Juniper Networks ScreenOS Release Notes

Release 6.3.0r16
December 2013
Revision 01

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 6.3.0r15, 6.3.0r14, 6.3.0r13, 6.3.0r12, 6.3.0r11, 6.3.0r10, 6.3.0r9, 6.3.0r7, 6.3.0r6, 6.3.0r5, 6.3.0r4, 6.2.0r15, 6.1.0r7, 6.0.0r8, and 5.4.0r26.

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.

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

- **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 in 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

    > ℹ️ 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.

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**
	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

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).

Dynamic Host Control Protocol (DHCP)

- **DHCP support**—The maximum number of DHCP relay agents supported is enhanced from 3 to 4.

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, advanced mode license is required to run it on the following devices:

  - ISG1000

  - ISG1000 with SM

  - ISG2000

  - ISG2000 with SM

- **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.

- **SIBR IPv6 Support**—Beginning with ScreenOS 6.3.0r13, the Source Interface-Based Routing (SIBR) feature supports IPv6 SIBR tables. When SIBR is enabled in a virtual router (VR), the security device performs route lookup in an SIBR routing table. The configuration of this feature remains the same, except for the fact that the interface gateway cannot be used as a next-hop if the IPv6 gateway parameter is not specified.

  The CLI command is updated as:**set vrouter <vr_name> route source in-interface <interface_name> <IPVX_addr1/mask> interface <interface_name> gateway <IPVX_addr2>**

- **Client-to-Site IPv6 VPN Support**—Beginning with ScreenOS 6.3.0r13, configuring IPv6 addresses from a server to a client is now supported with IPv6 IP pools. A new command has been introduced:**set ippool [ippool name]<ipv6 address> <ipv6 address>**.

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.

- **Boot Loader for SSG-140**—A new boot loader version Loadssg140v326.d has been released for SSG-140 platform. For more information, see the JTAC knowledge base number KB 23407 located at http://kb.juniper.net/KB23407

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

- **DSCP Marking for Self-Initiated Traffic**—Beginning in ScreenOS 6.3.0r12, you can configure IKE packets with DSCP values for self-initiated packets. During IKE module process negotiation, the configured IKE packets marked with the values can be used. To mark the IKE packets with the specified value, enable the service using the command **set ip service ike dscp <dscp-value>**.

- **DSCP Marking Based on Policy Configuration**—In ScreenOS 6.3.0r12, when a session matches a policy with DSCP enabled, the bidirectional traffic performs the DSCP marking.

  The DSCP feature is now enhanced to prevent DSCP re-marking packets that already have a DSCP value. This feature enables a DSCP group to have more than one DSCP value for a packet.

  The DSCP marking for each packet is checked to determine whether the DSCP value belongs to a DSCP group before the packet does the DSCP marking. If the DSCP value does not belong to a DSCP group, the device retains the packet's DSCP value.

  Low-End Platforms—For CPU-based platforms, all packets in the first path or fast path are checked for DSCP value and DSCP marking based on policy configuration. The configuration is effective in all conditions irrespective of whether the first packet matches the policy configuration or not.

  High-End Platforms—For high-end platforms, the DSCP marking for fast path is processed by the ASIC according to the session installed by the first path. Only the first

path is checked for the DSCP value to determine the DSCP marking based on policy configuration.

If the first packet arrives with an existing DSCP value and if the DSCP value does not belong to the DSCP group in the policy configuration, then the session will not perform DSCP marking for that packet. Subsequent packets in the session will also not have the DSCP marking done even if the DSCP value matches the DSCP group in the policy configuration.

> NOTE: If the policy has been configured as no-hw-sess in high-end platforms, then the implementation is same as in low-end platforms, as all the packets are processed by the CPU.

The DSCP group is used to classify traffic within the device and to classify a number of DCSP values having the same behavior as the configured DSCP group. The DSCP group allows you :

- To create a DSCP group and to define the DSCP group type. The maximum number of DSCP groups allowed per VSYS is 64. The DSCP group types are:

  - **Include**—Specifies adding or including the DSCP values to the configured DSCP group . By default, the DSCP value for a group is zero.

    set dscp-group name <group name> include

  - **Exclude**—Specifies to removing or excluding the DSCP values from the configured DSCP group. By default, the group contains 64 DSCP values.

    set dscp-group name <group name> exclude

- To configure a DSCP value for a policy. If a DSCP value is not configured for any policy, then you can insert a DSCP value into a DSCP group, or you can delete a DSCP value from a DSCP group.

  set dscp-group <group name> dscp-value <low number>-<high number>

- To display the DSCP group information.

  get dscp-group <group name>

- To bind a DSCP group to a policy for low-end platforms:

  Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic dscp enable <value> group-dscp <group name>

  Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic dscp enable group-dscp <group name>

  Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic dscp enable value <value> group-dscp <group name>

  Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic dscp enable group-dscp <group name>

- To bind a DSCP group to a policy for high-end platforms:

Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic priority <value> dscp value <value> group-dscp <group name>

Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic dscp value <value> group-dscp <group name>

Set policy from <zone_name> to <zone_name> <src_addr_name> <dst_addr_name> <service name> <action> traffic priority <value> group-dscp <group name>

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.

- **Adding Routes to BGP**—In ScreenOS 6.3.0r11, the Border Gateway Protocol (BGP) conditional advertisement feature supports route advertisement using different address family checks. By default, a BGP advertises the best routes in its routing table to its peers. You can use the BGP conditional advertisement feature by using the **check** option in **set vr** *<virtual-router-name>* **protocol bgp** command to configure conditional advertisement of BGP routes to a peer or a peer group in a different address family.

  BGP conditional advertisement is supported in IPv4 and IPv6 address families.

  - To configure and to advertise one IPv4 network route to peer and check the reachability of one IPv4 subnet or IPv6 subnet:

    set vr vr-1 protocol bgp ipv4 network *<ipv4_addr/mask>* check*<ipv4_addr/mask|pv6_add /prefix_length>*

  - To configure and to advertise one IPv6 network route to peer and check the reachability of one IPv4 subnet or IPv6 subnet:

    set vr vr-1 protocol bgp ipv6 network *<ipv6_addr/prefix_length >* check*<ipv6_addr/prefix_length | ipv4_addr/mask>*

  The conditional advertisement feature has been enhanced to include the following new configuration option and parameters to check the subnet of different address family:

  - **ipv4_addr/mask** — The IP address and subnet mask of the network. The subnet mask value indicates which bits of the address are significant. The mask does not have to be the same as the subnet mask used in the network. For example, 10.0.0.0/8 is a

valid network to be advertised by BGP. When the **check** option is used, ip4_addr1/mask1 can be a MIP address range.

- **ipv6_addr/prefix_length** — The IP address and prefix length of the network. The address is specified in hexadecimal format, using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

- **check**— Directs the device to check network reachability before advertising BGP peers.

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.

Virtual Private Network (VPN)

- **Enhancement to VPN support in VSYS**— The system can only support up to 16K static VPN tunnels in a VSYS. An enhancement was made to enlarge per-VSYS static tunnel capacity to the system max (25K) by preempting VPN group tunnels via environment variable "no-vpn-grp=yes".

- **Automatically Configuring a Local IPv6 Address for an IPv6 IKE Gateway**— In ScreenOS 6.3.0r11, you can automatically configure a local address for IPv6 IKE gateway.

  In order to configure an IPv6 IPsec tunnel, you must define the local IPv6 address in the IKE tunnel configuration. When you are configuring large number of devices, defining a local IPv6 address can be difficult. This enhancement enables you to automatically configure a local IPv6 address through DHCPv6 or IPv6 Stateless Address Auto Configuration (SLAAC) into the IKE tunnel configuration.

  To automatically configure a local address for an IPv6 IKE gateway, set the IPv6 address 0::0 as the local address in the following command:

  - For IKEv1

    set ike gateway *<name>* address *<peer-ipv6-addr>* aggressive outgoing-interface *<out-if-name>* local-address 0::0 preshare *<secret>* sec-level standard

Changes to Default Behavior

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

Changes to Default Behavior Introduced in 6.3.0

- **BGP Configuration** — After you upgrade from ScreenOS 6.1 to ScreenOS 6.3, only the connected route will be displayed in the routing table. However, the BGP route export will fail, because the firewall is not configured to the connected routes.

  To force the route export:

  ```
  set vrouter "trust-vr"
  set protocol bgp <protocol>
  [...]
  set ipv4 network <ip address> no-check
  [...]
  ```

Changes to Default Behavior Introduced in 6.3.0r13

- **NSRP Configuration**—The backup interface status (ifOperStatus) displays the state as **testing** when the physical interface status is UP and as **down** when the physical interface status is DOWN in an NSRP passive cluster member.

Changes to Default Behavior Introduced in 6.3.0r11

- **Public Key Infrastructure**— A new command is introduced to support manual certificate renewal process by using the same distinguished name without modifying the configuration but by updating the existing certificate in use by removing it.

  set pki x509 manual-renew

  To work on this feature, perform the following:

  - **Generate a key-pair**: If the key-pair with the DN is supported in PKI-store, then add a pad to PKI-store using **CN=NSMANAULRENEW** command to generate a new key-pair. As a result, there are two key-pairs in PKI-store.

  - **Generate a PKI request**: If there is a pad **CN=NSMANAULRENEW** already available in the DN for the key-pair, then remove the pad to generate PKI request. This is to ensure that the new certificate will have the same DN as the old certificate.

  - **Load the certificate**: The new certificate with the same DN replaces the old certificate.

- **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 6.3.0r8

- **IGMP packets compatibility** —A command was introduced to permit IGMP packets with TTL greater than one and to provide compatibility with other interoperability devices:

  set interface *<interface name>* protocol igmp no-check-ttl

- **Firewall can block packets with a Routing header**—Firewall has the ability to block packets with a routing header type 0. To avoid blocking all the routing headers, the firewall supports the routing header type filters using the following command:

  set service *< name>* protocol routing-ext-hdr type*<value>*

Changes to Default Behavior Introduced in 6.3.0r7

- **HMAC SHA-256 RFC 4868 compliance**—The previous implementation of HMAC SHA-256, incorrectly truncated the message digest at 96 bits. It now uses 128 bits, in accordance with RFC 4868.

Changes to Default Behavior Introduced in 6.3.0r5

- **IPv6 packet extension header**—To filter or deny the extension header with user-defined service, define the src-port and dst-port as wildcard 0-65535.

Changes to Default Behavior Introduced in 6.3.0r4

- **NSRP Configuration**—NSRP configuration is out of synchronization due to **set tftp source-interface <interface name>** command.

Changes to Default Behavior Introduced in 6.3.0r3

- **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.

- **Maximum timeout value of ipsec-nat alg**—The maximum value of **ipsec-nat alg timeout** has been changed from 180 to 3600 seconds.

- **VPN tunnel capacity for advanced license key**—On SSG550, the VPN tunnel capacity has been changed from 1000 to 2048 for advanced license key.

- **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 6.3.0r1

- 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 3.5.140185. For more information on the availability of new releases, see the Detector Engine 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:

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

The following operational issues from ScreenOS 6.2, 6.1, 6.0, and 5.4 release branches were resolved in this release:

Addressed Issues in ScreenOS 6.3.0r16

Others

- **769049** - An exception dump occurred when antispam and antivirus processes used too much system memory.

- **819171** - A brute force attack was triggered n+1 times its configured value.

- **888573** - [SSG5/SSG20] V.92 serial interface failed to reconnect when the call was terminated improperly.

