

Juniper Networks

Release Notes

Product: Juniper Networks SSG 520 and Juniper Networks SSG 550

Version: ScreenOS ssg500.5.1.0r4.6

Release Status: Public

Part Number: 530-014408-01 Rev B

Date: 05-01-06

Contents

1. [Version Summary on page 1](#)
2. [New Features and Enhancements on page 1](#)
 - 2.1 [Secure Services Gateway \(SSG\) 500 Series Devices on page 2](#)
 - 2.2 [New Features for ScreenOS ssg500.5.1.0r4.6 on page 2](#)
3. [Changes to Default Behavior on page 3](#)
4. [Known Issues on page 3](#)
 - 4.1 [Limitations of Features in ScreenOS ssg500.5.1.0r4.6 on page 3](#)
 - 4.2 [Known Issues in ScreenOS ssg500.5.1.0r4.6 on page 4](#)
5. [Getting Help on page 10](#)

1. Version Summary

ScreenOS ssg500.5.1.0r4.6 is the public version of ScreenOS firmware for the Juniper Networks Secure Services Gateway (SSG) 500 Series devices. This version is based on ScreenOS 5.1.0r4 and has all known and addressed issues in common with that release. (See the Juniper Networks Release Notes for ScreenOS 5.1.0r4 for more information.)

Note: *NetScreen-Security Manager 2005.3 supports this release. If you want to manage your SSG 500 Series device with NetScreen-Security Manager 2005.3, install a schema upgrade on the management server and User Interface. The upgrade is available at the same location as the ScreenOS code. Please refer to the schema upgrade installation document for instructions.*

2. New Features and Enhancements

The following sections detail new features and enhancements in ScreenOS 5.1.0r4.6 release. For a complete list and descriptions of new features and enhancements in ScreenOS 5.1.0, refer to the *Juniper Networks NetScreenOS Migration Guide*.

2.1 Secure Services Gateway (SSG) 500 Series Devices

The Juniper Networks Secure Services Gateway (SSG) is an integrated router and firewall platform designed for enterprise edge environments. The SSG 500 Series devices, SSG 520 and SSG 550, support Juniper Networks J-Series Services Router T1, E1, T3, and serial physical interface modules (PIMs) and provide protocol conversions between local area and wide area networks.

See the *Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide* for more detailed descriptions of the SSG 500 Series devices installation and configuration procedures.

The URL-filtering and DI features can be enabled on the device. See the *Juniper Networks Concepts & Examples Reference Guide* for ScreenOS 5.1.0 for more information on how to retrieve and install license keys.

Note: You must register your product at www.juniper.net/support so that certain ScreenOS features can be activated on the device. If you already have an account, enter your user ID and password; if you are a new Juniper 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 **exec license-key update** CLI command to make the device connect to the Juniper server to activate the feature.

2.2 New Features for ScreenOS ssg500.5.1.0r4.6

2.2.1 Support for SSG 500 Series Devices

This release supports installing and running ScreenOS on the SSG 500 Series devices. You configure these devices for your network using the ScreenOS CLI, WebUI, or NetScreen-Security Manager.

2.2.2 WAN Interfaces and Protocols

This release supports configuring and using the T1, E1, T3, and serial WAN Physical Interface Modules (PIMs) on the SSG 500 Series devices, as well as configuring the following WAN encapsulation protocols: Frame Relay, Multilink Frame Relay, Point-to-Point Protocol (PPP), Multilink PPP, and Cisco-compatible HDLC.

Note: In WAN configurations, an SSG Series devices only operates as a data terminal equipment (DTE) device. You cannot use a device as a data circuit terminating equipment (DCE) device.

See the *ScreenOS WAN Interfaces and Protocols Reference Guide* for more information about configuring and using these interfaces.

2.2.3 WAN Zone Binding

This release allows the WAN interfaces to be unnumbered and be bound to other interfaces and zones so that the WAN interfaces no longer require a separate IP address.

3. Changes to Default Behavior

The following is a list of changes to the default behavior:

- Four built-in 10/100/1000 Gigabit Ethernet ports on the SSG 500 Series devices provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic.
- When configuring the built-in Ethernet ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are: `ethernet0/0`, `ethernet0/1`, `ethernet0/2`, and `ethernet0/3`.
- The built-in Ethernet ports are bound by default to the following zones:
 - `ethernet0/0` is bound to the Trust zone (default IP address is 192.168.1.1/24)
 - `ethernet 0/1` is bound to the DMZ zone
 - `ethernet0/2` is bound to the Untrust zone
 - `ethernet0/3` is bound to the HA zone
- Ports on WAN PIMs installed in the SSG 500 Series devices are bound to the Untrust zone by default.

