

NetScreen Release Notes

Product: NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50,
NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200-8G

Version: ScreenOS 4.0.3r9

Release Status: Public Release

Part Number: 093-1739-000 Rev. A

Date: 8-17-05

Contents

1. [“Version Summary on page 3](#)
2. [“New Features and Enhancements on page 3](#)
 - 2.1 [“New Features and Enhancements in ScreenOS 4.0.3 on page 3](#)
 - 2.1.1 [“Feature Enhancements in ScreenOS 4.0.3r9 on page 3](#)
 - 2.1.2 [“Feature Enhancements in ScreenOS 4.0.3r7 on page 3](#)
 - 2.1.3 [“Feature Enhancements in ScreenOS 4.0.3r6 on page 3](#)
 - 2.1.4 [“Feature Enhancements in ScreenOS 4.0.3r4 on page 4](#)
 - 2.1.5 [“New Features in ScreenOS 4.0.3r3 on page 4](#)
 - 2.1.6 [“New Features in ScreenOS 4.0.3 on page 4](#)
 - 2.2 [“New Features in ScreenOS 4.0.2 on page 6](#)
 - 2.3 [“New Features and Enhancements in ScreenOS 4.0.1 on page 7](#)
 - 2.3.1 [“New Features in ScreenOS 4.0.1 on page 7](#)
 - 2.3.2 [“Feature Enhancements in ScreenOS 4.0.1 on page 8](#)
3. [“Changes to Default Behavior on page 12](#)
 - 3.1 [“Changes to Default Behavior in ScreenOS 4.0.3r4 on page 12](#)
 - 3.2 [“Changes to Default Behavior in ScreenOS 4.0.3r1 on page 12](#)
 - 3.3 [“Changes to Default Behavior in ScreenOS 4.0.1 on page 12](#)
4. [“Addressed Issues on page 13](#)
 - 4.1 [“Addressed Issues in ScreenOS 4.0.3r9 on page 13](#)
 - 4.2 [“Addressed Issues in ScreenOS 4.0.3r8 on page 15](#)
 - 4.3 [“Addressed Issues in ScreenOS 4.0.3r7 on page 16](#)
 - 4.4 [“Addressed Issues from ScreenOS 4.0.3r6 on page 16](#)

- 4.5 “Addressed Issues from ScreenOS 4.0.3r5 on page 20
- 4.6 “Addressed Issues from ScreenOS 4.0.3r4 on page 22
- 4.7 “Addressed Issues from ScreenOS 4.0.3r3 on page 29
- 4.8 “Addressed Issues from ScreenOS 4.0.3r2 on page 29
- 4.9 “Addressed Issues from Prior Releases on page 29
- 5. “Known Issues on page 37
 - 5.1 “Limitations of Features in ScreenOS 4.0 on page 38
 - 5.2 “Compatibility Issues on page 38
 - 5.2.1 “Compatibility Issues in ScreenOS 4.0 on page 38
 - 5.2.2 “Upgrade Paths from Previous Releases on page 39
 - 5.2.3 “Migrating NSRPv1 to NSRPv2 on page 40
 - 5.3 “Known Issues in ScreenOS 4.0 on page 41
 - 5.3.1 “Known Issues in ScreenOS 4.0.3r9 on page 41
 - 5.3.2 “Known Issues in ScreenOS 4.0.3r8 on page 41
 - 5.3.3 “Known Issues in ScreenOS 4.0.3r7 on page 41
 - 5.3.4 “Known Issues from ScreenOS 4.0.3r6 on page 41
 - 5.3.5 “Known Issues from ScreenOS 4.0.3r5 on page 41
 - 5.3.6 “Known Issues from ScreenOS 4.0.3r4 on page 42
 - 5.3.7 “Known Issues from ScreenOS 4.0.3r3 on page 44
 - 5.3.8 “Known Issues from ScreenOS 4.0.3r2 on page 44
 - 5.3.9 “Known Issues from ScreenOS 4.0.3r1 on page 44
 - 5.3.10 “Known Issues from ScreenOS 4.0.2 on page 45
 - 5.3.11 “Known Issues from ScreenOS 4.0.1r3 on page 46
 - 5.3.12 “Known Issues from ScreenOS 4.0.1r1 on page 47
- 6. “Getting Help on page 48

1. Version Summary

ScreenOS 4.0.3r9 is the latest release version of ScreenOS 4.0.3 firmware for the the NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204 and NetScreen-208 security appliances, and the NetScreen-500 and NetScreen-5200-8G security systems.

The ScreenOS 4.0.3r9 release is interoperable with, and provides basic support for NetScreen Remote versions 5.13, 7 and 8, and ScreenOS 2.6.1 and later versions. Please refer to the NetScreen-Global PRO release notes to find out which versions of ScreenOS are supported.

2. New Features and Enhancements

Occasionally, existing features are enhanced in ScreenOS maintenance releases to provide new functionality. The following subsections identify those features and the maintenance release in which they were enhanced. If there is no subsection for a particular ScreenOS release, that release included no feature enhancements.

2.1 New Features and Enhancements in ScreenOS 4.0.3

The following sections provide an overview of new features that were introduced in the initial release of this version of ScreenOS, as well as existing features that were enhanced. For more detailed descriptions, refer to the *NetScreen New Features Guide* pertaining to this release.

2.1.1 Feature Enhancements in ScreenOS 4.0.3r9

None.

2.1.2 Feature Enhancements in ScreenOS 4.0.3r7

The following is a feature enhancement in ScreenOS 4.0.3r7:

- **NISCC VULN 236929** – NISCC VULN 236929 has been addressed. See TAC knowledge base entry for further information.

2.1.3 Feature Enhancements in ScreenOS 4.0.3r6

The following is a feature enhancement in ScreenOS 4.0.3r6:

- **Increased Capacity in Auth Table** – The Auth Table on the NetScreen-5200-8G now handles more than 30,000 users, increasing its capacity from 12,288 users.

2.1.4 Feature Enhancements in ScreenOS 4.0.3r4

The following is a feature enhancement in ScreenOS 4.0.3r4:

- **Performance Enhancement** - TCP session creation and session tear-down has been accelerated while lowering CPU utilization.

2.1.5 New Features in ScreenOS 4.0.3r3

Following is a new feature in ScreenOS 4.0.3r3:

- **Blocking Traffic in Transparent Mode** - This release introduces a new command that provides administrative control over the forwarding of non-IPv4 and non-ARP unicast, multicast, and broadcast traffic when the device is in transparent mode.

By default, the device blocks all non-IP and non-ARP unicast traffic when it is in transparent mode. Now, you can also block multicast and broadcast traffic when you specify the **unset interface vlan1 bypass-non-ip-all** command. This new command blocks all Layer 2 non-IP and non-ARP unicast, multicast, and broadcast traffic.

You can still specify the existing command, **set interface vlan1 bypass-non-ip**, to allow all non-IP traffic to pass through the device. To revert to the default behavior of the device, which is to block all non-IP and non-ARP unicast traffic, specify the **unset interface vlan1-bypass-non-ip** command.

Note that the **unset interface vlan1 bypass-non-ip-all** command always overwrites the **unset interface vlan1 bypass-non-ip** command when both commands are in the configuration file. Therefore, if you had previously specified the **unset interface vlan1 bypass-non-ip-all** command and would like the device to revert to its default behavior of blocking only the non-IP, non-ARP unicast traffic, you should first specify the **set interface vlan1 bypass-non-ip** command to allow all non-IP traffic to pass through the device, then specify the **unset interface vlan1-bypass-non-ip** command to block only the non-IP, non-ARP unicast traffic.

2.1.6 New Features in ScreenOS 4.0.3

Following are new features in ScreenOS 4.0.3:

- **RSH ALG** - The NetScreen device supports the Remote Shell application-layer gateway (RSH ALG). RSH authenticates users based on their user names and passwords. This release of ScreenOS supports RSH in Transparent (L2), Route (L3) and NAT modes; but it does not support port translation of RSH traffic. The RSH service is in the Service drop-down list in the Policy Configuration dialog box (WebUI), and is included in the list of services displayed when you issue the get service command (CLI).
- **Source-based Routing** - By default, the NetScreen device uses only destination IP addresses to find the best route in the route table. When you enable source-based routing in a virtual router, the device performs route table lookups based on the source IP address. If the device does not find a route based on the source IP address, it uses the destination IP address for the route lookup.
- **IKE Pass-Through for MIP** - (NetScreen-5XP/XT, -25, -50) When the Untrust zone interface IP address is the same as a mapped IP (MIP) address, and there is no VPN configured on that interface, the NetScreen device forwards IKE traffic destined for the MIP, instead of attempting IKE negotiations.
- **Increased Number of VIPs** - The number of VIPs supported by each device has doubled. Therefore, the NetScreen-25 and NetScreen-50 support up to 4 VIPs, the NetScreen-200 series and NetScreen-500 support up to 8 VIPs, and the NetScreen-5200 supports up to 16 VIPs.
- **Local Auth Users in Multiple Groups** - To facilitate managing users and user groups, the device now allows an Auth user to be a member of up to four local user groups. A user who belongs to more than one group is required to supply a username and password only once, before being granted access to the resources defined for each group in which the user is a member.
- **Multiple Syslog Servers** - To provide a higher degree of reliability, you can configure a NetScreen device to send event and traffic logs to up to four syslog servers. To do so, use the **set syslog config ip_addr** command for each syslog server that you want to define. You can configure multiple syslog servers through the CLI only.
- **Shared IKE IDs** - The shared IKE ID feature facilitates the deployment of a large number of dialup users. With this feature, the NetScreen device authenticates multiple dialup VPN users using a single group IKE ID and preshared key.
- **WebTrends Log Enhancements** - In addition to critical, alert, and emergency events, you can now use WebTrends to customize syslog reports for debugging, information, notification, warning and error events.
- **Log Dialup User's IP Address** - The NetScreen device now logs the following information about a dialup user: user name and IP address.

- **PHY Hold-down Timer** - (NetScreen-5200-8G) You can now configure the hold-down timer on a physical port when it is in a redundant interface configuration. The hold-down timer is required for a smooth integration where spanning tree is involved on the switches.
- **OCSF Enhancement**- When a NetScreen device uses OCSF to verify the status of a certificate, it acts as an OCSF client and sends a verification request to an OCSF responder. When the NetScreen device receives the response, it verifies the validity of the responder's signature by using the certificate of the responder. In this release, the certificate of the responder may either be embedded in the OCSF response, or stored locally and specified in the OCSF configuration. If the certificate is stored locally, use the following command to specify the locally stored certificate:

set pki authority *id-num* cert-status ocsf cert-verify id *id-num*

2.2 New Features in ScreenOS 4.0.2

The following items are new features introduced in ScreenOS 4.0.2r1:

- **Password Minimum Length** - You can now set the following command to set a minimum length for the root admin password:
set admin password restrict length *number*
Only the root admin can set this command.
- **Console Access** - You can now set the following command to restrict the root admin to logging in to the NetScreen device through the console only:
set admin root access console
Only the root admin can set this command.
- **Login Attempts** - The root admin can now set the following command to limit the number of unsuccessful login attempts that are allowed before the device closes the Telnet connection:
set admin access attempts *number*
- **Telnet Access** - The root admin can now set the following command to require a VPN for admins that access the NetScreen device through a Telnet connection:
set admin telnet access tunnel
- **Concurrent Session Increase** - (NetScreen-25/50) The NetScreen-25 now supports 8,000 concurrent sessions and the NetScreen-50 now supports 32,000 concurrent sessions.

