Copyright Notice

Copyright © 2004 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Security Manager, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

This product includes software developed by SSHTools (http://www.sshtools.com/).

Information in this document is subject to change 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:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

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 NETSCREEN REPRESENTATIVE FOR A COPY.
# Contents

Preface ........................................................................................................................................... vii

Organization ............................................................................................................................... viii

Other Technical Publications ...................................................................................................... ix

Introduction .................................................................................................................................. 1

Installation Process Overview ..................................................................................................... 2
  Management System Install Process .......................................................................................... 2
  User Interface Install Process ................................................................................................... 2

Installation Package .................................................................................................................... 3

Minimum System Requirements ................................................................................................. 4
  System Requirements - Management System ......................................................................... 4
  System Requirements - User Interface ...................................................................................... 5

Configuration Options ................................................................................................................. 6
  Typical Configuration .............................................................................................................. 6
  Extended Configuration .......................................................................................................... 7

Next Steps ................................................................................................................................... 8

Typical Configuration .................................................................................................................. 9

Installing the Management System - Typical Configuration .................................................... 10

Defining System Parameters ....................................................................................................... 11

Prerequisite Steps ....................................................................................................................... 13
  Other Recommended Actions ................................................................................................ 14
  Upgrading the RPM Package (For Linux Users Only) ............................................................ 14
  Installing Unix Client Utilities For Automatic Database Backup Tool (Optional) .................. 16

Installing the Management System Software ........................................................................... 17
  Validating Management System Status .................................................................................. 23
  Viewing the Installation Log ................................................................................................... 23

Installing the User Interface ....................................................................................................... 25
  Viewing the Installation Log ................................................................................................... 29
  Running the User Interface ..................................................................................................... 29

Validating the Installation .......................................................................................................... 31
  Running the UI in Demo Mode ............................................................................................... 32

Next Steps ................................................................................................................................... 33

Extended Configuration .............................................................................................................. 35

Installing the Management System - Extended Configuration ............................................... 36
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining System Parameters</td>
<td>37</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>39</td>
</tr>
<tr>
<td>Installing the GUI Server</td>
<td>40</td>
</tr>
<tr>
<td>Installing the User Interface</td>
<td>46</td>
</tr>
<tr>
<td>Installing the Device Server</td>
<td>46</td>
</tr>
<tr>
<td>Installing the Device Server - Validating Management System Status</td>
<td>47</td>
</tr>
<tr>
<td>Transferring Certificate Files (optional)</td>
<td>53</td>
</tr>
<tr>
<td>Next Steps</td>
<td>54</td>
</tr>
<tr>
<td>Upgrading</td>
<td>55</td>
</tr>
<tr>
<td>Upgrading The Management System</td>
<td>56</td>
</tr>
<tr>
<td>Prerequisite Steps</td>
<td>57</td>
</tr>
<tr>
<td>Other Recommended Actions</td>
<td>58</td>
</tr>
<tr>
<td>Upgrading the RPM Package (For Linux Users Only)</td>
<td>58</td>
</tr>
<tr>
<td>Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)</td>
<td>60</td>
</tr>
<tr>
<td>Upgrading the Management System - Typical Configuration</td>
<td>61</td>
</tr>
<tr>
<td>Upgrading the Management System On Separate Servers</td>
<td>66</td>
</tr>
<tr>
<td>Validating the Upgrade</td>
<td>71</td>
</tr>
<tr>
<td>Next Steps</td>
<td>73</td>
</tr>
<tr>
<td>Administration</td>
<td>75</td>
</tr>
<tr>
<td>Controlling the Management System</td>
<td>76</td>
</tr>
<tr>
<td>Viewing Management System Commands</td>
<td>76</td>
</tr>
<tr>
<td>Starting Server Processes</td>
<td>77</td>
</tr>
<tr>
<td>Stopping Server Processes</td>
<td>77</td>
</tr>
<tr>
<td>Maintaining the Management System</td>
<td>79</td>
</tr>
<tr>
<td>Changing the Management System IP Address</td>
<td>79</td>
</tr>
<tr>
<td>Changing the Device Server IP Address</td>
<td>79</td>
</tr>
<tr>
<td>Changing the GUI Server IP Address</td>
<td>80</td>
</tr>
<tr>
<td>Changing Permissions To a Normal User</td>
<td>80</td>
</tr>
<tr>
<td>Uninstalling the Management System</td>
<td>81</td>
</tr>
<tr>
<td>Archiving and Restoring Logs and Configuration Data</td>
<td>82</td>
</tr>
<tr>
<td>Archiving Logs and Configuration Data</td>
<td>82</td>
</tr>
<tr>
<td>Restoring Logs and Configuration Data</td>
<td>83</td>
</tr>
<tr>
<td>Automatic Database Backup Option</td>
<td>84</td>
</tr>
</tbody>
</table>
Thank you for choosing NetScreen-Security Manager 2004 FP1 - integrated management software for all NetScreen firewall/VPN devices and systems.

This *NetScreen-Security Manager 2004 FP1 Installer's Guide* describes how you can install an initial working Security Manager system. This Installer's Guide is intended primarily for IT administrators who are responsible for installing Security Manager for the first time.

*Note: If you are currently using a previous version of NetScreen management software (i.e., NetScreen-Global PRO or NetScreen-Global PRO Express) refer to the NetScreen-Security Manager 2004 FP1 Migration Guide for more specific information.*
This manual contains the following 5 chapters and 2 appendices:

- **Chapter 1, “Introduction”** describes the installation process, minimum hardware and software requirements, and other key information to help you design and implement a management system that is appropriate for your network.

- **Chapter 2, “Typical Configuration”** describes specifically how to install the Security Manager management system for most typical cases - GUI Server and Device Server on the same server. It describes how to install and configure the required software for both management system components (GUI Server, Device Server) together on the same server.

- **Chapter 3, “Extended Configuration”** describes specifically how to install the Security Manager management system for enhanced scalability and performance - with the GUI Server and Device Server installed on separate servers.

- **Chapter 4, “Upgrading”** describes specifically how to upgrade previous installations of Security Manager to Feature Pack 1.

- **Chapter 5, “Administration”** describes how to maintain and uninstall the management system and UI.

- **Appendix A, “Technical Overview”** provides an overview of the Security Manager architecture and communications.

- **Appendix B, “Sizing and Capacity Planning”** discusses considerations for hardware sizing and capacity planning.
OTHER TECHNICAL PUBLICATIONS

To obtain technical documentation for any NetScreen product, visit:

www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit: www.netscreen.com/services/downloadソフト.
Select a category of software product from the dropdown list, then follow the displayed
instructions. (You must be a registered user to download NetScreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail
address below:

technical@netscreen.com
This chapter provides you with the information you need to plan how best to install Security Manager and integrate it into your network. It provides an overview of the Security Manager installation process. It also reviews minimum hardware and software requirements and options for configuring the management system to provide enhanced performance and scalability.
**INSTALLATION PROCESS OVERVIEW**

Security Manager is software that enables you to integrate and centralize management of your NetScreen security environment.

There are two main software components that you need to install and run Security Manager: the Security Manager management system and the Security Manager User Interface (UI).

The overall process for installing Security Manager is as follows:

- “Management System Install Process” on page 2
- “User Interface Install Process” on page 2

**Management System Install Process**

The management system installer enables you to install all the software required to run each component of the Security Manager management system. Refer to Appendix A “Technical Overview” for more information on the Security Manager management system.

The management system installer is a shell archive script that you can run on any dedicated, secure and trusted Solaris 8 or 9, Red Hat Linux 8.0, 9.0, or Red Hat Enterprise Linux ES server that meets minimum system requirements. Refer to “Minimum System Requirements” on page 4 for more information on the minimum required hardware and software that you need to install the Security Manager management system.

There are separate installer scripts for both Linux and Solaris installations. When you launch the management system installer, the script guides you through all the steps required to install and configure each management system component.

**User Interface Install Process**

The Security Manager User Interface installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer that meets minimum system requirements. Refer to “Minimum System Requirements” on page 4 for more information on the minimum required hardware and software that you need to install the Security Manager User Interface.

The InstallAnywhere wizard guides you through all the steps required to configure and install the User Interface. Once you install the User Interface, you can connect it to the management system.
**INSTALLATION PACKAGE**

All of the software files required to install Security Manager are located on the Security Manager installation CD or on the Internet at the NetScreen corporate support web site. It is recommended that you download these files to the computers on which you plan to install Security Manager before beginning the installation process.

The following table describes the contents of the Security Manager installation CD.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm04fp1_ui_win_x86.exe</td>
<td>Installer for the Security Manager UI (for Windows-based computers).</td>
</tr>
<tr>
<td>nsm04fp1_ui_linux_x86.bin</td>
<td>Installer for the Security Manager UI (for Linux-based computers).</td>
</tr>
<tr>
<td>nsm04fp1_servers_linux_x86.sh</td>
<td>Installer for the Security Manager management system for Linux</td>
</tr>
<tr>
<td>nsm04fp1_servers_sol_sparc.sh</td>
<td>Installer for the Security Manager management system for Solaris</td>
</tr>
<tr>
<td>nsm04fp1_gpexport_sol_sparc.sh</td>
<td>Installer for the Global PRO data export utility used to migrate data from Global PRO Express/Global PRO into Security Manager. You use this file only if you plan to migrate configuration data from Global PRO or Global PRO Express. If so, refer to the <em>NetScreen-Security Manager 2004 FP1 Migration Guide</em> for more specific information.</td>
</tr>
<tr>
<td>system_update_fp1.tar</td>
<td>System update utility. If you are installing on Linux, you use this file to update your RPM package for the version of Linux that you are using. If you are installing on Solaris, you use this file to install Unix client utilities required to run the automatic database backup option.</td>
</tr>
</tbody>
</table>
MINIMUM SYSTEM REQUIREMENTS

The following minimum hardware and software requirements must be met to properly install and run Security Manager.

System Requirements - Management System

The following table describes the minimum requirements that must be met for the GUI Server and Device Server:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI Server and Device Server on the same server</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES</td>
</tr>
<tr>
<td></td>
<td><strong>CPU:</strong></td>
</tr>
<tr>
<td></td>
<td>Sun Microsystems UltraSPARC IIi 500MHz (or higher), OR Linux 1GHz processor (or higher)</td>
</tr>
<tr>
<td></td>
<td><strong>RAM:</strong> 1GB (or higher); 2GB+ (depending on the number of managed devices and configuration size)</td>
</tr>
<tr>
<td></td>
<td><strong>Swap Space:</strong> 4 GB for both GUI Server and Device Server</td>
</tr>
<tr>
<td></td>
<td><strong>Storage:</strong> IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)</td>
</tr>
<tr>
<td></td>
<td><strong>Network Connection:</strong> 100MBps NIC Ethernet adapter</td>
</tr>
<tr>
<td></td>
<td>Server must be dedicated to running Security Manager only.</td>
</tr>
</tbody>
</table>

| GUI Server and Device Server on separate servers| Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES |
|                                                | **CPU:**                                                                            |
|                                                | Sun Microsystems UltraSPARC IIi 500MHz (or higher), OR Linux 1GHz processor (or higher) |
|                                                | **RAM:** 512MB (or higher); 1GB (recommended)                                        |
|                                                | **Swap Space:** 2 GB for the GUI Server, 2 GB for the Device Server                  |
|                                                | **Storage:** IDE Hard Disk Drive with 10K rpm (minimum) - 15K rpm (recommended); 18 GB disk space (minimum) - 40 GB disk space (recommended) |
|                                                | **Network Connection:** 100MBps NIC Ethernet adapter                                  |
|                                                | **I/O:** Split backplane (recommended for Device Server)                            |
|                                                | Each server must be dedicated to running Security Manager only.                      |

Note that you may extend system performance and data capacity by expanding on the minimum requirements specified for each component. Refer to Appendix B “Sizing and Capacity Planning” for more information.
System Requirements - User Interface

The following table describes the minimum system requirements that must be met for the User Interface:

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Interface - Software</td>
<td>Microsoft Windows XP, OR Microsoft Windows NT&lt;sup&gt;®&lt;/sup&gt; Workstation/Server 4.0, Service Pack 6a or higher, OR Microsoft Windows 2000 Server, Advanced Server, or Professional editions OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES US English versions only</td>
</tr>
</tbody>
</table>
| User Interface - Hardware| IBM<sup>®</sup> compatible PC 400MHz Pentium<sup>®</sup> II or equivalent (minimum); 700 MHz Pentium II or equivalent (recommended)  
**RAM:** 256 MB (minimum); 512 MB or above (recommended)  
384kbps (DSL) or LAN connection - minimum bandwidth required to connect to the Security Manager management system. |
**Configuration Options**

You can design and implement Security Manager to scale to small, medium, and large enterprises, as well as service provider deployments. There are two main options for configuring Security Manager:

- “Typical Configuration” on page 6
- “Extended Configuration” on page 7

*Note:* NetScreen-Security Manager 2004 FP1 provides support for only one GUI Server and one Device Server. In future releases of Security Manager, you will be able to install and deploy multiple Device Servers in your network in order to provide greater scalability and performance. You will also be able to configure the management system for high availability.