- **892843** - The default router would be automatically deleted from the IPv6 routing table because the IPv6 routing table was not refreshed when the RA was received.

- **897651** - IKE congestion displayed an error while calculating ike_nego_activity_count, because of an incorrect behavior that was set when the commit-bit was enabled.

- **898323** - The device printed data buffer information logs on the console when it received a UDP packet larger than 4000 bytes.

- **901137** - If IPv6 was enabled, the RADIUS auth IPv4 server address could fail because of the server's inability to create a RADIUS socket.

- **901422** - VSD Group 0 was created when the VSD group configuration exceeded the valid ID threshold.

- **907339** - The MIP settings on the dialer interface did not appear in the system output for the **get config** commands on the console. Although these settings did appear in the WebUI output and in the **get interface dialer mip** command console output, after the firewall was rebooted these MIP settings disappeared.

- **908829** - The MSRPC traffic failed because the ALG did not parse some authentication fields.

- **918217** - While renewing its SCEP certificate, the primary device failed to update and remained in the pending state.

- **919797** - The device under test (DUT) crashed when it was rebooted because it attempted to re-enter an unprotected resource.

- **929757** - Event log messages regarding the mode change were not displayed in the Root VSYS when the cpu-limit/vsys-profile feature triggered a shared-to-fair mode transition due to a high CPU incident.

Security

- **861671** - The firewall rebooted automatically when changes were made to the policy through the WebUI.

- **879680** - The firewall crashed when it attempted to assign memory because of a bug in the web task logic.

- **882566** - The firewall failed when the Multicast PIM module referred to a null pointer.

- **884567** - The firewall dropped UDP packets because the PPUs froze when the firewall attempted to process fragmented traffic.

- **892915** - The user had to restart syslog by using **apply & reset connections** from WebUI because SSG140 with syslog enabled over TCP, periodically failed to send syslog messages.

- **893808** - The firewall accepted the subnet ID as the IP address of the interface.

WebUI

- **776323** - TACACS+ in transparent mode could not be configured through the WebUI.

- **877558** - The WebUI did not display complete data for the default option **All Routers** in the Policy List drop-down when the user navigated through **Network** > **Routing** > **PBR** > **Policy**.

- **904619** - In the WebUI, the VLAN zone could not be blocked when the user navigated through **Network** > **Zones** > **Edit**.

Addressed Issues from ScreenOS 6.3.0r15

CLI

- **664162** - Track IP configured through the CLI did not always reflect the correct configuration when displayed in the WebUI.

- **688061** - While saving a configuration using the **get config** > **tftp** command, g-arp was automatically added to the config file.

- **789133** - In the CLI configuration, the trap versions were displayed only when SNMP was configured with networks that used the /32 subnets.

Others

- **841084** - The firewall in NSRP failed when a subinterface was removed.

- **694835** - The device experienced an exception dump when running multicast traffic with PIM, because of a null pointer.

- **734260** - IPv6 packets were dropped incorrectly because of sequence number checking.

- **743657** - A large number of configured PBR policies took a long time to be built, which resulted in a watchdog timeout. This caused the device to perform a core dump.

- **746210** - NSM does not allow you to set a VSI interface with a value greater than 7.

- **770815** - Under certain conditions, the device rebooted unexpectedly during an SSH connection to the Infranet Controller.

- **807561** - Irrespective of the status of the link, an SNMP walk performed to check ipv6IfOperStatus on backup devices returned the interface status as UP.

- **812703** - Traffic forwarding through GRE over a route-based IPsec tunnel failed when traffic shaping was enabled.

- **819292** - ISDN failed, because the protocol packet response was very slow.

- **836499** - Adding an incorrect subnet mask IP address to a multi-cell policy resulted in deletion of other addresses in the multi-cell policy.

- **840476** - Some Real Time Objects (RTOs) were not synchronized between primary and backup devices while performing a major ScreenOS upgrade.

- **850527** - Occasionally, a new NSRP master was not connected to the Infranet Controller after an NSRP failover. The **Get infranet controller** command displayed the status as *Closed*.

- **853577** - The device performed a core dump and rebooted because of a MIP on the loopback interface.

- **857406** - The MSRPC traffic failed because the port values were not compared while an rpc_map_search was performed.

- **859608** - The SNMP traps were not triggered when the source IP-based session limit was reached.

- **862597** - While setting the source address and the destination address as negate in the intra-zone policy, the intrazone policy did not match with the configured policy, and it defaulted to a global policy.

- **865894** - Unable to delete L2TP users, even though the L2TP tunnels were inactive, because of an incorrect count of active L2TP users.

- **867748** - Unable to manage secondary firewall through the backup manage-ip interface.

- **869155** - When the mgt.1 interface was created, it was accidentally added to a VSD group. This caused a change in the MAC address of the mgt interface.

- **869675** - The device encountered an exception error when the WSF module took too long to process a large, corrupted packet.

- **869698** - Issuing the **save config to tftp a.b.c.d filename.txt** command, enabled flow vector profiling.

- **872130** - Return packets dropped while they were being forwarded from one node to another.

- **872593** - Traffic logs were not generated for TCP port 1503.

- **874372** - The device experienced an exception dump when an SSH process referenced a null pointer.

- **875123** - Some applications, like FTP, failed because of an incorrect TCP ACK sequence number when in an NAT environment.

- **876229** - A read error in a real-time clock (RTC) chip caused the device to reboot.

- **878809** - A multicast session got stuck because of a time sync.

- **879511** - The device experienced an exception dump when a user with read or write privileges had their access changed to root privileges.

- **880797** - FTP-Get service was unable to restrict FTP upload through the APPEND command.

- **884643** - When the ICMP-ANY service was set to never time out, ICMP sessions were not closed even after the ICMP-Reply was received.

- **896357** - An exception dump occurred because of a memory corruption in the SIP Via list.

Security

- **722000** - [ISG] IDP Security Modules in an NSRP cluster were not shown in the WebUI.

VPN

- **750452** - A policy-based VPN session lost its tunnel information because of a route change. As a result, the packet was forwarded incorrectly to an interface (instead of to a tunnel).

- **804902** - VPN packets with sequence numbers greater than 0xffffff00 created frq1 duplication, resulting in a MAC flood.

- **843507** - EAP authentication information was not cleared when clearing IKEv2 SA, causing an exception dump.

- **845065** - A VPN could get reset when using SHA-2 because of a mismatch between software and hardware sequence numbers.

- **863127** - OSPFv3 got stuck in the EX_START state in a route-based VPN tunnel that was using unnumbered tunnel interfaces.

WebUI

- **678784** - The WebUI stopped responding while dialer interfaces were being configured.

- **704897** - When a static mroute was configured from the WebUI, the OIF was not displayed if one of the interfaces was in a custom VR and the other was in a default VR.

- **812494** - SurfControl integrated Web filtering was configurable even for unlicensed versions through the WebUI.

- **849169** - The device experienced an exception dump when it tried a lookup for group addresses through the WebUI, where the group address zone ID referenced a null pointer.

Addressed Issues from ScreenOS 6.3.0r14

Admin

- **803487** - ScreenOS failed when the auth table was large and the **exec infranet controller check-sessions** command took longer than 30 seconds.

ALG

- **818193** - Ocassionally, the SIP call timer timed out SIP messages earlier than expected.

- **832693** - When a client initiated a session with the NFS server, the dummy port (created previously when the NFS server was used as an NFS client) does not allow the NFS control session to be processed by the SUNRPC ALG. This resulted in the blockage of the subsequent data sessions.

- **834945** - Harmless RPC traces were printed on the console.

- **840673** - The SIP call dropped after 45 minutes because the session expire header was not updated when the re-invite was sent.

Antivirus (AV)

- **842538** - AV scan performance was slow when trying to relay an HTTP 302 message if the connection mode is not a keep-alive.

Others

- **817379** - The SSG Series devices failed to handle the NSM packets that contained an 0xffff TCP checksum.

- **822847** - The system experienced a memory leak when the pass-through traffic required authentication.

- **831747** - Device encountered an exception error when pinging a multicast group address due to a NULL pointer being incorrectly referenced.

- **833083** - The southern hemisphere DST setting, which begins in October and ends in April, automatically got disabled at the end of October. This resulted in the incorrect time being displayed.

- **835602** - The PKI information synchronized with the backup information even though the rto-mirror for PKI was disabled.

- **839155** - Packets were matched incorrectly by debug flow filter when either src/dst ip or src/dst port were the same.

- **842055** - NSRP flaps and packet drops were encountered due to a dead lock between SLU engine and PPU, this further resulted in ASIC to reinit.

- **853718** - A packet drop occurred as a result of an incorrect TCP sequence calculation.

Routing

- **828964** - The learned OSPF routes were lost when the remote peer router-id was changed; and the peer box failed to obtain the correct network LSA.

Security

- **818620** - The command **unset ike gateway <gateway> xauth accounting server <server>** cannot be synchronized, especially after one of the devices were rebooted.

- **828168** - The NSRP backup firewall failed and then rebooted repeatedly.

VPN

- **800584** - The firewall failed to verify ECDSA signature.

- **823285** - The policy based VPN tore down after NSRP failover, with remote peer reporting antireplay errors.

- **830423** - After enabling IPv6, the IPsec VPN traffic was dropped.

WebUI

- **833871** - Updating DI from WebUI on backup did not get synchronized to the primary device.

- **833873** - The modified OSPF neighbor list value was not updated properly.

- **842738** - The DNS server could not be modified when the device was in transparent mode.

- **701694** - The root administrator lost read/write privileges while modifying the administrator password.

Addressed Issues from ScreenOS 6.3.0r13

ALG

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

Antivirus (AV)

- **803148**—Websites occasionally fail to open when the AV is enabled and the syn-ack packet has window size of 0.

Logging

- **804620**—Redirection of logs to an external website might stop, and, although more than 10 percent of free space is available, the following message appears: There is less than 10% space available in current active file.

Other

- **585488**—The firewall core was dumped and rebooted when the **tftp get tech > tftp** command was used.
- **587570**—The multicast outgoing interface (OIF) was calculated incorrectly.
- **681596**—Firewall or pass through traffic intermitted when high-end platforms reported increase in CPU5 drop counters.
- **730059**—The firewall rebooted unexpectedly when net-pak contains the wrong flag.
- **730138**—The console output displayed a slot_num(1) or chip_num(2) error.
- **742169**—The firewall rebooted spontaneously because of a duplicate session issue.
- **745496**—The server had a large TCP window, causing the Notify-conn-close to fail.
- **751579**— VLAN traffic on ASIC-based platforms in Layer-2 Transparent Mode was dropped when the VSYS bound to the VLAN group was deleted and the same VLAN group was referenced in another VSYS.
- **754606**—SYN flood protection was triggered even though the attack threshold was not reached.
- **771666**—When IPv6 and BGP were both enabled, it caused the firewall to core dump.
- **771827**—The device rebooted with a crash dump in the IKMPD task due to a memory leak.
- **771959**—The Infranet controller connection was disconnected on the firewall as a result of missing Keep Alive messages in a scenario with a large number of policy configurations on the firewall.
- **775604**—In an NSRP cluster, **dhcp server auto** did not work.
- **775844**—On SSG 520M and SSG 550M devices, the fan status occasionally appeared as **down**.

- **777402**—PPTP occasionally failed because of a route lookup failure in the cross-VR design of the child GRE session.

