Juniper Networks ScreenOS Release Notes

Release 6.3.0
September 2009
Revision 02

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

Contents

Version Summary

ScreenOS 6.3.0 firmware can be installed on the following products: Secure Services Gateway (SSG) 5, SSG 20, SSG 140, SSG 320M/350M, SSG 520/520M, SSG 550/550M, Integrated Services Gateway (ISG) 1000, ISG 1000-IDP, ISG 2000, ISG 2000-IDP, and NetScreen-5000 series with the NS 5000-MGT2/SPM2 and NS 5000-MGT3/SPM3.

This release incorporates bug fixes from ScreenOS maintenance releases up to 6.2.0r2, 6.1.0r6, 6.0.0r8, and 5.4.0r13.

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 6.0.0r1 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 rule is SSG 500-series 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 6.3.0 release.

NOTE: You must register your product at http://support.juniper.net to activate licensed features such as antivirus (AV), deep inspection (DI), and virtual systems (vsys) 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 your desired features.

New Software Features and Enhancements Introduced in 6.3.0

The following sections describe the new features introduced in the ScreenOS 6.3.0 release.

Authentication

- **User Authentication**—Beginning with ScreenOS 6.3.0, the Juniper Networks security device supports authentication redirection for HTTP traffic that is directed to a nonstandard destination port.

Antivirus (AV) and Web Filtering

- **Sophos Anti-Spam to replace Symantec Anti-Spam**—Beginning mid-September 2009, Sophos Anti-Spam service will be 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.

- **Juniper Full Antivirus Database**—Beginning with ScreenOS 6.3.0, Kaspersky Lab supports only a single antivirus database known as Juniper Full Antivirus Database. The existing databases such as extended, itw and standard are removed.

- **Virus Description and Alert Message**—If the data sent to FTP or HTTP Traffic contains a virus, the security device replaces the data with a warning message or drops the data. In both cases, a message with a URL link that describes the virus is logged.

  For SMTP, IMAP and POP3 Traffic, the security device in addition to the above, changes the content type to text/plain, replaces the body of the message with a notice and a URL link that describes the virus, sends it to the appropriate recipient, and notifies the sender.

- **Web Filtering Whitelists and Blacklists Without a License**—Web filtering supports the following features even if the license key is not installed or has expired:

  - Define Web-filtering profiles and bind them to policies
  - Retrieve category information for HTTP requests
  - Define static whitelist and blacklist categories
  - Check cache for categories

NOTE: The device does not support checking the cache for categories if the key is not installed, but it does support this check if the key is expired.

- **Integrated Web Filtering Based on Group Membership**—In the previous release, the URL filter profile was bound to policy. Beginning with ScreenOS 6.3.0 release, the administrator can bind the profile to user group. The Web Filtering (WF)

Manager extracts the URL from the request and identifies the username and user group associated with the IP address. If the user belongs to multiple user groups, the WF Manager binds the profile with the user group that has highest priority. Then, the WF Manager identifies the category of the URL and permits or blocks the request accordingly. User groups can be prioritized.

- **Increased Number of Web-Filtering Profiles on SSG 500–series**—For integrated Web filtering, the number of customer-defined profiles for SSG 550 and SSG 520 devices is increased to 300 profiles from 50 (SSG 550) and 25 (SSG 520).

Border Gateway Protocol (BGP)

- **Redistributing Routes in BGP**—For each virtual router (VR), BGP can support up to 17000 redistributable routes. The increase in redistributable routes in BGP to 17000 applies to the NetScreen-5000 platforms only.
- **Display Format of BGP Community Lists**—Beginning with ScreenOS 6.3.0, the configuration file displays the BGP community lists in a new AA NN format, where AA identifies autonomous system and NN identifies community. This new format is in compliance with RFC-1997.

Device Management

- **Enabling Syslog on Backup Devices**—Backup devices in an Active/Passive NSRP configuration can now send all syslog messages to the syslog server, allowing an administrator to effectively monitor the backup devices. By default, this feature is disabled.
- **Simple Network Management Protocol Version 3 (SNMPv3)**— ScreenOS 6.3.0 supports SNMPv3 framework. System status data can be collected securely from the device without the data being tampered with and corrupted. The SNMPv3 USM allows ScreenOS to encrypt the confidential information to prevent the contents from being exposed on the network. The SNMPv3 VACM provides a configurable access control model for easy administration.
- **Interface Administrative Status**—ScreenOS 6.3.0 supports a command for setting an interface administrative status to the down state. By default, the administrative status of an interface is set as up. The administrator can disable the administrative status of an interface with the CLI:

  ```
  set interface xx disable
  ```

- **Increased Number of Hosts per SNMP Community**—Beginning with the ScreenOS 6.3.0 release, you can configure 64 hosts per SNMP community. In earlier releases of ScreenOS, this value was limited to no more than 40 hosts per SNMP community.
- **Include Device Serial Number in Log Messages**—Beginning with the ScreenOS 6.3.0 release, for system logs, the device serial number is used as a unique device identifier within the logs.

