as 0000(0)-(00) on SSG300 and SSG500 devices.

### Antivirus

- **478469**—In transparent mode, VLAN tag was removed from the HTTP traffic after AV scanning.

### Authentication

- **471517**—Protocol version check caused the RSA SecureID authentication failure.

### CLI

- **462860**—[SSG 140/300/500, ISG 1000/2000, NetScreen 5GT] After reboot, the **unset admin hw-reset** command was not saved.

### DNS

- **471892**—DNS queries did not work when device was configured to use itself as DNS server when DNS proxy was enabled on an interface.

### GPRS

- **448582**—GTP inspection dropped the SGSN Context Response message if the Next Extension Header type was 0xC2 (Suspend Response).
- **449284**—In certain conditions, the firewall failed to allocate GSN, causing the GTP traffic to drop.
- **456358**—The Common Flags GTP Information Element was not removed when **set remove-r6** command was configured.
- **457093**—For a new GTP tunnel, CreatePdpRequests from an SGSN were dropped if the response was not received before a certain time period.
- **472199**—When R6 IE removal was enabled, GTP CreatePdpRequest packets got corrupted if they contained both the MS-Time zone information element and a private extension.

### HA and NSRP

- **414183**—In certain situations, NTP synchronization in an NSRP cluster caused firewall to send the 'device change' flag to NSM.
- **420260**—The configuration checksum was inconsistent in the NSRP backup device after reboot.
- **449858**—Non-VSI PPTP session was not functioning as expected in the NSRP Active/Passive scenario.
- **461079**—[NetScreen 5000] The backup firewall would prematurely remove the sessions on the master in a VSD-less NSRP cluster and cross-ASIC traffics.

### IDP

- **467521**—In certain conditions, processing of RPC packets caused memory allocation problem which eventually caused the security module to hang.

### Management

- **408853**—SNMP requests for ip.ipNetToMediaTable information caused high task CPU.
- **433084**—After modifying the multi-cell IPv6 policy, the policy might not be completely functional.
- **459999**—The **set flow vpn-tcp-mss** command was not available for configuring in NSM.
- **466692**—The SNMP IPv6 IfIndex value was reported as incorrect from the firewall.
- **468659**—E-mail notifications for logs from the firewall were not formatted correctly.

### NAT

- **450989**—Unable to access MIP configured on loopback group from different zones on the firewall.

### Other

- **302382**—In certain conditions, the firewall might reset if a session incorrectly references a MAC address without route information.
- **387173**—Traffic was blocked intermittently because of an error in handling non-IDP traffic as IDP sessions.
- **448252**—[SSG 300] In transparent mode, packet going across the firewall was dropped because of the NMAP scan.
- **449723**—Firewall might reboot because of incorrect scheduling of SPF algorithm for the OSPF protocol.
- **452080**—The TCP 3-way handshake failed because of an error in the setup of IPsec VPN.
- **455183**—[NS–5000-M2/M3, ISG] Few packets might be dropped due to ASIC reinit.
- **459357**—In certain conditions, duplicated URL's were displayed on the redirection page when WebAuth feature was used on the firewall.
- **460233**—With DST enabled, the e-mail notification time from ScreenOS was an hour ahead of the actual time.
- **461492**—[ISG, NS-5000] When SQL IPMP NIC failover on the SQL servers was performed, subsequent traffic did not pass through the firewall.
- **462783**—Under certain conditions, sessions with timeout value of 0 or 1 were never aged out of the firewall.

- **463422**—TCP SYN-ACK packets did not pass through the firewall in transparent mode if there was no matching MAC table entry.
- **465718**—Under certain conditions, the device might reset when a Dial-Up user tried to connect.
- **466619**—The **set lic auto-update** command rolled back to unset after a device reboot.
- **468514**—Traffic log was not generated for a source or destination port equal to 1503.
- **468821**—Double quotation mark (" ") was not accepted in the middle of a comment or description for the definition of an address, route or group policy objects.
- **471298**—UDP MSRPC EnDPort mapper (MS-RPC-EPM) traffic incorrectly displayed its traffic log as MSRPC ENDPOINT MAPPER (TCP).
- **472178**—The **set zone trust screen udp-sweep threshold** command enabled the tcp-sweep option.
- **472433**—Packet might be corrupted due to ASIC buffer problem.
- **473325**—In certain conditions, backup device in NSRP cluster did not free RTSP objects and hence caused memory leak.
- **476618**—Due to memory constraints on NS-5GT, all UTM features were supposed to be disabled on ScreenOS 6.2 by design. However the Antispam and Web Filtering features were enabled. These feature will be disabled on ScreenOS 6.2.0r5.
- **477561**—The guaranteed bandwidth parameter was incorrectly allocated in traffic shaping.
- **481096**—Enabling the set log audit-loss-mitigation feature caused the device to halt the traffic after the log buffer was filled.
- **494468**—Data session of the protocol handled by ALG could be cleared if multi-cell policy was changed.

### Performance

- **491967**—Policy search was slow with complex and larger number of policy configurations causing high CPU.

### Routing

- **433987**—Memory leak because of large OSPF LSA might reset the device.
- **435956**—Firewall removed some RP-set when it received BSR messages with a tag zero.
- **436444**—Device might reset if IGMPv3 source specific report was sent.
- **448691**—BGP routes got stuck in route table when two neighbors sent the same prefix route and the routes changed frequently.
- **459513**—IPv6 static route to null interface could not be configured on the firewall.

