NetScreen-Security Manager 2004
Installer’s Guide

Release FP3
# Table of Contents

Audience ................................................................................................................................. 2
Conventions ............................................................................................................................ 3
  User Interface Conventions ................................................................................................. 4
  Illustration Conventions ...................................................................................................... 6
  Documentation ...................................................................................................................... 6
  NetScreen-Security Manager 2004 FP3 Installer’s Guide Overview ..................................... 6
  Related NetScreen-Security Manager Documentation ......................................................... 6
Web Access ............................................................................................................................. 8
Comments About the Documentation .................................................................................... 8
Contacting Customer Support ............................................................................................... 9

## Chapter 1  Introduction

11

Installation Process Overview ............................................................................................... 12
  Management System Install Process .................................................................................. 12
  User Interface Install Process ............................................................................................. 12
Installation Package .............................................................................................................. 13
Minimum System Requirements ............................................................................................ 14
  System Requirements - Management System ................................................................... 14
  System Requirements - User Interface ............................................................................. 15
Configuration Options ........................................................................................................... 16
  Typical Configuration ......................................................................................................... 16
    NetScreen-Statistical Report Server Interoperability ....................................................... 17
    Local/Remote Database Backup .................................................................................... 17
  Extended Configuration ...................................................................................................... 18
  High Availability Configuration .......................................................................................... 18
    HA Requirements ............................................................................................................ 19
    Data Replication .............................................................................................................. 20
    Failover Process .............................................................................................................. 20
    Restoring Connections .................................................................................................... 20
    Capacity Planning For Additional Redundancy ............................................................... 21
Next Steps ............................................................................................................................... 22

## Chapter 2  Installing Typical Configuration

23

Installing the Management System - Typical Configuration .............................................. 24
Defining System Parameters ................................................................................................. 25
Prerequisite Steps .................................................................................................................. 27
  Other Recommended Actions ............................................................................................. 27
Running the System Update Utility ....................................................................................... 28
Patching the Sun Solaris SSH Daemon .................................................................................. 29
Establishing a Trust Relationship ......................................................................................... 30
Installing the Management System Software ...................................................................... 32
Viewing the Management System Installation Log ............................................................. 38
Starting Server Processes Manually ...................................................................................... 38
<table>
<thead>
<tr>
<th>Chapter 3</th>
<th>Installing Extended Configuration</th>
<th>49</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Installing the Management System - Extended Configuration</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Defining System Parameters</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Prerequisites</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Installing the GUI Server</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Viewing the Installation Log</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Installing the User Interface</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Adding the Device Server</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Installing the Device Server</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Starting Server Processes Manually</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>Validating Management System Status</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>Transferring Certificate Files (optional)</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>Next Steps</td>
<td>70</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Installing the Management System with High Availability</th>
<th>71</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High Availability Overview</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>High Availability Installation and Configuration Options</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Installing the Management System - Typical Configuration With HA</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>Installing the Management System - Extended Configuration With HA</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>Defining System Parameters</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Typical HA Configuration Parameters</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Extended HA Configuration Parameters</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>Shared Disk Parameters</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>Prerequisites</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Verifying that Shared Partitions are Mounted Properly</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Verifying that All Required System Binaries are Available</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Verifying that Clocks are Synchronized</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Establishing an SSH Trust Relationship</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>Installing the Management System Software on the Primary Server</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Viewing the Management System Installation Log</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>Starting Server Processes Manually</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Validating Management System Status</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Transferring Certificate Files (optional)</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Installing the Management System Software on the Secondary Server</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>Example: Installing the Management System in a Typical HA Configuration</td>
<td>91</td>
</tr>
<tr>
<td></td>
<td>Primary GUI Server and Device Server Installation Script</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>Secondary GUI Server and Device Server Installation Script</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>Installing the User Interface</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Configuring the HA Cluster</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Testing the Initial HA Replication</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>Installing the Management System In an Extended Configuration with HA Enabled</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>Example: Installing the Management System in an Extended HA Configuration</td>
<td>105</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Upgrading to FP3</td>
<td>121</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>-----</td>
</tr>
<tr>
<td>Upgrading The Management System Overview</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>Defining System Parameters</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Typical Configuration Parameters</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Extended Configuration Parameters</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>HA Configuration Parameters</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>Shared Disk Parameters</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>Prerequisite Steps</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>Other Recommended Actions</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>Running the System Update Utility</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Patching the Sun Solaris SSH Daemon</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>Upgrading the Management System - Typical Configuration</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>Starting Server Processes Manually</td>
<td>136</td>
<td></td>
</tr>
<tr>
<td>Validating Management System Status</td>
<td>137</td>
<td></td>
</tr>
<tr>
<td>Viewing the Installation Log</td>
<td>137</td>
<td></td>
</tr>
<tr>
<td>Upgrading the User Interface</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Validating the Upgrade</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Upgrading the Management System - Extended Configuration</td>
<td>139</td>
<td></td>
</tr>
<tr>
<td>Upgrading the Management System With HA Enabled</td>
<td>140</td>
<td></td>
</tr>
<tr>
<td>Upgrading the Database Backup Files</td>
<td>141</td>
<td></td>
</tr>
<tr>
<td>In Case The Upgrade Fails</td>
<td>142</td>
<td></td>
</tr>
<tr>
<td>Next Steps</td>
<td>143</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Maintaining NetScreen-Security Manager</th>
<th>145</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling the Management System</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Viewing Management System Commands</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Common Management System Commands</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Starting All Server Processes Using the HA Server</td>
<td>147</td>
<td></td>
</tr>
<tr>
<td>Starting GUI Server and Device Server Processes Manually</td>
<td>147</td>
<td></td>
</tr>
<tr>
<td>Stopping Server Processes</td>
<td>148</td>
<td></td>
</tr>
<tr>
<td>Maintaining the Management System</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Changing the Management System IP Address</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Changing the Device Server IP Address</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Configuring the Device Server Manually</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Changing the GUI Server IP Address</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>Changing Permissions To a Normal User</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Archiving and Restoring Logs and Configuration Data</td>
<td>152</td>
<td></td>
</tr>
<tr>
<td>Restoring Logs and Configuration Data</td>
<td>153</td>
<td></td>
</tr>
<tr>
<td>Configuring High Availability</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>Enabling and Disabling High Availability Processes</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>Configuring High Availability Options</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>Running the Remote Replication Utility as a Non-Root User</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Backing Up the Database Locally</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Restoring the Database</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Validating the Database Recovery Process</td>
<td>156</td>
<td></td>
</tr>
<tr>
<td>Relocating the Database</td>
<td>157</td>
<td></td>
</tr>
<tr>
<td>Archiving the GUI Server Database and Device Server Log Database</td>
<td>157</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

- Installing NetScreen-Security Manager On a New System ........................................ 158
- Moving the Databases to the New System ............................................................. 158
- Installing a tftp Server .......................................................................................... 160
- Installing a tftp Server on Linux ............................................................................ 160
- Installing a tftp Server on Solaris .......................................................................... 161
- Downgrading from Feature Pack 3 to Feature Pack 2 ............................................. 162
- Removing the Management System ...................................................................... 163
- Uninstalling the User Interface ............................................................................. 164

## Appendix A Technical Overview

- Technical Overview ................................................................................................. 165
- About the Management System ............................................................................... 165
  - GUI Server ............................................................................................................ 166
  - Device Server ...................................................................................................... 166
  - HA Server ............................................................................................................ 166
- About the NetScreen-Security Manager User Interface (UI) ..................................... 167
- About Managed FW/VPN Devices .......................................................................... 167
- Communications ..................................................................................................... 168
  - Communication Ports and Protocols ................................................................ 168
- Using the Secure Server Protocol (SSP) ............................................................... 169
- Communications With Devices Running ScreenOS 5.0+ ..................................... 170
- Communicating With Devices Running Screen 4.x and Earlier .......................... 170
- Creating a Separate Management Network .......................................................... 171
About This Guide

This NetScreen-Security Manager 2004 FP3 Installer’s Guide describes how you can install an initial working NetScreen-Security Manager system.

**NOTE:** If you are currently using a previous version of NetScreen management software (i.e., Juniper Networks NetScreen-Global PRO or Juniper Networks NetScreen-Global PRO Express) refer to the NetScreen-Security Manager 2004 FP3 Migration Guide for more specific information.
Audience

This guide is intended primarily for IT administrators who are responsible for installing NetScreen-Security Manager for the first.
Conventions

The sample screens used throughout this guide are representations of the screens you will see when you install and configure the NetScreen-Security Manager software. The actual screens may differ.

For convenience and clarity, the installation and configuration examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

The following tables define notice icons used in this guide and text conventions used throughout the book.

Table 1: Notice icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Informational note" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>Indicates that you may risk losing data or damaging your hardware.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury.</td>
</tr>
</tbody>
</table>

Table 2: Text conventions (except for command syntax)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface</strong></td>
<td>Represents commands and keywords in text.</td>
<td>Command example: Issue the <strong>clock source</strong> command. Keyword example: Specify the keyword exp-msg.</td>
</tr>
<tr>
<td><strong>Bold sans serif typeface</strong></td>
<td>Represents text that the user must type. <strong>user input</strong></td>
<td>Key name in angle brackets Indicates the name of a key on the keyboard. Press &lt;Enter&gt;. Key names linked with a plus sign (+) in angle brackets. Indicates that you must press two or more keys simultaneously. Press &lt;Ctrl+B&gt;.</td>
</tr>
<tr>
<td><strong>Plain sans serif typeface</strong></td>
<td>Represents information as displayed on your terminal’s screen.</td>
<td>host1#show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Emphasize words. Identify variables. Identify chapter, appendix, and book names.</td>
<td>There are two levels of access, user and privileged. clusterId, ipAddress. Appendix A, System Specifications.</td>
</tr>
</tbody>
</table>

Table 3: Syntax conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords.</td>
<td>terminal length</td>
</tr>
</tbody>
</table>
Table 3: Syntax conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in italics</td>
<td>Represent variables.</td>
<td><em>mask, accessListName</em></td>
</tr>
<tr>
<td>Words separated by the</td>
<td>symbol</td>
<td>Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)</td>
</tr>
<tr>
<td>Words enclosed in [ brackets ]</td>
<td>Represent optional keywords or variables.</td>
<td>*[ internal</td>
</tr>
<tr>
<td>Words enclosed in [ brackets ]*</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>*[ level1</td>
</tr>
<tr>
<td>Words enclosed in { braces }</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

User Interface Conventions

The sample screens used throughout this guide are representations of the screens you will see when you administer the Netscreen-Security Manager 2004 FP3.
Throughout this book, a chevron ( > ) is used to indicate navigation through the UI by clicking menu options and links. For example, the path to the local user configuration is presented as **Object Manager > User Objects > Local User Objects**, as shown below.

**Figure 1: Sample Screen**

1. In the main navigation tree, select Object Manager. The Object Manager tree expands to reveal a subset of objects.

2. In the Object Manager navigation tree, select User Objects. The main display area displays all defined user objects.

3. In the User Objects navigation tree, select Local User Objects. The main display area displays all defined local user objects.
**Illustration Conventions**

The following graphics make up the basic set of images used in illustrations throughout this book.

**Figure 2: Illustration Conventions**

- Local Area Network (LAN) with a Single Subnet. (example: 10.1.1.0/24)
- Generic NetScreen FW/VPN Device
- Security Zone
- Desktop Computer
- Internet
- Laptop Computer
- Security Zone Interfaces
  - White = Protected Zone Interface (example: Trust Zone)
  - Black = Outside Zone Interface (example: Untrust Zone)
- Server
- Tunnel Interface
- Router Icon
- VPN Tunnel
- Switch Icon

**Documentation**

This section describes documentation for NetScreen-Security Manager.

**NetScreen-Security Manager 2004 FP3 Installer’s Guide Overview**

This guide details the steps to install the NetScreen-Security Manager management system on a single server or on separate servers. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NetScreen-Security Manager 2004 FP3.

**Related NetScreen-Security Manager Documentation**

The NetScreen-Security Manager 2004 FP3 documentation set includes the following guides:
**NetScreen-Security Manager 2004 FP3 Getting Started Guide**—This guide details the steps to install the NetScreen-Security Manager management system on a single server. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and initial setup of NetScreen-Security Manager.

**NetScreen-Security Manager 2004 FP3 Rapid Deployment Getting Started Guide**—This guide details the steps to install and implement Rapid Deployment (RD) configlets. It is intended for on-site administrators responsible for the installation and initial setup of devices to be managed by NetScreen-Security Manager in rapid deployment scenarios.

**NetScreen-Security Manager 2004 FP3 Migration Guide**—This guide details the steps to: Install NetScreen-Security Manager using new or existing hardware; Migrate data previously configured in Global PRO or Express (i.e., using scripts and other manual migration steps); Map data and features in Global PRO/Express to NetScreen-Security Manager. This guide is intended for existing administrators of NetScreen-Global PRO or NetScreen-Global PRO Express who are installing NetScreen-Security Manager 2004 FP3 for the first time.

**NetScreen-Security Manager 2004 FP3 Administrator's Guide**—This guide describes how to use and configure key management features in the NetScreen-Security Manager. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NetScreen-Security Manager 2004 FP3 Online Help, which provides step-by-step instructions for performing management tasks in the NetScreen-Security Manager UI.

This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.

**NetScreen-Security Manager 2004 FP3 Online Help**—The online help provides task-oriented procedures describing how to perform basic tasks in the NetScreen-Security Manager user interface. It also includes a brief overview of the NetScreen-Security Manager system and a description of the GUI elements.

The online help is best used in conjunction with the NetScreen-Security Manager 2004 FP3 Administrator's Guide, which provides conceptual information, suggested workflows, and examples for management tasks where applicable.

The online help is intended for network and security administrators who are using the UI to configure and manage devices.

**NetScreen-Security Manager 2004 FP3 Release Notes**—The release notes provide latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes.

Release notes are included on the corresponding software CD and are available on the Web.
The documentation is also available on the Web. You can order a set of printed documents from your Juniper Networks sales representative.

**Web Access**

To view the documentation on the Web, go to:

http://www.juniper.net/techpubs/

**Comments About the Documentation**

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Please e-mail your comments to:

- techpubs-comments@juniper.net

Along with your comments, be sure to indicate:

- Document name
- Document part number
- Page number
- Software release version
Contacting Customer Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).
Chapter 1

Introduction

In This Chapter:

- Installation Process Overview
- Installation Package
- Minimum System Requirements
- Configuration Options
- Next Steps

This chapter provides you with the information you need to install NetScreen-Security Manager and integrate it into your network. It provides an overview of the NetScreen-Security Manager installation process. It also reviews minimum hardware and software requirements and options for configuring the management system to provide enhanced functionality, performance and scalability.
**Installation Process Overview**

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

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

The overall process for installing NetScreen-Security Manager is as follows:

- Management System Install Process on page 12
- User Interface Install Process on page 12

**Management System Install Process**

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

The management system installer is a shell archive script that you can run on any dedicated Solaris 8 or 9, Red Hat Linux 8.0, 9.0, Red Hat Enterprise Linux ES 3.0, or Red Hat Enterprise Linux AS server that meets minimum system requirements. Refer to Minimum System Requirements on page 14 for more information on the minimum required hardware and software that you need to install the NetScreen-Security Manager management system.

There are separate installer scripts for 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 NetScreen-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 Minimum System Requirements on page 14 for more information on the minimum required hardware and software that you need to install the NetScreen-Security Manager UI.

The InstallAnywhere wizard guides you through all of the steps required to configure and install the UI. After you install the UI, you can connect it to the management system.
Chapter 1: Introduction

Installation Package

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

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

Table 4: NetScreen-Security Manager Installation Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsm04fp3_ui_win_x86.exe</td>
<td>Installer for the NetScreen-Security Manager UI (for Windows-based computers).</td>
</tr>
<tr>
<td>nsm04fp3_ui_linux_x86.bin</td>
<td>Installer for the NetScreen-Security Manager UI (for Linux-based computers).</td>
</tr>
<tr>
<td>nsm04fp3_servers_linux_x86.sh</td>
<td>Installer for the NetScreen-Security Manager management system for Linux.</td>
</tr>
<tr>
<td>nsm04fp3_servers_sol_sparc.sh</td>
<td>Installer for the NetScreen-Security Manager management system for Solaris.</td>
</tr>
<tr>
<td>systemupdate-nsm-linux.tar</td>
<td>System update utility for Linux. You use this file to update files on your system required for the installer to run properly.</td>
</tr>
<tr>
<td>systemupdate-nsm-solaris.tar</td>
<td>System update utility for Solaris. You use this file to update files on your system required for the installer to run properly.</td>
</tr>
</tbody>
</table>
Minimum System Requirements

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

System Requirements - Management System

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

Table 5: Minimum System Requirements - Management System on Same Server

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES 3.0, Red Hat Enterprise Linux AS</td>
</tr>
<tr>
<td>CPU</td>
<td>Sun Microsystems UltraSPARC Ili 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB (or higher); 2GB+ (depending on the number of managed devices and configuration size)</td>
</tr>
<tr>
<td>Swap Space</td>
<td>4 GB for both GUI Server and Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>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>Network Connection</td>
<td>100MBps NIC Ethernet adapter</td>
</tr>
<tr>
<td>Other</td>
<td>Server must be dedicated to running NetScreen-Security Manager</td>
</tr>
</tbody>
</table>

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

Table 6: Minimum System Requirements - Management System on Separate Servers

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Solaris 8, Solaris 9 operating system, OR Red Hat Linux 8.0, Red Hat Linux 9.0, Red Hat Enterprise Linux ES 3.0, Red Hat Enterprise Linux AS</td>
</tr>
<tr>
<td>NOTE: Both servers must be running the same operating system version. For example, you cannot run the GUI Server on a server running Linux, and the Device Server on a server running Solaris.</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Sun Microsystems UltraSPARC Ili 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)</td>
</tr>
<tr>
<td>RAM</td>
<td>512MB (or higher); 1GB (recommended)</td>
</tr>
<tr>
<td>Swap Space</td>
<td>2 GB for the GUI Server, 2 GB for the Device Server</td>
</tr>
<tr>
<td>Storage</td>
<td>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>Network Connection</td>
<td>100MBps NIC Ethernet adapter</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

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

Table 7: Minimum System Requirements - User Interface

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
</table>
| Software  | Microsoft Windows XP, OR  
Microsoft Windows NT® 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 3.0,  
Red Hat Enterprise Linux AS  
US English versions only |
| Hardware  | IBM® compatible PC  
400MHz Pentium® 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 NetScreen-Security Manager management system |
Configuration Options

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

- Typical Configuration on page 16
- Extended Configuration on page 18
- High Availability Configuration on page 18

NOTE: NetScreen-Security Manager 2004 FP3 provides support for only one GUI Server and one Device Server. In future releases of NetScreen-Security Manager, you will be able to install and deploy multiple Device Servers in your network to provide greater scalability and performance.

Typical Configuration

The most straightforward implementation of the NetScreen-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.

Figure 3: Typical Management System Configuration
**NetScreen-Statistical Report Server Interoperability**

If you are installing NetScreen-Statistical Report Server, you must configure it to work with NetScreen-Security Manager. During the installation or upgrade process, the installer script prompts you configure parameters enabling the management system to communicate with the Statistical Report Server database and web server. If you type “y”, the installer script prompts you to configure the following additional parameters enabling the management system to work with the NetScreen-Statistical Report Server database:

- database type
- database server IP address
- database port
- database name
- database user name
- database password

Refer to the *NetScreen-Statistical Report Server Installer’s Guide* for more information.

