



ISG 2000 with ScreenOS 5.0.0-IDP1

Release Notes

Release 5.0.0-IDP1 r2
07-27-05

Contents

- 1 “Version Summary” on page 2
- 2 “New Features” on page 2
- 3 “Changes to Default Behavior” on page 3
- 4 “Addressed Issues” on page 3
- 5 “Known Issues” on page 3
 - 5.1 “Limitations of Features” on page 3
 - 5.2 “Compatibility Issues” on page 4
 - 5.3 “Known Issues” on page 4
- 6 “Getting Help” on page 5

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1722-000

1 Version Summary

The Juniper Networks Integrated Security Gateway (ISG) Series delivers unmatched firewall, VPN, and IDP performance through the combination of a fourth generation security ASIC, the GigaScreen3, high speed microprocessors and pluggable security modules each with their own processing and memory.

The Juniper Networks ISG 2000 and ISG 1000—with integrated, best-in-class Intrusion Detection and Prevention (IDP) running on the security modules—stops worms, Trojans, Spyware, malware and other emerging attacks from penetrating and proliferating across the network.

ScreenOS 5.0.0-IDP1r2 is the latest software version based on the ScreenOS 5.0.0 firmware branch for the ISG 2000 security system.

You must install and use the appropriate version of NetScreen-Security Manager 2005.1 to configure and manage the ISG 2000 and the ISG 2000 security modules.

2 New Features

The following is a partial list of new features and enhancements in the main release. This revision also contains a new feature: SIP protocol decodes.

- **Integrated Intrusion Detection and Prevention (IDP) Mechanisms.** IDP extends Firewall/VPN functionality to protect the network against application level threats such as those proliferated by worms, Trojans, hackers, and spyware. The security modules for the ISG 2000 support multiple intrusion detection mechanisms including stateful signatures, protocol anomaly detection, and backdoor. IDP's traffic anomaly, SYN protector, and IP spoof are pre-existing ScreenOS features.
- **Support for all IDP Protocols And Contexts.** The security modules for the ISG 2000 provide extensive coverage of known and unknown threats by decoding 60+ protocols and searching within 500+ service fields, with pre-defined attack objects, as well as customizable ones. This release adds SIP protocol decoding.
- **Comprehensive Usability, Manageability and Reporting Using NetScreen-Security Manager.** Management of the ISG 2000 and security modules using NetScreen-Security Manager provides you access to easy to use monitoring and analysis tools including the Log Viewer, Log Investigator, log suppression, dynamic groups, auto reports, custom reports, scalability for large number of devices, HA for Device Server, and packet captures.
- **Zone-based and Other Virtualization Features for IP Policies.** Use NetScreen-Security Manager to define intrusion detection and prevention policies not only by IP addresses but by zones, and to contain policies and enforcement. VLAN-tags, overlapping IP addresses in route mode are also supported.
- **VPN Aggression to Intrusion Prevention Services.** You can further extend policy- and route-based VPNs to IP policies enabling you to inspect de-tunneled traffic at the network and application level.

- **Role-based Administration for Firewall and IP Rulebases.** You also have the ability to separate and filter between FW/VPN and IP rulebases (tab navigation) as an option.

3 Changes to Default Behavior

None.

4 Addressed Issues

The following are addressed issues in this release:

- **50274** – ScreenOS should sent an emergency log to NSM when SM failure is detected.

ScreenOS now sends a critical level log event when it detects an SM failure event.

- **50012** – Policy updates fail if compressed policy file is over 4 MB.

Policy updates now work even if policy file is very large.

5 Known Issues

This section describes known issues with the current release.

Section 5.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 5.2 “Compatibility Issues” describes known compatibility issues with other products, including but not limited to specific Juniper Networks’ appliances, versions of ScreenOS, Internet browsers, 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” describes deviations from intended product behavior in ScreenOS as identified by Juniper Test Technologies through their verification procedures. Whenever possible, information is provided to assist the customer in avoiding or otherwise working around the issue.

5.1 Limitations of Features

This release contains the following feature limitations:

- **ScreenOS 5.0.0-IDP1 is not supported on mainline ScreenOS firmware versions.** If you upgrade to ScreenOS 5.1, you will not be able to access the security module functionality. Security module functionality will be integrated into the mainline ScreenOS firmware in an upcoming release.

- **Enterprise Security Profiler functionality is currently not available.** This functionality will be available in a later release. Other standalone-IDP features including Honeypot are planned to be made available later in 2005.
- **Sniffer mode not supported.** The ISG 2000 is always deployed inline. You can not deploy the ISG 2000 with an external TAP or SPAN port on a switch. The Tap mode option is however, available supporting passive, inline detection of application layer threats. Sniffer mode for the TAP/SPAN port is currently available on standalone IDP devices only.
- **IDP Manager does not support management of the ISG 2000 or the ISG 2000 security modules.** You must install NetScreen-Security Manager FP3IDPr1 to manage the ISG 2000 and security modules.

5.2 Compatibility Issues

- None.

5.3 Known Issues

The following are known deficiencies at the time of this release. Whenever possible, a work-around is suggested following the description of the problem. Workaround information starts with "W/A:".

- **49924** – NSM-IDP gives error trying to update ISG-IDP.
- **49622** – IDP not dropping retransmitted packets for the signature WINDOWS RPC: LSASS MALICIOUS OPCODE in compound attacks when action is set to "Drop Packet."
W/A: Set action to Drop Connection instead of Drop Packet.
- **48468** – Servers do not receive a reset packet with NAT enabled. This occurs in the case where the server is in route mode and the client is in NAT mode.
- **45733** – IP action "close" sends an incorrect seq # in the RST packet. This prevents you from closing the connection on the host.
- **42416** – You are not able to clear or cancel IP action rules.
W/A: Reboot the device to clear the IP action table.
- **42341** – When firewall authentication is enabled, and you are using Linux as a client machine, the FTP client login does not prompt you to add a password.

6 Getting Help

For more 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 web address.

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

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: Deep Inspection, ERX, ESP, Instant Virtual Extranet, Internet Processor, J-Protect, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-IDP 1000, IDP 50, IDP 200, IDP 600, IDP 1100, ISG 1000, ISG 2000, NetScreen-Global Pro Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, GigaScreen ASIC, GigaScreen-II ASIC, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. 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.
ATTN: General Counsel
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
U.S.A.

www.juniper.net

