Juniper Networks

NetScreen Release Notes

Product: Juniper NetScreen-5XT, Juniper NetScreen-204, Juniper NetScreen-208, Juniper NetScreen-500, Juniper NetScreen-5200, Juniper NetScreen-5400

Version: ScreenOS 5.0.0r9-FIPS

Release Status: Private

Part Number: 093-1638-000, Rev. A

Date: 6-01-05

Contents

1. Version Summary

Juniper Networks NetScreen ScreenOS 5.0.0r9-FIPS is the latest version of ScreenOS firmware with FIPS mode for the Juniper NetScreen-5XT, Juniper NetScreen-200 Series security appliances, the Juniper NetScreen-500, and the Juniper NetScreen-5000 Series security systems.

The ScreenOS 5.0.0r9-FIPS release is interoperable with, and provides basic support for, all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions. This version of ScreenOS is fully supported by Security Manager, Juniper Networks-NetScreen's security management platform.

This version of ScreenOS also supports selection of either the Baseline or Advanced version of the firmware. To access a specific Advanced feature, you need to purchase the appropriate Advanced feature key.

Refer to the following table to understand what ScreenOS versions map to which product.

Product	Firmware
Juniper NetScreen-5XT	ns5xt.5.0.0r9.0
Juniper NetScreen-200 Series	ns200.5.0.0r9.0
Juniper NetScreen-500	ns500.5.0.0r9.0
Juniper NetScreen-5000 Series (with 5000-M)	ns5000.5.0.0r9.0

2. New Features and Enhancements

The following sections detail new features and enhancements in ScreenOS 5.0.0 releases. For a complete list and descriptions of new features and enhancements in ScreenOS 5.0.0, refer to the *Juniper Networks NetScreen ScreenOS Migration Guide*.

2.1 New Features and Enhancements in ScreenOS 5.0.0r9-FIPS

None.

2.2 New Features and Enhancements from ScreenOS 5.0.0r8

Destination NAT Enhancement – An enhancement has been added to the destination NAT feature to allow ARP responses for addresses that are on the same subnet as the device's interface. For further information on this feature please see the Juniper Networks/NetScreen Knowledgebase.

Scan Engine Update for Juniper NetScreen-5GT – ScreenOS now embeds Trend Micro's new scan engine version 7.0 to provide better scanning coverage and increase performance. All previous versions of pattern files will be compatible with this new version.

As part of the Scan Engine Update, Juniper Networks implemented the ability to increase scanning coverage using the following commands:

- **set av http skipmime**
- **unset av http skipmime**

Note: The feature may impact performance on the device for traffic that may match embedded text in HTML packets.

According to Trend Micro, the categories of viruses bypassed include HTML and Javascript. However, the subset of the bypassed viruses can be described as the following:

Javascript/Jscript/HTML embedded in HTML code (having HTTP content type of text/HTML) AND is accessed through a script-enabled browser from a remote web server (via HTTP).

For example, anti-virus scanning would NOT be bypassed for the following scenarios:

1. Javascript/HTML malware which is stand-alone in a *.js file
2. Javascript/HTML malware propagating via email attachments

So the viruses bypassed would be all Javascript and HTML based viruses, but accessed or contained with the above characteristics in HTTP traffic only.

2.3 New Features and Enhancements from ScreenOS 5.0.0r6

New Hidden Command - In response to the NISCC VULN 236929, a new hidden command is implemented in this release. The command is **set/unset flow check tcp-rst-sequence**. By default, the command is not set. This command alters the device's response to potentially spoofed TCP RST packets.

2.4 New Features and Enhancements from ScreenOS 5.0.0r1

Juniper NetScreen-5GT - Dial Backup, Dual Untrust, OSPF, and BGP are now available in the 10-user version. Previously these features were only available in the Plus version.

Juniper NetScreen-5GT - The Extended version provides the same capabilities as the Plus version with additional features: High Availability (NSRP Lite), the DMZ security zone, and additional sessions and tunnel capacity. For information on these features, refer to the *Juniper Networks NetScreen ScreenOS Concepts & Examples Reference Guide* for ScreenOS 5.0.0.

Note: You must register your product at www.juniper.net/support *so that certain ScreenOS features, such as antivirus or deep inspection, can be activated on the device. If you already have an account, enter your user ID and password; if you are a new Juniper customer, create your account first. To register your product, you need the model and serial number of the device. After registering your product, confirm that your device has internet connectivity. Issue the CLI command* **exec license-key update** *to make the device connect to the Juniper server to activate the feature.*

3. Changes to Default Behavior

There are numerous changes in default behavior. For detailed information on changes to default behavior in ScreenOS 5.0.0, refer to the *Juniper Networks NetScreen ScreenOS Migration Guide*.

Specific changes in default behavior in ScreenOS 5.0.0r9-FIPS release:

- The **unset vendor-def** CLI command removes all files stored in flash memory except the license file.
- Security Manager does not work with this release.

4. Addressed Issues in ScreenOS 5.0.0

The following sections detail addressed issues in each release of 5.0.0.

4.1 Addressed Issues in ScreenOS 5.0.0r9-FIPS

- **03875** – After attempting to update a new configuration to the device from Security Manager to the primary Juniper NetScreen-5200 system in an active-passive HA pair of Juniper NetScreen-5200 systems, the primary system failed. The backup system failed a minute and a half later.
- **03637** – When the firewall acted as a TCP proxy server, and if the server returned the syn-ack packet too late in response to a syn packet, the relevant firewall flow resource could be released too early and caused the firewall to fail.
- **03632** – When you have two VOIP phones connected to a trust and an untrust zone on a Juniper NetScreen-5GT running in extended mode, and you tried to place a call, the phone obtained its IP address from a DHCP server.
- **03607** – When two 5000-24FE system running in an NSRP active-passive transparent mode, where the e2/25 and e2/26 interfaces connected to a switch, stopped passing traffic and displayed the following meaningless message on the console:

    get log system saved
- **03600** – If you issued the **get tech** command for a Juniper NetScreen-5400 in an NSRP active-passive configuration while the system was busy, the system failed.
- **03569** – A Juniper NetScreen-5000 Series system could fail due to flow memory corruption from out-of-order TCP packets.
- **03558** – A trace route or ping operation sometimes caused memory corruption, causing the device to fail.

- **03537** – The device failed when it incorrectly sent the DHCPDISCOVER packet out in the callback function.
- **03528** – The subscription key retrieval operation worked only intermittently because the device did not close the SSL socket properly.
- **03522** – When Security Manager imported a Juniper NetScreen-5200 with a configuration with large amounts of policies (5,000) and VPNs (2,000), the device failed.
- **03495** – You could not retrieve mail from certain mail clients that send POP3 authentication requests (such as Mozilla Mail Client) because the device did not support POP3 authentication.
- **03478** – A few days after you first configured the Juniper NetScreen-5GT, the device could receive traffic, but not transmit it.
- **03463** – When ScreenOS performed an SNMP traversal over the MIB for the Juniper NetScreen-5200, the traversal halted because the device OID did not increment properly.
- **03435** – The Simple Mail Transfer Protocol (SMTP) client timed out when large attachments passed through a Juniper NetScreen-5GT anti-virus scan.
- **03433** – When two BGP peers established an adjacency and then lost the adjacency state, and the NetScreen peer attempted to reestablish the state, the NetScreen peer could be in the wrong state. This prevented it from reestablishing the adjacency.
- **03415** – You could not re-add a peer to a BGP peer group once you unset it.
- **03413** – A firewall device could fail when multiple users attempted unauthorized SSH sessions.
- **03404** – The device generated incorrect traffic log titles when it sent a traffic log based on a multicell policy. The traffic log title displayed the same source IP and destination IP addresses.
- **03397** – The device failed because VPN traffic did not handle interrupts properly.
- **03394** – You could not manage the untrust interface through a route-based VPN.
- **03379** – After successfully configuring the Juniper NetScreen-5GT in Extended mode, the WebUI incorrectly indicated that the device was in Trust-Untrust mode.
- **03369** – When the primary device in an HA pair performed a cold start synchronization, with a large number of VPN tunnels, the backup device in the HA pair sometimes dropped some SPI synchronization packets.
- **03367** – When you clicked the Cancel button on the WebUI admin page for Security Manager, you could no longer locate the page.

- **03358** – A very long URL entry when you attempt to perform URL filtering sometimes caused the device to fail.
- **03356** – The Phase 2 rekey sometimes failed after the Phase 1 expired when you used Kbytes as the criteria to trigger a Phase 2 rekey operation.
- **03355** – Track IP packets were sent out at the wrong interval, increasing failed counts (decreasing success rates) even though pings worked correctly.
- **03353** – When you configured a policy using the multiple service feature including more than 49 services, the Move checkbox of the policy disappeared from the WebUI and the WebUI displayed some field strings incorrectly.
- **03351** – When the Juniper NetScreen-5XP successfully upgraded to ScreenOS 5.0.X, the device incorrectly displayed the following message:

  The NetScreen device was unable to complete the upgrade of the file system.

