Juniper Networks

NetScreen Release Notes

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

Version: ScreenOS 5.1.0r4 Rev. A

Release Status: Public Release

Part Number: 093-1735-000

Date: 8/08/2005

Contents

1. Version Summary

ScreenOS 5.1.0 is the latest release version of ScreenOS firmware for the NetScreen-5XT, NetScreen-5GT, NetScreen-Hardware Security Client, NetScreen-25, NetScreen-50, NetScreen-204 and NetScreen-208 security appliances, and the NetScreen-500 and NetScreen-5200 and NetScreen-5400 security systems.

The ScreenOS 5.1.0r4 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 provides full support for NetScreen-Security Manager, Juniper Networks-NetScreen's security management platform.

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 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 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 were numerous changes in default behavior between ScreenOS 5.1.0r1 and the previous release, ScreenOS 5.0.0. For detailed information on those changes, refer to the *NetScreen ScreenOS Migration Guide*. There are no changes in default behavior between ScreenOS 5.1.0r1 and ScreenOS 5.1.0r4.

4. Addressed Issues

The following sections detail addressed issues in each release of ScreenOS 5.1.0.

4.1 Addressed Issues in ScreenOS 5.1.0r4

- **06404** – The device would reboot due to high volume of VPN multicast traffic.
- **06344** – High BGP activity led to an unresponsive WebUI.
- **06219** – The active user table did not clear after sessions were cleared.
- **06104** – Improved successive eBGP update performance.
- **06095** – (WebUI) An error message was displayed when configuring a subinterface.
- **06003** – Enabling inter-vsys multicast with some configurations led to device failure.
- **05981** – (WebUI) An error occurred when deleting an aggregate interface or subinterface.
- **05946** – In some cases, no IGMP group or route was created because translated multicast traffic failed to forward.
- **05907** – Incorrect translation of default OSPF type-7 LSA into type-5 caused multiple device problems.
- **05867** – The device dropped traffic in an Active/Passive NSRP configuration after processing fragmented IP multicast packets.
- **05859** – Repeated failures of a RADIUS user login authentication caused device failure.
- **05848** – In some cases, it was impossible to set the NSRP HA probe interval to the default.
- **05836** – Some debug formatting errors were fixed.
- **05787** – HA failover in an Active/Passive configuration cased device failure.
- **05761** – The device allowed incorrect source address object removal, causing device failure.
- **05750** – A TCP half open connection would not age out when the service timeout was set to never.
- **05738** – (WebUI) The Local Auth server timeout field incorrectly limited to a three digit value when the value should have been four digits.
- **05728** – In some cases, the IGMP Time caused device failure.
- **05721** – A redundant VPN failed after an NSRP failover revert.

- **05719** – There was an error while processing SNMP BGP information, causing device failure.
- **05683** – In some cases, processing IKE certificates resulted in device failure.
- **05682** – The "in vpn" counter incremented even though there were no VPNs configured.
- **05675** – (WebUI) After deleting a PIM instance, the **Edit PIM Instance** option was still present. Clicking this option after deleting, caused device failure.
- **05642** – Improper handling of ECMP routes caused device failure.
- **05632** – In some configurations, a DNS reverse lookup caused device failure.
- **05630** – With a route-based VPN configured, hundreds of invalid SPI message appeared in the log.
- **05624** – In some cases, it was impossible to manage the backup device in an Active/Passive cluster.
- **05598** – Anti Virus event logs were generated in the wrong format.
- **05515** – **Get service any** CLI command displayed the default timeout value as one minute. Previous versions of ScreenOS 5.0 displayed the default timeout value as 30 minutes. For ScreenOS 5.X, the default timeout value for service any depends on the service being used.
- **05511** – In some cases, changing xauth user added auth type to user.
- **05506** – (NetScreen-Security Manager) When pushing a multi-cell policy in an NSRP pair, the primary device received the correct policy configuration while the secondary device did not.
- **05479** – H.323 call failed when using a policy-based VPN configuration.
- **05478** – Unsupported communication between IKE peers caused device failure.
- **05476** – If one of attack/traffic/event alarms was enabled the NetScreen-Security Manager Agent would push all alarm types to the Management System.
- **05440** – A large ping reply over a VPN tunnel did not work with the VLAN1 interface of the device.
- **05423** – In some cases, firewall user authentication caused device failure.
- **05420** – In some cases, a change in the IDS screen configuration caused traffic to stop.
- **05417** – A DRQ message caused the RAS session to timeout after a call completed; therefore, causing failure of the next call.
- **05404** – The incorrect P1 was deleted after P2 was renegotiated in an IPSec VPN.