- **VPN Capacity Increase** - (NetScreen-25/50) The NetScreen-25 now supports up to 100 dialup VPN tunnels in addition to 25 site-to-site VPN tunnels. The NetScreen-50 now supports up to 400 dialup VPN tunnels in addition to 100 site-to-site VPN tunnels.
- **Redundant Interface** - (NetScreen-50) The NetScreen-50 now supports redundant interfaces.
- **Virtualization Key** - (NetScreen-200 Series) A new software key supports up to 32 VLANs, 5 additional custom virtual routers, and 10 additional user-configurable security zones.
- **SCREENs for Management Zone** - Firewall options are now available to the MGT zone. This will protect the management port from different types of attacks.
- **WebUI Traffic Log Display** - NetScreen provides traffic logs so you can monitor the traffic that policies permit across the firewall. The WebUI now displays traffic logs that include the number of bytes transmitted between a source and destination for each session.

2.3 New Features and Enhancements in ScreenOS 4.0.1

The following sections provide an overview of new features that were introduced in the initial release of this version of ScreenOS, as well as existing features that were enhanced. For more detailed descriptions, refer to the *NetScreen New Features Guide* pertaining to this release.

2.3.1 New Features in ScreenOS 4.0.1

The following items are new features introduced in ScreenOS 4.0.1:

- **Destination-Based Session Limit** – A new SCREEN option allows you to set a limit for the number of concurrent sessions directed to a single destination. This option permits the NetScreen device to deflect a flood of traffic targeting a host, such as a web server, at a specific IP address.
- **ICMP Port Unreachable Mapping** – In response to an ICMP echo request, an ICMP port unreachable message reports that the targeted host cannot be reached via the network. Because the delivery of such a message does not involve any further action, whenever a NetScreen device detects an ICMP port unreachable message, it marks the session to which it belongs for deletion, rather than waiting for the standard timeout to cause the session to expire.

- **Aggressive Aging** – When the session table nears its maximum capacity, the NetScreen device aggressively ages out the oldest entries from its session table. You need to set the following three parameters:
 - A high-watermark, at which point the aging-out process begins
 - A low-watermark, at which point the aging-out process stops
 - An early ageout time, which is the amount of time subtracted from the normal session age-out after the number of sessions exceeds the high-watermark and before it retreats below the low-watermark¹ (Note: When the number of sessions is under the low-watermark setting, the normal session age-out time takes effect.)

The Aggressive Aging feature is not supported on the NetScreen-5200.

- **SQL*Net Services** – The SQL*Net v1 and SQL*Net v2 services have been added to the list of predefined services. SQL*Net is a structured query language application protocol developed by Oracle. It provides a transparent TCP connection between a client host and a database server, or between one database and another. There are two primary differences between SQL*Net v1 and v2. Version 1 uses 1525 as the default destination port, and version 2 uses 1521. Another difference is that version 1 uses static port binding, version 2 uses dynamic port binding; that is, after the client and server conclude the TCP handshake on port 1521, the server sends a message that specifies a dynamically assigned host IP address and port number. When the NetScreen device receives this message, it creates a gate, or “pinhole”, in the firewall at that port number through which it allows SQL*Net v2 queries to pass.
- **UNIX Crypt() Password Hashing** – NetScreen now supports crypt() hashing for authentication user passwords.

2.3.2 Feature Enhancements in ScreenOS 4.0.1

The following items are modifications of existing features introduced in previous versions of ScreenOS:

- **H.323** – NetScreen has added support for H.323 Fast Start and H.245 tunneling. Both features reduce the setup time for H.323 calls.

1. When you set and enable the aggressive ageout option, the normal session timeout value displayed in the configuration remains unchanged. However, when the aggressive ageout period is in effect, these sessions time out earlier—by the amount you specify for early ageout—instead of counting down all the way to zero.

- **Layer 2 IP Spoof Checking** – A NetScreen device in Transparent mode (Layer 2) can detect packets whose source IP address has been spoofed. Layer 2 and Layer 3 IP spoof checking make use of different elements in the configuration.
 - **Layer 3** – When the NetScreen device is operating in Route or NAT mode, the mechanism to detect IP spoofing relies on route table entries. If, for example, a packet with source IP address 10.1.1.1 arrives at ethernet2, but the NetScreen device has a route to 10.1.1.0/24 through ethernet1, IP spoof checking notes that that address arrived at an invalid interface (as defined in the route table, a valid packet from 10.1.1.1 can only arrive via ethernet1, not ethernet2). Therefore, the device concludes that the packet has a spoofed source IP address and discards it.
 - **Layer 2** – When the NetScreen device is operating in Transparent mode, the IP spoof checking mechanism makes use of address book entries. For example, you have defined an address for “web server A” as 200.1.1.1/32 in the V1-DMZ zone. If a packet with source IP address 200.1.1.1 arrives at a V1-Untrust zone interface, IP spoof checking notes that that address arrived at an invalid interface (because the address belongs to the V1-DMZ zone, not to the V1-Untrust zone). Therefore, the device concludes that packet has a spoofed source IP address and discards it.
- **Logging** – Several logging enhancements have been added that increase your ability to mine the event, self, and traffic logs to obtain specific information. Also, the information that the NetScreen device sends to an external management application regarding configuration changes is more detailed than in previous ScreenOS releases.
 - **Event Log** – The message that appears in the event log displays the names of all dialup VPN users that are currently connected to the NetScreen device, even if they are members of a dialup group.
 - **Self Log** – You can use the following CLI command to filter information retrieved from the self log by destination port number:
get log self dst-port { port_low-port_high | port_num } [src-port { port_low-port_high | port_num }] | no-rule-displayed]. This addition allows you to sift through the log for all entries related to a particular service, such as Telnet (port 23), HTTP (port 80), and so on.
 - **Traffic Log** – Each traffic log entry now contains the action taken by the policy that applies to that traffic (permit, tunnel, or deny).
 - **Configuration Changes** – When the NetScreen device sends an event log message regarding a configuration change to an external management server running syslog, WebTrends, or NetScreen-Global PRO, the message now specifies the change made (as opposed to sending the generic statement “config changed”).

- **Granular Blocking of HTTP Components** – You can selectively choose which HTTP components—ActiveX controls, Java applets, .exe files, and .zip files—that you want the NetScreen device to block.
- **FQDN for Dynamic IKE Gateways** – For an IKE peer that has a static fully qualified domain name (FQDN) but a dynamically assigned IP address, you can specify the FQDN in the local configuration for the remote gateway. For example, an Internet service provider (ISP) might assign IP addresses via DHCP to their customers and maintain a Domain Name Service (DNS) mapping of the FQDN to the IP address. Without needing to know its current IP address, you can now configure an AutoKey IKE VPN tunnel to that peer using its FQDN instead.
- **Bidirectional Policies for Dialup VPN Users** – You can create bidirectional policies for dialup-to-LAN VPNs. This feature provides similar functionality as a dialup-to-LAN dynamic peer VPN configuration. However, in that configuration, the dialup user must configure an internal IP address, so that the admin at the LAN site can use it as the destination address when configuring an outgoing policy. With this new feature, the NetScreen device protecting the LAN uses the predefined address “Dial-Up VPN” as the source address in the incoming policy and the destination in the outgoing policy.
- **WebUI Support for Layer 3 Vsys** – You can now configure a virtual system (vsys) to use IP classification to distinguish traffic bound for itself either through the CLI or WebUI.
- **More Zones per Vsys** – In addition to the shared Untrust security zone and a dedicated Trust-*vsys_name* security zone, a vsys can have up to three dedicated user-defined security zones.
- **RADIUS Access-Challenge Support** – NetScreen devices can now process access-challenge packets from an external RADIUS server when an authentication user attempts to log on via Telnet. Access-challenge presents an additional condition to the login process after the approval of a user name and password. After an authentication user responds to a login prompt with the correct user name and password, the RADIUS server sends an access-challenge to the NetScreen device, which it then forwards to the user. When the user replies, the NetScreen device sends a new access-request with the user’s response to the RADIUS server. If the user’s response is correct, the authentication process concludes successfully.
- **Fragment Reassembly** – You can enable the reassembly of fragmented IP packets and TCP segments, so that the NetScreen firewall can examine them for content-based attack signatures that might be indiscernible when fragmented. The NetScreen device performs fragment reassembly only if the service is HTTP or FTP.

- **Interface Binding to MGT Zone** – You can now bind an interface to the MGT zone and then direct management traffic to the device through that interface. This option is especially useful for a NetScreen-25, -50, -204, and -208—none of which has a dedicated MGT interface—operating in Transparent mode. When replying to ARP requests to VLAN1, such a device replies from every interface. If you bind an interface to the MGT zone, the NetScreen device only responds from that interface.
- **DNS Refresh** – In addition to the existing method of setting a time for a daily automatic refresh of the DNS table, you can also define an interval of time from 4 hours to 24 hours.
- **VPN Monitoring** – By default, the NetScreen VPN monitoring feature uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address. You can now specify both the source and destination IP addresses used with the VPN monitoring feature. The CLI command is **set vpn name monitor [source-interface *interface* [destination-ip *ip_addr*]]**.
- **Attack Monitoring** – You can use the following CLI command to instruct the NetScreen device to notify you of an attack, but instead of taking action, it allows the packets to pass: **set zone *zone* screen alarm-without-drop**. This option is useful for attack analysis and forensics.
- **Auth Banners** – The size of the authentication banners that appear when the NetScreen device prompts an authentication user to log on has been increased from 127 bytes to 220 bytes.
- **Intrazone NAT Support** – You can now enable network address translation (NAT) on intrazone policies.
- **DHCP Settings Propagation** – When a NetScreen device is acting both as a DHCP client and a DHCP server, you can enable it to transfer DHCP settings (IP addresses for DNS servers, WINS servers, POP3 and SMTP servers, news, and NetInfo servers) learned through the DHCP client module to the DHCP server module.
- **SNMP Subnet** – You can define an SNMP community member as either an individual host or a subnet with the following CLI command: **set snmp host *comm_name ip_addr [mask]***. If you define a subnet, any device on that subnet can poll the NetScreen device for SNMP MIB information. However, the NetScreen device cannot send an SNMP trap to a subnet, only to an individual host.
- **NSRP** – A new command has been added to avoid the unnecessary synchronization of Network Time Protocol (NTP) clock updates when two devices in an NSRP cluster are in an active/active configuration: **set ntp no-ha-sync**. Because both devices simultaneously synchronize their system clocks with the same NTP server, it is unnecessary to relay that information to each other.