  The NetScreen device was unable to complete the upgrade of the loader.
- **03346** – The Juniper NetScreen-5200 sometimes failed when you set up IKE gateways in a Vsys on the Juniper NetScreen-5200.
- **03340** – Security Manager did not send the correct Action code when generating a traffic log.
- **03338** – The component blocking feature that forces a packet to be dropped did not work properly.
- **03311** – When the VIP server detection was set to the Manual setting, the VIP server status detection still displayed the same status when the server detection parameter was set to Automatic.
- **03308** – When you attempted to change a username in the WebUI, the system added a new user instead of changing the name of the existing user.
- **03295** – When you issued a **get interface** command or similar commands, ScreenOS truncated interface names that had too many characters.
- **03294** – When you issued the command **get log traffic | inc** on a Juniper NetScreen-5200, the system failed.
- **03281** – When you performed an incremental SPF (Shortest Path First) operation for an OSPF virtual routing instance, the device failed.
- **03278** – When updating a dynamic VPN tunnel's peer gateway IP, a new route lookup was not performed for the updated peer gateway IP. If the updated peer gateway IP was not reachable via the old route used for the previous peer gateway IP entry, the VPN would fail.
- **03273** – After you saved the value in the policy counter in the WebUI, the value was different from the actual policy count.

- **03269** – The Juniper NetScreen-5GT incorrectly autonegotiated to 10MBps half duplex after it had initially set itself to 10MBps full duplex.

- **03267** – The anti-virus feature had a problem handling the HTTP packets because a web server inserted too many unnecessary white spaces in the HTTP header.

- **03263** – When managing the device from the V1-untrust or V1-trust interface using Manage IP, multiple sessions were created for each packet.

- **03261** – When you have two VPNs active between two devices, with outgoing interfaces, after the VPN Monitor deactivated the tunnel after nine seconds, and caused a failover to the secondary VPN, the device did not update the session information.

- **03250** – A memory corruption caused the device to fail.

- **03243** – In an instance where the client on the Untrust side of the device connected to a MIP that connected the server to the trust side, when an ASP began the server, it used a zero-sized window, slowing down performance, with the server sending back one character at a time.

- **03239** – When you performed an FTP transfer or email download that went beyond the maximum bandwidth allocated in the traffic shaping feature, VOIP calls experienced a lot of intermittent voice transmissions.

- **03235** – When you forcefully closed several PKA/RSA SSH sessions without properly logging out first, the system randomly failed several times.

- **03232** – Under some conditions, an HA (High Availability) pair with a 5000-M2 module installed failed. This occurred when the primary device had 4,000 sessions on it and the backup device had 100,000 sessions.

- **03205** – When running two Juniper NetScreen-5200-24FE systems in an HA active-passive environment, the secondary path would fail and both devices would assume the primary role after you unplugged the two HA links.

- **03203** – The device sometimes failed when it traversed the session table.

- **03178** – The device sometimes failed with high CPU and the full session table due to session memory corruption.

- **03177** – Intermittent system failures occurred during an SNMP walk.

- **03152** – When running XAuth in the WebUI environment, the XAuth page displays the CHAP fragment reassembly method selected by default.

- **03142** – When you sent 64 bytes of packets through a route-based VPN between two Juniper NetScreen-5200 Series systems with an IXIA packet analyzer device, the Security Association failed and the packets did not pass through the IXIA device.

- **03136** – Gratuitous ARP packets sent out to broadcast the presence of a device were blocked from being sent.

- **03132** – When using Juniper NetScreen-Remote to connect to a Juniper NetScreen-500 dial-up VPN using the WebUI, the IKE Gateway Configuration displays as **user** instead of **user-group**.

- **03128** – Mistakes occurred with (MIP) Mapped IP translation when a remote shell used a secondary session initiated from the server for redirecting standard error output from the console.

- **03095** – If the Juniper NetScreen-5XT autonegotiated its speed and duplex settings with a Cisco 3550, the devices operated properly, but the connection would fail if you manually set 100MBps - Full and 100MBps - Half for both devices.

- **03092** – When the device was in transparent mode, it sometimes was unable to download the latest anti-virus signatures.

- **03081** – An anti-virus parsing error slowed performance for HTTP sessions.

- **03078** – With a very large configuration, when you attempt to save a very large configuration, the device sometimes generated false HA up-down messages incorrectly indicating alternatively that the device disconnected and connected.

- **03071** – If the first VIP (Virtual IP) in the VIP list did not have a service defined for it, if you added a service to the second to fourth VIP in the list, the VIP Summary Page displayed no data.

- **03068** – When you modified the IKE Phase 1 gateway name using the WebUI, the primary device in an HA pair could not synchronize properly with the backup device so that the backup device received the IKE gateway name.

- **03058** – After you successfully updated a device with the latest configuration in Security Manager, and then ran a Delta Configuration Summary operation, the summary still displayed commands indicating that the update did not successfully transfer all settings to the device.

- **03054** – The device did not update its ARP table because too many packets queued up for the same ARP entry.

- **03042** – The serial interface on the device disappeared after you downgraded from ScreenOS 5.0.0rx to a previous version with the Unlimited Number of Users Version 2 key installed.

- **03025** – In certain situations, when a user authenticated using WebAUTH with SecureID, and the user in the Auth table timed out, subsequent attempts to authenticate failed.

- **03010** – In certain situations when you ping a Juniper NetScreen-5200-24FE interface, an error condition occurred which sent out fragmented packets.

- **02988** – The ALG did not work for a custom-defined rsh (remote shell) service.

- **02986** – SSHv2 with RADIUS authentication failed to authenticate external users properly.
- **02985/02996** – The Juniper NetScreen-5000 Series systems sometimes failed from memory corruption due to kernel locking.
- **02975** – While performing a virus scan with the anti-virus engine, the anti-virus update failed, and no traffic could pass through a Juniper Networks security appliance because the policies blocked it, and the device failed repeatedly.
- **02972** – When you tried to transfer large files using SCP, the connection closed before the transfer completed.
- **02952** – A code loop in a SIP disconnect state occurred and resulted in a core the device failing when disconnecting a SIP call over a Cisco VOIP (Voice Over IP) network.
- **02941** – When you configured a device with a DIP (Dynamic IP) and traffic shaping, the first traffic the device sent failed to reach its destination.
- **02933** – While attempting to age out specific sessions, the device sometimes went into an infinite loop causing the watchdog timer to cause the device to fail.
- **02921** – A Juniper NetScreen-5400 stopped accepting all traffic after you reset the device and then unset a policy with multiple services.
- **02918** – A Juniper NetScreen-5000 Series system sometimes could not support HTTPS when the system occurred in an NSRP active-passive environment in Transparent mode when you used HTTPS to manage both the primary and backup devices.
- **02915** – An invalid pointer reference between FTP control channel and data caused the device to fail.
- **02913** – Although a session on the device has a timeout of one second, when the session exceeded the timeout, the device did terminate the session.
- **02911** – In some cases, sessions on the Juniper NetScreen-5000 Series systems never aged out even if there was no response to them.
- **02908** – When you lost a Web and SSH connection to the primary device in an active-passive HA configuration, you could not connect to the primary device using an SSH or WebUI session, although you could connect to the backup device.
- **02906** – You were unable to ping from one device to another over a VPN between two devices that were each in transparent mode running ScreenOS 5.0.0rX.
- **02893** – When high amounts of traffic transferred across the Fast Ethernet port on the Juniper NetScreen-500, the data could become corrupted.

- **02867** – If the DHCP relay server is set with an IP address, the device incorrectly attempted to resolve the IP address with the host name even though there was no hostname.

- **02861** – IP swapping issues occurred on the Juniper NetScreen-5000 Series systems sometimes because of invalid cache.

- **02845** – In an NSRP active-passive configuration, improper MAC table entries prevented the backup device from being managed.In some instances, you could not manage a backup device in an NSRP active-passive configuration.

- **02810** – A policy with the negate option did not free memory on the device properly, creating a memory leak, degrading performance on the device.

- **02798** – The Juniper NetScreen-5000 Series systems sometimes had a redundant buffer when receiving out-of-order fragmented VPN packets.

- **02787/03020** – A memory leak caused by a failed DNS query on a Juniper NetScreen-5200 in an HA pair caused the primary system to fail.

- **02774** – Multiple trace routes occurred after you created a BGP neighbor to a device in an HA pair, disabled HA synchronization, and then attempted to redistribute routes from the primary device to the backup device.

- **02768** – When the primary device attempted to synchronize with the backup device and sent it a new DIP session, the backup device could still have the existing DIP session and could not perform the synchronization.

- **02762** – If you attempted to display 100 logs per page in the WebUI Traffic Log, the WebUI displayed no logs.

- **02725** – In an NSRP device pair, the primary device generated a log that indicated that multiple failovers occurred, but the backup device only generated one log, indicating only one failover.