**Local/Remote Database Backup**

You can also configure the management system to perform an automatic backup of the GUI Server database to the local server machine and if necessary, to a remote server machine. During the installation or upgrade process, the installer script prompts you to specify if this server machine requires local database backups. If you type “y”, the installer script prompts you to configure the following additional parameters enabling the management system to perform automatic daily backups of the database:

- Hour of Day to store the database backup
- Number of database backups to keep
- Directory where local database backups are stored
- Full path to the rsync command—the management system uses the rsync utility to perform the database backup

If you want to send copies of the database backup to a remote machine, the installer script prompts you to configure the following additional parameters:

- IP Address of the remote machine
Full path to the ssh command—the management system uses the ssh utility to perform the database backup.

**NOTE:** If you want the management system to perform remote database backups, you will need to set up a trust relationship between the management system server and the remote machine.

**Extended Configuration**

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

**Figure 4: Extended Management System Configuration**

**High Availability Configuration**

You can also install and configure the management system to provide for high availability. This configuration option is recommended to minimize the impact of any unplanned server outages.

To implement the management system for high availability, you need to install two management systems: a primary server that runs on a server machine in active mode; and a secondary server that runs on a different server machine in standby mode. If for any reason, the primary server becomes unavailable, the secondary server takes over as the active management system.

During the installation or upgrade process, the installer script prompts you to specify whether or not you want the current server machine to participate in an HA cluster. If you type “y”, the installer script prompts you to configure additional parameters enabling the high availability features on the management system.
HA Requirements

Some system requirements that you need to keep in mind if you are planning on installing the management system for high availability:

- Both the primary and secondary management servers must share at least one network connection—there must be at least 1 network connection for data, and at least one network connection for heartbeat communication.

- The primary and secondary GUI Servers can be geographically separate.

The following illustration depicts the physical setup of the primary and secondary management systems:

Figure 6: Typical HA Management System Configuration
Data Replication

The GUI Server uses the rsync utility to replicate configuration data to the standby GUI Server. The remote replication process occurs every 60 minutes by default. You can also configure the GUI Server to perform a local backup copy of the database automatically.

Note that device log data is not remotely replicated because of the large data size. If you want the standby Device Server to access log data also on the active Device Server, you must connect both servers to an external shared disk.

Failover Process

During normal operations, both the primary and secondary management systems monitor the health of the other using a series of heartbeat communications. Each server sends a heartbeat message to the other server every 15 seconds. If a series of consecutive heartbeat messages is not received by the primary server, the secondary server takes over for the primary server. So for example, if you are running the primary GUI Server and Device Server on Server1 and the secondary GUI Server and Device Server on Server 2; and the primary GUI Server fails—both the primary GUI Server and primary Device Server on Server 1 are shutdown; and both the secondary GUI Server and Device Server on Server 2 start up.

In the event of a process failure on the primary server, the primary server proceeds as follows:

1. shuts down all local server processes
2. synchronizes all information to disk
3. un-mounts the shared partitions (if using a shared disk)
4. signals to the new server that it is done shutting down

The HA process in the old server then enters an ERROR mode, and stays in that mode until you manually restart the HA startup scripts. Refer to Controlling the Management System in Chapter 6, Maintaining NetScreen-Security Manager for more information.

The new server, after receiving the signal or a signal-timeout, mounts the shared partitions and then cleans the file system (i.e., runs fsck on the shared partitions). Note that the mount and fsck actions are only taken if a shared disk is used.

Restoring Connections

In the event that the GUI Server fails over, the Device Server detects this status and automatically reconnects to the secondary GUI Server.
If you are attempting to connect to the GUI Server using the User Interface, you must enter the Secondary Server IP Address to reconnect to the new GUI Server IP Address.

**NOTE:** After failover, it will take some time for the standby management system to become fully active with the replicated database. For large networks, this can take up to 10 minutes.

In the event that the Device Server fails over, the managed FW/VPN devices in your network detect this, and automatically reconnect to the secondary Device Server.

**Capacity Planning For Additional Redundancy**

For additional redundancy, it is recommended that you install at least two additional heartbeat network connections. This installation protects against the heartbeat network connection from being the single point of failure for the entire system. For example, if a shared disk setup is used, in case one of the heartbeat network connections goes down, both servers would not consider the other server as dead, thus mounting the shared disk simultaneously, resulting in a corrupted file system.

If you choose to install two network cards, it is recommended that you use one dedicated interface for heartbeat communications, in addition to one for network communications.
Next Steps

This chapter has provided you with:

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

Use this information to help you implement NetScreen-Security Manager and integrate it into your network. When you are ready to install NetScreen-Security Manager, there are three options for configuring the management system depending upon the size and requirements of your specific network: Typical, Extended, or HA Configuration.

- Refer to Chapter 2, Installing Typical Configuration for specific information describing how to install and run the management system on the same server.
- Refer to Chapter 3, Installing 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 Chapter 4, Installing the Management System with High Availability for specific information describing how to install and run the GUI Server and Device Server on the same server or separate servers with HA. This configuration option enables you to configure a primary and secondary management system that is highly available.
- Refer to Chapter 5, Upgrading to FP3 for specific information describing how to upgrade previous installations of NetScreen-Security Manager to Feature Pack 3.
- Refer to Chapter 6, Maintaining NetScreen-Security Manager for specific information describing how to maintain, control, backup/restore, and uninstall the management system and User Interface.
Chapter 2
Installing 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
- Next Steps

After you have decided how you want to deploy NetScreen-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 NetScreen-Security Manager management system for most typical cases — GUI Server and Device Server on the same server. This includes performing any prerequisite steps, running the management system installer, running the User Interface 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 NetScreen-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 50 minutes.

**Table 8: Typical Configuration Installation Process**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/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. (10 minutes)</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps. (10 minutes)</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site. (10 minutes)</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 local database backup option (optional). (10 minutes)</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface. (10 minutes)</td>
</tr>
<tr>
<td>6</td>
<td>Launch the User Interface, and then connect it to the management system. (5 minutes)</td>
</tr>
<tr>
<td>7</td>
<td>Validate that you have successfully installed the management system and User Interface. (5 minutes)</td>
</tr>
</tbody>
</table>

* If you are installing the GUI Server and Device Server on separate systems, refer to Chapter 3, Installing Extended Configuration for more information.
Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want 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 system parameters that you need to identify.

Table 9: Common System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. 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, then specify the new location during the install process. By default, the Device Server stores data in: /var/netscreen/DevSvr/</td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. 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, then specify the new location during the install process. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</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>Local database backup directory</td>
<td>Directory location where local database backup data is stored. By default, the GUI Server stores local database backup data at: /var/netscreen/dbbackup/</td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/rsync</td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable. The default path is: /usr/bin/sshd</td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
</tr>
</tbody>
</table>
### Defining System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour of the Day to Start</td>
<td>Time of day that you want the GUI Server to backup the database. Type a 2 digit number representing the time of day in a 24 hour day (00-25). For example, if you want the backup to begin at 4:00 A.M., type 04; if at 4:00 P.M., type 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI Server completes the daily backup process within the hour specified every day. By default, the GUI Server performs the daily backup within an hour after 2am.</td>
<td></td>
</tr>
<tr>
<td>Local Database Backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>Total number of database backup files that the GUI Server stores. When the GUI Server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI Server stores seven backup files.</td>
<td></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, then type the following command to become root:

   `su -`

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

   **NOTE:** The NetScreen-Security Manager management system runs as the root user. If you want to run the management system in a more secure mode, then refer to Changing Permissions To a Normal User on page 151.

3. Partition drives for sufficient disk space to accommodate your planned data requirements. Ensure that you have allocated a maximum amount of disk space for the data partition (i.e., `/var/netscreen` directory).

   Refer to the Hardware Sizing Recommendations document for NetScreen-Security Manager 2004 FP3 for more information about the disk space requirements appropriate for your specific network.

4. Run the system update utility for your appropriate platform to verify that you have all the prerequisite utilities and packages to run the installer properly. Refer to Running the System Update Utility on page 28 for more information on running the system update utility.

5. If you are installing the management system on Solaris 9, and are planning to perform local database backups, then you must update the Sun Solaris ssh daemon. Refer to Patching the Sun Solaris SSH Daemon on page 29 for more information.

6. If you are planning to send copies of your database backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine. Refer to Establishing a Trust Relationship on page 30 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 NetScreen-Security Manager. Disabling X server frees 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
```

### Running the System Update Utility

Use the system update utility to upgrade your system with the latest patches and packages required to run the NetScreen-Security Manager management system installer properly.

To run the system update utility:

1. Save the system update utility appropriate for your platform (for example, `systemupdate-nsm-linux` for Linux, `systemupdate-nsm-solaris` for Solaris) that is provided on the NetScreen-Security Manager Installation CD or from the directory where it is saved, to a suitable directory on the server.

2. Uncompress the system update utility file. For example, you would run the following command on Linux:

   ```
   gzip -d systemupdate-nsm-linux.tar.gz
   ```

3. Untar the appropriate system update utility file. For example, you would run the following command on Linux:

   ```
   tar xfv systemupdate-nsm-linux.tar
   ```

   A subdirectory called `/systemupdate-nsm-<platform>` is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the `/systemupdate-nsm-<platform>` subdirectory.

5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

   ```
   ./update.sh
   ```

---

**NOTE:** It is recommended that you save the utility in the `/usr` subdirectory.
Prerequisite Steps

Chapter 2: Installing Typical Configuration

The script proceeds to check your system for required updates. It next prompts you to type <Enter> to continue or <Ctrl-C> to stop.

6. Press <Enter> to continue. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 20 minutes. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 10 minutes depending upon the number of packages that need to be installed.

**Patching the Sun Solaris SSH Daemon**

If you are running NetScreen-Security Manager 2004 FP3 on a Solaris 9 system, and you want to perform a database backup, replicate the database remotely, or enable high availability functionality, you must patch the Sun Solaris SSH daemon on both servers. This is because of a known issue in the Sun Solaris SSH daemon that may result in a failure to replicate.

To patch the Sun Solaris SSH daemon on Solaris 9:

1. Login to the server machine that you are running NetScreen-Security Manager as root. You must also be in single user mode.

2. Use a web browser to download the Sun Solaris patch 113273-07 from the following URL:

<http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113273&rev=01>
3. Extract the packages. For example, run the following commands:

   `unzip /tmp/113273-07.zip`

4. Install the packages. Make sure that you are in the directory where you downloaded the packages. The following example installs the patch to a standalone system:

   `patchadd /tmp/113273-07`

   Checking installed patches...
   Verifying sufficient filesystem capacity (dry run method)...
   Installing patch packages...

   Patch number 113273-07 has been successfully installed.
   See /var/sadm/patch/113273-07/log for details

   Patch packages installed:
   SUNWsshdu

5. Verify that the patch has been installed. For example, run the following command:

   `showrev -p | grep 113273-07`

   Patch: 113273-07 Obsoletes: Requires: Incompatibles: Packages: SUNWsshdu

6. Restart the server machine.

   **Establishing a Trust Relationship**

   If you are planning to send copies of your database backups to a remote machine, then you must establish a trust relationship between the management system server and the remote machine.

   To establish a trust relationship between 2 machines:

   1. Run the following commands on the management system server:

      ```
      cd /root
      ssh-keygen -t rsa
      chmod 0700 .ssh
      ```

   2. Copy `.ssh/id_rsa.pub` to the remote machine’s `.ssh/authorized_keys`. For example:

      ```
      scp .ssh/id_rsa.pub root@<IP addr NSM2>: /root.ssh/authorized_keys2
      ```

   3. Run the following commands on the remote machine:

      ```
      cd /root
      ssh-keygen -t rsa
      chmod 0700 .ssh
      ```

   4. Copy `.ssh/id_rsa.pub` to the management system server’s `.ssh/authorized_keys`. For example:
scp .ssh/id_rsa.pub root@<IP addr NSM1>: /root.ssh/authorized_keys2

5. Test connectivity via SSH from the primary NSM server to the remote machine and vice versa. For example, to test SSH connectivity from NSM Server1 to remote machine, type the following command:

```
ssh root@<IP ADDRESS of remote machine>
```

6. Validate that you do not receive a prompt to enter a password to access the remote machine.
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 of the steps to configure the required system parameters, and then run it to completion.

To install the management system on the same system:

1. Load the management system installer software onto the server that you have decided to use as the NetScreen-Security Manager management system. You can run the installer directly from the NetScreen-Security Manager installation CD, copy the installer to a directory on the server, or download the installer from the Juniper Networks Customer Services Online web site.

2. Navigate to the directory where you 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, run the following command:

   ```sh
   sh nsm04fp3_servers_linux_x86.sh
   ```

   On Solaris, run the following command:

   ```sh
   sh nsm04fp3_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 of 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 unsuccessful.

The installer then prompts you to specify the components of the NetScreen-Security Manager management system that you want to install.
4. Type 3, then press <Enter> 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 similar prompts and messages.

4. Type 3, then press <Enter> 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 similar prompts and messages.

5. Type n, and then press <Enter> if you do not want the machine to participate in an HA cluster. If you are planning on configuring the management system with HA enabled, type y, and then press <Enter>. Refer to Chapter 4, Installing the Management System with High Availability for more information.

The script then prompts you to specify a location to store the management system data files.

6. Set the directory location for storing the management system data files:

   a. Type the directory location for storing the Device Server data files or press <Enter> to accept the default location /var/netscreen/DevSvr.

   The script then prompts you to specify a location for storing the GUI Server data files.

   b. Type the directory location for storing the GUI Server data files or press <Enter> to accept the default location /var/netscreen/GuiSvr.
Installing the Management System Software

7. Type the management IP address for the server. This address should be the same IP address as 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. The Device Server attempts to connect to the GUI Server using port 7800 by default.

The script then prompts you to type 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 NetScreen-Security Manager using the NetScreen-Security Manager User Interface (UI). This account is used to authenticate communication between the management system and the NetScreen-Security Manager UI. It possesses all administrative privileges by default.

8. Type any text string longer than 8 characters for the password. Type 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 then prompts you if you want to use a Statistical Report Server with the GUI Server.

9. Type `n` and then press `<Enter>`, if you are **not** planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type `y` and then press `<Enter>` if you are installing NetScreen-Statistical Report Server with NetScreen-Security Manager. If you typed `y`, the script then prompts you to configure parameters required for the management system to work with the Statistical Report Server (i.e., database type, database server IP address, database port, database name, database user name, database password). Refer to the *NetScreen-Statistical Report Server Installer’s Guide* for more information about these parameters.
The script next prompts if you want this machine to perform a backup of the database locally.

10. Type **y** and then press <Enter> if you want the management system to perform a local 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. **Type a two-digit number** (00-23) specifying the hour of day that you want 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, type 12; for midnight, type 00. Press <Enter> to accept the default setting of 02 (2:00 A.M.).

b. **Type n**, and then press <Enter> to specify that you do not want daily backups to be sent to a remote machine. If you select **y**, and then press <Enter>, then the script prompts you to enter an IP address for the remote backup machine.

c. **Type a number** (up to seven) specifying how many database backup files the management system stores. After 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 seven backup files. By default, the management system stores backup files in /var/netscreen/dbbackup.

d. **Type the full path to the ssh utility executable.**

Type **n**, and then press <Enter>, if you do not want the management system to backup the database locally.

The script then prompts you to start servers after installation is complete.
11. Type `y`, and then press `<Enter>`, if you want to start the GUI and Device Servers after the installation has finished. Type `n`, and then press `<Enter>`, if you do not want to start the servers.

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

12. Verify your settings, and if they are correct, type `y`, and then press `<Enter>` to proceed. If you type `n`, and press `<Enter>`, then the installer returns you to the original selection prompt.

The installer performs the following actions:

- Extracts the software payloads
- Performs any applicable migration tasks (disregard since this is a new installation)
- Installs the Device Server
- Installs the GUI Server
Installs the HA Server

Performs 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 returns you to the command prompt.

**Viewing the Management System Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes. 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 6:00 P.M., the installation log file would be named:

```
netmgtInstallLog.20031201180000
```

---NOTE: After the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.

**Starting Server Processes Manually**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, run the following command:

```
cd /usr/netscreen/hsrv/bin
```
2. Run the following command:

```
./haSvr.sh start
```

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

---

**Validating Management System Status**

If you did not specify the installer to start the server(s) when finished, then 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 (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 6, *Maintaining NetScreen-Security Manager* for more information on manual commands that you can send to the HA Server, Device Server and GUI Server.
Installing the User Interface

The NetScreen-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 of the steps required to configure and install the NetScreen-Security Manager UI. After you install the UI, you can connect it to the management system.

NOTE: It is recommended that you exit all running applications before installing the UI.

To install the NetScreen-Security Manager UI:

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

2. Download the UI installer from the NetScreen-Security Manager installation CD or the Juniper Networks 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, then double-click on the installer executable.

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

   ```sh
   nsm04fp3_ui_linux_x86.bin
   ```

   Alternatively, you can also run the following command:

   ```sh
   chmod755 nsm04fp3_ui_linux_x86.bin
   ./nsm04fp3_ui_linux_x86.bin
   ```

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

Follow the wizard through all the steps required to configure and install the UI, and then 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, and then click **Next** to continue.

**NOTE:** If you choose to not accept the terms of the License Agreement, then you are unable to proceed with the installation.

If you accepted the License Agreement, then 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, then 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, then the installer saves the UI software files in `/<install_user_homedir>/NetScreen-Security Manager` by default.

To specify a new or different folder location, click **Choose**... If you decide to accept the default install folder, then 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 NetScreen-Security Manager product icons. Or, if you are installing on a Linux-based computer, select where you would like to create links to the NetScreen-Security Manager UI program. Click Next to continue. The Pre-Installation Summary screen appears.

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, then the Select Browser screen appears. Click Choose... to navigate to the subdirectory where your web browser software files are located. Click Next to continue. When the installation is complete, a screen indicating “Install Complete” appears.

NOTE: If you do not select a default web browser, then the UI is not able to launch the NetScreen-Security Manager online help. If you still want to use the online help, then you can configure your web browser using the Preferences menu from the UI.

9. Click Done to exit the installation program.

Viewing the User Interface 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\n
For Linux-based computers:

/<install_user_homedir>/.nsm/
The Installation log file is named: _out.<date/time stamp>.dat

**NOTE:** The .nsm subdirectory is a hidden subdirectory on Linux systems.

---

**Running the User Interface**

After 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 into the UI for the first time:

1. Run the NetScreen-Security Manager UI.
   
   If you are running the UI on a Windows-based PC, then double-click on the NetScreen-Security Manager icon.
   
   If you are running the UI on a Linux-based computer, then launch it by double-clicking on the NetScreen-Security Manager application icon (specify that you want to run the program) or 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, type “super” in the Login field.

3. Type the password that you specified when you installed the management system in the **Password** field.

4. Type the IP address you assigned to the GUI Server in the **Server** field. If you have enabled DNS-lookup, then type the host name instead of the IP address.
5. Click OK.

The UI appears indicating that the installation was successful.

**Validating the NetScreen-Security Manager Installation**

After 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 NetScreen-Security Manager UI, select **Server Manager > Servers**. The Servers view appears displaying Device Server and GUI Server information.

2. Click on the Device Server and then click on the **Edit** icon or right-click on the Device Server and select **Edit** to view all information available on the Device Server.
3. Use the **General** tab to verify the following information:

   - **Device Server Manager Port** — the default port is 7800.
   - **Device Server ID** — the ID number identifies the Device Server; you cannot change the Device Server ID.
   - **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.

