

Juniper Networks  
NetScreen Release Notes

Product: NetScreen-5GT Wireless and NetScreen-5GT Wireless ADSL

Version: ScreenOS 5.0.0r10-DSLW

Part Number: 093-1679-000, Rev. A

Date: 6/30/05

## Contents

1. [Version Summary on page 2](#)
2. [Description of the NetScreen-5GT Wireless Devices on page 2](#)
3. [Addressed Issues in ScreenOS 5.0.0 on page 3](#)
  - 3.1 [Addressed Issues in ScreenOS 5.0.0r10 on page 3](#)
  - 3.2 [Addressed Issues from ScreenOS 5.0.0r6 on page 18](#)
4. [Known Issues on page 20](#)
  - 4.1 [Limitations of Features in ScreenOS 5.0.0r10-DSLW on page 20](#)
  - 4.2 [Compatibility Issues in ScreenOS 5.0.0r10-DSLW on page 21](#)
  - 4.3 [Known Issues in ScreenOS 5.0.0r10-DSLW on page 21](#)
5. [Getting Help on page 23](#)

## 1. Version Summary

ScreenOS 5.0.0r10-DSLW is the second version of ScreenOS firmware for the Juniper Networks NetScreen-5GT Wireless and NetScreen-5GT Wireless ADSL devices. This version is based on ScreenOS 5.0.0r10 and has all known and addressed issues in common with that release. (See the *Juniper Networks NetScreen Release Notes* for ScreenOS 5.0.0r10 for more information.)

## 2. Description of the NetScreen-5GT Wireless Devices

The Juniper Networks NetScreen-5GT Wireless devices provide IPSec Virtual Private Network (VPN) and firewall services for a branch office or a retail outlet that uses an integrated wireless 802.11b/g interface. The NetScreen-5GT Wireless devices use the same firewall, VPN, antivirus, deep inspection, and traffic management technology as NetScreen's high-end central site products.

**Note:** *The ScreenOS firmware version is now referred to as DSL Wireless (DSLW).*

Juniper Networks offers six models of the NetScreen-5GT device:

- **NetScreen-5GT**
- **NetScreen-5GT ADSL A:** Annex A model supports ADSL over standard telephone lines (POTS).
- **NetScreen-5GT ADSL B:** Annex B model supports ADSL over Integrated Services Digital Network (ISDN).
- **NetScreen-5GT Wireless:** The Wireless only model.
- **NetScreen-5GT Wireless ADSL A:** The Wireless with Annex A model supports ADSL over standard telephone lines (POTS).
- **NetScreen-5GT Wireless ADSL B:** The Wireless with Annex B model supports ADSL over Integrated Services Digital Network (ISDN).

The three wireless models support up to four wireless security zones. All ADSL models support ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt), and ITU 992.2 (G.lite) standards.

All NetScreen-5GT models support three software versions:

- The 10-user version supports up to 10 users.
- The Plus version supports an unrestricted number of users.
- The Extended version provides the same capabilities as the Plus version, with additional features: High Availability (NSRP Lite), the DMZ security zone, and additional sessions and tunnel capacity.

## 3. Addressed Issues in ScreenOS 5.0.0

The following sections detail addressed issues in each release of 5.0.0.

### 3.1 Addressed Issues in ScreenOS 5.0.0r10

**Note:** *The NetScreen-5GT DSLW firmware is not supported with NetScreen-Security Manager 2004 Feature Pack 3rX and below.*

- **47384** – There was packet loss with heavy traffic.
- **47380** – (NetScreen-Security Manager) Upgrading a device over a slow network connection caused the update to time out if the image download took more than five minutes.
- **45418** – (NetScreen-Security Manager) Connection failure occurred when updating a device because the NetScreen-Security Manager keys were not saved before rebooting the device.
- **45153** – Event logs erroneously showed "XAuth login expired and was terminated for username <> at <0.0.0.0>" after login attempt to Xauth failed.
- **40292** – A potential cross-site scripting attack existed in the anti-virus scan engine when processing compressed files.
- **39499** – (NetScreen-Security Manager) The CPU utilization on a device increased by 10 percent (%) if the device could not connect to the Device Server.
- **39458** – Configuration of 16 concurrent anti-virus messages could not be set, even though 16 is the maximum number of messages allowed when running the anti-virus Scan Manager utility in the WebUI.
- **38193** – A device could not access common public web sites when an administrator performed an anti-virus scan for HTTP on the device. The attempted connections expired after they exceed the time out threshold for connection attempts.
- **36670** – More VLANs on a device could be created than the number of VLANs the device officially supported. However, doing this sometimes caused unexpected results. Refer to the specifications sheet for your product to learn how many VLANs it supports.
- **36494** – Upon startup, a device using PPPoE sometimes generated a warning message informing that the interface gateway command was invalid. This message is a result of the gateway changing whenever the device restarts and does not effect the normal operation of the device.

