

# Juniper Networks Release Notes

Product: Juniper Networks ISG-1000 and Juniper Networks ISG-2000

Version: ScreenOS 5.0.0r10

Release Status: Public Release

Part Number: 093-1766-000, Rev. A

Date: 10-20-2005

## Contents

1. [Version Summary on page 2](#)
2. [Description of the ISG Systems on page 2](#)
  - 2.1 [ISG-1000 on page 2](#)
  - 2.2 [ISG-2000 on page 2](#)
3. [Addressed Issues on page 3](#)
  - 3.1 [Addressed Issues in ScreenOS 5.0.0r10 on page 3](#)
  - 3.2 [Addressed Issues from ScreenOS 5.0.0r9 on page 5](#)
4. [Known Issues on page 13](#)
  - 4.1 [Feature Limitations in ScreenOS 5.0.0r10 on page 14](#)
  - 4.2 [Compatibility Issues in ScreenOS 5.0.0r10 on page 15](#)
  - 4.3 [Known Issues in ScreenOS 5.0.0r10 on page 15](#)
  - 4.4 [Known Issues from ScreenOS 5.0.0r9 on page 15](#)
  - 4.5 [Known Issues from 5.0.0 on page 16](#)
5. [Documentation Errata on page 18](#)
  - 5.1 [Slot Guide Numbering on page 18](#)
  - 5.2 [Temperature Alarm Reporting on page 18](#)
6. [Getting Help on page 19](#)

## 1. Version Summary

The Juniper Networks ISG 1000 and ISG 2000 systems share the same ScreenOS code base. ScreenOS 5.0.0r10 is the first release of ScreenOS firmware for the ISG 1000 system. For general information about the ScreenOS 5.0.0r9 firmware, refer to the ScreenOS 5.0.0r9 release notes and ScreenOS documentation set.

The ScreenOS 5.0.0r10 release is interoperable with and provides basic support for all versions of NetScreen Remote and ScreenOS 2.6.1 and later versions.

## 2. Description of the ISG Systems

### 2.1 ISG-1000

The Juniper Networks ISG 1000 system is a purpose-built, Internet security gateway for medium-sized central enterprise sites, large regional sites, and security data centers or server farms. The ISG 1000 system integrates firewall, deep inspection, VPN, and traffic management functionality in a low-profile, modular chassis.

Built around a fourth generation security ASIC, the GigaScreen<sup>3</sup>, which provides accelerated encryption algorithms and policy searches., the ISG 1000 system provides for flexible configuration with the following interface options for its two open slots:

- 10/100 Mbps interface module, for 10/100 Base-T connections (4 and 8 ports)
- 10/100/1000 Mbps interface module (2 ports)
- Mini-GBIC interface module, for fiber-optic connections (2 ports)

The chassis also has four built-in 10/100/1000 ports for a maximum of 20 configurable ports per system.

### 2.2 ISG-2000

The Juniper Networks ISG 2000 is a purpose-built, high-performance security system designed to provide a flexible solution to medium and large central enterprise sites and service providers. The ISG 2000 security system integrates firewall, VPN, and traffic management functionality in a low-profile, modular chassis.

The ISG 2000 is built around Juniper Network's custom, third-generation purpose-built GigaScreen<sup>3</sup> ASIC, which provides accelerated encryption algorithms and policy searches. The ISG 2000 supports flexible I/O configuration with four- and eight-port 10/100 modules and two-port gigabit modules. Future releases of the ISG 2000 will support the ability to increase the system's power by adding optional security modules.

## 3. Addressed Issues

### 3.1 Addressed Issues in ScreenOS 5.0.0r10

This section describes addressed issues with the current release.

