NetScreen Release Notes

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

Version: ScreenOS 5.0.0r3

Release Status: Public Release

Part Number: 093-1141-000 Rev. A

Date: 01-23-04

Contents

1. Version Summary

ScreenOS 5.0.0 is the latest version of ScreenOS firmware for the NetScreen-Hardware Security Client, NetScreen-5XP, NetScreen-5XT, NetScreen-5GT, NetScreen-25, NetScreen-50, NetScreen-200 series security appliances, and the NetScreen-500 and NetScreen-5000 series security systems.

The ScreenOS 5.0.0 release is interoperable with, and provides basic support for all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions.

This version of ScreenOS is fully supported by NSM (NetScreen-Security Manager 2004), NetScreen's new security management platform.

2. New Features and Enhancements

Dial Backup, Dual Untrust, OSPF, and BGP are now available in the 10-user version of the NetScreen-5GT. Previously these features were only available in the Plus version.

For a complete list and descriptions of new features and enhancements in ScreenOS 5.0.0, refer to the *NetScreen ScreenOS Migration Guide*.

Note: *You must register your product at www.netscreen.com/cso 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 5.0.0, refer to the *NetScreen ScreenOS Migration Guide*.

4. Addressed Issues

This section describes issues that were addressed in the current release.

- **37027 -** The issue described in security advisory NS#54169 was addressed.
- **36935 -** You could not reset the NetScreen device to factory defaults settings if the NSRD wizard failed to connect the device to the NSM server.
- **36881 -** In certain cases, using the pinhole to reset the NetScreen device to factory default settings failed.
- **36865 -** When a serial interface had no IP address, even if it was in the "UP" state, the routing entry pointing to the serial interface stayed inactive.
- **36838 -** A device failure could occur if the interface information derived for a non-ip packet and received on a 24FE board is invalid.
- **36822 -** Entering the **get policy** CLI command sometimes caused the NetScreen device to crash.
- **36819 -** Under certain circumstances, IP-Spoof packets were incorrectly flagged and dropped.
- **36814 -** With dialup user group VPN manually configured proxy-id, it could not be used for bi-directional dial-up vpn policy.
- **36773 -** In Transparent mode, the IP Address Spoof Protection screen option caused the NetScreen device to incorrectly drop packets even if the "Generate Alarms without Dropping Packet" option was enabled.
- **36766 -** (NetScreen-5GT only) In transparent mode, during the initial connection attempt where the device had no established route to the destination, initial traffic was dropped on occasion by the device when AV scanning was active.
- **36736 -** A device configured with DHCP and via a configlet was unable to connect to NSM.
- **36717 -** When upgrading to ScreenOS 5.0.0, the maximum number of address groups allowed for Layer2 predefined zones incorrectly got set to the same number as for custom zones. As a result, if the number of address groups in Layer2 predefined zones surpasses the maximum number allowed, some address groups got removed during the upgrade.
- **32690 -** (NetScreen-5GT only) When multiple devices were connected with AV scanning enabled on policies, no traffic passed through the devices. For example, if two devices were connected together and both had AV scanning enabled on policies, no traffic traversed the devices.
- **02081 -** The active user table failed to clear automatically. New users were denied until the table was manually cleared.

- **02038 -** Core dumps occured occasionally when traffic matched policies which had authentication enabled.
- **02027 -** An SNMP sysObject OID reply returned in the wrong format.
- **02006 -** Enabling DHCP Relay could cause a NetScreen device to crash.
- **01972 -** A DHCP relay packet could cause a NetScreen device to crash.
- **01971 -** You were not able to add physical interfaces (different ports) of a NetScreen device in the same redundant interface group.
- **01968 -** (NetScreen-5GT and NetScreen-HSC only) Ident-reset packets that terminated on the device might have caused the device to restart.
- **01958 -** An internal mishandling of the MAC cache could cause a NetScreen device to crash.
- **01944 -** The group addresses for V1-untrust zone were getting lost after upgrading a device from a previous release. The group address for v1-untrust was incorrectly set to a maximum of 8 groups while it should have been 32.
- **01812 -** Using un-initialized memory space when creating an outgoing packet caused the device to fail.

5. Known Issues

This section describes known issues with the current release.

- Section 5.1 “Limitations of Features in ScreenOS 5.0.0” identifies features that are not fully functional at the present time, and will be unsupported for this release. NetScreen recommends that you do not use these features.
- Section 5.2 “Compatibility Issues in ScreenOS 5.0.0 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 5.0.0 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 5.0.0

The following limitations are present in ScreenOS 5.0.0.

- **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.

- **SSH Version 1 Interoperability** – The embedded SSH server in ScreenOS 5.0.0 has issues with the client from SSH Communications Security when operating in SSH version 1 mode.