- **02710** – The Unknown Protocol SCREEN option did not work on the Juniper NetScreen-5000 Series systems.

- **02656** – The WebUI home page did not display the status for Layer 2 interfaces.

- **02620** – Issuing the debug command for the WebSense server, caused the device to fail.

- **02604** – When a device exported routes from a Vsys to a root virtual router, the exported routes were not tagged with the correct Vsys ID.

- **02602** – Attempts to establish Telnet, WebUI, and SSH, sessions to the interface, where management was enabled, failed, when a route from the correct interface was not provided or the route pointed to a different gateway.

- **02580** – When you created a new custom service, and then configured a VPN using IKE, the Proxy ID setting in the VPN Autokey IKE configuration incorrectly defaults to the new custom service, and not the ANY service.
- **02555** – The system incorrectly created sessions for embedded ICMP packets.
- **02530** – A TCP stack error caused the BGP neighbor state to change to the Idle state before the BGP holddown time value (default of 180 seconds) expired. The BGP neighbor state, a setting determined by whether the current BGP routing instance, can detect its neighbor to be active, and is not supposed to render the neighbor Idle until no neighbor response occurs after the holddown time elapses.
- **02519** – In an instance where an active-passive HA pair of Juniper NetScreen-208, the SA (Security Association) went out of sync, the backup device became corrupted and the device failed because memory on both devices became corrupted.
- **02498** – The status link LED incorrectly indicated that the Fast Ethernet port on both the Juniper NetScreen-500 and Juniper NetScreen-200 was running at 10 Mbps while the physical link was correctly running at 100 Mbps.
- **02486** – In some instances, after enabling a WebSense server, when you accessed the Microsoft Outlook Calendar utility, you would lose connectivity to Outlook Email.
- **02482** – Slow http/https through vpn. Bug in H323 implementation can possibly cause session leak R. HTTP cant pass if unset flow tcp seq + set flow tcp syn combo is used.
- **02385** – When you selected multiple source address groups in an intra-zone policy where the source was Trust and the destination was Trust, then the groups were not displayed properly in the Policy list.
- **02152** – In instances where you created an intra-zone policy with the source zone was Trust and the destination zone was untrust and that used multiple addresses, the Policy list displayed the same entity for both the source and destination in the policy.
- **02101** – Messages logged with a VIP (Virtual IP) incorrectly indicated the VIP connection connected and disconnected repeatedly, indicating the presence of a false positive even though the VIP connection sent acknowledgment responses to the query. The messages displayed continuously were:

  VIP cannot be contacted.

  VIP is now alive.

- **01998** – You could not save the **set console aux disable** command into the device configuration.
- **01739** – Ping operations would not work if fast aging out of MAC addresses did not occur when a PC migrated from one Juniper NetScreen-5GT port to another in the same zone.
- **01635** – The system failed when an H323 recomputed a UDP checksum; the UDP packet lengths sometimes were too consistent with the IP lengths.
- **01584** – If a virtual routing instance acted as the ABR (area border router), then the routing instance did not advertise inter-area summary routes. An inter-area summary route is one value that encompasses a range of route prefixes contained in multiple routing areas.
- **01523** – An OSPF virtual routing instance sometimes unexpectedly dropped routes.

4.2 Addressed Issues from ScreenOS 5.0.0r8

- **40292** – A potential cross-site scripting attack existed in the anti-virus scan engine when processing compressed files.
- **39458** – You could not configure 16 concurrent anti-virus messages, the expected maximum number of messages allowed when running the anti-virus Scan Manager utility in the WebUI.
- **39087** – In certain circumstances, the first attempt to access a TCP application through a Juniper NetScreen-5000 system with authentication failed when the ARP entry for the application was not present.
- **38193** – A Juniper NetScreen-5GT could not access common public web sites when an administrator performed an anti-virus scan for HTTP on the device. The attempted connections will expire after they exceed the time out threshold for connection attempts.
- **37933, 37945** – If a number of different attacks entered the Juniper NetScreen-5000 Series system over a period of time, the system sometimes began to drop packets.
- **36708** – You could not view the traffic logs for a Vsys if you entered the Vsys as a root admin user.
- **36670** – You could create more VLANs on a Juniper Networks security appliance than the number of VLANs the device officially supported. However, doing this sometimes caused unexpected results. Refer to the specifications sheet for your NetScreen product to learn how many VLANs it supports.
- **36494** – Upon startup, Juniper Networks security appliances using PPPoE sometimes generated a warning message informing that the interface gateway command was invalid. This is a result of the gateway changing

whenever the device restarts and does not effect the normal operation of the device.

- **36473** – Restarting a Juniper Networks security appliance while it was performing an operation in flash sometimes damaged the data on the device and caused the device not to restart or to lose the configuration.

- **36235** – Adding the pre-defined service entry "ANY" in a multiple service policy sometimes resulted in a system fail.

- **36095** – You could not change the IP address of an interface if a VIP or MIP was configured on that interface, and the VIP or MIP was used in a policy configuration. DHCP and PPPoE could not change the interface IP address if a VIP was configured using the same-as-interface option.

- **35977 -** (Juniper NetScreen-5XT only) The Juniper Networks security appliance sometimes dropped TCP traffic because it miscalculated the length of the tcp-syn-check.

- **35904** – (Juniper NetScreen-5GT only) Juniper Networks security appliances needed to support two incoming IPSec keys. When the software lifetime was in use and after the re-key was successful, the device should have permitted traffic using older SA's to traverse the device.

- **35735** – A root administrator could not manage the root system from a host that resided on a virtual system.

- **35624** – If you set the negotiation mode on a 10/100 Ethernet port to Full Duplex and configured the holddown time on the interface to less than one second, it caused the interfaces to go up and down.

- **35615** – (Juniper NetScreen-5GT only) Any policies within the device indicated traffic shaping was active for the policy. Issuing a 'get policy' CLI command displayed an "X" under the "T", for traffic shaping, in each policy. However, issuing a 'get policy id <number>' CLI command indicated that traffic shaping was turned "off".

- **35528** – In an active-passive NSRP configuration, you needed to set a manage IP on both devices to enable each device to connect to the entitlement server and retrieve signatures.

- **34279** – (For Juniper NetScreen-5000 Series) Juniper Networks security appliances sometimes unexpectedly dropped traffic that was processed by the CPU module and that matched a policy in which the "Diffserv" option was enabled.

- **29619** – When you used the CLI to configure SCEP, you could not specify an already defined Certificate Authority as the recipient of the certificate requests.

- **02940** – The device sent out multiple SNMP traps associated with the same event after you changed the source interface for SNMP operations.

- **02926** – The number of syslog messages sent per second from the Juniper Networks security appliance were being limited by an internal process.
- **02924** – SMTP (Simple Mail Transfer Protocol) queued emails on Microsoft Outlook 2003 clients timed out when a policy had the anti-virus option enabled because you could not perform more than one SMTP transaction within one session.
- **02909** – Embedded ICMP caused the DIP (Dynamic IP) pool memory leak traffic flow to stop because the DIP allocation failed after no ports were present.
- **02897** – The WebUI displayed the autokey IKE list incorrectly in instances where a listing of 5, 10, 50, or 100 entries were in the list. It displayed only 20 items per instance.
- **02896** – An SA (Security Association) sometimes was visible in the wrong Vsys in an environment where two Vsys both had non-active dialup VPNs configured.
- **02880** – If you enabled the anti-virus option on a policy, and ran the windowsupdate.microsoft.com utility on the policy, the utility hung and the console displayed the Network Error page. The utility worked only when the the policy had the anti-virus operation disabled.
- **02874** – A fail occurred when the device prevented packets with the wrong/ inactive virtual MAC address from being forwarded.
- **02853** – The WebUI inadvertently allowed adding a subinterface in transparent mode causing the device to fail.
- **02841** – The device inadvertently displayed an inactive route as active in an environment where two route-based VPN unnumbered tunnels mapped to one VSI. This behavior only occurred when this VSI was assigned to the Untrust zone that had an IBGP routing instance configured inside the network.
- **02829** – When obtaining a traffic log using a specific IP address on an SSH session by issuing the **get log traffic | include** command, the device failed. For example, if you connected to the device using an SSH session and you issued the following command (which contains an explicit IP address):

  get traffic log | include 10.1.1.10

  the device shut down and failed.

- **02824** – Custom zones incorrectly supported half the number of IP address book and group entries than predefined zones did.
- **02823** – When applying the snoop filter with a destination IP address and destination port, the filter did not work.