4. Click **OK** when you are finished.

**Running the User Interface in Demo Mode**

Before you begin using NetScreen-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 NetScreen-Security Manager UI. The Login window appears.
2. Type any user name in the **Login** field provided.
3. Type any password in the **Password** field provided.
4. Select *DEMO MODE* from the **Server** field pull-down menu.
5. Click **OK**. The Log Viewer main window appears.
Next Steps

Congratulations! You have just completed installation of the NetScreen-Security Manager management system and UI. You can now begin to manage your network using NetScreen-Security Manager. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide for information describing how to plan and implement NetScreen-Security Manager for your network. You can also refer to the NetScreen-Security Manager 2004 FP3 Online Help for task-specific information.

If you plan to install the GUI Server and Device Server on separate servers, refer to Chapter 3, Installing Extended Configuration for more information.
Chapter 3
Installing 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 a large 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 NetScreen-Security Manager management system — GUI Server and Device Server on separate servers. This installation includes performing any prerequisite steps, running the management system installer, running the User Interface 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 50 minutes.

Table 10: Extended Configuration Installation Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/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. (10 minutes)</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps. (10 minutes)</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site. (10 minutes)</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. Install and configure the local database backup option (optional). (10 minutes)</td>
</tr>
<tr>
<td>5</td>
<td>Install the User Interface. (5 minutes)</td>
</tr>
<tr>
<td>6</td>
<td>Launch the User Interface, and then connect it to the GUI Server. Add and configure the Device Server. (5 minutes)</td>
</tr>
<tr>
<td>7</td>
<td>Run the management system installer on the server where you want to install the Device Server. Specify that you want to install the Device Server. Install and configure the local database backup option (optional). (10 minutes)</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. (10 minutes)</td>
</tr>
</tbody>
</table>
Defining System Parameters

During the installation process, you are required to configure common system parameters such as directory locations 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 system parameters that you need to identify.

**Table 11: Extended Configuration - System Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. 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, then specify the new location during the install process.</td>
<td></td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. 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, then specify the new location during the install process.</td>
<td></td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address and port used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Local Database Backup directory</td>
<td>Directory location where local database backup data is stored.</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable. The default path is: /usr/bin/ssh</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Your Value</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>Time of day that you want the GUI Server to backup the database. Type a 2 digit number representing the time of day in a 24 hour day (00-23). For example, if you want the backup to begin at 4:00 A.M., type 04; if at 4:00 P.M., type 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI Server completes the daily backup process within the hour specified every day. By default, the GUI Server performs the daily backup within an hour after 2am.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>Total number of database backup files that the GUI Server stores. When the GUI Server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server</td>
<td></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>
<td></td>
</tr>
</tbody>
</table>
Prerequisites

Perform the prerequisite steps described as if you were installing the management system on the same server. Refer to Prerequisite Steps in Chapter 1, Introduction for more information.
Installing the GUI Server

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

To install the GUI Server:

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

2. Run the management system installer.

   On Linux, run the following command:
   
   sh nsm04fp3_servers_linux_x86.sh

   On Solaris, run the following command:
   
   sh nsm04fp3_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 then prompts you to specify the components of the NetScreen-Security Manager management system that you want to install.

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

3. Type 2 to specify that you want to install the GUI Server only.

   The following depicts the installer running on Linux. The installer running on Solaris displays similar prompts and messages.
Chapter 3: Installing Extended Configuration

The script then prompts if you want this machine to participate in an HA cluster.

4. Type \texttt{n}, and then press \texttt{<Enter>} if you do not want the machine to participate in an HA cluster. If you are planning on configuring the management system with HA enabled, type \texttt{y}, and then press \texttt{<Enter>}. Refer to \textit{Chapter 4, Installing the Management System with High Availability} for more information.

The script then prompts you to configure the GUI Server.

5. Configure details about the GUI Server:

   a. Type the directory location for storing the data files for the GUI Server or press \texttt{<Enter>} to accept the default location \texttt{/var/netscreen/GuiSvr}.

   

   \begin{center}
   \begin{tabular}{|c|}
   \hline
   1) Install Device Server only \\
   2) Install GUI Server only \\
   3) Install both Device Server and GUI Server \\
   \hline
   \end{tabular}
   \end{center} 

   Enter selection (1-3) [>] \texttt{2}

   

   \textbf{NOTE}: If you specify a new directory location, then the installer creates it. The installer does not however, allow you to specify an existing directory location. This feature safeguards against overwriting any existing data. If you try to specify an existing directory, then the installer indicates that an existing directory already exists, and then prompts you to try again.

The script then prompts you to specify the IP address of the GUI Server.

   b. Type the IP address of the GUI Server. This address should be the same as the server on which you are installing. The installer sets the IP address and port number on the GUI Server enabling the Device Server to start and connect. The Device Server attempts to connect to the GUI Server using port \texttt{7801} by default.
The script then prompts you to type 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 NetScreen-Security Manager using the User Interface. This account is used to authenticate communication between the management system and the User Interface. It possesses all administrative privileges by default.

c. Type any text string longer than 8 characters for the password. Type the password again for verification.

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

The script then prompts you if you want to use the Statistical Reports Server with the GUI Server.

6. Type **n** and then press <Enter>, if you are not planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type **y** and then press <Enter> if you are installing NetScreen-Statistical Report Server with NetScreen-Security Manager. If you typed **y**, the script then prompts you to configure parameters required for the management system to work with the Statistical Report Server (i.e., database type, database server IP address, database port, database name, database user name, database password). Refer to the *NetScreen-Statistical Report Server Installer’s Guide* for more information about these parameters.

![Image of terminal output](image)

The script next prompts if you want to restart the server processes automatically in case of a failure.
7. Type `y` and then press `<Enter>` if you want the server processes to be
   restarted automatically in case of failure. Type `n` and then press `<Enter>` if
   you do not want to restart server processes automatically.

   The script next prompts you if you want the GUI Server to perform a local
   backup of the database.

8. Type `y` and then press `<Enter>` if you want to perform a backup of the
   database locally. If you specify that you want the management system to
   perform backups, the script prompts you to configure options for the backup
   operation:
   a. Type a **two-digit number** (00-23) specifying the hour of day that you want
      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, type `12`; for midnight, type `00`. Press `<Enter>` to
      accept the default setting of `02` (2:00 A.M.).
   b. Type `n`, and then press `<Enter>` so daily backups are not sent to a remote
      machine. If you select `y`, and then press `<Enter>`, then the script prompts
      you for and IP address for the remote backup machine.
   c. Type a number (up to seven) specifying how many database backup files
      the management system stores. After 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
      seven backup files.
   d. Designate a directory location for locally storing the management system
      database backup. Press `<Enter>` to accept the default location
      `/var/netscreen/dbbackup`.
   e. Type the path to the rsync executable.
   f. Type the path to the ssh executable.

**NOTE:** If you are installing the management system on Solaris, the path to the ssh
executable is typically different than the default setting of `/usr/bin/rsync`. It is
typically `/usr/local/bin`. 
Type **n** and then press **<Enter>**, if you do not want to backup the database locally.

The script then prompts if you want to restart the GUI Server after the installation process is completed.

9. Type **y** and then press **<Enter>** to start the GUI Server processes after the installer has completed the installation process. Type **n** and then press **<Enter>**, if you do not want to start the server processes.

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

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

10. Verify your settings, and if they are correct, type **y**, and then press **<Enter>** to proceed. If you type **n** and press **<Enter>**, then the installer returns you to the original Selection prompt.
The installation proceeds automatically. The installer proceeds to perform the following actions:

- Extracts the software payloads
- Performs migration tasks (disregard since this is a new installation)
- Installs the GUI Server
- Installs the HA Server
- Performs post installation tasks such as removing the staging directory, and starting the 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.

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 6:00 P.M., the installation log file would be named: `netmgtInstallLog.20031201180000`
**NOTE:** After 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 NetScreen-Security Manager User Interface. Refer to Installing the User Interface in Chapter 2, Installing Typical Configuration for more information on installing the User Interface (UI).

Adding the Device Server

After you have installed the UI, you need to add the Device Server in NetScreen-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.

To add the Device Server:

1. From the NetScreen-Security Manager UI, use Server Manager > Server.

2. In the Device Server area, click the + icon. The Device Server dialog box appears.

3. In the Name box, enter the name of the Device Server.

4. In the IP Address box, enter the IP address of the Device Server.

5. In the Password for GUI Server Connection box, enter the password you specified for the "super" user account, when you installed the GUI Server.

6. If you are using a Mapped IP Address, use the General tab, and click in the MIP section. The New MIP dialog box appears. Enter the mapped IP address and port of the Device Server in the fields provided. You can also edit the Device Server Manager port and Device Server ID. (Optional)

7. If you wish to configure polling attributes use the Device Polling tab. Device polling attributes enable you to configure the intervals with which the Device Server retrieves statistics from the managed FW/VPN devices in your network. These statistics appear in the Device Monitor and Realtime Monitor. (Optional)

8. Click OK to save your settings.

NetScreen-Security Manager sets the Device Server Manager port to 7800 by default. It also assigns an ID to the Device Server automatically (this ID appears in the Device Server ID box).

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, run the following command:

   ```
   sh nsm04fp3_servers_linux_x86.sh
   ```

   On Solaris, run the following command:

   ```
   sh nsm04fp3_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 NetScreen-Security Manager management system that you want to install.

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

3. Type 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 similar prompts and messages.

```
root@docsteam-attack:/tmp
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 requirements...............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]: 1
```

The script then prompts you to specify if you want the machine to have HA cluster enabled.

4. Type **n**, and then press <Enter> if you do not want the machine to participate in an HA cluster. If you are planning on configuring the management system with HA enabled, type **y**, and then press <Enter>. Refer to Chapter 4, *Installing the Management System with High Availability* for more information.

The script then prompts you to configure the Device Server.

5. Configure details about the Device Server:
   a. Type the directory location for storing the Device Server data files or press <Enter> to accept the default location `/var/netscreen/DevSvr`.
   b. The script then prompts you to enter parameters assigned by the UI to this Device Server.
   c. Type the Device Server ID. The script then prompts you to type the one time password for this Device Server.
   d. Type the One-Time Password for GUI Server connection.
   e. The script then 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.
   f. Type the IP address of the running GUI Server.
g. Type 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 7801 by default.

The script then prompts if you want to restart the server processes automatically in case of a failure.

6. Type yes (y) and then press <Enter> if you want the server processes to be restarted automatically in case of failure. Type no (n) and then press <Enter>, if you do not want to restart the server processes.

The script next prompts if you want to perform a backup of the database locally. If you installed and configured the local database backup on the GUI Server, then you are required to install and configure the option on the Device Server.

7. Type yes (y) and then press <Enter> if you want the Device Server to perform a backup of the database locally. Type no (n) and then press <Enter>, if you do not want the Device Server to perform a backup.

If you specified that you want the Device Server to perform automatic backups, the script prompts you to configure options for the backup operation:

a. Type a two-digit number (00-23) specifying the hour of day that you want 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, type 12; for midnight, type 00. Press <Enter> to accept the default setting of 02 (2:00 A.M.).
b. Type n, and then press <Enter> so daily backups are not sent to a remote machine. If you select y, and then press <Enter>, then the script prompts you to enter the IP address of the remote backup machine.

c. Type a number (up to seven) specifying how many database backup files the management system stores. After 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 seven backup files.

d. Designate a directory location for locally storing the management system database backup. Press <Enter> to accept the default location /var/netscreen/dbbackup.

e. Type the path to the rsync package.

f. Type the path to the ssh command.

The script then prompts if you want to restart the Device Server after the installation process is completed.

8. Type y and then press <Enter> to start the Device Server after the installer has completed the installation process. Type n and then press <Enter>, if you do not want the Device Server to start automatically.

**NOTE:** Whenever you restart your server, the Device Server starts automatically.
The script then prompts you to verify your installation configuration settings.

9. Verify your settings, and if they are correct, type **y**, and then press <Enter> to proceed. If you type **n** and then press <Enter>, then the installer returns you to the original Selection prompt.

If you confirmed your settings, 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 in Chapter 6, *Maintaining NetScreen-Security Manager* for more information on installing a tftp server

- Extracts the software payloads

- Performs any applicable migration tasks (disregard since this is a new installation)

- Installs the Device Server
Installs the HA Server

```
root@dooceam-attack:/tmp
$ cd
$ PERFORMING INSTALLATION TASKS

----- INSTALLING Device Server -----
Looking for existing RPM package .........................ok
Removing existing Device Server RPM ......................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 Device Server config file(s) .................ok
Setting permissions for Device Server .................ok
Restarting xinetd service .................................ok
Installation of Device Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package .........................ok
Removing existing HA Server RPM ........................ok
Installing HA Server RPM ................................ok
Creating var directory ...................................ok
Putting NSROOT into start scripts .........................ok
Filling in HA Server config file(s) .......................ok
Setting permissions for HA Server .......................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Enabling Device Server start script .....................ok
Enabling HA Server start script .........................ok
```

Performs 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), removing the staging directory, and starting up the Device Server and HA Server.

```
root@dooceam-attack:/tmp
$ cd
$ PERFORMING POST-INSTALLATION TASKS

Running nacCertGeneration ....................................ok
Removing staging directory ..................................ok
Starting Device Server .......................................ok
Starting HA Server ..........................................ok

NOTES:
- Installation log is stored in /usr/netscreen/DevSvr/var/errorLog/nets mtInstallLog.20040817.713
```

[root@dooceam-attack tmp]#
Starting Server Processes Manually

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, run the following command:

   ```
   /usr/netscreen/HaSvr/bin
   ```

2. Run the following command:

   ```
   ./haSvr.sh start
   ```

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

Validating Management System Status

To validate the management system is started and running properly, it is recommended that you view the status of all the running server processes (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 146 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 NetScreen-Security Manager to manage FW/VPN devices running ScreenOS 4.0.X, then 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:
   - cacerticate_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.
**Next Steps**

Congratulations! You have just completed installation of the NetScreen-Security Manager management system on separate servers. You are now ready to begin managing your network. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide for information describing how to plan and implement NetScreen-Security Manager for your network. You can also refer to the NetScreen-Security Manager 2004 FP3 Online Help for more task-specific information.
Chapter 4
Installing the Management System with High Availability

In This Chapter:

- High Availability Overview
- Installing the Management System - Typical Configuration With HA
- Installing the Management System - Extended Configuration With HA
- Defining System Parameters
- Prerequisites
- Installing the Management System Software on the Primary Server
- Installing the Management System Software on the Secondary Server
- Installing the User Interface
- Testing the Initial HA Replication
- Installing the Management System In an Extended Configuration with HA Enabled
- Next Steps

This chapter describes how to install the NetScreen-Security Manager management system and configure it to provide for high availability. This installation includes performing any prerequisite steps, running the management system installer on a primary and secondary server, configuring both servers to failover in the event that the primary server is unavailable, running the User Interface installer, and validating that you have installed the management system successfully.
NetScreen-Security Manager 2004 FP3 enables you to install the management system and configure it for high availability. This configuration option involves installing two management systems:

- a primary server that runs on a server machine in active mode
- a secondary server that runs on a different server machine in standby mode

If for any reason the primary server becomes unavailable, then the secondary server takes over as the active management system.

**High Availability Installation and Configuration Options**

There are two main options for installing NetScreen-Security Manager in a high availability configuration:

- Installing the Management System - Typical Configuration With HA on page 73 - involves installing and configuring the management system in an HA cluster on two server machines — the primary management system with the Device Server and GUI Server on the same machine, and a secondary management system with the Device Server and GUI Server together on another machine.

- Installing the Management System - Extended Configuration With HA on page 74 - involves installing and configuring the management system in an HA cluster on four server machines — the primary management system with the Device Server and GUI Server on separate machines and a secondary management system with the Device Server and GUI Server on separate machines.

You can also install and configure HA clusters in either scenario with access to a shared disk.
Installing the Management System - Typical Configuration With HA

The following table summarizes the process for installing the management system on the same server and configured to provide for high availability. 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 55 minutes.

Table 12: Typical HA Configuration Installation Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/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. (10 minutes)</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps. (10 minutes)</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site. (10 minutes)</td>
</tr>
</tbody>
</table>
| 4    | Run the management system installer on the system where you want to install the primary management system. Specify that you want to install both the GUI Server and Device Server. (10 minutes)  
Configure the server to participate in an HA Cluster. Configure other HA parameters for the primary server. (10 minutes)  
Configure management system access to a shared disk (optional). Note that if you are using a shared disk, you must install the primary server first, then the secondary server. |
| 5    | Run the management system installer on the system where you want to install the secondary management system. Specify that you want to install both the GUI Server and Device Server. (10 minutes)  
Configure the server to participate in an HA Cluster. Configure other HA parameters for the secondary server (10 minutes)  
Configure management system access to a shared disk (optional) |
| 6    | Install the User Interface. (10 minutes) |
| 7    | Launch the User Interface, and then connect it to the management system. (10 minutes) |
| 8    | Validate that you have successfully installed the management system and User Interface. (10 minutes) |
| 9    | Configure the HA Cluster (i.e., Device Server Secondary IP Address, e-mail notification) in the UI. (10 minutes) |
# Installing the Management System - Extended Configuration With HA

The following table summarizes the process for installing the management system on the same server and configured to provide for high availability. 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 55 minutes.

**Table 13: Extended HA Configuration Installation Process**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/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. (10 minutes)</td>
</tr>
<tr>
<td>2</td>
<td>Perform prerequisite steps. (10 minutes)</td>
</tr>
<tr>
<td>3</td>
<td>Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate website. (10 minutes)</td>
</tr>
</tbody>
</table>
| 4    | Run the management system installer on the system where you want to install the primary GUI Server. Specify that you want to install the GUI Server. (10 minutes)  
 Configure the server to participate in an HA Cluster. Configure other HA parameters for the primary GUI Server. (10 minutes)  
 Configure the GUI Server to access a shared disk (optional) |
| 5    | Install the User Interface. (10 minutes) |
| 6    | Launch the User Interface, and then connect it to the GUI Server. Add and configure the Device Server. (10 minutes) |
| 7    | Run the management system installer on the system where you want to install the primary Device Server. Specify that you want to install the Device Server. (10 minutes)  
 Configure the server to participate in an HA Cluster. Configure other HA parameters for the primary Device Server. (10 minutes)  
 Configure the Device Server to access a shared disk (optional) |
| 8    | Run the management system installer on the systems where you want to install the secondary GUI Server and Device Server. (10 minutes)  
 Configure both servers to participate in a HA Cluster. Configure other HA parameters for the secondary GUI Server and Device Server (10 minutes)  
 Configure management system access to a shared disk (optional) |
| 9    | Launch the User Interface, and then connect it to the management system. (10 minutes) |
| 10   | Validate that you have successfully installed the management system and User Interface. (10 minutes) |
| 11   | Configure the HA Cluster (i.e., Device Server Secondary IP Address, e-mail notification) in the UI. (10 minutes) |
Defining System Parameters

During the installation process, you are required to configure common system parameters such as the location of the directories where you want 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.

Typical HA Configuration Parameters

The following table describes the system parameters that you need to identify to install HA with the Device Server and GUI Server on the same server machine:

Table 14: Typical HA Configuration - System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. 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, then specify the new location during the install process. By default, the Device Server stores data in: /var/netscreen/DevSvr/</td>
<td></td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. 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, then specify the new location during the install process. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
<td></td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address and port used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>HA replications</td>
<td>Time interval with which you want the GUI Server to replicate the database. By default, the GUI Server replicates the database every 60 minutes.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Your Value</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| Heartbeat links between primary and secondary machine | Number of heartbeat communication paths between the primary and secondary machine.  
By default, there is 1 communication link between the primary and secondary machine. This in addition to the data network link already existing in the primary/secondary HA Server IP Address. |            |
| Shared password for heartbeat authentication         | This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers. |            |
| IP Address for Primary machine’s heartbeat link      | IP address used for heartbeat communications on the primary server machine. |            |
| Port used for heartbeat communication                | The port number used for heartbeat communications. The default port is 7802. |            |
| Heartbeat messages time interval                     | Time interval (in seconds) between heartbeat messages. The default is 15 seconds. |            |
| Missing heartbeats before switchover occurs          | Number of missing heartbeat messages before automatic switchover to the secondary machine occurs. The default is 4 messages. |            |
| IP Address outside the HA cluster                   | Network IP Address used to monitor this server’s network connection.         |            |
| HA directory                                         | Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups. By default, the HA Server stores data at: /var/netscreen/dbbackup/ |            |
| Path to the rsync utility executable                 | Path to the rsync utility executable. The default path is: /usr/bin/rsync |            |
| Path to the ssh utility executable                   | Path to the ssh utility executable. The default path is: /usr/bin/ssh |            |
| Remote Backup Machine IP Address                    | IP address of the machine where remote backups are sent. By default, the installer sets this to the IP address of the secondary HA Server. |            |
Extended HA Configuration Parameters

The following table describes additional system parameters that you need to identify to install HA with the Device Server and GUI Server on separate server machines:

Table 15: Extended HA Configuration - System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server</td>
<td></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>
<td></td>
</tr>
</tbody>
</table>

Shared Disk Parameters

If you are using a shared disk partition, the installer prompts you to configure additional information. The following table identifies the additional system parameters that you need to identify to install HA with access to a shared disk:

Table 16: Shared Disk System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition. The default command is: /bin/mount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to unmount the shared data partition. Before configuring this command, you must first verify that you have defined your mounts properly. The default command is: /bin/umount /var/netscreen/DevSvr</td>
<td></td>
</tr>
</tbody>
</table>
Command to check the integrity of the shared data partition

- The command to check the integrity on the shared data partition.
- The default command is:
  `/sbin/fsck`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory path for the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisites

Perform the prerequisite steps described as if you were installing the management system using the typical configuration. Refer to Prerequisite Steps on page 27 for more information on installing the management system on the same server.

After you have performed the prerequisite steps in Chapter 2, it is recommended that you perform the following additional steps before installing the management system with HA enabled:

- Verifying that Shared Partitions are Mounted Properly on page 79
- Verifying that All Required System Binaries are Available on page 79
- Verifying that Clocks are Synchronized on page 79
- Establishing an SSH Trust Relationship on page 80

Verifying that Shared Partitions are Mounted Properly

If you are using a shared disk, you must first verify that all partitions are mounted properly. You can verify this by checking the following files:

- etc/fstab (on Linux)
- etc/vfstab (on Solaris)

You also need to verify that all mounts are not set to restart automatically.

Verifying that All Required System Binaries are Available

For your convenience, a shell archive script is provided with your installation package that verifies that all required system binaries are available.

To run the verification script:

1. Navigate to the HA Server utilities subdirectory (/usr/netscreen/HaSvr/utils by default).
2. Run the validation shell archive script. You can do so by running the following command:

   ./validateBinaries

Verifying that Clocks are Synchronized

Before installing the management system with HA enabled, you must verify that the clocks on the server machines that you are using for the primary and secondary servers all have the same timestamp. This is because the failover logic determines whether to perform a restore from a database replicated remotely based on the timestamp of the last performed remote database replication.
Establishing an SSH Trust Relationship

You also need to ensure that you have established an SSH trust relationship between the primary and secondary servers.

The instructions for Linux are as follows:

1. Run the following commands on the primary NSM server:

   ```
   cd /root
   ssh-keygen -t rsa
   chmod 0700 .ssh
   ```

2. You then need to copy `.ssh/id_rsa.pub` to the peer machines’ `.ssh/authorized_keys`. For example:

   ```
   scp .ssh/id_rsa.pub root@<IP addr NSM2>: /root/.ssh/authorized_keys2
   ```

3. Run the following commands on the secondary NSM server:

   ```
   cd /root
   ssh-keygen -t rsa
   chmod 0700 .ssh
   ```

4. You then need to copy `.ssh/id_rsa.pub` to the peer machines’ `.ssh/authorized_keys`. For example:

   ```
   scp .ssh/id_rsa.pub root@<IP addr NSM1>: /root/.ssh/authorized_keys2
   ```

5. You should test connectivity via SSH from the primary NSM server to the secondary NSM server and vice versa. For example, to test SSH connectivity from NSM Server1 to NSM Server2, type the following command:

   ```
   ssh root@<IP ADDRESS of Secondary NSM Server>
   ```

6. Validate that you do not receive a prompt to enter a password to access the secondary NSM server.

---

**NOTE:** If you are prohibited from establishing a trust-relationship between root users on different machines, you can run the remote replication utility as a non-root user. For your convenience, a script called `setRsyncUser` is provided. Run this script after the installation is complete. Refer to Running the Remote Replication Utility as a Non-Root User on page 155 for more information.
Installing the Management System Software on the Primary Server

After you have successfully performed all prerequisite steps, you can install the management system software on the primary server.

To install the primary server with HA configured:

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

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, run the following command:

```
sh nsm04fp3_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm04fp3_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 of 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 unsuccessful.

The installer then prompts you to specify the components of the NetScreen-Security Manager management system that you want to install.

**NOTE:** If you have installed a previous version of the management system, then you may notice different menu options.
4. Type 3, and then press <Enter> to specify that you want to install the Device and GUI Servers on the same server.

The following screen depicts the installer running on Linux. The installer running on Solaris displays similar prompts and messages.

5. Type y, and then press <Enter> for the machine to participate in an HA cluster.

The script then prompts you to specify if the current server machine will act as the primary server for the HA cluster.

6. Type y, and then press <Enter> to specify the current machine as the primary server for the HA cluster.

The script then prompts you for information about the Device Server.

7. Configure setup details for the Device Server:
Installing the Management System Software on the Primary Server

Chapter 4: Installing the Management System with High Availability

a. Type `n` and then press `<Enter>` if you are not using a shared disk. Type `y` and then press `<Enter>` if the Device Server data directory is located on a shared disk partition. If you are using a shared disk partition, the installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to Shared Disk Parameters on page 77 for more information.

b. Type the directory location for storing the Device Server data files or press `<Enter>` to accept the default location `/var/netscreen/DevSvr`.

NOTE: If you specify a new directory location, then the installer creates it. The installer does not however, allow you to specify an existing directory location. This feature safeguards against overwriting any existing data. If you try to specify an existing directory, then the installer indicates that an existing directory already exists and prompts you to try again.

The script then prompts you to specify information about the GUI Server data files.

8. Configure setup details for the GUI Server:

a. Type `n` and then press `<Enter>` if you are not using a shared disk. Type `y` and then press `<Enter>` if the GUI Server data directory is located on a shared disk partition. If you are using a shared disk partition, the installer prompts you to enter additional parameters required to mount and unmount the partition. Refer to Shared Disk Parameters on page 77 for more information.

b. Type the directory location for storing the GUI Server data files or press `<Enter>` to accept the default location `/var/netscreen/GuiSvr`.

The script then prompts you to specify the management IP address for the server.

c. Type the management IP address for the server. This address should be the same IP address as 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. The Device Server attempts to connect to the GUI Server using port **7801** by default.
d. Type any text string longer than 8 characters for the password. Type the password again for verification.

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

The script then prompts you if you want to use a Statistical Report Server with the GUI Server.

9. Type n and then press <Enter>, if you are not planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type y and then press <Enter> if you are installing NetScreen-Statistical Report Server with NetScreen-Security Manager. If you typed y, the script then prompts you to configure parameters required for the management system to work with the Statistical Report Server (i.e., database type, database server IP address, database port, database name, database user name, database password). Refer to the NetScreen-Statistical Report Server Installer’s Guide for more information about these parameters.

The script next prompts you to configure settings for the HA cluster.

10. Configure setup details for the HA cluster:

   a. Type the IP address for the primary HA Server.

   b. Type the IP address for the secondary HA Server.
c. Type a time value (in minutes) indicating the frequency with which you want to perform HA replications. It is recommended that you set this value to 60 (i.e., 1 hour).

d. Type a shared password that will be used for authentication of the heartbeat links between the primary and secondary servers.

**NOTE:** Make a note of the shared password that you set for the heartbeat authentication. You need to configure the same password when installing the management system on the secondary server.

e. Type the number of heartbeat links between the primary and secondary machines.

f. Type the IP address for this machine’s primary heartbeat link.

g. Type the IP address for the peer’s primary heartbeat link.

h. If you entered '2' for # heartbeat links, you will need to configure the following additional parameters:
   a. Type the IP address for this machine's secondary heartbeat link
   b. Type the IP address for the peer's secondary heartbeat link
   c. Type the IP address that will be used for remote HA replications
   d. Type the port number used for heartbeat communication.

i. Enter a time interval in seconds between heartbeat messages.

**NOTE:** For larger deployments (i.e., more than 1000 managed devices), increase the default heartbeat interval to a value proportional to the number of devices that you are managing greater than 1000 devices. For example, the default heartbeat interval is 15 seconds. This is appropriate for deployments of less than 1000 managed devices. If you plan to use NetScreen-Security Manager to manage more than 1000 devices, it is recommended that you set the heartbeat interval to 30 seconds. As a rule of thumb, it is recommended that you double the timeout interval for every 1000 devices that you are managing.

j. Enter the number of missing heartbeat messages before automatic switchover occurs.

k. Enter an IP Address outside the cluster to be used to monitor this server’s network connection.

l. Enter the path to the High Availability directory.

m. Enter the full path to the rsync executable.
n. Enter the full path to the ssh executable.

![NOTE: If you are installing the management system on Solaris, the path to the ssh executable is typically different than the default setting of /usr/bin/rsync. It is typically /usr/local/bin.]

The script next prompts if you want to perform backups of the database locally.

11. Type **y** and then press **< Enter >** if you want the management system to perform a local backup of the database on a daily basis. The script prompts you to configure options for the backup operation:

   a. Type a **two-digit number** (00-23) specifying the hour of day that you want 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, type 12; for midnight, type 00. Press **< Enter >** to accept the default setting of 02 (2:00 A.M.).

   b. Type **n**, and then press **< Enter >** so daily backups are not sent to a remote machine. If you type **y**, then the script prompts for an IP address for the remote backup machine.

   c. Type a number (up to seven) specifying how many database backup files the management system stores. After 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 seven backup files.

The script then prompts you to start the HA daemon processes when installation is complete.
12. Type **y** and then press <Enter> if you want to start the HA daemon processes. Type **n** and then press <Enter> if you to start the HA daemon processes manually. Refer to Controlling the Management System on page 146 for more information.

13. Verify your settings, and if they are correct, type **y**, and then press <Enter> to proceed. If you type **n**, and then press <Enter>, the installer returns you to the original selection prompt.

The installer proceeds to perform the following actions:

- Extracts the software payloads
- Performs any applicable migration tasks (disregard since this is a new installation)
- Installs the Device Server
- Installs the GUI Server
- Installs the HA Server

The installer runs for several minutes, and then returns you to the command prompt.

**Viewing the Management System Installation Log**

The installer generates a log file with the output of the installation commands for troubleshooting purposes.

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 6:00 P.M., then the installation log file would be named:

netmgtInstallLog.20031201180000

---

**NOTE:** After the installation script finishes, it indicates the name of the installation log file and the directory location where it is saved.

---

**Starting Server Processes Manually**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, run the following command:

   cd /usr/netscreen/HaSvr/bin

2. Run the following command:

   ./haSvr.sh start

---

**NOTE:** The HA Server process automatically starts the GUI Server and Device Server processes.

---

**Validating Management System Status**

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 146 for more information on manual commands that you can send to the HA Server, Device Server, and GUI Server.

If you are experiencing problems with the HA Server, run the following command for more detailed information:

   /usr/netscreen/HaSvr/utils/haStatus

The haStatus utility provides additional information describing the state and status of the local/peer servers.
Transferring Certificate Files (optional)

If you are using NetScreen-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`
   - `ncncertificate_table.nml`

3. Save these files in the `/GuiSvr/var` subdirectory on the server where you have installed the GUI Server.
Installing the Management System Software on the Secondary Server

After you have successfully installed the management system software on the primary server, run the management system installer on the secondary server. Follow the installer script prompts to configure the secondary server.

Note that the secondary server and primary server must run on the same operating system. The two systems must also share the same directory structure for all NetScreen-Security Manager software and data.

Example: Installing the Management System in a Typical HA Configuration

For example, you want to install the management system in a typical HA configuration (GUI Server and Device Server on the same server machine) with the following parameters:

- no shared disk
- no Statistical Report Server
- only one heartbeat link between the primary/secondary servers
- IP Address of the primary HA server is 10.150.41.9
- IP Address of the secondary HA server is 10.150.41.10
- IP Address outside the HA Cluster is 10.150.47.254
- daily local database backup
- daily remote database backup
- heartbeat link sent over remote replications/backups

The following graphic depicts the configuration example above.
Primary GUI Server and Device Server Installation Script

A complete example of the installer script output for installing the primary GUI Server and Device Server on the same server computer using the configuration described in the example is as follows:

########## 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 for sufficient disk space..........................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) []> 3

########## GENERAL SERVER SETUP DETAILS ##########
Will this machine participate in an HA cluster? (y/n) [n]> y
Is this machine the primary server for the HA cluster? (y/n) [y]> y
WARNING: The servers need to be stopped on the secondary server during the installation of this software to avoid data corruption.

########## DEVICE SERVER SETUP DETAILS ##########
Will the Device Server data directory be located on a shared disk partition? (y/n) [n]> n
The Device Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/DevSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.
Enter data directory location [/var/netscreen/DevSvr]>

########## GUI SERVER SETUP DETAILS ##########
Will the GUI Server data directory be located on a shared disk partition? (y/n) [n]> n

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.
Enter data directory location [/var/netscreen/GuiSvr]>

Enter the management IP address of this server [10.150.41.9]>
Setting GUI Server address and port to 10.150.41.9:7801 for Device Server
Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]> n

########## HIGH AVAILABILITY (HA) SETUP DETAILS ##########
Enter the IP address for the primary HA Server [10.150.41.9]>
Enter the IP address for the secondary HA Server []> 10.150.41.10
Enter how often to perform HA replications (10 to 1440 minutes) [60]> NOTE: Please make sure the heartbeat PASSWORD is the same for primary and secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter number of Heartbeat links between the primary and secondary machines [1]> NOTE: Heartbeat link(s) are needed between the primary and secondary machines. The IP addresses entered here must be correct and match on both ends of the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.9]>
10.150.42.9
Enter the IP address for the peer's primary heartbeat link [10.150.41.10]>
10.150.42.10
Enter the IP address that will be used for remote HA replications [10.150.41.10]>
10.150.42.10
Enter the port used for heartbeat communication [7802]>
Enter a time interval (seconds) between heartbeat messages [15]>
Enter number of missing heartbeat messages before automatic switchover occurs [4]>
An IP address outside the HA cluster is needed to monitor this server's network connection.
Enter an IP address outside of the cluster[]> 10.150.47.254
Enter HA directory [/var/netscreen/dbbackup]>
The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>
The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>
Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Here are sample commands:
cd /root
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

########## BACKUP SETUP DETAILS ##########
Will this machine require local database backups? (y/n) [y]>
Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]>
Enter the IP address of the remote backup machine [10.150.41.10]> 10.150.42.10
Enter number of database backups to keep [7]>

########## POST-INSTALLATION OPTIONS ##########
Start High Availability daemon processes when finished? (y/n) []> n

########## CONFIRMATION ##########
About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Use IP address 10.150.41.9 for management
- Connect to GUI Server at 10.150.41.9:7801
- Set password for 'super' user
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.9
- IP address for the peer's primary heartbeat link: 10.150.42.10
- IP address for remote HA replications: 10.150.42.10
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: 10.150.42.10
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No
Are the above actions correct? (y/n) > y

########## EXTRACTING PAYLOADS ##########
Extracting payload..........................................ok
Decompressing payload.......................................ok

########## PERFORMING MIGRATION TASKS ##########

########## PERFORMING INSTALLATION TASKS ##########

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

----- INSTALLING GUI Server -----
Looking for existing RPM package...............................ok
Removing GuiSvr files from default location.......................ok
Unpacking GuiSvr..................................................ok
Installing JRE.....................................................ok
Creating var directory..............................................ok
Putting NSROOT into start scripts...............................ok
Filling in GUI Server config file(s)..............................ok
Setting permissions for GUI Server...............................ok
Running generateMPK utility........................................ok
Running fingerprintMPK utility......................................ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package...............................ok
Removing HaSvr files from default location.......................ok
Unpacking HaSvr.....................................................ok
Creating var directory..............................................ok
Putting NSROOT into start scripts...............................ok
Filling in HA Server config file(s)..............................ok
Setting permissions for HA Server...............................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling Device Server start script.............................ok
Disabling GUI Server start script................................ok
Enabling HA Server start script................................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Running nacnCertGeneration........................................ok
Removing staging directory.......................................ok

NOTES:
- Installation log is stored in
  /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20040824191744

- This is the GUI Server fingerprint:
  You will need this for verification purposes when logging into the GUI Server.
  Please make a note of it.

- To enable firmware updates to ScreenOS 4.x devices, the TFTP server on this
  machine must have its root directory set to '/usr/netscreen/DevSvr/var/cache'.

Secondary GUI Server and Device Server Installation Script
A complete example of the installer script output for installing the secondary GUI
Server and Device Server on the same server computer using the configuration
described in the example is as follows (changes from the primary installation script
highlighted in blue):

########## 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 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) [ ]> 3

########## GENERAL SERVER SETUP DETAILS ##########
Will this machine participate in an HA cluster? (y/n) [n]> y
Is this machine the primary server for the HA cluster? (y/n) [y]> n
WARNING: The servers need to be stopped on the secondary server during the installation of this software to avoid data corruption.

########## DEVICE SERVER SETUP DETAILS ##########
Will the Device Server data directory be located on a shared disk partition? (y/n) [n]> n
The Device Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/DevSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/DevSvr]>

########## GUI SERVER SETUP DETAILS ##########
Will the GUI Server data directory be located on a shared disk partition? (y/n) [n]> n
The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/GuiSvr]>

Enter the management IP address of this server [10.150.41.10]> Setting GUI Server address and port to 10.150.41.10:7801 for Device Server Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]> n

########## HIGH AVAILABILITY (HA) SETUP DETAILS ##########
Enter the IP address for the primary HA Server> 10.150.41.10
Enter the IP address for the secondary HA Server [10.150.41.10]>
Enter how often to perform HA replications (10 to 1440 minutes) [60]>
NOTE: Please make sure the heartbeat PASSWORD is the same for primary and secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter number of Heartbeat links between the primary and secondary machines [1]> NOTE: Heartbeat link(s) are needed between the primary and secondary machines. The IP addresses entered here must be correct and match on both ends of the link
for automatic failover to function correctly.