  W/A: Use SSH version 2 or a different SSH version 1 client, such as OpenSSH.

- **Primary & Backup Interfaces** – (NetScreen-5XT) 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.
- **Loading License Keys** – The NetScreen-5XP device does not properly load license keys via the WebUI. However, you can load license keys via the CLI using the **exec license-key** command.
- **Aggressive Aging** – The Aggressive Aging feature is not supported on the NetScreen-5000 Series devices.

5.2 Compatibility Issues in ScreenOS 5.0.0

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 1.3 VPN client is incompatible with ScreenOS 5.0.0 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 in 5.0.0:

    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 5.0.0 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

For detailed information on how to upgrade any NetScreen device from ScreenOS 4.0.0 and later to ScreenOS 5.0.0, refer to the *NetScreen ScreenOS Migration Guide*. The migration guide provides step-by-step upgrade procedures and important information about upgrading NetScreen devices.

The migration guide also provides a step-by-step procedure to downgrade a NetScreen device from ScreenOS 5.0.0 to ScreenOS 4.0.0 and later using the **exec downgrade** CLI command.

NetScreen-5000 series only: Before you upgrade a NetScreen device to ScreenOS 5.0.0, we recommend that you verify the amount of memory on the device using the **get system** CLI command. You need 1 gigabyte of memory for NetScreen-5000. If you start upgrading the device and run into memory problems, you might see the following messages: “insufficient memory, call TAC” or “see release notes for upgrade instructions”.

5.3 Known Issues in ScreenOS 5.0.0

The following are known deficiencies in features at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:” If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

5.3.1 Known Issues in ScreenOS 5.0.0r3

- **02117 -** For a uni-directional dialup or site-to-site route-based VPN, specific routes are required on the receiving VPN device so that the returning traffic can go back into the correct tunnel interfaces accordingly. This is a result of the dynamic routing failover feature in ScreenOS 5.0.0.

  W/A: Configure a static route to allow the returning traffic to go through the appropriate tunnel interface for each VPN tunnel.

- **02094 -** Address negate does not work for traffic coming from a VPN tunnel policy.
- **02076 -** (NetScreen-5XP only) The status LED light blinks considerably slow in comparison with ScreenOS 4.0.0.

- **02062 -** Under certain circumstances, track-ip is not sent out and causes NSRP failover operation to fail.
- **02059 -** Using the WebUI to change an IKE gateway from "static IP" to "dynamic IP" automatically changes the setting from "main mode" to "aggressive mode".
- **02057 -** Multiple custom addresses or service groups in a policy might cause a NetScreen device to crash during restart.
- **02050 -** Configuring an address group from a Mac computer using Internet Explorer might cause a NetScreen device to crash.
- **02045 -** Under certain circumstances, IP-Spoof packets where incorrectly flagged and dropped.
- **02044 -** An operation using SSH version 1 to the access the device failed when using Radius for admininistration authentication.
- **02034 -** In transparent mode, when selecting the WebAuth option in the WebUI for the V1-Untrust Zone, it appears to take effect, but when closing the window and then returning to the V1-Untrust configuration window, the WebAuth option is no longer selected.
- **02019 -** You cannot use the WebUI to remove the key-id and preshared key of the primary NTP server.
- **02001 -** When modifying the default gateway of an interface using DHCP or PPPOE, the Netscreen device does not update the corresponding routing entry accordingly.
- **01993 -** You cannot modify the Management Services on interfaces using DHCP via the WebUI.

  W/A: Use the CLI.

- **01985 -** You cannot schedule a policy via the WebUI.

  W/A: Use the CLI.

- **01970 -** Under certain circumstances, the NetScreen device does not send email alerts.

5.3.2 Known Issues from ScreenOS 5.0.0r2

- **36768 -** (NetScreen5XT and 5GT only) The modem TEST button is missing in the WebUI.
- **36708 -** You cannot view the traffic logs for a vsys if you entered the vsys as a root admin user.

  W/A: You must enter each vsys as the vsys admin to view the traffic logs for that vsys.

- **36669** - When 20,000 or more policies are configured on a NetScreen device, you might experience a two- to three-minute delay when scrolling through the Policy List page in the WebUI.
- **35620 -** (NetScreen-5GT only) If a policy is using a local address, any modification to the netmask of the address produces a trace dump on the console. This modification should not be a permitted action for the device.
- **36594 -** This release of ScreenOS does not support Bootstrap Protocol (BootP) requests.
- **36494 -** Upon startup, NetScreen devices using PPPoE might generate a warning message informing that the interface gateway command is invalid. This is a result of the gateway changing whenever the device restarts and does not effect the normal operation of the device.
- **36473 -** Restarting a NetScreen device while it is performing an operation in flash might damage the data on the device and cause the device not to restart or to lose the configuration.

