



# **Intrusion Detection and Prevention Release Notes**

*Release 4.0r1  
11-27-2006*

## ***Contents***

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 4
- 4 System Requirements on page 4
- 5 Addressed Issues on page 4
- 6 Known Issues on page 5
  - 6.1 Limitations of Features on page 6
  - 6.2 Known Issues on page 6
- 7 Getting Help on page 9

## **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 093-1764-000 Rev B

## 1 Version Summary

---

Juniper Networks Intrusion Detection and Prevention Sensors detect intrusions and prevent attacks on your network.

IDP 4.0 Sensors, and all subsequent releases, are now managed with Juniper Networks' NetScreen-Security Manager. This release contains the software and instructions necessary for migrating your existing IDP Sensors to NetScreen-Security Manager.

Juniper Networks NetScreen-Security Manager is a comprehensive security management solution designed to manage device, network, and security configuration for integrated firewall, intrusion detection and prevention, and virtual private network (VPN) appliances, sensors, and systems.

See the IDP-NSM Migration Guide, the NetScreen-Security Manager Administrator's Guide for a description of NetScreen-Security Manager and the migration process.

This version has been Common Criteria certified to the U.S. Government Intrusion Detection System, System Protection Profile, version 1.5, March 9, 2005, assurance level EAL2.

## 2 New Features

---

The following is a list of new features and enhancements.

- **NSM Management System for Standalone IDP**—Tie-in to NSM management architecture (GUI and Device Server). With IDP 4.0 and on, NSM becomes the definitive management system for IDP Sensors. Takes advantage of NSM's management of all Juniper Networks security devices, role based administration, and HA, among others (see NSM benefits).
- **Dynamic Image Loading**—Allows IDP to introduce new protocol decodes, C-signatures to improve accuracy and coverage without sensor reboot.
- **Signature Hierarchy**—Improves usability by reducing logs and collapsing related children attacks to a single parent attack.
- **New IDP Protocols**—Oracle TNS and H.225 (signaling protocol for H.323) anomaly detection engine. Going forward, you can introduce new protocol decodes "on the fly" due to dynamic image loading feature.
- **OS Fingerprinting**—Allows Profiler to detect OS type and version to complement current Application Fingerprinting.
- **Diffserv**—Creates Diffserv marking on an attack match or application identification (P2P, IM, etc.) for routers to enforce QoS handling and throttling.
- **SYN Cookie**—Enhances SYN flood protection by verifying the legitimacy of a SYN packet with a encrypted cookie with TCP sequence number.
- **GTP Traffic Support**—IDP inspection of GTP encapsulated traffic.

- **EasyConfig**—Simplified CLI-based startup utility that allows quick installation of IDP sensor.
- **Boolean Expressions**—Compound attack objects now have a Boolean Expressions field. You can construct complex match patterns using object members.
- **Standalone IDP Migration**—Migration of all configuration data and logs from IDP Manager to NSM. Upgrade of IDP Sensors to IDP 4.0.
- **Security Explorer**—The Security Explorer is a dynamic graphical tool that enables you to visualize network behavior based on profile, log, and report data. The main component is a touch graph that represents the relationships among data objects on multiple levels including hosts, services, and attacks. The Security Explorer also displays a Tool Area, Log Viewer, and Reports within contexts of the viewed graph.
- **Scalability**—100 IDP Sensors (20 of them running Profiler) and 2000 FW/VPN devices can be managed by 1 NetScreen-Security Manager installation.
- **Recommended Filter**—NSM now allows you to filter for Recommended attack objects when creating a custom group. Juniper Networks flags an attack as Recommended when it is currently circulating, represents a high risk of damage, or represents a common vulnerability. In addition, there is a new predefined attack group called Recommended which contains all attack objects with this flag on.
- **Template Improvements**—IDP policy templates have been modified based on customer recommendations. Since IDP policies may be pushed to ISG or standalone IDP devices, the templates have a firewall rulebase by default. Standalone IDP Sensor ignore the firewall rulebase. Less commonly used rulebases are no longer part of the templates, but they can be easily added to any policy.
- **Common Criteria Support**—The following features support Common Criteria compliance:
  - **Audit Table**—Enhanced audit table provides more comprehensive and accurate audit information.
  - **Audit Log Migration**—Old audit log data can be migrated into new audit log format.
  - **Audit Log Disk Space Management**—Logger can purge old entries before adding new ones to better manage disk space usage.
  - **Block Logins**—Ability to block logins by IP address after specified number of consecutive failed attempts.