- **36473** – Restarting a device while it was performing an operation in flash sometimes damaged the data on the device and caused the device not to restart or to lose the configuration.
- **36235** – Adding the pre-defined service entry "ANY" in a multiple service policy sometimes resulted in system failure.
- **36095** – The IP address of an interface could not be changed if a VIP or MIP was configured on that interface, and the VIP or MIP was used in a policy configuration. DHCP and PPPoE could not change the interface IP address if a VIP was configured using the same-as-interface option.
- **35904** – When the software lifetime was in use and after the re-key was successful, the device should have permitted traffic using older SA's to traverse the device.
- **35624** – If you set the negotiation mode on a 10/100 Ethernet port to Full Duplex and configured the holddown time on the interface to less than one second, it caused the interfaces to go up and down.
- **35615** – Any policies within the device indicated traffic shaping was active for the policy. Issuing a **get policy** CLI command displayed an "X" under the "T", for traffic shaping, in each policy. However, issuing a **get policy id number** CLI command indicated that traffic shaping was turned "off".
- **35528** – In an active-passive NSRP configuration, you needed to set a manage IP on both devices to enable each device to connect to the entitlement server and retrieve signatures.
- **29619** – When you used the CLI to configure SCEP, you could not specify an already defined Certificate Authority as the recipient of the certificate requests.
- **04992** – (NetScreen-Security Manager) Managed devices failed when there was a large amount of VPNs.
- **04960** – (NetScreen-Security Manager) Disconnecting from a NetScreen-Security Manager server caused device failure.
- **04934** – Unsetting syslog and enabling some debug settings caused device failure.
- **04836/4102** – Large fragmented packets caused device failure.
- **04798** – Using SCEP to retrieve certificates caused device failure.
- **04720** – Spaces were not supported in AV object names.
- **04716** – After the Extended license was installed, the 16 peers could not be configured.
- **04707** – Tcp-mss values were not applied to syn-ack packets leaving a tunnel.

- **04696** – If an interface IP was unset, then the VIP disappeared after PPPoE was disabled.
- **04688** – (NetScreen-Security Manager) Repeated contact failures to a NetScreen-Security Manager device caused memory leakage.
- **04672** – Reordering policies from the CLI occasionally caused them to be inoperative.
- **04660** – The CLI command **get config all** produced inconsistent results when multiple users performed the command simultaneously.
- **04587** – Messages that were sent to the syslog server were prepended with [No Name]; instead of [Root].
- **04585** – AV passed SMTP commands without inspecting if a line ended with bare LF.
- **04457** – A disabled IKE user could successfully connect through the VPN.
- **04408** – Adding a license key for virtual routers did not add the expected number of virtual routers.
- **04353** – The device dropped RTP packets because the ARP reply was delayed.
- **04350** – Scheduled DNS refresh was not operating.
- **04328** – Small packets did not forward correctly between ports.
- **04272** – The deep inspection log sent to the WebTrend server had an invalid format string.
- **04270** – Adding a VPN with the WebUI, caused device failure if the IKE gateway was created incorrectly.
- **04252** – Traffic did not filter consistently with extremely large policy configurations.
- **04162** – The **get rms ctx pol** CLI command displayed an incorrect number of rules associated with a specific policy.
- **04121** – (NetScreen-Security Manager) Enabling NetScreen-Security Manager debug caused device failure.
- **04106** – Erroneous handling of user authentication caused device failure.
- **04085** – When you created a hardware session on an active device in an HA pair, problems sometimes occurred. If the session went through a VPN tunnel, the Layer 2 table index in the hardware session became zero. This action caused irregular packet behavior.
- **04074** – Incorrectly aging out an OSPF session caused the CPU to be held too long, which then caused device failure.
- **04036** – The device failed because it returned a null pointer to an SNMP task.

- **04035** – Unknown or misaligned L2TP packets caused device failure.
- **04015** – RIP would not install a route from a neighbor under some conditions.
- **04009** – SNMP nsVpnMonIfIndex values were incorrect.
- **04003** – VLAN counters retrieved from the MIB were inconsistent.
- **03976** – Policies that were added a second time with the before option appeared in the wrong order.
- **03970** – A driver issue caused the interface to not receive traffic.
- **03925** – Migrating VPN tunnels from one cluster to another caused device failure.
- **03914** – The **set flow tcp mss** CLI command setting was unset after the device rebooted.
- **03879** – Installing new sessions incorrectly caused device failure.
- **03853** – A user could not establish a dialup session with a device after attempting to establish a remote connection to the device because the device returned a null pointer from the session. This action indicated that the device did not recognize the user and did not know how to process the session.
- **03833** – Some PDF files were unable to download when the Scan Manager was enabled.
- **03795** – The device did not properly free memory buffers after using them; therefore, they were not returned to the main memory pool.
- **03773** – The device drops some IPSec AH packets because of authentication failures, slowing packet transfer over an FTP session and causing large FTP data transfer session failures.
- **03758** – Moving or adding a policy caused device failure.
- **03751** – WebUI did not allow changing the offset-metric option.
- **03742** – Issuing the **get dlog** CLI command connected through Telnet session (instead of serial console) caused the device to hang.
- **03741** – WebUI showed incorrect RIP "Periodic Route Update Interval".
- **03705** – Duplicate expression and admin names caused device failure.
- **03637** – When the firewall acted as a TCP proxy server, and if the server returned the syn-ack packet too late in response to a syn packet, the relevant firewall flow resource was released too early and caused firewall failure.
- **03632** – When you have two VOIP phones connected to a Trust and an Untrust zone on a device running in Extended mode, and you tried to place a call, the phone obtained its IP address from a DHCP server.
- **03598** – Interface NAT was not working from Trust to DMZ security zones.