- **07156** — With some unsupported configurations, the device failed on a regular basis.
- **06738** — In some cases, a user could not load a shared zone into a virtual router after rebooting.
- **06517** — When Xauth is configured with an external RADIUS server and a local IP pool, allocated IP addresses on the gateway side were not always released.
- **06520** — Upon loading a policy at bootup, the device would hang for 30 seconds and reboot, but the same policy worked fine when it was added manually.
- **06354** — Operating as a relay agent, the device discarded BOOTP requests. ScreenOS does not support BOOTP as a server or client.
- **06301** — Malformed IKE packets led to device failure.
- **06245** — Users were unable to redistribute the route into BGP.
- **06156** — Device failed due to unusual OSPF activity.
- **06040** — In some cases, excessive syn close messages led to the failure of the NSRP Backup unit.
- **06036** — Device experienced extreme slowness during SNMP activity when DNS resolution was not forthcoming.
- **06008** — In some cases, RTC Time would be reset backwards upon reboot.
- **05867** — In some cases, Transparent mode fragmented IP multicast handling led to device failure.
- **05971** — Users were denied Internet access when a certain number of browsing requests were exceeded even if the URL fail mode was set to permit.
- **05833** — In some situations, heavy call volume caused device failure.

- **05746** — After some upgrades, the device responded very slowly.
- **05744** — Traffic 'in octets' counter on an interface stopped incrementing while the flow counter continued to count traffic.
- **05719** — In some cases, upgrading A/P NSRP devices led to system failure.
- **05703** — In some cases, NSRP backup unit experienced message corruption causing failure.
- **05697** — In some cases, multiple simultaneous configuration changes led to device failure.
- **05673** — Some kinds of BGP activity caused device failure.
- **05616** — FTP-PUT/FTP-GET deny policy changed to permit policy after importing through NSM Agent.
- **05615** — Creating some tasks, led to device failure or caused some features, such as Telnet, to fail.
- **05582** — Removing a policy from the source address, destination addresses, or service through a multi-cell policy CLI caused subsequent policies to be lost when rebooting.
- **05474** — An interface could be set to 1000MB in memory, but the settings could not be saved in Flash.
- **05440** — Large ping ( $\geq 1460$  bytes) to interface through VPN tunnel failed.
- **05385** — WebUI event log screen displayed incorrect characters in Microsoft Internet Explorer.
- **05322** — In some configurations, users saw SIN-ACK packet that had 14 extra bytes at the end.
- **05308** — Under some conditions, VOIP traffic led to device failure.
- **05246** — In some circumstances, the device set a route improperly in a site to site VPN configuration.
- **05188** — In some cases, the device failed during a cold start RTO sync.
- **05158** — In some cases, the device failed during very high WebAuth traffic.
- **05079** — In some cases, NSM did not import device configuration.
- **04941** — In some cases, packets going into an IPSec tunnel with NAT traversal were dropped.
- **04937** — Ping was enhanced to handle duplicated ICMP echo responses.
- **04960** — SME Agent configuration caused device failure.
- **04899** — When using a security device as DHCP relay, the relayed DHCP discovery packets (unicast packets) were erroneously intercepted.
- **04842** — After a remote gateway reboot, the device suffered an unusually long VPN outage.

- **04464** — Devices rekeyed inconsistently and independently of the VPN packet value.
- **04353** — In some configurations, the device did not send ARP packets when they arrived on a sub-interface.
- **04434** — In some circumstances with very high traffic load, managing the system was impossible.
- **04350** — In some configurations, DNS refresh was unreliable.
- **04252** — Some packets would be erroneously denied by a policy when the service group was very large.
- **04200** — In some instances, the NFS ALG opened the wrong port causing FTP traffic to match the incorrect session.
- **03789** — Downloading large files from the device over an SSH connection resulted in dropped connections.
- **03744** — In some cases, the device failed during VPN setup.