- **05385** – (WebUI) Microsoft Internet Explorer (IE) does not display < and > correctly in event logs.
- **05361** – The device would not allow NSRP backup management through a VLAN.
- **05346** – When using Microsoft Internet Explorer to view VPN logs (event), users do not see quotation marks (" ").
- **05345** – (WebUI) Navigating to **Reports > Counters > Hardware**, the hardware counters for the interface were empty. The wrong index was used to identify the interface.
- **05325** – A CLI command that was piped to a TFTP server generated an alarm.
- **05309** – A pass-through ESP fragment traffic failed in Transparent mode.
- **05308** – The NetScreen device would fail while busy.
- **05293** – Heavy MSRPC traffic with an unusual amount of calls per connections caused device failure.
- **05266** –In some cases, pushing a configuration to the device with NetScreen-Security Manager caused device failure.
- **05254** – The device would not display OSPF routes in routing tables.
- **05249** – (WebUI) Default values for the DI service limit were incorrectly displayed.
- **05248** – (WebUI) The DI HTTP Maximum Authorization Length option was missing.
- **05246** – Site-to-site VPN failed in Transparent mode after the device was rebooted.
- **05239** – HTTP sessions would hang due to internal comparison failures.
- **05208** – A BGP configuration was lost during setup on a passive NSRP device.
- **05188** – A NSRP passive device failed with a race condition in cold start sync.
- **05177** – Heavy MSRPC traffic with an unusual number of calls per connection caused device failure.
- **05169** – The DNS servers were over written with PPPoE data.
- **05167** – SNMP displayed incorrect uptime.
- **05156** – When entering the **get db s** CLI command, some SIP debugs appeared even when debug was not enabled.
- **05136** – A device would copy BGP route information from an inactive Virtual Security Interface.

- **05135** – A jumbo frame received on an interface caused device failure.
- **05123** – An ESP child session would copy bad Security Association information after a failover or rekey.
- **05079** – A vsys could not be updated on a NSRP cluster.
- **05069** – A VPN appeared by error on a NSRP peer.
- **05065** – The interface pointer was improperly set when editing an interface. This caused firewall failure when save changes was chosen at the prompt.
- **05037** – H.323 fast start call failed when progress message was used due to a decoding error.
- **05035** – A corrupted task queue caused device failure.
- **05034** – A device randomly restarted with no dynamic IP pool configured and the Application Layer Gateway incorrectly processing certain traffic.
- **05023** – The device could not revert traffic from a backup interface to a primary interface when set for dynamic routing.
- **04992** – The backup device failed in NSRP mode.
- **04986** – RTSP traffic would not pass through a device in Transparent mode.
- **04981** – The boot messages "Configuration Lost" or "Failed Command" would appear in NSRP-Lite configurations with MIP defined on a local interface.
- **04975** – In some configurations, a policy without address objects caused device failure.
- **04963** – In some cases, HDLC packets were dropped.
- **04961** – Unusual H.323 traffic setup caused device failure.
- **04956** – Unusual situations with an ARP or route changed device failure.
- **04952** – Some ARP packets could be lost after the NSRP primary device was cold started.
- **04945** – Unsupported L2TP/IPSec NAT traversal configuration caused device failure.
- **04938** – VSYS VPN traffic stopped in some cases.
- **04937** – Duplicate echo responses for ping were not handled properly.
- **04936** – In unusual situations in Active/Active cluster, the device failed.
- **04935** – There was an unusual amount of packet retransmissions after the OS was upgraded.
- **04934** – Unusual syslog activity caused device failure.
- **04900** – In some cases you could not add a user to a group.