### 3 Changes to Default Behavior

---

- Management of stand-alone IDP Sensors running IDP 4.0 handled via the NetScreen-Security Manager. The IDP Management Server and IDP UI cannot manage IDP 4.0 Sensors. See the IDP-NSM Migration Guide for a complete description of the changes.

### 4 System Requirements

---

Juniper Networks supports the following upgrade paths to IDP 4.0.

**Table 1: Upgrade Paths**

Existing Version	Upgrade Path
3.2r1	Directly to 4.0r1
3.1r4	Directly to 4.0r1
Other versions	Upgrade IDP sensors and Management Server to 3.1r4 or 3.2r1 using supported upgrade paths, then upgrade to 4.0r1.



**CAUTION:** Upgrade from IDP 3.2r2 to IDP 4.0r1 is not supported. You will be able to upgrade IDP 3.2r2 to IDP 4.0r2 during second half of 2006.

IDP Management Server is no longer supported with IDP 4.0. Instead, IDP Sensors are managed with NetScreen-Security Manager 2006.1. NetScreen-Security Manager 2006.1 requires one of the following operating systems:

- Red Hat ES/AS 3.0 with Update 5
- Red Hat ES/AS 4.0 with Update 1
- Solaris 8 or 9 with current patches from Sun

Refer to the *IDP-NetScreen Security Manager Migration Guide* and the *NetScreen-Security Manager Installer Guide* for detailed installation requirements and procedures.

### 5 Addressed Issues

---

The following issues are addressed in this release:

- **09391**—global.bee.address parameter was not set in idp.cfg.
- **07936** – IDP in Sniffer mode did not re-tag the VLAN packet when sending the TCP RST.
- **07714** – IDP Logs showed the destination IP as 0.0.0.0 if the same attack is matched multiple times.
- **07634** – ARP spoofs were reported as being dropped even though ARP spoofing was turned off. This happened when customer used a VR other than the default.

- **07485** – Update Attack 407 failed in 3.1r3.
- **07329** – Traffic flows through when NIC Bypass feature was disabled.
- **07311** – Src and Dst port swapped in Packet capture of Honeypot Impersonated.
- **07182** – LogWalker process stopped unexpectedly after an attack update.
- **07176** – ACM did not configure sniffer reset port back to default.
- **07038** – Sensors in active-passive HA mode sometimes dropped FTP ACK packets if both receive client-side packets but only one receives server-side packets.
- **06884** – RX drops and errors on sniffing interface of Fibre NIC.
- **06881** – Collisions and Errors on Interface when speed/duplex hard coded.
- **06668** – When detecting IP spoofing, logviewer and exported log didn't show Src IP address.
- **06581** – Time binding function of compound attack did not work.
- **06365** – Detecting and Dropping (drop packet) Mytob WORM (WORM: Mytob DNS Activity) caused ALL subsequent and normal DNS traffic from the source to be dropped.
- **05589** – Memory utilization kept increasing when running Dashboard and never went down.
- **dp03293** — ARP spoofs were always blocked. There was no “log only” function. ARP spoofs can now be logged only, if such is desired.
- **dp03111** — SMTP Anomalies USER\_TOO\_LONG and DOMAIN\_TOO\_LONG were not triggered.
- **dp02911** — Could not detect Shell Code when NNTP command line is greater than 512.
- **dp02874** — SMTP decoder didn't handle pcap without banner correctly.
- **dp02873** — FTP decoder didn't handle pcap without banner correctly.

## 6 Known Issues

---

This section describes known issues with the current release.

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

“Known Issues” describes deviations from intended product behavior in IDP 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.

## 6.1 Limitations of Features

- None.

## 6.2 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:”.

- **06705**—Copper Giga ports auto-negotiate speed even when set to a specific speed in ACM.
- **dp04276**—ACM accepts root passwords containing more than 20 characters, then truncates the password to 20 characters with no message.

W/A: Only use passwords of 20 characters or fewer.

