



Intrusion Detection and Prevention

Upgrade Guide

Release 3.2r2

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 093-1781-000

Copyright Notice

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.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writer: Mark Schlagenhauf

Overview

This guide describes the steps required to upgrade your Juniper Networks Intrusion Detection and Prevention (IDP) system to 3.2r2.

The Upgrade Process

You can upgrade the following versions to IDP 3.2r1 using the method described in this guide.

- IDP 3.0r4
- IDP 3.0r5
- IDP 3.1r2
- IDP 3.1r3
- IDP 3.2r1

For upgrades from IDP 2.X, please follow the instructions in *Upgrading the IDP System 2.0*, available for download from the Juniper Networks Support Web site at www.juniper.net/support.

To replace your existing IDP installation, please contact customer support.

Upgrade procedures do not depend on configuration or deployment-specific information. The upgrade process consists of four steps:

1. Upgrading the Sensor software on the IDP Sensor
2. Upgrading the Management Server software
3. Installing a new version of the IDP User Interface
4. Updating the Attack Object database

It is important to upgrade your IDP system in the order described. You must upgrade your Sensors first, then upgrade your Management Server, to avoid loss of connectivity.

You can download the upgrade software for the IDP Sensor, IDP Management Server, and the IDP User Interface from the Juniper Networks Support Web site at www.juniper.net/support. Patched or updated versions of the upgrade files may use different file names than those specified in this guide.

Because the 3.2 Attack Object database was enhanced with new data fields and information, **you must update your Attack Objects before you can install Security Policies on 3.2 IDP Sensors** if you are upgrading from a release prior to IDP 3.2r1. For instructions on updating your Attack Objects, see “Step 4: Update the Attack Object Database” on page 5.

Step 1: Upgrade the IDP Sensor Software

The first step in upgrading your IDP system to 3.2r2 is to upgrade each IDP Sensor with the new version of the IDP Sensor software. If a previous version of the IDP Sensor software is not installed on the IDP Sensor, the upgrade terminates and an error message appears.

NOTE: You must upgrade the Sensor software on each IDP Sensor in your network before upgrading the Management Server software.

You can perform the upgrade from a local system console (recommended) or use an SSH connection.

To upgrade the Sensor software:

1. Verify that you have SSH enabled for the Management Port.
To enable SSH, select **Modify SSH Access** from the ACM home page and follow the prompts.

Access ACM by pointing a web browser at `https://<sensorIPaddress>`.

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 port.
5. Change directory to the `/tmp` directory.
6. From the Sensor, FTP the file to the `/tmp` directory.

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 UI install script executable by typing:

```
chmod 755 sensor_3_2r2.sh
```

9. Type `sh sensor_3_2r2.sh` and press **Enter**.

The Sensor update script runs.

Reboot the device when the script is finished.

10. Type `reboot;reboot` and press `Enter`.
11. When you have finished upgrading all the Sensors in the cluster, reconnect the HA cable.

Proceed to Step 2: Upgrade the Management Server.

Step 2: Upgrade the Management Server

The second step in upgrading your IDP system to 3.2r2 is to upgrade to a new version of the IDP Management Server software.

NOTE: Juniper Networks recommends that you use a secure and trusted Red Hat Linux 7.2 or 8, RHEL AS/ES/WS 3, or Solaris 8 or 9 computer when running the IDP Management Server software.

The server must have 512 MB of RAM. 1 GB RAM is recommended. If you will be running the IDP Scheduler on the same box as the Management Server, 2 GB RAM are recommended.

To upgrade the Management Server:

1. Download the appropriate Management Server software (Linux or Solaris) from the Juniper Networks Support Web site at www.juniper.net/support.
2. Copy the file to the `/tmp` directory of the machine on which the Management Server is installed.
3. In a command shell, change directory to the `/tmp` directory:

```
cd /tmp
```

4. Make the UI install script executable by typing:

For Linux, type: `chmod 755 mgtsvr_linux_3_2r2.sh`

For Solaris, type: `chmod 755 mgtsvr_solaris_3_2r2.sh`

5. In a command shell, run the Management Server upgrade script:

For Linux, type: `sh mgtsvr_linux_3_2r2.sh`

For Solaris, type: `sh mgtsvr_solaris_3_2r2.sh`

The upgrade begins automatically, and several messages appear to confirm the upgrade progress. After the Management Server upgrade process is complete, the Management Server processes automatically start.

Proceed to Step 3: Install the User Interface.