- **466158**—Capability negotiation error between BGP peers caused BGP to stay in idle state.
- **474158**—Change in RPF source route or change in route towards the RP was not reflected properly to the multicast routing table.

#### VoIP

- **442077**—H.323 calls failed when it exceeded 10 OLC channels.

#### VPN

- **455520**—Tunnel interface was not created when route based VPN configuration was pushed from the NSM.
- **459053**—A logically down interface might respond to VPN monitor packets sent by a VPN peer device causing the VPN state to stay up.
- **460281**—ACVPN configuration could not be completed after the dialup VPN was set.
- **472618**—NS-Remote IPsec phase one negotiation would fail if IKE ID was changed.
- **479107**—The VPN proposals ordered through WebUI of the firewall was ambiguous and could lead to unintended selection of the proposal between the VPN peers.
- **486608**—The **set vpn <vpn> dscp-mark <dscp>** command for manual VPN failed to set the DSCP marking for outgoing ESP packets.

#### WebUI

- **463137**—IRDP could not be enabled on interface e0/0 using the WebUI.
- **465697**—In certain conditions, the WebUI management caused the system to reset because of incorrect parameter value.
- **468211**—In the WebUI, the IPv6 route entry did not accept uppercase characters for an IPv6 address.
- **469439**—VPN monitor configuration might rollback to default after editing the vpn entry from the WebUI.
- **474665**—In vsys, for ike gateway configuration, option to select shared root interface was not available in the outgoing interface drop box in the WebUI.

### Addressed Issues from ScreenOS 6.2.0r4

#### Administration

- **405317**—The device erroneously reports that the user was in use by L2TP and prevents editing of the user.
- **412352**—Net-buffer leak caused multiple SSH tasks to compete for the same resource and series of dots appeared on the console.
- **439172**—VSYS configuration gets lost when the VR is created by shared-dmz zone.

- **445431**—After a reboot, local configuration setting such as manage-ip or hostname were lost.
- **445491**—When displaying BGP route advertised without specifying a neighbor address, the error **bgp neighbor 0.0.0.0 doesn't exist** is displayed.
- **456056**—A warning message was displayed when the service with more than 16 dst ports was specified.
- **456101**—[ISG, NetScreen-5000] The **port mirror** command displayed erroneous **Failed command - set mirror port source ethernet4/1 destination ethernet1/1** message on console bootup, even though the command existed in the configuration file and was working.

### Antivirus

- **436526**—Under certain conditions, FTP PASV communication failed in control session when UTM was enabled.
- **440546**—The SMTP sessions were held up during the antivirus scanning process, if the client was using SMTP DSN (Delivery Status Notification) and the recipient's e-mail address contained the word "QUIT".
- **444440**—The firewall might reset if antivirus scanning was turned on for the latest version of AIM service.
- **448649**—Firewall resets if antivirus or antispam is enabled for SMTP traffic.
- **458125**—The VLAN tag information is lost on preparing a child session in ALG traffic when the UTM is enabled.

### Authentication

- **416043**—The device did not clear the existing System Information Block (SIB) when the associated radio caused the wireless authentication to fail.
- **429374**—Reauthentication for dot1x was not handled as expected.
- **455865**—After a reboot of the firewall, 802.1x authentication fails.

### CLI

- **435979**—[SSG 500] Output of the **get chassis** command does not include PIM name.
- **447541**—[NetScreen-5000 M3] The **clear session frag** command was not working as expected.

### DI

- **410393**—When updating offline from the Local Server, the automatic DI signature update fails.
- **429953** —DI updates might cause net-pak memory leak.
- **439093**—Unable to update attack db for worm sigpack.

- **449213**—[ISG 1000/2000] Unable to pass the traffic through back-to-back VPN using VSI interface after IDP was enabled.
- **454303**—When a DI policy is enabled, and ip-action is "notify", the packet will get dropped if it matches the DI group specified in the policy.

### DNS

- **436514**—No sanity check for time-to-live on DNS host caused abnormal condition.
- **439044**—If syslog server was referenced using the DNS hostname, syslog server messages were still sent to the original IP address even when the IP address of the hostname was changed.
- **444576**—DNS proxy was case sensitive for Domain Names.
- **458316** —A device might reset if a vsys that contains address book objects with DNS names is deleted.

### GPRS

- **437975**—When GTP inspection was enabled, occasionally a GTP Echo Response might drop and the message **bad state (message)** was showed in the log.
- **438896**—With GTP inspection enabled, a CreatePdpResponse that contains a duplicate TEID for the control or data plane was dropped.

### HA and NSRP

- **436123**—On VSD-less L3 mode, after adding CLI **unset nsrp link-up-on-backup**, the logical link state of physical interface was erroneously changed to down state.
- **437283**—The NSRP route synchronization fails if the next hop of the master device was a virtual router.
- **437661**—The RIP and OSPF MD5 authentication results in NSRP configuration were not in synchronization.
- **438794**—Backup NSRP firewall lost synchronized OSPF routes.
- **447031**—Backup device in NSRP cluster received corrupted HA packet and that caused some bits to be processed incorrectly, and the device to reset.
- **447577**—When in NSRP cluster, if manage-ip of loopback interface is modified, the loopback interface link state goes down.
- **448011**—Under certain conditions, WSF is not being updated in hardware session.
- **449011**—[SSG 140/300/500] When Active/Passive NSRP in L2 mode is configured, some traffic might stop for a few minutes just after failover under a specific condition.
- **450083**—In certain situations, with IPv6 enabled, NSRP data forwarding of IPv4 would have failed.

