



Juniper Networks
NetScreen-Security Manager 2006.1

Installer Guide

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

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

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

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

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

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

Disclaimer

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

Table of Contents

About This Guide	v
Audience.....	v
Conventions.....	v
User Interface Conventions	vi
Illustration Conventions.....	vii
Documentation.....	viii
NetScreen-Security Manager 2006.1 Installer Guide Overview	viii
Related NetScreen-Security Manager Documentation.....	viii
Web Access	ix
Comments About the Documentation	ix
Contacting Customer Support	x
Chapter 1 Introduction	1
Installation Process Overview	1
Management System Install Process.....	1
User Interface Install Process.....	2
Installation Package	2
Minimum System Requirements.....	3
System Requirements - Management System.....	3
System Requirements - User Interface.....	4
Installation Considerations.....	5
Configuration Options.....	6
Standalone Configuration	6
Local/Remote Database Backup	6
NetScreen-Statistical Report Server Interoperability	7
Device Server Database	7
Distributed Configuration	8
Simple High Availability Configuration	8
Extended High Availability Configuration	8
Next Steps.....	8
Chapter 2 Installing the Management System in a Standalone Configuration	11
Suggested Standalone Configuration Installation Order.....	11
Defining System Parameters.....	12
Prerequisite Steps	14
Running the System Update Utility.....	15
Patching the Sun Solaris SSH Daemon.....	16
Increasing Shared Memory Segment Maximum Size	17
Establishing a Trust Relationship	17
Installing the Management System Software.....	18
Typical Output for a Standalone Installation.....	22
Viewing the Management System Installation Log.....	25
Verifying the GUI Server Fingerprint.....	25
Starting Server Processes Manually	25
Validating Management System Status	26
Installing the User Interface	26
Viewing the User Interface Installation Log.....	29

	Running the User Interface.....	30
	Validating the NetScreen-Security Manager Installation.....	30
	Running the User Interface in Demo Mode.....	32
	Next Steps.....	32
Chapter 3	Installing the Management System in a Distributed Configuration	33
	Suggested Distributed Configuration Installation Order.....	33
	Defining System Parameters.....	34
	Prerequisites.....	36
	Installing the GUI Server.....	36
	Viewing the Installation Log.....	40
	Installing the User Interface.....	40
	Adding the Device Server.....	41
	Installing the Device Server.....	42
	Starting Server Processes Manually.....	44
	Validating Management System Status.....	45
	Transferring Certificate Files (optional).....	45
	Next Steps.....	45
Chapter 4	Installing the Management System with High Availability	47
	High Availability Overview.....	47
	HA Configuration Options.....	48
	HA Requirements.....	48
	Inter-Server Communications.....	48
	HA Server.....	49
	Data Synchronization.....	49
	HA Failover.....	51
	Restoring Connections.....	52
	Using a Shared Disk.....	52
	Creating a Trust Relationship Between Servers.....	52
	Server Authentication.....	53
	Changing Permissions for Data Synchronization.....	53
	Checking HA Status.....	54
	Viewing HA Error Logs.....	54
	High Availability Installation.....	54
	Suggested HA Installation Order.....	55
	Defining System Parameters.....	56
	Simple HA Configuration Parameters.....	56
	Extended HA Configuration Parameters.....	59
	Shared Disk Parameters.....	59
	Prerequisites.....	59
	Verifying that Shared Partitions are Mounted Properly.....	60
	Verifying that All Required System Binaries are Available.....	60
	Verifying that Clocks are Synchronized.....	60
	Establishing an SSH Trust Relationship.....	60
	Installing the Management System Software on the Primary Server.....	61
	Viewing the Management System Installation Log.....	66
	Starting Server Processes Manually.....	67
	Validating Management System Status.....	67
	Other Useful Commands.....	67
	Transferring Certificate Files (optional).....	68
	Installing the Management System Software on the Secondary Server.....	68
	Example: Installing the Management System in an HA Configuration.....	68

