



# Juniper Networks

## Intrusion Detection and Prevention

### Release Notes

*Release 4.1r2a*

*June 2008 (updated February 2009)*

#### *Contents*

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



**NOTE:** IDP 50, 200, 600, and 1100 cannot be upgraded to 4.1r2a. This release supports only the new IDP 75, IDP 250, and IDP 800 platforms.

---

#### **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://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 *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 or 2.0
- Netscape 7.2 or 8.1.2

## 3 New Features and Enhancements

---

### ***IDP 75, 250, and 800 Appliances***

This section briefly describes the new IDP 75, 250, and 800 appliances on which the IDP 4.1r2a sensor software is installed. See the *Installation Guide* for the IDP 75, 250, and 800 for more detailed descriptions of the appliance hardware and IDP system installation.

#### **IDP 75**

The IDP 75 appliance is optimal for small networks or low-speed network segments. It features:

- 150 Mbps maximum throughput
- 10,000 maximum sessions
- Two RJ-45 Ethernet ports (10/100/1000 Mbps) with bypass
- One RJ-45 Ethernet management port (10/100/1000 Mbps)
- One console serial port
- One USB port

## **IDP 250**

The IDP 250 appliance is optimal for medium central sites or large branch offices. It features:

- 300 Mbps maximum throughput
- 70,000 maximum sessions
- Eight RJ-45 Ethernet ports (10/100/1000 Mbps) with bypass
- One RJ-45 Ethernet management port (10/100/1000 Mbps)
- One dedicated RJ-45 Ethernet High Availability (HA) port (10/100/1000 Mbps)
- One console serial port
- One USB port

## **IDP 800**

The IDP 800 is optimal for medium-to-large central sites or high-traffic areas. It features:

- 1 Gbps maximum throughput
- 500,000 maximum sessions
- Ten RJ-45 Ethernet ports (10/100/1000 Mbps) with bypass
- One RJ-45 Ethernet management port (10/100/1000 Mbps)
- One dedicated RJ-45 Ethernet High Availability (HA) port (10/100/1000 Mbps)
- One console serial port
- One USB port
- Hot-swappable redundant power supplies

In this release, IDP 800 supports the following Modular I/O Cards as traffic interfaces:

- 4-port GE Copper with Bypass (IDP-1GE-4COP-BYP)
- 4-port GE Fiber with Bypass (IDP-1GE-4SX-BYP)
- 4-port GE Fiber without Bypass (IDP-1GE-4SFP)

### ***New Features for IDP 4.1r2a***

**On-box reporting**—IDP release 4.1r2a provides on-box web-based reports with details of 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 unavailable with this release.

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.

## 4 Compatibility

---

### Schema Update

Your version of Network and Security Manager (NSM) might require a schema update to support your IDP platform and software version.

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 75/250/800 platform and IDP 4.1r2a 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 4.1r2a 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.

### ***Attack Object/Detector Update***

You must update your Attack objects and the Detector to the latest version before you install a Security Policy. Detector Updates commonly include support for new protocols, anomalies, contexts, and false positive fixes. It is extremely important that you complete the Detector update and Attack update process immediately after installing your IDP system.

To update the detector engine, run the NSM GUI client and select **Devices > Load IDP Detector Engine**.

## 5 Known Issues

---

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

- **272782**—ERROR: /bin/insmoed exited abnormally! seen on console message.  
  
Workaround: Ignore the error message.
- **274182**—When coordinated threat control is used, the log suppression feature needs to be disabled in the IDP to use with UAC, as IDP does not send the repeat count in the logs to UAC.
- **275963** – The IDP 800 appliance with 1 GigE fiber IOC without bypass does not support peer port modulation (PPM).
- **277536**—When a policy has a large number of attacks under high traffic conditions, the IDP's CPU utilization increases to over 50%. Running `tcpdump` on the management interface shows the traffic flowing through the IDP, giving an impression that the traffic is leaking into the management network.
- **285445**—When “NIC OFF” is configured under “Graceful shutdown” option on the device, and when an interface goes down and comes back, the “Link down” log message appears in the log viewer but the corresponding “Link up” log is not seen or is seen only for one interface in the forwarding interface pair.
- **285447**—Link Up/Link Down log messages are not seen when an interface pair is configured for NIC BYPASS.
- **285452**—When a pair of interfaces is configured for NIC bypass, the NIC-specific logs are inconsistent; sometimes the logs identify the bypass status of just one interface in the pair, and other times the logs identify the bypass status of both interfaces in the pair.
- **285479**—During policy push, “Unknown application...” related messages may appear in job information window.
- **285755**—“NIC Normal” log messages are seen for interfaces that are not selected as forwarding interfaces.
- **285757**—“NIC OFF” log messages are seen for interfaces that are not selected as forwarding interfaces.
- **286034**—When multiple policies are loaded and flows are created with `kconst sc_policy_load_on_flow_reset disable` and then a policy is unloaded, `sctop` throws error message `sc_flow_service_lookup: sc_klib_get_svcmap() failed`.

## 6 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 © 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](http://www.juniper.net)