- **788853**—The firewall performed a core dump and rebooted because of a wrong parameter logic being used while generating logs.

- **789358**—On PIM interfaces, setting the **set int <phy link-down>** command did not keep the interface down even after a reboot.

- **796098**—When mirroring was configured on NS 2000 or ISG Series devices (including IDP-enabled devices), a TCP three-way handshake failed on the device during SYN proxy processing.

- **811257**—The NSRP backup device did not undergo a "never" timeout synchronization at session creation.

- **814516**—The SSG Series device did not start the PPPoE connection after NSRP failover.

Routing

- **768724**—In some instances, BGP routes failed to be advertised because of a broken SPF list.

- **783986**—When compatibility with RFC-1583 was set for OSPF and a network change occurred the device had to run several calculations for SPF.

Screen

- **790842**—The firewall performed a core dump and rebooted when the **set zone trust screen ip-spoofing include-default-route** command was executed.

SNMP

- **782678**—The device might send multiple traps for a single event, causing duplicate entries.

- **785140**—SNMP traps are not generated for a few Screen options.

- **807264**—In ScreenOS 6.3, when the SNMP listen port was configured, the change did not get updated and the default port value of 161 was retained.

VPN

- **780465**—The Ctrl+C option did not interrupt the output of the CLI through **get** commands.

- **783720**—After NSRP failover, the remote IPSec gateway might drop AH packets because of anti-replay protection.

WebUI

- **781483**—In the WeUI, several NHTB event-log pages are blank. Event logs do not display the correct number of entries per page.

- **793235**—In the WebUI, the Network > Interface Edit > OSPF page neighbor list from the Neighbor List drop down and then click drop-down menu and click Apply. However, the neighbor list drop-down menu setting is not updated after the Apply function, and the list does not appear on the device, which continues to display "None."

Addressed Issues from ScreenOS 6.3.0r12

ALG

- **678300**—Failed to translate IP on SET-PARAMETER within RTSP by ALG causes the video streaming to stop intermittently.

- **736470**—H.323 ALG was unable to handle cross vsys H.323 traffic.

- **752103**—RTSP SET_PARAMETER is not address translated.

- **771008**—Communictation failed when H232 ALG may change h245 address in the payload.

- **778810**—Policy change caused h323 alg hit a null pointer and device failed.

Authentication

- **778720**—Firewall stopped authenticating against RADIUS server.

Antivirus (AV)

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

Logging

- **740584**—When a sub-interface is created and cancelled an event message "MTU for interface has been changed to 1500." is displayed.

Management

- **726174**—Firewall might add additional padding to a reply packet.

- **737433**—The ifIndex value is not the same in standard MIB and Netscreen enterprise MIB while executing SNMP query for interfaces.

NSRP

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

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.

- **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.

- **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.

- **725966**—Firewall experiences core dump after HA fail over due to IKE-v2 parameter sync problem between the primary and the backup devices.

- **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.

- **728097**—On interface configuration, firewall is accepting network number (1.1.1.0/24) as an IP address.

- **728480**—Asymmetric traffic failed when IPv6 was enabled.

- **731534**—Firewall was spontaneously rebooting due to memory overwrite.

- **731582**—Debug flow drop, shows the packet information for the dropped packets.

- **732793**—Device might crash when you 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.

- **739175**—Illegal memory access causes spontaneous reboot of the firewall.

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

- **743309**—Multicast traffic can cause firewall to coredump.

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

- **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**—[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.

- **752246**—SCTP natted traffic might stop working when you set the envar x-in-ip.

- **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.

- **773293**—Harmless unnecessary debug message has been removed from the console output.

- **777142**—When performing snoop offset filter on VPN tunnel traffic firewall may crash.

- **777170**—After IPV6 was enabled there was high CPU on backup of NSRP firewall.

- **778730**—SIP ALG caused a system failure during a list erase function.

- **779261**—HA resync caused device with large configuration in NSRP failure.

- **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.

- **781815**—The new policy installation process was modified to be more compatible with NSM.

- **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.

- **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 arrives.

- **734361**—BGP neighbor parameter rejection command is deleted after BGP instance flap or upon reconnect.

SNMP

- **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.

VPN

- **705374**—IKEv2 failed in rekey after failover to backup.

- **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.

- **770471**—In WebUI, removing the configuration related to proxy-id was not possible.

- **780247**—Proxy ID mismatch between SA and policy was due to an endian issue.

WebUI

- **751661**—In PPPoA Interfaces WebUI the connect and disconnect buttons did not work.

- **777559**—In WebUI, event log was not showing the correct number of lines.

- **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 6.3.0r11

ALG

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

Antivirus(AV)

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

IDP

- **695082**—IDP module on the ISG platform used to hang when executing the command "get sm status".

Management

- **671719**—NSM was unable to update policy to device because sme_bulkcli was stuck.

- **687217**—Firewall failed when you run fprofile.

- **696588**—If SCP file transfer was used regularly then there was a high memory on firewall.

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

NAT

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

- **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.

NSRP

- **703949**—The expired tunnel sessions were not removed properly in a backup device.

Other

- **551755**—"IPv6 neighbor gateway [IP6] is reachable" was logged incorrectly when it is unreachable.

- **582089**—Pass through IPv6 IPSEC sessions are interrupted due to incorrect session timeouts set on ALG created child sessions.

- **592160**—After HA failover, the tunnel route pointing to the VPN stayed inactive for a long time by causing traffic loss on the new master.

- **599686**—FTP ALG did not work correctly when receiving unexpected ack from server, after the EPASV request from client.

- **661016**—when ACVPN was configured the device experienced a memory leak.

- **662330**—Asic classifier bug caused IGMP Query messages to trigger Source Route IP alert on ISG's.

- **662930**—Traffic through the IPSEC tunnel destined to one of the interfaces sometimes failed, because of reply packets getting sourced from tunnel interface IP.

- **675550**—When upgrading through tftp, the device might reboot with core dump.

- **686087**—Unable to bind an unnumbered tunnel interface within a VSYS if the VSYS name contains parenthesis.

- **686165**—If the IP of egress interface changed then existing sessions might not get updated with the new IP.

- **688228**—When layer 2 broadcast packet was received, it was incorrectly interpreted as Winnuke attack.

- **690786**—Unable to change the maximum number of sessions with envar command on ISG2000 box with advanced license and less than 2GB memory.

- **691510**—ASIC stopped forwarding traffic due to an issue with PPU-F.

- **692085**—Firewall was rebooted and core dumped due to multicast packets accessing the null pointer for a PIM neighbor.

- **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".

- **694306**—FW experienced high task CPU momentarily at polling times due to snmp task on 6.3. code.

- **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.

- **700331**—Firewall was rebooted and core dumped after adding VSD-Group.

- **700352**—DNS server cache snooping remote information disclosure is 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.

- **703689**—When DST was enabled and the system was rebooted, the SNMPv3 engine time was set to a higher value than the specified value in the RFC.

- **708406**—Firewall rebooted and core dumped due to accessing the invalid memory area.

- **709646**—Under a certain condition, Serial interface accepted traffic whereas Ethernet interface did not accept traffic.

- **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 occured.

- **724145**—During device reset, the custom NSM management port resets from 7900 to a default port of 7800.

- **727177**—Pass through IPsec sessions are not removed in NSRP VSD-less cluster.

Routing

- **686224**—BGP neighbor flapped at irregular intervals.

- **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.

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

- **592488**—Connection to VPN failed when the external IP changes on the NAT device that resides in-between VPN end points.

- **703677**—In redundant VPN configuration, OSPF did not come up during VPN failback from secondary to primary.

WebUI

- **676776**—WebUI was unable to display vrouter name, if the length was more than 15 characters.

- **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 6.3.0r10

ALG

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

- **679138**—RM resources are released incorrectly that subsequently causes RTSP traffic to drop.

IDP

- **697323**—Sometimes the security module stops forwarding the traffic due to a memory leak in IDP engine.

Management

- **578449**—Firewall was unable to connect to NSM using the first connect.

- **665355**—NSM supports "unset nsrp config sync vpn-non-vsi" command.

- **674637**—The firewall crashes sometimes when a long URL was described in custom category of sc-cpa.

- **675913**—SNMPwalk was not including logical interfaces in the output list for IFDESCR and IFNAME OIDs.

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.

- **574244**—Even after no preempt option was enabled, sometimes the device rebooted as master.

- **666641**—Data link was 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

- **578204**—Firewall forwarded duplicate log information to NSM due to an error in the session byte count.

- **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.

- **601364**—Interface physical link was brought up after reboot even after it was down.

- **610108**—IPv6 Auto-Discovered route was inactive when IPv6 over PPPoE is connected.

- **660288**—In non-HA mode, IPv6 multicast packet was dropped by the interface when ipv6 config is disabled. Do not consider VSI.

- **660950**—In NSRP Active or Active environment, PPTP might get disconnected unexpectedly.

- **662392**—Duplicate MAC addresses are returned in reports for the mac-tables of SSG bgroup interfaces.

- **662589**—Firewall experienced core dump and rebooted the system when accessing the Dlog process.

- **662930**—Traffic through the IPSEC tunnel destined to one of the interfaces sometimes fails, because of reply packets getting sourced from tunnel interface IP.

- **664485**—Policy might not compile exactly, when "negate" was used.

- **665008**—TCP connection was not established for MSRCP traffic in certain conditions, due to an endian issue.

- **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.

- **668859**—In SNMPv3 configuration, there was no option to specify the source interface.

- **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.

- **674245**—"Packet Too Big" message from ICMPv6 was dropped due to no session.

- **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 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 might cause crash dump and reboot unexpectedly.

- **677467**—Open SSH 5.8 client with pty-req greater than 256 bytes fails with "PTY allocation request failed" error.

- **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.

- **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.

- **687653**—Sometimes tftp fails due to save config (from device).

- **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.

Performance

- **607132**—Traffic might be affected by flow control mechanism on the interface.

Routing

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

Security

- **677385**—Transparent or L2 mode firewalls sends a SYN+ACK response packet to client with an all-zero MAC address.

VOIP

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

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

VPN

- **591501**—After reboot, the configuration pertaining to IKEv2 for EAP authentication was not preserved if the definition of the IKEv2 gateway name contained spaces.

- **604229**—IPv6 with IKEv2 VPN tunnel might not sometimes come up between the Motorola router and Juniper SSG device because of certain implementations.

- **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 was 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.

Addressed Issues from ScreenOS 6.3.0r9

Administration

- **580929**—Unable to add zone to proxy-id when zone name has a space.

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

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.

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.

- **607350**—Unable to retrieve the chassis slot information with SNMP walk.

Other

- **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.

- **574264**—Sometimes legitimate source IP address might be detected as an antispam blacklist IP address during high number of SMTP traffic.

- **578457**—SCP was not working on Ubuntu 10.10.

- **581190**—The device failed when memory was 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.

- **585139**—Sometimes device might reboot unexpectedly when certain TCP-based SIP traffic passed through the firewall.

- **585768**—SSH connections drop after 45 seconds of inactivity.

- **587433**—Sometimes after OS upgrade, the firewall might not start up because of certain condition in flash writing mechanism.

- **587809**—Negotiation event log was not generated when IKE phase one was initiated.

- **593583**—The device failed while processing SMTP traffic for Antispam.

- **595094**—In IPv6 environment, device might encounter HIGH flow CPU as IPv6 policy search algorithm might consume most of the FLOW CPU time.

- **596169**—SSG device running PPPoe core dumps when there was no DNS option defined in PPP control packet.

