



Intrusion Detection and Prevention Release Notes

Release 4.1r2
10-23-2007

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 3
- 6 Known Issues on page 3
 - 6.1 Limitations of Features on page 3
 - 6.2 Known Issues on page 3
- 7 Upgrading Your Sensor on page 4
 - 7.1 Upgrade Considerations on page 4
 - 7.2 Upgrade Procedure on page 4
- 8 Getting Help on page 5

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1777-000 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

- Packet Data Logging support for IDP Sensor — This feature is a find-grain log provisioned by the IDP device and is a new functionality supported by standalone IDP devices to reduce management traffic from the sensor to NSM. The packet-data logs are detached from the normal generated logs, stored on the device in a separate file, identified with a unique ID, and are retrievable on demand.

This configurable feature when set tells the IDP to send packet-data as an integral part of the logs generated from the device. When not-set, the IDP sends the logs with a unique ID instead of the packet-data, and stores the packet-data on the device itself. The IDP supplies the unique-id to NSM, which in turn allows NSM to send a query to retrieve the packet-data when needed by the user.

This feature will only be supported in NSM 2007.3.

- Interface Aliasing — This feature allows logs to be generated with alias names instead of the physical interface names, which will help users not only identify the kind of attacks, but also the source division/interface.

As an example:

Before this feature, the log was:

```
< time > < src-IP > < des-IP > < port > < src-intf:eth2 > < dst-intf:null >
```

With Interface Aliasing:

```
< time > < src-IP > < des-IP > < port > < Engineering Div > < dst-intf:null >
```

This configurable feature provides only source interface details when configured in IDP deployment mode. It is currently supported only for physical interfaces and not for tagged interfaces.

Interface Aliasing is supported through ACM. On the ACM menu, set it on the “Reconfigure Network Interface Hardware” page. This page contains a new edit box next to the interface name, which allows you to set this optional feature. You can view the set alias on the “Detailed Configuration Report” page in ACM.

4 Changes to Default Behavior

- None

5 Addressed Issues

The following issues are addressed in this release

- 221422 — Populate “Src Intf” column in log viewer
- 223699 — Admin\Root password changes are logged in NSM.
- 223700 — NIC up/down status are logged in NSM.
- 226151 — Blocking custom application without logging: Out of flow memory.
- 233208 — Oracle DB Sync fails.
- 236209 — Policy push fails in IDP-100 (low-end)

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

There are no known issues for this release.

7 Upgrading Your Sensor

IDP 4.1r2 is supported only on NSM 2007.1 and above.

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, and 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>Upgrade Procedure</i> on page 4.
4.0r4	Can be upgraded using the procedure in <i>Upgrading your sensor</i> .
4.1r1	Can be upgraded using the procedure in <i>Upgrading your sensor</i> .
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 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 install script executable.
chmod 755 sensor_4_1r2.sh
9. Run the install script.
sh sensor_4_1r2.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: Paul Guersch