



IDP

## Release Notes

***Release 3.2r2***

***2-27-06***

### ***Contents***

- 1 Version Summary on page 2
- 2 New Features on page 2
- 3 Changes to Default Behavior on page 2
- 4 Addressed Issues on page 2
- 5 Known Issues on page 3
  - 5.1 Limitations of Features on page 4
  - 5.2 Compatibility Issues on page 4
  - 5.3 Known Issues on page 4
- 6 Installing the Update on page 4
- 7 Getting Help on page 6

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

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 093-1782-000

## 1 Version Summary

---

This release contains updates for the IDP Sensor, IDP User Interface, and IDP Management Server. This release contains new features, as described below.

This release runs on the IDP 10, 50, 100, 200, 500, 600, 1000, and 1100. Though the *IDP 3.2r2 Installer's Guide* only covers IDP 50, 200, 600, and 1100 hardware, the software instructions are also applicable to the IDP 10, 100, 500, and 1000 Sensors.

## 2 New Features

---

The following is a list of new features and enhancements.

- **IVE Signaling** - Allows an IDP Sensor to send relevant log information to an IVE appliance.
- **QuickStart** - An add-on to the ACM, allows a new Sensor to be configured more quickly. The *IDP Installer's Guide* covers the QuickStart feature in *Chapter 4: Configuring the IDP Sensor*.

## 3 Changes to Default Behavior

---

- Opening a web browser to the Sensor (<https://sensorIPAddress>) no longer takes you directly into ACM. Now, the Sensor displays a page that lets you choose between ACM and the new QuickStart feature. The *IDP Installer's Guide* covers the QuickStart feature in *Chapter 4: Configuring the IDP Sensor*.

## 4 Addressed Issues

---

The following issues are addressed in this release:

- **07936** – IDP in Sniffer mode did not re-tag the VLAN packet when sending the TCP RST.
- **07714** – IDP Logs showed the destination IP as 0.0.0.0 if the same attack is matched multiple times.
- **07634** – ARP spoofs were reported as being dropped even though ARP spoofing was turned off. This happened when customer used a VR other than the default.
- **07485** – Update Attack 407 failed in 3.1r3.
- **07329** – Traffic flows through when NIC Bypass feature was disabled.
- **07311** – Src and Dst port swapped in Packet capture of Honeypot Impersonated.
- **07182** – LogWalker process stopped unexpectedly after an attack update.
- **07176** – ACM did not configure sniffer reset port back to default.

- **07038** – Sensors in active-passive HA mode sometimes dropped FTP ACK packets if both receive client-side packets but only one receives server-side packets.
- **06884** – RX drops and errors on sniffing interface of Fibre NIC.
- **06881** – Collisions and Errors on Interface when speed/duplex hard coded.
- **06668** – When detecting IP spoofing, logviewer and exported log didn't show Src IP address.
- **06581** – Time binding function of compound attack did not work.
- **06365** – Detecting and Dropping (drop packet) Mytob WORM (WORM: Mytob DNS Activity) caused ALL subsequent and normal DNS traffic from the source to be dropped.
- **05589** – Memory utilization kept increasing when running Dashboard and never went down.
- **dp03293** — ARP spoofs were always blocked. There was no “log only” function. ARP spoofs can now be logged only, if such is desired.
- **dp03111** — SMTP Anomalies USER\_TOO\_LONG and DOMAIN\_TOO\_LONG were not triggered.
- **dp02911**— Could not detect Shell Code when NNTP command line is greater than 512.
- **dp02874** — SMTP decoder didn't handle pcap without banner correctly.
- **dp02873** — FTP decoder didn't handle pcap without banner correctly.

## 5 Known Issues

---

This section describes known issues with the current release.

Section 5.1 “Limitations of Features” identifies features that are not fully functional at the present time, and are not supported for this release.

Section 5.2 “Compatibility Issues” describes known compatibility issues with other products, including but not limited to specific Juniper Networks' appliances, Internet browsers, and other vendor devices. Whenever possible, information is provided for ways to avoid the issue, minimize its impact, or in some manner work around it.

Section 5.3 “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.

### 5.1 *Limitations of Features*

- None.

### 5.2 *Compatibility Issues*

- None.

### 5.3 *Known Issues*

The following are known deficiencies 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:".

- 8766: Unable to use a custom service object as a filter for dynamic groups.
- 8611: IDP Scheduler fails to run automatically when the DISPLAY is defined as :5.0.

W/A: Export the DISPLAY environment variable as IP\_Address:6.0.

- 8123: IDP standalone HA failover times varies as the IDP does not send gratuitous ARP.
- 7965: The Source and destination IP Address are swapped for the log that detects the "HTTP Invalid: Invalid Value in Header Field" attack.
- 7922: Maximum policy versions that can be stored are 999.

W/A: Select the Policy and Save As a new policy and update the new policy to the device when the policy versions reach 999.

- 7949/7664: Attack Object version is not updated when the signatures are updated using Local.
- 7914: The CSV file has a mis-formatted output when the attack log for the "HTTP:OVERFLOW:CONTENT-OVERFLOW" attack object is present.
- 7896: Unable to delete an object from a custom static group.
- 07824 — On Solaris Management Server, Profiler fails to properly sync with the IDP Manager.
- 07644 — Attack Update window not displayed correctly when "emulate Windows XP" is selected from 'Tools > Preferences > Look & feel' tab.

W/A: Don't select "Emulate Windows XP" look & feel option.

## 6 Installing the Update

---

You must upgrade the IDP system components in the following order:

1. Upgrade the IDP Sensor software
2. Upgrade the IDP Management Server software

3. Upgrade the IDP UI software
4. Update attack objects

Use the following files to upgrade your system to IDP 3.1r3. You can also use these files to do new installations:

- `sensor_3_2r2.sh`: Sensor upgrade/installation script
- `mgtsvr_linux_3_2r2.sh`: Management Server upgrade/installation script, Linux version
- `mgtsvr_solaris_3_2r2.sh`: Management Server upgrade/installation script, Solaris version
- `install_3_2r2.exe`: UI upgrade/installation script, Windows version
- `install_3_2r2.bin`: UI upgrade/installation script, Linux version

For detailed information on upgrading IDP software, see the *IDP Upgrade Guide*.

## 7 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:** Mark Schlagenhauf



