



# **Intrusion Detection and Prevention Release Notes**

*Release 4.0r4*  
*5-21-2007*

## ***Contents***

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 2
- 4 System Requirements on page 3
- 5 Addressed Issues on page 4
- 6 Known Issues on page 4
  - 6.1 Limitations of Features on page 4
  - 6.2 Known Issues on page 4
- 7 Upgrading Your Sensor on page 7
- 8 Getting Help on page 8

## **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 093-1841-000, 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.

Refer to the NetScreen-Security Manager Administrator's Guide and the IDP-NetScreen-Security Manager Migration Guide for descriptions of NetScreen-Security Manager and the migration process.

## 2 New Features

---

The following is a list of new features and enhancements.

- **Application Volume Tracking**—Application Volume Tracking (AVT) uses the Profiler to collect fine-grained traffic statistics aggregated over particular time intervals. These statistics can then be viewed using command line utilities or copied off the Sensor to be viewed by third-party reporting applications.
- **QuickStart**—First introduced in IDP 3.2r2, QuickStart quickly creates the most common configuration on your Sensor.
- **Coordinated Threat Control**—First introduced in IDP 3.2r2, this feature lets your Sensor send indicated logs to an IVE appliance.

## 3 Changes to Default Behavior

---

- The detector installed on the IDP will not be replaced during upgrade if the installed detector version is higher in comparison to the one in the 4.0r4 image.
- 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. Refer to the *IDP-NetScreen-Security Manager Migration Guide* for a complete description of the changes.
- The IDP-NSM migration procedures now also migrate the IVE One-Time Password (OTP). If no IVE OTP password was set in IDP 3.2r2, a warning message may appear indicating that the IVE OTP was not found. This message can be ignored if the OTP was never initially.
- IDP 4.0r2 Sensor software installer file shipped with NSM 2006.1r2. If you will be migrating Sensors from IDP 3.x, you need to replace this installer file using the following procedure:

1. Download the IDP 4.0r3 Sensor software from the Juniper Networks support site (sensor\_4\_0r3.sh).
2. Rename the file to agent\_4\_0\_r3.sh.  
  
`mv sensor_4_0r3.sh agent_4_0r3.sh`
3. gzip the file to produce agent\_4\_0r3.sh.gz.  
  
`gzip agent_4_0r3.sh`
4. Remove the earlier sensor file from /usr/netscreen/DevSvr/var/firmware on the NSM Device Server.  
  
`rm /usr/netscreen/DevSvr/var/firmware/agent_idp_4.0_linux_x86_rpm_opt.sh.gz`
5. Copy the new file agent\_4\_0r3.sh.gz to /usr/netscreen/DevSvr/var/firmware.  
  
`cp agent_4_0r3.sh.gz /usr/netscreen/DevSvr/var/firmware/.`

You can now run the migration as before. Refer to the *IDP-NetScreen-Security Manger Migration Guide 4.0r3* for complete instructions.

## 4 System Requirements

Juniper Networks supports the following upgrade paths to IDP 4.0r4:



**CAUTION:** If a migration is being performed from 3.2, it is recommended to migrate to 4.0r3. Although NSM 2006.1r2 comes bundled with 4.0r2, it is recommended to change the version to 4.0r3 before continuing with the migration as the license for 4.0r2 expired on October 16th, 2006. Instructions for changing the version can be found in the migration.

**Table 1: Migration/Upgrade Paths**

Existing Version	Migration/Upgrade Path
3.1r4	Can be directly migrated to 4.0r1 and then upgraded to 4.0r4.
3.2r3 and 3.2r4	Can be migrated to 4.0r3 and then upgraded to 4.0r4. Refer <i>IDP-NetScreen-Security Manager Migration Guide</i> for migration instructions.
4.0r1 and 4.0r3	Can be upgraded to 4.0r4 using the procedure in <i>Upgrading Your Sensor</i> on page 7.
Other versions	Upgrade IDP Sensor/IDP Management Server to support 3.1 (3.1r4) and 3.2 (3.2r3 or 3.2r4) versions and use suggested migration paths to upgrade to 4.0r4.