- **VLAN1 Interface to Support DHCP and AUTO Configuration**—Beginning with the ScreenOS 6.3.0 release, the VLAN1 interface of a device in transparent mode supports the DHCP client and AUTO CONFIG features.
- **Loading Configuration from USB**—When the SSG device initializes, and if the administrator has configured envar properly, then ScreenOS can check if the USB device is connected to the port and loads the configuration file usb: auto_config.txt (if the file is stored in the USB device).

Internet Protocol Security (IPsec)

- **AC VPN Enhancements**—ScreenOS 6.3.0 supports dual-hub Auto Connect virtual private network (AC-VPN) where one hub remains active, passing the traffic from one spoke to another spoke until a dynamic VPN tunnel is established. The hub with the highest routing instance priority becomes the active one. The spokes use the VPN monitoring feature to check the status of the hubs. When the hub acting as a primary fails, the dynamic tunnel and its associated NHRP routing instance are removed at both the spokes. Traffic begins to pass through the other hub, which creates a new dynamic tunnel. If the failed hub comes back, the spokes choose this hub again because of the priority setting. However, the traffic continues to flow through the newly created dynamic tunnel until the other fails.
- **Support for Multiple Proxy IDs Over Route-Based VPN**—ScreenOS 6.3.0 supports multiple proxy IDs on a route-based VPN. If multiple tunnels exist between peers, the security device uses proxy IDs to route the traffic through a particular tunnel. For each proxy ID, a specific tunnel and Phase 2 SA are associated. When traffic matching a proxy ID arrives, the security device does a proxy-ID check to route that traffic. If multiple proxy IDs are defined for a route-based VPN, a proxy ID check is always performed, even if it is disabled. In a hub-and-spoke topology, proxy IDs should be defined for both hub-to-spoke and spoke-to-spoke configurations.
- **DPD Enhancement**—ScreenOS 6.3.0 provides a DPD enhancement that allows the dead peer to failover the tunnel to another VPN group member with the second highest weight. It uses the DPD reconnect parameter to renegotiate the tunnel with the dead peer at specific intervals. If the tunnel is successfully renegotiated, the tunnel fails back to the first member.
- **Elliptical Curve Diffie-Hellman Key Arrangement**—ScreenOS 6.3.0 supports elliptical curve Diffie-Hellman (ECDH) groups 19 and 20 for Internet Key Exchange version 1 (IKEv1) key exchange. ECDH uses elliptical curve cryptography to generate public-private key pair. The module sizes of DH groups 19 and 20 are 256 bits and 384 bits ECDH prime curves, respectively.
- **Support Authentication Header Transport Mode**—[ISG 1000/2000, NS 5200/5400 M2/SPM2 , NS 5200/5400 M3/SPM3] ScreenOS 6.3.0 supports authentication header (AH) transport mode on high-end systems for IPv4 packets only. This feature does not work if IPv6 is enabled in the system environment.
- **IKEv2 Configuration Payload (CP) and Dial-up Support**—Support for IKEv2 configuration payload (CP) for dynamic end points and IKEv2 dial-up group user VPN is available in this release. For details on the implementation, refer to the *Concepts & Examples ScreenOS 6.3.0 Reference Guide*.

Internet Protocol Version 6 (IPv6)

- **Support OSPFv3 for IPv6** —Beginning ScreenOS 6.3.0, Juniper Networks security device supports OSPFv3 for IPv6. Most configuration and operational commands function essentially the same as in OSPFv2.

  OSPFv3 does not support the following features:

  - NBMA link and neighbor authentication
  - Demand Circuit and NSSA
  - Multiple instances per link.

  OSPFv3 is supported across all platforms. However, license is required to run it on the following devices:

  - SSG320M
  - SSG350M
  - SSG520M
  - SSG520
  - SSG550
  - SSG550M
  - ISG1000
  - ISG1000 with SM
  - ISG2000
  - ISG2000 with SM
  - NS5200M2/SPM2
  - NS5200M3/SPM3-J2
  - NS5400M2/SPM2
  - NS5400M3/SPM3-J2

- **Command to Inhibit AAAA Requests Over IPv4**—ScreenOS 6.3.0 provides an option to enable or disable the Network Address Translation-Port Translation Domain Name System Application Layer Gateway (NAT-PT DNS ALG) to modify DNS requests received from the IPv6 domain. Besides translating the addresses for transmitted DNS requests, the NAT-PT DNS ALG also modifies the DNS request before forwarding it to another domain that has only IPv4 addresses. By default, this option is disabled.
- **IPv6 Prefix and DNS Information Update**—ScreenOS 6.3.0 supports dynamic IPv6 prefix and DNS information update from the upstream DHCPv6 server. A CPE router acting as a DHCPv6 and PPPoE client negotiates IPv6 prefixes and DNS information for the downstream DHCPv6 server on the other interface of

the same CPE router. If the connection between the CPE router and the upstream DHCPv6 server is disconnected and then re-established, the CPE router updates the newly learned IPv6 prefix and DNS information dynamically on the downstream DHCPv6 server without waiting for the delegated prefix to expire.

