



Juniper Networks

Intrusion Detection and Prevention

Release Notes

Release 4.2r1

December 2008 (updated February 2009)

Contents

- 1 Version Summary on page 2
- 2 New Features and Enhancements on page 2
- 3 Compatibility on page 4
- 4 Changes to Default Behavior on page 6
- 5 System Requirements on page 7
- 6 Known Issues on page 7
- 7 Getting Help on page 9



NOTE: IDP Release 4.2r1 supports only the IDP 8200 platform.

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-023833-01

1 Version Summary

Juniper Networks Intrusion Detection and Prevention (IDP) sensors detect intrusions and prevent attacks on your network.

Juniper Networks NetScreen-Security Manager (NSM) 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 *Network and Security Manager Administrator's Guide* and the *IDP Concepts and Examples Guide* for more information about NSM and IDP.

2 New Features and Enhancements

IDP 8200 Appliance

This section briefly describes the new IDP 8200 appliance on which the IDP 4.2r1 sensor software is installed. See the *Installation Guide* for the IDP 8200 for more a detailed description of the appliance hardware and IDP system installation.

The IDP 8200 is optimal for large central sites or high-traffic areas. It features:

- 10 Gbps maximum throughput
- 5,000,000 maximum sessions
- Any combination of four modular I/O cards:
 - Four-port gigabit Ethernet (copper) with bypass
 - Four-port gigabit Ethernet (fiber SFP non-bypass)
 - Four-port gigabit Ethernet (fiber SX with bypass)
 - Two-port 10-gigabit Ethernet (SR-bypass)
- One RJ-45 Ethernet management port (10/100/1000 Mbps)
- One console serial port
- One USB port
- Hot-swappable redundant power supplies

For IDP 8200 appliances running software version 4.2r1, you must download and install an updated network driver patch to support the following I/O modules.

IDP-1GE-4SX-BYP	4-port 1 GigE SX fiber interface card with bypass
IDP-10GE-2SR-BYP	2-port 10 GigE SR interface card with bypass
IDP-10GE-2XFP	2-port 10 GigE XFP interface card (non-bypass)

For details, see “Installing IDP 8200 I/O Modules,” on the Juniper Networks IDP 4.2 technical documentation Web site.

New Features for IDP 4.2r1

On-box reporting—IDP release 4.2r1 provides on-box web-based reports with details top attacks, destinations, and sources. These reports are accessible from the ACM home page or through an HTTPS connection to the IDP appliance. Application volume tracking (AVT) reports are not supported in release 4.2r1.

You can access the IDP Reporter user interface with the following browsers:

- Internet Explorer 6.x, 7.x
- Mozilla Firefox 2.x

NOTE: IDP Reporter does not support Mozilla Firefox 3.x.

For more information, see the *IDP Reporter User's Guide*.

3 Compatibility

This section provides information about updates required to complementary Juniper Networks products to ensure compatibility with IDP 4.2.

Schema Update

Your version of Network and Security Manager (NSM) might require a schema update to support your IDP platform and software version. The schema update is also known as forward support.

Check your NSM release notes for the latest version support for IDP devices.

At the time of this release, NSM 2007.3r2 support for the IDP 8200 platform and IDP 4.2r1 software version requires a schema update before you can add the IDP devices to the NSM Device Manager.

To download the schema update files, go to <http://www.juniper.net/customers/support/>.

See the following section for procedures on installing the schema update.

Downloading the Schema Update Installation Files

The schema update installation package for IDP release 4.2r1 includes the following files:

- nsm2007.3r2_schema_update_server.zip
- nsm2007.3r2_schema_update_ui_win.zip
- nsm2007.3r2_schema_update_ui_linux.zip

Installing the Schema Update on the Management System

To install the schema update on the management system (standalone configuration: GUI Server and Device Server on the same computer):

1. Log in to the management system computer as root.
2. Navigate to the directory where you saved the management system installer file and load the schema update file. It is recommended that you save the schema update file in the `/tmp` subdirectory.
3. Unzip the schema update. For example, type the following command:

```
unzip nsm2007.3r2_schema_update_server.zip
```

4. Run the schema update. For example, type the following command:

```
sh nsm2007.3r2_schema_update_server.sh
```

The update begins automatically. During the update process, the installer stops and restarts the management system.