- **451779**—MGT IP and hostname info is lost on device with VSYS configured, after NSRP config sync is performed.
- **454981**—[SSG 300M] When the NSRP failover occurs, the red alarm LED is triggered.

### IDP

- **431797**—Packets were dropped when the **TCP Error Reassembler Packet Memory Exhausted** signature was enabled.

### Management

- **401157**—Unable to log on to the master device when NSRP failover occurs with the IC configured.
- **408237**—Policy push using ntp-server failed because of incorrect syntax in get config data file for setting ntp-server in ScreenOS.
- **439271**—Task CPU was high if the ping was initiated from the firewall, and the destination was unreachable.
- **439970**—Firewall reported incorrect H.323 port information in NSM protocol distribution.
- **440766**—NSM agent caused negative session count in NSM.
- **443213**—In some scenarios, TFTP control block would be freed in other task that caused crash or stimer list broken.
- **447726**—Parser error message **StreamSetListParser** was displayed on NSM while updating the device.
- **448761**—Unable to set password complexity scheme using NSM.

### NAT

- **289915**—The reserved dip ID was checked incorrectly when a policy was configured with wildcard or group in NSM.
- **442461**—Service mapping for Sun or MS RPC showed incorrect IP mapping when dst-nat was used.
- **443304**—[NetScreen-5000, ISG series] P2P and ichat ALGs were incorrectly enabled on reboot and therefore MSN, Yahoo Messenger and AIM traffic were not processed by ASIC in hardware sessions. This situation could cause high CPU utilization if the traffic load for these services was high.
- **455943**—When the PPTP service and GRE service timeout are configured to never, the PPTP xlate fills up unless the PPTP connection is shutdown.

### Other

- **224935**—[SSG-20] Wireless radio was using incorrect frequency range.
- **403895**—[ISG 2000] There was no ALG to handle REXEC traffic.
- **430210**—The device unexpectedly rebooted when an SQL server with TCP fragments was accessed.

- **432190**—[NetScreen-5000 M3] VLAN retag does not work properly with 10 Gig interfaces.
- **432666**—The device reboots unexpectedly due to improper handling of RTSP ALG.
- **433329**—Websense failed due to incorrect session flag for URL_BLOCK and the debug message **Unknow message type: 8e** appeared in debug flow basic.
- **435161**—The **get led** command showed wrong LED power status.
- **435348**—[SSG 5/20, SSG 140, SSG 500] Firewall would reset due to an exception dump before the bootup process.
- **436622**—[SSG 140] The alarm LED did not turn red when large ICMP was detected.
- **437101**—Unable to renew certificate using SCEP with samekey option.
- **437660**—Firewall reset due to an invalid pointer in the MGCP module.
- **438488**—The firewall would reboot during the certificate validation process if the certificate was used for IPsec peer authentication and PKI source interface was not defined.
- **439211**—The pause frames sent from a switch on 4 port FE PIM card would erroneously be detected as "in misc".
- **440103**—The device reboots when an IP-Classification of an unused zone was deleted.
- **440113**—IPv6 Neighbor solicitation messages from source "::" were dropped by IP Spoofing.
- **441723**—The firewall did not send TCP RST for the traffic that matched IPv6 REJECT policies.
- **442251**—The device reboots due to keepalive sent between firewall and Infranet Controller.
- **445511**—The device was unstable and a net-pak leak occurred when an internal flag was changed abnormally.
- **446420**—Microsoft WMI control service failed in some scenario.
- **447395**—MS-RPC ALG mapping sometimes skipped an entry.
- **447799**—The NSM device update would reboot the firewall when DHCP option 78 was configured on the firewall.
- **448711**—The device reboots as the antivirus task exits when an invalid address was accessed.
- **450141**—[SSG 500] The FCB timeout can be set from 1 to 300 seconds using the **set fragage** command.
- **450681**—System instability would result in ScreenOS if the DHCP client on the firewall interface value was Null.
- **450819**—[ISG] Interface did not get updated with new MTU value when Jumbo frame was enabled.

- **451051**—[ISG] Internal memory corruption causes ISG devices to stop creating new sessions, thus impacting traffic.
- **455373**—The device might reset when some SQL ALG registers access an odd address.
- **455405**—ALG for FTP, RSTP, GTP, SQL, SIP and RSH was corrupting the control packet causing problems with the data packet.

### Performance

- **429821**—TCP 3-way handshake packets were randomly dropped due to a problem in TCP SYN-check feature.
- **455350**—For the interface, MTU is set to 1500 when a tunnel interface is added that might cause performance issues.

### Routing

- **416966**—When a route was displayed by **get route** command some of the flags were not freed, and the firewall rebooted. The route was frequently added and deleted by changing dynamic routing.
- **439759**—Firewall would reboot when an access-list tied to an RP configuration for multicast was unset.
- **442034**—Status change of tunnel or VSI interface should be handled for route advertisement.
- **444226**—OSPF flaps when it receives self originated LSA with different checksum.

### VoIP

- **422611**—Power Cycling H.323 IP Phone results in NAT pport leak.
- **442660**—VoIP calls using SIP failed randomly due to incorrect format of INVITE message.
- **443259**—SIP ALG cannot parse the quoted boundary in content-type:multipart. For example, content-type: multipart/mixed;boundary="boundary3".
- **443828**—H.323 phone did not function because of H.323 ALG mishandling.
- **458341**—SIP ALG was not handling the SIP calls that use multi-part message as expected.

