NetScreen Release Notes

Product: NetScreen-Hardware Security Client, NetScreen-5XP, NetScreen-5XT, NetScreen-5GT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400

Version: ScreenOS 5.0.0r6

Release Status: Public Release

Part Number: 093-1310-000 Rev. A

Date: 04-20-04

Contents

1. Version Summary

ScreenOS 5.0.0r6 is the latest version of ScreenOS firmware for the NetScreen-Hardware Security Client, NetScreen-5XP, NetScreen-5XT, NetScreen-5GT, NetScreen-25, NetScreen-50, NetScreen-200 series security appliances, and the NetScreen-500 and NetScreen-5000 series security systems.

The ScreenOS 5.0.0r6 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 NSM (NetScreen-Security Manager 2004), NetScreen's new 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.

2. New Features and Enhancements

The following is a partial list of new features and enhancement in this release of ScreenOS. For a complete list and descriptions of new features and enhancements in ScreenOS 5.0.0, refer to the *NetScreen ScreenOS Migration Guide*.

2.1 New Features and Enhancements for 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.

2.2 New Features and Enhancements for ScreenOS 5.0.0r1

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.

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 *NetScreen ScreenOS Concepts & Examples Reference Guide* for ScreenOS 5.0.0.

Note: *You must register your product at www.netscreen.com/cso 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 NetScreen 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 NetScreen 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 *NetScreen ScreenOS Migration Guide*.

3.1 Addressed Issues in ScreenOS 5.0.0r6

- **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 intermittenly failed.
- **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.
- **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.

- **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 NetScreen-50 devices in an Active-Passive environment in instances when the active device stopped creating new sessions when the session table was full.
- **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
- **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.
- **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.
- **02362** – In some instances, a debug session for NAT on the device timed out before the session timeout value elapsed.
- **02344** – When you tried to bind a PKA key to an admin account using the WebUI, the device generated a trace dump.
- **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.
- **02298** – Commands related to NHTB (Next Hop Tunnel Binding) did not run when you use a blank character when creating a tunnel name for NHTB.
- **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 NetScreen-5GT had AV HTTP scanning enabled.

- **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.
- **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.
- **02388** – You could not set the range of IP addresses available for a device through a DHCP address assignment session when using the auto-probing detection feature in the WebUI.
- **38200** – A non-specific error in H323 caused memory leaks in device sessions.
- **02413** – When you issued the command **set ike gateway**, the device always created a test certificate peer certificate type x509-signature.
- **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).
- **01657** – A redundant VPN did not fail over with a RTO (Run-Time Operation) synchronization enabled.
- **01793** – A redundant interface incorrectly learned an ARP when no IP address was configured for the interface.
- **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).
- **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.
- **02416** – If you rebooted a NetScreen-5200 after configuring NHTB entries in the current session on the system, the device lost the entries after the reboot.
- **02052** – NAT Traversal (NAT-T) for IPSec did not behave correctly when both the initiator and responder were behind NAT devices.
- **02041 –** The NetScreen-5000-specific command **unset/set hardware wdt-reset** was incorrectly available on all NetScreen devices.
- **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.

- **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.
- **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.
- **02377** – The NetScreen-200 did not always free up memory after VPN tunnels closed, requiring a manual device reboot to recover.
- **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.
- **02429** – HTTP packets could not pass through the NetScreen-5200 running ScreenOS 4.0.0 if you issue both the **unset flow tcp seq** and **set flow tcp syn** commands.
- **02446** – Unfreed memory buffers could be allocated to the point where the device could not send management traffic data.
- **02412** – The SNMP Get response values were not correct for the ifInOctets and ifOutOctets statistics.

3.2 Addressed Issues in ScreenOS 5.0.0r5

None.

3.3 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 NetScreen device, you experienced a two- to three-minute delay when scrolling through the Policy List page in the WebUI.
- **36939** – The NetScreen-25 and NetScreen-50 did not support up to eight VLANs as expected and the 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. NetScreen devices 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** – (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 NetScreen device to fail during restart.
- **02050** – Configuring an address group from an Apple computer using Internet Explorer sometimes caused a NetScreen device 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 NetScreen device 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 NetScreen device 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 NetScreen device was unavailable to send packets associated with the payload because the DHCP relay mechanism did not accept the packets.