**Typical Configuration**

The most straightforward implementation of the Security Manager management system is to install both components of the management system (GUI Server and Device Server) on the same server. This configuration is appropriate for most typical small to medium-sized enterprises.
Extended Configuration

For larger enterprises, specifically where you expect to generate and store an inordinate amount of traffic logs, it is recommended that you install the GUI Server and Device Server on separate servers.
Chapter 1 Introduction

Next Steps

This chapter has provided you with the following:

- an overview of the Security Manager installation process
- a description of the contents in the Security Manager installation package
- minimum system requirements to help you identify the appropriate hardware and software to install and run Security Manager
- options for implementing components of the Security Manager management system to provide for enhanced performance and scalability

You should use this information to plan how best to implement Security Manager and integrate it into your network. When you are ready to install Security Manager, there are two options for configuring the management system depending upon the size and requirements of your specific network.

Refer to Chapter 2, “Typical Configuration” for specific information describing how to install and run the management system for most typical cases, that is, on the same server.

Refer to Chapter 3, “Extended Configuration” for specific information describing how to install and run the GUI Server and Device Server on separate servers. This configuration option enables you to extend performance and scalability for large enterprises.

Refer to for Chapter 4, “Upgrading” for specific information describing how to upgrade previous installations of Security Manager to Feature Pack 1.

Refer to Chapter 5, “Administration” for specific information describing how to maintain, control, backup/restore and uninstall the management system and UI.
Typical Configuration

In This Chapter

- Installing the Management System - Typical Configuration
- Defining System Parameters
- Prerequisite Steps
- Installing the Management System Software
- Installing the User Interface
- Validating the Installation
- Next Steps

Once you have decided how you want to deploy Security Manager in your network, and you have identified and procured the appropriate hardware, you are ready to begin the installation process.

This chapter describes how to install the Security Manager management system for most typical cases - GUI Server and Device Server on the same system. This includes performing any prerequisite steps, running the management system installer, running the UI installer on your Windows or Linux client, and validating that you have installed the management system successfully.
**INSTALLING THE MANAGEMENT SYSTEM - TYPICAL CONFIGURATION**

The following table summarizes the process for installing Security Manager for most typical cases. It also provides an estimate of the overall amount of time that each step requires. The total expected time to complete the actual installation procedure is no longer than 30 minutes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Define system parameters that you need to provide during the installation process.</td>
<td>10 min.</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps.</td>
<td>20 min.</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and UI installer software from the Security Manager installation CD or the NetScreen corporate web site.</td>
<td>10 min.</td>
</tr>
<tr>
<td>4</td>
<td>Run the management system installer on the system where you want to install the management system. Specify that you want to install both the GUI Server and Device Server. Install and configure the automatic database backup option (optional). * If you are installing the GUI Server and Device Server on separate systems, refer to Chapter 3, “Extended Configuration” for more information.</td>
<td>5 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>2-3 min.</td>
</tr>
<tr>
<td>6</td>
<td>Launch the UI, and connect it to the management system.</td>
<td>2-3 min.</td>
</tr>
<tr>
<td>7</td>
<td>Validate that you have successfully installed the management system and UI.</td>
<td>2 min.</td>
</tr>
</tbody>
</table>
**Defining System Parameters**

During the installation process, you are required to configure common system parameters such as the location of the directories where you wish to store data for the GUI Server and Device Server. It is recommended that you define these system parameters before performing the management system installation.

The following table identifies the parameters that you need to identify:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address and port of the GUI Server</td>
<td>The IP address and port used by the running GUI Server are required to start the Device Server. The Device Server also needs this information enabling it to connect and communicate with the GUI Server.</td>
</tr>
<tr>
<td>Initial &quot;super&quot; user password</td>
<td>This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location where user data on the GUI Server is stored. By default, the installer creates the directory in the following location: /var/netscreen/GuiSvr/</td>
</tr>
<tr>
<td></td>
<td>Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</td>
</tr>
<tr>
<td>Device Server data directory</td>
<td>Directory location where device data on the Device Server is stored. By default, the installer creates the directory in the following location: /var/netscreen/DevSvr/</td>
</tr>
<tr>
<td></td>
<td>Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</td>
</tr>
<tr>
<td>Automatic Database Backup Directory (Optional)</td>
<td>Directory location where backup data on the server is stored. By default, the installer creates the directory in the following location: /var/netscreen/dbbackup/</td>
</tr>
<tr>
<td>Automatic Database Backup Tool Configuration Directory (Optional)</td>
<td>Directory location where configuration data for the automatic backup tool is stored. By default, the installer creates the directory in the following location: /var/netscreen/iHaSvr/</td>
</tr>
</tbody>
</table>
## Chapter 2 Typical Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path to the rsync Utility Package</td>
<td>Directory location where the rsync utility package is stored. This utility is required by the automatic database backup option. The package is typically stored in:</td>
</tr>
<tr>
<td></td>
<td><code>/usr/bin/rsync/</code></td>
</tr>
<tr>
<td>Automatic Database Backup Time</td>
<td>Time of day that you wish the automatic database backup tool to begin the daily backup process. You must enter a 2 digit number representing the time of day in military time (00-23). For example, if you want the backup to begin at 4:00am, enter 04; if at 4:00pm, enter 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. By default, the utility begins the daily backup process at 2:00am every day.</td>
</tr>
<tr>
<td></td>
<td>Refer to Automatic Database Backup Option in Chapter 5 for more information on the automatic database backup process.</td>
</tr>
<tr>
<td>Number of Automatic Database Backup Files Stored</td>
<td>Total number of database backup files that the automatic database backup tool stores. By default, the utility stores seven (7) backup files before it begins to overwrite the oldest file.</td>
</tr>
</tbody>
</table>
PREREQUISITE STEPS

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.
2. Login to the computer as root.

   If you are already logged in as a user other than root, you may become root by typing the following command:
   
   su

   At the password prompt, enter the root password for the computer.

   **Note:** The Security Manager management system runs as the root user. If you wish to run the management system in a more secure mode, refer to “Changing Permissions To a Normal User” on page 80.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.
4. If you are installing the management system on Linux, verify that you are running the correct version of RPM for the version of Linux that you are using.

   You can verify that you are running the correct version of RPM by running the following command:
   
   rpm -qi rpm

   For **Red Hat 8.0**, verify that you are running **version 4.1.1, release 1.8x**.

   For **Red Hat 9.0**, verify that you are running **version 4.2, release 1**.

   For **Red Hat Enterprise ES 3.0**, you are required to upgrade the RPM package.

   If you are not running the correct version of RPM for the version of Linux that you are using, you must upgrade it before proceeding. Refer to “Upgrading the RPM Package (For Linux Users Only)” on page 14 for more information.

5. (Optional) If you want the management system to perform automatic database backups, you must verify that you have installed the required UNIX client utilities for your version of Linux or Solaris (i.e., rsync and popt). If these packages are not installed, you must install them first before running the Security Manager management system installer. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 16 for more information.
Other Recommended Actions

It is highly recommended that you disable X server on all the server machines that you plan to install Security Manager. Disabling X server will free up additional server resources for enhanced system performance.

To disable X server on Linux:

1. Navigate to the /etc subdirectory.
2. Open the inittab file in any text editor.
3. Comment out the line that refers to /etc/X11/prefdm.
4. Run init q
5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

```
/etc/rc2.d/S99dtlogin stop
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/orig.S99dtlogin
```

Upgrading the RPM Package (For Linux Users Only)

Use the system update utility provided to upgrade to the correct version of RPM.

To upgrade your version of RPM:

1. Save the system update utility (the file is called system_update_fp1.tar) provided on the Security Manager Installation CD, or from the directory where it is saved, to a suitable directory on the server.

   Note: It is recommended that you save the utility in the /usr subdirectory.

2. Untar the file. You can do so by running the following command:

   `tar xvf system_update_fp1.tar`
A subdirectory called `/systemupdate` is created and all the files required to upgrade your rpm package are extracted into that directory.

3. Navigate to the `/systemupdate` subdirectory, where the update script is stored. You can do so by running the following command:

   `cd /usr/systemupdate`

4. Execute the update script. You can do so by running the following command:

   `./update.sh`
The script prompts you to press **Enter** to continue.

5. Press **Enter**. You can also press **Ctrl C** to stop the upgrade process. Let the script run to completion. This may take up to 20 minutes depending upon the number of packages that must be installed.

### Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)

If you want the management system to perform automatic database backups, you must have already installed the required Unix client utilities (i.e., rsync and popt) on your system. These packages are typically installed on Linux systems by default.

If you are installing Security Manager on a Solaris system, and you have not previously installed rsync or popt, you can use the system update utility (the same utility used to upgrade your Linux rpm package) to install the utilities on your system.

Follow the same procedures provided in the previous section to save, untar and run the system update utility.

**Note:** After installing rsync, note that you do **not** need to configure the daemon (rsync server).
Installing the Management System Software

In most typical cases, you install both the GUI Server and Device Server on the same server. The management system installer is designed to guide you through all the steps to configure required system parameters, then run to completion.

To install the management system on a single system:

1. Load the management system installer software onto the server which you have decided to function as the Security Manager management system. You can run the installer directly from the Security Manager installation CD. You can also copy the installer to a directory on the server, or you can download the installer from the NetScreen Customer Services Online website.

2. Navigate to the directory where you have saved the management system installer file. It is recommended that you save the management system installer in the \tmp subdirectory.

3. Run the management system installer.

   On Linux, you can run the management system installer using the following command:
   
   ```sh
   sh nsm04fp1_servers_linux_x86.sh
   ```

   On Solaris, you can run the management system installer using the following command:
   
   ```sh
   sh nsm04fp1_servers_sol_sparc.sh
   ```

   The installation begins automatically by performing a series of pre-installation checks. The installer ensures that:
   
   – you are installing the correct software for your operating system
   – all the needed software binaries are present
   – you have correctly logged in as root
   – the system has sufficient disk space and RAM

   The installer then stops any running servers.

   **Note:** The management system installer indicates the results of its specific tasks and checks:

   - **“Done”** indicates that the installer successfully performed a task.
   - **“ok”** indicates that the installer performed a check, and verified that the condition was satisfied.
   - **“FAILED”** indicates that the installer performed a task or check, but it was not successful.

   The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

   **Note:** If you have installed a previous version of the management system, you may notice different menu options.
4. Enter selection 3 to specify that you want to install the Device Server and GUI Server.

The following graphic depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

```
   root@docteam-attack:/tmp
File Edit View Terminal Go Help
Creating staging directory...ok

########### PERFORMING PRE-INSTALLATION TASKS ############
Running preinstallcheck...
Checking if platform is valid.........................ok
Checking for correct intended platform............ok
Checking if all needed binaries are present.......ok
Checking for platform-specific binaries.........ok
Checking if user is root...............................ok
Checking if user root exists.......................ok
Checking if system meets RAM requirement........ok
Checking for sufficient disk space................ok
Checking if RPM binary has been updated...........ok
Noting OS name............................................ok
Stopping any running servers
########### GATHERING INFORMATION ###############

1) Install Device Server only
2) Install GUI Server only
3) Install both Device Server and GUI Server
Enter selection (1-3) [1]> 3
```

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis. It is highly recommended that you install the automatic database backup option.

5. Enter y and then press ENTER if you want the management system to perform an automatic backup of the database on a daily basis. The script then prompts you to configure options for the backup operation:

   a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 16 for more information.

   b. Enter a two-digit number (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press ENTER to accept the default setting of 02 or 2:00am.

   c. Enter a directory location where you want the management system to store the database backup locally. Press ENTER to accept the default directory location of /var/netscreen/dbbackup.
d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press **ENTER** to accept the default setting of 7 backup files.

If you do not want to backup the database automatically, enter **n** and then press **ENTER**.

The script next prompts you to specify where you want to store the Device Server and GUI Server data files.

6. Configure the paths for the directories where you want to store the management system data files:
   a. Enter the path for the directory that you want to store the data files for the Device Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/DevSvr`).

   **Note:** If you specify a new directory location, the installer creates it. The installer does not however, allow you to specify an existing directory location. This is to safeguard against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and prompt you to try again.

   The script prompts you to specify where you want to store the GUI Server data files.

   b. Enter the path for the directory that you want to store the data files for the GUI Server, or press **ENTER** to accept the default path (the default location is `/var/netscreen/GuiSvr`).
7. If you specified that you want the management system to perform automatic backups, the script also prompts you to enter a directory location where you want the management system to store the configuration settings you have set for the database backup tool. Press **ENTER** to accept the default setting of `/var/netscreen/iHaSvr`.