## 3.2 Addressed Issues from ScreenOS 5.0.0r9

Addressed issues for this release of the ISG 2000 system include:

- **04162** – Execution of the **get rms ctx pol** CLI command displayed an incorrect number of rules associated with a specific policy.
- **04138** – The device sometimes dropped packets because of policy lookup problems. This was due to slow performance.
- **04092** – When converting a policy to a set of rules, the ASIC sometimes used a conversion algorithm that created a different number of rules than had previously been generated for the same policy. The ASIC now generates a consistent number of rules when it converts a policy to rules.
- **04089** – The device sometimes mishandled incoming FIN packets when enabling TCP sequence number checking by issuing the **unset flow no-tcp-seq** CLI command.
- **04085** – When creating a hardware session on an active device in an HA pair, problems sometimes occurred. If the session went through a VPN tunnel, the Layer 2 table index in the hardware session became zero. This caused irregular packet behavior.
- **04078** – The device sometimes failed when a vsys was removed while a large amount of traffic passed through the device.
- **04074** – A process sometimes engaged the CPU for too long, causing device failure.
- **04036** – The device failed because it returned a null pointer to an SNMP task.

- **04031** – After an NSRP failover, two BGP virtual routing instances lost their adjacency state and were not able to reestablish as peers.
- **04027** – The device failed when SSH access was prohibited because of a corrupted SSH administration table in the device.
- **03946** – The primary device in an NSRP pair failed after a failover because of an incorrect VPN context synchronization.
- **03926** – The device sometimes incorrectly handled the IP checksum process when a small time gap occurred between the first and second IP fragments entering the device.
- **03918** – The Fast Ethernet link on the MGT port did not operate in full duplex mode. The MGT port was able to send or receive traffic, but was not able to perform both tasks simultaneously when connected to a Fast Ethernet device.
- **03915** – The device stopped forwarding traffic because of a deadlock condition while the device forwarded heavy traffic.
- **03907** – The NSRP backup device failed when a high number of session synchronizations occurred between the backup and the primary device.
- **03795** – The device did not properly free memory buffers after using them. Consequently, the device could not return them to the main memory pool.
- **03853** – A user could not establish a dialup session with a device after attempting to establish a remote connection to the device because the device returned a null pointer from the session. This indicated that the device did not recognize the user and did not know how to process the session.
- **03847** – After an NSRP failover, traffic failed temporarily because of replay protection, due to an incorrect ESP sequence number synchronization.
- **03811** – The device sometimes incorrectly processed packets that contained unknown tag headers. This corrupted memory, causing device failure.
- **03841** – In instances where memory became corrupted on the primary device in an active-passive NSRP pair, it forced the system to fail when the system used 23 percent or more of the CPU's resources.
- **03758** – The device sometimes failed when the ordering of a policy within a virtual system was changed.
- **03637** – When the firewall acted as a TCP proxy server, and if the server returned the syn-ack packet too late in response to a syn packet, the relevant firewall flow resource could be released too early and caused the firewall to fail.
- **03633** – The internal table search for routing entries on a device in an HA pair took too much time, causing the backup device to fail.

- **03601** – Under heavy traffic conditions, the Fast Ethernet transmit queue could not process incoming packets quickly enough, sometimes dropping packets.
- **03558** – A trace route or ping operation sometimes caused memory corruption, causing device failure.
- **03537** – The device failed when it incorrectly sent the DHCPDISCOVER packet out in the callback function.
- **03528** – The subscription key retrieval operation worked only intermittently because the device did not close the SSL socket properly.
- **03495** – Mail could not be retrieved from certain mail clients that sent POP3 authentication requests (such as Mozilla Mail Client) because the device did not support POP3 authentication.
- **03470** – The 802.1q VLAN trunking feature did not work properly when the device was in Transparent mode.
- **03433** – When two BGP peers established an adjacency and then lost the adjacency state, and the peer attempted to reestablish the state, but it was in the wrong state. This prevented it from reestablishing the adjacency.
- **03420** – The device failed when queueing a corrupted packet.
- **03415** – A peer to a BGP peer group could not be added again once it was unset.
- **03413** – A firewall device failed when multiple users attempted unauthorized SSH sessions.
- **03408** – The device failed when a tag header on a packet entering the device became corrupted.
- **03404** – The device generated incorrect traffic log titles when it sent a traffic log based on a multicell policy. The traffic log title displayed the same source IP and destination IP addresses.
- **03397** – The device failed because VPN traffic did not handle interrupts properly.
- **03394** – The Untrust interface could not be managed through a route-based VPN.
- **03381** – An IPsec tunnel could not be constructed by initiating ping traffic from the device.
- **03369** – When the primary device in an HA pair performed a cold start synchronization, with a large number of VPN tunnels, the backup device in the HA pair sometimes dropped some SPI synchronization packets.
- **03367** – When you clicked the Cancel button on the WebUI admin page for NetScreen-Security Manager, the page could not be located.