ISG-IDP Diagnostic Improvements

- **IPv6 Full Support on ISG-IDP**—Beginning with ScreenOS 6.3.0, ISG Security Module provides IPv6 support for the following features: packet capture and packet logs for IPV6 traffic; configure header match information for IPv6 traffic and ICMPv6 messages; IPv6 traceroute anomaly; IPv6 log messages in the NSM log viewer.
- **ISG-IDP Means to Identify the Secure Module (SM) Used by a Session**—Beginning with ScreenOS 6.3.0, users can identify which SM card and CPU a session is using. It is possible to filter the session table output with the CLI command get session sm-slot *slot-id* sm-cpu *cpu-no*.
- **Command for Displaying CPU Usage on SM**—Beginning with ScreenOS 6.3.0, users can enable the security device to calculate the CPU usage of the ISG Security Module for the last 60 seconds, last 60 minutes, and last 24 hours by using the sc_enable_cpu_usage parameter.
- **Transfer Core Dump to the Management Module Flash or Compact Flash**—Beginning with ScreenOS 6.3.0, users can transfer the core dump files from the RAM disk of the ISG Security Module to the flash memory of the management module using the CLI command set sm-ctx coresave.
- **SNMP Trap and Event Log Entries for ISG with IDP**—From ScreenOS 6.3.0, ISG Security Module supports generating log messages and SNMP Traps when CPU usage, memory usage, and session count per IDP security module exceeds the user-defined threshold. The device also generates messages when it detects an IDP security module failure.

NOTE: The user-defined threshold value is not stored in NSM. The value is reset to the default once the system reboots.

- **Inspection of Multicast traffic by IDP Security Module**—Beginning with ScreenOS 6.3.0, users can enable ISG Security Module to inspect multicast traffic by using the CLI command set flow multicast idp.

NOTE: For multicast traffic inspection, all outgoing interfaces should belong to the same zone.

- **UAC Integration with Role-Based IDP Policy**—From ScreenOS 6.3.0, ISG Security Module can support role-based IDP policy. Administrators can configure the security device to inspect traffic using either user roles or source IPs. When user-role-based IDP inspection is selected, the security device starts checking user-role-based policies first; if a match is not found, only then the security device

searches for IP-based rules. This feature requires UAC deployment and role information is provided by Infranet Controller.

Network Address Translation (NAT)

- **Enhancement to IKE and ESP Passthrough Traffic**—Beginning with ScreenOS 6.3.0, Network Address Translation (NAT) supports both NAT-Traversal and Non-NAT-Traversal IKE and IPsec passthrough traffic. The Application Layer Gateway (ALG) is enabled to support interface NAT and IKE DIP pool NAT.
- **Support for More Than 62946 Sessions per IP in a DIP Pool** —When the security device performs NAT-src with a DIP pool containing an IP address range with PAT enabled, each DIP:DPort pair can only be assigned to one session. Beginning with ScreenOS 6.3.0, you can enable DIP to support multiple sessions per DIP:DPort. The DIP pool supports multiple session per DIP:DPort only if two packets have different destination IP addresses. After configuring the DIP pool scale size, every IP address contains multiple port pools that consist of all available ports for an IP address. Every IP can support up to scale-size* 62463 sessions.

  The maximum scale size for an interface cannot exceed the DIP scale size value specified in the vsys profile.
- **TCP Session Close Notification**—ScreenOS sends a TCP session close notification ACK message to both the client and the server when a session is being closed.

  To enable a policy to send TCP session close notification, complete the following prerequisites:

  - You must enable TCP SYN checking and TCP reset options in both the client and the server zones.
  - You must enable TCP sequence check only for ISG 1000/2000 and NS 5200/5400.
- **Creating a Session Cache to Accelerate HTTP Traffic**—Beginning with ScreenOS 6.3.0, you can create a session cache for HTTP-based protocols to minimize CPU utilization and to enhance performance. A session cache is a special structure that caches all the reusable information of both software and hardware sessions created by the first connection of an HTTP session bundle.

  A session cache supports other traffic but does not ensure performance enhancement.

  You cannot create a session cache for the following conditions:

  - When the session is synched from another security device.
  - When the session is created by an Application Layer Gateway (ALG).
- **Importing Traffic to the Correct VSI by Proxy ARP**—The administrator can enable importation of traffic to the correct VSI by setting the proxy ARP entry. Upon adding a proxy ARP entry on an interface, ScreenOS imports the traffic that is destined to the IP range using this interface.