The script next prompts you to specify the IP address of the Device Server.

8. Enter the management IP address for the server. This should be the same IP address of the server that you are installing on. The installer sets the IP address and port number on the GUI Server enabling the Device Server to connect. It attempts to connect to the GUI Server using port **7800** by default.

The script next prompts you to enter a password for the “super” user account. The initial administrator or “super” user account is the account that you use when you first login to Security Manager using the Security Manager UI. This account is used to authenticate communication between the management system and the Security Manager UI. It possesses all administrative privileges by default.

9. Enter any text string for the password. Enter the password again for verification.

**Note:** Make a note of the password that you have set for the super user account. You need this when you first login to the UI.

The script next prompts you if you want to start both servers once it has completed installation.
10. Enter `y` and then press **ENTER** to start both servers once the installer has completed the installation process. Enter `n` and then press **ENTER**, if you do not want to start both servers.

   Note: Whenever you restart your operating system, both the GUI Server and Device Server start automatically.

The script next prompts you to verify your installation configuration settings.

11. Verify your settings, and if they are correct, enter `y` and then press **ENTER** to proceed. If you enter `n` and then press **ENTER**, the installer returns you to the original Selection prompt.

   ![Image of terminal output showing verification prompts]

The installation proceeds automatically. The installer proceeds to perform the following actions:

- extract the software payloads
- perform any applicable migration tasks (disregard since this is a new installation)
- install the Device Server
- install the GUI Server
- install the Database Backup Tool (if applicable)
– perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.

```
File Edit View Terminal Go Help
************ EXTRACTING PAYLOADS ************
Extracting payload.................................ok
Decompressing payload.............................ok
gzip: payload.tgz: unexpected end of file
ok

************ PERFORMING MIGRATION TASKS ************

************ PERFORMING INSTALLATION TASKS ************

----- INSTALLING Device Server ----- Look for existing RPM package..................ok
Removing DevSvr files from default location.....ok
Installing Device Server RPM......................ok
Installing JRE...............................................ok
Creating var directory............................ok
Creating /var/netscreen/dbbackup..................ok
Putting NSROOT into start scripts................ok
Filling in config file(s)..............................ok
Setting permissions for Device Server..........ok
Restarting xinetd service..........................ok
Installation of Device Server complete.

----- INSTALLING GUI Server ----- Look for existing RPM package..................ok
Removing Guisvr files from default location.....ok
Installing GUI Server RPM......................ok
Installing JRE...............................................ok
Creating var directory............................ok
Clearing contents of /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts................ok
Filling in config file(s)..............................ok
Setting permissions for GUI Server.............ok
Running generateMPX utility.....................ok
Running fingerprintMPX utility...............ok
Installation of GUI Server complete.
```
Several messages display to confirm the installation progress.

![Installation Log](image)

The installer runs for several minutes, and then exits.

**Validating Management System Status**

If you did not specify the installer to start the server(s) when finished, you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (i.e., the HA server, Device Server and GUI Server) to confirm that all services are up and running.

Refer to **Controlling the Management System** in Chapter 5 for more information on manual commands that you can send to the HA Server, Device Server and GUI Server.

**Viewing the Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes. This file is saved by default in the `tmp` subdirectory.
The naming convention used for the installation log file is:
netmgtInstallLog.<current date><current time>

For example if you ran the installer on December 1, 2003 at 6:00pm, the installation log file would be named: netmgtInstallLog.20031201180000

Note: Once the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.
INSTALLING THE USER INTERFACE

The Security Manager User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer that meets minimum system requirements. Refer to Chapter 1, “Introduction” for more information on the minimum system requirements for the UI.

The InstallAnywhere wizard guides you through all the steps required to configure and install the Security Manager UI. Once you install the UI, you can connect it to the management system.

Note: It is recommended that you quit all running applications before installing the UI.

To install the Security Manager UI:

1. Login as an Administrator user on the computer where you are installing the UI.

   Note: For instructions on adding users to the Administrator group, please refer to your operating system manual.

2. Download the UI installer from the Security Manager installation CD or the NetScreen corporate web site to the computer where you are installing the UI.

3. Run the UI installer.

   If you are installing the UI on a Windows-based PC, you can double-click on the installer executable.

   If you are installing the UI on a Linux-based computer, you can launch it from a command line. From the command line, you can launch the UI installer using the following command:

   sh nsm04fp1_ui_linux_x86.bin

   Initially, the following messages appear in the Linux terminal.
An Introduction screen for the InstallAnywhere wizard appears.

Follow the wizard through all the steps required to configure and install the UI. Click **Next** to continue the installation. The License Agreement screen appears.

4. Review the License Agreement carefully. If you choose to accept the terms of the License Agreement, click the button next to the appropriate statement. Click **Next** to continue.

   **Note:** If you choose to not accept the terms of the License Agreement, you will not be able to proceed with the installation.

If you accepted the License Agreement, the Choose Install Folder screen appears.
5. To accept the default install folder, click **Next**.

*Note: If you are installing on a Windows-based computer, the installer saves the UI software files in C:\Program Files\NetScreen-Security Manager by default. If you are installing on a Linux-based computer, the installer saves the UI software files in /root/NetScreen-Security Manager by default.*

To specify a new or different folder location, click **Choose...**. If you decide to accept the default install folder, you can click **Restore Default Folder**.

On Windows-based computers, the Choose Shortcut Folder screen appears.
On Linux-based computers, the Choose Link Folder screen appears.
6. Select where you would like to create the Security Manager product icons. Or, if you are installing on a Linux-based computer, select where you would like to create links to the Security Manager UI program. Click Next to continue. The Pre-Installation Summary screen appears.

![Pre-Installation Summary](image)

7. Verify that the information is correct. To make a change to any of the previous configuration options, click Previous. When you are satisfied that the information is correct for this installation, click Install. The installer proceeds to install the software files for the UI.

8. If you do not have a default web browser configured, the Select Browser screen appears. Use the Choose button to navigate to the subdirectory where your web browser software files are located. Click Next to continue.

![Select Browser](image)
When the installation is complete, a screen indicating “Install Complete” appears.

Note: If you do not select a default web browser, the UI will not be able to launch the Security Manager online help. If you still wish to use the online help, you can configure your web browser using the Preferences menu from the UI.

9. Click **Done** to exit the installation program.

**Viewing the Installation Log**

The installer generates a log file with information describing the context of the installation process. For troubleshooting purposes, you may need to access it. The installation log is saved by default in the following directory locations:

For Windows-based computers:

C:\Documents and Settings\<user name>\.nsm\

For Linux-based computers:

/root/.nsm/

Note: The .nsm subdirectory is a hidden subdirectory on Linux systems.

The Installation log file is named:

_out.<date/time stamp>.dat

**Running the User Interface**

Once you have completed installing the UI, you can launch the application and verify that you can connect to the management system.

The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a user name, and password. The default user name for new installations is “super”; the default password is the password you specified when configuring the management system. Passwords and user names are case-sensitive.

To log in to the UI for the first time:

1. Run the Security Manager UI.

   If you are running the UI on a Windows-based PC, you can double-click on the NetScreen-Security Manager icon.
If you are running the UI on a Linux-based computer, you can either launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or you can launch it from a command line. From the command line, navigate to the subdirectory where you have installed the UI software files, and then launch the UI application by running the shell archive script provided. The Login window appears.

2. Verify that the user name in the Login field provided is the initial admin user called “super”. If not, enter “super” in the Login field.

3. Enter the password that you specified when you installed the management system in the Password field provided.

4. Enter the IP address you assigned to the GUI Server in the Server field provided. If you have enabled DNS-lookup, you can enter the host name instead of the IP address.

5. Click OK.

The UI appears indicating that the installation was successful.
VALIDATING THE INSTALLATION

Once you have installed the management system and UI, it is recommended that you validate basic information configured on the Device Server. You can use the Server Manager to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the Security Manager UI, double-click on the **Server Manager** module. The Server Manager module expands, and the Servers and Server Monitor appears.
2. Click on the **Servers** node. The Servers view appears displaying Device Server and GUI Server information.
3. Click on the Device Server and click on the **Edit** icon or right-click on the Device Server and select **Edit** to view all information available on the Device Server.

4. Use the **General** tab to verify the following information:
Chapter 2 Typical Configuration

- **Mapped IP address** - the IP address that is manually defined in the UI.

  Note: You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the FW/VPN device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.

- **Device Server Manager Port** - the default port is 7800.

- **Password for GUI Server Connection** - This password authenticates communication between the Device Server and GUI Server.

- **Device Server ID** - the ID number identifies the Device Server; you cannot change the Device Server ID.

5. Click OK when you are done.

Running the UI in Demo Mode

Before you begin using Security Manager to configure and manage your network, it is recommended that you first run the UI in Demo mode. Demo mode is an option in the UI enabling you to run the UI disconnected from the management system.

To run the UI in Demo mode:

1. Run the Security Manager UI. The Login window appears.
2. Enter any user name in the Login field provided.
3. Enter any password in the Password field provided.
4. Select *DEMO MODE* from the Server field pull-down menu.

![NetScreen - Security Manager Login](image)

5. Click OK.
Congratulations! You have just completed installation of the Security Manager management system and User Interface. You can now begin to manage your network using Security Manager. Refer to the *NetScreen-Security Manager 2004 FP1 Administrator’s Guide* for information describing how to plan and implement Security Manager for your network.

If you plan to install the GUI Server and Device Server on separate servers, refer to Chapter 3, “Extended Configuration” for more information.
Extended Configuration

In This Chapter

- Installing the Management System - Extended Configuration
- Defining System Parameters
- Prerequisites
- Installing the GUI Server
- Installing the User Interface
- Installing the Device Server
- Transferring Certificate Files (optional)
- Next Steps

For larger enterprises, specifically where you expect to generate an inordinate amount of traffic logs, it is recommended that you install the GUI Server and Device Server on separate servers.

This chapter describes how to install the Security Manager management system - GUI Server and Device Server on separate servers. This includes performing any prerequisite steps, running the management system installer, running the UI installer, and validating that you have installed the management system successfully.
## Installing the Management System - Extended Configuration

The following table summarizes the process for installing the management system on separate servers. It also provides an estimate of the overall amount of time that each step requires. The total time expected to complete the installation process is no longer than 30 minutes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Define system parameters that you need to provide during the installation process.</td>
<td>10 min.</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps.</td>
<td>20 min.</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and UI installer software from the Security Manager installation CD or the NetScreen corporate web site.</td>
<td>5 min.</td>
</tr>
<tr>
<td>4</td>
<td>Run the management system installer on the server where you want to install the GUI Server. Specify that you want to install the GUI Server only. Install and configure the automatic database backup option (optional).</td>
<td>5 min.</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface.</td>
<td>2-3 min.</td>
</tr>
<tr>
<td>6</td>
<td>Launch the UI, and connect it to the GUI Server. Add and configure the Device Server.</td>
<td>5 min.</td>
</tr>
<tr>
<td>7</td>
<td>Run the management system installer on the server where you want to install the Device Server only. Specify that you want to install the Device Server only. Install and configure the automatic database backup option (optional).</td>
<td>5 min.</td>
</tr>
<tr>
<td>8</td>
<td>Transfer certificate files from the server that you are installing the Device server to the server that you are installing the GUI Server.</td>
<td>5 min.</td>
</tr>
</tbody>
</table>
**Defining System Parameters**

During the installation process, you are required to configure common system parameters such as the location of the directories where you wish to store data for the GUI Server and Device Server. It is recommended that you define these system parameters before performing the management system installation.