- **03358** – The device failed when trying to save a very long URL entry when attempting to perform URL filtering.
- **03356** – The Phase 2 rekey sometimes failed after the Phase 1 expired when using Kbytes as the criteria to trigger a Phase 2 rekey operation.
- **03355** – Track IP packets were sent out at the wrong interval, increasing failed counts (decreasing success rates) even though pings worked correctly.
- **03353** – When a policy was configured using the multiple service feature including more than 49 services, the Move check box of the policy disappeared from the WebUI and the WebUI displayed some field strings incorrectly.
- **03350** – The policy lookup rate slowed down when more than 6,000 ASIC policy rules occurred between any two security zones.
- **03340** – NetScreen-Security Manager did not send the correct Action code when generating a traffic log.
- **03338** – The component blocking feature that forces a packet to be dropped did not work properly.
- **03320** – When an active device in an active-passive NSRP pair attempted to synchronize with the passive device, the password used in the active-passive session was not compliant with length restrictions set by the **set admin password restrict length** CLI command. This resulted in the command failing on the passive device, creating an unsynchronized state for the password length restriction between the two devices.
- **03311** – When the VIP server detection was set to the Manual setting, the VIP server status detection still displayed the same status when the server detection parameter was set to Automatic.
- **03308** – When attempting to change a username in the WebUI, the system added a new user instead of changing the name of the existing user.
- **03295** – When issuing a **get interface** CLI command or similar commands, ScreenOS truncated interface names that had too many characters.
- **03281** – When performing an incremental SPF operation for an OSPF virtual routing instance, the device failed.
- **03278** – When updating a dynamic VPN tunnel's peer gateway IP, a new route lookup was not performed for the updated peer gateway IP. If the updated peer gateway IP was not reachable via the old route used for the previous peer gateway IP entry, the VPN failed.
- **03273** – After saving the value in the policy counter in the WebUI, the value was different from the actual policy count.
- **03267** – The anti-virus feature had a problem handling the HTTP packets because a web server inserted too many unnecessary white spaces in the HTTP header.

- **03263** – When managing the device from the V1-untrust or V1-trust interface using Manage IP, multiple sessions were created for each packet.
- **03261** – When two VPNs were active between two devices, with outgoing interfaces, after the VPN Monitor deactivated the tunnel after nine seconds, and caused a failover to the secondary VPN, the device did not update the session information.
- **03250** – A memory corruption caused device failure.
- **03243** – In an instance where the client on the Untrust side of the device connected to a MIP that connected the server to the Trust side, when an ASP began the server, it used a zero-sized window, slowing down performance, with the server sending back one character at a time.
- **03239** – When performing an FTP transfer or email download that went beyond the maximum bandwidth allocated in the traffic shaping feature, VOIP calls experienced a lot of intermittent voice transmissions.
- **03235** – When forcefully closing several PKA/RSA SSH sessions without properly logging out first, the system randomly failed several times.
- **03222** – Some SIP packets caused the device to fail when it attempted to establish a call.
- **03218** – The device sometimes dropped traffic attempting to enter it in instances when the device software session table became corrupted, resulting in a loss of varying (sometimes high) amounts of software sessions. This condition prevented you from creating new sessions, leaving an insufficient amount of resources for the device to accept new traffic.
- **03203** – The device sometimes failed when it traversed the session table.
- **03178** – The device sometimes failed with high CPU and the full session table due to session memory corruption.
- **03177** – Intermittent system failures occurred during an SNMP walk.
- **03168** – IPSec traffic that used the source NAT feature could not pass through the device. Source NAT is a process where a NAT module translates the source address in the IP packet header before forwarding it either to its destination.
- **03152** – When running XAuth in the WebUI environment, the XAuth page displays the CHAP fragment reassembly method selected by default.
- **03136** – Gratuitous ARP packets sent out to broadcast the presence of a device were blocked from being sent.
- **03128** – Mistakes occurred with Mapped IP (MIP) translation when a remote shell used a secondary session initiated from the server for redirecting standard error output from the console.