- **596585**—If IPv6 was 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.

- **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.

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

- **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.

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

- **606118**—Internal duplicate policy log entries caused the send mail task on the firewall to loop that subsequently caused high CPU usage.

- **610023**—[SSG300/500]Byte count for log-self shows wrong value.

- **610123**—ASIC stopped forwarding traffic due to shared memory corruption problem.

- **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.

- **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.

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.

- **588275**—Unable to clean up the RIP routes learnt from demand circuit in a VR.

VOIP

- **537064**—Corrected the tunnel policy search logic, after opening a pinhole in the firewall because sometimes the tunnel policy search failed.

VPN

- **590496**—Firewall does not respond to notification message when phase 2 proposals mismatch in IkeV2.

WebUI

- **562438**—In WebUI, the "dialup user group" for IKEv2 was disabled and cannot be configured.

- **596093**—Java Script WebUI display error was corrected in Internet Explorer 9.

- **614616**—The 6 to 4 tunnel end point IP address from WebUI will be rolled out by clicking Ok button.

Addressed Issues from ScreenOS 6.3.0r8

Administration

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

ALG

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

Antivirus

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

Authentication

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

CLI

- **574045**— A command was introduced to permit IGMP packets with TTL greater than one and to provide compatibility with other interoperability devices.

DNS

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

IDP

- **546621**— IDP AVT timeout parameters caused high task CPU. This problem was seen more in NSRP cluster.

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

- **530282**— sme_image caused high task CPU and NSM failed to update ISG-IDP.

Management

- **428710**— Deleting the source interface bound to NSM module resulted in trace errors or crash dump causing the device to reboot unexpectedly.

Other

- **487640**— Hardware counters did not work on NS-5000-2XGE-G4 [2 x 10GigE Secure Port Module (SPM)].

- **539351**— MS-RPC sessions failed because of a cold start sync failure caused by RPC process.

- **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.

- **570868**— The firewall rebooted unexpectedly because of an unexceptional read error in an incorrect packet buffer.

- **572707**— Firewall failed because of a malfunction while running SPF in the OSPF task.

- **576128**— The security module information with error "sm_get_cmd transmit timeout" could not be obtained because of memory leak on SM.

- **580534**— Auth table entries for the Infranet-auth policies was not maintained correctly for the VPN tunnel sessions.

- **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.

Routing

- **554973**— PBR was unable to route traffic using tunnel interface when it was in the up state.

VPN

- **550440**— With IKEv2, firewall had responded to the create_child_sa message from peer successfully but showed VPN status as inactive.

- **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.

- **579094**— IKEv2 with AES encryption in proposal failed because of incorrect attributes.

- **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.

- **581469**— When IKEv2 was executed, clients located behind some NAT devices were disconnected.

WebUI

- **578196**— Hardware version displayed 0(0) on the WebUI.

- **582678**— Creating admin user with special characters resulted in creating an invalid user.

- **585834**— While domain name had resolved many different IP addresses, Policy Elements Addresses character were sometimes shown as garbled.

Addressed Issues from ScreenOS 6.3.0r7

ALG

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

Antivirus

- **503330**—Firewall was unable to process packets with the error, "Cannot allocate memory logged with AV dropped due to scan-engine error code 10".

- **514358**—High memory utilization in the AV engine resulted in error, "Cannot allocate 36880 bytes of memory".

- **519926**—Firewall rebooted unexpectedly because of an error when processing packet in the AV engine.

- **548601**—When ASP received out-of-seq TCP packets, it did not send back ACK until all packets were received in sequence.

- **559335**—File download stopped intermittently when AV was enabled because of an error in the TCP proxy connection.

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

- **559694**—When concurrent session was large, there was intermittent high task CPU for a second, when an interface was added or removed.

- **568937**—The tunnel interface description command was not displayed in the "get configuration" output, and the configuration was lost after the firewall was rebooted.

Management

- **548025**—NHRP configuration was not supported in the config data file when managing through NSM.

- **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.

- **569631**—The admin name and password could not be changed or edited using NSM.

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.

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.

- **547040**—ASIC dropped multicast packet when the last hop PIM router with SPT disabled packet was received.

- **548257**—Traffic stopped passing due to session allocation failure in certain condition.

- **548464**—Sometimes the tcp traffic was delayed by 1ms, when the tcp traffic passed through the 10G IO card.

- **552417**—Incorrect calculation of string length caused the device to reboot unexpectedly.

- **552804**—Firewall failed during SPF calculation in OSPF V3.

- **555254**—Implemented the support for UDP based fragment on data session when the session was part of the ALG like SIP protocol.

- **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 which were connected to the same switch and when one of the members interface state changed to down.

- **567976**—Firewall failed when collecting the debug data for a split-brain condition due to an ASIC problem.

- **568304**—Firewall failed when the DNS refresh occurred and the policies were updated, which also updates the proxy ID for the policy-based VPN.

- **569540**—Incorrect time stamp was displayed in the event log message during the last 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.

- **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.

- **570710**—Firewall did not allow MIP IPs of the same range to be configured in different VSYS.

- **570948**—Firewall failed when it received a last fragment packet size of 64 bytes.

- **582278**—Firewall dropped the pass through PIM multicast traffic due to an error in a policy lookup process.

- **584381**—Firewall failed due to 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.

VoIP

- **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

- **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.

- **572352**—VPN tunnels failed with proxy-id mismatch error after upgrading from ScreenOS release 6.0r4 to ScreenOS release 6.3r5.

WebUI

- **519824**—A device failed when a reject message was configured for integrated surf control using WebUI containing more than 500 double byte characters.

- **538758**—During deletion of VPN modecfg profile, "Unknown keyword" error was displayed due to the missing quotes when the profile was created in WebUI.

- **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 sub interfaces.

Addressed Issues from ScreenOS 6.3.0r6

Administration

- **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

- **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

- **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.

CLI

- **541186**—The **set log exclude-id** command did not work for some of the event-types.

DI

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

DNS

- **531507**—The status of Domain Name Server (DNS) entry in the address book was incorrect.

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.
- **529696**—Under certain circumstances, with the HA link probe configured, the device sometimes rebooted unexpectedly when the status of the HA link changed.
- **538250**—Communication through the master node sometimes failed when exchanging the backup device through NSM doing 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.

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.

- **504566**—The device sometimes rebooted unexpectedly if a tunnel session was treated as a normal session.

- **524232**—RTSP ALG erroneously treated two different packets as a pair of translated packet and then dropped the packet.

- **526243**—The device rebooted unexpectedly due to CPU deadlock.

- **527319**—[SSG20]No link was present for Copper SFP running JXM-1SFP-S module.

- **530924**—PPP negotiations sometimes failed because of failure in adding a host route.

- **535171**—Firewall failed when it received an IPv6 packet for an IPv4 session cache entry during the sanity check process.

- **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.

- **537316**—The device rebooted unexpectedly during DNS refresh.

- **538370**—External authentication server support was added for FIPS mode.

- **538766**—The device rebooted unexpectedly due to IPv6 address double free issue.

- **539010**—Firewall failed when the policy pointer was NULL because of wrong packet tag between ASIC and CPU.

- **540038**—Sometimes, in NSRP Active/Active mode, asymmetric traffic was dropped.

- **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.

- **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.

- **548449**—Firewall displayed a Trace dump when **get config** command was run with OSPFv3 and IPv6 enabled.

- **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.

- **558643**—With FIPS enabled, device failed to boot after upgrading to 6.3r5.

Routing

- **441711**—RIPv2 failed to advertise routes to the neighbors after few hours of operation in a hub-and-spoke VPN setup.

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

- **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.

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.

VPN

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

- **533635**—Route-based VPN failover did not work because of an error in the route look up process.

WebUI

- **534271**—Predefined service timeout could not be edited using the WebUI.

- **535613**—In the WebUI, adding a VIP using a service name with an ampersand (&) resulted in "400 Bad Request" error.

- **535995**—Unable to add profile name or user-group name with a blank space in WebUI when configuring URL filtering.

- **536474**—Replacing the NSRP configuration using the WebUI including certain specific CLI sometimes caused unexpected behavior after reset.

- **546601**—Adding track IP in a vsys using WebUI resulted in error.

Addressed Issues from ScreenOS 6.3.0r5

The following operational issues were resolved in this release:

Administration

- **509654**—[SSG 140] TX/RX LED remained ON even after the **set interface ethernet0/X phy link-down** command was executed.

- **511835**—The configuration sometimes got deleted while configuring the administration setting for custom L2-zone.

Antivirus

- **523759**—The firewall rebooted with "Exception Dump" when AV was enabled on the policy.

Authentication

- **511019**—802.1X authentication failed after PC hibernation.

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

DHCP

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

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.
- **519838**—Both firewalls in NSRP cluster sometimes became master.

IDP

- **522728**—Under certain conditions, the traffic dropped because the inline-tap mode was changed to inline mode.

Management

- **505106**—Under certain conditions, the policies were marked as "invalid" because of NSM policy push operation.
- **520991**—After reboot, the **unset http skipmime mime-list** command was added to the configuration.
- **522075**—TCP sweep and UDP sweep screen options could not be configured using NSM because these options were missing in the ScreenOS config datafile.
- **522349**—Signatures with 30 or more characters were truncated when passed through the syslog output.
- **524380**—The ifOperStatus reports wrong value in the NSRP passive cluster member.
- **526797**—When DNS response was fragmented, the reason for session close in the traffic log became ageout.
- **529788**—NSM view statistics sometimes caused the device to reboot unexpectedly with dump.

NAT

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

Other

- **478573**—[SSG300] The device sent corrupted IP packets on reboot.
- **483101**—The Elliptical Curve Diffie-Hellman (ECDH) IKE implementation populated both group type and description in the Payload, and caused interoperability issue with third party VPN devices.

- **503307**—Application-Specific Integrated Circuit (ASIC) hung and stopped passing traffic due to incorrect session pointer.

- **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.

- **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.

- **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.

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

- **500993**—Issue with RSH when the application reused source port while closing control connection. The data traffic still existed.

- **533822**—When using SQL redirect, the ALG did not open the pinhole correctly.

Routing

- **528011**—In specific circumstances, BGP did not send updates on routes that were unreachable.

- **528417**—Redistributed default IPv6 route in OSPFv3 was not advertised after an hour of redistribution.

VoIP

- **529845**—With SIP ALG enabled, the firewall sometimes experienced high CPU.

VPN

- **469089**—The VPN monitor did not function for a manual key VPN because a proxy id check was added on the packet sanity check, which was not required for a manual key VPN.

- **506464**—Under certain conditions, the device sometimes rebooted unexpectedly because of RSA authentication.

Addressed Issues from ScreenOS 6.3.0r4

The following operational issues were resolved in this release:

Administration

- **467398**—Local root user sometimes lost root privilege when the remote admin used the same user name.

- **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.

- **504196**—SSH management sometimes disconnected abruptly when large output commands were executed.

- **508319**—The device sometimes rebooted unexpectedly when the memory got overwritten by the EAP task.

ALG

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

- **498869**—Fragmented MSRPC packets were supported in the ALG.

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.

CLI

- **484141**—System rebooted unexpectedly when **get sip transactions** command was executed.

DHCP

- **495244**—DHCP custom option 43 was sent with an invalid length.

HA & NSRP

- **515159**—The backup device used virtual MAC for ip tracking in a PPPoE environment using interface redundancy.

IDP

- **507318**—IDP Engine failed on security module and created core file.