- **02822** – The DHCP utility did not work on one of the redundant interfaces on a device. The interface did not appear in the DHCP environment in the WebUI.
- **02814** – The SNMP interface index values were inconsistent through the SNMP tree. Interface index values uniquely identify each interface.
- **02805** – Under certain traffic conditions, some DNS and HTTP session timers were set with higher values than the DNS and HTTP service timeouts.
- **02796** – When the device sent out a trap that indicated an SNMP authentication failure when OSPF was enabled, the device failed.
- **02788** –In certain situations, an Juniper NetScreen-5000 device failed when it received a high number of bad IKE packets.
- **02786** – If the packet that had both a destination broadcast subnet IP address and a MAC multicast address attempted to enter the device, the device dropped it.
- **02785** – A Juniper Networks security appliance failed continuously because an interface on the device did not check that the PPP (Point-to-Point Protocol) encapsulation functioned properly.
- **02771** – Traffic through a MIP (Mapped IP) address with both source-based routing and traffic shaping enabled failed.
- **02765** – If a configuration is pushed to the device by Security Manager and the heartbeats to the device are lost, the device would invoke the configuration rollback feature because the heartbeat missed threshold was too short.
- **02740** – The Security Manager Log Viewer did not display data in the Alert column. The Alert column now correctly displays traffic logs associated with policies that have the Alert setting selected.
- **02736** – The Mgt-IP on a VSI replied with a virtual MAC address instead of a physical MAC address for the Ident-reset.
- **02734** – When you performed an SNMP walk operation on the Policy MIB, the procedure incorrectly displayed an integer to represent the custom service. It now correctly displays a string to represent a custom service in the Policy MIB.
- **02730** – For external LSAs (Link State Advertisements) that have a forwarding address, the priority for a forwarding route incorrectly used the interface cost as the priority value rather than the metric of intra- and inter-area OSPF routes. The metric is the correct value to use for setting a route priority.
- **02718** – Importing a device into Security Manager failed because the heartbeat timeout was exceeded and was not user configurable.

- **02709** – When you set a manual VPN authentication setting to NULL on a Juniper Networks security appliance, the device failed because a Null length is invalid.
- **02707** – When performing an anti-virus scan on a Juniper NetScreen-5GT device, the device displayed an error-constraint-drop status.
- **02699** – When multiple interfaces belonged to different Vsys had the same IP address and subnet mask, VPN traffic to these subnets could pass to the wrong Vsys.
- **02609** – The primary Juniper NetScreen-5200 device in an active-passive NSRP cluster failed, which caused a failover from the primary to the backup device.
- **02694** – ScreenOS did not send discovered SCREEN occurrences to Security Manager when Security Manager imported a configuration from a device.
- **02692** – The DIP (Dynamic IP) allocation failed and halted traffic entering the device, requiring the DIP allocation mechanism to be reset every two hours.
- **02688** – The CLI provided no maximum value check for BGP hold time entered on a device, incorrectly allowing you to enter any value for the hold time. If the value was greater than the maximum hold time setting of 65,525, the device incorrectly accepted the value, and the output from the **get hold-time** command incorrectly displayed it as a negative number.
- **02687** – Traffic shaping did not work properly when the traffic shaping policies traversed a route-based VPN on a device.
- **02685** – You could not unset the sql alg using the **unset flow sql-alg** command on Juniper NetScreen-5000 Series devices.
- **02679** – Some devices generated multiple logs for information associated with the self log.
- **02670** – When a Juniper NetScreen-5XT device obtained a new IP address from a DHCP server, one of the static routes did not update the default gateway with the proper IP address and DHCP payload information assigned to the device.
- **02668** – A VPN tunnel incorrectly displayed two different ESP sequence numbers which are associated with two different ASICs on the Juniper NetScreen-5000 Series devices.
- **02664** – Packets were sent out with the MAC address of the inactive VSI instead of the active VSI address in an active-active VSI cluster.
- **02663** – You could not manage two of the secondary IP addresses on an interface of the Juniper NetScreen-100p in the WebUI.
- **02660** – After importing a CA (Certificate Authority) certificate into a device and then rebooting the device, the device removed the certificate.

- **02655** – The event log timestamp changed to Daylight Savings Time (DST) even though DST was not enabled.

- **02642** – After configuring SCREEN setting thresholds on a device using the WebUI or CLI, the **get config | include *<screen_settings>*** command did not display the configured settings.

- **02641** – The PKI IKE memory pool on a device had a memory leak caused by the Security Manager agent.

- **02637** – A session allocation with less than 1,000 sessions on a Juniper NetScreen-5000 Series device failed.

- **02629** – When running a get config all command and redirecting the output to a file on the TFTP server when the Trust interface as the source, the file was not transferred correctly.

- **02627** – The policy move page only displayed the first 20 policies, and therefore you could not move a policy from the initial screen from where you copied the beyond the 20 policies displayed.

- **02624** – An anti-virus scan failed to scan .RAR files on a Juniper NetScreen-5GT.

- **02621** – When a Ping request is initiated through a VPN tunnel to a MIP configuration on a loopback interface, the ICMP reply through the tunnel did not get translated back to the MIP address.

- **02680** – The SNMP **name** command inappropriately propagated across the NSRP cluster.

- **02682** – When using the WebUI to set information on the backup device, the primary SNMP device was inappropriately deleted when using the **unset VSD ID 0**.

- **02606** – A ping packet through a tunnel in an NSRP environment between two Juniper Networks security appliances failed after a failover until you performed a rekey operation.

- **02581** – You incorrectly could define the same IP address to multiple loopback interfaces over multiple subnetworks by running the **set vrouter trust-vr ignore-subnet-conflict** command on a device. Juniper Networks security appliances support defining multiple loopback interfaces on the same subnetwork, but not with duplicate IP addresses.

- **02578** – A PPPoE (Point-to-Point-Protocol-Over-Ethernet) connection on a device incorrectly sent an acknowledgment for an unnumbered PPP session. The correct response to an unnumbered PPP session is a NAK (Non-Acknowledgment).

- **02552** – Policy authentication with an external authenticating server could run into the same memory corruption when authentication failed and caused the firewall to fail.

- **02551** – An NSRP backup device indicated that a failover occurred continuously when no failure on the primary device occurred.
- **02543** – A device rebooted because of an improperly processed checksum.
- **02542** – When upgrading a Juniper NetScreen-5GT from ScreenOS 4.0.0r4 to ScreenOS 5.0.0r3, a PPP connection from a Windows XP client to a Windows 2000 server stopped working.
- **02536** – The priority value on a WebTrends syslog message varied from device to device.
- **02531** – After changing manage options in the Untrust interface with a DHCP client configured, the device renewed its IP address with the DHCP server, causing loss of configuration of MIPS, DIPs, and VIPs.
- **02509** – A memory leak in the NSRP synchronization process between two devices caused some FTP sessions to stop working.
- **02477** – You cannot configure the NSRP Lite feature through the WebUI even though you applied an NS-5GT extended key.
- **02457** – The URL request function that sent content to a WebSense server sometimes engaged the CPU on a device for too long causing the device to reboot.
- **02403** – There was a flaw in the TCP stack buffer which caused the device to fail.
- **02390** – When you created an aggregate interface on a Juniper NetScreen-5000 system, a CLI **get** command and an SNMP get operation indicated different bandwidth values for the interface. In some cases, the CLI command revealed 100 Mbps and the SNMP command revealed 0 MBps.
- **02388** – You could not set the DHCP IP address range through the WebUI when detecting an auto-probe. By attempting to perform this operation, the system displayed the following message:

  The DHCP IP Pool not in the same subnet with gateway/interface
- **02372** – If you ran an OSPF virtual routing instance on a route-based VPN, under heavy traffic conditions, the device could continually spawn new sessions for the OSPF packets.
- **02369** – You could not change the IKE Authentication user's password when using the WebUI.
- **02362** – In some instances, a TCP session prematurely expired.
- **02344** – When you tried to bind a PKA key to an administrator account using the WebUI, the device generated a trace dump.
- **02342** – An OpenSSH client continued to use password authentication even when password authentication was not an option for SSH**.**
- **02335** – The SNMP iftype value was wrong on the Juniper NetScreen-5XP.

- **02333** – When a device attempted to block files with a .exe extension, it incorrectly blocked files with .zip extensions.
- **02326** – A device incorrectly created sessions if the IP address had a unicast destination while the destination MAC address had a multicast destination.
- **02298** – Commands related to NHTB (Next Hop Tunnel Binding) did not run when you used a blank character when creating a tunnel name for NHTB.
- **02297** – An anti-virus scan dropped connections with selected HTTP and HTTPS sites.
- **02116** – When the lifetime of an IKE Phase 2 SA (Security Association) reached a threshold defined by the soft lifetime buffer, a Phase 1 rekey and a delete notification for the P2 SA was generated after the P1 rekey.
- **02026** – When a device attempted to contact a RADIUS server and the server was unavailable, the device corrupted the server reply after it was stored in device memory.
- **02024** – When a device contacted a RADIUS server for authentication while the server was performing many RADIUS authentications, the device corrupted the server reply after it was stored in device memory.
- **01957** – The WebUI did not contain the ISP connection Test button under the Configure column in the ISP screen because a previous revision of ScreenOS was released with the button removed. The button now appears in this location.
- **01822** – A Juniper NetScreen-5000 device incorrectly sent packets from an inactive VSI (Virtual Security Interface). The device now first considers whether a VSI is active before it sends packets from it.
- **01862** – After upgrading a Juniper NetScreen-5400 to ScreenOS 4.0.1-SBR.2a2, the **get ip-classification** command displayed incorrect data for IP classifications currently on the device.
- **01782** – A hidden command incorrectly dropped an incoming packet to a Juniper NetScreen-5000 device when an ARP entry was not present on the device. The device now responds properly to an incoming packet when no ARP entry is present, placing the packet in a queue of other packets and forwarding it after six seconds.
- **01779** – The Track-IP operation in an Active-Active setup on an HA pair of Juniper NetScreen-5000 devices incorrectly selected an outgoing interface in a random manner.
- **39499** – The CPU utilization on a device increased by 10 percent if the device could not connect to the Security Manager Device Server.