The following table identifies the parameters that you need to identify:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address and port of the GUI Server</td>
<td>The IP address and port used by the running GUI Server are required to start the Device Server. The Device Server also needs this information enabling it to connect and communicate with the GUI Server.</td>
</tr>
<tr>
<td>Initial “super” user password</td>
<td>This is the password required to authenticate the initial user in the system. By default, the initial super user account receives all administrative privileges in the system.</td>
</tr>
<tr>
<td>Device Server ID</td>
<td>unique ID automatically assigned when you add the Device Server.</td>
</tr>
<tr>
<td>Password for GUI Server Connection</td>
<td>password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location where user data on the GUI Server is stored. By default, the installer stores data on the GUI Server in the following location: /var/netscreen/GuiSvr/</td>
</tr>
<tr>
<td></td>
<td>Because the data on the GUI Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</td>
</tr>
<tr>
<td>Device Server data directory</td>
<td>Directory location where device data on the Device Server is stored. By default, the installer stores data on the Device Server in: /var/netscreen/DevSvr/</td>
</tr>
<tr>
<td></td>
<td>Because the data on the Device Server can grow to be very large, you may want to place this data in another location. If you decide to have data stored in an alternative location, specify the new location during the install process.</td>
</tr>
<tr>
<td>Automatic Database Backup Directory (Optional)</td>
<td>Directory location where backup data on the server is stored. By default, the installer stores backup data in: /var/netscreen/dbbackup/</td>
</tr>
</tbody>
</table>
Chapter 3 Extended Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Database Backup Tool Configuration Directory (Optional)</td>
<td>Directory location where configuration data for the automatic backup tool is stored. By default, the installer stores data in:</td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/iHaSvr/</td>
</tr>
<tr>
<td>Path to the rsync Utility Package</td>
<td>Directory location where the rsync utility package is stored. This utility is required by the automatic database backup tool. The package is typically stored in:</td>
</tr>
<tr>
<td></td>
<td>/usr/bin/rsync/</td>
</tr>
<tr>
<td>Automatic Database Backup Time</td>
<td>Time of day that you wish the automatic database backup tool to begin the daily backup process. You must enter a 2 digit number representing the time of day in military time (00-23). For example, if you want the backup to begin at 4:00am, enter 04; if at 4:00pm, enter 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. By default, the utility begins the daily backup process at 2:00am every day.</td>
</tr>
<tr>
<td></td>
<td>Refer to Automatic Database Backup Option in Chapter 5 for more information on the automatic database backup process.</td>
</tr>
<tr>
<td>Number of Automatic Database Backup Files Stored</td>
<td>Total number of database backup files that the automatic database backup tool stores. By default, the utility stores seven (7) backup files before it begins to overwrite the oldest file.</td>
</tr>
</tbody>
</table>
Prerequisites

Perform the prerequisite steps described as if you were installing the management system on the same server. Refer to Chapter 2, “Typical Configuration” for more information on installing the management system on the same server.
**INSTALLING THE GUI SERVER**

The management system installer guides you through all the steps required to configure system parameters, then runs to completion.

To install the GUI Server:

1. Navigate to the directory where you have saved the management system installer file.
2. Run the management system installer.
   - On Linux, you can run the management system installer using the following command:
     ```sh
     sh nsm04fp1_servers_linux_x86.sh
     ```
   - On Solaris, you can run the management system installer using the following command:
     ```sh
     sh nsm04fp1_servers_sol_sparc.sh
     ```
   The installation begins automatically by performing a series of pre-installation checks to ensure that:
   - you are installing the correct software for your operating system
   - all the needed software binaries are present
   - you have correctly logged in as root
   - the system has sufficient disk space and RAM
   The installer then stops any running servers.

*Note: The management system installer indicates the results of its specific tasks and checks:*

- **“Done”** indicates that the installer successfully performed a task.
- **“ok”** indicates that the installer performed a check, and verified that the condition was satisfied.
- **“FAILED”** indicates that the installer performed a task or check, but it was not successful.

The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

*Note: If you have installed a previous version of the management system, you may notice different menu options.*

3. Enter selection 2 to specify that you want to install the GUI Server.
The following depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

![Installer Output](image)

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis. **It is highly recommended that you install the automatic database backup option.**

4. Enter `y` and then press **ENTER** if you want the management system to perform an automatic backup of the database on a daily basis. If you specify that you want the management system to perform automatic backups, the script prompts you to configure options for the backup operation:

   a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 16 for more information.

   b. Enter a **two-digit number** (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press **ENTER** to accept the default setting of 02 or 2:00am.

   c. Enter a directory location where you want the management system to store the database backup locally. Press **ENTER** to accept the default setting of `/var/netscreen/dbbackup`. 
d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press **ENTER** to accept the default setting of 7 backup files.

*Note: If you are installing the management system on separate servers (in the extended configuration), and you wish to perform automatic database backups, you must install and configure the option on both the GUI Server and Device Server.*

Enter **n** and then press **ENTER**, if you do not want to backup the database automatically.

The script then prompts you to specify where you want to store the GUI Server data files.

5. Enter the path for the directory that you want to store the data files for the GUI Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/GuiSvr`).

*Note: If you specify a new directory location, the installer creates it. The installer does not however, allow you to specify an existing directory location. This is to safeguard against over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, and prompt you to try again.*
6. If you specified that you want the management system to perform automatic backups, the script also prompts you to enter a directory location where you want the management system to store the configuration settings you have set for the database backup tool. Press **ENTER** to accept the default setting of `/var/netscreen/iHaSvr`.

   The script next prompts you to specify the IP address of the Device Server.

7. Enter the management IP address of this server. This should be the same IP address of the server that you are installing. The installer sets the IP address and port number on the GUI Server enabling the Device Server to start and connect. It attempts to connect to the GUI Server using port **7800** by default.

   The script next prompts you to enter a password for the “super” user account. The initial administrator or “super” user account is the account that you use when you first log into Security Manager using the UI. This account is used to authenticate communication between the management system and the UI. It possesses all administrative privileges by default.
8. Enter any text string for the password. Enter the password again for verification.

*Note: Make a note of the password that you have set for the super user account. You need this when you first login to the system.*

The script next prompts you if you want to start the server processes (GUI Server and watchdog process) once it has completed installation.

9. Enter `y` and then press **ENTER** to start the server processes once the installer has completed the installation process. Enter `n` and then press **ENTER**, if you do not want to start the server processes.

*Note: Whenever you restart your server, the GUI Server and watchdog process start automatically.*

The script next prompts you to verify your installation configuration settings.

10. Verify your settings, and if they are correct, enter `y` and then press **ENTER** to proceed.

    If you enter `n` and then press **ENTER**, the installer returns you to the original Selection prompt.

    The installation proceeds automatically. The installer proceeds to perform the following actions:
    - extract the software payloads
– perform and applicable migration tasks (disregard since this is a new installation)
– install the GUI Server
– install the automatic database backup tool (if applicable).
– perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.

Several messages display to confirm the installation progress. The installer runs for several minutes, and then exits.

**Viewing the Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes. This file is saved by default in the tmp subdirectory.

The naming convention used for the installation log file is:

netmgtInstallLog.<current date><current time>

For example if you ran the installer on December 1, 2003 at 6:00pm, the installation log file would be named: netmgtInstallLog.20031201180000

*Note: Once the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.*
INSTALLING THE USER INTERFACE

Install the Security Manager User Interface. Refer to Chapter 2, “Typical Configuration” for more information on installing the User Interface.

Adding the Device Server

Once you have installed the UI, you need to create the Device Server in Security Manager and configure the following:

- Device Server ID
- Password for GUI Server Connection

This information enables the Device Server to establish a connection with the GUI Server.

Note: Make a note of the Device Server ID and Password for GUI Server Connection. You will need this when you install the Device Server.
INSTALLING THE DEVICE SERVER

The management system installer guides you through all the steps required system parameters to configure, then runs to completion.

Note: Before installing the Device Server, verify that the GUI Server is up and running. After you install the Device Server, the installer starts the Device Server by default. If the GUI Server is not already up and running, the Device Server will fail to connect to it.

To install the management system on a single server:

1. Navigate to the directory where you have saved the management system installer file.

2. Run the management system installer.
   
   On Linux, you can run the management system installer using the following command:

   ```bash
   sh nsm04fp1_servers_linux_x86.sh
   ```

   On Solaris, you can run the management system installer using the following command:

   ```bash
   sh nsm04fp1_servers_sol_sparc.sh
   ```

   The installation begins automatically by performing a series of pre-installation checks. The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

   Note: If you have installed a previous version of the management system, you may notice different menu options.

3. Enter selection 1 to specify that you want to install the Device Server only.

   The following depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.
Chapter 3 Extended Configuration

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis.

If you installed and configured the automatic database backup on the GUI Server, you are required to install and configure the option on the Device Server.

4. Enter `y` and then press `ENTER` if you want the management system to perform an automatic backup of the database on a daily basis. If you specify that you want the management system to perform automatic backups, the script prompts you to configure options for the backup operation:

   a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 16 for more information.

   b. Enter a two-digit number (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press `ENTER` to accept the default setting of 02 or 2:00am.

   c. Enter a directory location where you want the management system to store the database backup locally. Press `ENTER` to accept the default setting of `/var/netscreen/dbbackup`. 
d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press **ENTER** to accept the default setting of 7 backup files.

The script then prompts you to specify where you want to store the Device Server data files.

5. Enter the path for the directory that you want to store the data files for the Device Server or press **ENTER** to accept the default path (the default location is `/var/netscreen/DevSvr`).

6. If you specified that you want the management system to perform automatic backups, the script also prompts you to enter a directory location where you want the management system to store the configuration settings you have set for the database backup tool. Press **ENTER** to accept the default setting of `/var/netscreen/iHaSvr`.

The script next prompts you to specify the IP address of the Device Server.

7. Enter the management IP address of this server. This should be the same IP address of the server that you are installing on.

The script next prompts you to enter the ID assigned by the UI to this Device Server.
Chapter 3 Extended Configuration

8. Enter the Device Server ID. The script next prompts you to enter the one time password for this Device Server.

9. Enter the Password for GUI Server connection.

   The script next prompts you for the IP address and port number of the running GUI Server. This is required to enable the Device Server to start and communicate with the GUI Server.

10. Enter the IP address of the running GUI Server.

11. Enter the port number of the running GUI Server. The installer sets the IP address and port number on the GUI Server enabling the Device Server to connect. It attempts to connect to the GUI Server using port 7800 by default.

   The script next prompts if you want to start the Device Server once it has completed installation.

Note: Do not specify that you want to start the Device Server service automatically unless you have already started the GUI Server.

12. Enter y and then press ENTER to start the Device Server once the installer has completed the installation process. Enter n and then press ENTER, if you do not want to start the device server.

   Note: Whenever you restart your server, the Device Server starts automatically.

   The script next prompts you to verify your installation configuration settings.

13. Verify your settings, and if they are correct, enter y and then press ENTER to proceed.
Installing the Device Server

If you enter `n` and then press ENTER, the installer returns you to the original Selection prompt.

The installation proceeds automatically. The installer proceeds to perform the following actions:

- checks if a tftp server is installed on the system. If the installer does not detect a tftp server, a message indicating that you must install a tftp server to enable firmware updates for FW/VPN devices running ScreenOS versions 4.0.x appears. Refer to “Installing a TFTP Server” on page 87 for more information on installing a tftp server.
- extract the software payloads
- perform any applicable migration tasks (disregard since this is a new installation)
- install the Device Server
- install the Automatic Database Backup Tool
– perform post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and FW/VPN devices running ScreenOS 4.0.X (using NACN), and enabling the startup scripts for the Device Server and GUI Server.

Several messages display to confirm the installation progress. The installer runs for several minutes, and then exits.

Validating Management System Status

If you did not specify the installer to start the server(s) when finished, you must manually start the management system processes.

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (i.e, the HA server, Device Server and GUI Server) to confirm that all services are up and running.

Refer to “Controlling the Management System” on page 76 for more information on manual commands that you can send to the HA Server, Device Server and GUI Server.
**TRANSFERRING CERTIFICATE FILES (OPTIONAL)**

If you are using Security Manager to manage FW/VPN devices running ScreenOS 4.0.X, you must manually copy the certificate files generated by the installer from the server that you are installing the Device Server to the server that you are installing the GUI Server.

To transfer certificate files to the GUI Server:

1. Navigate to the `/DevSvr/var/certDB/config` subdirectory on the server where you have installed the Device Server.
2. Locate and copy the following files:
   - `cacertificate_table.nml`
   - `crl_table.nml`
   - `nacncertificate_table.nml`
3. Save these files in the `/GuiSvr/var` subdirectory on the server where you have installed the GUI Server.
Congratulations! You have just completed installation of the Security Manager management system on separate servers. You are now ready to begin managing your network. Refer to the *NetScreen-Security Manager 2004 FP1 Administrator’s Guide* for information describing how to plan and implement Security Manager for your network.

**NEXT STEPS**

Congratulations! You have just completed installation of the Security Manager management system on separate servers. You are now ready to begin managing your network. Refer to the *NetScreen-Security Manager 2004 FP1 Administrator’s Guide* for information describing how to plan and implement Security Manager for your network.
This chapter describes how to upgrade the Security Manager management system and user interface. This includes patching the management system, upgrading the UI on your Windows or Linux client, and validating that you have upgraded successfully.
## Upgrading The Management System

The following table summarizes the process for installing Security Manager for most typical cases. It also provides an estimate of the overall amount of time that each step requires. The total expected time to complete the actual installation procedure is no longer than 30 minutes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Estimated Time to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Define system parameters that you need to provide during the installation process.</td>
<td>10 min.</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps. It is highly recommended that you backup all your data files before beginning the upgrade process.</td>
<td>10 min.</td>
</tr>
<tr>
<td>3</td>
<td>Download the NSM 2004 FP1 management system and UI installer software from the Security Manager installation CD or the NetScreen corporate web site.</td>
<td>10 min.</td>
</tr>
<tr>
<td>4</td>
<td>Run the FP1 management system installer on the system where Security Manager management system is currently installed. Specify that you want to upgrade both the GUI Server and Device Server.</td>
<td>5 min.</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade the User Interface.</td>
<td>2-3 min.</td>
</tr>
<tr>
<td>6</td>
<td>Launch the UI, and connect it to the management system.</td>
<td>2-3 min.</td>
</tr>
<tr>
<td>7</td>
<td>Validate that you have successfully installed the management system and UI.</td>
<td>2 min.</td>
</tr>
</tbody>
</table>
PREREQUISITE STEPS

Before you install the management system, you need to perform the following prerequisite steps:

1. Ensure that the computer you install the management system on is connected to a serial console or monitor and keyboard.
2. Login to the computer as root.
   