3. Changes to Default Behavior

Occasionally, the default behavior of the ScreenOS changes when a new release is issued. The following sections describe those changes. If there is no subsection for a particular ScreenOS release, that release included no default behavior changes.

3.1 Changes to Default Behavior in ScreenOS 4.0.3r4

- **NSRP State Change Logging** – The master of a VSD group records the state changes of other VSD group members in its event log.

3.2 Changes to Default Behavior in ScreenOS 4.0.3r1

- **Transparent Mode Defaults Secure** – NetScreen devices in Transparent mode do not permit any traffic between zones if there are no policies configured on the devices. Previously, NetScreen devices in Transparent mode transmitted ARP and other non-IP multicast traffic between zones even if there were no policies configured.
- **Monitor Timeout Setting** – The (fixed) VPN Monitor timeout has changed from 2 to 5 seconds to accommodate the longer latency on slower-speed links and to reduce the instances of falsely declaring the tunnel as Down.
- **Deprecated Command** – The **set intervlan-traffic deny** command was deprecated in this release. Use intrazone policies to control traffic between VLANs.
- **VPN Log Messages** – Messages that previously had quoted strings now use single quotes to identify these strings. Some log destinations (such as WebTrends) treated a double quote as a delimiter and truncated log messages.
- **XAuth Users** – If all available IP addresses are used and an Xauth user attempts to establish a tunnel, the NetScreen device logs this event and drops the connection to the Xauth user.

3.3 Changes to Default Behavior in ScreenOS 4.0.1

- **Initial Flow Timer Optimization** – The default value for the initial TCP session timeout has been changed from 60 seconds to 20 seconds. You can adjust this value in 10-second increments through the following CLI command: **set flow initial-timeout** *number*. If a TCP session is not established within the period of time defined, the NetScreen device removes the uncompleted connection request from the table.

- **Source and Destination Default Settings** – The default settings for source and destination SYN flood detection have been changed to a per-platform basis:

| | NetScreen-5XP/XT | NetScreen-25/50 | All Others |
|------------------|------------------|-----------------|------------|
| Same Source | 512 | 1024 | 4000 |
| Same Destination | 1024 | 2048 | 40,000 |

4. Addressed Issues

The following section identifies major bugs that have been fixed in each release of ScreenOS 4.0.3 and in prior releases.

4.1 Addressed Issues in ScreenOS 4.0.3r9

- **05706** – In some cases, DNS entries were updated incorrectly.
- **05510** – Fragmented packets were improperly forwarded through the device.
- **04848** – In an Active/Passive NSRP configuration, failover was not working for L2TP over IPsec VPN connections.
- **04803** – In some cases, a malformed SSH packet caused device failure in an Active/Passive configuration.
- **04595** – When upgrading software in Active/Passive configuration, the primary device failed.
- **04572** – PORT command re-transmission in FTP was handled incorrectly.
- **04544** – Device failure with BGP peer configuration.
- **04340** – (NetScreen-200 Series) In some configurations, the device failed to recycle IKE resources correctly.
- **04229** – The device failed after updates were sent to eBGP peers.
- **04197** – When upgrading software in Active/Passive configuration, the primary device failed.
- **04158** – In an Active/Active NSRP configuration, Track IP did not work on some interfaces.
- **04078** – Deleting a vsys caused device failure.
- **04009** – There was no consistent reference between the standard mib ii if index and a private mib table.
- **03786** – In some configurations, adding an object with long comments from the CLI led to a device failure.

- **03773** – AH authentication failed due to a timing condition between ASIC DES engine and HMAC engine when IPSec AH was used.
- **03643** – Internal NSRP failover process was long, causing device failure.
- **03593** – In some cases, port scan detection was incorrect.
- **03540** – In some situations, the device would experience NFS traffic loss.
- **03524** – The **get dns host cache** CLI command would give a Lookup Successful response, but not return any information.
- **03492** – Customers could not delete messages while accessing Hotmail through Outlook Express when web filtering was enabled.
- **03484** – If an interface repeatedly disconnects and reconnects too quickly, the number of OSPF routes dropped below the number of expected routes causing the OSPF routing instance to clear its route table.
- **03281** – The device failed during incremental SPF calculations.
- **03265** – Under some circumstances, the device stopped sending traffic from some interfaces in an aggregate.
- **03103** – Some registers listed when a device failed were incorrect.
- **03095** – (NetScreen-5XT) When the device auto negotiated its speed and duplex settings with a Cisco 3550, the devices operated properly, but the connection failed when both devices were manually set to 100 Mbps (half-half or full-full).
- **02893** – (NetScreen-500) Sometimes, when heavy traffic transferred across the Fast Ethernet port, the data became corrupted.
- **02798** – (NetScreen-5000 Series systems) Sometimes the device had a redundant buffer when receiving out-of-order fragmented VPN packets.
- **02733** – In some cases, an FTP session timed out prematurely.
- **02664** – Packets were sent out with the MAC address of the inactive Vise instead of the active VSI address in an Active-Active VSI cluster.
- **02618** – SNMP traffic was not sent after remapping the primary interface with SNMP trap traffic present.
- **02562** – A very large configuration caused device failure when the NSRP changed states.
- **02509** – Some FTP sessions would randomly fail related to DNS activity.
- **02498** – (NetScreen-200 Series and NetScreen-500) Link status LED incorrectly indicated link running at 10 Mbps when it was actually running at 100mbps.
- **02409** – Debugging a websense integration issue caused device failure.
- **01897** – Incorrect SNMP call led to device failure.

4.2 Addressed Issues in ScreenOS 4.0.3r8

- **40205** – In certain situations, the NetScreen SSHv1 (SCS) server incorrectly processed data from the client.
- **03129** – When you executed a **get file** command for a file that did not exist, the operation sometimes caused the device to fail.
- **03071** – The WebUI VIP Summary page displayed a blank screen if the Virtual IP (VIP) service was defined for all the VIPs except the first in the list.
- **03053** – In some cases, the return ESP traffic packet through the device could have been sent out with the incorrect source MAC address.
- **03043** – In some situations, the device was unable to respond to large quantities of TCP packets that arrived at the device out of order.
- **02989** – The pipe command could have caused the device to fail while parsing a log message longer than 300 bytes.
- **02898** – An incorrect handling of the internal clock counter could have prevented some ICMP replies from being sent from the device.
- **02855** – Insufficient internal nodes caused the system to display the following message:

WARNING: Insertion in tree failed when free a port.

When this message displayed, some traffic using a specific Dynamic IP (DIP) would fail to pass through the device.

- **02833** – Fragments were sent to a VSI on an active device rather than the active VSI device. These fragments split from the packet after earlier fragments from the packet did. The earlier fragments may have reached the active VSI device.
- **02770** – If the device attempted to process a corrupted message sent by Global PRO the device sometimes failed.
- **02736** – The Mgt-IP on a VSI replied with a virtual MAC address instead of a physical MAC address for the Ident-reset.
- **02730** – 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.
- **02727** – In some cases, when you sent a large number of logs from a device to Global PRO or Security Manager, the device could fail.
- **02710** – Packets would fail to traverse the device when the device inadvertently did not disable the unknown protocol SCREEN option. When this event occurred, the Debug mode displayed the message:

st_ids pak dropped: unknown protocol *number*

- **02604** – Routes exported from a Vsys to the root virtual router were tagged with the incorrect Vsys ID.
- **02588** – The device incorrectly handled TCP options inside of a packet, sometimes causing the device to fail.
- **02551** – An NSRP backup device indicated that a failover occurred continuously when no failure on the primary device occurred.
- **02302** – If you switched from one zone to another zone with a shorter list of address groups on the Address Group page in the WebUI, the device sometimes failed.
- **02047** – When a packet with Ethernet type 0x8888 was received, the device would crash.

4.3 Addressed Issues in ScreenOS 4.0.3r7

- **29343** – Under some circumstances, a NetScreen device sent packets from an incorrect interface.
- **02625** – Event log messages sometimes contained incorrect admin names or IP addresses with incorrect admin names.
- **02605** – When you created a Vsys, both the Vsys and root interfaces incorrectly had the same session token.
- **02362** – After issuing an FTP put command, the control channel and data sessions ended before the amount of time associated with the FTP channel time-out value elapsed.
- **02116** – When the lifetime of a P2 Security Association reached a threshold defined by the soft-lifetime-buffer, this event triggered a P1 rekey and delete notification for a P2 SA is generated after the P1 rekey.
- **01868** – After multiple NSRP failovers, OSPF sometimes learned routes from an inactive Virtual Security Interface (VSI).
- **01793** – A redundant interface learned ARP with no IP address configured.
- **01758** – The DHCP relay agent changed the source IP address of a device in a reply packet to 0.0.0.0 when it responded to a packet the device sent.

4.4 Addressed Issues from ScreenOS 4.0.3r6

This section identifies major bugs that have been fixed in ScreenOS 4.0.3r7:

- **37729** – The NSM RealTime Monitor did not display statistics for a VPN tunnel that terminates on a Vsys.

- **37728** – After configuring 500 tunnels and importing them to NSM, ScreenOS displayed error messages:
 - **Cannot add a list as an argument.**
 - **Cannot set string argument to list.**
 - **Cannot set integer argument to list.**
- **36866** – During an OSPF database update session, an OSPF virtual routing instance sent out superfluous updates for all LSAs generated by the routing instance, even if only one route changed on the device's route table, creating additional overhead.
- **36627** – If the route metric value associated with a route map on a virtual routing instance changed suddenly by a user issuing the **set metric** command, the routing instance may not advertise a redistributed route correctly.
- **36412** – When a Cisco terminal server connected to a NetScreen-500 device in an NSRP environment rebooted, the device failed.
- **36102** – FTP control channel hardware sessions on the NetScreen-5000 systems running TCP 4-way fin enhancement in either NAT or route mode, did not age out properly if you had not issued the following command
 - **set flow hardware close command**
- **32872** – The unnecessary message “time task was blocked but has mail” was removed.
- **25671** – When you issue the **get log sys** command, the output displayed invalid checksum messages for loopback traffic.
- **08168** – After multiple NSRP failovers, an OSPF virtual routing instance learned incorrect route entries when the Virtual Security Device (VSD) changed state.
- **02625** – The device allowed instances of incorrect pairings of administrator names and IP addresses to be logged as event logs.
- **02421** – The device fails when switching in the WebUI to a zone with a number of group names that is less than the number of group names in the previous zone causes the WebUI to display an incorrect list of group names.
- **02340** – A large number of sessions using a policy with counting enabled sometimes caused the device to fail.
- **02322** – With a Securid Server, the device could leak out sockets when you tried a new pin value or go into an indefinite wait state until the connection failed.
- **02238** – The inactive device in an NSRP environment sent log traffic to the syslog server with a sent and received value of 0.

