Juniper Networks

NetScreen Release Notes

Product: NetScreen-Hardware Security Client, NetScreen-5XT, NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-ISG 2000

Version: ScreenOS 5.2.0r3

Release Status: Rev A

Part Number: 093-1778-000

Date: 11-30-05

Contents

1. Version Summary

ScreenOS 5.2.0r3 is the latest release version of ScreenOS firmware for the NetScreen-5XT, NetScreen-5GT, NetScreen-5GT ADSL, NetScreen-Hardware Security Client, NetScreen-25, NetScreen-50, NetScreen-204 and NetScreen-208 security appliances, and the NetScreen-500, NetScreen-ISG 2000, NetScreen-5200 and NetScreen-5400 security systems.

The ScreenOS 5.2.0r3 release is interoperable with, and provides basic support for all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions.

2. New Features and Enhancements

For a list and descriptions of new features and enhancements in this release, refer to the *NetScreen ScreenOS Migration Guide*.

Note: *You must register your product at http://support.juniper.net 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

The following section identifies the major change to the default behavior from the 5.1 release.

- The session MAC address is no longer used to send traffic back to the source. From now on, the return traffic goes to the MAC address of the Layer 3 next hop (after a route lookup) instead of the MAC address that the traffic (http request) came from (the session MAC address).

There were other changes in default behavior between ScreenOS previous releases. For detailed information on those changes, refer to the *NetScreen ScreenOS Migration Guide*.

4. Addressed Issues

The following sections identify which major bugs have been fixed in each release of ScreenOS 5.2.0.

4.1 Issues Addressed from ScreenOS 5.2.0r3

- **07846** – Device failed while handling ISAKMP packets with invalid and/or abnormal contents.
- **07771** – Insufficient retry attempts to dequeue packets from the ASIC caused NSRP data forwarding to fail.
- **07569** – Upgrading firmware version from 5.2r2 to 5.3r1 caused device failure.
- **07558** – Repeatedly resetting the device led to device failure.
- **07553** (NetScreen ISG-2000) – After upgrading the device, it showed the error message, "### DIMM is not CL2 (23: 0x75, 63: 0x21)" and no longer handled traffic.
- **07504** – A certain sequence of operations on a NSRP pair led to the backup device to experience some failures.
- **07488** (NetScreen-Security Manager) – Updating the device to bring down a link failed.
- **07228** – The device reset when an Auth Policy was added.
- **07218** – Some VPN configurations led to device failure.
- **07207** – Certain traffic patterns requiring user authentication caused device failure.
- **07206** – In some configurations, mail queue traffic led to device failure.
- **07177** – After an IGMP configured sub-interface had participated in multicast, it could no longer be deleted or assigned to the null zone.
- **07156** – The device reset when a Peer VPN sent an IP address as the IKE phase I ID instead of an FQDN type.
- **07132** – Dial backup did not work (modem does not dial back) due to PPP LCP keepalives that were not sent.
- **07082** – Inbound NAT incorrectly allowed other traffic to cross the firewall.
- **07074** – Large numbers of policies led to incorrect RMS calculations.
- **07052** – "Unknown Keyword" error result of custom DI context list not being available from the WebUI.
- **07023** – Unusual fragmented packets led to device failure.
- **06958** – Backup device did not accept interface monitor threshold setting.

- **06947** – The DSCP priority option for a policy was not synced to the NSRP backup device.
- **06942** – Typo in error message "can't delete secondary ip since it is in using".
- **06934** – With some frame size, Source DR sends PIM register messages with incorrect PIM checksum.
- **06866, 06845** – SCP file transfers failed after the first transfer completed successfully.
- **06854** (NetScreen ISG-2000) – DIFFSERV code point marking was unavailable from the WebUI.
- **06808** – Cannot use port 161 SNMP when VIP is set to same as Untrust.
- **06795** (NetScreen-5GT) – Home-Work port mode loaded the policy incorrectly.
- **06779** – VPN traffic went through the incorrect interface after an interface failover occurred.
- **06770** – In some scenarios, the session synced over to backup and selected a different route. When the box became the primary device, traffic matching these sessions failed.
- **06743** – Incorrect handling of MSRPC messages occasionally caused a boot loop and the device to reset.
- **06738** – When the local interface route was deleted on the primary device, it was unintentionally deleted on the backup device.
- **06732** – A Java IO exception error was received when trying to run a NetScreen-Security Manager delta config, config summary, or push updates to the firewall cluster.
- **06719** – Some web site URLs did not work with HTTP URL Filtering enabled.
- **06708** – VOIP through a TCP proxy led to device failure.
- **06678** – FPGA malfunction led to device failure
- **06675** (NetScreen-5GT) – In PPPoE configuration, timeouts occurred when connected to an ADSL router.
- **06657** – The active user table displayed IPs that were not in the local Trust zone.
- **06614** – WebAuth was incorrectly used if the VSYS ID was greater than 255.
- **06613** – In some cases, the session table on the device filled, which led to device failure.
- **06586** – Forwarding large bootp packets was unsupported.
- **06573** (NetScreen-5GT and NetScreen-25) – Session timeouts happened in half the configured time.