If you are running NSM on a management system in the extended configuration (GUI Server and Device Server on separate computers), you must load and run the schema update on both computers where you have installed the GUI Server and Device Server. You can use the procedure described in this section to update the GUI Server and Device Server.

Installing the Schema Update on the Client

After you have installed the schema update, you must install the schema update on all your UI clients.

To install the schema update on the client:

1. Log in as an Administrator user on the computer where you are installing the UI.
2. Download the schema update file in the same location where you have installed the UI.
3. Unzip the schema update file.
4. Run the schema update.
 - If you are upgrading the UI on a Windows-based PC, double-click the installer executable.
 - If you are upgrading the UI on a Linux-based computer, launch it from a command line using the following command:

```
sh nsm2007.3r2_schema_update_ui_linux.bin
```

Verifying that Forward Support is Installed Properly

To verify that you have installed forward support properly, view NSM UI client login window and verify that the installed version number is displayed. You can also use the Help menu option to view the installed patch version number.

Detector and Attack Objects Update

After you have installed IDP device in your equipment rack, run the initial setup, and added IDP to NSM, you must update to the the latest IDP detector engine and attack object database.

To update the detector and attack objects database:

5. Download the latest detector and attack database to the NSM GUI server.

From NSM, select **Tools > View/Update NSM attack database** and complete the wizard steps.
6. Push the detector update to IDP devices.

From NSM, select **Devices > IDP Detector Engine > Load IDP Detector Engine** and complete the wizard steps.

7. Push a policy update to IDP devices.

From NSM, select **Devices > Configuration > Update Device Config** and complete the wizard steps.

4 Changes to Default Behavior

The following changes have been made to the default behavior of features related to traffic interfaces:

- NIC state **Normal state** has been deprecated. For networks where you do not want the appliance to enter bypass in the event of failure or shutdown, specify NIC state **NICs off** instead.
- In transparent mode, you can enable both NIC bypass and peer port modulation (PPM).

Note: The NIC state setting is related to the *health of the IDP operating system*. In transparent mode, if the IDP operating system encounters failure or is shut down, it cannot reset the interface bypass timer. When the timer expires, the IDP interfaces are turned off, form internal bypass, or trigger an external bypass unit, according to the NIC state setting. This happens regardless of the health of the link or the setting for PPM.

Note: The PPM feature is related to the *health of the link* when the IDP operating system is healthy. In a virtual router, if the status of one link is down, the PPM daemon brings the other link down as well. This happens regardless of the setting you specify for NIC state. Note also that PPM is an IDP process. If the IDP operating system is unavailable because of failure or because it has been shut down, the PPM feature is also unavailable.

- The default value of the bypass watchdog loop reset interval (the `nicBypass.loopInterval` setting in the `idp.cfg` file) was changed from 1 second to 200000 microseconds (.2 seconds).

The following features are not supported in IDP 4.2r1:

- Backdoor protection
- Honeypot
- SSL decryption
- GRE, GTP, IP-IP
- Profiling features, including AVT and OSFP
- Bridge, router, and proxy-ARP deployment modes
- High availability
- External Bypass unit
- Packet capture (packet logging)

5 System Requirements

IDP devices 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 or 2.0
- Netscape 7.2 or 8.1.2

6 Known Issues

This section describes known issues at the time of this release.

- **278471**—"scio ccap all" is not supported (as the profiler feature is currently not supported).
- **278695**—Interface hardware speed/duplex settings are not retained on the sensor after reboot.

Work around: In `/usr/idp/device/bin/user_funcs`, set the interface speed/duplex settings for each interface. For example:

```
user_start_begin ()
{
    # To change the duplex/speed of the onboard NIC like eth0 and eth1,
    # uncomment out the following two lines
    ethtool -s eth2 autoneg off
    ethtool -s eth2 speed 100 duplex full
}
```

- **279408**—UDP port scanning works if there is no response from the Victim PC. But if the response comes in the form of "UDP Port not reachable," the detection ignores the flow because the response packet is more than 20 bytes (default value).