You can use the CLI command proxy-arp-entry or WebUI Network > Interface > Edit> Proxy ARP Entries to set the proxy ARP entry.

- **NAT-Dst Port Shift using VIP**—Using the port-range VIP entry, a range of ports can be mapped between Virtual IP and Real Server IP.

NetScreen Redundancy Protocol (NSRP)

- **Add More Detail to the Output of** get nsrp—The output of the get nsrp vsd-group command includes a new column; the *uptime* column for VSD group or myself uptime column for current security device denotes the duration in the primary or backup state.

Other

- **Hot Patch Management**—Beginning with ScreenOS 6.3.0, the hot patch enables injecting the customer service patch into the running image without rebooting the security device. The hot patch as debug patch provides for easier debugging.

  The ScreenOS hot patch management component runs on the security device and performs the following functions:

  - Loads the hot patch file from TFTP to flash memory
  - Removes the hot patch file from flash memory
  - Maintains the patch finite state machine (FSM)

- **Cache Recently Used Route and ARP Entries**—Beginning with ScreenOS 6.3.0, Juniper Networks security device allows the user to cache recently used route and ARP entries for destination routes by using the set flow route-cache command. This feature does not work if ECMP is enabled.
- **Ability to Add** exec **and** save **Commands to Scripting Tool**—Beginning with ScreenOS 6.3.0 release, the ScreenOS scripting tool supports the exec and save commands. These commands are visible in the script context record. The parser identifies these commands in the script record context and saves them into the script. This enhancement enables the user to execute commands that facilitate troubleshooting.
- **Timeout for Track IP**—Beginning with ScreenOS 6.3.0, the user can set the maximum timeout value for track IP.
- **Boot with Default Gateway IP**—The new ScreenOS boot loader allows you to define a default gateway IP, then user can download image from a remote TFTP server.
- **Identifying Gigabit Interface**—Beginning with ScreenOS 6.3.0, users can identify the type of gigabit interface using the CLI command get interface *interface-name*.
- **Boot Loader for SSG and Boot ROM Version for ISG or NetScreen–5000 series Displayed in CLI**—Beginning with ScreenOS 6.3.0, you can view the boot loader for an SSG device and boot ROM version for ISG or NetScreen–5000 device using the get system command.

  Example 1:

```
ssg20-> get system
BOOT Loader Version: 1.3.2
```

Example 2:

```
nsisg2000-> get system
BOOT ROM Version: 1.1.0
```

- **WELF Log Format Enhancement**—Beginning with ScreenOS 6.3.0, enhancements have been made to the event log, traffic log and IDP log formats to follow the WELF log regulation. If backup for the logs is enabled, logs can be sent to a maximum of four WebTrends servers. TCP or UDP transport protocol can be used for communication. IP connections can be manually reset. The following log types must be sent along with the appropriate heading prefix:
  - Configuration log [Config Change]
  - URL Filter Detection [URL filtering]
  - AntiVirus Detection [AntiVirus]
  - Antispam Detection [AntiSpam]
  - IPS/DI Detection [IPS/DI]
  - Screen Attack [Attack]
- **SCTP Protocol Filtering**—Beginning with ScreenOS 6.3.0, the existing Stream Control Transmission Protocol (SCTP) stateful firewall supports protocol filtering. You can configure the security device to permit or deny traffic based on the SCTP Payload Protocol and M3UA Service Indicator. The Payload Protocol identifies the type of data being carried out by the SCTP data chunk, the M3UA Service Indicator identifies the type of data being carried out by the M3UA data message. Based on the Payload Protocol, you can create an SCTP profile and bind it to a policy.

NOTE: ScreenOS supports SCTP protocol filtering on NetScreen-5000 and ISG series devices only.

- **Converting** join-group igmp **Commands to** exec join-group—Beginning with ScreenOS 6.3.0, the **exec join-group** and **exec leave-group** commands replace the **set igmp join-group** and **unset igmp join-group** commands. The **exec join-group** command replaces the **set join-group** command. The **exec leave-group** command replaces the **unset join-group** command. There is no impact on the functionality of the commands. The **set** and **unset** commands are deprecated.

Policies

- **Policy Installation Enhancement** —Beginning with ScreenOS 6.3.0, the policy installation process has been enhanced.

  The new process provides the following advantages:

- Avoids frequent policy re-installation caused by dynamic DNS address changes.
- Eliminates traffic drops while installing the policy.
- Allows the user to configure the hold-interval option of policy installation using the following CLI command:

  set policy install hold-interval *seconds*

  The default value is 5 seconds. The minimum is 0 and the maximum is 10. This command specifies the maximum time interval between when policy configuration occurs and actual policy installation begins. When the user creates a new policy or modifies an existing policy, the policy installation is delayed by up to the value of hold-interval value specified. This allows the system to more efficiently process the session table by handling several updates at once or by reducing the thrashing caused by extremely rapid updates.

  unset policy install hold-interval

  The unset command resets the default value of hold-interval.