3.4 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 NetScreen device to factory defaults settings if the NSRD wizard failed to connect the device to the NSM server.
- **36881** – In certain cases, using the pinhole to reset the NetScreen device 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 NetScreen device to crash.
- **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 NetScreen device to incorrectly drop packets even if the "Generate Alarms without Dropping Packet" option was enabled.
- **36766** – (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** – (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** – Core dumps 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 NetScreen device to crash.
- **01972** – A DHCP relay packet sometimes caused a NetScreen device to crash.
- **01971** – You were not able to add physical interfaces (different ports) of a NetScreen device in the same redundant interface group.
- **01968** – (NetScreen-5GT and NetScreen-HSC 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 NetScreen device 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.

4. Known Issues

This section describes known issues with the current release.

- Section 4.1 “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. NetScreen recommends that you do not use these features.
- Section 4.2 “Compatibility Issues in ScreenOS 5.0.0 on page 13” describes known compatibility issues with other products, including but not limited to specific NetScreen appliances, other versions of ScreenOS, Internet browsers, NetScreen 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 4.3 “Known Issues in ScreenOS 5.0.0 on page 14” describes deviations from intended product behavior as identified by NetScreen Test Technologies through their verification procedures. Again, whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

4.1 Limitations of Features in ScreenOS 5.0.0

The following limitations are present in ScreenOS 5.0.0.

- **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** – (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 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 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.

4.2 Compatibility Issues in ScreenOS 5.0.0

Below are the known compatibility issues at the time of this release. Whenever possible, a work-around (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 NetScreen device.

- **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.

4.2.1 Upgrade Paths from Previous Releases

For detailed information on how to upgrade any NetScreen device 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 NetScreen devices.

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

NetScreen-5000 series only: Before you upgrade a NetScreen device 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 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.

4.3 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.

4.3.1 Known Issues in ScreenOS 5.0.0r6

- **38268** – A NetScreen device running a BGP peer virtual routing instance cannot use an MD5 type password when the device is connected to a Juniper Networks router.

4.3.2 Known Issues in ScreenOS 5.0.0r5

None.

4.3.3 Known Issues in 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 NetScreen-5000 or 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 NetScreen-5000 or NetScreen-500 device after you upgrade the device from ScreenOS 4.0.1r4.2 to ScreenOS 5.0.0UPGR.
- **37901** – After you upgrade a NetScreen-5000 or 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.

- **02372** – If you run an OSPF virtual routing instance to pass through a route-based VPN under heavy traffic conditions, the device could continually spawn new sessions for the routing instance.
- **02369** – You cannot change the IKE/AUTH user password in the WebUI environment.
- **02362** – The device drops sessions because the counter that measures the number of packets occurring as through traffic over the device inadvertently counts packets only reaching the device as through packets to the device, causing the through traffic counter threshold to be exceeded incorrectly.
- **02342** – An OpenSSH session continues to use password authentication even when password authentication is not an option for SSH**.**
- **02335** – The SNMP iftype value is wrong on the NetScreen-5XP.
- **02326** – The device inadvertantly creates numerous superfluous sessions if a packet attempting to enter the device contains both a destination IP address that is unicast and a destination MAC address that is multicast.
- **02324** – When configuring a non-default DHCP address range on the HSC (Hardware Security Client) device using the configuration wizard in the WebUI, the Summary screen indicates that you have overwritten the default range (beginning with address 192.168.1.33), although after you save your changes, the default range remains.
- **02323** – When issuing an FTP **put** or **get** command through the device to the device server, the WebUI always indicates any policies on the device to have a DENY action even if the policy contains a PERMIT action.
- **02298** – If you use a blank character (by typing the space bar) when creating a name for an NHTB (Next Hop Tunnel Binding), the device does not accept the command.
- **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.
- **02194** – If you issue the **get log traffic policy** command when running more than 15,000 VPN tunnels and an ICMP session, the device fails.

4.3.4 Known Issues from ScreenOS 5.0.0r3

- **02001 -** When modifying the default gateway of an interface using DHCP or PPPOE, the Netscreen device does not update the corresponding routing entry accordingly.

4.3.5 Known Issues from ScreenOS 5.0.0r2

- **36708 -** You cannot view the traffic logs for a vsys if you entered the vsys as a root admin user.