Step 3: Install the User Interface

The third step in upgrading your IDP system to 3.2r2 is to install a new version of the User Interface. The UI must be upgraded to IDP 3.2r2 to work with your IDP 3.2r2 Management Server. You can download the UI upgrade executables for Windows or Linux versions from the Juniper Networks Support Web site at www.juniper.net/support.

NOTE: You must install the UI on a system with a minimum of 512 MB of RAM. The UI does not run on systems with less than 512 MB of RAM.

Installing on a Windows Computer

1. Make a note of your existing UI preferences (Tools> Preferences). You will have to reset them after the upgrade.
2. Ensure that you are an Administrator user for the computer that you are installing the UI on. For instructions on adding users to the Administrator group, please see your OS manual.
3. Download the Windows UI software `install_3_2r2.exe` from www.juniper.net/support.
4. Uninstall the previous version of the UI.

Use **Start> Program Files> Control Panel> Add or Remove Programs**

5. To install the new version of the UI, double-click **install_3_2r2.exe**.
6. Follow the directions in the UI Installer dialog boxes to install the UI.

Installing on a Linux Computer

You can install the UI on a computer running Red Hat Linux 7.2 or 8, or RHEL AS/ES/WS 3.

1. Download the Linux UI software `install_3_2r2.bin` from www.juniper.net/support. Copy the UI install script to the `/tmp` directory.
2. In a command shell, change directory to the `/tmp` directory:

```
cd /tmp
```

3. Make the UI install script executable by typing:

```
chmod 755 install_3_2r2.bin
```

4. Run the UI install script by typing:

```
/tmp/install_3_2r2.bin
```

5. Follow the directions in the UI Installer dialog boxes to install the UI.

By default, the UI will be installed in a **Juniper_Networks** directory within the home directory of the user that is installing it. You can specify a different directory during the installation procedure.

6. When prompted for a Web browser, you can change the default location of your Web browser. Click **Choose** to display the Web browser dialog box.
7. In **Enter path or folder name**, enter the full path to the Web browser application and click Update.

A list of directories and files for the specified location displays. Specify your Web browser using one of the following methods:

- Choose your Web browser from the list and click **OK**, or
- In **Enter file name**, enter the name of the Web browser and click OK.

Opening the User Interface after Upgrading

When you open the User Interface for the first time after installing a new version of the UI, you must specify the following information to log in:

- **Host Name.** This is the IDP Management Server you want to connect to.
- **User Name.** The default user name for new UI installations is **admin**.
- **Password.** The default password is the password you specified when you originally installed the Management Server.

NOTE: Passwords and user names are case sensitive.

After logging in, reset your preferences in Tools> Preferences.

Proceed to Step 4: Update the Attack Object Database.

Step 4: Update the Attack Object Database

The fourth and final step in upgrading your IDP system is updating your Attack Object database. **You must update your Attack Objects before you can install a Security Policy on your 3.2 IDP Sensors if you are upgrading from a version prior to 3.2r1.** In any case, it is a good idea to upgrade your attack objects before pushing a policy. The Attack Update Client automatically appears the first time you open the IDP UI after upgrading. Do not cancel the update client.

NOTE: It is extremely important that you complete the Attack Update Client process immediately after upgrading your IDP system. The update includes several new predefined dynamic groups that are used in the Security Policy templates. The Attack Update Client will continue to automatically appear each time you open the IDP UI until you complete the Attack Object Update procedure.

Follow the instructions in the update client to search your existing Attack Object database and automatically download new or modified Attack Objects. Updates commonly include:

- Additional signature Attack Objects and removal of obsolete Attack Objects
- Modification of descriptions, severities, or signature attack patterns for existing Attack Objects
- Additional predefined dynamic groups

Juniper Networks provides new signature Attack Objects each week, so remember to update your Attack Objects frequently. To manually update your Attack Objects, select **Tools > Update Attacks** from the menu bar of the User Interface, then follow the instructions in the Attack Update Client wizard.

Congratulations!

You have successfully upgraded your IDP system. For further instructions on using your IDP system, use the IDP *Online Help* in the IDP User Interface. For detailed, step-by-step instructions on setting up and fine-tuning your IDP system, see the *Intrusion Detection and Prevention Concepts & Examples Guide*.

If you experienced problems during this upgrade or have an upgrade issue you want to discuss, we strongly encourage you to contact Juniper Networks customer support at support@juniper.net, or at 1-888-314-JTAC (within the United States) or + 1-408-745-9500 (from outside the United States). For general information about known issues, IDP versions, and the IDP FAQ, visit the Juniper Networks Support Web site at www.juniper.net/support.