Primary GUI Server and Device Server Installation Script.....	69
Secondary GUI Server and Device Server Installation Script.....	73
Installing the User Interface	76
Configuring the HA Cluster	76
Testing the Initial HA Replication	80
Installing the Management System in an Extended HA Configuration.....	81
Example: Installing the Management System in an Extended HA Configuration.....	81
Next Steps.....	83
Chapter 5	Upgrading to 2006.1
	85
Upgrade Overview	85
Defining System Parameters.....	86
Standalone Configuration Parameters	86
Distributed Configuration Parameters.....	88
HA Configuration Parameters	88
Shared Disk Parameters	90
Prerequisite Steps	90
Running the System Update Utility	91
Patching the Sun Solaris SSH Daemon.....	92
Increasing Shared Memory Segment Maximum Size	93
Upgrading the Management System - Standalone Configuration.....	93
Starting Server Processes Manually	96
Validating Management System Status	96
Upgrading the User Interface	97
Validating the Upgrade	97
Post Upgrade Steps: Migrating Domain Version Data	98
Upgrading the Management System - Distributed Configuration	99
Upgrading the Management System With HA Enabled.....	99
Upgrading the Database Backup Files.....	101
In Case The Upgrade Fails.....	101
Next Steps.....	101
Chapter 6	Maintaining NetScreen-Security Manager
	103
Controlling the Management System	103
Viewing Management System Commands.....	103
Common Management System Commands.....	104
Starting All Server Processes Using the HA Server	104
Starting GUI Server and Device Server Processes Manually	105
Stopping Server Processes	105
Configuring Server Options.....	106
Changing the Management System IP Address.....	106
Changing the Device Server IP Address	107
Changing the GUI Server IP Address	107
Configuring Disk Space Management	108
Disk Space Management on the GUI Server	109
Configuring Connection Timing	109
Changing Permissions To a Normal User	110
Setting Core File Naming on Solaris.....	111
Archiving and Restoring Logs and Configuration Data	111
Restoring Logs and Configuration Data.....	113
Configuring High Availability Options	113
Enabling and Disabling High Availability Processes	113

Configuring High Availability Options	114
Running the Remote Replication Utility as a Non-Root User	115
Backing Up the Database Locally	115
Restoring the Database.....	115
Validating the Database Recovery Process.....	116
Changing the HA Server IP Address.....	116
Relocating the Database.....	116
Archiving the GUI Server Database and Device Server Log Database.....	116
Installing NetScreen-Security Manager On a New System	117
Moving the Databases to the New System	117
Installing a tftp Server	118
Installing a tftp Server on Linux.....	119
Installing a tftp Server on Solaris	119
Modifying the Bulk CLI Status Timeout Value	120
Downgrade Procedures.....	120
Removing the Management System.....	121
Uninstalling the User Interface	123

Appendix A Technical Overview A-1

Technical Overview	A-1
About the Management System.....	A-1
GUI Server.....	A-2
Device Server.....	A-2
HA Server.....	A-3
About the NetScreen-Security Manager User Interface (UI)	A-3
About Managed Security Devices.....	A-3
Server Communications	A-3
Communication Ports and Protocols	A-3
Using the Secure Server Protocol (SSP)	A-5
Communications With Devices Running ScreenOS 5.0 +	A-6
Communicating With Devices Running Screen 4.x and Earlier	A-6
Creating a Separate Management Network.....	A-8

Appendix B Hardware Sizing Recommendations B-1

Formulas and Guidelines	B-1
Standalone or Distributed System for GUI Server and Device Server	B-1
Configuring Multiple Network Interface Cards.....	B-1
Memory Requirements.....	B-2
GUI Server.....	B-2
Device Server.....	B-2
UI Client.....	B-3
Storage Space Requirements	B-3
GUI Server.....	B-3
Audit Log	B-3
Error Log.....	B-4
Device Configuration Database	B-4
Nightly Backup.....	B-4
Device Server Requirements	B-4
Processor Speed Requirements	B-5
GUI Server.....	B-5
Device Server.....	B-6
Device Server Managing IDP Standalone Devices Running Profiler ..	B-6
Recommendations for Large Scale Installations	B-6

Migration to NetScreen-Security Manager from NetScreen-Global PRO or NetScreen-Global PRO Express	B-7
--	-----

Appendix C	Profiler Performance Tuning Recommendations	C-1
	Performance Tuning Recommendations	C-1
	Recommendations for Low-End Configurations:	C-1
	Medium-Size Configuration (3-8 IDP profiling devices):	C-2
	High end configuration (9-20 IDP profiling devices):	C-2
	System Components for Improving Profiler Performance	C-3
	UI System Preferences	C-3
	PostgreSQL Server	C-4
	Operating System	C-5
	Device Server	C-5
	NSM Generated Logs Impact on Performance	C-6
	Index	IX-1

About This Guide

This *NetScreen-Security Manager 2006.1 Installer Guide* describes how you can install an initial working NetScreen-Security Manager (NSM) 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




Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates that you may risk losing data or damaging your hardware.
	Warning	Alerts you to the risk of personal injury.