  Example: To configure hold-interval option to 2 seconds:

  set policy install hold-interval 2

Routing

- **IRDP Support for All Platforms**—Beginning with ScreenOS 6.3.0 release, ICMP Router Discover Protocol (IRDP) support is available on all platforms; however, IRDP support is available only on an Ethernet interface with an IP address.
- **DSCP Marking for Self-Initiated Traffic**—The administrator can configure the DSCP value for traffic initiated by the security device. The DSCP value can be configured for 11 services: BGP, OSPF, RIP, RIPNG, TELNET, SSH, WEB, TFTP, SNMP, SYSLOG, and WEBTRENDS. You can use both the CLI and the WebUI to configure DSCP marking.
- **QoS Classification Based on Incoming Markings**—In ScreenOS 6.3.0, traffic-shaping policies are enhanced to support quality of service (QoS) based on the IP precedence and Differentiated Services code point (DSCP) marking of incoming packets. The QoS classification feature for incoming traffic works only if the traffic-shaping mode is set to Auto or On.

Security

- **Denial of Service Attack Defenses**—ScreenOS 6.3.0 supports the feature of strict TCP-SYN-check wherein a strict syn check is applied to all the packets in a TCP three-way-handshake before the three-way handshake completes. Users can enable this feature by using the set flow tcp-syn-check strict command.

- **Verification of IP address in ASIC Whitelist**—Beginning with ScreenOS 6.3.0, users can verify if a specific IP-address is in the ASIC whitelist by using the get asic ppu whitelist *ip-address* command.
- **Support for SecurID Server Cluster**—RSA supports a primary server and up to 10 replica servers to process authentication requests. At least one of primary or slave servers must be configured with static IP. RSA SecurID Server Cluster supports the name locking, load balancing, and failover functions.

Changes to Default Behavior

This section lists changes to default behavior in ScreenOS 6.3.0 from earlier ScreenOS firmware releases.

- The set igmp join-group and unset igmp join-group commands for the interface are deprecated. If you execute the set/unset igmp join-group commands, the following warning appears:

  WARNING: This command is a deprecated command and cannot be saved to configuration. Please use the following new preferred syntax:
  exec igmp interface if_name join-group group_addr [{ include | exclude| to_include |to_exclude} sources_ip]

- The CLI command set interface *interface name*proxy-arp-entry *ip_min ip_max* takes precedence over the existing set arp nat-dst command. This means that when the proxy ARP entry is defined and matched, then the system does not respond to the ARP request via the physical interface.

  Because the set interface *interface name*proxy-arp-entry *ip_min ip_max* command allows the customer to have better control of the device, the command set arp nat-dst is not recommended.

- The SNMP changes might affect the management software as follows:
  - Logical interfaces are added to the interface table.
  - Several new SNMP traps are introduced in the ScreenOS 6.3.0. For details on the new SNMP traps, see the change history of published ScreenOS 6.3.0 MIB NS-TRAPS.mib.

  You can consider modifications as required.

Network and Security Manager (NSM) Compatibility

This section provides information about updates required to complementary Juniper Networks products to ensure their compatibility with ScreenOS 6.3.0.

Support for ScreenOS 6.3.0 has been introduced with NSM 2009.1r1. Navigate to the Support webpage 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 3.5.116331. Refer to the detector release notes for more information on the availability of new releases.

After you have performed the ScreenOS firmware upgrade, you must update to the latest IDP Detector Engine and Attack Object database:

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 the 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 the ISG-IDP devices. From NSM, select **Devices > Configuration > Update Device Config**, and complete the wizard steps.

Addressed Issues in ScreenOS 6.3.0

The following operational issues were resolved in this release:

Administration

- **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. However, this is not a supported configuration; admins should not be allowed to configure a VIP from a subnet other than the unnumbered tunnel interface IP.
- **414839**—The policy logs in syslog did not show the correct data sent or received for FTP.
- **416873**—After a reboot, some event log entries were not recorded in the syslog file, when the syslog was configured using UDP.
- **429883**—The MSS-based sockets were changed on the new accepted socket.
- **432014**—The authorized user with read and write privileges is able to issue the set admin password command because of which some user privileges are lost.
- **445491**—When displaying BGP, route advertised without specifying a neighbor address, the error **bgp neighbor 0.0.0.0 does not exist** is displayed.

Application Layer Gateway (ALG)

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

Antivirus (AV)

- **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 might drop.
- **388885**—The extended antivirus (AV) pattern file was too large for the flash memory devices that support this function. However, the standard antivirus pattern file worked as expected. ISG 1000/2000 and NetScreen 5000-series devices do not support the extended AV pattern file setting.

Authentication

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

Command Line Interface (CLI)

- **435979**—[SSG 500] The output of the get chassis command does not include PIM name.
- **392417**—The set tag <number> command under vsys was not configured correctly.