- **03592** – NTP did not work in a configuration without VSD.
- **03570** – Traffic shaping priority worked incorrectly with some small packets.
- **03562** – The device failed when using the **get config** CLI command after removing an address/service from a multi-cell policy.
- **03558** – A trace route or ping operation sometimes caused memory corruption, causing device failure.
- **03537** – The device failed when it incorrectly sent the DHCPDISCOVER packet out in the callback function.
- **03528** – The subscription key retrieval operation worked only intermittently because the device improperly closed the SSL socket.
- **03504** – The value of the sysUpTime variable from an SNMP query incorrectly displayed more than 497 days.
- **03499** – Webmail attachments were not retrieved when AV was enabled.
- **03498** – The **exec nsrp sync global-config checksum** CLI command caused device failure in some configurations.
- **03495** – You could not retrieve mail from certain mail clients that send POP3 authentication requests (such as Mozilla Mail Client) because the device did not support POP3 authentication.
- **03484** – The OSPF route table reset during network flapping.
- **03478** – A few days after you first configured the device, it would receive traffic, but could not transmit it.
- **03459/3919** – RTP packets incorrectly traversed a VPN tunnel after a SIP call was setup.
- **03435** – The Simple Mail Transfer Protocol (SMTP) client timed out when large attachments passed through a device anti-virus scan.
- **03433** – When two BGP peers established an adjacency and then lost the adjacency state, and the NetScreen peer attempted to reestablish the state, the NetScreen peer could be in the wrong state. This prevented it from reestablishing the adjacency.
- **03415** – You could not re-add a peer to a BGP peer group once you unset it.
- **03413** – A firewall device could fail when multiple users attempted unauthorized SSH sessions.
- **03405** – Resetting the root admin password through the WebUI would unset the SSH authentication.
- **03404** – The device generated incorrect traffic log titles when it sent a traffic log based on a multi-cell policy. The traffic log title displayed the same source IP and destination IP addresses.

- **03397** – The device failed because VPN traffic did not handle interrupts properly.
- **03394** – You could not manage the untrust interface through a route-based VPN.
- **03379** – After successfully configuring the device in Extended mode, the WebUI incorrectly indicated that the device was in Trust-Untrust mode.
- **03367** – When you clicked the Cancel button on the WebUI admin page for NetScreen-Security Manager, you could no longer locate the page.
- **03358** – A very long URL entry when you attempt to perform URL filtering sometimes caused device failure.
- **03356** – The Phase 2 rekey sometimes failed after the Phase 1 expired when you used Kbytes as the criteria to trigger a Phase 2 rekey operation.
- **03355** – Track IP packets were sent out at the wrong interval, increasing failed counts (decreasing success rates) even though pings worked correctly.
- **03353** – When you configured a policy using the multiple service feature including more than 49 services, the Move check box of the policy disappeared from the WebUI and the WebUI displayed some field strings incorrectly.
- **03340** – (NetScreen-Security Manager) The correct Action code was not sent when generating a traffic log.
- **03338** – The component blocking feature that forces a packet to be dropped did not work properly.
- **03320** – When an active device in an active-passive NSRP pair attempted to synchronize with the passive device, the password used in the active-passive session was not compliant with length restrictions set by the **set admin password restrict length** command. This resulted in the command failing on the passive device, creating an unsynchronized state for the password length restriction between the two devices.
- **03311** – When the VIP server detection was set to the Manual setting, the VIP server status detection still displayed the same status when the server detection parameter was set to Automatic.
- **03308** – When you attempted to change an admin name in the WebUI, the system added a new user instead of changing the name of the existing user.
- **03295** – When you issued a **get interface** CLI command or similar commands, ScreenOS truncated interface names that had too many characters.
- **03281** – When you performed an incremental Shortest Path First (SPF) operation for an OSPF virtual routing instance, the device failed.

- **03278** – When updating a dynamic VPN tunnel's peer gateway IP, a new route lookup was not performed for the updated peer gateway IP. If the updated peer gateway IP was not reachable through the old route used for the previous peer gateway IP entry, the VPN failed.
- **03273** – After you saved the value in the policy counter in the WebUI, the value was different from the actual policy count.
- **03269** – The device incorrectly auto negotiated to 10MBps half duplex after it had initially set itself to 10MBps full duplex.
- **03267** – The anti-virus feature had a problem handling the HTTP packets because a web server inserted too many unnecessary white spaces in the HTTP header.
- **03263** – When managing the device from the V1-untrust or V1-trust interface using Manage IP, multiple sessions were created for each packet.
- **03261** – When you have two VPNs active between two devices, with outgoing interfaces, after the VPN Monitor deactivated the tunnel after nine seconds, and caused a failover to the secondary VPN, the device did not update the session information.
- **03250** – A memory corruption caused device failure.
- **03243** – In an instance where the client on the Untrust side of the device connected to a MIP that connected the server to the Trust side, when an ASP began the server, it used a zero-sized window, slowing down performance, with the server sending back one character at a time.
- **03239** – When you performed an FTP transfer or email download that went beyond the maximum bandwidth allocated in the traffic shaping feature, VOIP calls experienced a lot of intermittent voice transmissions.
- **03235** – When you forcefully closed several PKA/RSA SSH sessions without properly logging out first, the system randomly failed several times.
- **03222** – Some SIP packets caused device failure when it attempted to establish a call.
- **03203** – The device sometimes failed when it traversed the session table.
- **03178** – The device sometimes failed with high CPU and the full session table due to session memory corruption.
- **03177** – Intermittent system failures occurred during an SNMP walk.
- **03152** – When running XAuth in the WebUI environment, the XAuth page displays the CHAP fragment reassembly method selected by default.
- **03136** – Gratuitous ARP packets sent out to broadcast the presence of a device were blocked from being sent.