### VPN

- **432400**—The IKE/IPsec passthrough ALG did not work when the loopback interface was used as source for NAT.
- **442719**—Unable to configure a C Class Broadcast IP address for the IKE Gateway address.
- **448720**—Unable to remove User Group that was previously bound to a VPN, even after that VPN has been removed.

- **451210**—VPN traffic failed when IPv6 was enabled in an NSRP Active/Active mode with NSRP Data Forwarding enabled.
- **459239**—Xauth information was erroneously removed when initial-notify was received.

### WebUI

- **293998**—In the WebUI, some alarm level events are not correctly sorted by log level.
- **438903**—In the WebUI, when HA link was Down, VSI status was erroneously shown as Inactive, while it should be Down as shown by CLI.
- **446866, 433589**—Global settings for IKE timers were not propagated to individual IKE gateways.
- **448780**—In the WebUI, there was no data saved in the file for "**Traffic Alarm**".
- **453298**—Advanced Policy Settings could not be configured using WebUI.
- **455462**—Using the WebUI, when an aggregate BGP route was added, a new option **summary-only** was added that was not specified in the WebUI.
- **459894**—Unable to remove the address book object "**DMZ Any**" after it was configured.

## Addressed Issues from 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**—With IPv6 policies, the command **exec policy verify** may give an incorrect result as the command is not supported for IPv6 policies, where IPv6 address is incorrectly interpreted as IPv4 address, and the fix skips IPv6 policies during policy verification.
- **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 failure.
- **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 failure.
- **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.

### 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.
- **398568**—SNMP query of the MIB object vrRouted in NETSCREEN-VR-MIB returned an IP address instead of an integer.
- **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.
- **296850**—RTSP media flow is disconnected after about a minute.
- **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.

### 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 6.2.0r15

#### ALG

- **796066**—SIP data session is no longer used in the same route as the control session. The data session now uses the route specified in the routing table.

#### Antivirus(AV)

- **803148**—Sometimes, websites failed to open with AV enabled and when syn-ack comes with a window size 0.

#### Logging

- **804620**—Redirecting logs to external USB drive may stop with an event message: "There is less than 10% space avaliable in current active file", even though there is more than 10% of free space available.

#### Other

- **796098**—If mirror is configured on ns2000 or ISG000 devices (including IDP enabled box), tcp three way handshake failed on the box during syn-proxy processing.
- **754606**—SYN flood protection is sometimes triggered, though the attack threshold is not reached.

#### WebUI

- **781483**—In WebUI, few pages are blank when reviewing the NHTB entries. Event logs in WebUI do not display the correct number of entries per page.
- **793235**—In WebUI, Network > Interface Edit > OSPF page select neighbor list from the Neighbor List drop down and then click Apply the neighbor list drop down menu setting is not updated after Apply function. The list does not appear in the device as it still shows `none.

## Known Issues from ScreenOS 6.2.0r14

### ALG

- **740513**—When SIP ALG fragments the packet, the first fragment is of small-sized which may not include the mandatory SIP headers.

### Management

- **737433**—The ifIndex value is not the same in standard MIB and Netscreen enterprise MIB while executing SNMP query for interfaces.
- **737747**—While using standard MIB2, indexes or mapping between Indexes of the OID 'ipAdEntIfIndex' and the OID 'ifDescr.x' are incorrect and as a result SNMP poll sends an incorrect result.
- **738116**—SNMP Authentication Failure Trap is generated when a GET-REQUEST with different SNMP version is received.

### NSRP

- **705438**—In asymmetric routing condition, if a session is not prepared and synchronized correctly might result in unexpected packet drop.

### Other

- **590160**—Device might crash when route id is a large number and the NSRP route sync is enabled.
- **710595**—When the "Pending Drop Notify" counter fills up the Infranet Controller process on the firewall and does not release regularly, results in Drop que full message and no Drop notify messages to be forwarded to Infranet Controller.
- **728480**—Asymmetric traffic fails when IPv6 is enabled.
- **732793**—Device might crash when you modify an existing policy.
- **740584**—When a sub-interface is created and cancelled an event message "MTU for interface has been changed to 1500." is displayed.
- **743309**—Multicast traffic can cause firewall to coredump.
- **744684**—Sometimes, after OS upgrade, the firewall starts rebooting continuously in loop condition, due to a memory overwrite issue. This is because of smaller buffer size of fat table in flash.
- **746646**—[ns5000 and ISG] ARP entries in Hardware and Software may mismatch due to inconsistent ARP update mechanism.
- **750929**—Device might crash when you delete the interface used by NTP module.
- **752103**—RTSP SET_PARAMETER is not address translated.
- **752246**—SCTP natted traffic might stop working when you set the envar x-in-ip.

### Routing

- **730018**—BGP IPv6 prefix is not advertised after reboot.

## Known Issues from ScreenOS 6.2.0r13

### ALG

- **710227**—SIP ALG is modified to ensure that all SIP data fragments have their call data modified according to any NAT parameters.

### Management

- **687217**—Firewall fails when running fprofile.
- **696588**— If SCP file transfer was used regularly then there was a high memory on firewall.

### NAT

- **700690**—Sometimes the Extended IP x.x.x.x or its range collides with IP y.y.y.y or its range when configuring an ext DIP on unnumbered tunnel interface.

### Other

- **551755**—"IPv6 neighbor gateway [IP6] is reachable" is logged incorrectly when it is unreachable.
- **692085**—Firewall reboots and core dumps due to multicast packets accessing the null pointer for a PIM neighbor.
- **700331**—Firewall reboots and core dumps after adding VSD-Group.
- **703677**—In redundant VPN configuration, OSPF does not come up when VPN failback from secondary to primary.
- **708406**—Firewall reboots and core dumps due to accessing the invalid memory area.
- **718372**—When a session is taken out of hardware and if the firewall receives a FIN then the firewall does not close the session.
- **722208**—SSG device stops passing traffic in all directions due to an error in read logic on the interfaces.