Table 2: Text conventions (except for command syntax)

Convention	Description	Examples
Bold typeface	Represents commands and keywords in text.	<ul style="list-style-type: none"> ■ Command example: Issue the clock source command. ■ Keyword example: Specify the keyword exp-msg.

Table 2: Text conventions (except for command syntax)Table continued on next page

Convention	Description	Examples
Bold sans serif typeface	Represents text that the user must type.	user input
Key name in angle brackets	Indicates the name of a key on the keyboard.	Press <Enter> .
Key names linked with a plus sign (+) in angle brackets.	Indicates that you must press two or more keys simultaneously.	Press <Ctrl+B> .
Plain sans serif typeface	Represents information as displayed on your terminal's screen.	host1# show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)
<i>Italics</i>	<ul style="list-style-type: none"> ■ Emphasize words. ■ Identify variables. ■ Identify chapter, appendix, and book names. 	<ul style="list-style-type: none"> ■ There are two levels of access, <i>user</i> and <i>privileged</i>. ■ <i>clusterId</i>, <i>ipAddress</i>. ■ <i>Appendix A, System Specifications</i>.

Table 3: Syntax conventions

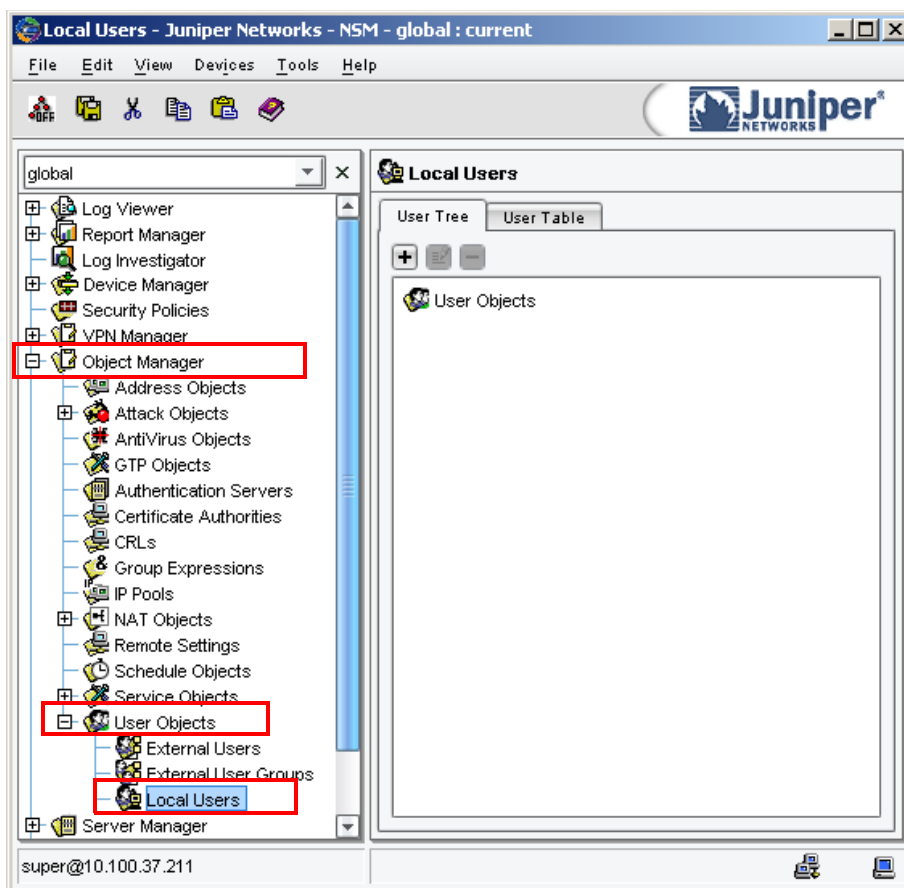
Convention	Description	Examples
Words in plain text	Represent keywords.	terminal length
Words in italics	Represent variables.	<i>mask</i> , <i>accessListName</i>
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic line
Words enclosed in [brackets]	Represent optional keywords or variables.	[internal external]
Words enclosed in [brackets]*	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
Words enclosed in { braces }	Represent required keywords or variables.	{ permit deny } { in out } { <i>clusterId</i> <i>ipAddress</i> }

User Interface Conventions

The sample screens used throughout this guide are representations of the screens you will see when you administer NetScreen-Security Manager.