- **513071**—With application identification enabled, invalid pointers had created an issue.

Management

- **491132**—ICMP packets to the management interface experienced delay at regular intervals.

- **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.

- **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.

Other

- **419637**—Many drop notification messages between IC and IE caused instability in the SSH connection between them.

- **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.

- **485192**—The GRE packets of PPTP session were dropped sometimes if PPTP server CALLID was set to 0.

- **488614**—The **set zone <zone name> tcp-rst** command did not work for SSH on high-end platforms.

- **491466**—SQL connections failed sometimes when the SQL ALG was enabled.

- **492796**—[NS5000] 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.

- **494276**—A URL blocked by Websense sometimes did not display the corresponding blocked message in the browser in an asymmetric routing environment.

- **494617**—ScreenOS devices managed by NSM version 2009 or above sometimes encountered memory leak issue.

- **494946**—[SSG 300] The alarm LED did not turn red when large ICMP packets were detected.

- **495554**—Firewall rebooted unexpectedly when the policies changed and read at the same time.

- **498529**—The SNMP get query for BGP related OID sometimes provided an incorrect output.

- **498562**—IPv6 did not work on PPPoE ADSL interface.

- **499421**—With edipi enabled, XAUTH user cannot inherit the IP information from old XAUTH session when rekeying new SA leading to memory leak.

- **500495**—With antispam enabled, e-mail with attachments greater than 3 to 4 MB sometimes dropped due to out of memory error.

- **500843**—Output of SNMP walk sometimes displayed incorrect interface for ARP table entries.

- **501256**—The Translated Dest column was empty when the traffic logs were saved using WebUI.

- **501343**—Even though there was no incoming traffic, alarm traffic for policy increased, because the self traffic was denied by the deny policy.

- **502419**—Traffic shaping statistics were not displayed on the NSRP VSI interfaces on the firewall.

- **504084**—The track IP failed sometimes when the interface was inactive.

- **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.

- **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.

- **509166**—SSG5 wireless device was not able to locate the best channel under certain conditions.

- **510473**—Typo in infranet **enforcer mode test** command resulted in syntax error after reboot.

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

- **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.

- **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.

- **520662**—Under certain conditions, the **get alg pptp xlat** command sometimes caused the device to reboot unexpectedly.

Performance

- **494910**—[SSG 140] In certain circumstances, when there was heavy traffic through the interface, all the traffic passing through the interface e0/9 was blocked.

Routing

- **501996**—In case of multiple virtual routers (VRs), sometimes, deleting a multicast route from one VR might not update information in the other VR causing the device to reboot unexpectedly.

- **504708**—With NSRP sync route enabled, the redistribution of routes from BGP to OSPF was delayed.

- **505962**—The RIP packets were constructed twice with the same RTE, but with different metrics.

- **501953**—The redistributed default route did not get advertised in the OSPFv3.

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.

VPN

- **441805**—The ikmpd task caused periodic high task CPU peaks.

- **500203**—ASIC based firewall sometimes stopped passing traffic when ESP packets with invalid SA value were received.

- **502729**—VPN failed to come up when the outgoing interface was a loopback interface.

- **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.

- **504014**—In some scenarios, VPN policy with MIP failed to translate Proxy ID.

- **505065**—VPN policy with domain name was not updating the right proxy-id after reboot.

- **508886**—Netscreen Remote Client for dial up VPN did not failover to redundant gateway when track-ip failed.

WebUI

- **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 an SA Series page.

- **502098**—Sometimes, the device rebooted unexpectedly when the vpn name was changed.

- **504696**—Potential unauthorized disclosure vulnerability was found, when the private address of the firewall was sometimes disclosed.

- **506282**—Whitelist URL was blocked by URL filtering because the code did not identify the port number (non 80) in the hostname header.

- **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 6.3.0r3

The following operational issues were resolved in this release:

Administration

- **417686**—Socket leak might occur when Internet Explorer (IE) with HTTPS was used for WebAuth management.

- **472816**—Sometimes the **clear socket <socket id>** command could not clear the tcp socket when it was in a certain state.

- **480480**—Under certain conditions, memory leak in the event log module caused high memory utilization.

- **481730**—The **get system** command displayed the hardware version as 0000(0)-(00) on SSG300 and SSG500 devices.

- **493627**—Under certain conditions, device might reboot unexpectedly when RPC (MS-RPC or SUN-RPC) traffic passes through the device and **show rpc map** command was executed.

Antivirus

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

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.

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, and hence caused 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 when both the MS-Time zone information element and a private extension were present.

- **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 and NSRP

- **472083**—When NSRP track-ip monitoring was configured within vsys, **configdata** file had incorrect track-ip information.

IDP

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

- **485928**—[ISG-IDP] The IDP engine resets due to application identification.

- **493618**—[ISG-IDP] IDP engine core dumps frequently due to DFA cache memory corruption.

Management

- **455186**—Firewall running OSPF rebooted unexpectedly after a delta configuration through NSM was performed.

- **456690**—The traffic log did not display IPv6 addresses correctly.

- **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.

- **468514**—Traffic log was not generated for a source or destination port equal to 1503.

- **468659**—E-mail notifications for logs from the firewall were not formatted correctly.

- **470754**—[NetScreen-5000] The redundant interface reported overflow errors when it was not initialized correctly after a system restart.

- **471298**—UDP MSRPC EnDPort mapper (MS-RPC-EPM) traffic incorrectly displayed the traffic log as MSRPC ENDPOINT MAPPER (TCP).

- **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.

- **485958**—Source interface of secondary NSM server was incorrectly removed from the configuration.

- **491026**—SNMP walk for certain MIBs did not return any value.

NAT

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

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

Other

- **463515**—MAC entries in the bgroup mac-table were not cleared after an interface went down.

- **465718**—Under certain conditions, the device might reboot unexpectedly when a Dial-Up user tried to connect.

- **466619**—The **set license-key auto-update** command rolled back to unset after a device reboot.

- **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.

- **472690, 264366**—ICMP flood screening option incorrectly dropped packet and generated alarm even when the packet rate was lower than the configured threshold.

- **477561**—The guaranteed bandwidth parameter was incorrectly allocated in traffic shaping.

- **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.

- **481096**—Enabling the set log audit-loss-mitigation feature caused the device to halt traffic after the log buffer was filled.

- **481805**—The bandwidth settings configured on the gigabit subinterfaces were not loaded after reboot.

- **484133**—With unknown protocol protection disabled, traffic with protocol number greater than 137 was dropped erroneously.

- **484169**—Firewall might reboot unexpectedly if GBIC card was not properly initialized during boot up.

- **484839**—In some scenarios, firewall might restart unexpectedly if **get alg pptp xlate** command was executed.

- **485332**—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 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.

- **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.

- **492544, 491555**—In certain situations, TCP-based SIP traffic in the environment could cause the firewall to reboot unexpectedly.

- **498306**—[SSG 300/500] Under certain conditions the firewall would reboot unexpectedly when UAC was configured.

Performance

- **413433**—[SSG-500] Internal sanity check caused higher CPU than expected resulting in intermittent packet drops.

- **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.

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

Routing

- **466158**—Capability negotiation error between BGP peers caused BGP to stay in idle state.

- **473625**—Under certain conditions, multicast traffic did not match the longest matching multicast group policy.

- **474158, 446155**—Change in RPF source route or change in route towards the RP was not reflected properly to the multicast routing table.

- **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.

VoIP

- **458341**—SIP ALG did not handle the SIP calls that used multi-part message as expected.

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

VPN

- **472618**—NS-Remote IPsec phase one negotiation failed when IKE ID was changed.

- **475831**—Quotation marks (" ") were removed from configuration when the **set vpn vpn_name bind zone "zone_name"** command was used.

- **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.

- **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.

- **486043**—Firewall might reboot unexpectedly when IKE/CLI and flow module accessed the NHTB table at the same time.

- **486608**—The **set vpn <vpn> dscp-mark <dscp>** command for manual VPN failed to set the DSCP marking for outgoing ESP packets.

- **489859**—In some scenarios, when the firewall was reset, the tunnel interface status remained down even when the security association (SA) was up.

- **494667**—Incorrect proxy-id with VPN Policy having MIP and overlapping source and destination address.

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.

- **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.

- **479160**—Unable to save AutoIKE configuration for VPN phase 2 in the WebUI when Proxy ID was enabled and vpn group was selected.

- **479440**—"unknown keyword ipv6" error was displayed when using VPN wizard for vpn setup with IPv6 disabled on the firewall.

- **480387**—"The value of time-out cannot be greater than interval" was displayed for certain interval values greater than the threshold values when creating Track IP entry using the WebUI.

- **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.

Addressed Issues from ScreenOS 6.3.0r2

The following operational issues were resolved in this release:

Administration

- **445491**—When displaying BGP route advertised without specifying a neighbor address, the error **bgp neighbor 0.0.0.0 doesn't exist** is displayed.

- **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 (AV)

- **458125**—In transparent mode, with the UTM enabled, when preparing a child session in the ALG traffic, the VLAN tag information was lost.

Authentication

- **416043**—The device did not clear the existing System Information Block (SIB) when the associated radio caused the wireless authentication failure.

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

Command Line Interface (CLI)

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

Deep Inspection (DI)

- **454303**—When a DI policy was enabled, and the ip-action was "notify", the packet that matched the DI group specified in the policy got dropped.

Domain Name System (DNS)

- **458316**—A device might reset if a vsys that contains address book objects with DNS names was deleted.

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

General Packet Radio Service (GPRS)

- **437975**—With GTP inspection enabled, at times, the GTP Echo Response might drop and the log displays the bad state message.

High Availability and NetScreen Redundancy Protocol (HA and NSRP)

- **448011**—Under certain conditions, WSF was not being updated in hardware session.

- **449011**—[SSG 140, SSG 300, SSG 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.

- **449858**—Non-VSI PPTP session was not functioning as expected in NSRP Active/Passive scenario.

- **454981**—[SSG 300M] When NSRP failover occurred, the red LED alarm was triggered.

- **461079**—[NetScreen 5000] The backup firewall would prematurely remove the sessions on the master in a VSD-less NSRP cluster and cross-ASIC traffics.

- **463752**—In NSRP Active/Active mode, if tcp syn-check was enabled, the user could not update the session after the three-way TCP handshake was complete.

Intrusion Detection and Prevention (IDP)

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

Management

- **455868**—[SSG Devices] Number of tasks has been increased on SSG devices to allow management to the device.

- **473110**—Format of IPv6 addresses were being sent incorrectly to NSM log viewer.

Network Address Translation (NAT)

- **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

- **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.

- **432190**—[NetScreen 5000 M3] VLAN retag did not work properly with 10 Gig interfaces.

- **437660**—Firewall reboots due to MGCP traffic.

- **448252**—[SSG 300] In transparent mode, the NMAP scan caused packet going across the firewall to drop.

- **449239**—SQL ALG did not function as expected when client request came into the SQL server's MIP address.

- **451051**—[ISG] Internal memory corruption caused ISG devices to stop creating new sessions and hence impacted traffic.

- **455183**—Few packets might be dropped due to ASIC reinit.

- **455373**—The device resets when some SQL ALG registers access an odd address.

- **455405**—ALG for FTP, RSTP, GTP, SQL, SIP, and RSH was corrupting the control packet which in turn was causing problems with the data packet.

- **459357**—WebAuth redirect from firewall contains a corrupted target URL when a proxy was used and the HTTP-request was split into two packets. The first packet includes the GET line and the second packet includes the HOST line.