- **06562** (NetScreen ISG-2000) – Multicast Transparent mode traffic led to slow throughput.
- **06558** – In a EBGP and IBGP environment, when routes learned from EBGP were redistributed, IBGP peers bounced.
- **06552** – Routes defined on local interfaces were incorrectly deleted during configuration sync from an NSRP peer.
- **06547** (WebUI) – Not able to enable the Antivirus scan-mgr on a policy.
- **06520** – VPN proxy ID information was unavailable after the device was restarted or synced.
- **06517** – When XAuth is configured with external RADIUS server and local IP Pool, the allocated IP address on the gateway side was improperly released.
- **06511** – Incorrect handling of unintended multicast S, G, RTP prune for (S,G).
- **06482** – VOIP traffic led to intermittent device failure.
- **06452** – When password authentication was disabled for specified administrators on the device, the administrator was still able to authenticate himself with password authentication when using the OpenSSH client.
- **06450** – IPSec Passthrough device halted VPN traffic because there was a change in the DIP address.
- **06441** – Antivirus option was unavailable when a policy is configured for multi-cell context.
- **06414** – Gratuitous ARPs are not sent for inactive VSI redundant interfaces manage-ip.
- **06401** (NetScreen-5GT) – In some cases, SIP inbound calls failed while outbound calls worked.
- **06366** – After upgrading a device, it could reset when using the **exec nsrp sync global-conf save** CLI command.
- **06358** – Large packets going into a policy based VPN tunnel were first fragmented and then encapsulated.
- **06344** – High BGP activity led to an unresponsive WebUI.
- **06334** – A device showed high flow CPU numbers even if a small amount of traffic was present.
- **06317** – The **set syslog VPN** CLI command, was deprecated in 5.2.
- **06312, 06295** – Intermittent device failure due to Policy database failure.
- **06301** – Occasionally, the processing of a PKI certificate caused device failure.

- **06297** – In some cases, the RADIUS authentication over policy based tunnels stopped working.
- **06294** – In some situations, the device sent DNS packets with incorrect source and/or destination addresses.
- **06283** – Only able to add 78 ARP entries to the ARP table. The remaining ARP packets were dropped. This was caused by insufficient memory allocated for this action.
- **06282** – Device SYN-flood detection was triggered too early.
- **06253** – A device occasionally reset after an invalid short frame was received.
- **06245** – The total number of redistributed routes exceeded the system limit messages received because there was an incorrect redistribute route counter.
- **06240** – Source-based NAT did not occur on traffic from Trust to DMZ.
- **06223** – With TCP_SYN_Check disabled, and a large number of TCP RST packets received the device experienced periods of high CPU and Telnet access was unavailable.
- **06221** – Device incorrectly used egress interface IP as RADIUS NAS-IP when the source interface was specified.
- **06205** – Ucast Pkt counters were incorrectly calculated.
- **06199** – Email notification did not work with some email servers.
- **06181** – Race condition in the VPN crypto engine intermittently caused the device to reset.
- **06170** – In some configurations, a VOIP call set up through a tunnel interface failed.
- **06161**– The policy search timed out in some cases, particularly when the policy configuration was large.
- **06160** (NetScreen-5XP and NetScreen-5XT) – After certain sequence of policy insert/delete/modify the new policy add/change was blocked. For example, changing a policy service to ANY resulted in the traffic no longer matching that policy; thus being denied by the explicit Deny Policy.
- **06127** – In some scenarios, the customer saw some system errors when the packets matched a session that had already been aged out.
- **06104** – Improved successive EBGP update performance.
- **06095** (WebUI) – An error message was displayed when configuring a sub-interface.
- **06093** – Very large files did not pass through the TCP proxy when AV or UF were enabled.