4.3 Addressed Issues from ScreenOS 5.0.0r7

Manufacturing-only release.

4.4 Addressed Issues from ScreenOS 5.0.0r6

- **38268** – A Juniper Networks security appliance running a BGP peer virtual routing instance cannot use an MD5 type password when the device is connected to a Juniper Networks router.
- **38200** – A non-specific error in H323 caused memory leaks in device sessions.
- **38103** – The DHCP client was unable to obtain an IP address if Dynamic Track IP was enabled and the DHCP client interface was down.
- **37711** – When you have established a VPN tunnel and tried to perform a Phase II rekey, the operation intermittently failed.
- **02449** – The server kept sending LCP requests as if it never received a packet because the PPP (Point-to-Point Protocol) request sent out never left the device.
- **02446** – Unfreed memory buffers could be allocated to the point where the device could not send management traffic data.
- **02429** – HTTP packets could not pass through the Juniper NetScreen-5200 running ScreenOS 4.0.0 if you issue both the **unset flow tcp seq** and **set flow tcp syn** commands.
- **02419** – The WebUI label **IP Sweep/Port Scan** in the IP and Port Scan field in the Screen menu contained incorrect references to milliseconds (5000 ms) instead of microseconds with the **ms** abbreviation (ms is the abbreviation for milliseconds).
- **02416** – If you rebooted a Juniper NetScreen-5200 after configuring NHTB entries in the current session on the system, the device lost the entries after the reboot.
- **02415** – A RIP routing instance dropped the default route (0.0.0.0) of another routing instance if it learned it on an unnumbered tunnel interface.
- **02413** – When you issued the command **set ike gateway**, the device always created a test certificate peer certificate type x509-signature.
- **02411** – An NSRP Track-IP session on a sub-interface failed in instances when the target address and the default route (0.0.0.0) were on the same subnet. In these instances, the Track IP query incorrectly selected the default route (0.0.0.0).
- **02387** – The command line displayed only 24 characters for a URL string, although ScreenOS supports URL strings with up to 64 characters.

- **02384** – The device failed if you connected an Ethernet cable to the untrust interface in the v1-untrust zone while the device was in transparent mode.
- **02383** – Under some circumstances, the OSPF routing instance could not build an adjacency because its memory buffer was not large enough to handle large databases.
- **02379** – You could not establish the Phase II portion of a VPN tunnel when you referenced a custom service that had spaces in its name with no quote marks around the string because ScreenOS did not recognize strings with spaces without quotes around the string.
- **02377** – The Juniper NetScreen-200 did not always free up memory after VPN tunnels closed, requiring a manual device reboot to recover.
- **02375** – The device was unable to detect and defend against a ping of death attack and would fail when these types of packets arrived at the device.
- **02372** – You could not clear sessions on Juniper NetScreen-50 devices in an active-passive environment in instances when the active device stopped creating new sessions when the session table was full.
- **02370** – When you manually created a VPN tunnel in an NSRP environment in the WebUI, using an extra comma in the key portion of the **set vpn** command, the primary device failed while the backup device kept the old configuration.
- **02368** – ScreenOS removed the quotation marks around the VPN name with a space when you configured an NHTB value on an interface.
- **02364** – The device generated an unknown keyword error to the keyword **all-virtual-system** when you tried to assign a new admin password to a VSYS.
- **02354** – Occasionally, the ScreenOS logging environment incorrectly displayed unusual logs that indicated a hacker attacked the device. A typical message that indicated a hacker was the following:

  2004-02-11 11:45:22 system notif 00001 Address _prefix_c0000000_2_p72_ for ip address 192.0.0.0 in zone V1- Untrust has been deleted by netscreen via web from host 128.32.199.217 to 128.32.199.71:80 session
- **02336** – In an NSRP active-active environment, when the customer disconnected all the cables from the HA1, HA2, and MGT interfaces on either device, and they reconnected cables to the HA1 and HA2 interfaces, the device rebooted.
- **02323** – When you ran FTP Put or Get commands to push or obtain data to or from the device, the WebUI always indicated the device had a Deny action in its policy even when the policy was configured to permit traffic.

- **02272** – HTTP and HTTPS packets passed through VPN tunnels more slowly than expected, sometimes to the point of timing out and causing the device to continually retransmit the packets.

- **02250** – The device sometimes generated an error when you updated a device and issued the following command with the following arguments:

  set interface tunnel.2 nhtb 10.1.2.5 vpn

- **02206** – An Apple Macintosh running Operating System 9 client using the HTTP protocol failed to connect to the internet while a Juniper NetScreen-5GT had AV HTTP scanning enabled.

- **02194** – The **get log traffic policy** command caused a device to fail when the device contained more than 15,000 VPN tunnels and received ICMP traffic.

- **02156** – When you enable Scan-MGR, it prevented access to certain web pages because during the TCP 3-way handshake, the web server advertised a window size of 0 to the client, preventing the web page window from opening.

- **02094** – The Address Negate feature had no effect on traffic entering the device through a VPN tunnel with a VPN tunnel policy applied to it.

- **02052** – NAT Traversal (NAT-T) for IPSec did not behave correctly when both the initiator and responder were behind NAT devices.

- **01793** – A redundant interface incorrectly learned an ARP when no IP address was configured for the interface.

- **01657** – A redundant VPN did not fail over with a RTO (Run-Time Operation) synchronization enabled.

- **02041** – The Juniper NetScreen-5000-specific command **unset/set hardware wdt-reset** was incorrectly available on all Juniper Networks security appliances.

- **02412** – The SNMP Get response values were not correct for the ifInOctets and ifOutOctets statistics.

4.5 Addressed Issues from ScreenOS 5.0.0r5

None.

4.6 Addressed Issues from ScreenOS 5.0.0r4

This section describes issues that addressed in the ScreenOS 5.0.0r4 release.

- **37070** – The initial configuration wizard in the WebUI required a toggled checkbox to enable switching the mode of the device back and forth from NAT Mode to Route Mode.

- **37069** – The configuration wizard option in the WebUI that enables you to skip the wizard screens was not present on the initial wizard screen. This option enables you to go directly to the WebUI login window to enter the device to manage it.

- **36669** – When 20,000 or more policies were configured on a Juniper Networks security appliance, you experienced a two- to three-minute delay when scrolling through the Policy List page in the WebUI.

- **36939** – The Juniper NetScreen-25 and Juniper NetScreen-50 did not support up to eight VLANs as expected and the Juniper NetScreen-20x did not support up to 32 VLANs as expected.

- **02259** – In an Active-Active NSRP configuration, the device did not accept traffic that terminated on the device interface in active mode on a different zone than the one with the source IP zone.

- **02211** – The IPSec pass-through operation failed because ScreenOS 5.0.0r3 required an incoming policy to work properly.

- **02206** – After the AV waited for HTTP get packets and did not receive them after a few seconds, the CSP sent resets to nodes on both sides of the device.

- **02175** – By performing a policy search (a scan of a policy group to locate a specified entry), the device failed because ScreenOS improperly initialized policy counters which keep track of policies, and the search improperly returned a null pointer.

- **02160** – When the Anti-Virus scan engine scanned large email messages, the device sometimes failed if the amount of time specified by the SMTP scan timeout elapsed before the amount of email data scanned exceeded the Max Content Size limit.

- **02156** – When the AV Scan-MGR option enabled in a policy detected a SYN-ACK packet associated with a site with a window size of zero, the device dropped the packet.

- **02153** – When trying to establish a GRE tunnel between two PCs with one connected to the Trust interface and the other to the Untrust interface, using policy-based source NAT, the tunnel failed because a GRE tunnel requires fixed source and destination ports and the policy-based source NAT process changes the port values.

- **02148** – The device might fail when Vsys traffic changes to the root sys mod when the traffic is en route to a Mapped IP (MIP) object.

- **02145** – When SMTP traffic entered the device and combined with the SMTP **rcpt** command, it sometimes bypassed the Anti-Virus scanning engine.

- **02142** – The SSH_MSG_IGNORE message and   SSH-1.99- version string were not handled by ScreenOS.

- **02134** – When a policy specified a service that contained the same ranges for both the source port and destination port, traffic associated with other services with the same port ranges matched the conditions of the policy and the policy would respond with actions associated with a match occurring.