- **460233**—With DST enabled, the e-mail notification time from ScreenOS was an hour ahead of the actual time.

- **461492**—When SQL IPMP failover was performed, subsequent traffic did not pass through the firewall.

- **462783**—Under certain conditions, sessions with timeout of 0 or 1 were never aged out of the firewall.

- **463422**—New TCP did not pass through the firewall in Transparent mode if there was no matching MAC table entry.

- **465223**—The **get gbe id 1** CLI command causes the device to reset.

- **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.

- **473279**—The **debug nsm nsp-debug** command might result in system reset.

Performance

- **455350**—MTU was set to 1500 when a tunnel interface causing performance issues was added to the interface.

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 IGMP v3 source specific report was sent.

- **448691**—BGP routes can get stuck in route table if two neighbors send the same prefix route and routes change frequently.

- **449723**—Firewall might reboot because of incorrect scheduling of SPF algorithm for the OSPF protocol.

- **459513**—Unable to set IPv6 static route to null interface.

Voice-over-Internet Protocol (VoIP)

- **422611**—Power Cycling H.323 IP Phone resulted in NAT pport leak.

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

- **442660**—Incorrect format of INVITE messages resulted in random failure of VoIP calls using SIP.

- **472554**—[SSG 140] Maximum number of NAT cookies has been increased to 512.

Virtual Private Network (VPN)

- **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.

- **452080**—The TCP 3-way handshake failed because of an error in the setup of IPsec VPN.

- **455520**—Tunnel interface was not created when route based VPN configuration was pushed from the NSM.

- **459053**—A logically down interface might still respond to VPN monitor packets sent by a VPN peer device, and hence not allowing the VPN state to go down.

- **459239**—Xauth information was erroneously removed when initial-notify was received.

- **474622**—[IKEv2] Tunnel IP address did not get released when Dial-Up IKE v2 SA was terminated.

- **474923**—[IKEv2] Rekey is unsuccessful when using Dial-Up VPN.

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.

- **463137**—IRDP cannot be enabled on interface e0/0 using the WebUI.

- **465697**—In certain conditions, the WebUI management causes 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 vpn entry from the WebUI.

Addressed Issues from 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.

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

- **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.

- **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

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 6.3.0r16

Others

- **920454** - SCCP does not function correctly when it is configured with a MIP.

Known Issues from ScreenOS 6.3.0r15

- None

Known Issues from ScreenOS 6.3.0r14

- None

Known Issues from ScreenOS 6.3.0r13

- None

Known Issues from ScreenOS 6.3.0r12

Other

- **782888**—OSPF routes synced on backup firewall are inactive after you perform unset or set protocol ospf enable command.

Known Issues from ScreenOS 6.3.0r11

ALG

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

Management

- **726174**—Firewall might add additional padding to a reply packet.

- **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.

Other

- **725966**—Firewall experiences core dump after HA fail over due to IKE-v2 parameter sync problem between the primary and the backup devices.

- **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.

- **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 is arrived.

- **739175**—Illegal memory access causes spontaneous reboot of the firewall.

- **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.

Routing

- **734361**—BGP neighbor parameter rejection command is deleted after BGP instance flap or upon reconnect.

VPN

- **740149**—VPN tunnel might fail to come up with AES192/256 in IKEV2, when one VPN peer is using 6.3r10 release and the other VPN peer is using 6.3r9 release or a below release.

Known Issues from ScreenOS 6.3.0r10

IDP

- **695082**—IDP Module on the ISG platform hangs when executing the command **"get sm status"** .

NSRP

- **703949**—The expired tunnel sessions were not removed properly in a backup device.

Other

- **582089**—Pass through IPv6 IPSEC sessions are interrupted due to incorrect session timeouts set on ALG created child sessions.

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

- **675550**—When upgrading through tftp,the device might reboot with coredump.

- **690786**—Unable to change the maximum number of sessions with envar command on ISG2000 box with advanced license and less than 2GB memory.

- **694306**—FW might experience high task CPU momentarity at polling times due to snmp task on 6.3. code.

- **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.

- **703949**—The expired tunnel sessions were not removed properly in a backup device.

VPN

- **592488**—Connection to VPN fails when the external IP changes on the NAT device that resides in-between VPN end points.

Known Issues from ScreenOS 6.3.0r9

DHCP

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

Management

- **578449**—Firewall was unable to connect to NSM using the first connect.

Other

- **601364**—Interface physical link is brought up after reboot even after it is down.

- **610108**—IPv6 Auto-Discovered route is inactive when IPv6 over PPPoE was connected.

- **662930**—Traffic through the IPSEC tunnel destined to one of the interfaces sometimes fails, because of reply packets getting sourced from tunnel interface IP.

- **664485**—Policy might not compile exactly, when "negate" is used.

- **666370**—Incorrect destination port is 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.

Performance

- **607132**—Traffic might be affected by flow control.

VPN

- **591501**—After reboot, the configuration pertaining to IKEv2 for EAP authentication was not preserved if the definition of the IKEv2 gateway name contained spaces.

WebUI

- **665076**—The maximum number of DHCP relay agents supported for WebUI/NSM is increased from 3 to 4.

Known Issues from ScreenOS 6.3.0r8

ALG

- **537064**— Corrected the tunnel policy search logic, after opening a pinhole in the firewall because sometimes the tunnel policy search might fail.

Management

- **610023**— [SSG300/500]Byte count for log-self shows wrong value.

Other

- **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.

- **587433**— Sometimes after OS upgrade, the firewall might not start up because of a certain condition in flash writing mechanism.

- **596585**— If IPv6 is not enabled on incoming interface, the multicast link local packet such as NA will not be considered as a to-self packet, and the device will forward these packets.

- **599609**— The "in packet" and "in ucast" counter keeps increasing, though the physical interface is down.

UTM

- **574264**— Sometimes legitimate source IP address might be detected as an antispam blacklist IP address during high number of SMTP traffic.

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

VoIP

- **585139**— Sometimes device might reboot unexpectedly when certain TCP-based SIP traffic passes through the firewall.

VPN

- **587809**— Negotiation event log is not generated when IKE phase one is initiated.

WebUI

- **562438**— In WebUI, the "dialup user group" for IKEv2 is disabled and cannot be configured.
- **596093**— Java Script WebUI display error is corrected in Internet Explorer 9.

Known Issues from ScreenOS 6.3.0r7

Admin

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

Antivirus

- **529357**—Firewall drops management traffic while the antivirus database was getting updated.

Authentication

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

CLI

- **574045**—A new command is introduced to permit IGMP packets with TTL greater than one and provide compatibility with other interoperability devices.

DNS

- **580838**—If Jumbo frame support is enabled, fragmented DNS packets fail to pass through device.

IDP

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

Management

- **428710**—Deleting the interface which is being bound to NSM module as source interface might cause trace errors or crash dump causing the device to reboot.

Other

- **487640**—Hardware counters are not working on NS-5000-2XGE-G4 [2 x 10GigE Secure Port Module (SPM)].

- **539351**—MS-RPC sessions fail due to a cold start sync failure caused by RPC process.

- **554007**—Sometimes, the device might fail due to a particular type of packet.

- **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.

- **570868**—Firewall reboots due to unexceptional read error in a wrong packet buffer.

- **572707**—Firewall fails due to a malfunction while running SPF in the OSPF task.

- **576128**—Cannot get security module information with error "sm_get_cmd transmit timeout" because of memory leak on SM.

- **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 an up state.

- **561446**—OSPF neighbor flaps due to a problem with the OSPF update task on a system level device.

VPN

- **479677**—Each VSYS can only use up to 16K tunnels.

- **550440**—With IKEv2, netscreen firewall responds to **create_child_sa** message from peer with success but shows VPN status as inactive.

- **579094**—IKEv2 with AES encryption in proposal fails due to incorrect attributes.

- **581469**—While running IKEv2, clients located behind some NAT devices might get disconnected.

WebUI

- **585834**—While domain name resolves many different IP addresses, Policy Elements Addresses character might show as garbled.

Known Issues from ScreenOS 6.3.0r6

The known issues listed in this section are specific to ScreenOS 6.3.0r6. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

None.

Known Issues from ScreenOS 6.3.0r5

The known issues listed in this section are specific to ScreenOS 6.3.0r5. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

None.

Known Issues from ScreenOS 6.3.0r4

The known issues listed in this section are specific to ScreenOS 6.3.0r4. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

Other

- **442729**—Traffic might stop on an interface when the system chip fails.
- **518253**—[SSG Series] Mapped IP (MIP) of the firewall does not respond to ARP query with source IP of 0.0.0.0.

VPN

- **506464**—Under certain conditions, the device might reboot unexpectedly related to RSA authentication.

Known Issues from ScreenOS 6.3.0r3

The known issues listed in this section are specific to ScreenOS 6.3.0r3. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

None.

Known Issues from ScreenOS 6.3.0r2

The known issues listed in this section are specific to ScreenOS 6.3.0r2. For the known issues identified for previous ScreenOS releases, see the Release Notes for the specific release.

Antivirus (AV)

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

DHCP

- **484087**—The destination IP is incorrectly set to 0.0.0.0 when DHCP relay agent receives a DHCP ACK in response to a DHCP INFORM.

General Packet Radio Service (GPRS)

- **448582**—GTP inspection drops the SGSN Context Response message if the Next Extension Header type is 0xC2 (Suspend Response).

- **456358**—The Common Flags GTP Information Element is not removed when **set remove-r6** command is configured.

- **457093**—For a new GTP tunnel, if a CreatePdpRequest does not receive any response, then the already used TEIDs cannot be reused for a certain time period. This can result in the dropping of CreatePdpRequests from an SGSN that reuses these TEIDs before a certain time period.

- **472199**—When R6 IE removal is enabled, GTP CreatePdpRequest packets get corrupted if they contain both the MS-Timezone information element and a private extension.

- **485578**—The GTP remove-r6 feature removes the mandatory RAI IE from SGSN Context Request and Identification Request messages.

- **486613**—When GTP traffic drops, the **bad system status** message appears in the log.

Intrusion Detection and Prevention (IDP)

- **485928**—[ISG-IDP] The IDP engine resets due to application identification.

Management

- **466692**—Certain IPv6 Index value is reported as incorrect.

Network Address Translation (NAT)

- **480667**—The firewall allocates only 2000 MIPs to an interface even when all the user ids configure MIP in one shared interface.

Other

- **468514**—Traffic log is not generated for a source or destination port equal to 1503.

- **471298**—UDP MSRPC EnDPort mapper (MS-RPC-EPM) traffic incorrectly displays its traffic log as MSRPC ENDPOINT MAPPER (TCP).

- **472433**—Packet might be corrupted due to ASIC buffer problem.

- **472690**—At times, ICMP flood might generate false alarm.

- **481096**—Enabling **set log audit-loss-mitigation** feature causes device to halt traffic after log buffer is filled.

- **481805**—After reboot, bandwidth settings configured on gigabit subinterfaces are not loaded.

- **484133**—With unknown protocol protection disabled, traffic with protocol number greater than 137 is erroneously dropped.

- **484839**—Firewall might fail if **get alg pptp xlate** command is executed.

Performance

- **478205**—When large amount of WebAuth transaction happens at a time, some HTTP SYN packets might be dropped during TCP 3-way handshake without returning SYN and ACK packets.

Routing

- **480470**—BGP anti-flap processing is removed from the backup NSRP node.

