



Intrusion Detection and Prevention Release Notes

Release 4.1 ***04-24-2007***

Contents

- 1 Version Summary on page 2
- 3 New Features on page 2
- 4 Changes to Default Behavior on page 3
- 5 Addressed Issues on page 4
- 6 Known Issues on page 5
 - 6.1 Limitations of Features on page 5
 - 6.2 Known Issues on page 5
- 7 Upgrading Your Sensor on page 6
 - 7.1 Upgrade Considerations on page 6
 - 7.2 Upgrade Procedure 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

Part Number: 093-1854-000. Rev B.

1 Version Summary

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

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 Concepts and Examples Guide* for more information about NSM and IDP.

2 System Requirements

IDP Sensors have two onboard, Web-based configuration tools called the Appliance Configuration Manager (ACM) and QuickStart. These tools are supported on the following browsers:

- Internet Explorer 6.0 SP2
- Firefox 1.5, 2.0
- Netscape 7.2, 8.1.2

3 New Features

The following is a list of new features and enhancements.

- **Application Identification**—The Sensor applies attack objects to traffic based on application. The Sensor can identify a particular application, and therefore know which attack objects to use, in one of two ways:
 - by port
 - by inspecting the traffic stream to identify the application

Versions of IDP prior to 4.1 used the destination port to identify the application. IDP 4.1 and later also use the Application Identification feature, which allows the Sensor to identify applications running on non-standard ports and apply the correct attack objects.

NOTE: By default, Application Identification is enabled. Use NSM to disable it. To do so, open NSM, select **Edit Device > Sensor Settings**, uncheck the option **Enable application identification**, then click **OK**. Update the device when done.

- **Recommended Action**—In Version 4.1 only, attack objects now include an additional field. This field indicates what action Juniper Networks recommends the Sensor should take when traffic matches that attack object. In your rulebase, you can set the Action column to Recommended. This setting tells the security policy to take whatever action is recommended.

- **Recommended Policy**—In Version 4.1 only, the recommended policy contains just the attack objects recommended by Juniper Networks. Each rule is set to take the recommended action for the given attack object.

The NSM Add Device wizard loads the Recommended Policy onto all new IDP Sensors automatically.

- **Syslog support**—You can configure the Sensor to forward all device logs to a Syslog server.
- **Health Monitoring Alerts (Includes SNMP traps and polling)**—CPU, hard disk, memory, and session usage are tracked by the Sensor. For each resource, when 90% usage is reached, a log entry is sent to NSM. In addition, the Sensor can be configured to send an SNMP trap to an SNMP Manager when the 90% threshold is reached. Another log entry (and SNMP trap, if configured) is sent when the usage again drops below 90%.

If SNMP is configured, you can also poll the Sensor for the current usage of any of the resources.

- **Proxy server support for attack object update**—In NSM, the attack object update dialog lets you specify proxy server information.
- **IDP Firmware Update via NSM**—You can now use the regular NSM firmware update functionality to update your IDP Sensors.
- **Configurable NIC states**—For the IDP 50, 200, 600, and 1100 only. Copper ports only. You can now specify what state copper NICs should be set to when the Sensor is shut down gracefully, and what state the copper NICs should be set to when the Sensor becomes unavailable unexpectedly. Options include the following: Bypass, External Bypass, Normal, and NICs Off.
- **RADIUS support for ACM login**—You can provide access to ACM via RADIUS authentication.
- **VLAN support in rulebases**—Rulebases can now use VLAN tags as part of matching criteria in Transparent and Sniffer mode of IDP.

4 Changes to Default Behavior

This section lists changes to default behavior.

- Starting with IDP 4.1 the licensing has been changed. Customers can access the Juniper Networks License Management System (LMS), and provide the IDP serial number to obtain the permanent license keys for IDP.

To generate the license:

1. Log into your online CSC account.
2. Go to the LMS tool at https://support.juniper.net/generate_license.
3. Scroll down the page and select your product type.

4. Enter your serial number and select the **Generate** button.
- SNMP connectivity for a Sensor is now configured through NSM Device Manager instead of through ACM.