Deep Inspection (DI)

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

Domain Name System (DNS)

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

Flow

- **235781**—Using transparent mode, under high traffic conditions, sometimes a small number of sessions cannot be cleared. The sessions appear to be "time 0" but continue to remain in the session table. Running set sat session-clean clears these sessions from the table after one round of session cleaning.

- **239631**—If you configure the initial session timeout below the valid range (20–300 seconds), the system interprets these values as minutes instead of seconds.

General Packet Radio Service (GPRS)

- **422979**—When GTP inspection was enabled, ICMP Destination Unreachable packets of the GTP session were dropped.
- **426075**—When GTP inspection was enabled, occasionally a DeletePdpResponse or EchoResponse dropped and the message **non-existent gsn** appeared in the log.

High Availability and NetScreen Redundancy Protocol (HA and NSRP)

- **235303**—Delay in the peripheral devices updating the forwarding table when a failover occurs in an NSRP cluster in transparent mode. When the devices have no gratuitous ARP mechanism as in NAT or Route mode, peripheral devices update the forwarding table only when the active physical interface is restarted. The update happens after five seconds by default.
- **236275**—In transparent mode, if the VSD group is not bound to a VLAN group, the security device incorrectly reports the VSD as being in Active-Passive mode.
- **236634**—In an Active-Passive configuration, if the active security device handles a large number of FTP connections, the CPU utilization of the backup device remains high even when the rate of the FTP connections per second on the backup is low.
- **253467**—If a device's SIP traffic is very heavy in an NSRP deployment, although the master box works well, there are delays when resources on the backup box are removed. Operational impact on the cluster is minimal, and the backup box recovers automatically.
- **303714**—For NSRP cluster deployments, when upgrading from ScreenOS 5.4 (or any earlier release), the following ALGs do not sync correctly until both devices in the pair are upgraded: SIP, SCCP, MGCP, RTSP, SQL, PPTP, P2P, AppleiChat, and H.323.
- **422747**—In the Active/Active mode, FIN packet in the NSRP data path is not processed correctly when SYN-CHECK is 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.
- **437661**—The RIP and OSPF MD5 authentication results in the NSRP configuration are not in synchronization.
- **438794**—Backup NSRP firewall lost synchronized OSPF routes.

Intrusion Detection and Prevention (IDP)

- **305128**—If only a destination port (dst-port) is specified in IDP flow filter, the filter does not capture traffic in both directions.
- **305295**—If an IDP rule is configured with the attack value NONE, then diffserv does 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 is unable to escalate the response and drop the connection.
- **410393**—When updating offline from the Local Server, the automatic DI signature update fails.
- **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.

Internet Protocol Version 6 (IPv6)

- **227934**—SSG platforms incorrectly process the ICMPv6 error packet that they receive in response to a non-first fragment packet that exceeds the outgoing interface MTU.
- **236085**—In transparent mode, you cannot manage a zone that is on a vsys using the zone nsrp manage CLI command, because it is a global setting based on vlan1 interface. In root mode, you can manage only the related vsys.
- **236087**—On SSG 320/350 devices, a 4-byte PVE tag is used to identify which interface the packet came from, limiting the maximum supported packet length to 1514 bytes.
- **236549**—When deployed in transparent mode, some high-end platforms such as ISG 1000-IDP do not support more than 20 reassembled segments. If you try to ping another device with data that requires more than 20 reassembled segments (for example, 30,000 bytes), the ping request fails.
- **239285**—ScreenOS does not verify the IP address that you enter when you configure the security device.
- **239598**—On some high-end platforms, after you have enabled IPv6, the CLI incorrectly allows you to enable parameters such as DSCP marking, IDP, and NSRP Data Forwarding that are not supported in IPv6 mode.
- **267239**—When modifying an IPv6 or a wildcard policy through the WebUI, all existing sessions for the policy are removed. However, existing sessions are not removed if you only modify some minor features—such as session-limit or alarm-without-drop—of an ordinary IPv4 policy through the WebUI.

Management

- **218168**—The incorrect range in integrated URL filtering SC-CPA cache is causing NSM validation error.
- **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.

- **292490**—NSM update fails when configuring IKEv2 soft lifetime buffer.
- **438684**—The set flow mac-cache-mgt command is not working for the management of the backup firewall using the master firewall.

Network Address Translation (NAT)

- **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.