Enter the IP address for this machine's primary heartbeat link [> 10.150.42.10
Enter the IP address for the peer's primary heartbeat link []> 10.150.42.9
Enter the IP address that will be used for remote HA replications [> 10.150.42.9
Enter the port used for heartbeat communication [7802]>
Enter a time interval (seconds) between heartbeat messages [15]>
Enter number of missing heartbeat messages before automatic switchover occurs [4]>

An IP address outside the HA cluster is needed to monitor this server's network connection.

Enter an IP address outside of the cluster [> 10.150.47.254
Enter HA directory [/var/netscreen/dbbackup]>
The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>
The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Here are sample commands:

cd /root
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines'.ssh/authorized_keys

########## BACKUP SETUP DETAILS ##########
Will this machine require local database backups? (y/n) [y]>
Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]> y
Enter the IP address of the remote backup machine [> 10.150.42.9
Enter number of database backups to keep [7]>

########## POST-INSTALLATION OPTIONS ##########
Start High Availability daemon processes when finished? (y/n) [> n

########## CONFIRMATION ##########
About to proceed with the following actions:
- Install Device Server
- Install GUI Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Use IP address 10.150.41.10 for management
- Connect to GUI Server at 10.150.41.10:7801
- Set password for 'super' user
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.42.10
- IP address for the peer's primary heartbeat link: 10.150.42.9
- IP address for remote HA replications: 10.150.42.9
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will be sent to a remote machine
- IP address of the remote backup machine: 10.150.42.9
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n)> y

########## EXTRACTING PAYLOADS ##########
Extracting payload..........................................ok
Decompressing payload........................................ok

########## PERFORMING MIGRATION TASKS ##########

########## PERFORMING INSTALLATION TASKS ##########

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

----- INSTALLING GUI Server -----  
Looking for existing RPM package.........................ok
Removing GuiSvr files from default location............ok
Unpacking GuiSvr.............................................ok
Installing JRE................................................ok
Creating var directory......................................ok
Putting NSROOT into start scripts.........................ok
Filling in GUI Server config file(s).....................ok
Setting permissions for GUI Server.......................ok
Running generateMPK utility...............................ok
Running fingerprintMPK utility...........................ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----  
Looking for existing RPM package.........................ok
Removing HaSvr files from default location.............ok
Unpacking HaSvr.............................................ok
Creating var directory......................................ok
Putting NSROOT into start scripts.........................ok
Filling in HA Server config file(s).......................ok
Setting permissions for HA Server.......................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----  
Disabling Device Server start script....................ok
Disabling GUI Server start script.......................ok
Enabling HA Server start script..........................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Running nacnCertGeneration...............................ok
Removing staging directory..............................ok

NOTES:  
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20040824191744

- This is the GUI Server fingerprint:
You will need this for verification purposes when logging into the GUI Server. Please make a note of it.

- To enable firmware updates to ScreenOS 4.x devices, the TFTP server on this machine must have its root directory set to '/usr/netscreen/DevSvr/var/cache'.
Installing the User Interface

Install the NetScreen-Security Manager User Interface. Refer to Installing the User Interface on page 40 for more information on installing the User Interface.

After you have installed the UI, launch the application and validate that you can connect to the primary server successfully.

Configuring the HA Cluster

After your have installed your primary and secondary servers, you must add information about your secondary servers in the UI and configure the HA Cluster. After you have done this, you must then update this configuration to all the managed FW/VPN devices in your network. In the event that the primary server becomes incapacitated, the managed FW/VPN devices will re-attempt to connect to the management system using the Secondary Server IP Address.

To add the secondary server:

1. From the NetScreen-Security Manager UI, use Server Manager > Server.
2. In the Device Server area, click the + icon. The Device Server dialog box appears.
3. In the Name box, enter the name of the Device Server.
4. In the IP Address box, enter the IP address of the Device Server.
5. In the Password for GUI Server Connection box, enter the password you specified for the "super" user account, when you installed the GUI Server.
6. If you are using a Mapped IP Address, use the General tab, and click in the MIP section. The New MIP dialog box appears. Enter the mapped IP address and port of the Device Server in the fields provided. You can also edit the Device Server Manager port and Device Server ID. (Optional)
7. If you wish to configure polling attributes use the Device Polling tab. Device polling attributes enable you to configure the intervals with which the Device Server retrieves statistics from the managed FW/VPN devices in your network. These statistics appear in the Device Monitor and Realtime Monitor. (Optional)
8. Click OK to save your settings.

To configure the GUI Server Cluster:

1. From the NetScreen-Security Manager UI, use Server Manager > Servers > GUI Server, then click on the Edit icon or right-click on the GUI Server and select Edit to view all information available on the GUI Server.
2. Use the Server Type pull-down to select GUI Server Cluster. The HA and Email Notification tabs become available.
3. Click to activate the HA tab. Configure the following parameters:
   a. Enter the IP Address of the Secondary Server.
b. Enter the **Secondary GUI Server Manager Port** (if applicable)

c. **Mapped IP Address** (if applicable)

4. Click *Apply* when you are done.

5. Click to activate the **Email Notification** tab (optional). Configure the following parameters:

   a. Enter the **IP Address of the SMTP Server**.

   b. Enter the email address referenced in the email notification in the **From Email Address** field.

   c. Click the + button to add recipients of the email notification. The New Add/Edit E-mail Address window appears enabling you to enter an e-mail address. Click *OK* when you are done.

   d. Click the - button to remove recipients of the email notification.

   e. Click to select an email address entry from the To Email Address list and click on the Edit button to edit the email address.

6. Click *Apply* when you are done.

To configure the Device Server Cluster:
1. From the NetScreen-Security Manager UI, use **Server Manager > Servers > Device Server**, then click on the **Edit** icon or right-click on the Device Server and select **Edit** to view all information available on the Device Server.

2. Use the **Server Type** pull-down to select **Device Server Cluster**. The HA and Email Notification tabs become available.

3. Click to activate the **HA** tab. Configure the following parameters:
   
a. Enter the **IP Address of the Secondary Server**.

   b. Enter the **Secondary Device Server Manager Port** (if applicable)

   c. **Mapped IP Address** and **Port of the Secondary Server** (if applicable)

4. Click **Apply** when you are done.

5. Click to activate the **Email Notification** tab (optional). Configure the following parameters:
   
a. Enter the **IP Address of the SMTP Server**.

   b. Enter the email address referenced in the email notification in the **From Email Address** field.

   c. Click the + button to add recipients of the email notification. The New Add/Edit E-mail Address window appears enabling you to enter an e-mail address. Click **OK** when you are done.

   d. Click the - button to remove recipients of the email notification.
e. Click to select an email address entry from the To Email Address list and click on the Edit button to edit the email address.

6. Click **Apply** when you are done.
# Testing the Initial HA Replication

Once you have installed the management system on your primary and secondary servers, it is highly recommended that you test that server replication is functioning properly.

To test HA replication:

1. Start the primary servers.
2. Start the secondary servers.
3. Login to the UI and verify that both the primary GUI Server and Device Server appear as “active”. Check and verify that both the secondary GUI Server and Device Server appear as “standby”.
4. Login to the primary GUI Server and replicate the database. You can do so by running the following command:

   ```bash
   /usr/netscreen/HaSvr/utils/replicateDb ha
   ```

5. Verify that the command was successful.
6. Login to the primary Device Server and replicate the database. You can do so by running the following command:

   ```bash
   /usr/netscreen/HaSvr/utils/replicateDb ha
   ```

7. Verify that the command was successful.
Installing the Management System In an Extended Configuration with HA Enabled

If you are installing the management system in an extended configuration (GUI Server and Device Server on separate server machines) with HA enabled, you will need to run the management system installer on four separate server machines:

1. primary GUI Server
2. secondary GUI Server
3. primary Device Server
4. secondary Device Server

Use the system parameters referred to in Extended HA Configuration Parameters on page 77 to configure HA on both servers. If you are using a shared disk, you will also need to configure the system parameters referred to in Shared Disk Parameters on page 77.

After installing the primary management system and secondary management system, you will need to use the UI to configure the HA cluster. Lastly, it is highly recommended that you test the initial replication process.

Example: Installing the Management System in an Extended HA Configuration

For example, you want to install the management system in an extended HA configuration (GUI Server and Device Server on separate server machines) with the following parameters:

- no shared disk
- no Statistical Report Server
- only one heartbeat link between the primary/secondary servers
- IP Address of the primary GUI Server is 10.150.41.9
- IP Address of the secondary GUI Server is 10.150.41.10
- IP Address of the primary Device Server is 10.150.41.7
- IP Address of the secondary Device Server is 10.150.41.8
- IP Address outside the HA Cluster is 10.150.47.254
- daily local database backup
- no daily remote database backup
- heartbeat link sent over remote replications/backups

The following graphic depicts the configuration example above:
The installer script output for the primary GUI Server installations follows.

**Primary GUI Server Installation Script**

A complete example of the installer script output for installing the primary GUI Server is as follows:

```
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 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) [ ]> 2

########## GENERAL SERVER SETUP DETAILS ##########
Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]> y
```

WARNING: The servers need to be stopped on the secondary server.
during the installation of this software to avoid data corruption.

############ GUI SERVER SETUP DETAILS ############

Will the GUI Server data directory be located on a shared disk partition? (y/n) [n]> n

The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/GuiSvr]>

Enter the management IP address of this server []> 10.150.41.9

Please enter a password for the 'super' user

Enter password (password will not display as you type)>

Please enter again for verification

Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]> 

############ HIGH AVAILABILITY (HA) SETUP DETAILS ############

Enter the IP address for the primary HA Server [10.150.41.9]>

Enter the IP address for the secondary HA Server []> 10.150.41.10

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and secondary machines.

Please enter shared password that will be used for Heartbeat authentication

Enter password (password will not display as you type)>

Please enter again for verification

Enter number of Heartbeat links between the primary and secondary machines [1]> 

NOTE: Heartbeat link(s) are needed between the primary and secondary machines. The IP addresses entered here must be correct and match on both ends of the link for automatic failover to function correctly.

Enter the IP address for this machine's primary heartbeat link [10.150.41.9]>

Enter the IP address for the peer's primary heartbeat link [10.150.41.10]>

Enter the IP address that will be used for remote HA replications [10.150.41.10]>

Enter the port used for heartbeat communication [7802]>

Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs [4]>

An IP address outside the HA cluster is needed to monitor this server's network connection.

Enter an IP address outside of the cluster[]> 10.150.47.254

Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program. Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program. Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.

Here are sample commands:

cd /root

ssh-keygen -t rsa

chmod 0700 .ssh

Installing the Management System In an Extended Configuration with HA Enabled  ■  107
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

########## BACKUP SETUP DETAILS ##########
Will this machine require local database backups? (y/n) [y]>
Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]>
Enter number of database backups to keep [7]>

########## POST-INSTALLATION OPTIONS ##########
Start High Availability daemon processes when finished? (y/n) []> n

########## CONFIRMATION ##########
About to proceed with the following actions:
- Install GUI Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store GUI Server data in /var/netscreen/GuiSvr
- Use IP address 10.150.41.9 for management
- Set password for 'super' user
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.9
- IP address for the peer's primary heartbeat link: 10.150.43.10
- IP address for remote HA replications: 10.150.43.10
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n) y

########## EXTRACTING PAYLOADS ##########
Extracting payload..........................................ok
Decompressing payload.......................................ok

########## PERFORMING MIGRATION TASKS ##########

########## PERFORMING INSTALLATION TASKS ##########

----- INSTALLING GUI Server -----
Setting permissions for GUI Server..........................ok
Running generateMPK utility...............................ok
Running fingerprintMPK utility............................ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package..........................ok
Removing HaSvr files from default location..................ok
Unpacking HaSvr.............................................ok
Creating var directory......................................ok
Putting NSROOT into start scripts..........................ok
Filling in HA Server config file(s)..........................ok
Setting permissions for HA Server..........................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling GUI Server start script..........................ok
Enabling HA Server start script............................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Removing staging directory..................................ok

NOTES:
- Installation log is stored in
  /usr/netscreen/GuiSvr/var/errorLog/netmgtInstallLog.20040831155617
- This is the GUI Server fingerprint:
  You will need this for verification purposes when logging into the GUI
  Server. Please make a note of it.

Secondary GUI Server Installation
A complete example of the installer script output for installing the secondary GUI
Server is as follows:

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 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) []> 2

########## GENERAL SERVER SETUP DETAILS ##########

Will this machine participate in an HA cluster? (y/n) [n]> y

Is this machine the primary server for the HA cluster? (y/n) [y]> n
WARNING: The servers need to be stopped on the primary server during the installation of this software to avoid data corruption.

############ GUI SERVER SETUP DETAILS ############

Will the GUI Server data directory be located on a shared disk partition? (y/n) [n]
The GUI Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/GuiSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition. Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.
Enter data directory location [/var/netscreen/GuiSvr]>
Enter the management IP address of this server []> 10.150.41.10

Please enter a password for the 'super' user
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

Will a Statistical Report Server be used with this GUI Server? (y/n) [n]

############ HIGH AVAILABILITY (HA) SETUP DETAILS ############
Enter the IP address for the primary HA Server []> 10.150.41.9
Enter the IP address for the secondary HA Server [10.150.41.10]>
Enter how often to perform HA replications (10 to 1440 minutes) [60]
NOTE: Please make sure the heartbeat PASSWORD is the same for primary and secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines. The IP addresses entered here must be correct and match on both ends of the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.10]>
10.150.43.10
Enter the IP address for the peer's primary heartbeat link [10.150.41.9]>
10.150.43.9
Enter the IP address that will be used for remote HA replications [10.150.41.9]>
10.150.43.9
Enter the port used for heartbeat communication [7802]>
Enter a time interval (seconds) between heartbeat messages [15]
Enter number of missing heartbeat messages before automatic switchover occurs [4]
An IP address outside the HA cluster is needed to monitor this server's network connection.
Enter an IP address outside of the cluster[]> 10.150.47.254
Enter HA directory [/var/netscreen/dbbackup]>
The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>
The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.
Here are sample commands:
cd /root
ssh-keygen -t rsa
Chapter 4: Installing the Management System with High Availability

chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

########## BACKUP SETUP DETAILS ##########

Will this machine require local database backups? (y/n) [y]>
Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...) [02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]>

Enter number of database backups to keep [7]>

########## POST-INSTALLATION OPTIONS ##########

Start High Availability daemon processes when finished? (y/n) []> n

########## CONFIRMATION ##########

About to proceed with the following actions:
- Install GUI Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: No
- Store GUI Server data in /var/netscreen/GuiSvr
- Use IP address 10.150.41.10 for management
- Set password for 'super' user
- IP address for the primary HA Server: 10.150.41.9
- IP address for the secondary HA Server: 10.150.41.10
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.10
- IP address for the peer's primary heartbeat link: 10.150.43.9
- IP address for remote HA replications: 10.150.43.9
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: n
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n) > y

########## EXTRACTING PAYLOADS ##########

Extracting payload.................................ok
Decompressing payload..............................ok

########## PERFORMING MIGRATION TASKS ##########

########## PERFORMING INSTALLATION TASKS ##########

----- INSTALLING GUI Server ----- 
Looking for existing RPM package....................ok
Removing GuiSvr files from default location........ok
Unpacking GuiSvr.....................................ok
Installing JRE.......................................ok
Creating var directory.............................ok
Creating /var/netscreen/dbbackup....................ok
Putting NSROOT into start scripts..........................ok
Filling in GUI Server config file(s)........................ok
Setting permissions for GUI Server........................ok
Running generateMPK utility................................ok
Running fingerprintMPK utility..............................ok
Installation of GUI Server complete.

----- INSTALLING HA Server -----
Looking for existing RPM package............................ok
Removing HaSvr files from default location..................ok
Unpacking HaSvr.............................................ok
Creating var directory......................................ok
Putting NSROOT into start scripts...........................ok
Filling in HA Server config file(s)...........................ok
Setting permissions for HA Server............................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----
Disabling GUI Server start script...........................ok
Enabling HA Server start script.............................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Removing staging directory..................................ok

NOTES:
- Installation log is stored in 
  /usr/netscreen/GuiSvr/var/errorLog/netmgtInstallLog.20040831155809
- This is the GUI Server fingerprint:
  You will need this for verification purposes when logging into the GUI Server. Please make a note of it.

Primary Device Server Installation

A complete example of the installer script output for installing the primary Device Server is as follows:

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 for sufficient disk space........................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

########## GENERAL SERVER SETUP DETAILS ##########
Will this machine participate in an HA cluster? (y/n) [n]> y
Is this machine the primary server for the HA cluster? (y/n) [y]>

WARNING: The servers need to be stopped on the secondary server during the installation of this software to avoid data corruption.

############ DEVICE SERVER SETUP DETAILS ############

Will the Device Server data directory be located on a shared disk partition? (y/n) [n]>

n

The Device Server stores all of the user data under a single directory. By default, this directory is /var/netscreen/DevSvr. Because the user data (including logs and policies) can grow to be quite large, it is sometimes desirable to place this data in another partition.

Please enter an alternative location for this data if so desired, or press ENTER for the location specified in the brackets.

Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1

Enter the one-time password for this Device Server
Enter password (password will not display as you type)>

Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must provide the IP address and the port of the running GUI Server
Enter the IP address of the running GUI Server []> 10.150.41.9
Enter the port number (1-65535) of the running GUI Server [7801]>

############ HIGH AVAILABILITY (HA) SETUP DETAILS ############

Enter the IP address for the primary HA Server []> 10.150.41.7
Enter the IP address for the secondary HA Server []> 10.150.41.8
Enter how often to perform HA replications (10 to 1440 minutes) [60]>

NOTE: Please make sure the heartbeat PASSWORD is the same for primary and secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>

Please enter again for verification
Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines. The IP addresses entered here must be correct and match on both ends of the link for automatic failover to function correctly.

Enter the IP address for this machine's primary heartbeat link [10.150.41.7]>

10.150.41.7
Enter the IP address for the peer's primary heartbeat link [10.150.41.8]>

10.150.41.8
Enter the IP address that will be used for remote HA replications [10.150.41.8]>

10.150.41.8
Enter the port used for heartbeat communication [7802]>

Enter a time interval (seconds) between heartbeat messages [15]>

Enter number of missing heartbeat messages before automatic switchover occurs [4]>

An IP address outside the HA cluster is needed to monitor this server's network connection.
Enter an IP address outside of the cluster[]> 10.150.47.254
Enter HA directory [/var/netscreen/dbbackup]>

The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>

The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>
Note: A trust relationship between the primary and the secondary server, via ssh-keygen, is a requirement for the remote replication to work properly.
Here are some sample commands:
cd /root
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

############ BACKUP SETUP DETAILS ############

Will this machine require local database backups? (y/n) [y]> Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 = 2pm ...)[02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]>
Enter number of database backups to keep [7]>

############ POST-INSTALLATION OPTIONS ############

NOTE: Do not start up the Device Server unless you have already added it to the system from the UI.
Start High Availability daemon processes when finished? (y/n) []> n

############ CONFIRMATION ############

About to proceed with the following actions:
- Install Device Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: Yes
- Store Device Server data in /var/netscreen/DevSvr
- Connect to GUI Server at 10.150.41.9:7801
- IP address for the primary HA Server: 10.150.41.7
- IP address for the secondary HA Server: 10.150.41.8
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.7
- IP address for the peer's primary heartbeat link: 10.150.43.8
- IP address for remote HA replications: 10.150.43.8
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: y
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No

Are the above actions correct? (y/n) > y

############ EXTRACTING PAYLOADS ############

Extracting payload..........................................ok
Decompressing payload.......................................ok

############ PERFORMING MIGRATION TASKS ############

############ PERFORMING INSTALLATION TASKS ############
Installing the Management System In an Extended Configuration with HA Enabled

Chapter 4: Installing the Management System with High Availability

----- INSTALLING Device Server -----  
Looking for existing RPM package............................ok
Removing existing Device Server RPM.........................ok
Unpacking DevSvr............................................ok
Installing JRE..............................................ok
Creating var directory......................................ok
Creating /var/netscreen/dbbackup............................ok
Putting NSROOT into start scripts.........................ok
Filling in Device Server config file(s).....................ok
Setting permissions for Device Server.......................ok
Installation of Device Server complete.