### Routing

- **718144**—During route failover some sessions are not getting cleared.
- **728946**—BGP cannot be established between two loopback interfaces belonging to different Virtual routers on the same device.

### VPN

- **686818**—Asic based firewall stops passing IPSEC traffic due to wrong logic check in the ESP sequence numbers.

### WebUI

- **687935**—In WebUI, the policy search feature is unable to display the selected service if it belongs to multi-cell service.
- **688016**—WebUI is unable to display NHTB table entries if the list of NHTB entries is more than 582.
- **717325**—Monitor Zone and Monitor Interface configuration is not available in WebUI.

## Known Issues from ScreenOS 6.2.0r12

### ALG

- **665008**—TCP connection is not established for MSRCP traffic in certain conditions, due to an endian issue.
- **678300**—Failure to translate IP on SET-PARAMETER within RTSP by ALG causes the video streaming to stop intermittently.
- **679138**—RM resources are released incorrectly that subsequently causes RTSP traffic to drop.

### Authentication

- **676984**—Authentication in NSRP from an Infranet Controller can sometimes lead to duplicate authentication entry and might cause crash dump and reboot unexpectedly.

### Management

- **600543**—With NSM enabled, the device management is very slow and crashes frequently.

### NSRP

- **568133**—IPv6 RA messages are processed on VSD 0 interfaces and are not processed on VSI interfaces which are part of VSD 1 and VSD 2.
- **666641**—Data link is unavailable when there is only one link in HA zone connected to 16 port uPIM.
- **672901**—After failback due to preempt, the new master (with preempt) sometimes lost connection to IC4500 (Infranet Controller).

### Other

- **543870**—An error is reported when a route in VR of shared DMZ zone on VSYS device from NSM is added.
- **578204**—Session byte count function was mistakenly used to carry additional information that should be carried by the packet byte count function. This caused duplicate logging data being sent to NSM.
- **599808**—Ability to log UDP floods on ASIC based systems is added.
- **660288**—In non-HA mode, IPv6 multicast packet is dropped by the interface when ipv6 config is disabled. Do not consider VSI.
- **662589**—Firewall experienced core dump and rebooted the system when accessing the Dlog process.
- **665355**—NSM supports "unset nsrp config sync vpn-non-vsi" command.
- **674637**—The firewall crashes sometimes when a long URL is described in custom category of sc-cpa.
- **674736**—GTP IDreq packets are incorrectly dropped by sanity check due to unknown IE.
- **675296**—In L2 mode, the vsdless session must have time sync mechanism.
- **676289**—The device crashes while running certain commands through SSH or telnet.
- **676354**—SSG140 dlog queue fullness causes session leak.
- **677467**—Open SSH 5.8 client with pty-req greater than 256 bytes fails with "PTY allocation request failed" error.
- **680365**—Firewall crashes when AV is enabled.
- **687653**—Sometimes tftp fails due to save config (from device).

### Routing

- **683325**—OSPF neighbour ship gets affected in loading while the OSPF messages fragment size is bigger than 1668 bytes.

### Screening

- **677385**—Transparent or L2 mode firewalls sends a SYN+ACK response packet to client with an all-zero MAC address.
- **681955**—Syn-cookie may not get triggered sometimes for the traffic that traverses custom L2 zones.
- **683501**—The MSS option and length are incorrectly built when using SYN proxy.

### VOIP

- **604887**—With SIP ALG enabled, the device might sometimes send TCP packets with window size zero which might stall the SIP session.

- **664502**—H323 messages are still flooding in ISG2000 even after disabling h323 app-screen message-flood.

### VPN

- **673075**—IKE DPD messages are generated from the NSRP backup device even after the NSRP failover occurs.

### WEBUI

- **610921**—WebUI has limitations on ipv6 client-duid length.
- **671222**—The WebUI login might not accept a username of 31 or greater characters even though the username is valid through CLI.
- **678280**—Unable to modify WEB filter custom message on screenos firewall through NSM GUI for integrated SurfControl CPA.
- **685269**—The "activate" command fails while saving the BGP neighbor through WebUI.

## Known Issues from ScreenOS 6.2.0r11

### IDP

- **601092**— Device name is missing in the syslog message forwarded from the firewall.

### Management

- **556535**— PBR configuration is lost after the firewall is rebooted.
- **607350**— Unable to retrieve the chassis slot information with snmp walk.

### Other

- **487640**— Hardware counters are not working on NS-5000-2XGE-G4 [2 x 10GigE Secure Port Module (SPM)].
- **558343**— Memory utilization of "sys pool" increases as some of the memory allocated in SMTP parser are not freed when the SMTP sessions are released.
- **574264**— Sometimes legitimate source IP address might be detected as an antispam blacklist IP address during high number of SMTP traffic.
- **581190**— The device fails when memory is allocated.
- **584827**— The backup firewall might not get all IPSec SA synchronized from system restart due to large number of VPN connections on NSRP setup.
- **593583**— The device fails while processing SMTP traffic for Antispam.
- **598630**— Event log displays "route is invalid" even though there are no route changes.
- **598836**— ASIC resets when FTP service is configured with a never timeout.
- **599609**— The "in packet" and "in ucast" counter keeps increasing, though the physical interface is down.