4. Known Issues

This section describes known issues with the current release.

- [Section 4.1 “Limitations of Features in ScreenOS ssg500.5.1.0r4.6”](#) identifies features that are not fully functional at the present time and will be unsupported for this release.
- [Section 4.2 “Known Issues in ScreenOS ssg500.5.1.0r4.6 on page 4](#) describes deviations from intended product behavior as identified by Juniper Networks 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 ssg500.5.1.0r4.6

This section describes the limitations in various features in ScreenOS ssg500.5.1.0r4.6.

- To run the ScreenOS Deep Inspection (DI) feature, you must have 1 gigabyte (GB) of memory (two 512 MB SIMM DRAM memory modules) installed in the SSG 500 series device. See the *Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide* for instructions on how to upgrade memory from 256 MB to 1 GB.
- Setting the framing option for E1 interfaces is not supported.

4.2 Known Issues in ScreenOS ssg500.5.1.0r4.6

The following are known deficiencies in features at the time of this release. Whenever possible, a workaround 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.

- In some cases, the WebUI online help points to the wrong location.

W/A: In the WebUI, go to Configuration > Admin > Management, click on the **Default** button at the Help Link Path field, then click **Apply**. The URL, http://help.juniper.net/help/english/5.1.0/ssg500/home_cnt.htm should be displayed in the link path.
- 53880 – When NSRP is enabled, there is a UDP throughput drop of up to 5% for both firewall and VPN.
- 51123 – The WebUI does not allow the building of the SNMP community with a subnet mask other than /32.
- 49105 – Under heavy fragmented traffic, some fragments are dropped.
- 48299 – In an NSRP active-active configuration, a duplicate IP address may be detected for the manage-ip interface at start up.
- 47290 – E1 framing only supports g704 format.
- 47223 – In an Active/Active NSRP environment, changes in the Phase 1 gateway name is not synchronized over.
- 46500 – When adding a multi-cell policy, the event log may display multiple identical entries.
- 45041 – In cases when two DNS servers are used, and the primary DNS is no longer available, the secondary DNS server does not search fast enough to properly populate the host table.
- 45034 – In some cases in an Active/Active NSRP configuration, NetScreen-Remote does not connect with two connections simultaneously.
- 43882 – In some cases when the device reboots with a large number of VPNs, the device displays periods of high CPU usage. It may take a while before all of the VPNs are reestablished.
- 43220 – If a manage IP is set for a tunnel interface, it is not put into the configuration file; therefore, this setting is lost on a reboot or power off.
- 07840 – The device may fail while handling ISAKMP packets with invalid and/or abnormal contents. This addresses NISCC # 273756.
- 07795 – When UDP flooding control is turned on, the set CLI command for IDS screen feature causes traffic to stop.
- 07627, 04215 – In a route based VPN multi-VR environment, the security device incorrectly performs a route lookup in the wrong VR.
- 07098 – Message guide error “Error(00034) Message: SSH: Maximum number of SSH sessions (< number >) exceeded” is incorrectly documented. The error “SSH: Max number () of session reached.” is posted to the system log.
- 07072 – Setting or unsetting the secondary IP address for a redundant interface could lead to “General system errors”.
- 07045 – A TCP sequence check fails on the second packet of a three-way handshake.
- 07030 – Some L2TP connections using passwords could lead to device failure.

- 07010 – After a network re-route, DHCP relay performance could suffer.
- 07003 – In some configurations, sessions could be dropped if there is no policy in the direction of the session.
- 06840 – Modifying the name of a VPN object is not synced to the NSRP backup device.
- 06808 – A VIP with the name **untrust** cannot use port 161 SNMP.
- 06770 – In some scenarios, the session that is synced to backup device can select a different route. As a result, when the device becomes the primary device, traffic matching these sessions fails.
- 06738 – When a local interface route is deleted, the secondary device is unintentionally deleted.
- 06714 – When performing a Device Update from NetScreen-Security Manager, the device being updated fails if there is a vsys configured.
- 06710 – The error message, **No more counters**, is changed to **Maximum number of X counters exceed** to indicate that no more counters are available.
- 06677 – The user cannot select an interface in **Reports > Counters > Hardware** when using the WebUI with Java.
- 06669 – After a ping to the management interface on a different zone, the active user is still seen even if the session is deleted.
- 06621 – In some situations, the device fails.
- 06579 – The group user VPN is disconnected after 60 minutes of idle time.
- 06552 – Routes that are defined on local interfaces are incorrectly deleted while configuring synchronization from an NSRP peer.
- 06525 – The **get zone zone screen attack** CLI command output is formatted incorrectly.
- 06520 – The VPN proxy ID information is unavailable after a device is restarted or synchronized.
- 06517, 05839 – When Xauth is configured with an external RADIUS server and local IP Pool, the allocated IP address on the gateway side is not released properly.
- 06452 – When password authentication is disabled for specific device administrators, the administrator is still able to authenticate with the password when the OpenSSH client is used.
- 06450 – An IPSec passthrough device halts VPN traffic due to DIP address change.
- 06414 – Gratuitous ARPs are not sent for inactive VSI redundant interface manage-ip.
- 06369 – When an HTTP header has Content-Length and Transfer-Encoding header fields, the user cannot retrieve the HTTP content.
- 06334 – The device displays high flow CPU numbers even when there is little traffic.
- 06312, 06295 – The device fails when a policy change is saved.
- 06301 – The device fails in some cases related to PKI configuration.
- 06294 – In some situations, the device sends DNS packets with incorrect source and/or destination addresses.
- 06256 – Flood of non SYN packets leads to high CPU usage and device failure even with SYN check enabled.
- 06253 – The device occasionally resets after an invalid short frame is received.