Other

- **226768**—The limit-session screen option is enforced even if the alarm-without-drop option is enabled.
- **255774**—The debug command unset console dbuf might make the box unstable, especially under heavy traffic. Administrators are advised to use care when running this command.
- **258931**—Due to a memory limitation, NS 5000 devices are currently unable to support 500 vsys when an advanced license key—such as for virtual router or Layer 2 Active-Active support—is part of the deployment.
- **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.
- **263512**—ScreenOS 6.1.0 includes a new SSHv2 secondary login banner feature. However, unless the feature is enabled, if the secondary banner is displayed before a login prompt on a console or via a Telnet connection, no positive acknowledgment to the secondary banner is required (applicable to console, Telnet, SSHv1, and SSHv2 connections).
- **263585**—In certain situations, Network Address Translation (NAT) traffic using H.323 ALG resets the device.
- **266022**—Because the NS 5400 supports 2 million sessions by default in 6.1 (and 6.0.0r2 and later), you must ensure that the device has a minimum of 450MB of free memory when upgrading from 5.4 or 6.0.0r1 to 6.1.0 or 6.0.0r2. One million sessions require approximately 340MB of memory.
- **274425**—The drop of to-self IKE packets is not logged when no IKE is configured.
- **278668**—[SSG 550/550M] An error in the boot-loader code caused the interface references to be switched and the motherboard version to be incorrectly reported while upgrading from boot mode.
- **312046**—On some devices, an attempt to negotiate the maximum transmission unit (MTU) using the ICMP "packet too big" packet might fail. Failure to negotiate the MTU might, for example, cause an FTP session failure. The failure is caused in part because the ICMP packet is sent only once.
- **387143**—The alarm LED is cleared automatically without issuing the clear led alarm command.

- **391304**—The duration of time reported by policy traffic logs is shorter than the actual time duration.
- **393301**—During Web authentication, when an ACK packet was received, the firewall erroneously sent a FIN packet to end the session.
- **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.
- **419564**—The ppp multi link bundle supports only two BRI channels.
- **427094**—Occasionally, the connection between the Catalyst switch and the Copper Gigabit interface with manual duplex setting is down.
- **427467**—[SSG 140] The device reboots unexpectedly because of ARP traffic across bgroup interfaces.
- **428914**—[ISG, NetScreen-5000] When Websense was enabled, access to certain websites dropped due to application error.
- **429239**—When the remote authentication server was primary, the authentication failback option did not function as expected.
- **431675**—The defragmentation limit is changed to support up to 65535 bytes of IP packet.
- **431762**—During an upgrade to Release 6.1.0r5, MGCP-related messages might appear on the console.
- **431944**—In transparent mode, MPLS pass-through traffic is dropped.
- **433456**—The original source and destination address are missing from the log to USB flash.
- **435348**—[SSG 5/20, SSG 140, SSG 500] The firewall could reset due to an exception before the boot up process. The device shows the exception dump.
- **439759**—When an access list that is tied to an RP configuration for multicast is not set, the firewall might reboot.
- **440546**—The antivirus scanning process might get stuck the SMTP sessions, if the client is using SMTP DSN (Delivery Status Notification) and the recipient's e-mail address contains word **QUIT**.
- **441723**—Firewall does not send TCP RST for traffic matched by IPv6 REJECT policies.

Performance

- **297405**—Inter-Vsys traffic are dropped if it do not pass through an ALG or ICMP.

Routing

- **258978**—For the SSG 320M/350M, the supported maximum number of Border Gateway Protocol (BGP) redistributed routes is 4096. However, if a large number of routes are added with an automated script, it is possible to exceed the supported limit. Routes entered or redistributed manually should not be able to exceed 4096.
- **398277**—OSPF adjacencies were lost due to an FPGA error.
- **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.
- **430932**—Secondary VPN Tunnel configured with point to multi-point OSPF stopped in ExStart.
- **440113**—IPv6 Neighbor solicitation messages from the source "::" are dropped by IP Spoofing.

Voice-over-Internet Protocol (VoIP)

- **310928, 314481**—In NAT mode, the security device might stop responding under heavy Media Gateway Control Protocol (MGCP) traffic.
- **421768**—When the H.323 ALG was enabled, the H.323 RAS admissionConfirm packets were dropped.

Virtual Private Network (VPN)

- **395216**—The fragmented packets of cross-chip ASIC VPN traffic were dropped.
- **395312**—When Baltimore Unitrust CA was used, the PKI negotiation using the SCEP failed.
- **430028**—The device reboots when auto renewal of the same SCEP key was performed.
- **433028**—The device reboots on its own when SCEP auto-renewal of the same key is performed.

WebUI

- **393022**—ECDSA signature authentication is missing from the authentication methods list in the IKE phase 1-proposal editing WebUI page.

Known Issues in ScreenOS 6.3.0

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

The known issues listed in this section are specific to ScreenOS 6.3.0r1. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

Flow

- **456996**—The syn-cookie does not function for IPv6 SYN packet with fragment header. This packet type is generated when IPV4 translates to IPV6 and the DF bit is not set in original V4 packet.

  This does not impact the IPv4 only deployment in any way. The syn-cookie feature can be used in IPv4 deployment. For IPv6 deployment, syn-proxy option can be used.

General Packet Radio Service (GPRS)

- **440783**—[ISG] The CPU does the GTP packet check only for the first GTP-DROP UserGtPdu and drops it correctly.