- **604785**— While creating VSYS with VR in the same line an incorrect and mandatory VR id number syntax is required as an optional field.
- **604069**— When Antispam or Antivirus is enabled, under certain conditions during TCP establishment, the TCP traffic might not flow properly.
- **606118**— Internal duplicate policy log entries might cause the send mail task on the firewall to loop subsequently causing high CPU usage.
- **610023**— [SSG300/500]Byte count for log-self shows wrong value.
- **610271**— While logging multicast traffic, the policy based traffic log is incorrect.
- **612248**— During high traffic, frequently pressing Crtl+C on console might cause wrong output in the event log and subsequently device fails.
- **613108**— After deleting a policy, the "traffic logs" for that policy is not removed and cannot be cleared manually.

### Routing

- **613600**— Path attribute length not set in BGP route update causes BGP neighborship to flap.

## Known Issues from ScreenOS 6.2.0r10

### Administration

- **580933**—High task CPU triggers flow CPU utilization alarm.

### Authentication

- **587578**—802.1x authentication is not supported on a bgroup interface.

### Other

- **554007**—Sometimes, the device might fail because of a particular type of packet.
- **555070** —SCTP traffic fails when it is moved to ASIC using the command **set envar x-in-ip=yes**.
- **561219**—Firewall experiences high CPU while receiving ICMP ECHO request with fixed sequential ID.
- **563425**—Firewall might fail if there is a communication error, such as duplex mismatch with the Infranet Controller.
- **563494**—Syslog messages contain 'T' character between date and time causing parsing errors.
- **568377**—ASIC might go into hung state with IPSEC-DSCP marking enabled.
- **572707**—Firewall fails because of a malfunction while running SPF in the OSPF task.

- **585314**—SCP to the firewall fails from an UNIX machine with error "unknown file '--ns_sys_config."
- **590147**—Members of aggregate interface become physically up after reboot even though they are set for physically down.

#### Routing

- **554973**—PBR is unable to route traffic using tunnel interface when it is in the up state.
- **561446**—OSPF neighbor flaps because of a problem with the OSPF update task on a system level device.

### Known Issues from ScreenOS 6.2.0r9

#### Other

- **568304**—Firewall fails when the DNS refresh occurs and the policies are updated, which also updates the proxy ID for the policy base VPN.

### Known Issues from ScreenOS 6.2.0r8

None.

### Known Issues from ScreenOS 6.2.0r7

None.

### Known Issues from ScreenOS 6.2.0r6

None.

### Known Issues from ScreenOS 6.2.0r5

None.

### Known Issues from ScreenOS 6.2.0r4

**None**

## Known Issues from ScreenOS 6.2.0r3

### CLI

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

### Other

- **427467**—[SSG 140] The device reboots unexpectedly due to ARP traffic across bgroup interfaces.

## 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 documentation.

## Concepts & Examples ScreenOS Reference Guide

- *Configuring a DHCP Server* section in the ScreenOS 6.1.0, *Concepts & Examples ScreenOS Reference Guide: Vol 2, Fundamentals* has the following incorrect information.

  **WebUI**

  > Addresses > New: Enter the following, then click **OK**:

  Reserved: (select)

  IP Address: 172.16.10.11

  Ethernet Address: 1234 abcd 5678

  **CLI**

  DHCP Server

  **set interface ethernet0/1 dhcp server option domainname dynamic.com**

  **set interface ethernet0/1 dhcp server option lease 0**

  **set interface ethernet0/1 dhcp server option dns1 172.16.10.240**

  **set interface ethernet0/1 dhcp server option dns2 172.16.10.241**

  **set interface ethernet0/1 dhcp server option smtp 172.16.10.25**

  **set interface ethernet0/1 dhcp server option pop3 172.16.10.110**

  **set interface ethernet0/1 dhcp server ip 172.16.10.10 to 172.16.10.19**

  **set interface ethernet0/1 dhcp server ip 172.16.10.120 to 172.16.10.129**

  **set interface ethernet0/1 dhcp server ip 172.16.10.210 to 172.16.10.219**

  **set interface ethernet0/1 dhcp server ip 172.16.10.11 mac 1234abcd5678**

  **set interface ethernet0/1 dhcp server ip 172.16.10.112 mac abcd1234efgh**

  **set interface ethernet0/1 dhcp server service**

  **save**

  To successfully configure the example, make the following corrections to the above WebUI and CLI:

  Do not perform the following in the WebUI:

  > Addresses > New: Enter the following, then click **OK**:

  Reserved: (select)

  IP Address: 172.16.10.11

  Ethernet Address: 1234 abcd 5678

  Remove the command **set interface ethernet0/1 dhcp server ip 172.16.10.11 mac 1234abcd5678** from the CLI.

- ScreenOS releases prior to 6.2.0 support VLAN retagging option only on NetScreen-5200 and NetScreen-5400 devices. VLAN retagging is not supported on

ISG and SSG series. This limitation is not included in the release 6.0.0 *Concepts and Examples ScreenOS Reference Guide*.

- The following note is incorrect in the *NetScreen Redundancy Protocol* chapter of the ScreenOS 6.2.0 and 6.3.0 *Concepts & Examples ScreenOS Reference Guide*:

  NOTE: ScreenOS does not support NSRP IPv6 related RTO synchronization. This example explains only about the configuration synchronization.

  Synchronization of IPv6 RTO is supported from ScreenOS 6.2.0 onwards.