  W/A: You must enter each vsys as the vsys admin to view the traffic logs for that vsys.

- **35620 -** (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.
- **36494 -** Upon startup, NetScreen devices using PPPoE might generate a warning message informing that the interface gateway command is 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 NetScreen device while it is performing an operation in flash might damage the data on the device and cause the device not to restart or to lose the configuration.

  W/A: Wait until the NetScreen device has completed its operation in flash before restarting 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.

- **34279 -** (For NetScreen-5000 Series) NetScreen devices might unexpectedly drop traffic that is processed by the CPU module and that matches a policy in which the “Diffserv” option is enabled.

  W/A: Disable the “DiffServ” option on the policy.

4.3.6 Known Issues from ScreenOS 5.0.0r1

- **Documentation Correction -** Page 3 of the *What's New in NetScreen ScreenOS 5.0* states incorrectly that NetScreen devices support routing based on the source interface. The current implementation does support routing based on source IP address.
- **36670 -** You can create more VLANs on a NetScreen device than the number of VLANs the device officially supports. However, doing this might cause unexpected results. Refer to the specifications sheet for your NetScreen product to learn how many VLANs it supports.
- **36235 -** Adding the pre-defined service entry "ANY" in a multiple service policy may result in a system reboot.

  W/A: Do not enter "ANY" as a service in a multiple service policy.

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

  W/A: Unset the policy that uses the VIP or MIP before you change the IP address of an interface. For interfaces using DHCP or PPPoE, do not use virtual IP addresses.

- **36018 -** (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".
- **35977 -** (NetScreen-5XT only) The NetScreen device might drop TCP traffic because it miscalculates the length of the tcp-syn-check.

  W/A: Do not enable the TCP sequence checking feature on the device.

- **35904 -** (NetScreen-5GT only) NetScreen devices need to support two incoming IPSec keys. When the software lifetime is in use and after the re-key is successful, the device should permit traffic using older SA's to traverse the device.
- **35735 -** A root administrator cannot manage the root system from a host that resides on a virtual system.

  W/A: You must connect from the root network to be able to manage the root system.

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

W/A: Set auto-negotiation on the interface. You can do this using the **set interface interf_name phy auto** CLI command.

- **35615 -** (NetScreen-5GT only) Any policies within the device indicates traffic shaping is active for the policy. Issuing a 'get policy' CLI command displays an "X" under the "T", for traffic shaping, in each policy. However, issuing a 'get policy id <number>' CLI command indicates that traffic shaping is turned "off".
- **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.
- **35528 -** In an active/passive NSRP configuration, you must set a manage IP on both devices to enable each device to connect to the entitlement server and retrieve signatures.
- **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 -** (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 NetScreen device, 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 -** (NetScreen-5000 only) Failover between two layer 2 interfaces in the same layer 2 security zone is not supported.

- **34922 -** (NetScreen-50 only) You cannot configure a VSI when the NetScreen device is in an active/passive NSRP configuration.
- **34880 -** (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 -** (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 NetScreen device does not perform a revocation check on the signature attack database upon requesting an update.
- **34070 -** (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 NetScreen device supports a maximum of 256 OSPF interfaces.
- **33598 -** For inter-vsys traffic, if both vsys define a policy with user authentication, the NetScreen device does not prompt the user for authentication for each policy, but only once when it matches the first policy.
- **33544 -** Normally upon startup, a NetScreen device 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 NetScreen device logs the event.
- **33027 -** NetScreen devices 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 NetScreen device 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 -** NetScreen devices 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 -** (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 -** (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 NetScreen device 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 NetScreen device 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.
- **29619** - When you use the CLI to configure SCEP, you cannot specify an already defined Certificate Authority as the recipient of the certificate requests.

  W/A: Use the WebUI.

- **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 NetScreen device displays.
- **28016 -** NetScreen devices do not support a MIP in the same zone as the destination host.

  W/A: Use policy-based destination NAT.

4.3.7 Known Issues from Previous Releases

- **27083 -** When you enter the **set service** command to create a custom service, the NetScreen device does not check if you entered valid source and destination port numbers.
- **25841 -** When you configure RIP on the NetScreen device 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.

5. Getting Help

For further assistance with NetScreen products, visit

www.netscreen.com/services/contact_tac

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

www.netscreen.com/cso

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com