- **06074** – Device did not synchronize the physical port settings after a change was made from full to half duplex mode.
- **06052** – RTSP traffic caused device failure.
- **06036** – SNMP MIB walk hung.
- **06031** – PPPoE did not insert the default route into routing table.
- **06030** – In some cases, deleting a VSYS and VPN led to device failure.
- **05983** – RIP summary routes were not added to the routing table.
- **05981** (WebUI) – An error occurred when an aggregate interface or sub-interface was deleted.
- **05977** – Antivirus option was lost when configuring a policy in multi cell format.
- **05965** – RTSP traffic with MIP failed. QuickTime player did not receive the streaming data from the Helix server.
- **05961** – In some situations, passive FTP traffic hung.
- **05956** – Configuration of a policy with Application and ANY service port in a multi-cell format was incorrectly saved.
- **05945** – With some DIP/MIP configurations, the RTSP traffic did not work.
- **05867** – The device dropped traffic in an Active/Passive NSRP configuration after fragmented IP multicast packets were processed.
- **05861** – RTSP traffic with MIP did not work.
- **05850** – Objects were not returned in OID order for SNMP get/get_next requests.
- **05831** – In some situations, sessions were not properly duplicated to a backup device.
- **05759** – In some cases, the console became disconnected.
- **05744** – Interface counter stopped increasing when it reached its limit.
- **05718** – In some cases, the telnet task table filled with disconnected Telnet jobs.
- **05683** – In some cases, processing IKE certificates resulted in device failure.
- **05623** – When the name of a VPN object was modified on an active node, a new VPN was generated on the backup device.
- **05586** – The hardware counter report was blank for all interfaces.
- **05545** – Some WebUI Help URLs for Deep Inspection attack objects did not work properly.
- **05495** – User experienced problems with TCP sequence check on failback after a failover when NSRP was enabled with the **unset vsd 0** CLI command.

- **05478** – Unsupported communication between IKE peers caused device failure.
- **05474** – Manually setting the GE copper interface to 1000/full did not save.
- **05448** – Received "Can't allocate xxxx bytes memory" and "Cannot check AV pattern file. VSAPI code: -98" errors due to an AV memory allocation issue.
- **05447** – During a cold start sync of a Backup NSRP A/P device, a portion of the sessions were dropped if there was more than 30,000 sessions.
- **05420** – In some cases, a change in the IDS screen configuration caused traffic to stop.
- **05385** (WebUI) – Microsoft Internet Explorer (IE) did not display < and > correctly in event logs.
- **05367** (NetScreen-5GT ADSL) – Only able to save or receive a PPPoE/PPPoA mask length of /32.
- **05331** – CLI incorrectly allowed the primary port configuration for a redundant sub-interface.
- **05322** (NetScreen ISG-2000) – The device appended an extra 14 bytes to every packet that passed through the device.
- **05309** – A pass-through ESP fragment traffic failed in Transparent mode.
- **05297** – In some NSRP configurations, the device generated false SYN-flood alarms.
- **05254** – The device did not display OSPF routes in routing tables.
- **05169** – In some cases, the DNS servers were over written with PPPoE data.
- **05165** – In the WebUI report, 'event level' incorrectly had content of 'event description'.
- **05158** – The device occasionally failed during heavy WebAuth traffic when external authentication servers for WebAuth authentication were used.
- **05123** – After a tunnel failover or P2 rekey, the ESP session did not update route and tunnel information properly.
- **05101** – Under certain conditions, log messages were erroneously duplicated.
- **05001** – Intermittent failures occurred while issuing a **get** CLI command because of a missing check for null strings.
- **04978** – Antivirus information in the WebUI incorrectly contained 'Recent Event' information.
- **04960** – Occasionally disconnecting from the NetScreen-Security Manager server caused device failure.
- **04882** – The device did not allow PPPoE instances in non-untrust zones with separate virtual routers.