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

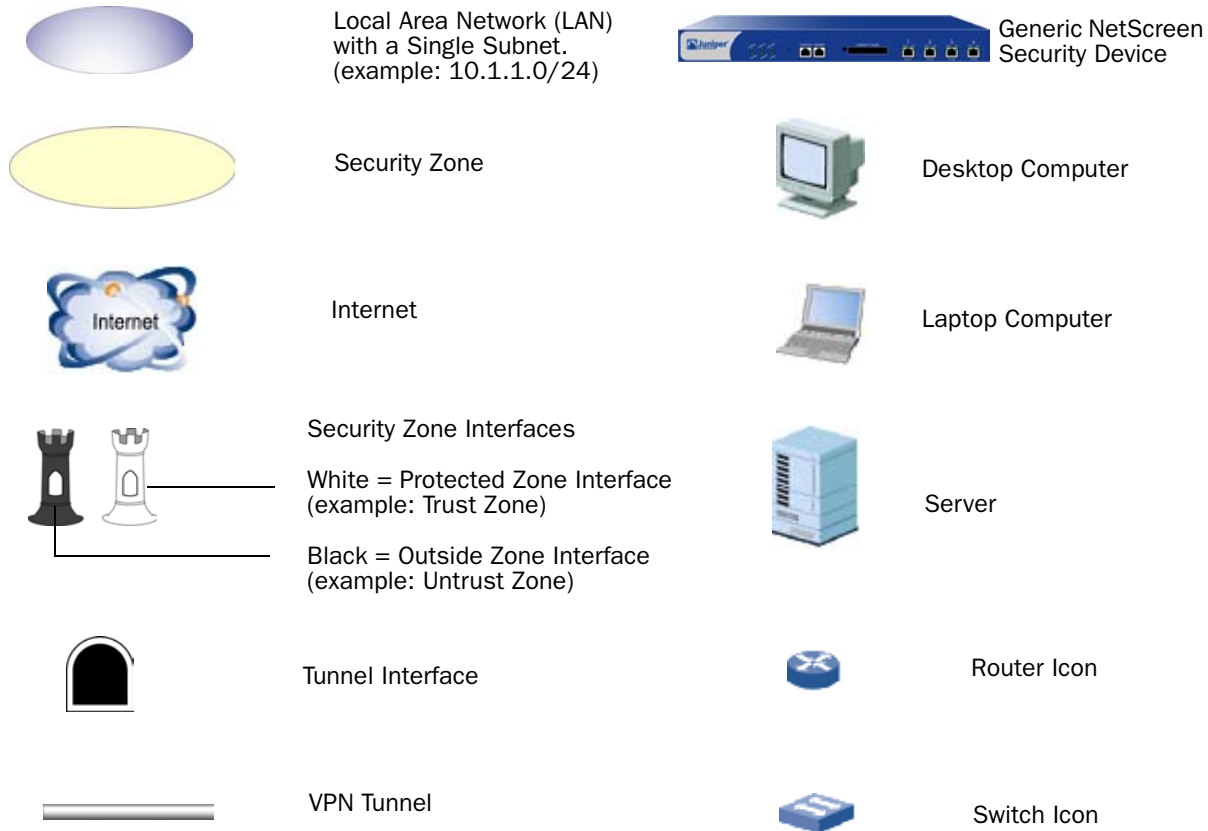


1. In the main navigation tree, select Object Manager. The Object Manager tree expands to reveal a subset of objects.
2. In the Object Manager navigation tree, select User Objects. The main display area displays all defined user objects.
3. In the User Objects navigation tree, select Local User Objects. 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



Documentation

This section describes documentation for NetScreen-Security Manager.