- **01981** – You could not set the priority of the modem to any values.

- **01957** – (NetScreen5XT and 5GT only) The modem TEST button was missing in the WebUI.

- **01907** – Previous releases of ScreenOS 5.0.0 did not support Bootstrap Protocol (BootP) requests.

- **02139** – If you created a session on the device and no other session is active on the device, the device still generated a log. Juniper Networks security appliances should generate logs only if you create a session on the device and at least one other session is active on the device.

- **02117** – For a uni-directional dialup or site-to-site route-based VPN, specific routes were required on the receiving VPN device so that the returning traffic could go back into the correct tunnel interfaces accordingly. This was a result of the dynamic routing failover feature in ScreenOS 5.0.0.

- **02106** – After changing the local Auth server timeout in the WebUI from the default value of 10 minutes to any other timeout value, you could not reset the timeout back to 10 minutes.

- **02104** – In transparent mode, devices dropped VTP (VLAN Trunking Protocol) and Spanning Tree packets.

- **02095** – The device failed when it performed a custom Deep Inspection examination on a signature that contained a string of characters that was long enough to cause the device memory buffers to overflow.

- **02094** – The address negate feature did not work for traffic coming from a VPN tunnel policy.

- **02078** – If the same Auth/L2TP user was defined on both the device and a remote Radius server, the device did not release the assigned IP address back to the address pool, as expected, after the user disconnected from the tunnel connection on the device.

- **02076** – (Juniper NetScreen-5XP only) The device Status LED light blinked with a longer interval between each illumination (more slowly) than it did when running ScreenOS 4.0.0.

- **02072** – Several SNMP Object ID (OID) data types that identify a specific vendor were incorrect. Some counters associated with OIDs always returned a zero value.

- **02065** – SNMP traps were improperly formatted with numerical values that indicated an incorrect trap type. SNMP maps specific integers to indicate specific trap types, or events that generate traps. Because of this

discrepancy, you had to read the text description of the trap type to identify it. Now you can refer to the trap type value to identify it. For example, the traditional SNMP trap type value for a Cold Start event is 0. Please check the ScreenOS Messages Guide for the correct values in ScreenOS 5.0.0.

- **02062** – Under certain circumstances, Track-IP was not sent out and caused the NSRP failover operation to fail.
- **02059** – When you changed an IKE gateway from Static IP to Dynamic IP using the WebUI, the procedure automatically changed the setting from Main Mode to Aggressive mode.
- **02057** – Multiple custom addresses or service groups in a policy sometimes caused a Juniper Networks security appliance to fail during restart.
- **02050** – Configuring an address group from an Apple computer using Internet Explorer sometimes caused a Juniper Networks security appliance to fail.
- **02047** – When the device received a packet with Ethernet type 0x8888, the device failed.
- **02045** – Under certain circumstances, the device incorrectly flagged and dropped IP-Spoof packets.
- **02044** – An operation using SSH version 1 to access the device failed when using Radius for administration authentication.
- **02035** – The device did not allow URL filtered traffic when the URL queue was full and the URL queue size was too small to process heavy traffic.
- **02034** – In transparent mode, when selecting the WebAuth option in the WebUI for the V1-Untrust Zone, it appeared to take effect, but when closing the window and then returning to the V1-Untrust configuration window, the WebAuth option was no longer selected.
- **02019** – You could not use the WebUI to remove the key id and preshared key of the primary NTP server.
- **02018** – The Juniper Networks security appliance failed when applying debug commands, for example, the **set ffilter** command.
- **02001** – If a dynamically added route and a static route on a device both used the same interface default gateway as the next hop, when the dynamic route's interface default gateway changed, the static route's gateway did not change with it as expected.
- **01993** – You could not modify management services on interfaces configured in the WebUI environment to obtain addresses using DHCP.
- **01986** – In an NSRP environment, the primary device sometimes had more active XAuth users than the backup device because the garbage collection mechanism for IPSec SA removed XAuth users from the backup device at a more accelerated rate than it did from the primary device.

- **01985** – You could not schedule a policy using the WebUI.
- **01970** – Under certain circumstances, the Juniper Networks security appliance did not send email alerts.
- **01943** – When the DHCP payload (information included with the issuance of an IP address from a DHCP server) exceeded 550 bytes in length, the Juniper Networks security appliance was unavailable to send packets associated with the payload because the DHCP relay mechanism did not accept the packets.

4.7 Addressed Issues from Previous Releases

This section describes issues addressed in ScreenOS 5.0.0 release prior to ScreenOS 5.0.0r4.

- **37027** – The issue described in security advisory NS#54169 was addressed.
- **36935** – You could not reset the Juniper Networks security appliance to factory defaults settings if the NSRD wizard failed to connect the device to the Security Manager server.
- **36881** – In certain cases, using the pinhole to reset the Juniper Networks security appliance to factory default settings failed.
- **36865** – When a serial interface had no IP address, even if it was in the "UP" state, the routing entry pointing to the serial interface stayed inactive.
- **36838** – A device failure could occur if the interface information derived for a non-ip packet and received on a 24FE board is invalid.
- **36822** – Entering the **get policy** CLI command sometimes caused the Juniper Networks security appliance to reboot.
- **36819** – Under certain circumstances, IP-Spoof packets were incorrectly flagged and dropped.
- **36814** – With dialup user group VPN manually configured proxy-id, it could not be used for bi-directional dial-up vpn policy.
- **36773** – In Transparent mode, the IP Address Spoof Protection screen option caused the Juniper Networks security appliance to incorrectly drop packets even if the "Generate Alarms without Dropping Packet" option was enabled.
- **36766** – (Juniper NetScreen-5GT only) In transparent mode, during the initial connection attempt where the device had no established route to the destination, initial traffic was dropped on occasion by the device when AV scanning was active.
- **36736** – A device configured with DHCP and via a configlet was unable to connect to NSM.

- **36717** – When upgrading to ScreenOS 5.0.0, the maximum number of address groups allowed for Layer2 predefined zones incorrectly got set to the same number as for custom zones. As a result, if the number of address groups in Layer2 predefined zones surpasses the maximum number allowed, some address groups got removed during the upgrade.

- **32690** – (Juniper NetScreen-5GT only) When multiple devices were connected with AV scanning enabled on policies, no traffic passed through the devices. For example, if two devices were connected together and both had AV scanning enabled on policies, no traffic traversed the devices.

- **02081** – The active user table failed to clear automatically. New users were denied until the table was manually cleared.

- **02079** – In an instance where the system was running in transparent mode, when you enabled traffic shaping mode, the system dropped all packets.

- **02038** – Reboots occurred occasionally when traffic matched policies which had authentication enabled.

- **02027** – An SNMP sysObject OID reply returned in the wrong format.

- **02006** – Enabling DHCP Relay could cause a Juniper Networks security appliance to crash.

- **01972** – A DHCP relay packet sometimes caused a Juniper Networks security appliance to crash.

- **01971** – You were not able to add physical interfaces (different ports) of a Juniper Networks security appliance in the same redundant interface group.

- **01968** – (Juniper NetScreen-5GT only) Ident-reset packets that terminated on the device might have caused the device to restart.

- **01958** – An internal mishandling of the MAC cache could cause a security appliance to crash.
- **01944** – The group addresses for V1-untrust zone were getting lost after upgrading a device from a previous release. The group address for v1-untrust was incorrectly set to a maximum of 8 groups while it should have been 32.
- **01812** – Using un-initialized memory space when creating an outgoing packet caused the device to fail.

5. Known Issues

This section describes known issues with the current release.

- Section 5.1 "Limitations of Features in ScreenOS 5.0.0" identifies features that are not fully functional at the present time, and will be unsupported for this release. Juniper recommends that you do not use these features.
- Section 5.2 "Compatibility Issues in ScreenOS 5.0.0 on page 30" describes known compatibility issues with other products, including but not limited to specific Juniper NetScreen appliances, other versions of ScreenOS, Internet browsers, Juniper management software and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.
- Section 5.3 "Known Issues in ScreenOS 5.0.0 on page 32" describes deviations from intended product behavior as identified by Juniper Networks Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

5.1 Limitations of Features in ScreenOS 5.0.0

The following limitations are present in ScreenOS 5.0.0.

- **No Support for Packet Attribute Features** – The Juniper NetScreen-5000 Series systems do not support the aggressive aging, maximum fragment size, path MTU (Maximum Transmission Unit), and Interface MTU features.
- **Vsys for Group IKE ID** – Group IKE ID users cannot be used in a vsys if that vsys uses a shared untrust interface.

  W/A: Use a private Untrust interface (tagged VLAN subinterface or dedicated physical interface) for the vsys.

- **SSH Version 1 Interoperability** – The embedded SSH server in ScreenOS 5.0.0 has issues with the client from SSH Communications Security when operating in SSH version 1 mode.

  W/A: Use SSH version 2 or a different SSH version 1 client, such as OpenSSH.