- **02196/02403** – An infinite loop condition in the TCP stack buffer caused the device to fail.
- **02164** – When improperly disconnecting an L2TP tunnel, the device had a memory leak.
- **02155** – When an OSPF routing instance runs on a tunnel interface, the internal timestamp does not work properly at the flow level when indicating elapsed time between the task and flow level, causing the device to fail.
- **02143** – When the device acted as an Autonomous System Border Router (ASBR), it failed to correctly update the type-4 ASBR summary LSA information to other routers in the area during Shortest Path First (SPF) calculation.
- **02141** – A TCP buffer handling session engaged the CPU for too long, causing enough time to elapse so that the watchdog timeout value was exceeded, causing the device to fail.
- **02140** – When the state of a device in an NSRP pair changed a number of times from primary to backup to primary, and so on (a process called “flapping”), the ESP sequence numbers of packets traversing a VPN tunnel on the device became out of synchronization and the peer device responded to the packets as if they were ESP relay packets and dropped them.
- **02120** – ScreenOS did not create the SQL*NET pin hole.
- **02112** – In an instance where a UDP packet fragmented, after the first one that arrived at the NetScreen device, all subsequent fragments contained incorrect Transport layer port numbers.
- **02082** – The device successfully established a VPN in NAT-Traversal mode with an incorrect peer gateway IP address specified for the VPN.
- **02078** – If you defined the same Auth/L2TP user on both the local device user database and a remote Radius server, the device did not release the assigned IP address back to the pool after the user disconnected from the corresponding L2TP/IPSEC connection.
- **02077** – The amount of time associated with the WatchDog Timeout (WDT) variable elapsed on the device forcing the device to fail. The device generates watchdog interrupts at a preset interval. If ScreenOS does not respond to the interrupts within an allotted time, the WDT times out.
- **02010** – (NetScreen-5200) The device incorrectly reported the nsResMemLeft OID value.
- **01955** – Unwanted log messages containing information about TCP head size were removed.
- **01945** – When no sockets were available for an Network Time Protocol (NTP) request, the request went into a looping state, engaging the CPU too long, causing the device to fail.

- **01943** – The device dropped packets larger than 550 bytes that contained DHCP payload information sent from a DHCP server. DHCP payload information includes details like the IP address being assigned to a host, the lease on the address, and the subnet mask value of the address.
- **01936** – When you attempted to establish a ping session with an unreachable host, the session would not naturally end with the prescribed timeout.
- **01934** – SNMP MIB ipNetToMediaTable only reported MAC addresses for physical interface, not the full ARP cache table.
- **01898** – When the device imported an SCS key that is 4,096 bits or longer, the device failed.
- **01895** – The get auth table allowed usernames with more than 40 characters. The table now only allows usernames with 10 characters, the correct character limit for a username.
- **01822** – An inactive Virtual Security Interface (VSI) incorrectly transmitted packets. Inactive interfaces should not be able to send out traffic.
- **01734** – You could not establish a ScreenOS Telnet session or create a WebUI session to the Trust interface on the device. using a Mapped IP (MIP) on a tunnel interface.
- **01626** – The initial session timeout failed when the device received an “ICMP unreachable” message.
- **01612** – When trying to remove a device from the Policy Manager device map, Policy Manager displayed the following error message:
The specified directory name is incorrect. Please try with a correct context and name.
- **01494** – Issuing the **get event | inc packet** command prevented the device from transmitting a Track IP session, causing the device to fail over.
- **01488** – The device failed when it attempts to load an unsupported PKI certificate.
- **00989** – The ScreenOS console continuously displayed an error message related to the TCP_send_task function even when the debug mode was not active.
- **00987** – When you sent ping operations to some interfaces, the interface would send back the MAC address of another interface. This discrepancy caused problems with the default router of the device.
- **00958** – When a packet fragmented in an active-active NSRP environment, a device accepted only the first fragment associated with the packet.
- **00952** – An SNMP reply error incorrectly halted the MIB walker as it traversed the MIB tree.

- **00809** – (5000-8G Management module) The device failed after receiving packets at a throughput rate of 162,000 packets per second.

4.5 Addressed Issues from ScreenOS 4.0.3r5

This section identifies major bugs that have been fixed in ScreenOS 4.0.3r5:

- **01876** – A Cisco terminal server configured with "modem inout" and connected to a NetScreen device sent meaningless/garbage messages. The NetScreen device's echo back and the Cisco terminal server's lack of response to these messages caused a loop on the NetScreen in/out console, blocking processing of other traffic through the NetScreen device.
- **01830** – The NetScreen device enforced a policy check on traffic generated from the device itself, such as SNMP traps and pings. A deny policy from the Trust zone to the destination zone (including a default deny policy) would block such traffic.
- **01827** – Removal of a duplicate entry in the OSPF internal retransmit queue could cause the device to crash.
- **01813** – When SCREEN protection for component-block "EXE" is enabled, CSV extension files were also blocked.
- **01812** – Using uninitialized memory space when creating an outgoing packet could cause the device to crash.
- **01808** – The NetScreen device attempted to match the IKE ID multiple times for certificate-based NAT traversal VPNs, which caused failures in IKE negotiation.
- **01772** – (NetScreen-5200) The session limit threshold count was not decremented on the correct zone for passive FTP or TFTP sessions. This caused false alarms and prevented sessions from being established.
- **01745** – Configuring a large number of tunnel interfaces on the same zone would cause abnormally high CPU utilization.
- **01718** – The GlobalPro agent retrieving VPN information when a VPN was constantly changing its state caused slow management performance. The workaround was to disable GlobalPro on the NetScreen device.
- **01660** – When the NetScreen device was in NAT Traversal mode, the device could crash if no NAT device was detected and a peer sent a payload that the NetScreen device was not able to handle properly.
- **01659** – The GlobalPro agent did not send information for logical interfaces to the Data Collector.
- **01610** – In an NSRP active-active environment, during manual VSD failover the device could incorrectly pick up a route that pointed toward an inactive VSI interface.

- **01556** – Unsetting DNS auto-refresh still caused it to refresh at 00:00. It could not be completely disabled.
- **01523** – (OSPF) If the NetScreen device was performing SPF processing at the time an LSA refresh occurred, some LSAs could be missing.
- **01498** – Connecting to a MIP host while traffic shaping was enabled could cause packets to be dropped.
- **01485** – When the GlobalPro agent task held on to the CPU for more than several seconds, ScreenOS would trigger the error message "sme hold cpu more than X seconds" in the system log.
- **01469** - An information log sent to Report Manager could cause a buffer overflow if it exceeded its allowed length. This, in turn, could cause a crash.
- **01461** – The BGP next-hop selection was not functioning correctly during NSRP failover.
- **01456** – Under certain NSRP failover scenarios, OSPF routes could inadvertently fail to update for the VSI and point to incorrect interfaces.
- **01397** – Multiple reboots of one of the devices in an active-active NSRP cluster could cause many session change messages to be sent over the HA link, which could in turn cause high CPU usage or a system crash.
- **01289** – DHCP Relay did not work in transparent mode when the vlan1 IP address and the managed IP address were not the same.
- **00127** – If a ping from the NetScreen device to an unreachable IP address received an ICMP TTL expired message due to a routing loop, then the Netscreen device would incorrectly interpret this and display a completed ping.
- **36000** – Importing a large configuration file to GlobalPro could exhaust the available memory for the GlobalPro agent, causing the following error message to appear on the console: `get_policy_tbl_name_mib:cannot allocate memory for the list of lists`.
- **35997** – The Netscreen Security Manager was unable to reflect correct OCSP settings after attempting a Refresh CA operation.
- **35662** – When you created a user-defined virtual router with one or more spaces in the virtual router name, ScreenOS did not put quotation marks around the name.
- **35660** – The NetScreen device was unable to extract names (email, IP or FQDN) from the subject alternate name extension of End entity certificates. This caused establishment of IKE security associations for certificate-based VPNs to fail.

4.6 Addressed Issues from ScreenOS 4.0.3r4

This section identifies major bugs that have been fixed in ScreenOS 4.0.3r4:

- **34578** – There were errors in ASN.1 parsing.
- **33745** – The session limit setting did not always work correctly.
- **32858** – If an XAuth user logged in with the correct password after several failed attempts, the NetScreen device might crash.
- **32560** – (WebUI) The default XAuth setting overwrote the bypass-auth option for specific VPN tunnel configurations.
- **32329** – The NetScreen device sometimes sent Real-Time Transport Protocol (RTP) traffic out of order.
- **32235** – It was possible to change the bandwidth of an interface through the WebUI when the NetScreen device was operating in Transparent mode.
- **31880** – When an OSPF neighbor enabled authentication but the NetScreen device did not, the two devices still formed an adjacency.
- **31867** – It was possible to move an interface with a secondary IP address to the Untrust zone.
- **31862** – Enabling and then disabling OSPF for a virtual router containing an unnumbered tunnel interface that borrowed its IP address from a virtual security interface (VSI) caused the NetScreen device in an active/active NSRP configuration to crash.
- **31861** – The NetScreen device did not allow you to create an address book entry with a subnet mask of /30 or /31.
- **31860** – If all the IP addresses in the L2TP IP pool were in use, an L2TP client was allowed to propose and use its own IP address.
- **31855** – (NetScreen-500) When you set the NetScreen device and the switch to which it connects to 100-MB full-duplex and then disconnect and reconnect the cable on the switch, the 100 MB fast ethernet interface became unstable.
- **31854** – (NetScreen-5200) The alarm LED remained red when you turned the second power supply off and on.
- **31851** – When you ran OSPF over two active VSIs on the same NetScreen device, they did not form an adjacency. The two VSIs could not detect each other during the neighbor discovery process.
- **31850** – Internal multicast servers were not able to register to the Internet grid. Packets failed to reach the next hop because the fragments that the NetScreen device sent had the wrong MAC address.

- **31847** – It was not possible to reset the manage IP address to that of the physical IP address using the WebUI. You had to unset the manage IP address through the CLI.
- **31836** – The default Help link was incorrect.
- **31823** – Sometimes the passive device in an NSRP active/passive configuration, erroneously processed ICMP port-unreachable messages.
- **31790** – Addresses NetScreen Security Alert. For details, please see http://www.netscreen.com/services/security/security_notices.jsp.
- **31719** – Under certain conditions, HA messages between the master and backup units sometimes caused CPU usage to increase to 70%.
- **31703** – When logged in through the WebUI and console, clicking **Apply** on the VPNs > L2TP > Default Settings page caused an error message to appear in the console.
- **31679** – The NetScreen device did not apply any changes that were made to the service timeout value for the predefined service Network File System (NFS). Sessions continued to use the default timeout.
- **31673** – When the NetScreen device was processing large amounts of traffic, the message “can’t append, entry already in queue” sometimes appeared in the console.
- **31509** – Enabling all NetScreen-Global PRO options on a NetScreen device configured with a large number of policies caused the CLI to become sluggish in both Telnet and console sessions.
- **31354** – If there were two NSRP clusters in the same network, a NetScreen device in one cluster sometimes accepted traffic sent to the virtual MAC address of the other cluster.
- **31335** – The NetScreen device sometimes sent BGP keepalives at half the configured interval.
- **31126** – (NetScreen-5000) NSRP: When the number of entries in the ARP table on the backup device were not synchronized with those on the master device, the number of sessions were lower on the backup than on the master.
- **31067** – The NetScreen reported differently for an SNMP walk and an SNMP **get** command.
- **31015** – If you logged out from a WebUI management session and then logged in again, the NetScreen device only recorded the first login, not the second or any subsequent logins.
- **30997** – TCP sockets sometimes failed to close after management connections to the NetScreen device terminated.
- **30728** – If you enabled counting in a policy, the counter sometimes increased unceasingly until the system crashed.