NetScreen-Security Manager 2006.1 Installer 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 2006.1.

Related NetScreen-Security Manager Documentation

The NetScreen-Security Manager 2006.1 documentation set includes the following guides:

NetScreen-Security Manager 2006.1 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 2006.1 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 2006.1 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 2006.1 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 2006.1 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 Internet. 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”
- “Installation Considerations”
- “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 3
- User Interface Install Process on page 4

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 “Technical Overview” on page 1 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 Enterprise Linux ES 3.0 or 4.0, or Red Hat Enterprise Linux AS** server that meets minimum system requirements. Refer to “Minimum System Requirements” on page 3 for more information on the

minimum required hardware and software that you need to install the NetScreen-Security Manager management system.

NOTE: NetScreen-Security Manager 2005.3 and later no longer supports installations on servers running Red Hat Linux 8 or 9. If you plan to install the management system on a server running Red Hat Linux 8 or 9, you must upgrade the system to Red Hat Enterprise Linux ES 3.0 or 4.0, or Red Hat Enterprise Linux AS.

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 3 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.

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.

Table 4 describes the contents of the NetScreen-Security Manager installation CD.

Table 4: NetScreen-Security Manager Installation Files

File Name	Description
nsm2006.1_ui_win_x86.exe	Installer for the NetScreen-Security Manager UI (for Windows-based computers).
nsm2006.1_ui_linux_x86.bin	Installer for the NetScreen-Security Manager UI (for Linux-based computers).
nsm2006.1_servers_linux_x86.sh	Installer for the NetScreen-Security Manager management system for Linux.
nsm2006.1_servers_sol_sparc.sh	Installer for the NetScreen-Security Manager management system for Solaris.
systemupdate-nsm-linux.tar	System update utility for Linux. You use this file to update files on your system required for the installer to run properly.
systemupdate-nsm-solaris.tar	System update utility for Solaris. You use this file to update files on your system required for the installer to run properly.

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

Table 5 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

Component	Minimum Requirements
Operating System	Solaris 8, Solaris 9 operating system, OR Red Hat Enterprise Linux (ES/AS) 3.0-Update 5 or 4.0-Update 1 NOTE: No later versions of RHEL are supported. If you are running NetScreen-Security Manager on Linux, you must install one of these versions.
CPU	Sun Microsystems UltraSPARC III 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)
RAM	1GB (or higher); 2GB + (depending on the number of managed devices and configuration size)
Swap Space	4 GB for both GUI Server and Device Server
Storage	IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)
Network Connection	100Mbps NIC Ethernet adapter
Other	Server must be dedicated to running NetScreen-Security Manager. Install NetScreen-Security Manager on a physical system rather than a virtual system such as VMWare, Microsoft VM Server etc.

Table 6 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

Component	Minimum Requirements
Operating System	Solaris 8, Solaris 9 operating system, OR Red Hat Enterprise Linux (ES/AS) 3.0-Update 5 or 4.0-Update 1 NOTE: No later versions of RHEL are supported. If you are running NetScreen-Security Manager on Linux, you must install one of these versions. 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.
CPU	Sun Microsystems UltraSPARC Ili 500MHz (or higher), OR Linux 1GHz (x86) processor (or higher)
RAM	512MB* (or higher); 1GB (recommended) *512MB for small deployments that are not managing IDP Sensors or ISG running IDP
Swap Space	2 GB for the GUI Server, 2 GB for the Device Server
Storage	IDE Hard Disk Drive with 10K rpm (minimum); 15K rpm (recommended); 18 GB disk space (minimum); 40 GB disk space (recommended)
Network Connection	100MBps NIC Ethernet adapter
Device Connection	19200 bits per second (minimum)
I/O	Split backplane (recommended for Device Server)
Other	Each server must be dedicated to running NetScreen-Security Manager. Install NetScreen-Security Manager on a physical system rather than a virtual system such as VMWare, Microsoft VM Server etc.

NOTE: You can extend system performance and data capacity by expanding the minimum requirements specified for each component. Refer to “Recommendations for Large Scale Installations” on page 6 for more information about the hardware and software appropriate for your specific network.

System Requirements - User Interface

Table 7 describes the minimum system requirements that must be met for the User Interface:

Table 7: Minimum System Requirements - User Interface

Component	Minimum Requirement
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 Enterprise Linux ES 3.0 or 4.0, 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.