  W/A: Wait until the NetScreen device has completed its operation in flash before restarting the device.

- **36365 -** In the WebUI, on the Traffic Log page for policies (under Reports), the table displaying the information might disappear after viewing multiple pages of traffic logs.

  W/A: Refresh the Traffic Log page for policies by clicking the Refresh button on your Internet Browser.

- **34279 -** (For NetScreen-5000 Series) NetScreen devices might unexpectedly drop traffic that is processed by the CPU module and that matches a policy in which the “Diffserv” option is enabled.

  W/A: Disable the “DiffServ” option on the policy.

5.3.3 Known Issues from ScreenOS 5.0.0r1

- **Documentation Correction -** Page 3 of the *What's New in NetScreen ScreenOS 5.0* states incorrectly that NetScreen devices support routing based on the source interface. The current implementation does support routing based on source IP address.
- **36670 -** You can create more VLANs on a NetScreen device than the number of VLANs the device officially supports. However, doing this might cause unexpected results. Refer to the specifications sheet for your NetScreen product to learn how many VLANs it supports.

- **36235 -** Adding the pre-defined service entry "ANY" in a multiple service policy may result in a system reboot.

  W/A: Do not enter "ANY" as a service in a multiple service policy.

- **36095 -** You cannot change the IP address of an interface if a VIP or MIP is configured on that interface, and the VIP or MIP is used in a policy configuration. DHCP and PPPoE cannot change the interface IP address if a VIP is configured using the same-as-interface option.

  W/A: Unset the policy that uses the VIP or MIP before you change the IP address of an interface. For interfaces using DHCP or PPPoE, do not use virtual IP addresses.

- **36018 -** (NetScreen-5GT only) The two month entitlement expiration notice in the event log is triggering during the incorrect timeframe. For example, if the AV entitlement expires in 52 day, the event log indicates "License key av_key is about to expire in 2 months".
- **35977 -** (NetScreen-5XT only) The NetScreen device might drop TCP traffic because it miscalculates the length of the tcp-syn-check.

  W/A: Do not enable the TCP sequence checking feature on the device.

- **35904 -** (NetScreen-5GT only) NetScreen devices need to support two incoming IPSec keys. When the software lifetime is in use and after the re-key is successful, the device should permit traffic using older SA's to traverse the device.
- **35735 -** A root administrator cannot manage the root system from a host that resides on a virtual system.

  W/A: You must connect from the root network to be able to manage the root system.

- **35624 -** If you set the negotiation mode on a 10/100 Ethernet port to Full Duplex and configure the holddown time on the interface to less than one second, it causes the interfaces to go up and down.

  W/A: Set auto-negotiation on the interface. You can do this using the **set interface interf_name phy auto** CLI command.

- **35615 -** (NetScreen-5GT only) Any policies within the device indicates traffic shaping is active for the policy. Issuing a 'get policy' CLI command displays an "X" under the "T", for traffic shaping, in each policy. However, issuing a 'get policy id <number>' CLI command indicates that traffic shaping is turned "off".

- **35582 -** In an NSRP configuration, active/active or active/passive, if you move a physical interface to a different zone on one device, you must manually do the same on the other device because this type of change does not get automatically synchronized.
- **35528 -** In an active/passive NSRP configuration, you must set a manage IP on both devices to enable each device to connect to the entitlement server and retrieve signatures.
- **35516 -** In an active/passive NSRP configuration, when you load a PKA key onto the master device, the master does not automatically synchronize the backup device.

  W/A: Manually synchronize the two devices.

- **35439 -** (NetScreen-5GT only) Within the WebUI, identical routes are displayed on multiple pages. When the number of routing table entries exceeds the maximum number of routes permitted on a single page, all subsequent pages display the routes from the first page.
- **35417 -** If you set the guaranteed or maximum bandwidth (GBW or MBW) higher than the interface bandwidth, traffic does not pass through if there is a policy configured that specifies traffic shaping.

  W/A: Adjust the GBW or MBW to be equal or less than the interface bandwidth.

- **35336 -** If you enabled VPN tunneling for syslog traffic and the source interface is bound to a zone that contains multiple interfaces, after upgrading a device from ScreenOS 4.0.0 to ScreenOS 5.0.0, the source interface might have changed.

  W/A: After upgrading the NetScreen device, verify the VPN settings for syslog and modify if necessary.