- **03128** – Mistakes occurred with Mapped IP (MIP) translation when a remote shell used a secondary session initiated from the server for redirecting standard error output from the console.
- **03111** – When issuing the **get nat registry vector** CLI command, the device did not display any output on the console.
- **03092** – When the device was in transparent mode, it sometimes was unable to download the latest anti-virus signatures.
- **03089** – Point-to-Point Protocol (PPP) traffic that uses both source NAT and fixed port Dynamic IP (DIP) features could not pass through the device.
- **03081** – An anti-virus parsing error slowed performance for HTTP sessions.
- **03071** – If the first Virtual IP (VIP) in the VIP list did not have a service defined for it or if you added a service to the second to fourth VIP in the list, the VIP Summary Page displayed no data.
- **03068** – When you modified the IKE Phase 1 gateway name using the WebUI, the primary device in an HA pair could not synchronize properly with the backup device so that the backup device received the IKE gateway name.
- **03058** – (NetScreen-Security Manager) After successfully updating a device with the latest configuration, and then running a Delta Configuration Summary operation, the summary still displayed commands indicating that the update did not successfully transfer all settings to the device.
- **03054** – The device did not update its ARP table because too many packets queued up for the same ARP entry.
- **03042** – The serial interface on the device disappeared after you downgraded from ScreenOS 5.0.0rX to a previous version with the Unlimited Number of Users Version 2 key installed.
- **03025** – In certain situations, when a user authenticated using WebAUTH with SecureID, and the user in the Auth table timed out, subsequent attempts to authenticate failed.
- **02988** – The ALG did not work for a custom-defined remote shell (rsh) service.
- **02986** – SSHv2 with RADIUS authentication failed to authenticate external users properly.
- **02962** – Some auth messages that were formatted incorrectly caused device failure.
- **02940** – The device sent out multiple SNMP traps associated with the same event after you changed the source interface for SNMP operations.
- **02926** – The number of syslog messages sent per second from the were being limited by an internal process.

- **02924** – Simple Mail Transfer Protocol (SMTP) queued e-mails on Microsoft Outlook 2003 clients timed out when a policy had the anti-virus option enabled because you could not perform more than one SMTP transaction within one session.
- **02909** – Embedded ICMP caused the Dynamic IP (DIP) pool memory leak traffic flow to stop because the DIP allocation failed after no ports were present.
- **02975** – While performing a virus scan with the anti-virus engine, the anti-virus update failed, and no traffic could pass through the device because the policies blocked it, and the device failed repeatedly.
- **02972** – When you tried to transfer large files using SCP, the connection closed before the transfer completed.
- **02962** – When the device sent multiple authentication requests to an authentication server while waiting for a reply to a previous request, memory corruption sometimes occurred. This happened when the server sent a rejection response.
- **02952** – A code loop in a SIP disconnect state occurred and resulted in the device failing when disconnecting a SIP call over a Cisco Voice Over IP (VOIP) network.
- **02941** – When you configured a device with a Dynamic IP (DIP) and traffic shaping, the first traffic the device sent failed to reach its destination.
- **02933** – While attempting to age out specific sessions, the device sometimes went into an infinite loop causing the watchdog timer to cause device failure.
- **02915** – An invalid pointer reference between FTP control channel and data caused device failure.
- **02913** – Although a session on the device has a timeout of one second, when the session exceeded the timeout, the device did terminate the session.
- **02906** – You were unable to ping from one device to another over a VPN between two devices that were each in transparent mode running ScreenOS 5.0.0rX.
- **02869** – A device could not deliver mail and the Post Office Protocol 3 (POP3) session timed out when the device ran an anti-virus scan on an SMTP or POP3 policy.
- **02867** – If the DHCP relay server is set with an IP address, the device incorrectly attempted to resolve the IP address with the host name even though there was no host name.
- **02897** – The WebUI displayed the autokey IKE list incorrectly in instances where a listing of 5, 10, 50, or 100 entries were in the list. It displayed only 20 items per instance.

