Juniper Networks

NetScreen Release Notes

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

Version: ScreenOS 5.1.0r1

Release Status: Public Release

Part Number: 093-1293-000

Date: 10-27-04

Contents

1. Version Summary

ScreenOS 5.1.0 is the latest release version of ScreenOS firmware for the NetScreen-5XT, NetScreen-5GT, 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 5.1.0r1 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 or ScreenOS 5.1.0r1, 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 are numerous changes in default behavior. For detailed information on changes to default behavior in ScreenOS 5.1.0r1, refer to the *NetScreen ScreenOS Migration Guide*.

4. Addressed Issues

As this is the initial release of ScreenOS 5.1.0, there are no addressed issues at this time.

5. Known Issues

This section describes known issues with the current release.

- Section 5.1 “Limitations of Features in ScreenOS 5.1.0r1” 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 5.1.0r1 on page 5 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 5.1.0r1 on page 6 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 5.1.0r1

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 5.1.0r1.

- **SIP** – When using SIP and you configure two phones in the Trust zone, you must configure the Gatekeeper in the Trust zone too. If you configure the Gatekeeper in the Untrust zone, the two phones will not be able to communicate with each other.
- **(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-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)** - ScreenOS 5.1.0 does not support the external AV feature.
- **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; Digital 6408D
  - Analog Phones: Polycom: Phones were connected to an OKI H.323 gateway to convert the analog signal into H.323.
  - SIP IP Phones: Cisco IP Phone 7960 and 7940, image version 6.3

5.1.2 Limitations from Previous Releases

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

- **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 5.1.0r1

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 5.1.0r1 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 5.1.0r1 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 5.1.0r1

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.

- **44099** (NetScreen 5000 series) – When running high volumes of calls on the NetScreen device, some media sessions fail when the call setup rate is equal to or greater than 50 cps.
- **43260** (NetScreen-5GT) – When the NetScreen device is in Extended port mode, the WebUI erroneously displays the port mode as Trust/Untrust and does not allow you to change it.

  W/A: Use the **get system** CLI command to display the correct port mode and to change the port mode.

- **43113** – When the NetScreen device is in transparent mode, internal servers cannot initiate sessions to dialup VPN clients.
- **43100** – When running SIP in a High Availability (HA) configuration, the backup NetScreen device may crash on continuos heavy load testing.

  W/A: Reset the backup device.

- **43097** – When the NetScreen device is in transparent mode, it creates duplicate multicast sessions.
- **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.
- **43008** – Before you put a NetScreen device into a cluster, you cannot add/ modify/remove NSRP track-IP objects on the Track IP page of the WebUI.
- **42992** – The NetScreen device could crash when the new RTSP session rate goes over 100 RTSP sessions and there is additional traffic going through the device.
- **42801** – When you use the redirect URL filtering feature with a SurfControl server, sending a URL that is longer than 512 bytes may cause the SurfControl server to go down.

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 94089-1206
U.S.A.
ATTN: General Counsel

www.juniper.net