- **04892** – The device did not allow some traffic through after multicast and VPN traffic use.
- **04884** – After upgrade, device would not allow authentication to outlook.
- **04882** – The device did not allow two PPPoE instances using separate virtual routers.
- **04880** – Some unusual situations with H.323 traffic caused device failure.
- **04876** – Some unusual situations with RTSP traffic caused device failure.
- **04872** – Internal access problem caused device failure.
- **04869** – The device made incorrect assumptions about routes in IP spoofing.
- **04851** – The device failure in some test situations during NSRP sync.
- **04844** – When passing VPN traffic in Active/Active mode, the device dropped all fragmented packets.
- **04842** – The device used incorrect IKE cookies after rebooting.
- **04836** – (NetScreen-5XT) A VPN tunnel dropped windows domain login traffic.
- **04831** – Strict type-checking for expected DHCP fields and values was removed to forward DHCP boot requests with unrecognized values.
- **04819** – IGMP proxy to multiple host interfaces for the same group was disallowed.
- **04813** – Advanced license key was lost in unusual NSRP situation.
- **04810** – A secondary device could not establish OSPF adjacencies after OS was upgraded.
- **04806** – A GRE tunnel failed to send the appropriate encapsulated response.
- **04801** – The device failed in an unusual race condition with the command task.
- **04768** – A core dump could occur when interface ethernet4 received a jumbo frame while interface ethernet1 was receiving normal packets.
- **04764** – The user was unable to bind an interface to an OSPF area with the WebUI.
- **04735** – The HTTP Maximum Authorization Length option was missing from the WebUI.
- **04716** – (NetScreen-5GT) The extended license incorrectly limited the number of BGP peers to 16.
- **04707** – In some cases, slow performance was seen on a route-based VPN tunnel encrypted with IPSec.
- **04688** – With NSM in use, some connections caused memory to not be released.

- **04672** – After moving policies, the device could not search them properly.
- **04647** – The NetScreen-Security Manager Agent always displayed BGP keep-alive as the default value.
- **04646** – An HA backup device in Transparent mode learned the MAC address at an incorrect interface in some situations.
- **04629** – A driver error caused some SQL traffic to be inadvertently dropped by the device.
- **04603** – A malformed packet containing a large value in the verifier length field caused device failure.
- **04588** – The device could set BGP to Active state in some cases with a failed TCP connection.
- **04585** – AV monitoring skipped incorrectly formatted email messages.
- **04432** – The CPU spiked in due to packet loop issues.
- **04336** – The device dropped or routed packets to the wrong destination in some policy-based NAT configurations.
- **04288** – The device failed in some circumstances while processing HTTP traffic.
- **04182** – With loopback in hub and spoke configuration, some VPN traffic was sent to the wrong gateway
- **04178** – The device did not match loopback L2TP sessions through an IPSec tunnel.
- **04137** – The MIP on a shared loopback in VSYS was not visible.
- **04115** – Sequence of service objects listed in the configuration was inconsistent.
- **03825** – Service timeout was not configurable in a vsys.
- **03771** – CLI displayed the up time correctly while SNMP reply did not.
- **03714** – When loopback sessions occurred, the auth table entry session count was incremented but never decremented. When the session was cleared from the session table, the corresponding auth entries were not deleted.
- **03492** – When accessing HotMail through Outlook Express with Websense enabled, access into the mailbox was granted, but messages could not be deleted.

4.2 Addressed Issues from ScreenOS 5.1.0r3

- **45341** – The SIP ALG parser used to report an error when there was no CRLF in the last line of the message.
- **45042** – If you upgraded to ScreenOS 5.1.0r1, then downloaded a large file from the Internet, the client received the following message: Connection with server has been reset.
- **43793** – The default service timeout value for H.323 was reduced to 30 minutes. You can configure the timeout by specifying the **set service h.323 timeout** <*minutes*> command.
- **03756** (NetScreen-5GT) – The scan engine treated a zero-byte file within a ZIP file as a file in ZIP format instead of a file of any other format.