- **30721** – In some cases, a NetScreen device with virtual systems that was in an NSRP configuration sent system critical messages with VLAN tags instead of sending them from the root system.
- **30701** – The NetScreen device failed to log traffic when logging was enabled in a policy referencing a dialup VPN tunnel.
- **30680** – Incorrect socket processing occasionally caused the NetScreen device to crash.
- **30668** – Enabling URL filtering and the ALG reassembly option caused some legitimate sites to become unreachable to HTTP traffic.
- **30581** – When the manage IP address was different from the interface IP address for the interface connecting to a SecurID server, the NetScreen device erroneously sent the node secret from the interface IP address instead of from the manage IP address.
- **30570** – The message “Unexpected error: 501 5.5.4 Invalid Address” erroneously appeared in the console.
- **30332** – When a dedicated MGT port on a NetScreen device was connected to a network forwarding device such as a switch and both devices were configured to negotiate half- or full-duplex mode automatically, the mode chosen was half-duplex instead of full-duplex.
- **30299** – A NetScreen device in Transparent mode with the malicious URL SCREEN option configured dropped HTTP traffic with destination port 8080, regardless of the URL.
- **30033** – If an XAuth user whose user account was stored on an external RADIUS server submitted an incorrect user name and the policy enforcing authentication specifically referenced that user or user group (not “any”), the NetScreen device forwarded the login information to the RADIUS server instead of dropping it.
- **29987** – The NetScreen-Global PRO Report Manager erroneously classified the IKE message reporting that the NetScreen device had received a bad SPI as an attack alarm.
- **29906** – Traffic generated from the NetScreen device itself first matched a global policy instead of an interzone policy.
- **29821, 26138** – Enabling NetScreen-Global PRO caused several erroneous messages to appear in the console.
- **29709** – Loading a digital certificate with an unsupported SubjectAltName caused the NetScreen device to crash.
- **29649** – The monitoring device in a redundant VPN gateway configuration sometimes used the SPI for one VPN tunnel when responding to ICMP echo requests sent through a different tunnel.

- **29586** – When an HTTPS window closed abruptly, the NetScreen device did not correctly close sockets.
- **29578** – NSRP: The NetScreen device used the physical MAC address instead of the virtual MAC address in the sender-mac field in ARP request packets.
- **29555** – When performing URL filtering and the URL was exceptionally long, the NetScreen device dropped the packet instead of forwarding it to the Websense server.
- **29465** – When a NetScreen-Remote client was using a virtual adapter, the NetScreen device required the XAuth user to log in again.
- **29404** – In some cases, the NetScreen-Remote client displayed a malformed packet message when trying to connect to a NetScreen device using XAuth.
- **29386** – The NetScreen device sometimes failed to release pseudo ports when sessions ended. This caused address allocation problems when attempting to draw them from dynamic IP (DIP) pools.
- **29212** – The NetScreen device did not detect a Land attack if the source IP address was the same as the translated host IP address of a MIP.
- **28997** – The NetScreen device sometimes failed to clear TCP sockets for terminated connections.
- **28966** – The HA1 and HA2 out-byte counters were erroneously high.
- **28949** – When performing URL filtering and the NetScreen device received HTTP POST and HTTP continuation packets, it forwarded the first packet (HTTP POST) to the Websense server, but allowed the second packet (HTTP continuation) to pass.
- **28787** – When you loaded ScreenOS 4.0.3r3, the console displayed the message “failed to start RU”.
- **28677** – The NetScreen device rejected duplicate default routes learned through dynamic routing protocols.
- **28640** – If the ID number of a user group was longer than three digits, the **get user-group all** command displayed the wrong ID number.
- **28512** – The NetScreen device advertised a default route even when there was an existing default route learned from OSPF. Now, OSPF checks for default routes, and if it finds one, it advertises the default route from OSPF.
- **28429** – The NetScreen device did not advertise routes to networks connected to secondary interfaces even if OSPF was enabled on the main interface.
- **28194** – Putting a NetScreen device in FIPS mode when there were multiple outbound policies referencing the same VPN tunnel caused the device to stop functioning.

- **28188** – Under certain conditions, ScreenOS might have damaged supported Sandisk flash cards.
- **28126** – If the SSH session terminated while saving a configuration to a TFTP server, the process of saving the configuration continued indefinitely.
- **27985** – SNMP notifications in the event log did not display correct port numbers.
- **27951** – NSRP: In certain conditions, the backup unit—instead of the master unit—in an active/passive NSRP configuration sent syslog and SNMP traffic through VPN tunnels.
- **27918** – Using the WebUI to set an NSRP secondary link caused the illuminated HA LED to become dark.
- **27864** – When Open Shortest Path First (OSPF) was enabled on the virtual security interface (VSI) of a NetScreen device in an NSRP configuration and after the OSPF database had been refreshed, the NetScreen device did not send some routes to its neighbors.
- **27144** – NSRP: When you created an auth user or user group, the master device passed a different hash password to the backup device.
- **27127** – A NetScreen device in Transparent mode erroneously generated gratuitous ARP packets when an interface was moved to the Null zone.
- **27105** – Under certain conditions, the system clock shifted 58 seconds back, causing problems with OSPF.
- **27069** – NSRP: The backup device sometimes propagated the wrong MAC address to the master device.
- **27019** – Adding a device to an NSRP cluster caused all interfaces set in 100-MB full-duplex mode to stop functioning.
- **26954** – NSRP: Although DNS sessions aged out on the master unit in an active/passive NSRP configuration, they did not always age out on the backup unit.
- **26915** – NSRP: After the failover of a NetScreen device running in Transparent mode, the new master stopped forwarding VLAN-tagged traffic in existing sessions.
- **26907** – The SSH messages included non-ASCII text that some SNMP browsers, such as HP OpenView, were unable to decode.
- **26884** – When the NetScreen device was in Transparent mode, ICMP traffic caused unnecessarily high CPU utilization.
- **26845** – After the NetScreen device booted up, the initial DNS lookup occasionally failed.

- **26802** – If you defined a name for a route map that used part of the name of a previously defined route map—such as “rtmap100” and then “rtmap1”, it was not possible to delete the second route map (“rtmap1”) until you had deleted the first one (“rtmap100”).
- **26790** – The NetScreen device did not block .exe files from Microsoft Internet Information Servers (IIS).
- **26786** – The NetScreen device erroneously updated the proxy ID after an admin entered the **set flow vpn-untrust-mip** command, edited a policy, and then reset the device.
- **26770** – Telnet access became unnecessarily slow when CPU utilization increased.
- **26725** – If a vsys shared the Untrust zone with the root system and there was at least one Untrust zone address group configured at the root level, any Untrust zone address groups configured at the vsys level were not available as options when configuring vsys-level policies.
- **26718** – When a NetScreen device was in FIPS mode, it failed to load policies whose action was “deny”.
- **26688** – A new dialup VPN connection from one XAuth user sometimes caused the NetScreen device to disconnect other XAuth users.
- **26653** – When a large number of VPN tunnels renegotiated at the same time, the NetScreen device dropped some active security associations (SAs) because the soft-lifetime buffer expired.
- **26633** – The IP spoof protection feature occasionally treated valid packets as spoofed.
- **26620** – When an auth user initiated an HTTP connection and URL filtering was enabled, the NetScreen device displayed the message “Page Not Found”, even if the Websense server had approved the destination.
- **26598** – Incorrect messages sometimes appeared in the event log regarding the rekey option, which is an element of the VPN monitoring feature.
- **26572** – When VPN monitoring with the rekey option was enabled, duplicate messages indicating that the status had changed from up to down appeared in the event log.
- **26529**– The error message “system-error: no cb is found for peer” sometimes appeared in the event log.
- **26520** – When you made a static ARP entry on the NetScreen device, it did not reply to ARP requests.
- **26501** – When you used both iBGP and eBGP, the NetScreen device did not use the eBGP local preference for BGP path selection. If the eBGP local preference was set higher than the iBGP preference, the NetScreen device still used the iBGP routes.

- **26489** –The NetScreen device did not pass IS-IS routing updates.
- **26478** – FTP data sessions failed when the ARP entry aged out before the FTP control session ended.
- **26444** – (NetScreen-5200) In some cases, traffic between DNS servers failed due to a session timing issue.
- **26417** – In certain conditions, incorrectly processing IKE negotiations caused the NetScreen device to crash.
- **26408** – The NetScreen device crashed if the internal tunnel information became invalid.
- **26377** – The NetScreen device built a VPN tunnel with NAT-Traversal even if the peer gateway IP address was incorrect.
- **26350** – It was not possible to manage a Nortel Optera Metro optical switch through the NetScreen device.
- **26194** – The NetScreen device allowed the number of sessions to exceed the destination-IP-based session threshold.
- **26145** – The NetScreen device was unable to send fragmented OSPF packets through a VPN tunnel.
- **26110** – The NetScreen device received ICMP echo requests sent to a virtual security interface (VSI) on the wrong interface and sent back ICMP echo replies with the wrong MAC address.
- **26104** – The NetScreen device was unable to forward Network File System (NFS) traffic when in an NSRP active/active configuration.
- **25877** – Modifying the OSPF hello interval did not automatically increase the dead interval to a value four times greater than the new hello interval.
- **25807** – The BGP send-community did not work when the NetScreen device learned the route from a peer.
- **25603** – When the NetScreen device received data from a non-NetScreen device in response to an authentication request, the console displayed an alert message.
- **25510** – The untrust-vr did not send an OSPF summary route update to its neighbor after the link went down then came up again.
- **25411** – ScreenOS permitted you to set an address group ID of 0, which produced erroneous output for the **get user-group all** command. An address group ID must be between 1 and 65,535.
- **25123** – It was not possible to create a service group after the maximum number of custom services was reached.
- **25021** – The number of entries in the traffic log differed between the local traffic log and the traffic log sent via e-mail.

- **24627** – Only an authentication user was allowed in multiple groups.

4.7 Addressed Issues from ScreenOS 4.0.3r3

This section identifies a major bug that was fixed in this release:

- **28406** – In some cases, the NetScreen device rebooted because the TCP options may have started at odd address boundaries.

