



IDP

Release Notes

Release 3.2 r5

07-23-07

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
- 6 Upgrading Your Sensor on page 3
- 7 Getting Help on page 4

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-021865-01

1 Version Summary

This release contains updates for the IDP 3.2 software release.

2 New Features

- None.

3 Changes to Default Behavior

- None.

4 Addressed Issues

The following are issues have been addressed in this release.

- **213120**—False Positive for SSL: Invalid Client Hello Message Data
- **213780**—For Dell Platform: Support for Intel Pro/1000 GT quad card
- **215552**—False Positive for IKE: TCPDUMP Identification Payload Underflow
- **218264**—False Positive for PORTMAPPER: Call it and PORTMAPPER: Short Read
- **218454**—Kconst to allow valid ARP packets with all '0' as source IP
- **218939**—False Positive for SMTP: INVALID-FILENAME
- **219934**—ACK packets are dropped by IDP when it detects a half-closed connection
- **221358**—Daylight saving time change for 2007
- **222540**—Lockup for sunrpc protocol
- **223637**—IDP fails to pass HTTPS uploads greater than 1M
- **226152**—IDP drops custom applications due to TCP reassembler memory overflow
- **227055**—IDP drops legitimate HTTP/HTTPS traffic for large http downloads. This problem is also seen for other protocols when downloading large files.
- **227446**—UTF-8 parser update: HTTP content scanning system full-width/half-width Unicode encoding bypass. Various HTTP content scanning systems fail to properly scan full-width/half-width Unicode traffic. This can allow malicious HTTP traffic to bypass content scanning systems.

5 Known Issues

There are no new known issues with the 3.2 r5 release. For a list of previously detected issues, see the 3.2 r4 release notes.

6 Upgrading Your Sensor

6.1 Upgrade Considerations

Juniper Networks supports the following upgrade paths to IDP 3.2 r5:

Table 1: Migration/Upgrade Paths

Existing Version	Upgrade Path
3.1 r4	Can be upgraded to 3.2 r5.
3.2 r4	Can be upgraded to 3.2 r5.
3.2 r4a	Can be upgraded to 3.2 r5.

Refer to the next section and the *IDP-NetScreen-Security Manager Migration Guide* and the *NetScreen-Security Manager Installer Guide* for detailed installation about requirements and procedures.

6.2 Upgrade Procedure

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. You can also use these files to do new installations:

- `sensor_3_2r5.sh`: Sensor upgrade/installation script
- `mgtsvr_linux_3_2r5.sh`: Management Server upgrade/installation script, Linux version
- `mgtsvr_solaris_3_2r5.sh`: Management Server upgrade/installation script, Solaris version
- `install_3_2r5.exe`: UI upgrade/installation script, Windows version
- `install_3_2r5.bin`: UI upgrade/installation script, Linux version
- `install_scheduler_3_2r5.bin`: IDP Scheduler, Linux version. See the *IDP Concepts and Examples Guide* for more information.

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

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: Claudette Hobbart