

Juniper Networks Release Notes

Product: Juniper Networks ISG 1000

Version: ScreenOS 5.0.0r9

Release Status: Public Release

Part Number: 093-1512-000, Rev. B

Date: 5-24-2005

Contents

1. Version Summary on page 2
2. Description of the ISG 1000 System on page 2
3. Addressed Issues on page 2
4. Known Issues on page 2
 - 4.1 Feature Limitations in ScreenOS 5.0.0r9 on page 3
 - 4.2 Compatibility Issues in ScreenOS 5.0.0r9 on page 4
 - 4.3 Known Issues in ScreenOS 5.0.0r9 on page 4
5. Documentation Errata on page 5
 - 5.1 Slot Guide Numbering on page 5
 - 5.2 Temperature Alarm Reporting on page 5
6. Getting Help on page 6

1. Version Summary

The Juniper Networks ISG 1000 and ISG 2000 systems share the same ScreenOS code base. ScreenOS 5.0.0r9 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 5.0.0r9 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 1000 System

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 GigaScreen3, 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.

3. Addressed Issues

This is the first release of ScreenOS firmware for the ISG 1000. There are no addressed issues.

4. Known Issues

This section describes known issues with the current release.

- Section 4.1 “Feature Limitations in ScreenOS 5.0.0r9” 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 5.0.0r9” 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.
- Section 4.3 “Known Issues in ScreenOS 5.0.0r9” describes deviations from intended product behavior. Whenever possible, information is provided for ways to avoid the issue or minimize its impact.

4.1 Feature Limitations in ScreenOS 5.0.0r9

The following feature limitations are present in this version of ScreenOS 5.0.0r9 and affect ISG 1000 systems.

- **Features Not Supported**

- Flow options: aggressive aging, max-frag-size, tcp-seq-check, and path MTU
- Interface MTU
- TCP sequence number check

- **Redundant Interfaces on the ISG 1000 System**— You can configure redundant interfaces across modules, but you cannot combine a Gigabit module with an FE module.

- **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 5.0.0r9

Compatibility issues in ScreenOS 5.0.0r9 include:

- **General Compatibility Issues**

- **Freeswan** - The Freeswan 1.3 VPN client is incompatible with ScreenOS 5.0.0r9 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 5.0.0r9 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 5.0.0r9

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
```

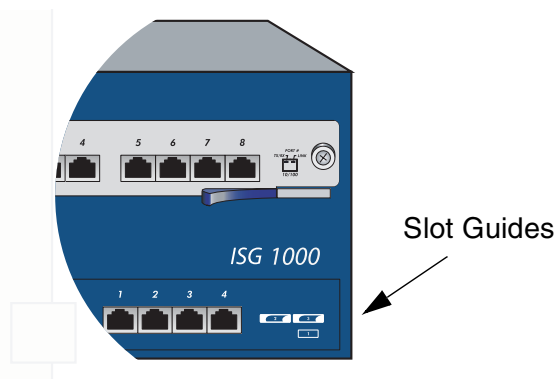
- **46672** - Under certain specific circumstances deleting an OSPF instance within a vsys may cause a device core-dump.
- **44767** - After setting PHY characteristic of an interface to AUTO mode, “get interface” output does not indicate that the interface has been set to AUTO mode.

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, Rev. A*, 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** command. For details about the TEMP LED range, refer to "LED Dashboard" on page 2 of the *ISG 1000 User's Guide, Rev A*.

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 © 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