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 5.2.0r2

Release Status: Rev A

Part Number: 093-1697-000

Date: 7-11-05

# Contents

# 1. Version Summary

ScreenOS 5.2.0r2 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 5.2.0r2 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

There were changes in default behavior between ScreenOS 5.2.0r2 and the 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 5.2.0r2

- **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.

## 4.2 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 6 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 5.2.0 on page 7 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 5.2.0

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

### 5.1.1 Limitations in ScreenOS 5.2.0r2

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.

### 5.1.2 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 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** – 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 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 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 NetScreen 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 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 or 5.2.0. 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 5.2.0

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 5.2.0r2

- **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.

### 5.3.2 Known Issues from ScreenOS 5.2.0r1

- **49320** – When you upgrade a NS-5XT device from ScreenOS 5.0.0 or ScreenOS 5.1.0 to ScreenOS 5.2, you must download the latest attack db for the NS-5XT.
- **49293** – If multicast-group translation is enabled, then any interface enabled for IGMP version 3 cannot process IGMP version 2 reports.
- **49199** – The "account" feature for vsys Websense URL filtering does not work in the WebUI, and must be configured through the CLI.
  - The item "account" is missing from vsys websense URL Filtering configuration page:

    Screening > URL Filtering > Websense/Surfcontrol

    It is impossible to edit Websense URL filtering from here.
  - Empty account names are not allowed.

  Both of these issues are caused by attempts to add an account using the WebUI.

  W/A: Enter the vsys to do any vsys-based URL filtering configuration. Do all such configuration through the CLI instead of the WebUI. The CLI command is **set url**.

- **48134** – NetMeeting across VPN requires execution of **unset alg h245** when it is necessary to upgrade to 5.2 policy-based VPN between two NetScreen appliances. All traffic is then permitted across the VPNs.

  However, when the end hosts run MicroSoft NetMeeting between them, NetMeeting connects but the options are grayed out.

  W/A: If you execute **unset alg h245** on the NetScreen devices, it works.

- **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 NS-5000 is 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.
- **45988** – RTSP service with Realplayer version 10.5 is not supported in this release. Other versions of Realplayer may work with this release, although they have not undergone official testing.
- **45785** – A high CPU utilization has been observed on NS-200 platforms when they are 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