----- INSTALLING HA Server -----  
Looking for existing RPM package............................ok
Removing existing HA Server RPM.............................ok
Unpacking HaSvr.............................................ok
Creating var directory......................................ok
Putting NSROOT into start scripts.........................ok
Filling in HA Server config file(s).........................ok
Setting permissions for HA Server.........................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----  
Disabling Device Server start script........................ok
Enabling HA Server start script.............................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Running nacnCertGeneration..................................ok
Removing staging directory..................................ok

NOTES:
- Installation log is stored in
  /usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20040901163346

- To enable firmware updates to ScreenOS 4.x devices, the TFTP server on
  this machine needs to be enabled.

- To enable firmware updates to ScreenOS 4.x devices, the TFTP server on
  this machine must have its root directory set to
    '/usr/netscreen/DevSvr/var/cache'.

Secondary Device Server Installation

A complete example of the installer script output for installing the secondary
Device Server is as follows:

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 for sufficient disk space..........................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]> 1

########## GENERAL SERVER SETUP DETAILS ##########
Will this machine participate in an HA cluster? (y/n) [n]> y
Is this machine the primary server for the HA cluster? (y/n) [y]> n
WARNING: The servers need to be stopped on the primary server
during the installation of this software to avoid data corruption.

########## DEVICE SERVER SETUP DETAILS ##########
Will the Device Server data directory be located on a shared disk partition? (y/n) [n]>

The Device Server stores all of the user data under a single directory.
By default, this directory is /var/netscreen/DevSvr. Because
the user data (including logs and policies) can grow to be quite
large, it is sometimes desirable to place this data in another
partition.
Please enter an alternative location for this data if
so desired, or press ENTER for the location specified in the
brackets.
Enter data directory location [/var/netscreen/DevSvr]>

Enter the ID assigned by the GUI to this Device Server (1-65535) []> 1
Enter the one-time password for this Device Server
Enter password (password will not display as you type)>
Please enter again for verification
Enter password (password will not display as you type)>

To enable the Device Server to communicate with the GUI Server, you must
provide the IP address and the port of the running GUI Server
Enter the IP address of the running GUI Server []> 10.150.41.10
Enter the port number (1-65535) of the running GUI Server [7801]>

########## HIGH AVAILABILITY (HA) SETUP DETAILS ##########
Enter the IP address for the primary HA Server []> 10.150.41.7
Enter the IP address for the secondary HA Server []> 10.150.41.8
Enter how often to perform HA replications (10 to 1440 minutes) [60]>
NOTE: Please make sure the heartbeat PASSWORD is the same for primary and
secondary machines.
Please enter shared password that will be used for Heartbeat authentication
Enter password (password will not display as you type)>
Please enter again for verification
Enter number of Heartbeat links between the primary and secondary machines [1]>

NOTE: Heartbeat link(s) are needed between the primary and secondary machines.
The IP addresses entered here must be correct and match on both ends of
the link for automatic failover to function correctly.
Enter the IP address for this machine's primary heartbeat link [10.150.41.8]>
10.150.43.8
Enter the IP address for the peer's primary heartbeat link [10.150.41.7]> 10.150.43.7
Enter the IP address that will be used for remote HA replications [10.150.41.7]> 10.150.43.7
Enter the port used for heartbeat communication [7802]>
Enter a time interval (seconds) between heartbeat messages [15]>
Enter number of missing heartbeat messages before automatic switchover occurs
[4]>
An IP address outside the HA cluster is needed to monitor this server's network
connection.
Enter an IP address outside of the cluster[> 10.150.47.254
Enter HA directory [/var/netscreen/dbbackup]>
The HA server(s) requires that you have previously installed the rsync program.
Enter the full path to rsync [/usr/bin/rsync]>
The HA server(s) requires that you have previously installed the ssh program.
Enter the full path for the ssh command [/usr/bin/ssh]>

Note: A trust relationship between the primary and the
secondary server, via ssh-keygen, is a requirement for the
remote replication to work properly.
Here are sample commands:
cd /root
ssh-keygen -t rsa
chmod 0700 .ssh
-- then copy .ssh/id_rsa.pub to the peer machines' .ssh/authorized_keys

########## BACKUP SETUP DETAILS ##########
Will this machine require local database backups? (y/n) [y]>
Enter hour of day to start the database backup (00 = midnight, 02 = 2am, 14 =
2pm ...)[02]>
Will daily backups need to be sent to a remote machine? (y/n) [n]>
Enter number of database backups to keep [7]>

########## POST-INSTALLATION OPTIONS ##########
NOTE: Do not start up the Device Server unless you have already added it to
the system from the UI.
Start High Availability daemon processes when finished? (y/n) []> n

########## CONFIRMATION ##########
About to proceed with the following actions:
- Install Device Server
- Install High Availability Server
- This machine participates in an HA cluster
- This server is the primary: No
- Store Device Server data in /var/netscreen/DevSvr
- Connect to GUI Server at 10.150.41.10:7801
- IP address for the primary HA Server: 10.150.41.7
- IP address for the secondary HA Server: 10.150.41.8
- HA replication frequency 60 minutes
- Number of Heartbeat links: 1
- IP address for this machine's primary heartbeat link: 10.150.43.8
- IP address for the peer's primary heartbeat link: 10.150.43.7
- IP address for remote HA replications: 10.150.43.7
- Port for HA heartbeat communication: 7802
- Seconds between heartbeat messages: 15
- Missing heartbeat messages: 4
- Outside pingable IP address: 10.150.47.254
- Become primary in the event of a tie: n
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Path for the ssh command: /usr/bin/ssh
- Local database backups are enabled
- Start backups at 02
- Daily backups will not be sent to a remote machine
- Number of database backups to keep: 7
- Start High Availability daemon processes when finished: No
Are the above actions correct? (y/n)> y

########## EXTRACTING PAYLOADS ##########
Extracting payload..........................................ok
Decompressing payload.......................................ok

########## PERFORMING MIGRATION TASKS ##########

########## PERFORMING INSTALLATION TASKS ##########

----- INSTALLING Device Server -----  
Looking for existing RPM package.........................ok
Removing existing Device Server RPM.......................ok
Unpacking DevSvr............................................ok
Installing JRE..............................................ok
Creating var directory....................................ok
Creating /var/netscreen/dbbackup............................ok
Putting NSROOT into start scripts........................ok
Filling in Device Server config file(s)....................ok
Setting permissions for Device Server.....................ok
Installation of Device Server complete.

----- INSTALLING HA Server -----  
Looking for existing RPM package............................ok
Removing existing HA Server RPM.............................ok
Unpacking HaSvr.............................................ok
Creating var directory....................................ok
Putting NSROOT into start scripts........................ok
Filling in HA Server config file(s).........................ok
Setting permissions for HA Server.........................ok
Installation of HA Server complete.

----- SETTING START SCRIPTS -----  
Disabling Device Server start script........................ok
Enabling HA Server start script.............................ok

########## PERFORMING POST-INSTALLATION TASKS ##########
Running nacnCertGeneration.................................ok
Removing staging directory................................ok

NOTES:
- Installation log is stored in
/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20040901164212

- To enable firmware updates to ScreenOS 4.x devices, the TFTP server on
  this machine must have its root directory set to
  '/usr/netscreen/DevSvr/var/cache'.
Next Steps

Congratulations! You have just completed installation of the NetScreen-Security Manager management system with HA enabled. You are now ready to begin managing your network. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide and Online Help for information describing how to plan and implement NetScreen-Security Manager for your network.
Next Steps
Chapter 5
Upgrading to FP3

In This Chapter:

- Upgrading The Management System Overview
- Defining System Parameters
- Prerequisite Steps
- Upgrading the Management System - Typical Configuration
- Upgrading the User Interface
- Upgrading the Management System - Extended Configuration
- Upgrading the Management System With HA Enabled
- In Case The Upgrade Fails...
- Next Steps

This chapter describes how to upgrade the management system and User Interface to NetScreen-Security Manager 2004 Feature Pack 3. This includes patching the management system, upgrading the User Interface on your Windows or Linux client, and validating that you have upgraded successfully.
Upgrading The Management System Overview

The following table summarizes the process for upgrading NetScreen-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 upgrade is no longer than 45 minutes.

Table 17: Upgrade Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description/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. (10 minutes)</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. (10 minutes + time to backup files)</td>
</tr>
<tr>
<td>3</td>
<td>Download the NetScreen-Security Manager 2004 FP3 management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate Web site. (10 minutes)</td>
</tr>
<tr>
<td>4</td>
<td>Run the NetScreen-Security Manager 2004 FP3 management system installer on the system where the management system is currently installed. Specify that you want to upgrade both the GUI Server and Device Server. (10 minutes)</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade the User Interface. (10 minutes)</td>
</tr>
<tr>
<td>6</td>
<td>Launch the User Interface, and then connect it to the management system. (10 minutes)</td>
</tr>
<tr>
<td>7</td>
<td>Validate that you have successfully installed the management system and User Interface. (10 minutes)</td>
</tr>
</tbody>
</table>
Defining System Parameters

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

Typical Configuration Parameters

The following table identifies the system parameters that you need to identify if you are upgrading a typical configuration of the management system — both GUI Server and Device Server on the same server machine.

Table 18: Typical Configuration - System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server data directory</td>
<td>Directory location on the Device Server where device data is stored. 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, then specify the new location during the install process. By default, the Device Server stores data in: /var/netscreen/DevSvr/</td>
<td></td>
</tr>
<tr>
<td>GUI Server data directory</td>
<td>Directory location on the GUI Server where user data is stored. 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, then specify the new location during the install process. By default, the GUI Server stores data in: /var/netscreen/GuiSvr/</td>
<td></td>
</tr>
<tr>
<td>Management IP address</td>
<td>The IP address used by the running GUI Server. The default is the IP address of the machine that you are installing on.</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Local database backup directory</td>
<td>Directory location where local database backup data is stored. By default, the GUI Server stores local database backup data at: /var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable. The default path is: /usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable. The default path is: /usr/bin/ssh</td>
<td></td>
</tr>
</tbody>
</table>
Extended Configuration Parameters

The following table describes additional system parameters that you need to identify if you are upgrading an extended configuration of the management system — GUI Server and Device Server on separate server machines:

Table 19: Extended Configuration - System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Server ID</td>
<td>Unique ID assigned when you add the Device Server</td>
<td></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>
<td></td>
</tr>
</tbody>
</table>

HA Configuration Parameters

The following table describes the system parameters that you need to identify if you are upgrading a typical configuration of the management system with HA enabled:

Table 20: HA Configuration - System Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary HA Server IP address</td>
<td>IP address of the primary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Secondary HA Server IP address</td>
<td>IP address of the secondary server participating in the HA cluster.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Your Value</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>HA replications</td>
<td>Time interval with which you want the GUI Server to replicate the database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the GUI Server replicates the database every 60 minutes.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat links between primary and secondary machine</td>
<td>Number of heartbeat communication paths between the primary and secondary machine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, there is only 1 communication link between the primary and secondary machine.</td>
<td></td>
</tr>
<tr>
<td>Shared password for heartbeat authentication.</td>
<td>This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</td>
<td></td>
</tr>
<tr>
<td>IP Address for Primary machine’s heartbeat link</td>
<td>IP address used for heartbeat communications on the primary server machine.</td>
<td></td>
</tr>
<tr>
<td>Port used for heartbeat communication</td>
<td>The port number used for heartbeat communications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default port is 7802.</td>
<td></td>
</tr>
<tr>
<td>Heartbeat messages time interval</td>
<td>Time interval (in seconds) between heartbeat messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default is 15 seconds.</td>
<td></td>
</tr>
<tr>
<td>Missing heartbeats before switchover occurs</td>
<td>Number of missing heartbeat messages before automatic switchover to the secondary machine occurs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default is 4 messages.</td>
<td></td>
</tr>
<tr>
<td>IP Address outside the HA cluster</td>
<td>Network IP Address used to monitor this server’s network connection.</td>
<td></td>
</tr>
<tr>
<td>HA directory</td>
<td>Directory location where high availability data is stored. Note that the same directory location is used if you configure this machine to perform local database backups.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the HA Server stores data at:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/var/netscreen/dbbackup/</td>
<td></td>
</tr>
<tr>
<td>Path to the rsync utility executable</td>
<td>Path to the rsync utility executable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/usr/bin/rsync</td>
<td></td>
</tr>
<tr>
<td>Path to the ssh utility executable</td>
<td>Path to the ssh utility executable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default path is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>/usr/bin/ssh</td>
<td></td>
</tr>
<tr>
<td>Remote Backup Machine IP Address</td>
<td>IP address of the machine where remote backups are sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, the installer sets this to the IP address of the secondary HA Server.</td>
<td></td>
</tr>
</tbody>
</table>
Defining System Parameters

Shared Disk Parameters

The following table identifies the additional system parameters that you need to identify to upgrade the management system with HA enabled with access to a shared disk:

**Table 21: Shared Disk Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour of the Day to Start Local Database Backup</td>
<td>Time of day that you want the GUI Server to backup the database. Type a 2 digit number representing the time of day in a 24 hour day (00-23). For example, if you want the backup to begin at 4:00 A.M., type 04; if at 4:00 P.M., type 16. It is recommended that you set this parameter to a time of day that effectively minimizes your network downtime. The GUI Server completes the daily backup process within the hour specified every day. By default, the GUI Server performs the daily backup within an hour after 2am.</td>
<td></td>
</tr>
<tr>
<td>Number of Local Database Backup Files Stored</td>
<td>Total number of database backup files that the GUI Server stores. When the GUI Server reaches the maximum number of backup files you configure, it overwrites the oldest file. By default, the GUI Server stores seven backup files.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to mount the shared disk partition</td>
<td>The command to mount the shared data partition. The default command is: /bin/mount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to unmount the shared disk partition</td>
<td>The command to unmount the shared data partition. Before configuring this command, you must first verify that your mounts are defined properly. The default command is: /bin/umount /var/netscreen/DevSvr</td>
<td></td>
</tr>
<tr>
<td>Command to check the integrity of the shared data partition</td>
<td>The command to check the integrity on the shared data partition. The default command is: /sbin/fsck</td>
<td></td>
</tr>
<tr>
<td>Directory path for the shared disk</td>
<td>Directory path of the shared disk mount point.</td>
<td></td>
</tr>
</tbody>
</table>
Prerequisite Steps

You can upgrade the management system from any previous running version of NetScreen-Security Manager.

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, then run the following command to become root:

   su -

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

   **NOTE:** In NetScreen-Security Manager 2004 FP3, the NetScreen-Security Manager management system runs as the root user. If you want to run the management system in a more secure mode, then refer to Changing Permissions To a Normal User on page 151.

3. Partition drives for sufficient disk space to accommodate your planned data requirements. Ensure that you have allocated a maximum amount of disk space for the data partition (i.e., /var/netscreen directory).

   Refer to the Hardware Sizing Recommendations document for NetScreen-Security Manager 2004 FP3 for more information about the disk space requirements appropriate for your specific network.

4. Perform a backup of all files on the Device Server and GUI Server. Refer to Archiving and Restoring Logs and Configuration Data on page 152 for more information archiving your data files.

5. Run the system update utility for your appropriate platform to ensure that you have all the up to date utilities and packages required to run the installer properly. Refer to Running the System Update Utility on page 128 for more information on running the system update utility.

6. If you are installing the management system on Solaris 9, and are planning to perform local database backups, then you must update the Sun Solaris ssh daemon. Refer to Patching the Sun Solaris SSH Daemon on page 129 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 NetScreen-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
```

**Running the System Update Utility**

Use the system update utility to upgrade your system with the latest patches and packages required to run the NetScreen-Security Manager management system installer properly.

To run the system update utility:

1. Save the system update utility appropriate for your platform (for example, `systemupdate-nsm-linux` for Linux, `systemupdate-nsm-solaris` for Solaris) that is provided on the NetScreen-Security Manager Installation CD or from the directory where it is saved, to a suitable directory on the server.

2. Uncompress the system update utility file. For example, you would run the following command on Linux:

```
gzip -d systemupdate-nsm-linux.tar.gz
```

3. Untar the appropriate system update utility file. For example, you would run the following command on Linux:

```
tar xfv systemupdate-nsm-linux.tar
```

A subdirectory called `/systemupdate-nsm-<platform>` is created and all of the files required to update your system packages and utilities are extracted into that directory.

4. Navigate to the `/systemupdate-nsm-<platform>` subdirectory.

5. Run the update shell archive script. For example, you can execute the shell archive script by running the following command:

```
./update.sh
```
The script proceeds to check your system for required updates. It next prompts you to type <Enter> to continue or Ctrl-C to stop.

6. Press <Enter> to continue. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 20 minutes. The script proceeds to cleanup the RPM database. Let the script run to completion. This process can take up to 10 minutes depending upon the number of packages that need to be installed.

**Patching the Sun Solaris SSH Daemon**

If you are running NetScreen-Security Manager 2004 FP3 on a Solaris 9 system, and you want to perform a database backup, replicate the database remotely, or enable high availability functionality, you must patch the Sun Solaris SSH daemon on both servers. This is because of a known issue in the Sun Solaris SSH daemon that may result in a failure to replicate.

To patch the Sun Solaris SSH daemon on Solaris 9:

1. Login to the server machine that you are running NetScreen-Security Manager as root. You must also be in single user mode.

2. Use a web browser to download the Sun Solaris patch 113273-07 from the following URL:

    <http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=113273&rev=01>
3. Extract the packages. For example, run the following commands:

   `unzip /tmp/113273-07.zip`

4. Install the packages. Make sure that you are in the directory where you downloaded the packages. The following example installs the patch to a standalone system:

   `patchadd /tmp/113273-07`

   Checking installed patches...
   Verifying sufficient filesystem capacity (dry run method)...
   Installing patch packages...

   Patch number 113273-07 has been successfully installed.
   See /var/sadm/patch/113273-07/log for details

   Patch packages installed:
   SUNWsshdu

5. Verify that the patch has been installed. For example, run the following command:

   `showrev -p | grep 113273-07`

   Patch: 113273-07 Obsoletes: Requires: Incompatibles: Packages: SUNWsshdu

6. Restart the server machine.
### Upgrading the Management System - Typical Configuration

In most typical cases, you 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 - Extended Configuration on page 139.

To upgrade the management system on a single system:

1. Load the NetScreen-Security Manager 2004 FP3 management system installer software onto the server where the NetScreen-Security Manager management system is currently installed. You can run the installer directly from the NetScreen-Security Manager installation CD. You can also copy the installer to a directory on the server, or you can download the installer from the Juniper Networks Customer Services Online web site.

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

3. Run the management system installer.

   On Linux, run the following command:
   
   ```sh
tensh nsm04fp3_servers_linux_x86.sh
```

   On Solaris, run the following command:
   
   ```sh
tensh nsm04fp3_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 NetScreen-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 whether you want to perform a clean install or repair of the existing management system components.