- **03111** – When issuing the **get nat registry vector** command on a device running ScreenOS 5.0.0, the device did not display any output on the console.
- **03092** – When the device was in transparent mode, it sometimes was unable to download the latest anti-virus signatures.
- **03089** – PPP traffic that uses both source NAT and fixed port DIP features could not pass through the device.
- **03081** – An anti-virus parsing error slowed performance for HTTP sessions.
- **03078** – With a very large configuration, when attempting to save a very large configuration, the device sometimes generated false HA up-down messages incorrectly indicating alternatively that the device disconnected and connected.
- **03071** – If the first VIP in the VIP list did not have a service defined for it, if you added a service to the second to fourth VIP in the list, the VIP Summary Page displayed no data.
- **03068** – When modifying the IKE Phase 1 gateway name using the WebUI, the primary device in an HA pair could not synchronize properly with the backup device so that the backup device received the IKE gateway name.
- **03058** – After successfully updating a device with the latest configuration in NetScreen-Security Manager, and then ran a Delta Configuration Summary operation, the summary still displayed commands indicating that the update did not successfully transfer all settings to the device.
- **03054** – The device did not update its ARP table because too many packets queued up for the same ARP entry.
- **03042** – The serial interface on the device disappeared after downgrading from ScreenOS 5.0.0rx to a previous version with the Unlimited Number of Users Version 2 key installed.
- **03025** – In certain situations, when a user authenticated using WebAUTH with SecureID, and the user in the Auth table timed out, subsequent attempts to authenticate failed.
- **02988** – The ALG did not work for a custom-defined rsh service.
- **02986** – SSHv2 with RADIUS authentication failed to authenticate external users properly.
- **02975** – While performing a virus scan with the anti-virus engine, the anti-virus update failed, and no traffic could pass through a device because the policies blocked it, and the device failed repeatedly.
- **02972** – When trying to transfer large files using SCP, the connection closed before the transfer completed.

- **02962** – When the device sent multiple authentication requests to an authentication server while waiting for a reply to a previous request, memory corruption sometimes occurred. This happened when the server sent a rejection response.
- **02952** – A code loop in a SIP disconnect state occurred and resulted in a core the device failing when disconnecting a SIP call over a Cisco VOIP network.
- **02941** – When you configured a device with a DIP and traffic shaping, the first traffic the device sent failed to reach its destination.
- **02933** – While attempting to age out specific sessions, the device sometimes went into an infinite loop causing the watchdog timer to cause the device to fail.
- **02915** – An invalid pointer reference between FTP control channel and data caused device failure.
- **02913** – Although a session on the device has a timeout of one second, when the session exceeded the timeout, the device terminated the session.
- **02908** – When losing a Web and SSH connection to the primary device in an active-passive HA configuration, the primary device could not be connected with an SSH or WebUI session, although it could connect to the backup device.
- **02906** – Pinging was unavailable from one device to another over a VPN between two devices that were each in transparent mode running ScreenOS 5.0.0rX.
- **02867** – If the DHCP relay server is set with an IP address, the device incorrectly attempted to resolve the IP address with the host name even though there was no hostname.
- **02845** – In an NSRP active-passive configuration, improper MAC table entries prevented the backup device from being managed. In some instances, you could not manage a backup device in an NSRP active-passive configuration.
- **02810** – A policy with the negate option did not free memory on the device properly, creating a memory leak, degrading device performance.
- **02774** – Multiple trace routes occurred after creating a BGP neighbor to a device in an HA pair, disabled HA synchronization, and then attempted to redistribute routes from the primary device to the backup device.
- **02768** – When the primary device attempted to synchronize with the backup device and sent it a new DIP session, the backup device could still have the existing DIP session and could not perform the synchronization.
- **02762** – If attempting to display 100 logs per page in the WebUI Traffic Log, the WebUI displayed no logs.