   If you are already logged in as a user other than root, you may become root by typing the following command:
   
   ```
   su -
   ```
   
   At the password prompt, enter the root password for the computer.

   **Note:** In NetScreen-Security Manager 2004 FP1, the Security Manager management system runs as the root user. If you wish to run the management system in a more secure mode, refer to “Changing Permissions To a Normal User” on page 80.

3. Partition drives for sufficient disk space to accommodate your planned data requirements.
4. **Perform a backup of all files on the Device Server and GUI Server.** Refer to “Archiving Logs and Configuration Data” on page 82 for more information archiving your data files.
5. If you are upgrading your management system on Linux, verify that you are running the correct version of RPM for the version of Linux that you are using. You can verify that you are running the correct version of RPM by running the following command:
   
   ```
   rpm -qi rpm
   ```
   
   For Red Hat 8.0, verify that you are running version 4.1.1, release 1.8x.
   
   For Red Hat 9.0, verify that you are running version 4.2, release 1.
   
   For Red Hat Enterprise ES 3.0, you are required to upgrade the RPM package.
   
   If you are not running the correct version of RPM for the version of Linux that you are using, you must upgrade it before proceeding. Refer to “Upgrading the RPM Package (For Linux Users Only)” on page 58 for more information.
6. (Optional) If you want the management system to perform automatic database backups, you must verify that you have installed the required UNIX client (i.e., rsync and popt) packages for your version of Linux or Solaris. If these packages are not installed, you must install them first before running the Security Manager management system installer. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 60 for more information.
Other Recommended Actions

It is highly recommended that you disable X server on all the server machines that you plan to install Security Manager. Disabling X server will free up additional server resources for enhanced system performance.

To disable X server on Linux:

1. Navigate to the /etc subdirectory.
2. Open the inittab file in any text editor.
3. Comment out the line that refers to /etc/X11/prefdm.
4. Run init q
5. Log out of the graphical console and make sure X does not re-appear.

To disable X server on Solaris, run the following commands:

```
/etc/rc2.d/S99dtlogin stop
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/orig.S99dtlogin
```

Upgrading the RPM Package (For Linux Users Only)

Use the system update utility provided to upgrade to the correct version of RPM.

To upgrade your version of RPM:

1. Save the system update utility (the file is called system_update_fp1.tar) provided on the Security Manager Installation CD, or from the directory where it is saved, to a suitable directory on the server.

   Note: It is recommended that you save the utility in the /usr subdirectory.

2. Untar the file. You can do so by running the following command:

   `tar xvf system_update_fp1.tar`
A subdirectory called /systemupdate is created and all the files required to upgrade your rpm package are extracted into that directory.

3. Navigate to the /systemupdate subdirectory, where the update script is stored. You can do so by running the following command:
   
   ```bash
   cd /usr/systemupdate
   ```

4. Execute the update script. You can do so by running the following command:
   
   ```bash
   ./update.sh
   ```
The script prompts you to press **Enter** to continue.

5. Press **Enter**. You can also press **Ctrl C** to stop the upgrade process. Let the script run to completion. This may take up to 20 minutes depending upon the number of packages that must be installed.

---

### Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)

If you want the management system to perform automatic database backups, you must have already installed the required Unix client utilities (i.e., rsync and popt) on your system. These packages are typically installed on Linux systems by default.

If you are installing Security Manager on a Solaris system, and you have not previously installed rsync or popt, you can use the system update utility (the same utility used to upgrade your Linux rpm package) to install the utilities on your system.

Follow the same procedures provided in the previous section to save, untar and run the system update utility.

*Note: After installing rsync, note that you do **not** need to configure the daemon (rsync server).*
UPGRADING THE MANAGEMENT SYSTEM - TYPICAL CONFIGURATION

In most typical cases, you will upgrade both the GUI Server and Device Server on the same server. If you are upgrading the GUI Server and Device Server on separate systems, refer to “Upgrading the Management System On Separate Servers” on page 66.

To upgrade the management system on a single system:

1. Load the NSM 2004 FP1 management system installer software onto the server where the Security Manager management system is currently installed. You can run the installer directly from the Security Manager installation CD. You can also copy the installer to a directory on the server, or you can download the installer from the NetScreen Customer Services Online website.

2. Navigate to the directory where you have saved the management system installer file (typically the /tmp/ subdirectory).

3. Run the management system installer.

On Linux, you can run the management system installer using the following command:

    sh nsm04fp1_servers_linux_x86.sh

On Solaris, you can run the management system installer using the following command:

    sh nsm04fp1_servers_sol_sparc.sh

The installation begins automatically by performing a series of pre-installation checks. The installer ensures that:

- you are installing the correct software for your operating system
- all the needed software binaries are present
- you have correctly logged in as root
- you have installed a version of Security Manager that precedes the current version that you are installing
- the system has sufficient disk space and RAM

The installer then stops any running servers.

Note: The management system installer indicates the results of its specific tasks and checks:

- “Done” indicates that the installer successfully performed a task.
- “ok” indicates that the installer performed a check, and verified that the condition was satisfied.
- “FAILED” indicates that the installer performed a task or check, but it was not successful.
The installer next prompts you to specify the components of the Security Manager management system that you wish to install.

**Note:** If you have installed a previous version of the management system, you may notice different menu options.

4. Enter selection 2 to specify that you want to patch both the Device Server and GUI Server. The following graphic depicts the installer running on Linux. The installer running on Solaris displays essentially the same prompts and messages.

```
Creating staging directory...ok

********** PERFORMING PRE-INSTALLATION TASKS **********
Running preinstallcheck...
Checking if platform is valid...............ok
Checking for correct intended platform......ok
Checking if all needed binaries are present...ok
Checking for platform-specific binaries.....ok
Checking if user is root....................ok
Checking if user root exists.................ok
Checking if installed Device Server is newer.ok
Checking if installed GUI Server is newer....ok
Checking if system meets RAM requirement...ok
Checking for sufficient disk space..........ok
Checking if RPM binary has been updated....ok
Noting OS name.............................ok
Stopping any running servers

********** GATHERING INFORMATION **********

1) Reinstall both Device Server and GUI Server
2) Patch both Device Server and GUI Server
Enter selection (1-2) [] > 2
```

**Note:** Selecting to patch your previous management system ensures that all data previously configured in the system is restored in FP1. If you do not wish to restore your previous configuration data, you can choose to reinstall the management system.

The script next prompts if you want the management system to perform an automatic backup of the database on a daily basis. **It is highly recommended that you install the automatic database backup option.**

5. Enter `y` and then press ENTER if you want the management system to perform an automatic backup of the database on a daily basis. If you specify that you want the management system to perform automatic backups, the script prompts you to configure options for the backup operation:
a. Enter the path to the rsync package. The local database backup option requires that you have previously installed the rsync package. If you have not already installed the rsync package, exit the installer and install it. Refer to “Installing Unix Client Utilities For Automatic Database Backup Tool (Optional)” on page 60 for more information.

b. Enter a **two-digit number** (00-23) specifying the hour of day that you wish the management system to perform the daily backup operation. For example, if you want the management system to perform the daily backup operation at noon, enter 12; for midnight, enter 00. Press **ENTER** to accept the default setting of 02 or 2:00am.

c. Enter a directory location where you want the management system to store the database backup locally. Press **ENTER** to accept the default setting of `/var/netscreen/dbbackup`.

d. Enter a number (up to 7) specifying how many database backup files the management system stores. Once the management system reaches the maximum number of files configured, it overwrites the oldest file and creates a new backup. Press **ENTER** to accept the default setting of 7 backup files.

e. Enter a directory location where you want the management system to store the configuration settings you have set for the local database backup. Press **ENTER** to accept the default setting of `/var/netscreen/iHaSvr`.

```
$ root@docteam-attack:~$ rsync -a /var/netscreen/dbbackup /var/netscreen/dbbackup/oldbackups
```

```
1) Reinstall both Device Server and GUI Server
2) Patch both Device Server and GUI Server
Enter selection (1-2) [1]> 2

Will this machine require nightly local database backup? (y/n) [y]> y

The local database backup option requires that you have previously installed the rsync program. Enter path to rsync program [/usr/bin/rsync]>
Enter hour of day to start the database backup. GUI server will be restarted for backup purpose at this time everyday. All connected GUI clients will be disconnected at this time (00 = midnight, 02 = 2am, 14 = 2pm ...
)[02]> 03

Enter database backup directory [/var/netscreen/dbbackup]>
Enter number of nightly database backups to keep. The default value will keep backup copies for last seven days. The oldest backup copy will be overwritten by the new backup copy. [7]> 3

The Database Backup Tool stores all of the user data under a single directory.
By default, this directory is /var/netscreen/iHaSvr.

NOTE: This location is different from the backup directory. This directory is used to store configuration information.

```
Start server(s) when finished? (y/n) [y]> y
```

Enter `n` and then press **ENTER**, if you do not want to backup the database automatically.

The script then prompts you to specify whether or not you want to start both servers once the installer has completed the upgrade process.

6. Enter `y` and then press **ENTER** to start both servers once the installer has completed the upgrade process. Enter `n` and then press **ENTER**, if you do not want to start both servers.

---

**Note: Whenever you restart your operating system, both the GUI Server and Device Server start automatically.**

The script next prompts you to verify your installation configuration settings.

7. Verify your settings, and if they are correct, enter `y` and then press **ENTER** to proceed. If you enter `n` and then press **ENTER**, the installer returns you to the original Selection prompt.

The installation proceeds automatically. The installer proceeds to perform the following actions:

- extract the software payloads
- perform all applicable migration tasks
- patch the Device Server/GUI Server RPMs and set correct permissions.
- install the Database Backup Tool (if applicable)
- set start scripts
Upgrading the Management System - Typical Configuration

- start the server processes (if configured)

```
$ sudo docteam attack/tmp
```

```plaintext
************ EXTRACTING PAYLOADS ************
Extracting payload..........................ok
Decompressing payload.......................ok
gzip: payload.tgz: unexpected end of file
   ok

************ PERFORMING MIGRATION TASKS ************

************ PERFORMING INSTALLATION TASKS ************

----- PATCHING Device Server -----
Patching DevSvr RPM..........................ok
Putting NSROUT into start scripts............ok
Found crypto parameter, no need to add
Setting permissions for Device Server........ok
Patch of DevSvr complete.

----- PATCHING GUI Server -----
Patching GUI Svr RPM..........................ok
Putting NSROUT into start scripts............ok
Setting permissions for GUI Server..........ok
Patch of GUI Svr complete.

```

Several messages display to confirm the installation progress.