- **04813** – Advanced license key was incorrectly transferred during synchronization of NSRP peers.
- **04810** – A secondary device could not establish OSPF adjacencies after OS was upgraded.
- **04221** – The 'remove' option on the WebUI did not remove a CA certificate.
- **03976** – The policy "before" option did not work with existing policies.
- **03771** – CLI displayed the up-time correctly while SNMP reply displayed it incorrectly.
- **03714** – When loopback sessions occurred, the auth table entry session count showed additional disconnected sessions.
- **03498** (NetScreen ISG-2000) – Occasionally the device reset when the **exec nsrp sync global checksum** CLI command was executed.
- **02751** – ICMP destination unreachable message was displayed as type 8 in the log.

4.2 Issues Addressed in ScreenOS 5.2.0r2

- **50579** – Three commands caused CPU packet issues.
  - **set zone trust screen fin-no-ack**
  - **set zone trust screen syn-fin**
  - **set zone trust screen tcp-no-flag**

  Enabling all of the above commands caused the CPU to see every multicast and unicast packet. Disabling the above commands caused the CPU to see no packets. Having one or more of the commands enabled caused the CPU to see every packet.
- **50566** – Enabling syn cookie created invalid packet information, causing the packet to loop.
- **50173** – When enabling Surfcontrol with caching, the device crashed.
- **50166** – The active user table did not show an accurate session number on the device.
- **50093** – The device crashed when Deep Inspection (DI) was enabled and when http and ftp attacks occurred.
- **50091** – The device crashed when packets encountered DI policy enabled interfaces.
- **49339** – (NetScreen-5GT) The dial command would not execute.
- **49144** – In a virtual router, the protocol “H” could be deleted.
- **45383** – When a tunnel session was anchored on a loopback interface, the device dropped packets that went into the packet-shaping queue.

4.3 Issues Addressed from ScreenOS 5.2.0r1

Because this is an initial r1 release, there are currently no addressed issues.

5. Known Issues

This section describes known issues with the current release.

- Section 5.1 "Limitations of Features in ScreenOS 5.2.0" identifies features that are not fully functional at the present time, and will be unsupported for this release.
- Section 5.2 "Compatibility Issues in ScreenOS 5.2.0 on page 13 describes known compatibility issues with other products, including but not limited to specific security appliances, other versions of ScreenOS, Internet browsers, security 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 5.2.0 on page 13 describes deviations from intended product behavior as identified by Juniper NetScreen product 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 5.2.0

This section describes the limitations in various features in ScreenOS. They apply to all platforms, unless otherwise noted.

5.1.1 Limitations in ScreenOS 5.2.0r3

None.

5.1.2 Limitations in ScreenOS 5.2.0r2

The following limitations are present in ScreenOS 5.2.0.

- **NetScreen-500 OS Loader** – Before you can upgrade a NetScreen-500 to ScreenOS 5.2.0, you must upgrade the OS loader and file system. For additional information, refer to the *NetScreen ScreenOS Migration Guide*.
- **NetScreen-ISG 2000** – Before the NetScreen-ISG 2000 can support ScreenOS 5.2.0, you must upgrade the OS loader if it is not v1.1.5. You can see the OS loader version scroll by during the bootup process or by entering the get envar command.For information on upgrading the OS loader, refer to the *NetScreen ScreenOS Migration Guide*.

- **NS-5XT Deep Inspection Signature Reduction** – Due to memory limitations, the Deep Inspection signature file has been reduced to "critical" signatures only for the NetScreen-5XT. Customers should consider this potential security trade-off when upgrading to ScreenOS 5.2.0.
- **H.323 Synchronization** – After upgrade to ScreenOS 5.2.0, any existing H.323 sessions may not be synchronized in high availability relationship.

5.1.3 Limitations from Previous Mainline Releases

The following limitations from previous releases are also present in this release.