- **02880** – If the anti-virus option was enabled and the windowsupdate.microsoft.com utility was run on the policy, the utility hung and the console displayed the Network Error page. The utility worked only when the policy had the anti-virus operation disabled.
- **02874** – A fail occurred when the device prevented packets with the wrong/inactive virtual MAC address from being forwarded.
- **02853** – The WebUI inadvertently allowed adding a sub-interface in transparent mode, which caused device failure.
- **02845** – In an NSRP active-passive configuration, improper MAC table entries prevented the backup device from being managed. In some instances, you could not manage a backup device in an NSRP active-passive configuration.
- **02841** – The device inadvertently displayed an inactive route as active in an environment where two route-based VPN unnumbered tunnels mapped to one VSI. This behavior only occurred when this VSI was assigned to the Untrust zone that had an IBGP routing instance configured inside the network.
- **02829** – When obtaining a traffic log using a specific IP address on an SSH session by issuing the **get log traffic | include** CLI command, the device failed. For example, if you connected to the device using an SSH session and you issued the following command (which contains an explicit IP address):  
**get traffic log | include 10.1.1.10**  
the device shut down and failed.
- **02824** – Custom zones incorrectly supported half the number of IP address book and group entries than the predefined zones.
- **02823** – When applying the snoop filter with a destination IP address and destination port, the filter did not work.
- **02822** – The DHCP utility did not work on one of the redundant interfaces on a device. The interface did not appear in the DHCP environment in the WebUI.
- **02814** – The SNMP interface index values were inconsistent through the SNMP tree. Interface index values uniquely identify each interface.
- **02805** – Under certain traffic conditions, some DNS and HTTP session timers were set with higher values than the DNS and HTTP service timeouts.
- **02810** – A policy with the negate option did not free memory on the device properly, creating a memory leak, degrading performance on the device.
- **02796** – When the device sent out a trap that indicated an SNMP authentication failure when OSPF was enabled, the device failed.

- **02786** – If the packet that had both a destination broadcast subnet IP address and a MAC multicast address attempted to enter the device, the device dropped it.
- **02785** – A device failed continuously because an interface on the device did not check the Point-to-Point Protocol (PPP) encapsulation functionality properly.
- **02771** – Traffic through a Mapped IP (MIP) address with both source-based routing and traffic shaping enabled failed.
- **02768** – When the primary device attempted to synchronize with the backup device and sent it a new DIP session, the backup device could still have the existing DIP session and could not perform the synchronization.
- **02765** – (NetScreen-Security Manager) If a configuration is pushed to the device and the heartbeats to the device are lost, the device would invoke the configuration rollback feature because the heartbeat missed threshold was too short.
- **02762** – If you attempted to display 100 logs per page in the WebUI Traffic Log, the WebUI displayed no logs.
- **02740** – (NetScreen-Security Manager) The Log Viewer did not display data in the Alert column. The Alert column now correctly displays traffic logs associated with policies that have the Alert setting selected.
- **02736** – The Mgt-IP on a VSI replied with a virtual MAC address instead of a physical MAC address for the Ident-reset.
- **02734** – When you performed an SNMP walk operation on the Policy MIB, the procedure incorrectly displayed an integer to represent the custom service. It now correctly displays a string to represent a custom service in the Policy MIB.
- **02730** – For external Link State Advertisements (LSAs) that have a forwarding address, the priority for a forwarding route incorrectly used the interface cost as the priority value rather than the metric of intra- and inter-area OSPF routes. The metric is the correct value to use for setting a route priority.
- **02725** – In an NSRP device pair, the primary device generated a log that indicated that multiple failovers occurred, but the backup device only generated one log, indicating only one failover.
- **02718** – (NetScreen-Security Manager) Importing a device failed because the heartbeat timeout was exceeded and was not user configurable.
- **02709** – When you set a manual VPN authentication setting to NULL on a Juniper Networks security appliance, the device failed because a Null length is invalid.

- **02707** – When performing an anti-virus scan on a device, it displayed an error-constraint-drop status.
- **02694** – (NetScreen-Security Manager) ScreenOS did not send discovered SCREEN occurrences to NetScreen-Security Manager when it imported a configuration from a device.
- **02692** – The Dynamic IP (DIP) allocation failed and halted traffic entering the device, requiring the DIP allocation mechanism to be reset every two hours.
- **02688** – The CLI provided no maximum value check for BGP hold time entered on a device, incorrectly allowing you to enter any value for the hold time. If the value was greater than the maximum hold time setting of 65,525, the device incorrectly accepted the value, and the output from the **get hold-time** CLI command incorrectly displayed it as a negative number.
- **02687** – Traffic shaping did not work properly when the traffic shaping policies traversed a route-based VPN on a device.
- **02682** – When using the WebUI to set information on the backup device, the primary SNMP device was inappropriately deleted when using the **unset VSD ID 0** CLI command.
- **02680** – The SNMP **name** command inappropriately propagated across the NSRP cluster.
- **02679** – Some devices generated multiple logs for information associated with the self log.
- **02664** – Packets were sent out with the MAC address of the inactive VSI instead of the active VSI address in an active-active VSI cluster.
- **02660** – After importing a Certificate Authority (CA) certificate into a device and then rebooting the device, the device removed the certificate.
- **02656** – The WebUI home page did not display the status for Layer 2 interfaces.
- **02655** – The event log timestamp changed to Daylight Savings Time (DST) even though DST was not enabled.
- **02648** – A corrupt user login table caused device failure.
- **02642** – After configuring SCREEN setting thresholds on a device using the WebUI or CLI, the **get config | include <screen\_settings>** command did not display the configured settings.
- **02641** – (NetScreen-Security Manager) The agent caused the PKI IKE memory pool on a device to have a memory leak.
- **02629** – When running a **get config all** CLI command and redirecting the output to a file on the TFTP server when the Trust interface as the source, the file was not transferred correctly.