```
----- INSTALLING Database Backup Tool -----
Looking for existing RPM package..........ok
Removing existing Database Backup Tool RPM...ok
Installing Database Backup Tool RPM........ok
Creating var directory.....................ok
Creating /var netscreen/dbbbackup.........ok
Putting NSROUT into start scripts.........ok
Filling in config file(s)..................ok
Setting permissions for Database Backup Tool..ok
Installation of Database Backup Tool complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script.........ok
Enabling GUI Server start script............ok
Enabling Database Backup Tool start script...ok

************ PERFORMING POST-INSTALLATION TASKS ************
Removing staging directory..................ok
Starting GUI Server.........................ok
Starting Device Server......................ok
Starting Database Backup Tool..............ok

NOTES:
- Installation log is stored in /usr/netscreen/DevSvr/var/errorlog/installing.20040429123200

```

The installer runs for several minutes, and then exits.
The process for installing the management system on separate servers (i.e., in the extended configuration) is as follows:

1. Perform the pre-requisites steps described as if upgrading the management system in a typical configuration.
2. Run the management system installer on the server where you have currently installed the GUI Server. Specify that you want to patch the GUI Server only. Enable and configure automatic database backups (optional).
3. Run the management system installer on the server where you have currently installed the Device Server. Specify that you want to patch the Device Server only. Enable and configure automatic database backups (optional).
4. Give the Device Server approximately 10-15 minutes to successfully re-connect to the GUI Server.
5. Run the UI installer on the computers where you have currently installed the UI client.
6. Connect the UI installer to the management system.
7. Validate that you have successfully upgraded to Netscreen-Security Manager 2004 FP1.
Validating Management System Status

If you specified that you want the installer to start server(s) when finished, it is recommended that you view the status of the HA Server, Device Server and GUI Server to confirm that all services are up and running.

To check the status of the HA Server process:

1. Navigate to the iHaServer bin subdirectory (i.e., /usr/netscreen/iHaSvr/bin).
2. Run the following command:
   
   `sh iHaSvr.sh status`

   ![Status of iHaServer](image1)

To check the status of the GUI Server:

1. Navigate to the GUI Server bin subdirectory (i.e., /usr/netscreen/GuiSvr/bin).
2. Run the following command:
   
   `sh guiSvr.sh status`

   ![Status of GUI Server](image2)

To check the status of the Device Server:

1. Navigate to the Device Server bin subdirectory (i.e., /usr/netscreen/DevSvr/bin).
2. Run the following command:

   ![Status of Device Server](image3)
sh devSvr.sh status

Refer to “Controlling the Management System” on page 76 for more information on manual commands that you can send to the management system.
Viewing the Installation Log

The installer generates a log file with the output of the installation commands for troubleshooting purposes. This file is saved by default in the tmp subdirectory.

The naming convention used for the installation log file is:
netmgtInstallLog.<current date><current time>

For example if you ran the installer on December 1, 2003 at 6:00pm, the installation log file would be named: netmgtInstallLog.20031201180000

*Note: Once the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.*
UPGRADING THE USER INTERFACE

The Security Manager User Interface (UI) installer launches an InstallAnywhere wizard that you can run on any Windows or Linux-based computer that meets minimum system requirements. The InstallAnywhere wizard guides you through all the steps required to configure and install the Security Manager UI.

Refer to Chapter 1, “Introduction” for more information on running the UI installer. Once you install the UI, you can connect it to the management system.
VALIDATING THE UPGRADE

Once you have upgraded the management system and UI, it is recommended that you validate basic information configured on the Device Server. You can use the Server Manager in the Security Manager UI to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the Security Manager UI, double-click on the **Server Manager** module. The Server Manager module expands, and the Servers and Server Monitor appears.
2. Click on the **Servers** node. The Servers view appears displaying Device Server and GUI Server information.
3. Click on the Device Server and click on the **Edit** icon or right-click on the Device Server and select **Edit** to view all information available on the Device Server.

4. Use the **General** tab to verify the following information:
- **Mapped IP address** - the IP address that is manually defined in the UI.

Note: You can configure the Device Server to use a Mapped IP (MIP) address. A MIP maps the destination IP address in an IP packet header to another static IP address, enabling the FW/VPN device to receive incoming traffic at one IP address, and automatically forward that traffic to the mapped IP address. MIPs enable inbound traffic to reach private addresses in a zone that contains NAT mode interfaces.

- **Device Server Manager Port** - the default port is 7800.

- **Password for GUI Server Connection** - This password authenticates communication between the Device Server and GUI Server.

- **Device Server ID** - the ID number identifies the Device Server; you cannot change the Device Server ID.

5. Click **OK** when you are done.

6. Click **OK**.
Next Steps

Congratulations! You have successfully completed upgrading the Security Manager management system and User Interface. You can now begin to manage your network using Security Manager 2004 FP1. Refer to the *NetScreen-Security Manager 2004 FP1 Administrator’s Guide* for information describing how to plan and implement Security Manager for your network.
In This Chapter

- Controlling the Management System
- Maintaining the Management System
- Archiving and Restoring Logs and Configuration Data
- Automatic Database Backup Option
- Installing a TFTP Server
- Uninstalling the User Interface

This chapter describes basic procedures used to administer Security Manager. This includes instructions describing how to manually send commands to the management system such as start and stop, change the IP address of the GUI Server (in the event that you move the GUI Server to another server), install a TFTP server (required if you are managing FW/VPN devices running ScreenOS 4.0.x), and uninstall the management system and UI.
CONTROLLING THE MANAGEMENT SYSTEM

On occasion, it may become necessary to start or stop the management system processes manually. You can control the management system by navigating to the appropriate “bin” subdirectory for the Device Server, GUI Server, or HA Server, and issuing a manual command.

The management system supports the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload</td>
<td>sends a hangup signal to the management system process, then instructs the process to reload its configuration and start again.</td>
</tr>
<tr>
<td>restart</td>
<td>stops the management system process for 2 seconds, then restarts the process.</td>
</tr>
<tr>
<td>start</td>
<td>starts the management system process</td>
</tr>
<tr>
<td>stop</td>
<td>stops the management system process</td>
</tr>
<tr>
<td>status</td>
<td>provides a status of the management system process</td>
</tr>
<tr>
<td>version</td>
<td>lists the current version of the management system</td>
</tr>
</tbody>
</table>

Viewing Management System Commands

To view all the manual commands that you can send to the GUI Server:

1. Navigate to the GUI Server bin subdirectory (i.e., `/usr/netscreen/GuiSvr/bin`).
2. Run the following command:
   ```bash
devSvr.sh
   ```

To view all the manual commands that you can send to the Device Server:

1. Navigate to the Device Server bin subdirectory (i.e., `/usr/netscreen/DevSvr/bin`).
2. Run the following command:
   ```bash
devSvr.sh
   ```

To view all the manual commands that you can send to the HA Server:

1. Navigate to the HA Server bin subdirectory (i.e., `/usr/netscreen/iHaSvr/bin`).
2. Run the following command:
   ```bash
   iHaSvr.sh
   ```
Starting Server Processes

You can manually start each server process as follows.

To start the GUI Server manually:
1. Navigate to the GUI Server bin subdirectory (i.e., /usr/netscreen/GuiSvr/bin).
2. Run the following command:
   ./guiSvr.sh start

*Note: Always start the GUI Server before starting the Device Server. When started, the Device Server attempts to connect to the GUI Server. If the GUI Server is not already up and running, the Device Server will fail to connect to it.*

To start the Device Server manually:
1. Navigate to the Device Server bin subdirectory (i.e., /usr/netscreen/DevSvr/bin).
2. Run the following command:
   ./devSvr.sh start

To start the HA Server process manually:
1. Navigate to the HA Server bin subdirectory (i.e., /usr/netscreen/iHaSvr/bin).
2. Run the following command:
   ./iHaSvr.sh start

*Note: If you start the HA Server process, it automatically starts the GUI Server and Device Server processes.*

Stopping Server Processes

You can manually stop each server process as follows.

To stop the GUI Server manually:
1. Navigate to the GUI Server bin subdirectory (i.e., /usr/netscreen/GuiSvr/bin).
2. Run the following command:
   ./guiSvr.sh stop

To stop the Device Server manually:
1. Navigate to the Device Server bin subdirectory (i.e., /usr/netscreen/DevSvr/bin).
2. Run the following command:
   ./devSvr.sh stop
To stop the HA Server process manually:

1. **Navigate to the HA Server bin subdirectory (i.e., /usr/netscreen/iHaSvr/bin).**
2. **Run the following command:**
   ```bash
   ./iHaSvr.sh stop
   ```
MAINTAINING THE MANAGEMENT SYSTEM

The following procedures are provided for your reference:

- "Changing the Management System IP Address" on page 79
- "Changing the Device Server IP Address" on page 79
- "Changing the GUI Server IP Address" on page 80
- "Changing Permissions To a Normal User" on page 80
- "Uninstalling the User Interface" on page 89

Changing the Management System IP Address

If you have installed the Security Manager management system on a single server (i.e., in the basic configuration), and you move it later to a different server, you need to re-configure the management IP address and port enabling your managed FW/VPN devices to connect to it at its new location.

To change the management system IP address:

1. Update the Device Server IP on each FW/VPN device (or set the secondary management server IP to the new IP address).
2. Login to the server where you are running the Device Server as root.
4. Open the Device Server configuration file (devSvr.cfg) in any text editor.
5. Edit the values for the guiSvr.addr and guiSvr.port variables using the new IP address and port number.
6. Open the server_table.nml file in any text editor.
7. Edit the values for the IP Address in both GUI and Device Server sections.
8. Restart the GUI Server, then restart the Device Server.

Changing the Device Server IP Address

If you have installed the Security Manager management system on separate servers (i.e., in the extended configuration), and you later move the Device Server to a different server, you need to re-configure the management IP address and port enabling your managed FW/VPN to connect to it at its new location.

To change the Device Server IP address:

1. Update the Device Server IP on each FW/VPN device (or set the secondary management server IP to the new IP address).
2. Login to the server where you are running the Device Server as root.
4. Open the server_table.nml file in any text editor.
Chapter 5 Administration

7. Edit the values for the IP Address in the Device Server section only.
8. Restart the GUI Server.

Changing the GUI Server IP Address

If you have installed the Security Manager management system on separate servers (i.e., in the extended configuration), and you later move the GUI Server to a different server, you need to re-configure the management IP address and port enabling the Device Server to connect to it at its new location.

To change the GUI Server IP address:
1. Login to the server where you are running the Device Server as root.
3. Open the Device Server configuration file (devSvr.cfg) in any text editor.
4. Edit the values for the guiSvr.addr and guiSvr.port variables using the new IP address and port number. Save the file.
5. Login to the server where you are running the GUI Server as root.
7. Open the server_table.nml file in any text editor.
8. Edit the values for the IP Address in the GUI Server section only. Save the file.
9. Restart the GUI Server, then restart the Device Server.

Changing Permissions To a Normal User

The Security Manager management system runs by default as the root user. If you want change this default behavior to a more secure setup, you can create a normal user (i.e., called “nsm”), and change permissions to that user. For your convenience, a script called “setperms.sh” is included for both the Device Server and GUI Server that will automatically change the setuid.user value in case they want to switch to the more secure setup.

Note: You cannot change permissions and run the HA Server as any user other than root. You must run the HA Server as root.

To create a normal user and change permissions:
1. Stop the Device Server. For example, you can do this by running the following command:
   
   cd /usr/netscreen/DevSvr/bin
   ./devSvr.sh stop

2. Stop the GUI Server. For example, you can do this by running the following command:
   
   cd /usr/netscreen/GuiSvr/bin
   ./guiSvr.sh stop
3. Create a normal user called “nsm”. Create a group called “nsm”, with the user nsm as the only member. You can do this by typing the following commands:

```bash
    groupadd nsm
    useradd -g nsm nsm
```

4. Run the change permissions script on the Device Server. For example, you would run the following command:

```
    /usr/netscreen/DevSvr/utils/setperms.sh DevSvr
```

5. Run the change permission script on the GUI Server. For example, you would run the following command:

```
    /usr/netscreen/GuiSvr/utils/setperms.sh GuiSvr
```

6. Start the GUI Server.

7. Start the Device Server

8. Verify that the permissions you set are working correctly. One way to check is to verify that Security Manager servers can write to disk. You can do this by adding a new device and seeing if it appears in the device table file.

## Uninstalling the Management System

To uninstall previous management system installations:

1. Stop the Device Server. For example, you can do this by running the following command:

```
    cd /usr/netscreen/DevSvr/bin
    ./devSvr.sh stop
```

2. Stop the GUI Server. For example, you can do this by running the following command:

```
    cd /usr/netscreen/GuiSvr/bin
    ./guiSvr.sh stop
```

3. Stop the HA Server. For example, you can do this by running the following command:

```
    cd /usr/netscreen/iHaSvr/bin
    ./iHaSvr.sh stop
```

4. Navigate to the var subdirectory, and remove all files in the netscreen subdirectory. For example, you can do this by running the following commands:

```
    rpm -e netscreen-DevSvr
    rpm -e netscreen-GuiSvr
    rm -rf netscreen
```
ARCHIVING AND RESTORING LOGS AND CONFIGURATION DATA

You can archive and retrieve log and configuration data in Security Manager using standard Unix commands. Logs reside on the Device Server. All other configuration information, including device configuration data, administrators, policies, audit logs and job information resides on the GUI Server.

Before you begin archiving, it is important that you first stop the processes running on both servers. After you have stopped both servers, use the “ls -al” command to identify the actual paths of the GUI Server and Device Server data directories. You should issue this command on the following directory locations:

- For all information on the GUI Server: /usr/netscreen/GuiSvr/var
- For all information on the Device Server: /usr/netscreen/DevSvr/var

These directories are links representing paths that are entered at the time you installed the server.

After you have completed archiving, restart both server processes.

Archiving Logs and Configuration Data

To archive log and configuration data:

1. Stop the Device Server.
2. Stop the GUI Server.
3. Use the "ls -al" command to discover the actual paths of the GUI Server and Device Server data directories. These are the directories that you need to back up. For example:
   
   ```
   ls -al /usr/netscreen/GuiSvr/var
   lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr var -> /var/netscreen/GuiSvr
   ```
   
   The output in the example indicates that the actual location of the GUI Server data is in /var/netscreen/GuiSvr. Verify on your own system where your data is stored and which directories should be backed up. Follow the same procedure to determine the location of your data on the Device Server.

4. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example:
   
   ```
   tar -cvf /netscreen_backup/db-date.tar /var/netscreen/GuiSvr
   ```

5. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data. Using tar may not be appropriate for log data in the Device Server which may be very large. It is recommended that you use either Secure Copy or FTP to backup the Device Server data.

   For example using scp:
   
   ```
   scp -r <local directory> usr@host:<remote-directory>
   ```
For example, using ftp:

```plaintext
ftp <host name>
b
hash
lcd <local directory>
prompt
mput
```

7. Start the Device Server.

## Restoring Logs and Configuration Data

To restore log and configuration data:

1. Stop the Device Server.
2. Stop the GUI Server.
3. Use the `mv` command to transfer data from the "var" directories to a safe location.
4. Untar or otherwise place your backups into both of the locations described above.
5. Start GUI Server.

**Note:** These instructions apply only to systems where the "var" links point to a true location outside the prescribed locations (e.g., `/usr/netscreen/GuiSvr` or `/usr/netscreen/DevSvr`). It is not recommended that you have these links point to locations that are inside `/usr/netscreen/GuiSvr` or `/usr/netscreen/DevSvr`. This will complicate any upgrade of Security Manager and will require special precautions during backup and restore.
AUTOMATIC DATABASE BACKUP OPTION

If you installed and configured the option to perform automatic database backups, the utility performs the following actions on a daily basis:

- waits for all processes on the server to complete
- stops the running server process.

*Note: During this time, all UI clients currently connected to the management system are disconnected.*

- backs up all relevant data in a file called backupN where N is the number day of the week (i.e., backup1 is the backup file saved on Monday, backup7 is the backup file saved on Sunday). The file is saved in the database directory location specified at installation.
- restarts the running server process(es)

During this time, users will not be able to perform any changes to the management system until the system is restarted.

*Note: If you have installed the management system on separate servers (in the extended configuration), and you wish to perform automatic database backups, you must install and configure the option on both the GUI Server and Device Server.*

Configuring the Automatic Database Backup Option

You can manually configure the behavior of the automatic database backup option by manually editing a configuration file (called iHaSvr.cfg) in the automatic database backup configuration directory.

To configure the automatic database backup tool:

1. Stop the running server process(es).
2. Navigate to the automatic database backup configuration directory (this is var/netscreen/iHaSvr by default).
3. Open the automatic database backup option configuration file (iHaSvr.cfg) in any text editor.
4. Configure the file as needed:
   a. To change the automatic database backup directory, edit the value for the iHighAvail_pathDbBackup variable.
   b. To change the time of day that the automatic database backup begins, edit the value for the iHighAvail_backupTimeHour variable.
   c. To change the number of backup files that the tool saves, edit the value for the iHighAvail_numofBackup variable.
   d. To change the path to the rsync package, edit the value for the iHighAvail_rsyncLocation variable.
Automatic Database Backup Option

For example, if you wanted to change the time of day that the automatic database backup begins to 4:00am, and you wanted to reduce the number of backup files to 3, the configuration file would appear as follows:

```
5. Save the file.
6. Restart the running server process.

Restoring the Database

If for any reason you are required to restore the database, you can do so by invoking a shell archive script.

To restore the database:

1. Install NetScreen-Security Manager 2004 FP1 on a new server machine. The new server machine is required to use:
   - the same IP Address as the previous server that you ran the GUI Server
   - the same operating system that you ran on the previous server

   During the installation, you must also install and configure the automatic database backup option on both the GUI Server and Device Server.

2. Save your remote copy of the database backup file(s) for the appropriate day of the week to the automatic database backup data directory on your new management system server.

3. Navigate to the HA Server utilities subdirectory `/usr/netscreen/iHaSvr/utils` by default.

4. Run the database restore shell archive script and specify the number day of the week for the backup file that you wish to restore from (i.e, N = backup day of the week). You can do so by running the following command:
   `restoreDbFromBackup.sh N`
   For example, if you wanted to restore the backup file from Friday, you would run the following command:
   `sh restoreDbFromBackup.sh 5`
The restore script runs automatically. It first prompts you to confirm stopping the running server process(es). It then proceeds to verify that you have properly logged in as the root user. It then verifies that the backup file specified exists. If so, the script proceeds to stop all running server processes. It then uses rsync to copy the backup file to the appropriate server directories. Once it has completed restoring the files, it restarts all server processes.

Validating the Database Recovery Process

If you are using the automatic database backup option on a network where the GUI Server and Device Server are installed on separate systems, it is possible that you may experience issues with devices reconnecting to the management system after you have restored the database. This is likely to occur if you did not install the automatic database backup option properly on both the GUI Server and Device Server. In this event, contact technical support for assistance.
Installing a TFTP Server

If you are using Security Manager to manage FW/VPN devices running ScreenOS 4.0.x, you must install and run a TFTP server on the system that you are running the GUI Server. The TFTP server is required to enable firmware updates for FW/VPN devices running ScreenOS versions 4.0.x.

Installing a TFTP Server on Linux

Before installing the TFTP server on your Red Hat Linux server, you should first check to see if it is already installed.

To verify if the TFTP server is already installed on your Linux server, run the following command:

```bash
rpm -q tftp-server
```

If the TFTP server is installed, the output indicates the following:

```
tftp-server-<version>-<revision>
```

For example, the output for an unpatched Red Hat 9.0 server is as follows:

```
tftp-server-0.32-4
```

If the TFTP server is not installed, download and install the package from the Red Hat Linux installation CD, or from the Internet at the Red Hat or Red Hat mirror site. Once the package is installed, you must enable and configure the TFTP server.

To configure and enable the TFTP server on Linux:

1. Open the `/etc/xinetd.d/tftp` file in any text editor.
2. Edit the parameter “server_args =” so that the value is “-s /usr/netscreen/DevSvr/var/cache.”
3. Edit the parameter “disable” so that the value is “no”. The file should now appear as follows:

   ```
   service tftp
   {
   socket_type = dgram
   protocol = udp
   wait = yes
   user = root
   server = /usr/sbin/in.tftpd
   server_args = -s /usr/netscreen/DevSvr/var/cache
   disable = no
   per_source = 11
   cps = 100 2
   }
   ```
4. Restart the xinetd service. You can do so by running the following command:
   
   ```
   service xinetd restart
   ```

## Installing a TFTP Server on Solaris

By default, Solaris installs the TFTP service on your machine but leaves it disabled. To configure and enable the TFTP service on Solaris:

1. Open the `/etc/inetd.conf` file in any text editor.
2. Uncomment the line that begins with the word “tftp” or “#tftp”.
3. Edit the same line by replacing the words “in.tftpd -s /tftpboot” at the end of the line with “in.tftpd -s /usr/netscreen/DevSvr/var/cache”. The line should now appear as follows:

   ```
   tftp dgram udp wait root /usr/sbin/in.tftpd
   in.tftpd -s /usr/netscreen/DevSvr/var/cache
   ```

4. Restart the inetd service. You can do so by running the following commands:

   ```
   /etc/init.d/inetsvc stop
   /etc/init.d/inetsvc start
   ```
UNINSTALLING THE USER INTERFACE

If it is necessary to uninstall the Security Manager UI, run the Security Manager uninstall program.

Note: If you are uninstalling the UI on a Windows-based computer, it is not recommended that you use the Add/Remove Programs utility to remove the Security Manager UI.

To uninstall the Security Manager UI:

1. On a Windows-based computer, use the Start menu, and select NetScreen-Security Manager>Uninstall Security Manager.

   On a Linux-based computer, you can either double-click on the Uninstall_NetScreen_Security Manager icon, or you can launch the UI uninstaller from a command line. From the command line, you can run the following command:

   sh Uninstall_Netscreen-Security_Manager

   The uninstaller launches.

2. Click the Uninstall button to uninstall the UI. The uninstaller proceeds to uninstall all the UI software files, shortcuts, folders and registry entries.

   When the uninstaller has finished, a window appears indicating that all files were successfully uninstalled.

3. Click Done to exit the uninstaller.
Technical Overview

This appendix describes the Security Manager three-tiered architecture. This includes a description of the management system, User Interface (UI), and the FW/VPN devices managed in your network.
**TECHNICAL OVERVIEW**

The Security Manager management architecture is designed to provide optimum security, scalability, and flexibility for integrating with your specific network security environment. It includes the following key components:

- Management System
- User Interface (UI)
- Managed FW/VPN devices

---

**About the Management System**

The management system used in Security Manager provides all the functionality required to integrate management of all the components in your network security environment. It enables you to centrally gather, store, configure, manage, monitor and generate reports on the FW/VPN devices you have deployed in your network.

The management system itself is composed of two distinct components:

- GUI Server
- Device Server
Both the GUI Server and Device Server working together are collectively referred to as the Security Manager “management system”.

You can install both components of the management system on the same physical server or on separate servers. By separating the two server components, you can improve system performance.

### GUI Server

The GUI Server receives and responds to requests and commands from the Security Manager User Interface. It manages all the system resources and configuration data required to manage your network. It also contains a local data store where information about your managed FW/VPN devices, administrators, and configurations are centralized.

*Note: The GUI Server can accommodate no more than 20 User Interfaces connected to it at any time. This is the maximum number of UI clients supported in this release of Security Manager.*

### Device Server

The Device Server acts as a collection point for all data generated by each FW/VPN device in your network. The Device Server stores this data, primarily traffic logs generated by the device, in a local data store.

*Note: The Device Server can accommodate no more than 1000 FW/VPN devices connected to it at any time. This is the maximum number of FW/VPN devices supported in this release of Security Manager.*
HA Server

There is an additional server process called the HA Server that continuously monitors the GUI Server and Device Server processes. If the HA Server process detects that either the GUI Server or Device Server is down, it automatically restarts the process.

About the Security Manager User Interface (UI)

The Security Manager User Interface (UI) is a java-based software application that you use to access and configure data about your network on the management system. Once you have installed the UI, you can launch it and connect it to the management system. From the UI, you can view, configure, and manage your network from a single, central administrative location. Refer to the NetScreen-Security Manager 2004 FP1 Administrator's Guide or the Online Help included in the UI for more information about the Security Manager UI.

About Managed FW/VPN Devices

The managed FW/VPN devices that you have implemented in your network are the lowest tier of the Security Manager management architecture. All of the information about your network security environment originates from the devices that you have installed in your network.

The following table details the FW/VPN devices and versions of ScreenOS supported by Security Manager.

<table>
<thead>
<tr>
<th>FW/VPN Device</th>
<th>ScreenOS Versions Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS5XP</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5XT</td>
<td>4.0.0, 4.0.0-DIAL2, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS25</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS50</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS100</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS204</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS208</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS500</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5200/8</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0</td>
</tr>
<tr>
<td>NS5200/24</td>
<td>4.0.0-SBR, 4.0.1-SIBR, 5.0</td>
</tr>
<tr>
<td>NS5400</td>
<td>4.0.0-SBR, 4.0.0-SIBR, 5.0</td>
</tr>
<tr>
<td>NS5GT</td>
<td>4.0.0-DIAL2, 5.0 only</td>
</tr>
<tr>
<td>NS-HSC</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS-ISG-2000</td>
<td>5.0 only</td>
</tr>
</tbody>
</table>
You need to enable each FW/VPN device to communicate and work with Security Manager. Refer to the *ScreenOS 5.0 Concepts and Examples Guide* for more information describing how to enable management on your FW/VPN devices.

Once enabled, each FW/VPN device communicates and sends information to the Security Manager management system. From Security Manager, you can centralize all configuration data, and manage the network from a single, central, administrative location. You can then implement your security policies by “pushing” or sending configuration updates back to your devices.

Based on the configuration policies you define in Security Manager, the managed FW/VPN devices provide the firewall and VPN services required to secure your network environment.

**Communications**

As you plan your installation, it helps to understand how Security Manager establishes communication between the User Interface, Management System, and FW/VPN devices.

**Communication Ports and Protocols**

For optimum security, the number of total ports on the GUI Server and Device Server is kept to a minimum:

- there is only one open port on the GUI Server - an inbound TCP port that listens for incoming connection requests from the UI(s) and Device Server.
- there are six ports on the Device Server: 4 inbound TCP ports supporting connection requests from existing FW/VPN devices; and 2 outbound TCP ports used to establish communication with FW/VPN devices running ScreenOS 4.0.X.