- **35238 -** For devices in an NSRP configuration, active/active or active/passive, you have to manually issue the **delete ssh device all** CLI command on both devices.
- **34950 -** (NetScreen-5000 only) Failover between two layer 2 interfaces in the same layer 2 security zone is not supported.
- **34922 -** (NetScreen-50 only) You cannot configure a VSI when the NetScreen device is in an active/passive NSRP configuration.
- **34880 -** (NetScreen-5GT only) Issuing the CLI command 'set interface <interface> manage ident-reset' displays incorrectly as 'set interface <interface> ident-reset' (without the word "manage" in the configuration file).

- **34670 -** (NetScreen-5GT only) Issuing the CLI command 'set/unset firewall exclude log-self exclude ike' does not change the state of "Log Self for IKE". The 'get firewall' command displays "Log Self for IKE" constantly in the "Off" state.
- **34663 -** Enabling the RTO mirror group direction feature using the **set nsrp rto-mirror id** <*id*> **direction** { **in** | **out** } CLI command, might cause the preempt mode feature not to work.
- **34414 -** The NetScreen device does not perform a revocation check on the signature attack database upon requesting an update.
- **34070 -** (NetScreen-5GT only) The event message 'AV: Suspicious client <Source IP> <Source Port> -> <Destination IP> <Destination Port> used <X> percent of AV resources, and exceeded the max. of <y> percent' displays only when you issue a 'get event' CLI command, and not when you issue a 'get log event' CLI command.
- **33916 -** A NetScreen device supports a maximum of 256 OSPF interfaces.
- **33598 -** For inter-vsys traffic, if both vsys define a policy with user authentication, the NetScreen device does not prompt the user for authentication for each policy, but only once when it matches the first policy.
- **33544 -** Normally upon startup, a NetScreen device with the URL filtering feature enabled, tries to connect to a Websense server. Currently this attempt to connect to a Websense server fails and the NetScreen device logs the event.
- **33027 -** NetScreen devices do not support policy-based dialup VPN and MIP if the MIP is configured on the tunnel interface which belongs to a tunnel zone.

  W/A: For dialup user VPNs only: use routing-based VPN and configure the MIP on a tunnel interface bound to a security zone.

- **32983 -** You can select multiple services in a policy, but later on, if you want to modify the services to ANY, the NetScreen device does not let you. Instead, you get a message prompting you to use the multiple service selection dialog box, which does not contain ANY, to modify the services.

  W/A: In the multiple service selection dialog box, remove all but one service from the previous selection, and then click **OK**. Next, select "ANY" from the Service drop-down list.

- **32159 -** NetScreen devices do not support a second level of certificate verification if the end entity certificate and OCSP responder certificate are issued by the same CA.

- **32077 -** (NetScreen-5GT only) When you enable or disable HTTP Webmail functionality, log entries are not generated in the event log (i.e. 'set/unset av http webmail enable'; 'set/unset av http webmail url-pattern-name <name for the URL pattern>').
- **32072 -** (NetScreen-5GT only) When you disable AV functionality for HTTP, SMTP, and POP3, log entries are not generated in the event log (i.e. 'unset av scan-mgr content http'; 'unset av scan-mgr content smtp'; 'unset av scan-mgr content pop3').
- **31364 -** When performing source port translation for passive FTP data channel, the NetScreen device translates the source port number to the same port number as the original destination port. This does not affect traffic.
- **30844 -** When AV is enabled, you cannot download files to the NetScreen device through a VPN using the WebUI.

  W/A: Specify a permit policy and place it above the policy with AV in the policy list.
- **30842 -** Source and destination NAT are not supported for RTP and RTCP traffic for H.323.
- **29619** - When you use the CLI to configure SCEP, you cannot specify an already defined Certificate Authority as the recipient of the certificate requests.

  W/A: Use the WebUI.
- **28878 -** Removing a vsys does not free the memory (30 bytes) used by that vsys.
- **28138 -** The Websense server provides erroneous protocol version information, which the NetScreen device displays.
- **28016 -** NetScreen devices do not support a MIP in the same zone as the destination host.

  W/A: Use policy-based destination NAT.

5.3.4 Known Issues from Previous Releases

- **27083 -** When you enter the **set service** command to create a custom service, the NetScreen device does not check if you entered valid source and destination port numbers.
- **25841 -** When you configure RIP on the NetScreen device and enter the **get config** command, the output displays the **set protocol rip** command twice. This is a display issue that does not affect the performance of the device.

6. Getting Help

For further assistance with NetScreen products, visit

www.netscreen.com/services/contact_tac

NetScreen occasionally provides maintenance releases (updates and upgrades) for ScreenOS firmware. To have access to these releases, you must register your device with NetScreen at the following address:

www.netscreen.com/cso

Copyright © 2004 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-Hardware Security Client, 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 NetScreen Technologies, 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:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com