- **02725** – In an NSRP device pair, the primary device generated a log that indicated that multiple failovers occurred, but the backup device only generated one log, indicating only one failover.
- **02656** – The WebUI home page did not display the status for Layer 2 interfaces.
- **02620** – Issuing the debug command for the WebSense server, caused device failure.
- **02604** – When a device exported routes from a vsys to a root virtual router, the exported routes were not tagged with the correct vsys ID.
- **02602** – Attempts to establish Telnet, WebUI, and SSH, sessions to the interface, where management was enabled, failed, when a route from the correct interface was not provided or the route pointed to a different gateway.
- **02594** – A trace route or ping operation sometimes caused memory corruption, which caused device failure.
- **02580** – When creating a new custom service, then configuring a VPN using IKE, the Proxy ID setting in the VPN Autokey IKE configuration incorrectly defaults to the new custom service, and not the ANY service.
- **02555** – The system incorrectly created sessions for embedded ICMP packets.
- **02530** – A TCP stack error caused the BGP neighbor state to change to the Idle state before the BGP holddown time value (default of 180 seconds) expired. The BGP neighbor state, a setting determined by whether the current BGP routing instance, can detect its neighbor to be active, and is not supposed to render the neighbor Idle until no neighbor response occurs after the holddown time elapses.
- **02486** – In some instances, after enabling a WebSense server, when you accessed the Microsoft Outlook Calendar utility, you would lose connectivity to Outlook Email.
- **02482** – Slow http/https through VPN. Bug in H.323 implementation could cause session leak R. HTTP cannot pass if the **unset flow tcp seq** and **set flow tcp syn combo** CLI commands are used.
- **02385** – When selecting multiple source address groups in an intra-zone policy where the source was Trust and the destination was Trust, the groups were not displayed properly in the policy list.
- **02152** – In instances where an intra-zone policy was created so that the source zone was Trust and the destination zone was Untrust and that used multiple addresses, the Policy list displayed the same entity for both the source and destination in the policy.

- **02101** – Messages logged with a VIP incorrectly indicated the VIP connection connected and disconnected repeatedly, indicating the presence of a false positive even though the VIP connection sent acknowledgment responses to the query. The messages displayed continuously were:
  - VIP cannot be contacted.**
  - VIP is now alive.**
- **01998** – The **set console aux disable** CLI command could not be saved into the device configuration.
- **01635** – The system failed when an H323 recomputed a UDP checksum; the UDP packet lengths sometimes were too consistent with the IP lengths.
- **01584** – If a virtual routing instance acted as the ABR, then the routing instance did not advertise inter-area summary routes. An inter-area summary route is one value that encompasses a range of route prefixes contained in multiple routing areas.
- **01523** – An OSPF virtual routing instance sometimes unexpectedly dropped routes.

## 4. Known Issues

This section describes known issues with the current release.

- [Section 4.1 “Feature Limitations in ScreenOS 5.0.0r10”](#) identifies features that are not fully functional at the present time and will be unsupported for this release. We recommend that you not use these features.
- [Section 4.2 “Compatibility Issues in ScreenOS 5.0.0r10”](#) describes known compatibility issues with other products, including but not limited to specific Juniper Networks 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 or minimize its impact.

## 4.1 Feature Limitations in ScreenOS 5.0.0r10

The following feature limitations are present in this version of ScreenOS 5.0.0r10 and affect ISG 1000 and ISG 2000 systems.