Installation Considerations

The NetScreen-Security Manager management system is designed to scale from the management of a few devices to huge networks of up to 6000 devices. For the smaller customer, you can install the entire system on a single Linux or Solaris server. For large customers, you can install the NetScreen-Security Manager management system on four servers which makes use of external shared disk systems. There are two main factors to consider when making the decision as to what combination to implement:

- Scale - for example, how much server resource is needed to cope with the firewall network. This influences the decision to have the GUI Server and Device Server on separate machines.
- Failure Tolerance - the effect on the organization upon failure of a NetScreen-Security Manager component and the downtime during repair. This influences the decision to have either one or two management systems.

Some of the factors to consider include but are not limited to:

- Number of devices managed
- Size of devices managed (i.e. 10xNS5200 may have a larger impact compared to 100xNS5GT)
- Impact on the organization to temporary loss of logs during server failure (if not using multiple Device Servers the logs from firewalls would be lost until the single server is repaired)
- Amount of log data stored (this is a combination of the number of logs per day sent from the devices and the number of days the logs are required to remain on the management system)
- Customer's Linux/Solaris knowledge/skills

- Industry regulations governing the customer that might dictate the efforts they must go to in order to protect continuous log collection
- Main reason for using NetScreen-Security Manager (i.e., firewall configuration only with occasional logging, heavy logging...)
- Budget
- Future expansion of firewall network (future proofing)

For more information on Juniper Networks recommended hardware for various types of networks refer to “Recommendations for Large Scale Installations” on page 6.

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:

- Standalone Configuration on page 6
- Distributed Configuration on page 8
- Simple High Availability Configuration on page 8
- Extended High Availability Configuration on page 8

Standalone 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 small firewall networks (recommended for no more than 100 devices, considerably less for networks containing large firewalls. It has the advantage of low cost and simplicity. Local backup for disaster recovery and external data storage are options for this configuration.

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 IP Address of the remote machine

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

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 to 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.

Device Server Database

The installer also script prompts you to configure the additional parameters enabling the management system to work with a PostgreSQL Database used for the Device Server. This database stores data related to the Profiler in NetScreen-Security Manager. You must specify a port number, super username and password. By default, the PostgreSQL Database uses port 5432; the super user is “netscreen”.

Distributed 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. This system would be used for larger networks. The distributed system enables greater processing power per service. In addition a failure of the GUI Server would not result in the loss of log information as the Device Server can continue to communicate with firewalls. You can also tailor the choice of hardware to the needs of each service (typically large RAM for GUI Server and large disk capacity for the Device Server).

Simple 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 unplanned server outages.

To implement the management system for high availability, you need to install two physical servers: 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. Upon the failure of any service on the primary server (or a hardware fault which results in the same effect) would cause both the GUI Server and Device Server to failover to the standby server. The added benefit is automatic recovery of management service resulting in fewer lost firewall logs and reduced administrative down time. Note that the device logs would not be replicated to the peer server (only the config database).

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.

Extended High Availability Configuration

This is the most expensive and complex configuration but has the greatest protection against component failure. A failure of the primary Device Server would cause failover to the standby Device Server. This new Device Server would attempt connection with the primary GUI Server. Failure of a GUI Server would also cause failover to the standby GUI Server. The current Device Server would attempt to connect to the standby GUI Server after a timeout period. In this configuration the failure of a single component has minimal impact on the system as a whole. In addition the distributed system gives each service more system resource.

For more information about installing the management system for high availability, refer to “High Availability Overview” on page 47.

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, scalability, and high availability.

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 four main options for configuring the management system depending upon the size and requirements of your specific network: Standalone, Distributed, or Simple HA or Extended HA configuration.

- Refer to *Chapter 2, Installing the Management System in a Standalone Configuration* for specific information describing how to install and run the management system on the same server.
- Refer to *Chapter 3, Installing the Management System in a Distributed 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 for *Chapter 5, Upgrading to 2006.1* for specific information describing how to upgrade previous installations of NetScreen-Security Manager to this version.
- 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 the Management System in a Standalone Configuration

In This Chapter:

- “Suggested Standalone Configuration Installation Order”
- “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.

