



ISG with ScreenOS 5.0.0-IDP1

Release Notes

Release 5.0.0-IDP1 r10b
7-31-06

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 6
 - 5.1 “Limitations of Features” on page 7
 - 5.2 “Compatibility Issues” on page 7
 - 5.3 “Known Issues” on page 7
- 6 “Getting Help” on page 9

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1818-000, Rev. B

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:

- **09946**—Time Binding attributes for the IDP signatures fail to detect attacks within the specified scope.
- **09860**—The IDP modules crashed when the DFA table index was set incorrectly for contexts with more than 16 tables.
- **09786**—DFA FPGA issue causing detection failure.
- **09681**—NSM agent crashes if interface is disconnected during communication with NSM Device Server.
- **09652**—When the IDP devices are in TAP mode, the IDP modules fail to detect attacks after a policy is installed. This affects firewalls with the j3.4 patch installed.
- **09562**—On an ISG1000 device with two Security modules, the Module 1 LED does not glow.
- **09474**—One-time crash after speed/duplex change.
- **09453**—Link list issue causing Yahoo Messenger packet loss.
- **09379**—Incorrect addition of "set task name ospf priority normal" to the command chain caused NSRP flapping at intervals.
- **09238**—Certain logging options causing high CPU usage.
- **09083**—Exceeding bandwidth on interface over extended period caused packet loss.
- **09111**—When the Transmit queue is full and causes packet to drop, both devices go to the Active state.
- **09059/09596**—Due to an incorrect hash value calculation, hardware sessions are not cleared.
- **08986**—When an update from NSM is performed, the detector engine for ScreenOS 5.0.0r10a gets updated on a firewall with the i2.4 patch installed. Since both the releases use the same version of detector software, the detector should not get updated.
- **08891**—Device rebooted after booting. Only happened once.
- **08741**—Occasionally, the device drops PMTUD packets, return Type 3 and 4, and then receives the messages, "source MAC is not virtual MAC".

- **08694**—VLAN throughput drop with HTTP download (FPGA stuck for 65-68 packet size).
- **08693**—When the command `get led`, is executed, incorrect details relating to the On/OFF status are displayed.
- **08667**—Redistributed routes into OSPF exceeded system limit 1024.
- **08651**—A policy-based VPN failed in the IDP TAP mode.
- **08614/08560/08630**—90 - 100% traffic loss when pushing IDP security policy. Pushing a policy causes performance problems on a device because the CPU is unavailable while installing a policy.

Use *Cut-through mode* on page 2 resolve the problem.

- **08612**—URL too long when WebSense is enabled.
- **08565**—When executing the command, `get service`, the output displays the incorrect timeout values.
- **08547**—Device accepts an older version of detector software.
- **08495**—SIP calls cause the device to reboot.
- **08454**—ISG-1000 buffers and sessions stuck in ASIC.
- **08432**—Configuration goes out of sync and static route removed.
- **08249**—When too many custom service objects are defined, a watchdog timeout occurs.
- **08162**—OSPF int cost not taking into effect and next hop 0.0.0.0.
- **08158**—Incorrect replay packets deactivating VPN tunnel.
- **08111**—Free session link list broken.
- **08103**—WebUI: Dst-NAT with IP shifting cannot set range= 0.
- **08085**—WebUI: custom port name containing trailing blank gets set to 0.
- **08083**—High CPU when using nuttcp to transfer data across VPN tunnel.
- **08003**—Broken link list.
- **07991**—Logs displays action as ACCEPTED even though IDP drops the traffic.
- **07901**—Policy with a VSYS with IP classification issue.
- **07753/08871**—Master and backup have run out of tcp sockets.
- **07491/08736**—Throughput low on ISG1000 with Mini-GB SX module.