- 06245 – The total number of redistributed routes exceeds the system limit messages received due to an incorrect redistribute route counter.
- 06219 – The active user table does not clear consistently after all sessions are cleared.
- 06205 – Ucast packet counters are incorrectly calculated.
- 06181 – A race condition in the VPN crypto engine intermittently causes the device to reset.
- 06170 – With VLAN tagging configured on the interface, RTP requests could fail after SIP calls are established.
- 06156 – OSPF issues lead to an inconsistent device failure.
- 06127 – Configurations that have a high number of session timeouts can cause the device to reset.
- 06107 – A VPN failover may fail when using an Asymmetric VPN tunnel with ECMP on high-end devices.
- 06079 – In some cases, the error “Auth user cannot belong to more than 4 user groups...” is received when attempting to add an auth user, already in use in a policy, to a User Group.
- 06074 – An interface duplex mode change does not reset and synchronize the physical port settings.
- 06056 – In some circumstances an NSRP single primary device, without the backup device, fails.
- 06036 – SNMP MIB walk hangs on NTP MIBs.
- 06031 – PPPoE does not insert default routes into the routing table.
- 06030 – In some cases, deleting a vsys and VPN leads to device failure.
- 05971 – Users are denied Internet access when a certain number of browsing requests are exceeded even if URL fail mode is set to permit.
- 05961 – In some situations, passive FTP traffic hangs.
- 05951 – NSRP backup machine does not synchronize the clock automatically with the NTP server.
- 05947 – Downloading large files leads to system failure.
- 05945 – RTSP traffic does not work with some DIP/MIP configurations.
- 05900 – With a large number of tasks, the NSM Agent fails to import devices.
- 05889 – In some cases, the device displays unnecessarily high CPU usage.
- 05884 – The device fails when SIP uses route based tunnel information.
- 05882 – After a manual failover to a secondary NetScreen-Security Manager server, some of the devices fail to reconnect.
- 05874 – Passive FTP transfers to a server behind a MIP IP intermittently fail.
- 05863 – An NSRP standby device reboots unnecessarily.
- 05859 – The device fails with the Exception (task queue broken) error message.
- 05857 – Unable to import device into NetScreen-Security Manager; receive error “Unable to get device DM needed for Import!”.
- 05850 – Objects are not returned in OID order for SNMP get and get_next requests.
- 05833 – In some situations, heavy call volume causes device failure.
- 05826 – The device fails when VOIP ALGs are turned on.