Suggested Standalone Configuration Installation Order

summarizes the process for installing NetScreen-Security Manager for most typical cases.

Table 8: Installation Process for Standalone Configuration

Step	Description/Estimated Time to Complete
1	Define system parameters that you need to provide during the installation process.
2	Perform prerequisite steps.
3	Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site.
4	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)

* If you are installing the GUI Server and Device Server on separate systems, refer to *Chapter 3, Installing the Management System in a Distributed Configuration* for more information.

Step	Description/Estimated Time to Complete
5	Install the User Interface.
6	Launch the User Interface, then connect it to the management system.
7	Validate that you have successfully installed the management system and User Interface.

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.

Table 9 identifies the system parameters that you need to identify.

Table 9: Common System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>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.</p> <p>By default, the Device Server stores data in:</p> <p><code>/var/netscreen/DevSvr/</code></p>	
GUI Server data directory	<p>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.</p> <p>By default, the GUI Server stores data in:</p> <p><code>/var/netscreen/GuiSvr/</code></p>	
GUI Server database log directory	<p>Directory location on the GUI Server where database logs are stored. Because the data on the GUI Server can grow to be very large, you may want to place this log data in another partition. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI Server stores data in:</p> <p><code>/var/netscreen/GuiSvr/xdB/Log</code></p>	
Management IP address	<p>The IP address used by the running GUI Server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
Initial “super” user password	<p>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.</p>	
Local database backup directory	<p>Directory location where local database backup data is stored.</p> <p>By default, the GUI Server stores local database backup data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable	<p>Path to the rsync utility executable.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Remote Backup Machine IP Address	<p>IP address of the machine where remote backups are sent.</p> <p>By default, the installer sets this to the IP address of the secondary HA Server.</p>	

Parameter	Description	Your Value
Hour of the Day to Start Local Database Backup	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 4:00am, type 04; if at 4:00pm, 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.	
Number of Local Database Backup Files Stored	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.	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 1800 seconds before timing out.	
Enable Logging	Enable logging related to local backup and HA.	
Device Server Database Parameters	Parameters required for the Postgres Database used for the Device Server. You must specify a port number, super username and password. By default, the Postgres Database uses port 5432; the super user is "netscreen".	

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. Log into 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, refer to "Changing Permissions To a Normal User" on page 110.

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 appendix on “Hardware Sizing Recommendations” on page 1 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 15 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 16 for more information.
6. If you are installing the management system on Solaris 8 or 9, it is highly recommended that you increase the maximum size of your shared memory segment. Refer to “Increasing Shared Memory Segment Maximum Size” on page 17 for more information.
7. 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 17 for more information.

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.

NOTE: The NetScreen-Security Manager 2005.3 system update utility is compatible with Red Hat Enterprise Linux 3.0 Update 5 and Red Hat Enterprise Linux 4.0 Update 1.

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.

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

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 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. Log into 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.

Increasing Shared Memory Segment Maximum Size

If you are installing the management system on Solaris, it is highly recommended that you increase the maximum size of your shared memory segment.

To increase the maximum size of shared memory:

1. Open the `/etc/system` file in any text editor.
2. Edit the OS kernel parameters by adding the following lines.

```
set shmsys:shminfo_shmmax=0x2000000
set shmsys:shminfo_shmmn=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmsl=32
```

3. Save the file.
4. Restart your system.

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
```

NOTE: If prompted to enter a passphrase, leave the value blank.

2. Run the following commands on the remote machine:

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

NOTE: If prompted to enter a passphrase, leave the value blank.

3. 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_keys
```