Work around:

1. In NSM, in the device list, double click the name of the device to display the Device dialog box.
 2. Select **Sensor Settings**.
 3. Click the **Run-time Parameters** tab.
 4. Under Traffic Signatures, increase the value for **Byte threshold for suspicious flows**.
- **286020**—In ACM, the default interface setting for all interfaces that support bypass is "NIC OFF"; but for 10 GigE with bypass, the default is "NIC Bypass."
 - **286327**—When an appliance is loaded with 1 GigE IOC without bypass, the ACM page displays the NIC State-Bypass drop-down menu. (It should not list the NIC State-Bypass drop-down menu, as it does not support NIC Bypass).

- **287003**—External Bypass is not supported in 4.2r1, but ACM list this option.
- **287179**—The very first NIC Bypass/NIC OFF logs do not appear in NSM.
- **288030**—After a policy push, “Unknown application...” messages might appear in NSM job window (depending on the policy that is pushed).
- **288644**—Inconsistent “NIC OFF” logs (for non-sniffing IFs) when the device is in Sniffer mode.
- **288651**—“NIC OFF” log messages are displayed for interfaces that are not selected as forwarding interfaces.
- **288662**—Reboot in sniffer mode brings interfaces down and attack detection stops.

Work around: You must use ACM to reconfigure the device in Sniffer mode.

Note: IDP 8200 with either 10 GigE IOC or with 1 GigE fiber with bypass IOC does not encounter this problem after installing the updated network driver patch. For details, see “Installing IDP 8200 I/O Modules,” on the Juniper Networks IDP 4.2 technical documentation Web site.

- **288663**—Link status (up/down) messages do not appear when the device comes up.
- **288824**—Under high traffic conditions, the following exception messages are displayed in the console:

```
ata1.00: exception Emask 0x2 SAct 0xfe SErr 0x400000 action 0x2 frozen
ata1.00: (spurious completions during NCQ issue=0x0 SAct=0xfe
FIS=005040a1:00000001)
ata1.00: cmd 61/30:08:8d:6e:16/00:00:00:00/40 tag 1 cdb 0x0 data
24576 out
res 50/00:38:a5:70:16/00:00:00:00/40 Emask 0x2 (HSM violation)
```

Work around: You can safely ignore these messages.

- **288997**—The IDP 8200 appliance 10 GigE IOC does not support peer port modulation (PPM).
- **290280**—When the device is under high stress, SSH/Console access to IDP via the management interface might freeze when checking flow table entries via sctop or scio.
- **298918**—ACM does not reject poorly formed alias names. In particular, ACM does not reject constructions with incomplete double-quote strings. For example, “hello (missing end-quote). As a result, the alias name does not appear in NSM.

Work around: When using ACM, be careful to use complete double-quote constructions for alias names. For example, “hello”.

- **299413**—After installing I/O modules, if the number of interfaces is fewer than six, you might encounter ACM or console messages indicating “cannot find eth6 and eth7.” You can safely ignore these messages. To resolve them so the event is no longer reported:

1. In NSM, edit the policy and verify that only the existing interfaces are set.
2. Push a policy update to the sensor.

The policy update synchronizes the configuration with the new hardware.

- **299514**—The ACM online help for Choose Forwarding Interfaces options needs to be revised to remove internal comments to reviewers. Please disregard the two messages in red text beginning with “ < < REVIEWERS:”.
- **299531**—The ACM online help for Configure Network Interface Hardware options needs to be revised to list support for 10 GigE interfaces. You configure the 10 GigE interfaces as you would other network interfaces. As with other network interfaces, we recommend you specify auto negotiation for speed and duplex.

7 Getting Help

For more assistance with Juniper Networks products, visit www.juniper.net/support. Juniper Networks occasionally provides maintenance releases (updates and upgrades) for IDP firmware. To have access to these releases, you must register your IDP device with Juniper Networks at the above web address.

Copyright © 2008 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