- **02627** – The policy move page only displayed the first 20 policies, and therefore you could not move a policy from the initial screen from where you copied the beyond the 20 policies displayed.
- **02624** – An anti-virus scan failed to scan .RAR files.
- **02621** – When a Ping request is initiated through a VPN tunnel to a MIP configuration on a loopback interface, the ICMP reply through the tunnel did not get translated back to the MIP address.
- **02620** – Issuing the **debug** CLI command for the WebSense server, caused device failure.
- **02602** – Attempts to establish a Telnet, WebUI, and SSH sessions, to the interface where management was enabled, would fail when a route from the correct interface was not provided or the route pointed to a different gateway.
- **02594** – A trace route or ping operation sometimes caused memory corruption, causing device failure.
- **02581** – You incorrectly could define the same IP address to multiple loopback interfaces over multiple subnetworks by running the **set vrouter trust-vr ignore-subnet-conflict** CLI command.
- **02580** – When you created a new custom service, and then configured a VPN using IKE, the Proxy ID setting in the VPN Autokey IKE configuration incorrectly defaulted to the new custom service, and not the ANY service.
- **02578** – A Point-to-Point-Protocol-Over-Ethernet (PPPoE) connection on a device incorrectly sent an acknowledgment for an unnumbered PPP session. The correct response to an unnumbered PPP session is a Non-Acknowledgment (NAK).
- **02555** – The system incorrectly created sessions for embedded ICMP packets.
- **02552** – Policy authentication with an external authenticating server could run into the same memory corruption when authentication failed and caused the firewall to fail.
- **02551** – An NSRP backup device indicated that a failover occurred continuously when no failure on the primary device occurred.
- **02543** – A device rebooted because of an improperly processed checksum.
- **02542** – When upgrading a device from ScreenOS 4.0.0r4 to ScreenOS 5.0.0r3, a PPP connection from a Windows XP client to a Windows 2000 server stopped working.
- **02536** – The priority value on a WebTrends syslog message varied from device to device.

- **02531** – After changing manage options in the Untrust interface with a DHCP client configured, the device renewed its IP address with the DHCP server, causing loss of configuration of MIPS, DIPs, and VIPs.
- **02530** – A TCP stack error caused the BGP neighbor state to change to the Idle state before the BGP holddown time value (default of 180 seconds) expired. The BGP neighbor state, a setting determined by whether the current BGP routing instance, can detect its neighbor to be active, and is not supposed to render the neighbor Idle until no neighbor response occurs after the holddown time elapses.
- **02486** – In some instances, after a WebSense server was enabled, when the Microsoft Outlook Calendar utility was accessed, connectivity to Outlook Email would be lost.
- **02482** – Slow http/https through VPN. Bug in H323 implementation can possibly cause session leak R. HTTP cant pass if unset flow tcp seq + set flow tcp syn combo is used.
- **02477** – You cannot configure the NSRP-Lite feature through the WebUI even though you applied an extended key.
- **02457** – The URL request function that sent content to a WebSense server sometimes engaged the CPU on a device for too long causing the device to reboot.
- **02403** – There was a flaw in the TCP stack buffer which caused the device to fail.
- **02388** – You could not set the DHCP IP address range through the WebUI when detecting an auto-probe. By attempting to perform this operation, the system displayed the following message:  
**The DHCP IP Pool not in the same subnet with gateway/interface**
- **02385** – When you selected multiple source address groups in an intra-zone policy where the source was Trust and the destination was Trust, then the groups were not displayed properly in the Policy list.
- **02372** – If you ran an OSPF virtual routing instance on a route-based VPN, under heavy traffic conditions, the device could continually spawn new sessions for the OSPF packets.
- **02362** – In some instances, a TCP session prematurely expired.
- **02344** – When you tried to bind a PKA key to an administrator account using the WebUI, the device generated a trace dump.
- **02342** – An OpenSSH client continued to use password authentication even when password authentication was not an option for SSH.
- **02333** – When a device attempted to block files with a .exe extension, it incorrectly blocked files with .zip extensions.

- **02326** – A device incorrectly created sessions if the IP address had a unicast destination while the destination MAC address had a multicast destination.
- **02298** – Commands related to Next Hop Tunnel Binding (NHTB) did not run when you used a blank character when creating a tunnel name for NHTB.
- **02297** – An anti-virus scan dropped connections with selected HTTP and HTTPS sites.
- **02162** – Unable to use the WebUI for a second IP Address.
- **02152** – In instances where you created an intra-zone policy with the source zone was Trust and the destination zone was Untrust and that used multiple addresses, the Policy list displayed the same entity for both the source and destination in the policy.
- **02116** – When the lifetime of an IKE Phase 2 Security Association (SA) reached a threshold defined by the soft lifetime buffer, a Phase 1 rekey and a delete notification for the P2 SA was generated after the P1 rekey.
- **02101** – Messages logged with a Virtual IP (VIP) incorrectly indicated the VIP connection connected and disconnected repeatedly, indicating the presence of a false positive even though the VIP connection sent acknowledgment responses to the query. The messages displayed continuously were:
  - **VIP cannot be contacted.**
  - **VIP is now alive.**
- **02026** – When a device attempted to contact a RADIUS server and the server was unavailable, the device corrupted the server reply after it was stored in device memory.
- **02024** – When a device contacted a RADIUS server for authentication while the server was performing many RADIUS authentications, the device corrupted the server reply after it was stored in device memory.
- **01955** – Unnecessary "tcp head size = 28, opt\_size=8 MSS found 0x05b4" messages appeared while debugging.
- **01998** – You could not save the **set console aux disable** CLI command into the device configuration.
- **01739** – Ping operations would not work if fast aging out of MAC addresses did not occur when a PC migrated from one port to another in the same zone.
- **01635** – The system failed when an H323 recomputed a UDP checksum; the UDP packet lengths sometimes were too consistent with the IP lengths.
- **01584** – If a virtual routing instance acted as the area border router (ABR), then the routing instance did not advertise inter-area summary routes. An inter-area summary route is one value that encompasses a range of route prefixes contained in multiple routing areas.

