



ISG with ScreenOS 5.0.0-IDP1

Release Notes

Release 5.0.0-IDP1 r10c
9-28-06

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 4
- 5 “Known Issues” on page 5
 - 5.1 “Limitations of Features” on page 5
 - 5.2 “Compatibility Issues” on page 6
 - 5.3 “Known Issues” on page 6
- 6 “Getting Help” on page 8

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1843-000

1 Version Summary

NOTE: This is the fourth revision of ScreenOS 5.0.0-IDP1. However, it is being released as “r10” to make it clear that it is in sync with ScreenOS 5.0.0r10.

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-IDP1r10 is the latest software version based on the ScreenOS 5.0.0 firmware branch for the ISG security system.

Juniper Networks recommends that customers administer ISG devices with the latest available version of NetScreen-Security Manager. ScreenOS 5.0.0-IDP1r10 requires NetScreen-Security Manager 2005.2 or later.

2 New Features

The following is a list of improvements in this maintenance release.

NOTE: These improvements are available only with the IDP license key.

2.1 *Cut-through mode*

Optionally turns off packet inspection for flows during policy push if CPU usage is higher than a specified threshold. Prevents traffic loss during policy push during periods of high traffic.

If packets from a given flow arrive in the security module during a policy push, and if CPU utilization exceeds the threshold, the security module does not inspect those packets or subsequent packets for the given flow. If packets from a flow arrive during policy push and the CPU threshold has not been reached, then the packets are inspected. This feature only effects processing during a policy push.

Replace the # symbol in the instructions with the number of the security module you are configuring.

To turn on cut-through mode for a security module (default is off):

```
exec sm # ksh "scio const set sc_enable_packet_loopback 1"
```

To turn off cut-through mode for a security module (default):

```
exec sm # ksh "scio const set sc_enable_packet_loopback 0"
```

To change the threshold CPU setting for a security module, expressed as a percentage (default is 30):

```
exec sm # ksh "scio const set sc_loopback_cpu_usage <0-100>"
```

2.2 *Persistent scio commands*

scio command settings are now persistent across reboots. If you set an scio command, rebooting will not unset it.

2.3 *Features from the main release*

The following is a partial list of new features and enhancements in the main release.

- **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 Series 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 Series 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.
- **Comprehensive Usability, Manageability and Reporting Using NetScreen-Security Manager.** Management of the ISG Series 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

This release contains all Addressed Issues included in ScreenOS 5.0.0r10. For more information see

www.juniper.net/techpubs/software/screenos5x/screenos5xmaintenance/rn_5.0.0_r10_RevC.pdf

The following ISG-IDP specific issues are also addressed in this release:

Management

- **cs10112**—(ISG) In some cases, traffic would fail to pass through the device after an NSM Policy was pushed down. This was due to incorrectly updated internal table.
- **cs09159**—NSM updates to the master NSRP firewall fails if agent reporting is turned on.
- **os64302**—If an AIM attack object was updated with an older version of Detector than the version present on the device, an NSM Update returned a "-1" error message and the device reset.
- **cs10636**—Import of a configuration, with a large number of VSYS defined, into NSM 2005.3r2 fails with the error "Unable to get device DM needed for Import! Device failed to return valid data!"

Other

- **cs05750**—A TCP half-open connection would not age out when the service timeout was set to never.
- **cs10001**—(ISG) Due to an incorrect IP checksum calculation, IDP modules did not pass fragmented packets.
- **cs09451**—Passive FTP to a MIP address fails.
- **cs06127**—In configurations in which a high number of session timeouts occur, the device could reset.

Performance

- **os62675**—Incorrect initialization of an internal table caused performance degradation of http traffic.
- **cs06223**—With TCP_SYN_Check disabled, and a large number of TCP RST packets received the device experienced periods of high CPU and Telnet access was unavailable.
- **cs11091**—Due to a packet matching multiple signatures, multiple times, processing was not unique. This resulted in a packet loss on the IDP module and the CPU increasing.

Routing

- **cs10883**—In a Win2003 environment, TFTP through the firewall would fail due to the ALG handling.
- **cs06562**—(ISG-2000) Multicast Transparent mode traffic led to slow throughput.
- **cs04336**—Packets are dropped or are improperly routed when passing through a VSYS configured with DST-NAT in a Multi-VR environment.
- **cs09968**—(ISG-1000) After the IDP is enabled via a policy push, the device stops forwarding packets. This is caused by a combination of fragmented packets (TCP & UDP) with a TTL value of 1.

VPN

- **cs10151**—(ISG) In NAT-T VPN environment, the device improperly handled the reassembling of fragmented packets during an IKE negotiation causing the VPN to fail.

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:

- **Security module functionality is integrated into the mainline ScreenOS firmware with release 5.4r1.** Security Module functionality is not supported in Screen OS versions 5.1, 5.2 or 5.3.
- **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.

- **Sniffer mode not supported.** The ISG Series is always deployed inline. You can not deploy the ISG Series 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 or the ISG security modules.** You must install NetScreen-Security Manager to manage the ISG 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:".

CLI

- **cs08629**—A "get session" displays sessions with a time value of "time 0". Sessions in this state do not clear from the table.

W/A: Upgrade to ScreenOS 5.4r1 release.

HA & NSRP

- **cs08876**—(ISG) Currently, the IDP modules do not support the NSRP option "master-always-exist"; thus, the devices will go into an inoperable state if both cluster members fail.
- **cs07279**—In an NSRP Active-Backup configuration, the message "corrupt session pointer" was displayed on the console every 5 to 10 minutes.

Management

- **cs07029**—The device had high CPU usage when syslog and policy logging were enabled.
- **cs10444**—Firewall erroneously reports high number of sessions through SNMP.
- **cs07714**—IDP Logs shows the destination IP as 0.0.0.0. Some attacks based on TCP stream matching will generate multiple logs for a single matching attack instance. The later ones likely show destination IP of the log set to 0.0.0.0.

W/A: The issue is fixed in ScreenOS 5.4r1.

- **cs05079**—Import of a device configuration by NetScreen-Security Manager fails with "java.io.IOException: Parse error."

- **cs08746**—When the logging rate is heavy on the device, any updates from NSM fails causing a timeout exception message.

W/A: Contact JTAC for a patch.

Other

- **cs09711**—ISG with IDP module produces a False Positive of SMTP: MIME Filename Directory Traversal for ISO-2022-JP encoded files.

Performance

- **cs08494 / cs09904**—ISG with a Security Module could encounter performance problems when a policy is pushed. This happens when CPU0 is made unavailable while a policy is being installed. Device performance remains stable if the Security Module is disabled.

W/A: Contact JTAC for a workaround.

Security

- **cs08510**—A device might reset with an error when the initial NetScreen-Security Manager configuration push included URL filtering.

VOIP/H323

- **cs10158**—False positive generated on "SIP Syntax Error" protocol anomaly.

VPN

- **cs08074**—A device might drop VPN traffic when replay protection was enabled.

Web UI

- **cs05488**—In some cases telnet administration to the device will disconnect when a WebUI operation does a save.

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 device with Juniper Networks at the above Web address.

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.