- **TCP Reassembly for H.323 Traffic** – You must use the **set zone** *zone* **reassembly-for-alg** command to enable TCP reassembly for zones in which you expect to send and receive H.323 traffic. This allows the security device to examine H.323 TPKT packets that are larger than the maximum transmission unit (MTU), which is required for application layer gateway (ALG) filtering.
- **H.323 Gatekeeper Routed Calling** – Juniper Networks has certified Gatekeeper routed calling and Gatekeeper to Gatekeeper support for Avaya products. However, other vendors may function properly, depending upon their adherence to standards.
- **(NetScreen-5000 Series) Transparent Mode** – Moving sessions (both sessions and VPNs) from one interface to another in the same L2 zone is not supported on these platforms.
- **(NetScreen-200 Series) Deep Inspection** – Installing the Deep Inspection (DI) license key on the NetScreen-200 in advanced mode decreases the maximum number of sessions to 64,000 sessions. To restore the number of sessions supported to 128,000 sessions, remove the DI license key and reboot the security device.
- **Antivirus (AV)** – Trend Micro discontinued the VirusWall scanner, which is used with the external AV feature. Although the external AV feature might work in ScreenOS 5.1.0 and above, Juniper Networks does not support it.
- **Large File Transfers** – The maximum size file inspected by the integrated AV feature defaults to 10MB (Range: 4000 through 16000). If AV and Deep Inspection (DI) are enabled, 6 MB is the recommended maximum. If AV, DI, and URL filtering are all enabled, 4MB is the recommended maximum.

- **VoIP** – Juniper Networks tested VoIP with the following IP phone vendors:
  - H.323 IP Phones: Avaya 4612/4606/4624/4602/4620 and Digital 6408D with Avaya S8300/G700 server; Microsoft Netmeeting; OKI VoIP TA (H.323 Fast Start Gateway)
  - SIP IP Phones: Cisco IP Phone 7960 and 7940 (Version 6.3) with Cisco SIP Proxy Server (Version 2.1/2.2); Cisco 2600 SIP Gateway

  Note: Products manufactured by vendors other than the ones mentioned above may interoperate with this version of ScreenOS. However, these products have not undergone official testing by Juniper Networks.
- **SSH Version 1 Interoperability** – The embedded SSH server in ScreenOS 5.1.0 has issues with the client from SSH Communications Security when operating in SSH version 1 mode.

  W/A: Use the SSH Communications client in version 2 mode, or use a different SSH version 1 client, such as OpenSSH.
- **SSHv2 Interoperability** – The only tested and certified SSHv2 clients are OpenSSH and Secure CRT.
- **(NetScreen-5XT and NetScreen-5GT) Primary & Backup Interfaces** – 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.
- **(NetScreen-500 and NetScreen-5000 Series) 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.
- **(NetScreen-5000 Series) Aggressive Aging** – The Aggressive Aging feature is not supported on the NetScreen-5000 Series devices.

5.2 Compatibility Issues in ScreenOS 5.2.0

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 VPN client is incompatible with ScreenOS 5.2.0 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:

    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 security device.
- **Compatible Web Browsers** - The WebUI for ScreenOS 5.2.0 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.

5.2.1 Upgrade Paths from Previous Releases

If you are upgrading a security device from a release that is earlier than ScreenOS 5.0.0, you must upgrade it to ScreenOS 5.0.0 before upgrading to ScreenOS 5.1.0 or 5.2.0. For detailed information on how to upgrade any security device, refer to the *NetScreen ScreenOS Migration Guide*. The migration guide provides step-by-step upgrade procedures and important information about upgrading security devices.

5.3 Known Issues in ScreenOS 5.2.0

The following are known deficiencies in features at the time of this release. Whenever possible, a work-around is suggested following the problem description. 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 5.2.0r3

None.

5.3.2 Known Issues from ScreenOS 5.2.0r2

- **06470** – (NetScreen 500) When upgrading from 5.1 to 5.2r2 using the CLI, the device fails.

  W/A: Upgrade the device with the WebUI.

5.3.3 Known Issues from ScreenOS 5.2.0r1

- **47927** – Changing the root password from WebUI disables SSH for the root admin. WebUI does not offer the option to re-enable SSH.

  W/A: Re-enable SSH from the CLI.

- **46978** – Establishment of a PPPoE connection overwrites manually-configured DNS settings.
- **46828** – When a NetScreen-5000 Series systems are subjected to high (10000) connection-per-second overnight test, there is a possibility of having very minimal (< 10) sessions with zero time out left on the device.
- **45785** – A high CPU utilization has been observed on NetScreen-200 Series devices when they pass 64-byte packets sent at a rate of 10 Mbps.

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.

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

www.juniper.net