- The following information is missing in the *Dialup Virtual Private Networks* chapter in the *Concepts & Examples ScreenOS Reference Guide*:

  When creating a VPN policy with address group and service group, the proxy ID is **0.0.0.0/0.0.0.0/0/0**. While creating a second VPN policy with different address group and service group using the same VPN tunnel, the following error message appears:

  **The new policy id <#> has identical IKE id as that of policy id <#>.. vpn invalid or not exist.**

  To resolve this error, create a new VPN tunnel using a different IKE gateway with different dialup user and IKE ID. The new VPN tunnel creates a new VPN ID. Create the second policy with a different address group and a service group using the new VPN tunnel. Therefore, the proxy ID check refers to the new tunnel.

- In the *Configuring an Active/Active NSRP Cluster* section in the *Concepts & Examples ScreenOS Reference Guide*, the figure displays the following incorrect title and labeling:

  1. The title of the figure reads Active/Passive NSRP Configuration.
  2. The label to the left of the figure reads the following:
     a. On device A the Manage IP is 10.1.1.21 and is on the redundant2 Interface.
     b. On device B the Manage IP is 10.1.1.22 and is on the redundant2 Interface.

  The correct information is as follows:

  1. The title of the figure should read Active/Active NSRP configuration.
  2. The label to the left of the figure should read the following information:
     a. On device A, the Manage IP is 10.1.1.1 and is on the redundant2 Interface.
     b. On device B, the Manage IP is 10.1.1.2 and is on the redundant2 Interface.

- The following information is missing in the *Reconnaissance Deterrence* and *Advanced Virtual Private Network Features* chapters in the *Concepts & Examples ScreenOS Reference Guide*:
  - The **set flow tcp-syn-bit-check** command checks the SYN bit but does not refresh the session. The **set flow tcp-syn-bit-check** command enables the PPU to perform the SYN check and sends the packet to the CPU for session creation.
  - The **set flow tcp-syn-check** command does a SYN check and refreshes session after a three-way-handshake refresh.

  - The **set flow tcp-syn-check-in-tunnel** command enables SYN Check for tunnel traffic. The **set flow tcp-syn-check-in-tunnel** command causes the PPU to check the SYN bit. If you disable this command, all SYN packets, tunnel and non-tunnel will be sent to the CPU for processing.

- The following information is not available in the *Denial of Service Attack Defenses* chapter of the *Concepts & Examples ScreenOS Reference Guide*: The threshold is set only for the average CPU. As the management traffic uses the average CPU for threshold, there is no recommended value to prioritize.
- The following information is not available in the *H.323 Application Layer Gateway* chapter of the *Concepts & Examples ScreenOS Reference Guide*: A single policy with policy-based NAT (DIP ID 2) fails due to the twin-pair port limitations on the DIP pool. The policy segments the traffic so that they do not have more than 512 phones (the DIP limitation) on each DIP pool.
- The Redundant VPN Gateways section in the *Advanced Virtual Private Network* chapter of the *Concepts & Examples ScreenOS Reference Guide* incorrectly states that Dead Peer Detection (DPD) is an alternate to the IKE heartbeat feature. However, this functionality for redundant VPN is supported only from ScreenOS 6.3.0 release onwards.
- The following URL is incorrect in the *Deep Inspection* chapter of the *Concepts & Examples ScreenOS Reference Guide*: https://services.juniper.net. The correct URL is: https://services.netscreen.com.
- The following information is not available in the *Digital Subscriber Line* chapter of the *Concepts & Examples ScreenOS Reference Guide*. The adsl1/0 interface acts as a PPPoE client. Ethernet 0/2 and ethernet 0/1 act as the DHCP server. On successful PPPoE of adsl1/0, the DHCP parameters that also contain the DNS information are applied to the DHCP server. Although the DNS option is automatically updated by PPPoE server, the user must select the Automatic Update of DHCP Server's DNS Parameters option.
- The following Addressed Issue is not documented in the ScreenOS 6.0.0r5 release notes:

  **258534**—VRRP transitions within ScreenOS were not reported in the event logs.
- The following information is missing in the *Monitoring Security Devices* Chapter in the ScreenOS 6.2.0r1 *Concepts & Examples ScreenOS Reference Guide*:

  ifName variable is added in the Link Up and Link Down traps in SNMP to determine the status of the trap.
- The SSG5 and SSG20 devices meet the requirements in the following European Community directives:
  - Regulation 1275/2008/EC (classified as Class B per EN55022)

    

    NOTE: **The standby mode described in 1275/2008/EC is not applicable to the SSG5 and SSG20, which must remain active at all times while in operation.**
  - Regulation 278/2009/EC for the external power adapter

- The following information is not available in the *Border Gateway Protocol (BGP)* chapter of the *Concepts & Examples ScreenOS Reference Guide*:
  - A BGP route is considered unresolvable when the system routing table in the same virtual router does not contain any route which is used to resolve this BGP route and match the BGP route's nexthop. Mutually recursive routes (routes resolving each other) also fail the resolvability check.
- The *Supported RADIUS Enhancements for Auth and XAuth Users* section in the *Concepts & Examples ScreenOS Reference Guide*, *Fail-Over* page displays the following incorrect information:

  If authentication via a backup server is successful, and the revert interval has elapsed, the device sends subsequent authentication requests to the backup server.