4.8 Addressed Issues from ScreenOS 4.0.3r2

This section identifies major bugs that have been fixed in ScreenOS 4.0.3r2:

- **27123** – The NetScreen device dropped traffic that it erroneously identified as having spoofed source IP addresses.
- **26762** – Enabling Websense URL filtering caused the NetScreen device to enable the lightweight TCP reassembly feature for ALGs. This resulted in several problems, such as the inability to access a mail accounts across the NetScreen device.
- **26633** – When the NetScreen device was in an Active/Active configuration, it dropped NSRP packets that it erroneously identified as having spoofed source IP addresses.

4.9 Addressed Issues from Prior Releases

This section identifies major bugs that have been fixed in releases after ScreenOS 4.0.0.

- **25679** – When the redundant power supply was powered on, the alarm LED did not clear.
- **25500** – The DHCP server CLI command did not save quotes for the name.
- **25461** – In some cases, when fragmented packets passed through a VPN they did not retain the proper VSD pointer.
- **25451** – NAT-Traversal VPNs would fail when the **set interface vlan1 ip manageable** option was not set.
- **25407** – H.245 translate failed or stopped after a few calls using IP phones.
- **25344** – Some syslog message for H.323 were incorrect.
- **25315** – (WebUI) You could not select an address group in the untrust zone in a VSYS.
- **25283** – The NetScreen-204 did not auto-sense (MDI/MDI-X) properly on the following interfaces: ethernet2, ethernet3, and ethernet4.

- **25256** – In some instances the NetScreen device would crash when getting an address from the DHCP Server.
- **25198** – The NetScreen device would freeze when you used the “@” or “\$” characters in the admin password.
- **25151** – You could not set a policy for layer-2 zones if at least one zone did not have an interface bound to it
- **25139** – Redistribution of BGP routes to OSPF by matching the community failed. Therefore matching any routes with BGP attributes would fail.
- **25117** – If the TCP data length was larger than the IP length, the console would display the following message: “###invalid size when invalidate cache”.
- **25110** – When a root-level admin set a service timeout, this was not propagated to the individual VSYS.
- **25106** – When you executed the command **set interface untrust dhcp-client settings update-dhcpserver**, the NetScreen device did not save it in the configuration file.
- **25078** – The NetScreen device sent BGP keepalives at half the configured intervals.
- **25075** – When you configured a route-based VPN, firewall authentication did not work.
- **25066** – Bidirectional dial-up VPN policies would fail if the remote client’s IP address changed.
- **25064** – The DIP port manager memory size has been increased to support the entire DIP pool.
- **25024** – You could not configure an interface with an IP address if the last octet was 0.
- **25018** – There was a discrepancy between the number of traffic logs generated internally and the number of logs generated via e-mail.
- **25015** – Disabling OSPF on the Trust-VR caused the NetScreen device to reboot.
- **25004** – If the first packet over a VPN was fragmented, a session was not created and would fail to match the VPN policy.
- **24999** – NetScreen devices in an NSRP cluster were unable to synchronize configurations when NSRP encryption or authentication was configured.
- **24982** – The NetScreen device was not able to communicate with Report Manager 4.0.0r2.
- **24980** – Changing the address book configuration in the WebUI generated a different log report from the one generated by making the same change through the CLI.

- **24979** – When you created an address book or address group, the device logged the event differently depending on whether you used the WebUI or the CLI.
- **24961** – (NetScreen-5XP/5XT) Addresses NetScreen Security Alert 56305. For details, please see [http:// www.netscreen.com/services/security/security_notices.jsp](http://www.netscreen.com/services/security/security_notices.jsp).
- **24958** – (NetScreen-5XP/5XT) While under heavy load, on rare occasions, the device would revert to factory settings.
- **24954, 24633** – (NetScreen-5XP/5XT) The device did not save the **set/unset interface untrust dhcp-client settings update-dhcpserver** command in the configuration file.
- **24938** – (WebUI) There were problems configuring groups in a policy.
- **24921** – When the PPPoE connection of the device went down, the default route remained active. This was anomalous behavior.
- **24912** – Policy Manager was unable to read the VPN configuration settings of a device because the device added double quotes when it stored these settings.
- **24893** – The device would drop traffic to a zone with redundant interfaces when traffic shaping was configured in a policy.
- **24888** – There were problems generating a PKI Certificate from an IBM360 using PKCS10 file format
- **24880** – The SQLNET V2 secondary data channels could not be created
- **24859** – (NS5200) The device would update the counter statistics on the WebUI only when you entered the command **get counter stat** on the CLI.
- **24839** – (NS5200) Packets with L2TP type signatures created multiple sessions.
- **24819** –When Report Manager responded to a NetScreen device, it displayed information in clear text.
- **24715** – The NetScreen device failed to connect to the PPPoE server after the **set pppoe static-ip** command was issued.
- **24693** – A NetScreen device in an NSRP cluster would report a PKI synchronization error, even though the synchronization was successful.
- **24673** – Occasionally, multicast traffic unnecessarily increased CPU utilization to 70%.
- **24642** – A device running OSPF would stop advertising default routes, if other routes were withdrawn.
- **24624** – Large FTP downloads - typically larger than 25 megabytes of data - failed

- **24605** – You could not manage the NetScreen device using the WebUI via PPPoE.
- **24601** – IPSec reassembled packets were sent with the incorrect IP header checksum.
- **24597** – Traceroute via UDP displayed the IP address of the untrust interface twice instead of displaying the IP address of the untrust interface as a hop, then the host MIP address as the final end point.
- **24591** – The device did not store the physical interface settings on aggregate ports in the configuration file. Therefore these settings were not retained after the device was reset.
- **24545** – The NetScreen device did not update the SNMP MIB statistics for packet and octet counters.
- **24515** – You could not edit a service name with Korean characters.
- **24468** – The online help file was not pointing to the correct location.
- **24458** – (WebUI) You could not view statistics from aggregate ports.
- **24451** – (NetScreen-50) The alarm LED light did not turn off when you issued the **clear led alarm** command.
- **24449** – Attempting to create a new policy via the WebUI caused the NetScreen to reboot.
- **24443** – (NetScreen-5XP) The device rebooted every 24 hours because a pointer in the session table was not reset.
- **24442** – You could not establish an IKE dial-ip VPN if the protocol was not set to ANY.
- **24430** – When a NetScreen device was configured as a DHCP server, performance suffered due to issues with Macintosh DHCP clients.
- **24406** – (NetScreen-5200) The device would reboot after the MAC learning table was cleared and there was a UDP packet stream flowing.
- **24401** – The firewall attack LED erroneously turned green after the system booted up.
- **24392** – (NetScreen-5200) There were multiple aggregate interface issues.
- **24338** – The device sent e-mail notifications for “critical” events, even if this severity level was not selected in the Log Settings section of the WebUI.
- **24323** – (WebUI) The pre-defined service page was not complete, and some custom services did not appear.
- **24322** – (NetScreen 5XP/5XT) The user limit did not account for incoming traffic on a device in transparent mode.

- **24319** – (WebUI) When you used the WebUI to define a policy that specified a VPN Group and authentication, the device would not save the policy with the authentication option.
- **24307**– OSPF did not advertise networks defined on a secondary interface.
- **24284** – Addresses CERT VU#412115: Network device drivers reused old frame buffer data to pad packets.
- **24283** – (Addresses CERT VU#412115) Network device drivers reused old frame buffer data to pad packets.
- **24278** – With NAT traversal, after the IKE Phase 2 lifetime expired, the NetScreen device stopped sending keepalive packets which were required by the NAT device to keep a session alive. This caused the session to end and the NetScreen device to negotiate a new IKE Phase 1 SA when the client tried to establish a new Phase 2 SA.
- **24263** – (WebUI) Log viewer message for DNS lookup included the message “DNS lookup time has been changed to start at <hour:minute> with an interval of <number> hours”.
- **24262** – You could release the DHCP lease from the CLI only.
- **24257**– (WebUI) If you enabled PPPoE on the untrust interface, then tried to configure a static IP address on that interface, the PPPoE settings remained enabled and could not be disabled.
- **24243** – BGP advertised all reachable routes, including the default route. A route was advertised via BGP if it had reachability by any means including the default route. Now, only routes that have an exact match in the routing table are advertised.
- **24226** – The NetScreen device rebooted when there was a high number of PKI certificate-based VPN tunnels.
- **24217** – When the NetScreen device tried to connect to an SQL server using a non-MIP address, the return packet used the MIP IP instead of the untrust IP, causing an SQL connection failure.
- **24208** – PPPoE login failed due to the PPP server if the ISP side tried to renegotiate the LCP once the NetScreen LCP was up.
- **24196** – Internal multicast servers were not registering to the Internet grid. Root cause was fragments in the reverse order were being sent with the incorrect MAC header, and failing to reach the next hop.
- **24193** – (NS5200) Management of the NetScreen device was slow if the number of sessions exceeded 600,000.
- **24178** – When the trust interface of the NetScreen device was in NAT mode, access to Oracle resulted in a core dump.

- **24176** – Frequently reordering policies within a large policy set sometimes caused policies to be deleted and the NetScreen device to reboot.
- **24158** – When a device is in transparent mode, the VLAN1 interface is bound by default to the MGT zone. When you initiated management traffic from the device, it would use the wrong source IP address - 192.168.1.1.
- **24132** – When you entered the command **set admin name** <string> in the CLI, the NetScreen device erroneously stored the command in the configuration file as **set admin vsys name** <string>. This caused the device to display an error message after you rebooted.
- **24116** – After the device connected to NetScreen-Global PRO, the event log showed that the config was saved from host <random ip address>.
- **24073** – The DHCP status report did not update the lease time countdown for allocated IP addresses.
- **24069** – (NetScreen-25) It was not possible to clear sessions when the drop-unknown-mac SYN flood option was enabled.
- **24053** – If the default auth server for L2TP was configured as a RADIUS server, and you tried changing the default auth server to “Local”, the WebUI reported an error and did not allow you to change the default auth server to “Local”.
- **24028** – You could not add a static route if the interface was bound to a zone that was not in the trust-vr.
- **24012** – Firewall and VPN performance numbers did not match the specifications for the NetScreen-50.
- **23990** – It was not possible to configure a route metric for a tunnel interface through the WebUI.
- **23957** – (WebUI) You could not use the “/” character.
- **23955** – Firewall authentication using an external RADIUS authentication server did not work properly after upgrading to ScreenOS 4.0.0r8.
- **23932** – The NAT-Traversal UDP checksum was incorrect, which caused any NAT device in the data path to drop encapsulated packets and thus block VPN traffic.
- **23917** – (NetScreen-5XP) When adding users to a user group through the CLI, you could add up to 80 user entries per group; however, the maximum limit is 32.
- **23909** – Editing a BGP peer from the WebUI caused a flow of registry information, known as a trace dump, to appear in the console.