- **Primary & Backup Interfaces** – (Juniper NetScreen-5XT) The primary and backup interfaces bound to the Untrust security zone cannot both use DHCP for address assignment at the same time. You can use DHCP for one interface and PPPoE for the other. Or you can use PPPoE for both interfaces.

- **Loading License Keys** – The Juniper NetScreen-5XP device does not properly load license keys via the WebUI. However, you can load license keys via the CLI using the **exec license-key** command.

- **Aggressive Aging** – The Aggressive Aging feature is not supported on the Juniper NetScreen-5000 Series devices.

- **SSHv2 Implementations** – The SSHv2 feature specification requires support for two implementations: OpenSSH and Secure CRT.

- **Upgrade Limitations** – When upgrading a device to ScreenOS 5.0.0UPGR in Transparent mode, the device experiences the following problems:
  - The device fails during upgrading from ScreenOS 4.0.1 to ScreenOS 5.0.0 in a VPN scenario.

  - In clear text situations (where traffic is not encrypted to pass through a VPN tunnel), after the upgrade to ScreenOS 5.0.0UPGR, the user had to run the **clear arp** and **clear mac-l** commands to enable the device to work because some ARP entries learn on the wrong port.

- **Updated Message ID Numbers** – The *NetScreen Message Log Reference Guide* (Part Number 093-0917-000 Rev. D) now contains an updated message ID number for Deep Inspection attack messages. The message, formerly associated with ID number 00001, now maps to ID number 00601. Although the ID number has already been changed in the guide, the ID number will not change in the code until the next revision of ScreenOS 5.0.0.

5.2 Compatibility Issues in ScreenOS 5.0.0

Below are the known compatibility issues at the time of this release. Whenever possible, a workaround (starting with "W/A:") has been provided for your convenience.

- **General Compatibility Issues**

– **Freeswan -** The Freeswan 1.3 VPN client is incompatible with ScreenOS 5.0.0 in certain configurations due to IKE features that Freeswan does not fully support. The result is that Phase 2 negotiations and Phase 2 SA will not complete if the following commands are enabled in 5.0.0:

> **set ike initiator-set-commit**
> **set ike responder-set-commit**
> **set ike initial-contact**

W/A: Unset these commands to ensure compatible configuration on the Juniper Networks security appliance.

- **Compatible Web Browsers -** The WebUI for ScreenOS 5.0.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, and Netscape Navigator 6.X for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS 10.x. Other versions of these and other browsers, were reported to display erroneous behavior.

- **SNMP Trap Type Values Different in ScreenOS 5.0.0** – ScreenOS 5.0.0 uses a different numbering system than previous ScreenOS releases to identify trap types. SNMP maps specific integers to indicate specific trap types, or events that generate traps. For example, the traditional SNMP trap type value for a Cold Start is 0. However, different vendors deploy different values to indicate different trap types. Please check the ScreenOS Messages Guide for the correct values in ScreenOS 5.0.0.

5.2.1 Upgrade Paths from Previous Releases

For detailed information on how to upgrade any Juniper Networks security appliance from ScreenOS 4.0.0 and later to ScreenOS 5.0.0, refer to the *NetScreen ScreenOS Migration Guide*. The migration guide provides step-by-step upgrade procedures and important information about upgrading Juniper Networks security appliances.

Important: To avoid downtime while upgrading devices in an NSRP configuration (active-passive or active/active), refer to the NetScreen ScreenOS Migration Guide *which describes procedures to upgrade the devices without causing any downtime.*

The migration guide also provides a step-by-step procedure to downgrade a Juniper Networks security appliance from ScreenOS 5.0.0 to ScreenOS 4.0.0 and later using the **exec downgrade** CLI command.

Juniper NetScreen-5000 series only: Before you upgrade a Juniper Networks security appliance to ScreenOS 5.0.0, we recommend that you verify the amount of memory on the device using the **get system** CLI command. You need 1 gigabyte of memory for Juniper NetScreen-5000. If you start upgrading the device and run into memory problems, you might see the following messages: "insufficient memory, call TAC" or "see release notes for upgrade instructions".

To avoid network downtime while upgrading devices in an NSRP configuration, refer to the Upgrading Devices in an *NSRP Configuration without Downtime* document. You can download this document from the location on the CSO where the revision image resides.

NSM does not support the NSRP Configuration without Downtime feature.

5.3 Known Issues in ScreenOS 5.0.0

The following are known deficiencies in features at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with "W/A:" If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

5.3.1 Known Issues in ScreenOS 5.0.0r9-FIPS

- **04960** – A burst of logs sent from a device running ScreenOS to the Security Manager server sometimes creates memory corruption, causing the device to fail.
- **03773** – The device drops some IPSec AH packets because of authentication failures, slowing the transfer of packets over an FTP session and sometimes causing large FTP data transfer sessions to fail.

- **03504** – The value of the sysUpTime variable from an SNMP query incorrectly displays as more than 497 days.

- **03495** – When the device drops packets after you issued the **set flow tcp-syn-check** command, ScreenOS does not log the drop instances.

- **03492** – When you enable the URL filtering service, the device drops HTTP Move packets.

- **03484** – If an interface rapidly repeatedly disconnects and reconnects, the number of OSPF routes drops below the number of expected routes causing the OSPF routing instance to clear its route table.

- **02751** – After resubmitting the ICMP destination unreachable setting through the device, the packet passes through the device, but the device generates the following log message:

  Apr 21 20:07:41 10.155.132.247 Iapetus: NetScreen device_id=Iapetus system-notification-00257(traffic):

  start_time="2004-04-21 21:12:34" duration=0 policy_id=22 service=icmp proto=1 src zone=Trust dst zone=Trust

  action=Permit sent=0 rcvd=0 src=69.91.47.31 dst=128.157.5.23 icmp type=8 session_id=19178

5.3.2 Known Issues from ScreenOS 5.0.0r8

- **03153** – When you attempt to download plugin and main program files in one file, the system generates errors.

- **03065** – When you download the asset recovery log from the WebUI, it appears with the incorrect date and time with the date being seven years different than the correct date.

- **02927** – Devices upload HTTP traffic very slowly after you enable both the anti-virus and URL filtering options in a policy on the device.

- **02869** – A Juniper NetScreen-5GT cannot deliver mail and the POP3 (Post Office Protocol 3) session times out when the device runs an anti-virus scan on an SMTP or POP3 policy.

- **02297** – An anti-virus scan drops connections with selected HTTP and HTTPS sites.

- **02266** – When you make one configuration change on a device, the device sometimes sends out more than one entry associated with that change to both the syslog and WebTrends servers.

- **01237** – In an NSRP configuration of two Juniper NetScreen-200 devices, you cannot save a device configuration from flash memory on the device to slot 1.

W/A: Execute the **save** command first, before executing the **save config from flash to slot1** command.

5.3.3 Known Issues from ScreenOS 5.0.0r7

None.

5.3.4 Known Issues from ScreenOS 5.0.0r6

None.

5.3.5 Known Issues from ScreenOS 5.0.0r5

None.

5.3.6 Known Issues from ScreenOS 5.0.0r4

- **38109** – When running 5,000 UDP sessions between two non-ScreenOS 5.0.0 devices and you upgrade one device to ScreenOS 5.0.0UPGR and the other to ScreenOS 5.0.0r4 via ScreenOS 5.0.0UPGR, only 3,000 of the UDP sessions synchronize properly.

- **37938** – The Juniper NetScreen-5000 or Juniper NetScreen-500 device sometimes fails after upgrading from an older version of ScreenOS to ScreenOS 5.0.0UPGR.

- **37925** – The L2TP tunnel and Telnet utility both do not work on the Juniper NetScreen-5000 or Juniper NetScreen-500 device after you upgrade the device from ScreenOS 4.0.1r4.2 to ScreenOS 5.0.0UPGR.

- **37901** – After you upgrade a Juniper NetScreen-5000 or Juniper NetScreen-500 device from a running ScreenOS 5.0.0UPGR B (backup) to ScreenOS 5.0.0UPGR M (primary), the current session on the device disappears.

- **02369** –You could not change the IKE/AUTH user password using the WebUI. The WebUI apparently takes the change but it does NOT change it when the configuration is viewed.

- **02297** – The Anti-Virus scanning engine drops connection with some HTTP/ HTTPS sites.

- **02207** – The NS Lookup operation completes without first authenticating to a WebAuth policy. The NS Lookup utility resolves unknown hostnames and URLs.

5.3.7 Known Issues from ScreenOS 5.0.0r3 for the 5000-M2

- **38001** – When you run the **get session** command, ScreenOS sometimes displays the policy ID number incorrectly as a negative number.

- **37993** – When enabled on a Juniper NetScreen-5000 Series system, the inter-zone IP record route option does not update the counter associated with this option. The record route option records the IP addresses of the network devices along the path that an IP packet travels. The destination device then can extract and process the route information.