5 Addressed Issues

The following issues (listed alphabetically in reverse order) 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.
- **cs12444**—ACM access with a NAT IP is not working.
- **cs12033**—Error while configuring the timezone in ACM.
- **cs11444**—Issues with MSN decoder.
- **cs10915**—The quad card “Intel[R] PRO/1000 GT QUAD PORT Server Adapter” is not compatible with IDP Sensors. With the Intel[R] PRO/1000 GT QUAD PORT Server Adapter installed in the sensor, error messages appear when the kernel module is getting started. The drivers used by the Sensors do not support this quad card. Only applies to IDP 100, 500, and 1000.
- **cs08123**—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.)
- **dp04958**—After upgrading to the 4.1 release this issue can be found in the Report Settings window. If the user modifies settings in **Network/Host** table to update the configuration, SNMP polling/traps stops working.
- **dp04954**—When using the ACM wizard to configure NIC Bypass/OFF in IDP-50 the settings are not retained on the **Choose Forwarding Interfaces** page.
- **dp04938**—After upgrading to the 4.1 release this issue appears in the Report Settings window. In the **Network/Host** table, all allowed hosts are not retained if the allowed hosts were added in previous releases.
- **dp04937**—After upgrading to the 4.1 release this issue appears in the Report Settings window. The values of **SNMP Contact** and **SNMP Location** are truncated after the first space used in each field if either values were configured in previous releases
- **dp04824**—Sensor crashed due to PNG parser issue.
- **dp04814**—SNMP configuration allows community strings with spaces.
- **dp04811**—SNMPD sometimes does not restart after upgrade.
- **dp04810**—Log-viewer shows junk in Details column for IDP attacks.

- **dp04767**—tcpdump is not capturing packets in both directions.
- **dp04501**—If Sensor image is installed from CD, policy push fails if a new IDP Detector Engine has been loaded.
- **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.
- **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.
- **dp04090**—The STP port status doesn't change when the interface goes down.
- **gl32018**—After upgrade from IDP 4.0 to IDP 4.1, SNMP configuration info retained on Sensor, but not displayed in NSM. IDP 4.0 uses ACM to configure SNMP. IDP 4.1 uses NSM to configure SNMP. However, the information does not appear in NSM after upgrade.

6 Known Issues

This section describes known issues (listed alphabetically in reverse order) 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.

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:”.

- **cs12638**—Variable data is incorrectly displayed for “TCP S2C Exploit: Urgent Data Without Flags” anomaly.

- **cs06705**—Copper Giga ports auto-negotiate speed even when set to a specific speed in ACM.
- **dp05033**—IDP 4.1 is not supported on a small set of initial IDP-100 boxes with the OneSecure logo. Unsupported IDP 100 platforms have a label on the underside that says "Dell 1550 Poweredge server".
- **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 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.

- **dp04213**—On some Dell 1550 (IDP 100) Sensors, agent sometimes doesn't start after upgrade from 3.2r1 to 4.0r1.
- **dp04081**—The HA logs are not consistent when IDPs are rebooted in Active/Active mode.
- **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.

7 Upgrading Your Sensor

IDP 4.1r1 is supported only on NSM 2007.1.

7.1 Upgrade Considerations

Juniper Networks supports the following upgrade paths to IDP 4.1:

Table 1: Migration/Upgrade Paths

Existing Version	Migration/Upgrade Path
3.1 or 3.2	Must be migrated to IDP 4.0r1 or IDP 4.0r3, then upgraded to IDP 4.1. Refer to the IDP 4.0r1 or IDP 4.0r3 release notes for more information on upgrade paths supported and <i>IDP-NetScreen-Security Manager Migration Guide</i> for migration instructions.
4.0r1 or 4.0r3	Can be upgraded using the procedure in <i>Upgrading Your Sensor</i> on page 6.
Other versions	Upgrade IDP Sensor/IDP Management Server to a supported 3.2 version and use the suggested migration path to upgrade to 4.1.
NSM 2007.1	NSM 2007.1 does not support the migration of the IDP Sensor/IDP Management Server.

IDP Management Server is no longer supported with IDP 4.0 and later. 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.

7.2 Upgrade Procedure

This procedure describes how to upgrade your Sensor from IDP 4.0r1 to IDP 4.1 or IDP 4.0r3 to IDP 4.1. If your Sensor is running IDP 3.2r2, upgrade first to IDP 4.0r3 and then to IDP 4.1 or refer to the *IDP-NetScreen-Security Manager Migration Guide* for instructions.

NOTE: This procedure describes the traditional out-of-band upgrade method. With NSM 2007.1, you can also use the NSM Firmware Manager to upgrade your Sensors. Refer to the *IDP Concepts and Examples Guide* or the *NetScreen-Security Manager Administrator's Guide* for instructions.

To upgrade your Sensor from either IDP 4.0r1 or IDP 4.0r3 to IDP 4.1, use the steps in the following procedure:

1. Upgrade your installation of NetScreen-Security Manager to 2007.1.
2. Download the Sensor software from 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 or MGT port.
5. Change directory to the `/tmp` directory.
6. From the Sensor, use FTP 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 install script executable.
chmod 755 sensor_4_1r1.sh
9. Run the install script.
sh sensor_4_1r1.sh
10. Reboot the Sensor.
reboot;reboot
11. When you have finished upgrading the Sensors in the cluster, reconnect the HA cable.
12. 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. Use this step only if you are upgrading from 4.0r1 or 4.0r3.
13. Log into Juniper Networks License Management system (https://support.juniper.net/generate_license) and provide the IDP serial number to obtain a permanent license for IDP. The IDP serial number is displayed in the ACM and also in NSM.

8 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 © 2007 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

Writer: Patricia Wright