- **SIP ALG** — Enabling SIP ALG on a device running ScreenOS firmware that was released prior to 5.0.0r10 can cause device instability. Disable ALG with the **unset alg sip** CLI command or upgrade to the latest ScreenOS firmware version.
- **Features Not Supported**
  - Flow options: aggressive aging, max-frag-size, tcp-seq-check, and path MTU
  - Interface MTU
  - TCP sequence number check
  - DHCP server and client (ISG 2000 only)
  - AV (CSP) (ISG 2000 only)
- **Redundant Interfaces**
  - You can configure redundant interfaces across modules, but you cannot combine a Gigabit module with an FE module.
  - Using redundant interfaces in an active-active HA pair of ISG 2000 systems does not allow traffic to pass through the device in the packet forwarding case.
- **Aggregate Interfaces** — Using aggregate interfaces in an active-active HA pair of ISG 2000 systems does not allow traffic to pass through the device in the packet forwarding case.
- **Vsys for Group IKE ID** — Group IKE ID users cannot be used in a vsys if that vsys uses a shared untrust interface.

We recommend using a private Untrust interface (tagged VLAN subinterface or dedicated physical interface) for the vsys.

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

We recommend using SSH version 2 or a different SSH version 1 client, such as OpenSSH.

## 4.2 Compatibility Issues in ScreenOS 5.0.0r10

Compatibility issues in ScreenOS 5.0.0r10 include:

- **General Compatibility Issues**

- **Freeswan** — The Freeswan 1.3 VPN client is incompatible with ScreenOS 5.0.0r10 in certain configurations due to IKE features that Freeswan does not fully support. The result is that Phase 2 negotiations and Phase 2 SA will not complete if the following commands are enabled in 5.0.0:

```
set ike initiator-set-commit
set ike responder-set-commit
set ike initial-contact
```

We recommend unsetting these commands to ensure compatible configuration on the system.

- **Compatible Web Browsers** — The WebUI for ScreenOS 5.0.0r10 was tested with and supports Microsoft Internet Explorer (IE) browser versions 5.5 and above, and Netscape Navigator 6.X for Microsoft Windows platforms, and Microsoft Internet Explorer version 5.1 for MacOS 10.x. Other versions of these and other browsers were reported to display exceptional behaviors.

## 4.3 Known Issues in ScreenOS 5.0.0r10

- **46465** — (ISG 2000) Redundant and aggregate interfaces in an active-active HA pair cannot pass traffic through the device in a packet forwarding case.

W/A: Use physical interfaces or configure the device using non-packet forwarding configurations when using redundant or aggregate interfaces.

## 4.4 Known Issues from ScreenOS 5.0.0r9

Known issues for this release of the ISG 1000 system include:

- **46720** — Self-traffic generated from a vsys will not be able to trigger a security association (SA) and a resulting VPN tunnel will not come up.
- **46451** — When the connection to the primary NTP server for an ISG 1000 system fails and a backup NTP server is not configured, the ISG 1000 system generates event entries indicating that the device tried to send an NTP request but failed due to a missing key id for the backup server.

```
NTP request cannot be sent. No key id found for Network Time
Protocol server backup
```

- **46672** — Under certain specific circumstances deleting an OSPF instance within a vsys may cause a device core-dump.
- **44767** — After setting PHY characteristic of an interface to AUTO mode, **get interface** command output does not indicate that the interface has been set to AUTO mode.

## 4.5 Known Issues from 5.0.0

The following are known deficiencies in features at the time of this release on the ISG 2000. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with “W/A:” If there is no subsection for a particular ScreenOS release, no new known issues were identified for that release.