- **01523** – An OSPF virtual routing instance sometimes unexpectedly dropped routes.
- **01957** – The WebUI did not contain the ISP connection Test button under the Configure column in the ISP screen because a previous revision of ScreenOS was released with the button removed. The button now appears in this location.

### 3.2 Addressed Issues from ScreenOS 5.0.0r6

- **38268** – A Juniper Networks security appliance running a BGP peer virtual routing instance cannot use an MD5 type password when the device is connected to a Juniper Networks router.
- **38200** – A non-specific error in H323 caused memory leaks in device sessions.
- **38103** – The DHCP client was unable to obtain an IP address if Dynamic Track IP was enabled and the DHCP client interface was down.
- **37711** – When you have established a VPN tunnel and tried to perform a Phase II rekey, the operation intermittently failed.
- **02449** – The server kept sending LCP requests as if it never received a packet because the PPP (Point-to-Point Protocol) request sent out never left the device.
- **02446** – Unfreed memory buffers could be allocated to the point where the device could not send management traffic data.
- **02419** – The WebUI label **IP Sweep/Port Scan** in the IP and Port Scan field in the Screen menu contained incorrect references to milliseconds (5000 ms) instead of microseconds with the **ms** abbreviation (ms is the abbreviation for milliseconds).
- **02415** – A RIP routing instance dropped the default route (0.0.0.0) of another routing instance if it learned it on an unnumbered tunnel interface.
- **02413** – When you issued the command **set ike gateway**, the device always created a test certificate peer certificate type x509-signature.
- **02387** – The command line displayed only 24 characters for a URL string, although ScreenOS supports URL strings with up to 64 characters.
- **02384** – The device failed if you connected an Ethernet cable to the untrust interface in the v1-untrust zone while the device was in transparent mode.
- **02383** – Under some circumstances, the OSPF routing instance could not build an adjacency because its memory buffer was not large enough to handle large databases.
- **02379** – You could not establish the Phase II portion of a VPN tunnel when you referenced a custom service that had spaces in its name with no quote

marks around the string because ScreenOS did not recognize strings with spaces without quotes around the string.

- **02375** – The device was unable to detect and defend against a ping of death attack and would fail when these types of packets arrived at the device.
- **02370** – When you manually created a VPN tunnel in an NSRP environment in the WebUI, using an extra comma in the key portion of the **set vpn** command, the primary device failed while the backup device kept the old configuration.
- **02369** – You could not change the IKE/AUTH user password using the WebUI. The WebUI apparently took the change but it did NOT change it when the configuration was viewed.
- **02368** – ScreenOS removed the quotation marks around the VPN name with a space when you configured an NHTB value on an interface.
- **02354** – Occasionally, the ScreenOS logging environment incorrectly displayed unusual logs that indicated a hacker attacked the device. A typical message that indicated a hacker was the following:  
**2004-02-11 11:45:22 system notif 00001 Address  
\_prefix\_c0000000\_2\_p72\_ for ip address 192.0.0.0 in zone V1-  
Untrust has been deleted by netscreen via web from host  
128.32.199.217 to 128.32.199.71:80 session**
- **02323** – When you ran FTP Put or Get commands to push or obtain data to or from the device, the WebUI always indicated the device had a Deny action in its policy even when the policy was configured to permit traffic.
- **02272** – HTTP and HTTPS packets passed through VPN tunnels more slowly than expected, sometimes to the point of timing out and causing the device to continually retransmit the packets.
- **02250** – The device sometimes generated an error when you updated a device and issued the following command with the following arguments:  
**set interface tunnel.2 nhtb 10.1.2.5 vpn**
- **02207** – The NS Lookup operation completed without first authenticating to a WebAuth policy. The NS Lookup utility resolves unknown hostnames and URLs.
- **02206** – An Apple Macintosh running Operating System 9 client using the HTTP protocol failed to connect to the internet while a device had AV HTTP scanning enabled.
- **02156** – When you enable Scan-MGR, it prevented access to certain web pages because during the TCP 3-way handshake, the web server advertised a window size of 0 to the client, preventing the web page window from opening.
- **02094** – The Address Negate feature had no effect on traffic entering the device through a VPN tunnel with a VPN tunnel policy applied to it.