- **23815** – (CLI) If you configured a policy referencing an L2TP-over-IPSec tunnel that used an IKE ID that was already used in an L2TP-over-IPSec tunnel referenced in another policy, the NetScreen device rejected the policy upon device reboot.
- **23809** – When operating in an NSRP cluster, the ipAddTable MIB variables sent by the master and backup devices were not different, as is required by HP OpenView.
- **23807** – When acting as a DHCP server, the NetScreen-5XT did not offer IP addresses in the “siaddr” portion of the DHCP offer packet, and consequently failed to allocate IP addresses.
- **23791** – When you tried to authenticate yourself using WebAuth, the device performed a core dump and displayed the following message on the console: “ewsResume: bad scheduling state”.
- **23783** – A UDP traceroute to a MIP revealed the internal private address as a hop.
- **23778** – URL filtering did not work properly when a proxy server was used in conjunction with a Websense server in the DMZ zone.
- **23774** – When two virtual systems had overlapping subnets, the NetScreen device sometimes responded to ARP requests with a MAC address from the wrong vsys.
- **23773** – (NetScreen-204/208) The DHCP client on ethernet1 bound to the Untrust zone was unable to obtain an IP address from its ISP.
- **23772** – NetScreen-5200: It was not possible to manage the passive device in an NSRP active/passive pair via the manage-ip.
- **23743** – It was not possible to add a custom service to a virtual IP (VIP) address.
- **23686** – When the NetScreen-5200 was in Transparent mode, the SYN flood protection counter did not function properly.
- **23684** – The default Help link in ScreenOS 4.0.0r7 pointed to the wrong URL.
- **23639** – The output of the **get global-pro proto-dist table { bytes | packets }** command did not display protocol distribution counters for NetScreen devices in Transparent mode.
- **23626** – The backup device in an active/passive NSRP cluster erroneously sent an empty traffic log to a syslog server.
- **23615** – (Telnet) If you performed a traceroute operation, disconnected before the operation completed, opened a new session, and tried to perform another traceroute, an error message appeared stating that a traceroute was already in progress.

- **23609** – Addresses NetScreen Security Alert 51897. For details, please see [http:// www.netscreen.com/services/security/security_notices.jsp](http://www.netscreen.com/services/security/security_notices.jsp).
- **23601** – From 60 seconds after bootup, a NetScreen device displayed the average system utilization continuously and erroneously as 1%.
- **23599** – Although the NetScreen-5200 successfully passed ICMP traffic through VPN tunnels between virtual systems if both vsys shared the Untrust zone, it dropped TCP and UDP packets sent through intervsys VPN tunnels.
- **23570** – Addresses NetScreen Security Alert 52020. For details, please see [http:// www.netscreen.com/services/security/security_notices.jsp](http://www.netscreen.com/services/security/security_notices.jsp).
- **23557** – PPPoE: Changing the IP address caused VPN tunnel failures because IKE peers continued to use the old IP address.
- **23553** – It was not possible to load the NetScreen SNMP MIB files in HP OpenView because of a syntax error.
- **23526** – NSRP: When a master with the preempt option enabled rebooted, it did not synchronize ESP sequence numbers, which resulted in VPN failures.
- **23511** – The DiffServ codepoint marking option for traffic shaping did not appear in the WebUI.
- **23497** – The XAuth lifetime did not refresh after a Phase 1 rekey occurred.
- **23494** – When run-time user authentication was enabled, the NetScreen device created entries in the session table for RESET replies to connection requests for services other than FTP, HTTP, and Telnet, instead of simply dropping the packets.
- **23452** – After rebooting the backup device in an NSRP cluster, the master was unable to synchronize all security associations (SAs) with the backup if the number of SAs exceeded 1500.
- **23443** – You could not use a space in a VPN group name because the configuration file did not add quotation marks around the name. Consequently, the space was treated as a delimiter.
- **23422** – It was not possible to save a large configuration from an external location to flash memory using the WebUI.
- **23397**– H.323 calls failed when passing through a VPN using a MIP.
- **23395** – (NetScreen-5200) It was not possible to set a secondary path for NSRP heartbeats.
- **23392** – It was not always possible to use the manage IP address to manage a NetScreen device through a VPN tunnel.

- **23358** – The maximum number of service groups was set lower than in previous ScreenOS releases. After upgrading from a previous release in which the maximum number of service groups had been configured, the NetScreen device rejected service groups that exceeded the new maximum settings.
- **23339, 23415** – When the NetScreen-500 is the master in an HA configuration and you manually force it to fail over, the link status for any interface set for full-duplex (100 Mbps) toggles erratically.
- **23334** – Session timeouts became unstable when there was a large number of concurrent UDP, Telnet, and HTTP sessions.
- **23328** – NetScreen-5200: Setting the timeout value of a service as “never” did not work properly; the service still timed out at its default setting.
- **23313** – The DHCP client module on the NetScreen-5XP did not properly renew its IP address lease.
- **23266** – When a NetScreen device operating in Transparent mode received fragmented UDP packets, they occasionally became corrupted and were dropped.
- **23240** – After the time change caused by Daylight Saving Time, timestamps on traffic log entries were one hour off, although the system clock was correct.
- **22970** – If you rebooted a NetScreen device and then cleared the DNS cache, there sometimes was a delay of up to one minute for IKE negotiations to complete if the remote IKE gateway configuration used an FQDN.
- **22968** – When you created a policy for a LAN-to-LAN VPN tunnel referencing a service group, the WebUI erroneously displayed the following warning message: “Warning: Service group selected, IKE will negotiate a tunnel for all IP”.
- **22934** – The text that appeared after typing **set zone v1-<name> screen ip-spoofing ?** erroneously related to IP spoofing at Layer 3 as opposed to Layer 2.
- **22690** – The device erroneously allowed you to bind a redundant interface to the MGT zone. You can bind only physical interfaces to the MGT zone.

5. Known Issues

This section describes known issues with the current release.

- [Section 5.1 “Limitations of Features in ScreenOS 4.0”](#) 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 5.2.1 “Compatibility Issues in ScreenOS 4.0 on page 38](#) 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 4.0 on page 41](#) 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 4.0

The following limitations are present in ScreenOS 4.0.

- **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.
- **SCS Connection to SSH Client** - The NetScreen SCS utility has issues with the client from SSH Communication Security.
W/A: Use a different SSH version 1 client, such as OpenSSH.
- **Dynamic Routing Unsupported** - The NetScreen-5XP does not support dynamic routing.

5.2 Compatibility Issues

The following sections detail compatibility issues in the current and previous releases.

5.2.1 Compatibility Issues in ScreenOS 4.0

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 4.0 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 4.0:

set ike initiator-set-commit

set ike responder-set-commit

set ike initial-contact

WA: Unset these commands to ensure compatible configuration on the NetScreen device.

- **Compatible Web Browsers** – The WebUI for ScreenOS 4.0 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.0 and 5.5, 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, might result in erroneous behavior.
- **AES Settings** – Predefined IPsec Phase 1 and Phase 2 proposals using the American Encryption Standard (AES) only use AES128. If you want to use AES192 or AES256, you must create your own proposals.
- **AES Interoperability with Pre-ScreenOS 4.0.0 Release** – If two IKE peers—one running ScreenOS 4.0 and the other running a previous version of ScreenOS—attempt Phase 1 negotiations with AES as the encryption algorithm, interoperability problems can result.

5.2.2 Upgrade Paths from Previous Releases

The following previous releases of ScreenOS support direct upgrades to ScreenOS 4.0.

| Model | Most Recent Version | Upgrade to 4.0 Supported |
|-------------------|----------------------------|------------------------------------|
| NetScreen-5XP | 3.0.3r1 | Yes |
| NetScreen-5XT | 3.0.3r1 | Yes |
| NetScreen-25/50 | 3.0.3r1 | Yes |
| NetScreen-204/208 | 3.1.0r7 | Yes, with High Availability issues |
| NetScreen-500 | 2.7.1r5, 3.0.3r1, 3.1.0r7 | Yes, with High Availability issues |
| NetScreen-5200 | 3.1.0r1 | Yes, with High Availability issues |

NetScreen-500 Limitation: ScreenOS 4.0 supports direct upgrades on the NetScreen-500 from versions of ScreenOS 2.7.1r5 and later. To upgrade from a supported previous release of ScreenOS to ScreenOS 4.0, you need to first make sure you have successfully upgraded to ScreenOS 2.7.1r5 or later and then perform the recommended upgrade procedure to ScreenOS 4.0.

5.2.3 Migrating NSRPv1 to NSRPv2

Upon completing the upgrade procedure, you will still have an Active/Passive configuration, but you will now be able migrate to an Active/Active environment on the NetScreen-200, NetScreen-500, and NetScreen-5200 devices. To install your new software for a High Availability device pair, perform the following procedure.

Note: *Upgrading a High Availability device pair to ScreenOS 4.0 is disruptive to user traffic and should be scheduled in advance.*

1. Back up the current configuration files of both devices to .cfg files.
2. Disconnect the backup device from the network.
3. Upgrade the ScreenOS version on the backup device to ScreenOS 4.0.0.
4. Verify the configuration of the device.
5. Remove the master device from the network and replace it with the newly upgraded device.
6. Reset the newly installed device. When it boots, it becomes the new master.
7. Upgrade the ScreenOS version on the original master (now disconnected from the network) to ScreenOS 4.0.
8. Verify the configuration on this device.
9. Reinstall the device onto the network. It becomes the backup.
10. Type the CLI command **exec nsrp sync global checksum** to verify your newly upgraded devices synchronized correctly.

NetScreen recommends you back up existing configuration files prior to upgrading to a new version of ScreenOS. If you decide you want to install an earlier version of ScreenOS onto your device, you need this configuration file.

To save the configuration file from the CLI, you need either a flash memory card installed in your NetScreen device or Trivial File Transfer Protocol (TFTP) server software running on the PC connected to the management and console ports.

- To save the configuration file to a flash memory card, issue the CLI command **save config to slot** using a specified slot number and filename as arguments, for example:

save config to slot1 backup.cfg

- To save the configuration file to a TFTP server, issue the CLI command **save config to tftp** using a specified TFTP server IP address and filename as arguments, for example

save config to tftp 10.247.2.1 backup.cfg

Remember to save the filename in Microsoft MS DOS 8.3 format with a proper extension.

5.3 Known Issues in ScreenOS 4.0

The following are known deficiencies in features at the time of this release. Whenever possible, a workaround 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 4.0.3r9

None.

5.3.2 Known Issues in ScreenOS 4.0.3r8

- **41016** – When removing one IP pool entry from the WebUI, another one will inadvertently disappear also even though the entry is still visible from the CLI.

5.3.3 Known Issues in ScreenOS 4.0.3r7

None.

5.3.4 Known Issues from ScreenOS 4.0.3r6

- **02008** – After running the command **unset log module** for the syslog, the set syslog config setting disappeared after rebooting the device.
- **01928** – When you attempted to create an address group where you selected a custom zone that had a name with a character space in the string, the WebUI session would freeze.

5.3.5 Known Issues from ScreenOS 4.0.3r5

- **01856** – The NetScreen device does not include TCP/UDP port information in traffics log inside "email alert" mails.
- **01846** – If you use the CLI to create a custom service without specifying a source port, the default source port is 0-0. In the WebUI, the default ports are 0-65535 for both source and destination ports.