Virtual Private Network (VPN)

- **472606**—False replay protection alarm occurs when the sequence number is updated incorrectly due to race condition between the rekey process and the update from ASIC.

- **472618**—NS-Remote IPsec phase one negotiation might fail if IKE ID is changed.

- **475831**—Quotation marks (" ") are removed from the configuration when using the **set vpn vpn_name bind zone "zone_name"** command.

- **480642**—User cannot pair a VPN policy when multiple MIPs are used as destination.

- **480691**—The VPN tunnel down message (for example, VPN *<vpn-name>* from *<IP-address>* is down) is not generated in the event log when the NSRP backup device becomes the master.

- **489859**—After the firewall is reset, the tunnel interface is down, even though the security association (SA) is up.

Known Issues from 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.

Errata

This section lists outstanding issues with the 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 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 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 global **scan-mgr** command is not supported for the ScreenOS 6.x release:

  set av scan-mgr queue-size

- 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 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 information in the *VLAN-Based Traffic Classification* chapter of the 6.2.0 and 6.3.0 *Concepts & Examples ScreenOS Reference Guide*: example currently contains the following incorrect information:

  VLAN Group Name: v10

  Start: 10

  End: 10

  Network > VLAN > Group > Edit (for group v10)

  Interface Name: (select) ethernet2/1

  set vlan group name v10

  set vlan group v10 10 10

  set vlan port eth2/1 group v10 zone v1-trust

  set vlan port eth2/2 group v10 zone v1-untrust

  set policy from v1-trust to v1-untrust any any any permit

  set vlan retag name secure_vlan 10 20

  set vlan retag name secure_vlan 10 20 untag

  set vlan port eth2/1 retag secure_vlan

To configure the examples, make the following corrections to the CLI commands as follows:

VLAN Group Name: v20

Start: 20

End: 20

Network > VLAN > Group > Edit (for group v20)

Interface Name: (select) ethernet2/2

set vlan group name v20

set vlan group v20 20 20

set vlan port eth2/1 group v20 zone v1-trust

set vlan port eth2/2 group v20 zone v1-untrust

set policy from v1-trust to v1-untrust any any any permit

set vlan retag name secure_vlan 10 20

set vlan retag name secure_vlan 10 20 untag

set vlan port eth2/2 retag secure_vlan

- In the *Transport mode IPsec VPN* section of the *Site-to-Site Virtual Private Networks* chapter ScreenOS 6.3.0, *Concepts & Examples ScreenOS Reference Guide* the *Figure 234: Transport Mode IPsec VPN* incorrectly states the Gateway 2 values as "lo3: 4.4.4.4/32 and lo4: 4.4.4.5/32" which must be corrected to "lo1: 6.6.6.6/32 and lo2: 6.6.6.7" and the following information is missing in Gateway - 1 and Gateway - 2 Configurations. To successfully configure the example, make the following corrections to the configurations:

Gateway-1 Configuration:

1. **IKE Configuration on host-1 and host-2**

   set ike gateway gateway1 address 1.1.1.1 aggressive outgoing-interface loopback.1 preshare test1 sec-level standard
   set ike gateway gateway2 address 1.1.1.10 aggressive outgoing-interface loopback.2 preshare test1 sec-level standard

2. **VPN Configuration on host-1 and host-2**

   set vpn v1 gateway gateway1 transport sec-level standard
   set vpn v2 gateway gateway2 transport sec-level standard

3. **Proxy configuration for v1 and v2**

   set vpn "v1" proxy-id local-ip 4.4.4.4/32 remote-ip 6.6.6.6/32 "ANY"
   set vpn "v2" proxy-id local-ip 4.4.4.5/32 remote-ip 4.4.4.7/32 "ANY"

4. **MIP Configuration**

   set interface loopback.1 mip 3.3.3.3 host 6.6.6.6
   set interface loopback.2 mip 3.3.3.4 host 6.6.6.7

5. **IKE Configuration for GW-2**

set ike gateway s1 address 6.6.6.6 aggressive outgoing-interface loopback.3 preshare
 test1 sec-level standard
set ike gateway s2 address 6.6.6.7 aggressive outgoing-interface loopback.4
preshare test1 sec-level standard

6. **VPN Configuration for s1 and s2**

set vpn v3 gateway s1 transport sec-level standard
set vpn v4 gateway s2 transport sec-level standard

7. **DIP Configuration**

set interface eth2 ext ip 4.4.4.4 255.255.255.255 dip 10 4.4.4.4 4.4.4.4
set interface eth2 ext ip 4.4.4.5 255.255.255.255 dip 11 4.4.4.5 4.4.4.5

8. **Policy Setup**

Outgoing policy

set policy id 3 from trust to untrust "1.1.1.1" "3.3.3.3" any nat src dip-id 10 tunnel vpn
 v3
set policy id 4 from trust to untrust "1.1.1.10" "3.3.3.4" any nat src dip-id 11 tunnel vpn
 v4

Incoming policy

set policy id 1 from trust to untrust "1.1.1.1" "(MIP)3.3.3.3" any tunnel vpn v1
set policy id 2 from trust to untrust "1.1.1.10" "(MIP)3.3.3.4" any tunnel vpn v2

> NOTE: Users need to configure the outgoing policy before configuirng
> the incoming policy. This is because we do policy search twice, the first
> one is to check the incoming packet, and the second one is to find
> another VPN (the outgoing VPN) through which we send the packet.

9. **Flow check**

set flow ply-chk-self-out-tunnel

Gateway-2 Configuration:

1. **IKE and VPN Configuration to Server-PC**

set ike gateway gateway1 address 5.0.0.1 aggressive outgoing-interface lo.3 preshare
 test sec-level standard
set ike gateway gateway2 address 5.0.0.2 aggressive outgoing-interface lo.4 preshare
 test sec-level standard

2. **VPN Configuration on server-1 and server-2**

set vpn v3 gateway gateway1 transport sec-level standard
set vpn v4 gateway gateway2 transport sec-level standard

3. **Proxy configuration for v3 and v4**

set vpn "v3" proxy-id local-ip 3.3.3.3/32 remote-ip 1.1.1.1/32 "ANY"
set vpn "v4" proxy-id local-ip 3.3.3.4/32 remote-ip 1.1.1.10/32 "ANY"

4. **Reversed MIP (Traffic Is from Untrust to Trust)**

set interface lo.3 mip 7.7.7.7 host 4.4.4.4
set interface lo.4 mip 7.7.7.8 host 4.4.4.5

5. **IKE and VPN configuration to GW-1 (Client-PC)**

set ike gateway h1 address 4.4.4.4 aggressive outgoing-interface lo.1 preshare test
sec-level standard
set ike gateway h2 address 4.4.4.5 aggressive outgoing-interface lo.2 preshare test
sec-level standard

6. **VPN Configuration on host-1 and host-2**

set vpn v1 gateway h1 transport sec-level standard
set vpn v2 gateway h2 transport sec-level standard

7. **MIP**

set interface lo.1 mip 6.6.6.6 host 5.0.0.1
set interface lo.2 mip 6.6.6.7 host 5.0.0.2

8. **Policy Setup** Outgoing policy

Outgoing policy

set policy id 7 from untrust to trust "4.4.4.4" "6.6.6.6" any tunnel vpn v3
set policy id 8 from untrust to trust "4.4.4.5" "6.6.6.7" any tunnel vpn v4

Incoming policy

set policy id 5 from untrust to trust "4.4.4.4" "(MIP)6.6.6.6" any tunnel vpn v1
set policy id 6 from untrust to trust "4.4.4.5" "(MIP)6.6.6.7" any tunnel vpn v2

9. **Flow check**

set flow ply-chk-self-out-tunnel

- 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 the *Denial of Service Attack Defenses* chapter in the *ScreenOS 6.3.0 Concepts & Examples ScreenOS Reference Guide* Teardrop Attack section is correct when the firewall expects 548 (Including IP header) but contains 528 (excluding IP header).

  When the sum of the offset and size of one fragmented packet differ from that of the next fragmented packet, the packets overlap, and the server attempting to reassemble the packet can crash, especially if it is running an older operating system that has this vulnerability. After you enable the Teardrop Attack SCREEN option, and when the device detects this discrepancy in a fragmented packet. The packets are dropped.

- The following information is updated in Denial of Service Attack Defenses Chapter in the Concepts & Examples ScreenOS Reference Guide:

  In the Attack threshold, Alarm Threshold, Source Threshold, and Destination Threshold sections the statement same destination address and port number must be updated as same destination address and ingress interface port (physical port or logical port like sub interface) in all the occurrences.

  The following is the list of updated thresholds:

  - **Attack Threshold**—Attack threshold is triggered based on same destination IP plus same Ingress Interface Port (physical port or logical port like sub interface) per sec required to activate the SYN proxying mechanism.

    NOTE: Threshold is not triggered based on Transport Layer ports (TCP ports or UDP ports).

    For example, if Attack threshold is 20, so if there are 20 PPS to same destination IP and on same Ingress interface, then the ATTACK threshold will be triggered. However, if there are 20 PPS to the same destination, but distributed among multiple incoming interfaces, then ATTACK threshold will not be triggered.

  - **Alarm Threshold**—The value you set for an alarm threshold triggers an alarm when the number of proxied, half-completed connection requests to the same destination address and ingress interface port (physical port or logical port like sub interface) per second exceeds that value. For example, if you set the SYN attack threshold at

2000 SYN segments per second and the alarm at 1000, then a total of 3001 SYN segments to the same destination address and ingress interface port (physical port or logical port like sub interface) per second is required to trigger an alarm entry in the log.

For each SYN segment to the same destination address and ingress interface port (physical port or logical port like sub interface) in excess of the alarm threshold, the attack detection module generates a message. At the end of the second, the logging module compresses all similar messages into a single log entry that indicates how many SYN segments to the same destination address and ingress interface port (physical port or logical port like sub interface) arrived after exceeding the alarm threshold. If the attack persists beyond the first second, the event log enters an alarm every second until the attack stops.

- **Source Threshold**—This option allows you to specify the number of SYN segments received per second from a single source IP address—regardless of the destination address and ingress interface port (physical port or logical port like sub interface)—before the security device begins dropping connection requests from that source.

  Tracking a SYN flood by source address uses different detection parameters from tracking a SYN flood by destination address and ingress interface port (physical port or logical port like sub interface). When you set a SYN attack threshold and a source threshold, you put both the basic SYN flood protection mechanism and the source-based SYN flood tracking mechanism in effect.

- **Destination Threshold**—This option allows you to specify the number of SYN segments received per second for a single destination IP address before the security device begins dropping connection requests to that destination. If a protected host can be reached through multiple ingress interfaces, you might want to set a threshold based on destination IP address only—regardless of ingress interface

  Tracking a SYN flood by destination address uses different detection parameters from tracking a SYN flood(Attack Threshold) where destination address plus ingress interface port (physical port or logical port like sub interface) is used. Consider the following case where SYN Flood Attack threshold is 20, and Interface 1 as well as Interface 2 are the ingress interfaces to reach the same server. An attacker sends 19 PPS to Interface 1 and 19 PPS to Interface 2; neither set of packets (where a set is defined as having the same destination address and same ingress interface) activates the SYN proxying mechanism. The basic SYN flood attack mechanism (ATTACK Threshold) tracks destination address and ingress interface (physical or logical like sub interface), and neither set exceeds the attack threshold of 20 pps. However, if the destination threshold is 20 pps, the device treats traffic with same destination address to both the ingress interfaces as members of a single set and rejects the 21st packet—on Ingress Interface 1 or Ingress interface 2 to that destination.