- **37974** – When attack packets associated with the syn-and-fin, block-fragment, and unknown-protocol events attempt to enter a Juniper NetScreen-5000 Series system using a 5000-24FE secure port module when the system experiences heavy traffic, the system ASIC may not be able to transmit packets from the device. A *syn-and-fin* attack is an instance where a TCP header contains both syn and fin flags set. A *block-fragment* event is when the NetScreen system attempts to deny entry of fragments of a larger packet that have been disassembled so they may enter the device with undetected attack content. An *unknown-protocol* attack is a packet that contains a protocol that the NetScreen system does not recognize.

- **37712** – You cannot remove an SSH key from a Vsys by running the command **unset ssh pka all**. When you run the command, ScreenOS does not remove the SSH key and displays a generic error message.

- **37640** – You can create a password name with a greater number of characters than the usual character limit (15) for passwords in ScreenOS for the Juniper NetScreen-5000 Series systems.

- **37497** – You could not create more than 1,500 IKE sessions (attempting to establish VPN tunnels) while the system experienced heavy traffic.

- **37422** – When you loaded an older ScreenOS configuration image on a new Juniper NetScreen-5000 Series system, the system failed. If the system now functions correctly, remaining active with ScreenOS displaying an error message on the console indicating a mismatch between the loaded image and the image(s) the system accepts.

- **37303** – You can create an environment variable with a greater number of characters than the usual character limit (255) for environment variable strings in ScreenOS for the Juniper NetScreen-5000 Series systems.

- **36926** – After you created the maximum number of sessions (1 million) allowed on the Juniper NetScreen-5000 Series system, and you disable a policy, the sessions do not age out in the expected way from the system.

- **36807, 36876** – When a 100Mbps link between a Juniper NetScreen-5000 Series system and another device reverts to a 10Mbps throughput level on the other device, the Juniper NetScreen-5000 Series system remains at the 100Mbps throughput level when it should synchronize with the speed of the connected device and revert to the lesser speed.

5.3.8   Known Issues from ScreenOS 5.0.0r3

None.

5.3.9   Known Issues from ScreenOS 5.0.0r2

- **35620 -** (Juniper NetScreen-5GT only) If a policy is using a local address, any modification to the netmask of the address produces a trace dump on the console. This modification should not be a permitted action for the device.
- **36365 -** In the WebUI, on the Traffic Log page for policies (under Reports), the table displaying the information might disappear after viewing multiple pages of traffic logs.

  W/A: Refresh the Traffic Log page for policies by clicking the Refresh button on your Internet Browser.

5.3.10 Known Issues from ScreenOS 5.0.0r1

- **Documentation Correction -** Page 3 of the *What's New in NetScreen ScreenOS 5.0* states incorrectly that Juniper Networks security appliances support routing based on the source interface. The current implementation does support routing based on source IP address.
- **36018 -** (Juniper NetScreen-5GT only) The two month entitlement expiration notice in the event log is triggering during the incorrect timeframe. For example, if the AV entitlement expires in 52 day, the event log indicates "License key av_key is about to expire in 2 months".
- **35582 -** In an NSRP configuration, active/active or active-passive, if you move a physical interface to a different zone on one device, you must manually do the same on the other device because this type of change does not get automatically synchronized.
- **35516 -** In an active-passive NSRP configuration, when you load a PKA key onto the master device, the master does not automatically synchronize the backup device.

  W/A: Manually synchronize the two devices.

- **35439 -** (Juniper NetScreen-5GT only) Within the WebUI, identical routes are displayed on multiple pages. When the number of routing table entries

exceeds the maximum number of routes permitted on a single page, all subsequent pages display the routes from the first page.

- **35417 -** If you set the guaranteed or maximum bandwidth (GBW or MBW) higher than the interface bandwidth, traffic does not pass through if there is a policy configured that specifies traffic shaping.

  W/A: Adjust the GBW or MBW to be equal or less than the interface bandwidth.

- **35336 -** If you enabled VPN tunneling for syslog traffic and the source interface is bound to a zone that contains multiple interfaces, after upgrading a device from ScreenOS 4.0.0 to ScreenOS 5.0.0, the source interface might have changed.

  W/A: After upgrading the Juniper Networks security appliance, verify the VPN settings for syslog and modify if necessary.

- **35238 -** For devices in an NSRP configuration, active/active or active-passive, you have to manually issue the **delete ssh device all** CLI command on both devices.

- **34950 -** (Juniper NetScreen-5000 only) Failover between two layer 2 interfaces in the same layer 2 security zone is not supported.

- **34922 -** (Juniper NetScreen-50 only) You cannot configure a VSI when the Juniper Networks security appliance is in an active-passive NSRP configuration.

- **34880 -** (Juniper NetScreen-5GT only) Issuing the CLI command 'set interface <interface> manage ident-reset' displays incorrectly as 'set interface <interface> ident-reset' (without the word "manage" in the configuration file).

- **34670 -** (Juniper NetScreen-5GT only) Issuing the CLI command 'set/unset firewall exclude log-self exclude ike' does not change the state of "Log Self for IKE". The 'get firewall' command displays "Log Self for IKE" constantly in the "Off" state.

- **34663 -** Enabling the RTO mirror group direction feature using the **set nsrp rto-mirror id** <id> **direction** { **in** | **out** } CLI command, might cause the preempt mode feature not to work.

- **34414 -** The Juniper Networks security appliance does not perform a revocation check on the signature attack database upon requesting an update.

- **34070 -** (Juniper NetScreen-5GT only) The event message 'AV: Suspicious client <Source IP> <Source Port> -> <Destination IP> <Destination Port> used <X> percent of AV resources, and exceeded the max. of <y> percent'

displays only when you issue a 'get event' CLI command, and not when you issue a 'get log event' CLI command.

- **33916 -** A Juniper Networks security appliance supports a maximum of 256 OSPF interfaces.

- **33598 -** For inter-vsys traffic, if both vsys define a policy with user authentication, the Juniper Networks security appliance does not prompt the user for authentication for each policy, but only once when it matches the first policy.

- **33544 -** Normally upon startup, a Juniper Networks security appliance with the URL filtering feature enabled, tries to connect to a Websense server. Currently this attempt to connect to a Websense server fails and the Juniper Networks security appliance logs the event.

- **33027 -** Juniper Networks security appliances do not support policy-based dialup VPN and MIP if the MIP is configured on the tunnel interface which belongs to a tunnel zone.

  W/A: For dialup user VPNs only: use routing-based VPN and configure the MIP on a tunnel interface bound to a security zone.

- **32983 -** You can select multiple services in a policy, but later on, if you want to modify the services to ANY, the Juniper Networks security appliance does not let you. Instead, you get a message prompting you to use the multiple service selection dialog box, which does not contain ANY, to modify the services.

  W/A: In the multiple service selection dialog box, remove all but one service from the previous selection, and then click **OK**. Next, select "ANY" from the Service drop-down list.

- **32159 -** Juniper Networks security appliances do not support a second level of certificate verification if the end entity certificate and OCSP responder certificate are issued by the same CA.

- **32077 -** (Juniper NetScreen-5GT only) When you enable or disable HTTP Webmail functionality, log entries are not generated in the event log (i.e. 'set/unset av http webmail enable'; 'set/unset av http webmail url-pattern-name <name for the URL pattern>').

- **32072 -** (Juniper NetScreen-5GT only) When you disable AV functionality for HTTP, SMTP, and POP3, log entries are not generated in the event log (i.e. 'unset av scan-mgr content http'; 'unset av scan-mgr content smtp'; 'unset av scan-mgr content pop3').

- **31364 -** When performing source port translation for passive FTP data channel, the Juniper Networks security appliance translates the source port

number to the same port number as the original destination port. This does not affect traffic.

- **30844 -** When AV is enabled, you cannot download files to the Juniper Networks security appliance through a VPN using the WebUI.

  W/A: Specify a permit policy and place it above the policy with AV in the policy list.

- **30842 -** Source and destination NAT are not supported for RTP and RTCP traffic for H.323.

- **28878 -** Removing a vsys does not free the memory (30 bytes) used by that vsys.

- **28138** – The Websense server provides erroneous protocol version information, which the Juniper Networks security appliance displays.

- **28016** – Juniper Networks security appliances do not support a MIP in the same zone as the destination host.

  W/A: Use policy-based destination NAT.

5.3.11 Known Issues from Previous Releases

- **27083** – When you enter the **set service** command to create a custom service, the Juniper Networks security appliance does not check if you entered valid source and destination port numbers.

- **25841** – When you configure RIP on the Juniper Networks security appliance and enter the **get config** command, the output displays the **set protocol rip** command twice. This is a display issue that does not affect the performance of the device.

6. Getting Help

For further assistance with Juniper Networks products, visit

www.juniper.net/support

Juniper Networks occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your NetScreen device with Juniper Networks at the above address.

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-ISG 2000, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.
1194 N. Mathilda Ave.
Sunnyvale, CA 94089-1213
U.S.A.
ATTN: General Counsel

www.juniper.net