W/A: Specify the desired ports when defining a custom service, or upgrade to ScreenOS 5.0.

- **01845** – When an IP address on an interface is changed, all routes in the routing table that reference the modified interface are deleted.

W/A: Upgrade to ScreenOS 5.0

- **01796** – When NetScreen devices that are configured for NSRP receive packets with MAC addresses for another virtual MAC address, the packets are forwarded instead being dropped
- **01779** – When the NetScreen device is configured for NSRP active-active, both VSDs are active on the same unit, and the track-IP interface is configured as auto, track-IP may fail.

W/A: Define the track-IP interface instead of specifying auto.

- **01758** – When the NetScreen device acts as a DHCP-relay agent, the source IP address in the forwarded message is changed to 0.0.0.0, which causes some DHCP clients to reject the DHCP message.

W/A: Assign a static IP address for a DHCP client that rejected the DHCP message.

- **01746** – The NetScreen alarm log lists each ICMP fragment individually instead of summarizing them into one log entry.

5.3.6 Known Issues from ScreenOS 4.0.3r4

- **35660** – The NetScreen device cannot establish a VPN tunnel with certificates that use the SubAltName extension.
- **32593** – It is not possible to change the dynamic port timeout interval for the Oracle SQL*Net V2 service.
- **31007** – Any attempt to access a MIP via a dialup VPN tunnel may fail.

W/A: For MIP access in this circumstance, use a tunnel interface.

- **30971** – When an admin user logs in with all privileges, each logged event incorrectly indicates that the user has read-only privilege.
- **30710** – When two NetScreen devices work in an HA link, and the devices use manual keys, changing the VPN gateway IP address on the primary device does not automatically propagate to the backup device.

W/A: Execute the CLI command **save config ha-master** on the backup device and perform a restart.

- **30696** – IP-spoofing protection counters do not work for the Trust zone on the NetScreen-5XT platform.

- **30577** – When two NetScreen devices run in an Active/Passive HA link, frequent execution of scripts from a console application (such as Telnet) might cause the devices to switch master/backup status.
- **30150** – DHCP Relay does not work when the device is in transparent mode, and the vlan1 IP address is not identical to the manage IP address.
- **30145** – Attempts to perform a FTP download of any file 1 gigabyte or larger through a VPN tunnel may fail.
- **29780** – If your system uses a hub-and-spoke topology, and you perform a ScreenOS upgrade from version 3.0.3 to version 4.0.x, tunnel interfaces that have DIP settings no longer work.
- **27049** – When a VPN policy is currently in use, and you use the WebUI to change the addresses used by that policy, the change has no effect. The WebUI does not present an error prompt.
- **26739** – When there are redundant entries in a VPN group, and the designated gateway on the high-priority peer device changes to an inoperative or nonexistent gateway, failover to another device does not occur.
- **26669** – If you restart a NetScreen device, having previously executed the following command has no effect, even if you executed **save** before restarting:

unset log module name_str level alert destination syslog

- **26484** – Setting up an FTP session causes the device to generate extra traffic log messages.
- **26472** – When an interface shuts down, BGP does not automatically remove any static or connected route associated with that interface.
- **26450** – Use of the “+” character for an object name (such as a zone name) is not supported.
- **01830** – The NetScreen device enforces a policy check on traffic generated from the device itself, such as SNMP traps and pings. If there is a user-defined policy denying traffic from the Trust zone to the destination zone of the self-initiated traffic, it blocks that traffic.

W/A: Add a policy permitting traffic from the Trust zone to the destination zone above the policy denying it.

5.3.7 Known Issues from ScreenOS 4.0.3r3

- Documentation and WebUI - Services definitions in ScreenOS have one or more destination ports or port ranges, and one or more source ports or source port ranges. There is no consistency in the source port definitions. Some are defined with source port ranges of 0-65535; others are defined with a range 1-65535. Many services are defined with a source port range starting at port 1024. Current documentation and the WebUI do not list the predefined services and their source ports.

W/A: Use the CLI command **get service** to list the predefined and custom services and their source ports.

5.3.8 Known Issues from ScreenOS 4.0.3r2

- **26090** – IP spoof protection does not work for traffic received on VLAN-tagged subinterfaces.
- **28201** – Enabling the TCP reassembly feature for ALGs (application-layer gateways) may cause problems when the NetScreen ALGs process HTTP or FTP traffic with protocol data units that are more than 1500 bytes.

WA: Do not enable the TCP reassembly feature.

5.3.9 Known Issues from ScreenOS 4.0.3r1

- **26336** – The device does not remove the BGP routes from the route table when you disable BGP.
- **26274** –Route-maps default to the action PERMIT instead of DENY.

W/A: Explicitly set the action to DENY.

- **26223** – When you add a zone to a virtual system, the device does not check if there are available zones in the global zone pool.
- **26209** – The device does not synchronize the management services configured on VLAN1 of the master unit to the backup unit.

W/A: Configure the management services on VLAN1 of the backup unit.

- **26197** – The Policy and VPN wizards in virtual systems don't work.
- **26110** – When you ping an interface bound to a security zone, another interface in the same zone responds with the MAC address of the original interface.
- **26104** – In an active-active configuration in an HA (High Availability) cluster, packet forwarding over the HA link fails between the two firewalls if the packet to create a session is not the first fragment.

- **26069** – The device drops traffic destined to a MIP on an interface in the Trust-VR, if the Trust-VR is the shared VR between two virtual systems.

W/A: Use the Untrust-VR as the shared VR.

W/A: Configure a static route to the MIP in the Trust-VR.

- **25887** – When you specify the **set zone tcp-rst** command, the device erroneously responds to TCP resets with TCP reset packets.
- **25837** – When you enter the cluster ID through the WebUI, the device erroneously allows you to specify 0.
- **25807** – BGP send-community doesn't work when the route is learned from its peer.
- **25781** – When the device detects a loose route attack, it increments both the loose route and restricted route counters.
- **25496** – (NetScreen-5000) In a redundant interface configuration, if the link of the primary interface is disconnected and then reconnected, the preempt option fails.
- **25244** – If you configure a primary and secondary IP address on an interface and change the primary IP address, the device does not retain the secondary IP address in the route table.
- **24166** – (NetScreen-5000-8G) If you use the AH (Authentication Header) protocol, the device does not display statistics when you issue the **get sa active stat** command.
- **24076** – (5000) The **set flow tcp-syn-check-in-tunnel** command fails.

W/A: Use the **set flow tcp-syn-check** command.

- **23856** – (5400) When you save the **set nsrp rto-mirror** command, the device displays it twice in the configuration file. (This is a display issue only; it does not affect the behavior of the device.)

5.3.10 Known Issues from ScreenOS 4.0.2

- **24316** – When you set the IKE heartbeat globally, the **set ike gateway heartbeat** appears twice in the configuration file.
- **24279** – The NetScreen device erroneously allows you to assign an IP address to an interface that is bound to the Self zone.
- **24108** – If the root admin initiates a Telnet connection to the NetScreen device and then enters the **set admin telnet access tunnel** command through the console, the device allows the original Telnet connection to go through, even if it does not use a VPN tunnel. The command takes effect only when the root admin terminates the original Telnet connection and initiates another Telnet connection after the command is set.

5.3.11 Known Issues from ScreenOS 4.0.1r3

- **24718** – The NetScreen device cannot pass SQLNetv2 traffic from the DMZ to the Trust zone when the Trust zone interface is in NAT mode and the NetScreen device is not configured to apply policy-based NAT to the SQLNetv2 traffic.

W/A: Use policy-based NAT for the SQLNetv2 traffic from the DMZ to the Trust zone.

- **24158** – When the members of an NSRP cluster in an active/passive configuration in Transparent mode synchronize the global configuration from the master to the backup, administrative traffic (such as syslog or SNMP) sent from the NetScreen device uses 192.168.1.1 as its source IP address, even if the IP address of VLAN1 is not 192.168.1.1.
- **24153** – The WebUI does not allow you to configure a policy if the zone contains the slash (/) character.
- **24132** – A vsys configuration does not get synchronized to the backup unit when issuing the **exec nsrp sync global-config save** command.
- **24116** – When a NetScreen device is being managed by Policy Manager, the event log reports that the system configuration has been saved from a random, erroneous IP address.
- **24115** – Using Korean characters in a service group name can cause the NetScreen device to crash.
- **23957** – The WebUI does not allow you to configure policies referencing zones with redundant interfaces.
- **23895** – The members of an NSRP cluster with three or more VSD groups do not follow the preempt rules.
- **23881** – If you move a policy with more specific restrictions above another policy with more generic restrictions, and both policies reference the same VPN tunnel, the NetScreen device applies the second, more generic policy.
- **23842** – The NetScreen device does not always clear unused TCP sockets, causing a loss of device manageability via the WebUI when the number of available sockets is consumed.
- **23757** – When attempting an SSH connection to a NetScreen device that does not allow SCS management, the device reports the wrong IP address as attempting to manage the NetScreen device.

- **23714** – Manual key VPNs sometimes reverse the order of the proxy IDs; that is, the local proxy ID is treated as the remote, and vice versa.
- **23705** – Policies do not use the assigned DIP pool for network address translation (NAT) when there are multiple policies referencing multiple DIP pools with fixed ports.

5.3.12 Known Issues from ScreenOS 4.0.1r1

- **23647** – The NetScreen device does not save the **set admin scs password disable username *usr_str*** in its configuration.
- **23562** – When a NetScreen device has a MIP with the same IP address as an Untrust zone interface and the device happens to lie in the data path of two VPN tunnel terminators involved in IKE negotiations, the NetScreen device sometimes intercepts the IPSec packets.
- **23529** – WebUI: Typing single quotation marks in a message entered in the NetScreen Blocked URL Message field (Configuration > URL Filtering) produces the text string “'”.
- **23523** – The NetScreen device is unable to load the **set nsrp monitor interface redundant*number*** if that redundant interface is defined in a virtual system.
- **23511** – The NetScreen device accepts all traffic shaping settings, but the WebUI only shows the priority level as high priority, no matter what its actual setting might be. You can see the true priority level with the CLI command: **get policy id *number***.
- **23460** – The NetScreen device does not save an authentication server configuration to flash if the “HA Session Backup” option is disabled on the policy.
- **23390** – The CLI does not allow the generation of a PKA key with a key length equal to or greater than 768 bytes.

W/A: Load a PKA key equal to or greater than 768 bytes by importing it in a file.

- **23349** – If you try to use the VPN Wizard when the NetScreen device is in Route or Transparent mode, an error message appears that states that you cannot create a VPN tunnel when the device is in either of these modes.
- **22780** – The NetScreen device is unable to block HTTP components—ActiveX controls, Java applets, .exe files, and .zip files—on an individual basis.

6. Getting Help

For further assistance with Juniper Networks products, visit

www.juniper.net/support

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

Copyright © 2004 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
ATTN: General Counsel

www.juniper.net