Hardware

- **440062**—On executing the set interface X/X phy link-down command on the JXU-1SFP-S card, the interface link status is erroneous. This is because the TX of fiber transceiver cannot be disabled on the JXU-1SFP-S card.

Intrusion Detection and Prevention (IDP)

- **313252** —On the ISG series device, when the Security Module is functioning in the TAP mode, then ScreenOS only transfers the first fragment of packets to Security Module.
- **436544** —The Security Module of the ISG series cannot detect certain DNS compound attack. This is because of the detector functionality.

Other

- **416822**— If you execute the CLI command save many times, there is no FBTL available to extend the flash life. Because this conflict with the FAT cluster

allocation process, it leads to logic flash block leakage. This will be fixed in the subsequent ScreenOS release.

- **453156**— ScreenOS crashes when the USB device mount fails. This occurs due to continued and repetitive execution of the get file command.
- **454916**— On a Jupiter chip, when clearing the ARP table several times with heavy VPN encryption traffic poured out, all of the VPN encrypted packets are sent to CPU for l2 entry reinstall. This causes a buffer leak.
  W/A—Reinitialize the ASIC. This can take up to three minutes.

Routing

- **430289**—On certain Virtual Routers, after configuring the interface rp candidate (interface xx mgroup-list yy;) if you configure the Virtual Router access-list (yy) in a range such as 231.6.0.1/32 to 231.6.0.100/32; then some groups cannot create (s,g) on untrust vrouter and some other groups cannot forward.

Voice-over-Internet Protocol (VoIP)

Security

- **431084**—Support for UDP and ICMP flood is not available on the aggregate interface.

Virtual Private Network (VPN)

- **423941**—When configuring overlapped proxy ids for route-based VPN, the IKEv2 negotiation might fail. The issue can be resolved if traffic selector narrowing is supported by IKEv2.
  W/A—The issue can be resolved if traffic selector narrowing is supported by IKEv2.
- **469089**—The VPN monitor does not function for a manual key VPN. This is because of adding a proxy id check on the packet sanity check, which is not required for a manual key VPN.

Limitations and Compatibility

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

Limitations of Features in ScreenOS 6.3.0

This section describes the limitations of some features in the ScreenOS 6.3.0 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 (For example, a cable is unplugged or the client is not closed normally) leaves the associated sessions open and leave an active entry in the admin table. The entries are not 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 experience load balancing issues. This second example is not a supported or recommended configuration.
- **Use of DIPs and SCTP multi-homing**—There are several Stream Control Transmission Protocol (SCTP) limitations when the ScreenOS devices uses DIPs.
  - When SCTP multi-homing is used with DIPs, there is source port translation error that results in erroneous source port translation and ultimately dropped traffic.
  - When DIPs are used in an SCTP multi-homing deployment, sessions cannot be immediately cleared when a shutdown message is received. Sessions are freed after a timeout.
  - When SCTP multi-homing is employed on a device using DIPs, not all sessions are synched by devices in an NSRP cluster.
  - When DIPs are used with SCTP multi-homing, SCTP heartbeat traffic is dropped by the device, thus the SCTP heartbeat function is not supported.
  - ScreenOS 6.3.0 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.

- **NetScreen-5000 series throughput stability**—For NetScreen–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, the TCP and UDP sweep screen sometimes reports 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 might cause the device to overheat, resulting in equipment damage and network outage.

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

- **Call unhold fails**—According to RFC 3261, a calling party shall use a=sendonly to hold a call and a=sendrecv to unhold 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 unhold 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 a telephony system issue that cannot be resolved by ALG. Hence, there is no work around for this issue available through a firewall. [300723].
- **Maximum number of OSPF Redistributed Routes**—For the SSG 320M/350M , the supported maximum number of Open Shortest Path First (OSPF) redistributed routes is 4096, but it might be possible to exceed the maximum. OSPF redistributed routes are handled in two parts: route task and OSPF task. The route task adds redistributed routes to OSPF continuously during one CPU time slice. The redistributed routes counter are not, however, updated until the OSPF task is processed by the CPU, so more routes might be added in OSPF when the routes are added using an automated script. Routes entered or redistributed manually should not be able to exceed 4096.[258979]

Documentation Changes

- Starting with the ScreenOS 6.3.0 documentation, the content presentation of the following guides is standardized to align with Juniper Technical Publications Standards:
  - *Concepts & Examples ScreenOS 6.3.0 Reference Guide*
  - *ScreenOS 6.3.0 IPv4 CLI Reference Guide*
  - *ScreenOS 6.3.0 IPv6 CLI Reference Guide*
  - *Upgrade Guide*

  Because of the alignment, the content presentation of ScreenOS 6.3.0 documentation differs from that of ScreenOS 6.2.0 and earlier documentation

Getting Help for ScreenOS 6.3.0 Software

For further assistance with Juniper Networks products, visit: www.juniper.net/customers/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.