- 05771 – SNMP sysUpTime value returns incorrect values when NetScreen-Security Manager is also monitoring the device.
- 05762 – The NetScreen-Security Manager template message "Enable Syslog Messages" does not reflect on the device. Issue will be resolved in an NetScreen-Security Manager release.
- 05752 – Traffic could erroneously fail with NAT-T enabled on Route-based VPN tunnels.
- 05750 – A TCP half connection does not time out when the service timeout is set.
- 05746 – The device responds very slowly with NetScreen-Security Manager after some upgrades.
- 05721 – When using Redundant VPN Gateways, after the NSRP failover reverts back to the master device, the VPN tunnels may fail.
- 05719 – In some cases, upgrading Active-Passive NSRP devices leads to system failure.
- 05712 – The device fails when using a pattern match on console or Telnet sessions.
- 05697 – In some cases, multiple simultaneous connections with continuous connection/disconnection to the device, while issuing get commands, lead to device failure.
- 05673 – Some types of BGP activity cause device failure.
- 05624 – The user is unable to manage the backup device in an Active-Passive cluster.
- 05623 – When the VPN object name is modified on an active node, the object generates a new VPN on the backup device.
- 05616 – The FTP-PUT and FTP-GET deny policy changes to permit policy after importing through the NSM Agent.
- 05615 – Overuse of administration leads to manageability issues.
- 05582 – Rebooting with no SRC/DST address or service in a policy could lead to the removal of some configuration items.
- 05485 – With BGP configured, issuing the **get tech** CLI command could lead to device failure.
- 05476 – If either attack, traffic or event alarms are enabled, then NSM Agent pushes all types of alarms to the NetScreen-Security Manager.
- 05471 – The discard counter does not increment properly.
- 05420 – In some cases, packet forwarding flow stops after disabling IP Spoofing or enabling the unknown protocol detection screen option on the Trust zone.
- 05401 – A device with NSM Agent configured could led to high CPU and device failure.
- 05385 – (WebUI) Microsoft Internet Explorer (IE) does not display < and > correctly in the event logs.
- 05380 – Emails with large attachments fail to pass through the device when AV Scan Manager is enabled. The user may receive the error message "Content is not scanned for virus due to error or constraint (code 65460), and is dropped".
- 05338 – In some cases, traffic does not get forwarded through back-to-back tunnels.
- 05309, 05158 – Pass-through of fragmented ESP traffic fails when the device is configured in Transparent mode.
- 05308, 03789, 04844 – Under some conditions, VOIP traffic leads to device failure.

- 05298 – Automatic NTP updates do not work for NSRP backup device; the error message “Cannot send NTP request. (No active VSDs in this device)” is received.
- 05284 – After a reboot, the tunnel of a policy-based VPN, with SRC NAT and DIP configured, does not activate due to an incorrect Proxy-ID getting set.
- 05269 – Interface MTU is erroneously synced in an NSRP-Lite cluster.
- 05266 – The device could fail when referring to an incorrect task priority.
- 05254 – The device does not display OSPF routes in routing tables.
- 05246 – In a manual key, site-to-site VPN, routes are installed improperly when they are configured for Transparent mode.
- 05200, 04941 – When configured as route based VPN hub and spoke, packets from the device contain incorrect ESP sequence numbers.
- 05194 – A NSRP backup fails when clear ARP is issued on the master device.
- 05162 – In some situations, enabling SIP debugging could lead to device failure.
- 05158 – During heavy WebAuth traffic using an external RADIUS server for WebAuth authentication, the device occasionally fails.
- 05123 – After a P2 rekey and NSRP failover, the ESP session contains incorrect route and tunnel information.
- 05079 – Import of a device configuration by NetScreen-Security Manager fails with **java.io.IOException: Parse** error.
- 05029 – BGP route metrics are incorrectly modified when receiving a more specific route filtered by route-map. The weight and preference of the less specific route, if any, changes to zero.
- 05024, 04785 – Users received "Error! The URL is too long" message when browsing a URL longer than 512 bytes while using redirect URL filtering with fail-mode set to block.
- 04981 – Policies with MIP defined on local interface should not be synchronized to the peer device. Customer experiences configuration lost or "failed command" warning during boot-up when the issue occurs.
- 04941 – An ICMP packet size of 50 - 400 bytes through an IPSec tunnel with NAT-Traversal is dropped.
- 04937 – Ping is enhanced to handle duplicated ICMP echo responses.
- 04899 – When using a device as DHCP relay, the relayed DHCP discovery packets (unicast packets) are erroneously intercepted.
- 04847 – Under certain conditions, the device resets after unsetting a vsys.
- 04844 – Under heavy encrypted traffic conditions fragmented packets could get dropped.
- 04801 – The device could fail when a VPN tunnel is removed in an NSRP environment.
- 04649 – When using RADIUS Auth and local IP Pool, VPN users could receive the error message “No more IP address in pool”.
- 04553 – Occasionally, packets are not routed correctly even though they match the session.
- 04522 – Incoming mail does not pass through a MIP when AV is enabled.

- 04513 – When configured for local authentication, the session reference counter is not correctly decremented when the session times out.
- 04353 – If the incoming interface is a sub-interface, SIP packets cannot be sent; as the VLAN info in the tag is not initialized.
- 04336 – Packets are dropped or are improperly routed when passing through a vsys configured with dst-NAT in a multi-VR environment.
- 04182 – Modifying the remote tunnel end point on a NetScreen-Remote client to point to another interface on the device causes it to use the wrong gateway.
- 04018 – After a VIP IP is defined and a VIP service is added, on occasion the VIP summary page is blank.
- 03871 – In some cases the backup device resets after issuing the **exec nsrp sync global-config save** CLI command.
- 03447 – CLI and WebUI have conflicting time zone data, leading to a one hour discrepancy.

5. 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.

Copyright 2006, Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

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

www.juniper.net