The following table summarizes the port that is open on the GUI Server.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7801</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming connection requests from the Security Manager UI(s) and Device Server. Used to establish communication session with <strong>Device Server</strong> and/or <strong>Security Manager UI(s)</strong>. This communication session uses an <em>encrypted</em> form of TCP called Secure Server Protocol (SSP). It is also a duplexed connection enabling the UI and GUI Server to communicate back and forth to each other after the connection is established.</td>
</tr>
</tbody>
</table>
The following table summarizes the ports that are open on the Device Server.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7800</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming connection requests from FW/VPN device(s) running ScreenOS version 5.0+. Used to establish encrypted communication sessions with the GUI Server and FW/VPN devices (running ScreenOS v5.0+).</td>
</tr>
<tr>
<td>15400</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming Report Manager NetScreen protocol (NSP) connection requests from FW/VPN device(s) using ScreenOS 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>11122</td>
<td>TCP</td>
<td>INBOUND</td>
<td>listens for incoming NACN connection requests from FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>INBOUND</td>
<td>listens for incoming TFTP connection requests from FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS v4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
<tr>
<td>22/23</td>
<td>TCP</td>
<td>OUTBOUND</td>
<td>sends outbound Telnet/SSH connection requests to FW/VPN device(s) using ScreenOS v4.0.x. Used to establish communication sessions with FW/VPN devices running ScreenOS v4.0.x. While SSH sessions are encrypted, Telnet sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.</td>
</tr>
</tbody>
</table>
Security Manager uses the Secure Server Protocol (SSP) to provide secure communication between each management system component (i.e., GUI Server, Device Server, and User Interface), as well as between the Device Server and the FW/VPN devices managed in your network. SSP offers strong encryption and authentication mechanisms, so management traffic is protected and kept confidential. SSP utilizes RSA public key cryptography, AES symmetric encryption, and HMAC-SHA-1 hashing.

Using the Secure Server Protocol (SSP)

Communications With Devices Running ScreenOS 5.0+

If you are deploying Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and higher, note that SSP uses two TCP ports for communication:
• TCP port 7800 for the Device Server
• TCP port 7801 for the GUI Server

You must therefore, allow TCP port 7800 on firewalls deployed between the Security Manager management system and the FW/VPN devices managed in your network. You must also configure firewalls between the GUI Server and UI clients to allow TCP port 7801.

The following table lists and describes the ports used specifically in communications between Security Manager and ScreenOS 5.0 devices.

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 7800</td>
<td>Accepts incoming ScreenOS 5.0 device connections</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 7801</td>
<td>On a separated install, used to communicate with GUI server</td>
</tr>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to import initial configs of 5.0 devices.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7801</td>
<td>Accepts communication from Device Server and Client GUI</td>
</tr>
</tbody>
</table>

**Note:** The Device Server may use port 22 (SSH) to import the configuration of existing FW/VPN devices running ScreenOS 5.0. After device import, all communication goes over SSP port 7800. FW/VPN devices running ScreenOS 5.0 also support SSH v2.

**Communicating With Devices Running Screen 4.x and Earlier**

FW/VPN devices running ScreenOS 4.x and earlier utilize the same communication protocols for communicating with Security Manager that were supported with NetScreen-Global PRO:

• Device configuration is performed via telnet or SSH1.
• Logging information is sent over the NetScreen Server Protocol (TCP port 15400).
• TFTP (UDP port 69) is used for sending firmware updates.
• NetScreen Address Change Notification (NACN), supported in ScreenOS 4.x devices, uses TCP port 11122.

Since some of these protocols (i.e., TCP port 15400, Telnet port 23, TFTP) are not encrypted or authenticated, an IPSEC tunnel between the management server and the FW/VPN devices running 4.x and earlier is strongly recommended.
The following table lists and describes the ports used specifically in communications between Security Manager and ScreenOS 4.x and earlier devices.

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server</td>
<td>Outbound TCP: 22/23</td>
<td>SSH/Telnet to manage FW/VPN devices running ScreenOS 4.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 15400</td>
<td>Management for FW/VPN devices running ScreenOS 4.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound UDP: 69</td>
<td>TFTP server for updating FW/VPN devices running ScreenOS 4.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 11122</td>
<td>Accepts incoming NACN requests for FW/VPN devices running ScreenOS 4.x.</td>
</tr>
</tbody>
</table>

**Creating a Separate Management Network**

It is recommended you isolated the Security Manager management system from the rest of your network traffic. You should send management traffic on a separate management network, and you should deploy a firewall to enforce access policies on the management network.

If you are deploying Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and ScreenOS 4.x, you must configure the firewall protecting the management network to allow:

- TCP ports 7800 and 11122 to the Device Server
- TCP port 15400 and UDP port 69 to the Device Server over VPN tunnels
- TCP port 22 outbound from the Device Server

You do not need to allow traffic to or from the GUI Server if you deploy your UI clients inside the management network. If you must deploy UI clients outside the management network, you must allow TCP port 7801 access to the GUI Server in the firewall protecting the management network.

For management of ScreenOS 5.0 devices, it is recommended that you use SSP on the untrust interface, as this configuration reduces the possibility of losing access to the device due to an invalid configuration update.

For management of ScreenOS 4.x and earlier devices, it is recommended that you use SSH to the untrust interface. In addition, you should configure a VPN tunnel to send logs/events via TCP port 15400 and firmware updates via TFTP.
Sizing and Capacity Planning

This appendix provides guidelines to help you size your hardware to accommodate specific network requirements.
SIZING AND CAPACITY PLANNING

As you plan to implement Security Manager in your network, you will want to consider issues specific to your network (i.e., sizing, memory or capacity) that may influence the hardware you choose to install on. The following guidelines are provided to help you size your hardware to accommodate specific network requirements.

Key hardware components that are affected by specific usage requirements include:

- “Memory” on page B-II
- “Processor Requirements” on page B-II
- “Disk Storage” on page B-II
- “Network Bandwidth” on page B-III

Memory

Log viewing, querying and investigating, as well as importing device configurations are all activities that increase the overall memory requirements for your management system. The number of devices and the complexity of their configurations also contributes to overall memory requirements. If you anticipate keeping a large amount of data available (online), it is highly recommended that you add additional memory to your system.

Processor Requirements

Security Manager is a multi-process, multi-threaded environment. The more processing power provided the better.

Disk Storage

The requirement for disk storage on the management system is largely determined by the amount of traffic logs that you are expected to generate, as well as those that you are required to record on a daily basis.

Traffic logs are stored on the Device Server in separate files, each covering a 24 hour time period. Each log on average is typically 100 bytes or less in size. Each daily log file varies in size depending on the total number of logs that you receive. The exact number of days you can store depends on the total size of these files.

You can store as many logs as you have chosen to provide disk space for. As disk space allocated for logs on the Device Server is maxed out, the system begins deleting the oldest logs currently stored on the system.

Configuration data is stored on the GUI Server. This information is not expected to exceed minimum system requirements for disk storage.
Network Bandwidth

Security Manager employs a symmetric key encryption algorithm that does not impact the size of data transported over the network. In most cases, a 56K connection is the minimum connection required for the User Interface to communicate with the Security Manager management system; and a 10/100MBps Ethernet connection for communications between the Security Manager management system and your managed FW/VPN devices.

Hardening Your System

Since Security Manager is a software-only product, it is highly recommended that you take all the necessary precautions to reduce any hardware security vulnerabilities.

Refer to documentation relevant to the platform on which you are installing Security Manager (e.g., Bastille Linux project, Sun BluePrints, the Linux Administrators’ Security Guide, YASSP or www.openssh.com) for more specific information describing how to harden your system.

The following guidelines are provided as general recommendations for improving your hardware security.

- Firewall Protection
- Dedicating the System
- Securing Communications
- Installing Updates and Security Patches

Firewall Protection

It is recommended that you implement a layered approach to system security.

The first layer of protection for your Security Manager system is the network firewall. As you plan to deploy Security Manager, it is highly recommended that you place the management system behind a network firewall.

If you are implementing Security Manager components behind a firewall, you must create a security rule permitting traffic through all management system communication ports. Refer to Communications for more information on the management system’s communication ports.

Dedicating the System

The management system computer should run only those components required for Security Manager.

It is recommended that you remove all unnecessary components and services. For example, if you do not need e-mail on the management system, turn SMTP off. If you do not need DNS server functionality, you can turn DNS off. If not set, you can turn telnet off.
Securing Communications

The management system server should not listen on any ports except those used by Security Manager for management. It is also recommended that you create security policies governing the use of the management system server.

Installing Updates and Security Patches

It is highly recommended that you install all the latest manufacturer-supplied updates and security patches.

Additional Information

The detailed system requirements for each deployment of Security Manager can vary greatly from installation to installation, depending on the size and topology of the network. For additional information, it is recommended that you consult with your NetScreen Professional Services representative.
Index

A
adding, Device Server 46
automatic database backup
  configuring manually 84
  overview 84
automatic database backup option
  configuring 18, 41, 48

C
capacity planning, management system B-II–B-IV
certificates
  files 53
  transferring 53
changing
default user management system runs as 80
communication ports A-V–A-IX
communications A-V–A-IX
configuration options
  installing management system on same server
    (typical) 6
  installing management system on separate
    servers (extended) 7
configuring
  automatic database backup option 18, 41, 48
  Device Server data directory 19
  Device Server ID 50
  GUI Server data directory 19
  management system IP addresses 80
  password for GUI Server connection 50
  password for super user 20
CPU
  requirements on management system, same
    server 4
  requirements on management system, separate
    servers 4

D
data directory
  for device-server, described 11, 37
  for GUI-server, described 11, 37
defining system parameters 11, 37
Demo Mode 32
Device Server
  adding 46
  communication ports, described A-VI
  data directory, configuring 19
  described A-III
  installing 47–52
  starting 77
  stopping 77
Device Server ID
  configuring 50
  described 37
devices
  see FW/VPN devices
disabling
  X Server 14, 58
disk storage
  requirements on management system, same
    server 4
  requirements on management system, separate
    servers 4

d E
  extended configuration option 7

F
FW/VPN devices
  maximum number supported A-III
  platforms supported A-IV

G
Global PRO data export utility 3
GUI Server
  communication ports, described A-V
  data directory, configuring 19
  described A-III
  installing 40–45
  starting 77
  stopping 77
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>

**H**
- hardening your system B-III–B-IV
- hardware
  - capacity planning B-II-B-III
  - requirements for UI 5

**I**
- installation
  - log file for management system 23–24, 45, 69
  - log file for UI 29
- installing
  - configuration options 6
  - Device Server 47–52
  - GUI Server 40–45
- management system on same server 10–24
- management system on separate servers 36–53
- prerequisite steps 13–16, 57–60
- TFTP server on Linux 87
- TFTP server on Solaris 88
- UI 25–29

**L**
- Linux RPM package
  - requirements 13, 57
  - verifying 13, 57
- log file
  - management system install 24, 69
  - UI installation 29
- logging in to the UI 29

**M**
- management IP address
  - for GUI-server, described 37
  - management IP address for GUI-server 11
- management server
  - see management system
  - management system
    - capacity planning B-II-B-IV
    - changing default user 80
    - commands 76
    - described A-II–A-III
    - installing on same server 10–24
    - installing on separate servers 36–53
    - restarting 76

- starting 76
- status 76
- stopping 76
- uninstalling 81
- upgrading 56–69

**memory requirements**
- capacity planning B-II
  - for UI 5
  - management system on same server 4
  - management system on separate servers 4

**minimum system requirements**
- described 4–5
  - for UI 5
  - management system 4

**N**
- network connection
  - requirements for UI 5
  - requirements on management system, same server 4
  - requirements on management system, separate servers 4

**O**
- operating system
  - requirements for management system 4
  - requirements for UI 5

**P**
- password
  - super user, configuring 20
  - super user, described 11
- Password for GUI Server connection
  - configuring 50
  - described 37
  - prerequisites before installing 13–16, 57–60
  - prerequisites before upgrading 57–60

**R**
- restarting
  - management system manually 76
- restarting management system 76
- restoring
  - database 85
root user
    changing user that management system runs as 80
rsync
    defining path to utility 12
running
    UI 29
    UI, in Demo Mode 32
S
ScreenOS versions supported A-IV
securing Security Manager B-III–B-IV
Security Manager technical overview A-II–A-IX
server
    see management system
sizing
    see capacity planning
starting
    Device Server 77
    GUI Server 77
    management system manually 76
stopping
    Device Server 77
    GUI Server 77
    management system manually 76
super user
    password, configuring 20
    password, described 11, 37
swap space
    requirements on management system, same server 4
    requirements on management system, separate servers 4
system parameters 11, 37
system update utility
    described 3
T
TFTP server
    installing 87–88
    installing on Linux 87
    installing on Solaris 88
    typical configuration option 6
U
UI
    described A-IV
    hardware requirements 5
    installing 25–29
    operating system requirements 5
    running 29
    uninstalling 89
    upgrading to FP1 70
    uninstalling
        management system 81
        UI 89
    upgrading
        management system 56–69
        management system on separate servers 66
        prerequisite steps 57–60
        UI 70
    upgrading RPM package (for Linux only) 14–16, 58–60
    user interface
        See UI
V
validating
    database recovery 86
    management system installation 31
    management system status 23, 52, 67
    management system upgrade 71
verifying Linux RPM package 13, 57
viewing management system commands 76
X
X Server
    disabling 14, 58