4. Type 2 to specify that you want to upgrade both the Device Server and GUI Server. The following graphic depicts the installer running on Linux. The installer running on Solaris displays similar prompts and messages.

```
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 installed Device Server is newer...... ok
Checking if installed GUI Server is newer.......... ok
Checking if installed DB Backup Tool 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
Noting name........................................ ok
Stopping any running servers

############## GATHERING INFORMATION ##############

1) Clean install of both Device Server and GUI Server
2) Upgrade both Device Server and GUI Server from v1.1.1 to v1.2.1
Enter selection (1-2) [2]> 2
```

**NOTE:** If you specify that you want to upgrade the Device Server and GUI Server, all data previously configured in the system is restored in FP3. If you do not want to restore your previous configuration data, then choose to have the installer perform a clean install of both the Device Server and GUI Server.

The script then gathers information about your previous installation of NetScreen-Security Manager. If the script detects that you installed certain features or components, for example, the HA Server watchdog process, it prompts you to configure additional parameters required so that the feature/component continues to work in NetScreen-Security Manager FP3.
The script prompts you to specify whether or not you want this machine to participate in an HA cluster.

5. Type **n** and then press <Enter>, if you do not want to upgrade the management system with high availability. Type **y** and then press <Enter>, if you do want to upgrade the management system with high availability. Refer to Upgrading the Management System With HA Enabled on page 140 for more information about upgrading and configuring the management system with high availability enabled.

The script next prompts if you want to migrate data about your versioned domains. Depending upon the size of the data that may be involved in this process, domain version migration can take an extremely long time to complete. For previous installations of NetScreen-Security Manager with many domain versions, it is not recommended that you migrate your versioned domains as part of the upgrade process. A tool is provided so that you can migrate this information manually after upgrading.

6. Type **n** and then press <Enter>, if you do not want to migrate your versioned domains. Type **y** and then press <Enter>, if you still want to migrate data about your versioned domains.

    ![Statistical Report Server](image)

The script next prompts if you want to use a Statistical Report Server with this GUI Server.

7. Type **n** and then press <Enter>, if you do not want to use a Statistical Report Server. Type **y** and then press <Enter>, if you are using a Statistical Report Server. If you are using a Statistical Report Server, the installer prompts you for additional information (i.e., database type, database user name, database password). Refer to the NetScreen-Statistical Report Server Installer’s Guide for more information about these configuration parameters.

The script next prompts if you want to restart the server processes automatically in case of a failure.

8. Type **y** and then press <Enter> to restart the server processes automatically in case of a failure. Type **n** and then press <Enter>, if you do not want to restart server processes.

The script next prompts if you want to perform a backup of the database locally.

9. Type **n** and then press <Enter>, if you do not want to perform a local database backup. Type **y** and then press <Enter>, if you want to perform local database backups.
If you want to perform local database backups, the installer prompts you to configure additional information (i.e., time to start the database backup, backup directory, path to the rsync executable).

The script next prompts you to specify whether or not you want to start the servers when the upgrade process is finished.

10. Type y and then press <Enter> to start both servers after the installer has completed the upgrade process. Type n and then press <Enter>, if you do not want to start both servers after the upgrade process is complete.

**NOTE:** When you restart your operating system, the GUI and Device Servers start automatically.

The script then prompts you to verify your upgrade configuration settings.

11. Verify your settings, and if they are correct, type y and then press <Enter> to proceed. If you type n and then press <Enter>, the installer returns you to the original selection prompt.
The upgrade proceeds automatically. The installer proceeds to perform the following actions:

- Extracts the software payloads
- Upgrades the Device Server
- Upgrades the GUI Server
- Installs the HA Server
- Sets start scripts
Performs post-installation tasks such as removing the staging directory and starting the server processes (if configured)

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

**Starting Server Processes Manually**

If you did not specify the installer to start the server(s) when finished, then you must manually start the management system processes. You can start all the management system processes by starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, run the following command:

   ```
   cd /usr/netscreen/HaSvr/bin
   ```

2. Run the following command:

   ```
   ./haSvr.sh start
   ```

**NOTE:** If you start the HA Server process, then it automatically starts the GUI Server and Device Server processes.
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 HA Server bin subdirectory. For example, run the following command:
   
   ```bash
   cd /usr/netscreen/HaSvr/bin
   ```
2. Run the following command:
   
   ```bash
   sh haSvr.sh status
   ```

To check the status of the GUI Server:
1. Navigate to the GUI Server bin subdirectory. For example, run the following command:
   
   ```bash
   cd /usr/netscreen/GuiSvr/bin
   ```
2. Run the following command:
   
   ```bash
   sh guiSvr.sh status
   ```

To check the status of the Device Server:
1. Navigate to the Device Server bin subdirectory. For example, run the following command:
   
   ```bash
   cd /usr/netscreen/DevSvr/bin
   ```
2. Run the following command:
   
   ```bash
   sh devSvr.sh status
   ```

Refer to Controlling the Management System on page 146 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 November 1, 2004 at 6:00 P.M., then the installation log file would be named: `netmgtInstallLog.20041101180000`

**NOTE:** After 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 NetScreen-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 NetScreen-Security Manager UI.

Refer to Running the User Interface on page 44 for more information on running the UI installer. After you install the UI, you can connect it to the management system.

Validating the Upgrade

After 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 NetScreen-Security Manager UI to view and edit your configuration on the management system.

To validate your configuration on the Device Server:

1. From the NetScreen-Security Manager UI, select Server Manager > Servers. The Servers view appears displaying Device Server and GUI Server information.

2. 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.

3. Use the General tab to verify the following information:
   
   - **Device Server Manager Port** — the default port is 7800.
   - **Device Server ID** — the ID number identifies the Device Server; you cannot change the Device Server ID.
   - **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.

4. Click OK when you are done.
Upgrading the Management System - Extended Configuration

The process for upgrading 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 upgrade the GUI Server only.

3. Run the management system installer on the server where you have currently installed the Device Server. Specify that you want to upgrade the Device Server only.

4. Wait approximately 10-15 minutes so that the Device Server can successfully re-connect to the GUI Server.

5. Run the UI installer on the computers where you have installed the UI client.

6. Launch the UI and verify that you can connect to the upgraded GUI Server.
Upgrading the Management System With HA Enabled

The process for upgrading the management system with HA enabled is as follows:

1. Perform the pre-requisites steps as described in Prerequisite Steps on page 27. Perform the additional prerequisite steps as described in Chapter 4, Installing the Management System with High Availability.

2. Stop the primary and secondary GUI and Device Servers.

3. Run the management system installer on the primary server(s) where you have currently installed the GUI and Device Servers. Specify that you want to upgrade the server(s).

4. Configure the following HA parameters when prompted during the General Server Setup Details, the Device Server Setup Details, and the GUI Server Setup Details:
   - Type `y` and then press `<Enter>` when prompted if this machine will participate in an HA Cluster.
   - Type `y` and then press `<Enter>` when prompted if this machine is the primary server for the HA Cluster.
   - Type `y` and then press `<Enter>` if the Device Server data directory is located on a shared disk partition. Type `n` and then press `<Enter>`, if you are not using a shared disk partition for the Device Server.
   - Type `y` and then press `<Enter>` if the GUI Server data directory is located on a shared disk partition. Type `n` and then press `<Enter>`, if you are not using a shared disk partition for the GUI Server.

5. Configure the following HA parameters when prompted during the High Availability (HA) Setup Details:
   - Enter the IP address for the primary HA Server.
   - Enter the IP address for the secondary HA Server.
   - Type the number of HA replications.
   - Type the number of heartbeat links between the primary and secondary machines.
   - Type the IP address for this machine’s primary heartbeat link.
   - Type the IP address for the peer’s primary heartbeat link.
   - Type the port number used for heartbeat communication.
   - Enter a time interval in seconds between heartbeat messages.
   - Enter the number of missing heartbeat messages before automatic switchover occurs.
Enter an IP address outside the HA Cluster to monitor this server’s network connection

- Enter the HA/database backup directory
- Type the full path to the rsync executable
- Type the full path for the ssh executable

NOTE: If you are installing the management system on Solaris, the path to the ssh executable is typically different than the default setting of /usr/bin/rsync. It is typically /usr/local/bin.

6. Run the management system installer on the secondary server machines (if applicable). Configure parameters that are appropriate for the secondary server.

7. Start the primary and secondary GUI and Device Servers.

8. Run the UI installer on the computers where you have installed the UI client. Refer to Upgrading the User Interface on page 138 for more information.

9. Launch the UI and verify that you can connect to the upgraded GUI Server.

10. Configure the HA cluster. Refer to Chapter 4, Installing the Management System with High Availability for more information.

11. Test HA replication. Refer to Chapter 4, Installing the Management System with High Availability for more information.

Upgrading the Database Backup Files

If you have implemented your previous installation of NetScreen-Security Manager 2004 FP2 with high availability, and upgraded to NetScreen-Security Manager 2004 FP3, you will also need to upgrade the data in your previous local and remote database backup directories. It is recommended that you do so manually by running the replicateDb script on the primary server. Refer to Backing Up the Database Locally on page 155 for more information. If you do not manually replicate the database, the upgrade occurs automatically during the next scheduled remote database replication interval (default is 1 hour).

NOTE: In the unlikely event that the primary server goes down before the next scheduled remote database replication, the data on the secondary server will not be upgraded. In this case, you will need to perform a manual data replication/upgrade on the secondary server.
In Case The Upgrade Fails...

In the event that the upgrade fails, it is possible to restore data from your previous installation back to the version of NetScreen-Security Manager that you were previously running. This is only possible if you performed the required backup of your GUI Server configuration data and Device Server log data before performing the upgrade and migration process.

The process for restoring your previous installation is as follows:

1. Check the audit log in the UI for any changes that you might have made after installing NetScreen-Security Manager 2004 FP3. This will provide you with guidelines for any data that you might need to restore.

2. Remove all existing components of the NetScreen-Security Manager management system. Refer to Removing the Management System on page 163 for more information.

3. Perform a clean installation of NetScreen-Security Manager. Refer to the appropriate version of NetScreen-Security Manager documentation for more information about installing your version of NetScreen-Security Manager.

4. Restore your configuration and log data from backup. Refer to Restoring Logs and Configuration Data on page 153 for more information.
Next Steps

Congratulations! You have just completed installation of the NetScreen-Security Manager management system with HA enabled. You are now ready to begin managing your network. Refer to the NetScreen-Security Manager 2004 FP3 Administrator’s Guide and Online Help for information describing how to plan and implement NetScreen-Security Manager for your network.
Chapter 6

Maintaining NetScreen-Security Manager

In This Chapter:

- Controlling the Management System
- Maintaining the Management System
- Archiving and Restoring Logs and Configuration Data
- Configuring High Availability
- Relocating the Database
- Installing a tftp Server
- Downgrading from Feature Pack 3 to Feature Pack 2
- Removing the Management System
- Uninstalling the User Interface

This chapter describes basic procedures used to administer NetScreen-Security Manager. This includes instructions describing how to manually send commands to the management system such as start and stop, configure the GUI Server, Device Server and HA Server manually, configure the local database backup option, install a tftp server (required if you are managing FW/VPN devices running ScreenOS 4.0.x), and uninstall the management system and User Interface.
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 then issuing a manual command.

Viewing Management System Commands

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

1. Navigate to the GUI Server bin subdirectory. For example, you would run the following command:

   ```bash
cd /usr/netscreen/GuiSvr/bin
   ```

2. Run the following command:

   ```bash
./guiSvr.sh
   ```

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

1. Navigate to the Device Server bin subdirectory. For example, you would run the following command:

   ```bash
cd /usr/netscreen/DevSvr/bin
   ```

2. Run the following command:

   ```bash
./devSvr.sh
   ```

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

1. Navigate to the HA Server bin subdirectory. For example, you would run the following command:

   ```bash
cd /usr/netscreen/HaSvr/bin
   ```

2. Run the following command:

   ```bash
./haSvr.sh
   ```

Common Management System Commands

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, and then instructs the process to reload its configuration and start again.</td>
</tr>
<tr>
<td>restart</td>
<td>Stops the management system process for two seconds, and then restarts the process.</td>
</tr>
</tbody>
</table>
Starting All Server Processes Using the HA Server

If you have installed the HA Server process, it is highly recommended that you start all the management server processes by simply starting the HA Server process.

To start the HA Server process manually:

1. Navigate to the HA Server bin subdirectory. For example, you would run the following command:
   
   ```
   cd /usr/netscreen/HaSvr/bin
   ```

2. Run the following command:
   
   ```
   ./haSvr.sh start
   ```

**NOTE:** The HA Server process automatically starts the GUI Server and Device Server processes.

Starting GUI Server and Device Server Processes Manually

If you have not installed the HA Server process, you can manually start the GUI Server and Device Server processes.

To start the GUI Server manually:

1. Navigate to the GUI Server bin subdirectory. For example, you would run the following command:
   
   ```
   cd /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 inactive and not running, then the Device Server fails to connect to it.

To start the Device Server manually:

1. Navigate to the Device Server bin subdirectory. For example, you would run the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<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>
cd /usr/netscreen/DevSvr/bin

2. Run the following command:

./devSvr.sh start

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. For example, you would run the following command:

   cd /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. For example, you would run the following command:

   cd /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. For example, you would run the following command:

   cd /usr/netscreen/HaSvr/bin

2. Run the following command:

   ./haSvr.sh stop
Maintaining the Management System

The following procedures are provided for your reference:

- Changing the Management System IP Address on page 149
- Changing the Device Server IP Address on page 149
- Changing the GUI Server IP Address on page 150
- Changing Permissions To a Normal User on page 151

Changing the Management System IP Address

If you have installed the NetScreen-Security Manager management system on a single server (in the basic configuration), and you move it later to a different server, then 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 that is 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.
7. Navigate to `usr/netscreen/GuiSvr/var`.
8. Open the `server_table.nml` file in any text editor.
9. Edit the values for the IP Address in both GUI and Device Server sections.
10. Save the `server_table.nml` file.
11. Restart the GUI Server, and then restart the Device Server.

Changing the Device Server IP Address

If you have installed the NetScreen-Security Manager management system on separate servers (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 devices 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 that is running the GUI Server as root.

3. Navigate to `usr/netscreen/GuiSvr/var`

4. Open the `server_table.nml` file in any text editor.

5. Edit the values for the IP Address in the Device Server section only.


7. Restart the GUI Server.

**Configuring the Device Server Manually**

You can also manually configure parameters on the Device Server that control connection timing with the managed FW/VPN devices in your network.

1. Login to the server that is running the Device Server as root.

2. Navigate to `usr/netscreen/DevSvr/var`

3. Open the Device Server configuration file (called `devSvr.cfg`) in any text editor.

4. Edit the time value (in thousandths of a second) for the `devSvrDirectiveHandler.fastCli.timeout` parameter to change the way the Device Server controls connection timing with managed FW/VPN devices running ScreenOS 4.x.

5. Save the file.

6. Restart the Device Server.

**NOTE:** The `devSvrDirectiveHandler.fastCli.timeout` parameter determines the amount of time that the Device Server waits for a CLI response from a FW/VPN device running ScreenOS 4.x before it disconnects the connection. By default, the Device Server waits 40 seconds before disconnecting the connection.

**Changing the GUI Server IP Address**

If you have installed the NetScreen-Security Manager management system on separate servers (in the extended configuration), and you later move the GUI Server to a different server, then 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 that is running the Device Server as root.

2. Navigate to `usr/netscreen/DevSvr/var`

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 Device Server configuration file.

5. Login to the server that is running the GUI Server as root.

6. Navigate to usr/netscreen/GuiSvr/var

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.

9. Save the server_table.nml file.

10. Restart the GUI Server, then restart the Device Server.

Changing Permissions To a Normal User

The NetScreen-Security Manager management system runs by default as the root user. If you want to 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 shell archive script called “setperms.sh” is included for both the Device Server and GUI Server that automatically changes the setuid.user value in case you want to switch to the more secure setup.

To create a normal user and change permissions:

1. Stop the HA Server, the Device Server, then the GUI Server.

2. On each of the management system server machines, create a normal user called “nsm” and a group called “nsm”, with the user nsm as the only member.

   You can do so by running the following commands:

   groupadd nsm
   useradd -g nsm nsm

3. Run the change permissions script on the Device Server.

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

4. Run the change permission script on the GUI Server.

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

5. Start the HA Server, GUI Server, and then the Device Server.

6. Verify that the permissions you set are working correctly. One way to check is to verify that the NetScreen-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.
Archiving and Restoring Logs and Configuration Data

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

Before you begin archiving, it is important that you first stop the processes running on both servers. After you have stopped both servers, you will then need to identify the actual location of the GUI Server and Device Server data directories. These are the directories that you need to back up. You can do this by running an "ls -al" command on the following directory locations:

- /usr/netscreen/GuiSvr/var (or the path that you configured when you initially installed the GUI Server)
- /usr/netscreen/DevSvr/var (or the path that you configured when you initially installed the Device Server)

To archive log and configuration data:

1. Stop the HA Server; stop the Device Server; and then stop the GUI Server.
2. Use the "ls -al" command to discover the actual paths of the GUI Server and Device Server data directories.

```
ls -al /usr/netscreen/GuiSvr/var
```

```

lrwxrwxrwx 1 root root 21 Feb 25 16:04 /usr/netscreen/GuiSvr/var -> /var/netscreen/GuiSvr
```

The output above indicates that the actual location of the GUI Server data is in: /var/netscreen/GuiSvr

Verify where your data is stored and which directories should be backed up on your own system. Follow the same procedure to determine the location of your data on the Device Server.

3. Run the appropriate backup command on your Solaris or Linux platform to backup the GUI Server data. For example, you can do so by running the following command:

```
tar -cvf /netscreen_backup/db-data.tar /var/netscreen/GuiSvr
gzip db-data.tar
```

4. Run the appropriate backup command on your Solaris or Linux platform to backup the Device Server data. It is recommended that you use either Secure Copy or FTP to backup the Device Server data.