IDP Management Server is no longer supported with IDP 4.0. Instead, IDP Sensors are managed with NetScreen-Security Manager 2006.1 or later. 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:

- **cs12829**—IDP fails to pass HTTPS uploads greater than 1M .
- **cs12681**—Session table shows sessions with negative timeout values.
- **cs12469**—Lockup on Sun RPC Protocol.
- **cs12394**—Logviewer displays incorrect rule#.
- **cs12033**—Error while configuring the timezone in ACM.
- **cs11816**—Ack packets are dropped in IDP.
- **cs11678**—Kconst to allow valid ARP packets with all '0' as source IP.
- **cs11259**—IDP intermittently drops to bypass mode and never recovers back to normal mode until restart of the IDP services.
- **cs10915**—Support for Intel Pro/1000 GT Quad Card.
- **dp04149**—Daylight Saving Time change for 2007.

## 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

- Only pre-defined IDP services can be used in the Service column of a backdoor rulebase rule. ScreenOS services cannot be used. This is as designed, but it is not clear in the NSM GUI.
- Migrated custom and compound attack objects have unpopulated Category fields after migration. This is because IDP Manager did not support populating this field. After migration, the user should populate this field for all migrated custom and compound attacks.

### 6.2 Known Issues

The following are known issues 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:”.

- **cs13560**—IDP intermittently drops legitimate traffic due to TCP Reassembler memory overflow.

- **cs12807**—IDP hangs during detector update.

W/A: Please contact JTAC for a patch.

- **dp05089**—Standalone HA is not stable. This issue is seen only on IDPs with dual CPUs.

- **dp05086**—ACM does not validate netmask for ssh\nsnmp 'restrict networks'.

W/A: Use the correct netmask to restrict a network. To restrict a host use 32 as the netmask.

- **dp04419**—Using QuickStart to set Sensor to sniffer mode does not disable HA settings if HA was already configured.

- **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**—Crash detected on an IDP 50 platform when Ethernet interfaces went up and down frequently.

- **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 sciop processes.

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

If the policy update fails, this message may appear in the NSM jobmanager 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.

W/A: Push new policies during periods of low traffic.

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

W/A: Some 1550 units did 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 stop after Sensor upgrade and restart.

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 Upgrading Your Sensor

---

This procedure describes how to upgrade your sensor from IDP 4.0r1 or r3 to IDP 4.0r4. Refer to “System Requirements” in this document for supported migration/upgrade paths. If your sensor is running 3.x, refer to *IDP-Netscreen Security Manager Migration Guide* for instructions.

To upgrade your sensor from 4.0r1 or r3 to 4.0r4, do the following:

1. Upgrade your installation of NetScreen-Security Manager to 2006.1r2.
2. Download the Sensor software from [www.juniper.net/support](http://www.juniper.net/support).
3. Unplug the HA port cable, if one is attached.
4. Log into the IDP Sensor as **root** via the Console port.
5. Change directory to the `/tmp` directory.
6. From the Sensor, use FTP in binary mode to copy the file to the `/tmp` directory. Alternatively, you can use `scp` to copy the file.

---

**NOTE:** The Sensor does not run an FTP server, so you must FTP *from* the Sensor.

---

7. In a command shell, change directory to the `/tmp` directory:

```
cd /tmp
```

8. Make the UI install script executable by typing:

```
chmod 755 sensor_4_0r4.sh
```

9. Type **sh sensor\_4\_0r4.sh** and press **Enter**.

The Sensor update script runs.

10. Type **reboot;reboot** and press **Enter**.

11. When you have finished upgrading all the Sensors in the cluster, reconnect the HA cable.

12. After upgrading the Sensors, connect to the IDP ACM and apply a save configuration from the ACM.

13. In NSM, right-click on the Sensor in Device Manager and select **Adjust OS Version**. This will update the Sensor OS in the NSM database.

## 8 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:** Patricia Wright