- **dp04266**—Sensor may crash if connections go up and down rapidly over an extended period.
- **dp04246**—Policy push fails if Sensor or agent process restarts during policy push and compile.

W/A: Do not restart Sensor or agent process while policy is being pushed and compiled. If Sensor does crash, restart the idp and scioid processes.

- **dp04245**—Message "Failed to update device. Get unmatched correlation id in reply" appears in policy push.

If a policy update fails, this message may appear in the when the policy update is sent a second time. The system is unable to match the first policy push ID with the second.

W/A: Push policy again.

- **dp04242**—IDP 10 failed update under high traffic.

Push new policies during periods of low traffic.

- **dp04213**—On Dell 1550 (IDP 100) Sensor, agent sometimes doesn't start after upgrade from 3.2r1 to 4.0r1.

W/A: Some 1550 units do not have serial numbers embedded in the hardware. Contact JTAC.

- **dp04212**—Upgrade failed because of date mismatch.

W/A: Make sure Sensor has current date/time system setting before attempting upgrade.

- **dp04180**—CPU usage for processes shows 0%. Some processes are I/O intensive but not CPU intensive. As a result, Sensor may be busy, but not showing a CPU load.
- **dp04142**—Profiler database auto-purge may not work if Sensor disconnects from the server, then reconnects, during profiling.

W/A: Manually purge profiler database using the following commands:

```
# profiler.sh status
(should say stopped.)
# cd /usr/idp/device/var/profile
# ls -l
(print list of *.db files)
# rm -f *
# profiler.sh start
Profiler starts again.
```

- **dp04129**—Kernel panic if Sensor booted with USB keyboard.

W/A: USB devices not supported. Use console connection instead.

- **dp04105**—After upgrade to 4.0, Sensor agent may not start until device is initially added to NSM.

W/A: Add Sensor to NSM. Agent will start automatically.

- **dp04091**—3rd party HA with STP doesn't work in transparent mode when STP is enabled on the IDPs but not on the switches.

W/A: Enable STP on the Sensor *and* on switches connected to the Sensor. Or, enable STP on both switches, disable STP on the Sensor, and turn on Layer 2 Bypass for the Sensor.

- **dp04090**—The STP port status doesn't change when the interface goes down.
- **dp04081**—The HA logs are not consistent when IDPs are rebooted in Active/Active mode.
- **dp04036**—idpLogReader and pkid processes occasionally go off after upgrading the sensor.

W/A: Restart the processes.

- **dp03967/dp04227**—“Internal error” error message when trying to change ACM configuration. ACM files may have wrong file permissions.

W/A: The directory /root/public\_html and the files in it must have the following permissions or an error will occur. Make sure the directory and files have the permissions indicated here.

```
drwxr-xr-x  2 root  root    4096 Apr 19 17:18 .
drwxr-xr-x  5 root  root    4096 Apr 18 20:30 ..
```

-rwx-----	1	root	root	1392	Apr 18 20:30	mode25a.pl
-rwx-----	1	root	root	1300	Apr 18 20:30	mode25b.pl
-rwx-----	1	root	root	1585	Apr 18 20:30	mode30.pl
-rwx-----	1	root	root	2136	Apr 18 20:30	mode32.pl
-rwx-----	1	root	root	2795	Apr 18 20:30	mode43.pl
-rwx-----	1	root	root	1844	Apr 18 20:30	mode9.pl

- **dp03895**—On IDP 1000 with tg3 drivers, Peer Port Modulation does not bring interfaces back up after connection is restored if interfaces are set to 1000Mbps.
- **dp03881**—IDP failover from standby IDP back to primary IDP may take up to 45 seconds. (Initial failover, from primary to hot standby, is considerably faster.)

WA: One or both of these changes may improve failover times:

- Enable gratuitous ARP on both Sensors.

Add **:garp-unicast (1)** to the top of /usr/idp/device/cfg/schad.set

- Reduce CAM aging timeouts on the connected switches.
- **gl29223**—Secondary NSM server is not configured on the IDP Sensor when the device is added to NSM. Sensor disconnects from NSM if primary server fails over to backup.

W/A: Use ACM to specify secondary server for each Sensor.

## 7 Getting Help

---

For more 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 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.

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

**Writer:** Mark Schlagenhauf