```
scp -r <local directory> usr@host:<remote-directory>
```

**NOTE:** Using tar may not be appropriate for log data in the Device Server which may be very large.

For example, you can use scp by running the following command:

```
scp -r <local directory> usr@host:<remote-directory>
```
For example, you can use ftp by running the following command:

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

5. It is recommended that you relocate backup copies of both the GUI Server configuration data and Device Server log data to an external location or disk.

6. Start the HA Server, GUI Server, and then the Device Server.

**Restoring Logs and Configuration Data**

To restore log and configuration data:

1. Stop the HA Server, Device Server, and then the GUI Server.

2. Use the mv command to move data from the "var" directories to a safe location.

3. Untar or place your backups into both of the locations described above.

4. Start the HA server, the GUI Server, and then finally, the Device Server.

**NOTE:** These instructions apply only to systems where the "var" links point to a true location outside the prescribed locations (/usr/netscreen/GuiSvr or /usr/netscreen/DevSvr). It is not recommend that you have these links point to locations that are inside /usr/netscreen/GuiSvr or /usr/netscreen/DevSvr. This will complicate any upgrade of NetScreen-Security Manager and will require special precautions during backup and restore.
Configuring High Availability

You can manually configure the high availability options on the management system by editing the High Availability configuration file (called haSvr.cfg).

Enabling and Disabling High Availability Processes

To enable high availability:

1. Stop the running server process(es).

1. Navigate to the High Availability configuration directory. For example, you would run the following command:

   \texttt{cd /usr/netscreen/HaSvr/var/}

2. Open the High Availability configuration file (haSvr.cfg) in any text editor.

3. Configure the following parameters:

   \texttt{highAvail.isHaEnabled=y}
   \texttt{highAvail.isWatchdogEnabled=n}

4. Save the file.

5. Restart the running server process. You can do so by running the following command:

   \texttt{/usr/netscreen/HaSvr/bin/haSvr.sh restart}

To disable high availability, follow the above procedures to High Availability configuration file, configure the following parameter, and save the file:

\texttt{highAvail.isHaEnabled=n}

Configuring High Availability Options

Other parameters in the High Availability configuration file enable you to change how high availability works in your network.

To configure other high availability options:

1. Stop the running server process(es).

2. Navigate to the HA Server configuration directory (var/netscreen/HaSvr by default).

3. Open the HA Server configuration file (haSvr.cfg) in any text editor.

4. Configure the file as needed:

   - To change the HA Server (and local database) backup directory, edit the value for the highAvail.pathDbBackup variable.
To change the time of day that the HA replication begins, edit the value for the `highAvail.backupTimeHour` variable.

To change the number of backup files that the tool saves, edit the value for the `highAvail.numOfBackup` variable.

To change the path to the rsync package, edit the value for the `highAvail.rsyncLocation` variable.

To change the heartbeat interval, edit the value for the `highAvail.heartbeatInterval` variable.

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

**Running the Remote Replication Utility as a Non-Root User**

If you are prohibited from establishing a trust-relationship between root users on different machines, you can run the remote replication utility as a non-root user. For your convenience, a script called `setRsyncUser` is provided in the `utils` directory of the HaSvr under `/usr/netscreen` (i.e., `/usr/netscreen/HaSvr/utils/setRsyncUser`), enabling you to run the remote replication utility as non-root user. A README called `README.remote.replication.as.nonroot` file is also provided (in the same directory) with instructions on running the script.

**Backing Up the Database Locally**

A shell archive script is provided for your convenience to manually backup the database locally.

To replicate the database locally:

1. Stop the running server process(es).
2. Navigate to the HA Server utilities subdirectory (`/usr/netscreen/HaSvr/utils` by default).
3. Run the replicate database shell archive script. You can do so by running the following command:

   ```
   ./replicateDb backup
   ```

   The local backup is created under the directory specified by the `highAvail.pathDbBackup` parameter in the High Availability configuration file. By default, it is created in `/var/netscreen/dbbackup`.

**Restoring the Database**

If for any reason you are required to restore the database, then you can invoke a shell archive script.

To restore the database:
1. Install NetScreen-Security Manager 2004 FP3 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 local 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 local database backup data directory on your new management system server.


4. Run the database restore shell archive script and specify the number day of the week for the backup file that you want to restore from (N = backup day of the week). You can do so by running the following command:

   ```bash
   restoreDbFromBackup.sh N
   ```

   For example, to restore the backup file from Friday:

   ```bash
   sh restoreDbFromBackup.sh 5
   ```

   The restore script first prompts you to confirm stopping the running server process(es). It proceeds to verify that you have properly logged in as the root user. It then verifies that the backup file specified exists. If so, then the script proceeds to stop all running server processes. It then uses rsync to copy the backup file to the appropriate server directories. After it has completed restoring the files, it restarts all server processes.

**Validating the Database Recovery Process**

If you are using the local database backup option on a network where the GUI Server and Device Server are installed on separate systems, then 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 local database backup option properly on the GUI and Device Servers. In this event, contact technical support for assistance.
Relocating the Database

The following process is recommended in the event that you want to move the database from one system to another:

- Archive the database on the GUI Server
- Archive the log database on the Device Server
- Install NetScreen-Security Manager on a new system.
- Copy over the GUI Server database on the new system
- Copy over the Device Server log database on the new system.

Archiving the GUI Server Database and Device Server Log Database

To archive the GUI Server database and the Device Server log database:

1. Verify that the system is working properly.

2. Stop the GUI Server and any High Availability processes (for example, iHaSvr, if you are running NetScreen-Security Manager 2004 FP1 or haSvr, if you are running NetScreen-Security Manager 2004 FP3). You can do so by running the following commands:

   ```
   /etc/init.d/haSvr stop
   /etc/init.d/guiSvr stop
   ```

3. Tar and compress the current GUI Server database. You can do so by running the following commands:

   ```
   tar -cvf guidb.tar /var/netscreen/GuiSvr
   gzip guidb.tar
   ```

4. Stop the Device Server and any High Availability processes (for example, iHaSvr, if you are running NetScreen-Security Manager 2004 FP1 or haSvr, if you are running NetScreen-Security Manager 2004 FP2). You can do so by running the following commands:

   ```
   /etc/init.d/haSvr stop
   /etc/init.d/devSvr stop
   ```

5. Verify that you have sufficient disk space available on the Device Server to backup your current logs.

6. Tar and compress the current Device Server logs. You can do so by running the following commands:

   ```
   tar -cvf devsvrdb.tar /var/netscreen/DevSvr/logs
   gzip devsvrdb.tar
   ```
Installing NetScreen-Security Manager On a New System

Refer to Chapter 2, Installing Typical Configuration for more information on installing the management system on the same server machine.

Refer to Chapter 3, Installing Extended Configuration for more information on installing the management system on separate server machines.

Moving the Databases to the New System

To move the GUI Server database on the new system:

1. On the new GUI Server, make a backup directory for your configurations. You can do so by running the following commands.

   mkdir /backup
   cp /var/netscreen/GuiSvr/server_table.nml /backup
   cp /var/netscreen/GuiSvr/shadow_server_table.nml /backup
   cp /var/netscreen/GuiSvr/global/admin_table.nml /backup

2. Unzip and untar the database. You can either recursive copy the files or replace the new database with the old one.

3. Replace the configuration files from backup. You can do so by running the following commands:

   # cp /backup/server_table.nml /var/netscreen/GuiSvr
   # cp /backup/shadow_server_table.nml /var/netscreen/GuiSvr
   # cp /backup/admin_table.nml /var/netscreen/GuiSvr/global

   **NOTE:** This is only required if the passwords/admins are different.

4. Start the GUI Server and verify that all processes are running properly. You can do so by running the following commands:

   /etc/init.d/guiSvr start
   /etc/init.d/haSvr start
   /etc/init.d/guiSvr status
   /etc/init.d/haSvr status

To copy the Device Server log database on the new system:

1. On the Device Server, unzip and untar the old Device Server logs database. You can either recursive copy the files or replace the new database with the old one.

2. Navigate to the /var/netscreen/DevSvr/logs directory and delete all the ".mark" files. You can do so by running the following commands:

   rm -rf *.mark

3. Start the Device Server and verify that all the server processes are running.

   /etc/init.d/devSvr start
/etc/init.d/devSvr status
/etc/init.d/haSvr start
/etc/init.d/haSvr status
Installing a tftp Server

If you are using NetScreen-Security Manager to manage FW/VPN devices running ScreenOS 4.0.x, then you need to 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.

It is not recommended that you use a tftp server to download software for your ScreenOS 4.0.x device because communications are not secured. If your devices are running ScreenOS 4.0.x, and you want to use a tftp server to download software to your devices, then it is highly recommended that you use the ScreenOS WebUI to download software via https.

Installing a tftp Server on Linux

Before installing the tftp server on your Red Hat Linux server, check for previous installations.

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

```
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, then 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. After 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:

```
server 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
}
```
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
   ```
Downgrading from Feature Pack 3 to Feature Pack 2

If you upgrade to FP3, and then decide to downgrade back to FP2, then you need to reinstall FP2 and restore your old data. Before you upgrade NetScreen-Security Manager to Feature Pack 3, verify that you have made a backup copy of all of your existing data from Feature Pack 2.

NOTE: Before downgrading, check the audit log for any changes that you might have made, that you may need to restore once the downgrade is complete.

To downgrade from FP3 to FP2:

1. Make a backup copy of all your existing data.
2. Remove the management system. Refer to Removing the Management System on page 163 for more information.
3. Install FP2.
4. Restore your backup database. Refer to Restoring the Database on page 155 for more information.
Removing the Management System

To remove previous management system installations:

1. Stop the HA Server by running the following commands:
   
   ```
   cd /usr/netscreen/HaSvr/bin
   ./HaSvr.sh stop
   ```

2. Stop the Device Server by running the following commands:
   
   ```
   cd /usr/netscreen/DevSvr/bin
   ./devSvr.sh stop
   ```

3. Stop the GUI Server by running the following commands:
   
   ```
   cd /usr/netscreen/GuiSvr/bin
   ./guiSvr.sh stop
   ```

4. Navigate to the `/usr` subdirectory, and remove all the files in the `netscreen` subdirectory.
   
   ```
   rpm -e netscreen-DevSvr
   rpm -e netscreen-GuiSvr
   rpm -e netscreen-HaSvr
   rm -rf netscreen
   ```

5. Navigate to the `/var` subdirectory, and remove all the files in the `netscreen` subdirectory.

   ```
   rm -rf netscreen
   ```
Uninstalling the User Interface

If you need to uninstall the NetScreen-Security Manager UI, run the NetScreen-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 NetScreen-Security Manager UI.

To uninstall the NetScreen-Security Manager UI:

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

   `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.
Appendix A
Technical Overview

This appendix describes the NetScreen-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 NetScreen-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 NetScreen-Security Manager provides all of 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 NetScreen-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 NetScreen-Security Manager UI. 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 NetScreen-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 NetScreen-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, then it automatically restarts the process.
About the NetScreen-Security Manager User Interface (UI)

The NetScreen-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. After 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 FP3 Administrator’s Guide or the Online Help included in the UI for more information about the NetScreen-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 NetScreen-Security Manager management architecture. The following table details the FW/VPN devices and versions of ScreenOS supported by NetScreen-Security Manager.

Table 23: NetScreen FW/VPN Devices and ScreenOS Versions Supported

<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, 5.1</td>
</tr>
<tr>
<td>NS5XT</td>
<td>4.0.0, 4.0.0-DIAL2, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS25</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS50</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS100</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.1</td>
</tr>
<tr>
<td>NS204</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS208</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS500</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS500 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5200/8</td>
<td>4.0.0, 4.0.1, 4.0.3, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5200/8 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5200/24</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5200/24 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5400</td>
<td>4.0.1-SBR, 4.0.1-SIBR, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5400 GPRS</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS5GT</td>
<td>4.0.0-DIAL2, 5.0, 5.1</td>
</tr>
<tr>
<td>NS5GT ADSL</td>
<td>5.0.0r6, 5.0.0-1483, 5.1</td>
</tr>
<tr>
<td>NS-HSC</td>
<td>5.0 only</td>
</tr>
<tr>
<td>NS-ISG-2000</td>
<td>5.0 only, 5.1</td>
</tr>
</tbody>
</table>

You need to enable each FW/VPN device to communicate and work with NetScreen-Security Manager. Refer to the ScreenOS 5.1 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 NetScreen-Security Manager management system. From NetScreen-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 device configuration and security policies you define in NetScreen-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 NetScreen-Security Manager establishes communication between the UI, 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 — four inbound TCP ports supporting connection requests from existing FW/VPN devices and two 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 NetScreen-Security Manager UI(s) and Device Server. Used to establish communication session with Device Server and/or NetScreen-Security Manager UI(s). 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.
Using the Secure Server Protocol (SSP)

NetScreen-Security Manager uses the Secure Server Protocol (SSP) to provide secure communication between each management system component (i.e., GUI Server, Device Server, and UI), 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.

### Table 25: Device Server Communication Ports

<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 5+. Used to establish encrypted communication sessions with the GUI Server and FW/VPN devices (running ScreenOS 5+).</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 4.0.x. <strong>These sessions are not encrypted.</strong> 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 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>These sessions are not encrypted.</strong> 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 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>These sessions are not encrypted.</strong> 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 4.0.x. Used to establish communication session with FW/VPN devices running ScreenOS 4.0.x. <strong>While SSH sessions are encrypted, Telnet sessions are not encrypted.</strong> To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections. If your devices are running with ScreenOS 4.0.x, then use a SSH connection.</td>
</tr>
</tbody>
</table>

**Using the Secure Server Protocol (SSP)**

NetScreen-Security Manager uses the Secure Server Protocol (SSP) to provide secure communication between each management system component (i.e., GUI Server, Device Server, and UI), 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.
Communications With Devices Running ScreenOS 5.0+

If you are deploying NetScreen-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 NetScreen-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 permit TCP port 7801.

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

Table 26: Management System Communications With Devices Running ScreenOS 5.x

<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 devices running ScreenOS 5.0.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>Inbound TCP: 7801</td>
<td>Accepts communication from the Device Server and UI.</td>
</tr>
</tbody>
</table>

**NOTE:** The Device Server can use port 22 (SSH) to do a first connect to devices running ScreenOS 5.0, enabling you to set the NetScreen-Security Manager agent. The agent enables the device to communicate back to the Device Server using 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 use the same communication protocols for communicating with NetScreen-Security Manager that were supported with Juniper Networks NetScreen-Global PRO:

- Device configuration is performed via telnet or SSH1.
- Logging information is sent over the Juniper Networks 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 (TCP port 15400, Telnet port 23, and 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 NetScreen-Security Manager and ScreenOS 4.x and earlier devices.

**Table 27: Management System Communications With Devices Running ScreenOS 4.x and Earlier**

<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 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 15400</td>
<td>Management for FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound UDP: 69</td>
<td>tftp server for updating FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
<tr>
<td>Device Server</td>
<td>Inbound TCP: 11122</td>
<td>Accepts incoming NACN requests for FW/VPN devices running ScreenOS 4.0.x.</td>
</tr>
</tbody>
</table>

**Creating a Separate Management Network**

It is recommended you isolated the NetScreen-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 NetScreen-Security Manager in a network with FW/VPN devices running ScreenOS 5.0 and ScreenOS 4.0.x, then 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, then 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.
Index

A
adding, Device Server .................................................................................. 61

C
certificates
files .......................................................................................... 69, 90
transferring ........................................................................ 69, 90
changing
default user management system runs as ........................................ 151
configuration options
database backup ........................................................................ 17
high availability .................................................................................. 18–21
installing management system on same server (typical) .................. 16
installing management system on separate servers
(extended) ..................................................................................... 18
Statistical Report Server .................................................................... 17
configuring
Device Server data directory ................................................................ 33, 83
Device Server ID .................................................................................. 63
developed by user management system ........................................... 52, 77, 124
downgrading
from FP2 to FP1 ........................................................................ 162
disk storage
requirements on management system, same server .................. 14
downgrading
requirements on management system, separate servers ........... 14
downgrading
from FP2 to FP1 ........................................................................ 162
downgrading
requirements on management system, separate servers ........... 14
downgrading
from FP2 to FP1 ........................................................................ 162

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

downgrading
requirements on management system, same server .................. 14

downgrading
requirements on management system, separate servers ........... 14

CPU
requirements on management system, same server .................. 14
requirements on management system, separate servers ........... 14

customer support .................................................................................... 9

D
data directory
for Device Server, described .................................................. 25, 51, 75, 123
for GUI Server, described .................................................. 25, 51, 75, 123
database
backup options ........................................................................ 17
replicating ...................................................................................... 155
restoring ...................................................................................... 155
defining system parameters .................................................. 25, 51, 75, 123
Demo Mode ...................................................................................... 46
Device Server
adding .............................................................................................. 61
configuring manually ...................................................................... 150
data directory, configuring .................................................. 33, 83
installing .......................................................................................... 62–68
starting .......................................................................................... 147
stopping .......................................................................................... 148
Device Server ID
configuring ...................................................................................... 63
described ...................................................................................... 52, 77, 124
downgrading
X Server ...................................................................................... 27, 127
disk storage
requirements on management system, same server .................. 14
disk storage
requirements on management system, separate servers ........... 14
downgrading
from FP2 to FP1 ........................................................................ 162

E
establishing
SSH trust relationship .................................................................. 80
extended configuration option ..................................................... 18

G
GUI Server
installing .......................................................................................... 54–59
starting .......................................................................................... 147
stopping .......................................................................................... 148

H
HA Cluster
configuring .................................................................................... 100–103
HA Server
starting .......................................................................................... 147
stopping .......................................................................................... 148
heartbeat communications
described ...................................................................................... 20
heartbeat links
described ...................................................................................... 76
high availability
configuring manually ...................................................................... 154–156
installing .......................................................................................... 73–118
overview .......................................................................................... 18–21

I
installation
CD .................................................................................................. 13
files .................................................................................................. 13
log file for management system .................................................. 38, 59, 88, 137
log file for UI .................................................................................... 43
package ............................................................................................ 13
installing
configuration options .................................................................... 16
Device Server .................................................................................. 62–68

Index  ■  173
Index

L
log file
management system install..................................38, 137
UI installation....................................................43
logging in to the UI .............................................44
logs restoring......................................................153

M
management IP address
for GUI Server, described.................................25, 51, 75, 123
management system changing default user.............151
commands ........................................................146
installation process ...........................................12
installing on same server ...................................24–38
installing on separate servers ..........................50–69, 74–90
restarting .........................................................146
starting ..........................................................147
status ..............................................................147
stopping ..........................................................147
uninstalling ......................................................163
upgrading ........................................................122–137
memory requirements
for UI..................................................................15
management system on same server....................14
management system on separate servers .............14
minimum system requirements
described ..........................................................14–15
for UI ..............................................................15
management system ..........................................14–15

N
network connection
requirements for UI ..............................................15
requirements on management system, same server 14
requirements on management system, separate servers 14

O
operating system
requirements for management system...................14
requirements for UI .............................................15

P
password
super user, configuring ........................................34, 84

R
replicating
database ...........................................................155
restoring
database ...........................................................155
logs and configuration data ................................153
root user changing user that management system runs as........151
rsync using with database backup .........................17
running
UI ..................................................................44
UI, in Demo Mode .............................................47

S
SSH trust relationship
establishing .......................................................80
starting
Device Server ..................................................147
GUI Server ......................................................147
HA Server .......................................................147
management system manually ..........................147
Statistical Report Server
installing with NetScreen-Security Manager ...........17
stopping
Device Server ..................................................148
GUI Server ......................................................148
HA Server .......................................................148
management system manually ..........................147
Sun Solaris SSH daemon
patching ..........................................................29–30, 129–130
super user password, configuring .......................34
password, described .........................................25, 51, 75, 123
swap space requirements on management system, same server 14
requirements on management system, separate servers 14
system parameters ...........................................25, 51, 75, 123
system update utility described .............................13
running ..........................................................28–29, 128–129

T
testing
initial HA replication ........................................104
TFTP server


NetScreen-Security Manager 2004 FP3 Installer’s Guide
installing on Linux ................................................... 160
installing on Solaris ................................................. 161
typical configuration option ........................................ 16

U
UI
  installation process ..................................................... 12
  installing .............................................................. 40–43
  running .................................................................... 44
  uninstalling ............................................................. 164
  upgrading to FP1 ....................................................... 138
uninstalling
  UI ............................................................................ 164
upgrading
  management system ................................................. 122–137
  management system on separate servers ................ 139
  prerequisite steps ...................................................... 127
  UI ............................................................................ 138

V
validating
  database recovery ..................................................... 156
  management system installation ............................... 45
  management system status ...................................... 39, 68, 89, 137
  management system upgrade .................................. 138
viewing management system commands ..................... 146

X
X Server
  disabling ............................................................... 27, 127