- In Setting a Service Timeout section of Concepts & Examples ScreenOS Reference Guide, the behavior of timeout value function is as follows:

  - For 5.3.0r2 and earlier releases, when a policy is configured with multiple services or groups and if the matched service has an overlapped service timeout then the option is to select the last service timeout configured.

- From 5.3.0r3 and later releases, when a policy is configured with multiple services or groups and if the matched service has an overlapped service timeout then the option is to select the first matching service in the policy in alphabetical order.

  For more information see the JTAC Knowledge base number KB11970 located at http://kb.juniper.net/KB11970 .

- 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 information in Configuring Active/Active NSRP in Transparent Mode chapter is incorrect:

  2. Cluster and VSD Groups for Device B

  set interface ethernet2/7 zone ha

  set interface ethernet2/7 zone ha

  set interface ethernet2/8 zone ha

  set nsrp cluster id 7

  unset nsrp vsd id 0

  set nsrp vsd id 7 priority 100

  set nsrp vsd id 7 preempt

  set nsrp vsd id 7 priority 50

  set nsrp vsd id 7 preempt

  set nsrp rto-mirror sync

  The correct information is mentioned as follows:

  2. Cluster and VSD Groups for Device B

  set interface ethernet2/7 zone ha

  set interface ethernet2/8 zone ha

  set nsrp cluster id 7

  unset nsrp vsd id 0

  set nsrp vsd id 5 priority 100

  set nsrp vsd id 5 preempt

> set nsrp vsd id 7 priority 50
>
> set nsrp vsd id 7 preempt
>
> set nsrp rto-mirror sync

- The following information is missing from the *Route-cache* section of the "Routing" chapter in the *Concepts & Examples ScreenOS Reference Guide* for ScreenOS release 6.3.0:

  > **(i)** NOTE: We do not recommend that route-cache be enabled in dynamic routing and route flap scenarios.

- In ScreenOS 6.3.0 Concepts & Examples ScreenOS Reference Guide, *Policy-Based Routing* chapter, *Configuring an Extended Access List* section is updated with WebUI procedure for the creation of access list 20.

- In ScreenOS 6.2.0 and 6.3.0 Concepts & Examples ScreenOS Reference Guide, Deep Inspection chapter, Brute Force Attack Objects section, table 11 incorrectly lists the protocols supported to prevent against brute force attack. The protocols that are supported against the brute force attack depend on the protocol anomaly attack object that is included in the DI signature database. The latest DI signature database protocols supported are FTP, POP, IMAP, and HTTP.

- In ScreenOS 6.0.0, 6.1.0, and 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 6, Voice-over-Internet Protocol*, in the *SIP Headers* section, the *Requesting Messages with NAT* table contains the following incorrect information:

  - For the Outbound Request (from private to public) message type, the action for the Route field is Replace ALG address with local address.

    The correct action for Route is Replace local address with ALG address.

  - For the Outbound Request (from private to public) message, the action for the Call-ID field is Replace ALG address with local address.

    The correct action for Call-ID is None.

  - For the Outbound Response (from public to private) message type, the action for the Call-ID field is Replace ALG address with local address.

    The correct action for Call-ID is None.

- In ScreenOS 6.0.0, 6.1.0, and 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 6, Voice-over-Internet Protocol*, in the *SIP NAT Scenario* section, the value for Call-ID should not change between the internal and external networks in the *SIP NAT Scenario 1* and *SIP NAT Scenario 2* figures.

- In ScreenOS 6.0.0, 6.1.0, and 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 6, Voice-over-Internet Protocol*, in the *SIP Headers* section, the following sample SIP request message field is not supported, because ScreenOS does not perform NAT for the Call-ID header in the SIP ALG:

  Call-ID: a12abcde@*10.150.20.3*

- In the ScreenOS 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 4 Attack Detection and Defense Mechanisms*, in the *AV Resource Allotment* section, the following note is incorrectly documented for the WebUI:

  NOTE: You must use the CLI to configure this option.

  The correct information is:

  Security > Antivirus > Global: In the AV Scanner Global Settings, change the *Maximum AV Resources Allowed per AV Client* value (70% by default), and then click **Apply**.

- In the ScreenOS 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 4 Attack Detection and Defense Mechanisms*, in the *Fail-Mode Behavior* section, the following information is incorrectly documented for the WebUI:

  Security> Antivirus> Global: Select **Fail Mode Traffic Permit** to permit unexamined traffic, or clear it to block unexamined traffic, then click **Apply**.

  The correct information is:

  Security > Antivirus > Global: In the AV Scanner Global Settings, select **Permit**, which appears next to When Unable to Scan, to permit unexamined traffic, or select **Block All Traffic** to block unexamined traffic, and then click **Apply**.

- In the ScreenOS 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Part 5 VPNs*, in the *WebUI (Tokyo)* section of the *Site-to-Site Virtual Private Networks* chapter, the following information is incorrectly documented for the VPN WebUI:

  VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

  Gateway Name: To_Paris

  Security Level: Custom

  RemoteGateway Type:

  Static IP Address: (select), IP Address/Hostname: 2.2.2.2

  Preshared Key

  Preshared Key: h1p8A24nG5

  Outgoing Interface: ethernet3

  > Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

  Security Level: Custom

  Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

  Mode (Initiator): Main (ID Protection)

  The correct information is:

  VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click **OK**:

  Gateway Name: To_Paris

RemoteGateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic Gateway configuration page:

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

- In ScreenOS 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Volume 4, Attack Detection and Defense Mechanisms*, in the *Attack Object Database Server* section, the reference to URL https://services.netscreen.com/restricted/sigupdates is incorrect.

  The correct URL is: https://services.netscreen.com/restricted/signupdates.

- In ScreenOS 6.3.0 *Concepts & Examples ScreenOS Reference Guide: Volume 4, Attack Detection and Defense Mechanisms*, in the *SYN Flood* section, the *SYN Flood Protection Parameters* table contains the following incorrect information for *Source Threshold*:

  If the device tracks 25 SYN packets from the same source IP address, beginning with the 26th packet, it rejects all further SYN packets from that source for the remainder of that second and the next second as well.

  The correct action for Route is:

  If the device tracks 25 SYN packets from the same source IP address, beginning with the 26th packet, it rejects all further SYN packets from that source for the remainder of that second.

ScreenOS CLI Reference Guide: Command Descriptions

- The **set flow log-dropped-packet** and **unset flow log-dropped-packet** commands are not documented in the 6.3.0 *ScreenOS IPv4 CLI Reference Guide: Command Descriptions*. You can access the description of these commands from the 6.3.0 *ScreenOS IPv6 CLI Reference Guide: Command Descriptions*.

- In the *ping* chapter of the 6.2.0 and 6.3.0 *ScreenOS IPv4 CLI Reference Guide: Command Descriptions*, the following feature is not supported, because ScreenOS does not perform ping from MIP:

  ping 192.168.11.2 from mip 10.1.1.3

- 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 IPv6 CLI Reference Guide: Command Descriptions* does not support IPv6:

add-default-route

- 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 Message Log Reference Guide

- The following information is missing in the *ScreenOS Message Log Reference Guide*:

  - TCP Sweep Protection

    Alert (00442)

    Message TCP sweep! From <src-ip> to zone <zone-name>, proto TCP (int <interface-name>). Occurred <none>times.

    Meaning The security device has detected an excessive number of IP attempts to establish a connection at the specified interface from the specified source IP address.

    Action No recommended action.

  - UDP Sweep Protection

    Alert (00443)

    Message UDP sweep! From <src-ip> to zone <zone-name>, proto UDP (int <interface-name>). Occurred <none>times.

    Meaning The security device has detected an excessive number of IP attempts to establish a connection at the specified interface from the specified source IP address.

    Action No recommended action.

  - ICMP Ping ID Zero Protection

    Critical (00441)

Message ICMP ping id=0! From <src-ip> to <dst-ip>, proto 1 (zone <zone-name>, int <interface-name>). Occurred <none>times.

Meaning The security device received either an Echo Request or an Echo Reply packet with the Identifier set to Zero.

Action Verify the screen option to allow the required packets.

- TCP Packet without Flag Protection

Critical (00413)

Message No TCP flag! From <src-ip>:<src-port>to <dst-ip>:<dst-port>, proto TCP (zone <zone-name>, int <interface-name>). Occurred <none>times.

Meaning The security device received in the TCP packet with no flags set in TCP segment header.

Action No recommended action.

ScreenOS Online Help

- The following note is incorrect in the **SCREEN Options** page in the ScreenOS 6.3.0 Online Help:

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

The correct information is:

> ℹ **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 ScreenOS 6.3.0 Online Help, the reference to URL https://services.netscreen.com/restricted/sigupdates is incorrect on the *Deep Inspection Signature Pack Update* page.

The correct URL is: https://services.netscreen.com/restricted/signupdates.

ScreenOS Upgrade Guide

- The following note has to be added in the *ScreenOS Upgrade Procedures* chapter in the *Figure 1: Firmware Upgrade Path*

> ℹ **NOTE:** For the SSG 500 device, it is strongly recommend to update the upgrade path with the boot loader 6.0 before proceeding to the ScreenOS latest version.

- The following note has to be added in the *ScreenOS Upgrade Procedures* chapter *Upgrading Security Devices in an NSRP Active/Passive Configuration* section in the From CLI heading after point e.

  > **NOTE:** If the command **save soft from tftp ip_addr screenos_filename to flash** is executed while the device is still NSRP Master, then an NSRP failover would be automatically performed when executing this command.

- In the *ScreenOS Upgrade Procedures* chapter, in *Table 1: Upgrade Paths to ScreenOS 6.3.0*, the upgrade recommendation (boot-loader filename) for SSG520, SSG550, SSG520M, and SSG550M is incorrect.

  The correct upgrade recommendation (boot-loader filename) for SSG520, SSG550, SSG520M, and SSG550M is Loadssg500v107.

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.

- **UDP and ICMP Flood Screening**—ScreenOS 6.3.0 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, 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]

- **ISG and NetScreen 5000 series Multicast Hardware Support**—Multicast sessions can be handled by the ASIC only if there is a single output interface per virtual router.

The mcast group address can be pushed to ASIC so frames are forwarded in hardware. To use this feature run the **set/unset flow multicast install-hw-session** command. [309007, 427260]

- **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.

- **ASIC Hardware Support**—ICMP-flood and UDP-flood detections are done by ASIC on high-end platforms such as ISGs and NS-5000. There is no detection method to let the ASIC know if the alarm-without-drop is configured. Therefore, the ASIC drops the attack packets. On SSG series, the flow CPU detects and determines if the alarm-without-drop is configured or not and takes appropriate actions.

- **Policies**—Policy Verification **exec policy verify** command is not supported for IPv6 policies. It is only supported for IPv4 policies.

- **ICSA** —ScreenOS captures raw IP packets of types 0, 6, 17, 43, 44, and 60 to the packet log when the **set flow log-dropped-packet** and **set firewall log-illegal-packet** commands are configured. The packet log may be accessed through the command **get log packet**. However, the packet log is available only on the device. It may not be transmitted to an external syslog server.

- **Client-to-Site IPv6 VPN Support**—IPv6 IP pools are supported in the IKEv1 protocol, but they are not supported in the L2TP, PPP, and IKEv2 protocols.

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.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.