- **37732** — The loopback interface field on the WebUI incorrectly displays SCS instead of SSH.
- **37573** — Under heavy traffic, the console response might become sluggish.
- **37125** — The **get counter flow interface** *<interface>* CLI command does not display the updated Teardrop SCREEN counter when the device is experiencing teardrop attacks.
- **37111** — When .exe files are blocked, the alarm log incorrectly indicates that zip files are blocked instead.
- **37090** — The **clear LED alarm** command does not actually clear the alarm LED. The alarm LED continues to glow red.
- **37076** — When using a custom shared zone in a vsys, the device allows you to configure a policy with an address of “any”, even if this address entry was not previously configured. Note that the device does not create an “any” address by default.
- **37074** — When a user creates custom zones with names like "a", "al", or "all", the **get zone** *<zone>* command does not work correctly.
- **36864** — The "nsIfSecondaryIpZone" SNMP query string returns incorrect zone information.
- **36625** — When using Microsoft IE 6.0, logging into a device via the Web sometimes displays a menu without a background.
- **36570** — When all four slots are populated with 8-port FE cards, the last four ports on slot 4 are disabled, so they cannot be used for traffic.
- **35878** — The consoles displays traces when using the **debug web all** CLI command while creating a VPN using the wizard.
- **35412** — When editing a member of an aggregate interface on the WebUI, it indicates that the member belongs to the incorrect aggregate interface.

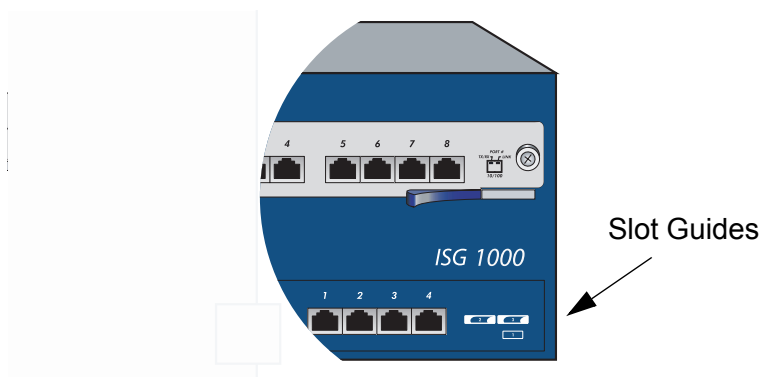
- **35262** — The device displays incorrect bandwidth information for aggregate interfaces.
- **35261** — The device erroneously allows ports with dissimilar speed/duplex settings to be configured as members of an aggregate interface.
- **35100** — When an SSH user connects to a device and types invalid commands, the device does not display any error messages.
- **35064** — When you click the help icon on the WebUI, it does not return the correct link.
- **34453** — The console temporarily stops for a few seconds when removing an interface from a layer 2 zone in transparent mode.
- **33652** — During a VPN stress test, the device occasionally increments the VPN auth failure counter and drops packets.
- **31553** — The SCREEN protection Syn-ack-ack-proxy counter does not increment correctly.

## 5. Documentation Errata

This section lists errata contained in the documentation for the ISG 1000 system.

### 5.1 Slot Guide Numbering

The slot guides shown in all of the illustrations of the ISG 1000 chassis in the *ISG 1000 User's Guide*, are inaccurate. Three slot guides should appear in the bottom right-hand corner on the front panel of the chassis to aid the system administrator with port numbering. The following illustrations show the correct slot guides.



Slot guide 1 represents the four built-in ports, slot guide 2 represents the module in the upper left-hand corner of the chassis, and slot guide 3 represents the module in the upper right-hand corner of the chassis.



### 5.2 Temperature Alarm Reporting

The TEMP LED alarm triggers when the ISG 1000 system temperature exceeds the allowed temperature range. The reported system temperature is the highest recorded temperature obtained from the CPU board and the system board. You can monitor the current system temperature by executing the **get chassis** CLI command. For details about the TEMP LED range, refer to the *ISG 1000 User's Guide*.

## 6. Getting Help

For further assistance with Juniper Networks products, visit

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

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

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, ISG 1000, ISG 2000, 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 94089-1213  
U.S.A.  
ATTN: General Counsel

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