  The correct information is as follows:

  If authentication via a backup server is successful, and the revert interval has not elapsed, the device sends subsequent authentication requests to the backup server
- The following note is incorrect in *Authentication Servers* chapter of the *ScreenOS 6.2.0 and 6.3.0 Concepts & Examples ScreenOS Reference Guide*:

  

  NOTE: **This feature applies to RADIUS and LDAP servers only.**

  The correct note is as follows:

  

  NOTE: **This feature applies to RADIUS, LDAP, and TACACS servers only.**
- The following note is incorrect and has to be deleted in *Mapped and Virtual Addresses* chapter of the *ScreenOS 6.2.0 and 6.3.0 Concepts & Examples ScreenOS Reference Guide*:

  

  NOTE: **You can only set a VIP on an interface in the Untrust zone.**
- The following command is incorrect in *Authentication Servers* chapter of the *ScreenOS 6.2.0 and 6.3.0 Concepts & Examples ScreenOS Reference Guide*:

  **set admin auth timeout 0**

  The correct command is as follows:

  **set admin auth web timeout 0**
- The following information in Service Timeout Configuration and Lookup section in the Building Blocks for Policies chapter is incorrect:

  Services with multiple rule entries share the same timeout value. If multiple services share the same protocol and destination port range, all services share the last timeout value configured.

  The correct information is as follows:

Services with multiple rule entries share the same timeout value. When we set multiple services in a policy, and if these services share the same protocol and destination port range, then the service entries are arranged in alphabetical order. The first service timeout value is selected when processing the timeout lookup.

- The following note information is missing in *Configuring Layer 2 Virtual Systems* section of *Concepts & Examples ScreenOS Reference Guide*:

NOTE: Mix Mode (L2/L3) within custom VSYS is not supported but the Mix Mode between root VSYS and custom VSYS is supported. You cannot have both Layer 3 and Layer 2 mode in Custom VSYS, but we can have root VSYS in L3, and Custom VSYS in L2.

## ScreenOS CLI Reference Guide: Command Descriptions

- The following information in the *ntp Through RIPng* chapter of the 6.2.0 and 6.3.0 *ScreenOS IPv6 CLI Reference Guide: Command Descriptions* is incorrect and redundant:

  av

  set policy { ... } av ***name_str***
  set av ***name_str***
  unset policy { ***pol_num*** | id ***pol_num*** } av ***name_str***
  unset av ***name_str***

| | |
|---|---|
| **av** ***name_str*** | Sends HTTP or SMTP traffic to which the policy applies to the specified antivirus (AV) scanner, which examines the data for viruses. If it finds a virus, the AV scanner quarantines the infected data for further study and returns the SMTP or HTTP file—without the infected data—to the security device, which then forwards the file to the intended recipient |

  **Example:** The following command instructs the security device to forward SMTP traffic originating from the remote mail server r-mail in the Untrust zone and destined for the local mail server mail1 in the DMZ zone to an AV scanner named **av1**:

  **set policy id 1 from untrust to dmz r-mail1 mail1 smtp permit av av1**

  ScreenOS 6.2.0 and ScreenOS 6.3.0 IPv6 policies do not support **av**.

- The following command available in the *rm Through zone* chapter in the *ScreenOS CLI Reference Guide: IPv6 Command Descriptions* does not support IPv6:

  **add-default-route**

- The following command not available in the *alarm* chapter in the *ScreenOS CLI Reference Guide: IPv6 Command Descriptions* :

  - The **set alarm threshold audit-storage<*percentage value*>** command sets the alarm threshold percentage for audit storage capacity.

- The **unset alarm threshold audit-storage** command turns off this feature.

- In *ScreenOS CLI Reference Guide: IPv6 Command Descriptions*, ntp Through RIPng chapter **exec policy verify** command information is provided though the command is not supported on IPv6.

### ScreenOS Online Help

- The following note is incorrect in the **SCREEN Options** page in the ScreenOS 6.2.0 online Help:

  NOTE: The following options are available for physical interfaces only: SYN Attack, ICMP Flood, UDP Flood, and Port Scan Attack.

  The correct information is:

  NOTE: The SYN Attack, ICMP Flood, UDP Flood, and Port Scan Attack options are defined in the zone level. For high-end platforms, the ICMP or UDP flood attack option defined at the sub-interface level is applied only to physical interface and not to the sub-interface level. Only the SYN flood/Port Scan attack option is applied to the sub-interface level.

- In the WebUI, **IP Address Group Configuration** page for Policy is updated with a **Type** button. The button allows you to select multiple MIP or VIP configurations while creating an address group in a global zone. The selected **Type** is displayed while editing this address group.

### ScreenOS Hardware Installation and Configuration Guide

- The following information available is incorrect in the Basic firewall protection section of *Configuring the Device* chapter in the *ScreenOS Hardware Installation and Configuration Guide* for the platforms SSG-20, SSG-140 , SSG-300M , SSG-500 , and SSG-500M:

  The device is configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide.*

## 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.
- **UDP and ICMP Flood Screening**—ScreenOS 6.2.0 does not support UDP and ICMP flood screening for aggregate interfaces in ISG and NetScreen 5000 series. [428057]
- **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.
- **VLAN retagging**—ScreenOS releases do not support VLAN retagging on SSG series.
- **HA pair on ISG2000 devices**—Currently ScreenOS does not support redundant or aggregate interfaces in an active-active HA pair on ISG2000 devices. Packets received on the backup device cannot pass through the cluster in an active-active ISG2000 pair.
- **Policies**—Policy Verification **exec policy verify** command is not supported for IPv6 policies. It is only supported for IPv4 policies.

## 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)
  - Antispam
  - Antivirus
  - Web Filtering
- 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) database. When an NS-5GT device is upgraded from an early release to ScreenOS 6.2.0, the AV 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.

 