- **02052** – NAT Traversal (NAT-T) for IPSec did not behave correctly when both the initiator and responder were behind NAT devices.
- **01793** – A redundant interface incorrectly learned an ARP when no IP address was configured for the interface.
- **02412** – The SNMP Get response values were not correct for the ifInOctets and ifOutOctets statistics.

## 4. Known Issues

This section describes issues with the current release. For a complete listing of ScreenOS 5.0.0 issues, refer to the *Juniper Networks NetScreen Release Notes* for ScreenOS 5.0.0r10.

### 4.1 Limitations of Features in ScreenOS 5.0.0r10-DSLW

Same as ScreenOS 5.0.0r6-WLAN.

#### 4.1.1 Limitations of Features in ScreenOS 5.0.0r6-WLAN

The following limitations are present in ScreenOS 5.0.0r6-WLAN.

- You must register your product at [www.juniper.net/support/](http://www.juniper.net/support/) to activate the Deep Inspection (DI) and anti-virus (AV) services on your device. After registering your product, use the WebUI to obtain a subscription for the service.
- Only one Service Set Identifier (SSID) on the device can use wired equivalent privacy (WEP). If multiple SSIDs are configured on the device, the others must be Open or use either Personal or Enterprise Wi-Fi Protected Access (WPA).

## 4.2 Compatibility Issues in ScreenOS 5.0.0r10-DSLW

Same as ScreenOS 5.0.0r6-WLAN.

### 4.2.1 Compatibility Issues in ScreenOS 5.0.0r6-WLAN

Below is the known compatibility issue at the time of this release. A work around (starting with “W/A:”) has been provided for your convenience.

- **WEP Support for Apple Airport Extreme Adapters** – There is a known compatibility issue between ScreenOS 5.0.0r6-DSLW and Apple’s Airport Series of wireless adapters. The Apple Airport Extreme Adaptor does not support multiple WEP keys. In order for the APX card to associate with a NetScreen-5GT Wireless device, configure a 40- or 104-bit WEP key with keyID 1, and set it to be the default key.

W/A: Use WPA-PSK or WPA (either Personal or Enterprise).

## 4.3 Known Issues in ScreenOS 5.0.0r10-DSLW

- **50869** – An ADSL box configured for DHCP server trust port displays a trace message on the console. The trace message is harmless and does not inhibit functionality.
- **48977** – Fragment MAC Service Data Unit (MSDU) does not transmit at the rate that is set in the profile.
- **48005** – WPA does not function correctly when wireless1 interface is bound to the Null zone.

W/A: Bind wireless1 interface to wzone1 zone when using WPA.

- **23681** – (NetScreen-Security Manager) Updating firmware version from 5.0.0r6-WLAN to 5.0.0r10-DSLW fails with an image corruption error.

W/A: Use the WebUI or CLI to update the firmware.

- **23462** – (NetScreen-Security Manager) The percentage (%) sign cannot be used in the SSID name string.
- **05367** – PPPoA on the NetScreen-5GT Wireless ADSL device can only have a 32-bit subnet mask.

W/A: To achieve a static IP on the 5GT Wireless ADSL device, do the following:

1. **set interface adsl ip** *ip\_addr/mask*
2. **set pppoa name** *name\_str* **static-ip**
3. **unset pppoa name** *name\_str* **clear-on-disconnect**

or

1. **set interface adsl ip** *ip\_addr/mask*
2. **set pppoa name** *name\_str netmask* [ *mask* ]
3. **set pppoa name** *name\_str static-ip*

- **04788** – The ADSL LED goes off after the ADSL line reconnects. The new hardware does not have this issue.
- **04245** – The status of the untrust interface is active, but cannot pass traffic.

W/A: Bind the adsl and untrust interfaces to the Untrust zone. After the binding is set, use the **set interface adsl1 track-ip dynamic CLI** command to dynamically ping the default gateway on the adsl interface. This setting allows the untrust and adsl interfaces to automatically failover when an error occurs. Another options is to delete the adsl interface from the Untrust zone, so that the untrust interface is the only way untrust traffic can pass through the device.

### 4.3.1 Known Issues in ScreenOS 5.0.0r6-WLAN

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:”

- **46557** – Under certain specific conditions, the NetScreen device fails to send RADIUS packets to an 802.1X RADIUS server for WPA authentication. These conditions include when the RADIUS server is not on the same subnet as the NetScreen device, dynamic routing via OSPF is the only way to access the RADIUS server, and there is no reactivate operation after ScreenOS has booted on the device.

W/A: Define a static route to the RADIUS server on the NetScreen device.

- **46556** – (WebUI) If you configure the device to enable 802.1X authentication when the Auth server is already in use, the WebUI does not accept the configuration and no error message is generated.
- **46352** – (WebUI) Under certain circumstances, the WebUI may fail to display the default vales when clicking the **Cancel** button on the wireless > General Settings > Advanced page.
- If you are using an external antenna, you no longer need to configure the antenna type. The rev A documentation set describes the antenna type configuration settings. This configuration setting has been deleted in the rev B documentation set.

## 5. Getting Help

For further assistance with Juniper Networks products, visit

[www.juniper.net/support](http://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 © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

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

[www.juniper.net](http://www.juniper.net)