4.3 Addressed Issues from ScreenOS 5.1.0r2

- **44099** (NetScreen 5000 series) – When there were high volumes of calls on the NetScreen device, some media sessions failed when the call setup rate was equal to or greater than 50 calls-per-second (CPS).
- **43847** – When upgrading from ScreenOS 5.0 to 5.1, if the bandwidth was set to zero, traffic shaping options were missing.
- **43776** – When you upgraded from ScreenOS 5.0 to ScreenOS 5.1, previously configured VIPs disappeared.
- **43344** – In ScreenOS 5.1.0r1, the interface-based IP tracking options were hidden commands on the NetScreen-5XT and NetScreen-5GT. These commands are not hidden in this release.
- **43260** (NetScreen-5GT) – When the NetScreen device was in Extended port mode, the WebUI erroneously displayed the port mode as Trust/Untrust and did not allow you to change it.
- **43097** – When the NetScreen device was in transparent mode, it created duplicate multicast sessions.
- **43008** – Before you put a NetScreen device into a cluster, you could not add/modify/remove NSRP track-IP objects on the Track IP page of the WebUI.
- **42992** – The NetScreen device crashed when the new RTSP session rate went over 100 RTSP sessions and there was additional traffic going through the device.
- **42801** – When you used the redirect URL filtering feature with a SurfControl server, sending a URL that was longer than 512 bytes sometimes caused unexpected results on the SurfControl server.

5. Known Issues

This section describes known issues with the current release.

- Section 5.1 "Limitations of Features in ScreenOS 5.1.0r4" 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 5.1.0r4 on page 12 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 5.3 "Known Issues in ScreenOS 5.1.0 on page 13 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.

5.1 Limitations of Features in ScreenOS 5.1.0r4

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

5.1.1 Limitations in ScreenOS 5.1.0

The following limitations are present in ScreenOS 5.1.0r4.

- **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 NetScreen 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** – In ScreenOS 5.1, 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-500) Saving Firmware to Flash** – You cannot save ScreenOS 5.1.0 firmware to flash memory using the boot loader. Use the WebUI or CLI to save ScreenOS 5.1.0 firmware to flash memory.
- **(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-5000 Series)** – The MGT-2 board does not support ScreenOS 5.1.0. You must use the MGT board.

- **(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 NetScreen 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, Juniper Networks does not support it, except for security-related issues.

- **Large File Transfers** – The maximum size file inspected by the integrated AV feature defaults to 10MB. If AV and Deep Inspection (DI) are enabled, this is reduced to 6 MB. If AV, DI, and URL filtering are all enabled, this is reduced to 4MB.

- **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

5.1.2 Limitations from Previous Releases

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

- **Aggressive Mode is Insecure** – Due to protocol limitations, Main Mode IKE in combination with PSK is not supported for dialup VPN users. In addition, it is never advisable to use Aggressive Mode because this mode has inherent insecurity problems.

  W/A: It is strongly advisable to configure dialup VPN users with PKI certificates and Main Mode.

- **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 5.1.0r4

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 5.1.0r4 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 NetScreen device.

- **Compatible Web Browsers** - The WebUI for ScreenOS 5.1.0r4 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 NetScreen 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. For detailed information on how to upgrade any NetScreen device, refer to the *NetScreen ScreenOS Migration Guide*. The migration guide provides step-by-step upgrade procedures and important information about upgrading NetScreen devices.

5.3 Known Issues in ScreenOS 5.1.0

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 5.1.0r4

- **51686** – (NetScreen-500) There is no firmware upgrade available.
- **48525** – In ScreenOS 5.0 you had the option to create an SMTP service. In ScreenOS 5.1 the SMTP service is predefined.
- **43777** – There is not option in the WebUI to set vsys NSRP threshold monitoring.

    W/A: Use the CLI.

5.3.2 Known Issues from ScreenOS 5.1.0r3

- **44873** (NetScreen-5XT) – Using the **set dbuf size** command to increase the debug buffer size results in a memory allocation failure. Even if this command is successful, a failure occurs when you download the Deep Inspection attack database.

    W/A: Do not use the **set dbuf size** command to increase the debug buffer size. If you did, use the **unset dbuf size** command to restore the default buffer size.

- **44586** – In NetScreen devices that support virtual systems, if the secondary banner is set at the root level, updating a vsys through NetScreen-Security Manager fails. NetScreen-Security Manager displays an error message indicating that the secondary banner is set at the vsys level, even if this option is not available.

    W/A: Unset the secondary banner at the root level.

5.3.3 Known Issues from ScreenOS 5.1.0r2

There are no known issues from this release.

5.3.4 Known Issues from ScreenOS 5.1.0r1

- **43113** – When the NetScreen device is in transparent mode, internal servers cannot initiate sessions to dialup VPN clients.
- **43054** – When you use the integrated URL filtering feature, the port number range (1024 -32767) allowed by the WebUI is incorrect. The CLI allows 1024 to 65535, which is correct.

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