- **07279**—Corrupt session pointer msg on console of backup firewall every 5 to 10 minutes.
- **07001**—Issues with HTTP:BRUTE FORCE protocol anomaly causing security module restarts.
- **06707**—Time Binding function doesn't work properly.
- **06996** – BGP “set network check” doesn't work for routes imported from other vr.
- **06986**—Spoofed ARP packet causes DOS.
- **06652**—Traffic log stops updating after 2 days.
- **06557**—Firewall is adding bytes to the payload of certain packets.
- **06036**—SNMP walk hangs.
- **06005/07789** – NSM directives fail when there are around 1500 logs per second or 1500 HTTP connects per second.
- **05771**—Incorrect system.sysUpTime.sysUpTime value.
- **05474**—Hard-setting the GE copper interface to 1000/full shows 100MB in config.

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.
- **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:”.

IDP (Security Module)

- **10736**—IDP policy validation failure.
W/A: Contact JTAC for a workaround.
- **10158**—False positive on SIP Syntax Error Anomaly.
- **10112**—Traffic loss after NSM Policy push due to use of no longer existent DFA tables.
W/A: Contact JTAC for a patch.
- **10001**—The ISG with IDP modules not recalculating checksum on some reassembled packets, causing network to drop those packets.
W/A: Contact JTAC for a patch.
- **09968**—After the IDP is enabled via a policy push, the device starts losing packets. This is caused by a combination of fragmented packets (TCP & UDP) with a TTL value of 1.

W/A: Contact JTAC for a patch.

- **09904/08494**—IDP crashes due to a DFA merge. The root cause is under investigation.

W/A: Execute the command below on all security modules:

```
exec sm < #> ksh "scio const set sc_dfa_run_merged 0"
```

where < #> is the number of the security module.

- **09711**—IDP generated a false positive when it received a file encoded in iso-2022-jp. Particular sequence of characters matched the SMTP: MIME Filename Directory Traversal signature.
- **09458**—Unusual Yahoo IM packet format crashes Security Module.
- **08876**—IDP modules enter an inoperable state when IDP modules on both cluster members fail.
- **07714**—Log shows 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.

Fixed in ScreenOS 5.4r1.

- **06872**—IDP modules not allowing TCP/512 traffic.

Firewall

- **10151**—In NAT-T traffic, if the peer's cert file is too big, it has to be fragmented. In 5.0, ISG platforms have trouble reassembling these fragmented packets in IKE negotiation, which then fails the VPN traffic.
- **10444**—Firewall erroneously reports high number of sessions through SNMP.
- **09451**—Passive FTP fails with MIP.

W/A: Contact JTAC for a patch.

- **09159**—NSM updates to the master firewall fails if agent reporting is turned on.
- **09003**—Unable to execute delta/update/import on firewall when multiple VSYS are defined. This happens when the NSM agent fails to exit from the VSYS when the directive completes.

W/A: Unset the NSM agent using "unset nsm enable", wait 5 seconds, then set it again using "set nsm enable".

- **08746**—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.

- **08629**—After executing the command `get session`, there are sessions that display the time as “time 0”. These sessions do not clear on the device.
- **08510**—Coredump when initial NSM push includes URL filtering configurations.
- **08222**—Clock on the FW lags after NTP update.
- **08074**—With certain traffic patterns, the peer gateway device of the IPSEC tunnel may get IPSEC packets with a different sequence number resulting in replay errors.
- **09968**—Pushing a policy causes performance problems on a device because the CPU is unavailable while installing a policy.
- **07279**—Corrupt session pointer msg on console of backup firewall every 5 to 10 minutes.
- **07029**—Syslog issue causes high CPU load.
- **05833**—tv2 patch unstable.

W/A: If running tv2 patch, upgrade to tv4 patch.

- **05488**—Saving the configuration via the WebUI causes telnet sessions to time out.
- **05079**—Directives executed from NSM (delta config, update config, etc.) fail with an exception error. This happens when the configuration that is sent from the device to the NSM server reaches a certain sizes.

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.