4. 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_keys
```

5. Test connectivity via SSH from the primary 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, 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 nsm2006.1_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2006.1_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 the correct version PostgreSQL database
- 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 script then prompts if this machine will participate in an HA cluster.
5. Type **n**, 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**, then press **< Enter >**. Refer to “Installing the Management System with High Availability” on page 47 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`.

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 over-writing any existing data. If you try to specify an existing directory, the installer indicates that an existing directory already exists, then prompts you to try again.

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`.

- c. Type the directory location for storing the database files for the GUI Server or press <Enter> to accept the default location
/var/netscreen/GuiSvr/xdb/1og.

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, then prompts you to try again.

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

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.
8. 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 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.
9. 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 log into the UI.

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

10. Type **n**, then press <Enter>, if you are not planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type **y**, 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.

11. Type **y**, 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 (2:00am).
- b. Type **n**, then press **< Enter >** to specify that you do not want daily backups to be sent to a remote machine. If you select **y**, 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 a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- e. Type **y** or **n** to enable logging.
- f. Designate a directory location for locally storing the management system database backup. Press **< Enter >** to accept the default location `/var/netscreen/dbbackup`.
- g. Type the full path where the rsync utility is located.

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

The script then prompts you to configure the Device Server database.

12. To configure the Device Server database:

- a. Enter a port number for the Device Server database.
- b. Enter a name for the database super user.
- c. Enter a password for the database super user. Enter the password again for verification.

The script then prompts you to start servers after installation is complete.

13. Type **y**, then press **< Enter >**, if you want to start the GUI and Device Servers after the installation has finished. Type **n**, then press **< Enter >**, if you do not want to start the servers.

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

14. Verify your settings, and if they are correct, type **y**, 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 security 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, then returns you to the command prompt.

Typical Output for a Standalone Installation

An example of the output for a typical standalone installation is as follows:

```
sh nsm2006.1_servers_linux_x86.sh
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 for PostgreSQL.....ok
Checking if user is root.....ok
Checking if user root exists.....ok
Checking if system meets RAM requirement.....ok
Checking for sufficient disk space.....ok
Checking if RPM binary is the minimum version .....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]> n
##### DEVICE SERVER SETUP DETAILS #####
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 #####
```

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 database data 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]>

The GUI Server stores all of the database logs under a single directory. By default, this directory is /var/netscreen/GuiSvr/xdb/log. Because the database log can grow to be quite large, it is sometimes desirable to place this log in another partition.

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

Enter database log directory location [/var/netscreen/GuiSvr/xdb/log]>

Enter the management IP address of this server []> 10.100.37.219

Setting GUI Server address and port to 10.100.37.219:7801 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

Will server processes need to be restarted automatically in case of a failure? (y/n) [y]>

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]>

Enter the rsync backup timeout [1800]>

Will logging be enabled? (y/n) [n]>

Enter database backup directory [/var/netscreen/dbbackup]>

The database backup server(s) requires that you have previously installed the rsync program.

Enter the full path to rsync [/usr/bin/rsync]>

DEVSVR DB SETUP DETAILS

Enter Postgres DevSvr Db port [5432]>

Enter Postgres DevSvr Db super user [netscreen]>

Enter Postgres DevSvr Db password for user 'netscreen'

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

Please enter again for verification

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

POST-INSTALLATION OPTIONS

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

CONFIRMATION

About to proceed with the following actions:

- Install Device Server
- Install GUI Server
- Install High Availability Server
- This machine does not participate in an HA cluster
- Store Device Server data in /var/netscreen/DevSvr
- Store GUI Server data in /var/netscreen/GuiSvr
- Store GUI Server database log in /var/netscreen/GuiSvr/xdb/log
- Use IP address 10.100.37.219 for management
- Connect to GUI Server at 10.100.37.219:7801
- Set password for 'super' user
- Servers will be restarted automatically in case of a failure
- 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
- HA rsync command backup timeout: 1800
- Logging is disabled: n
- Create database backup in /var/netscreen/dbbackup
- Use rsync program at /usr/bin/rsync
- Postgres DevSvr Db Server port: 5432
- Postgres DevSvr Db super user: netscreen
- Postgres DevSvr Db password set for 'netscreen'
- Start server(s) when finished: Yes
Are the above actions correct? (y/n)> y
##### EXTRACTING PAYLOADS #####
Extracting payload.....ok
Decompressing payload.....ok
##### PERFORMING INSTALLATION TASKS #####
----- INSTALLING Device Server -----
Looking for existing RPM package.....ok
Removing DevSvr files from default location.....ok
Installing Device Server RPM.....ok
Installing JRE.....ok
Creating var directory.....ok
Creating /var/netscreen/dbbackup.....ok
Putting NSROOT into start scripts.....ok
Filling in Device Server config file(s).....ok
Setting permissions for Device Server.....ok
Setting up PostgreSQL for DevSvr.....ok
Installation of Device Server complete.
----- INSTALLING GUI Server -----
Copying dbbackup data to the installer backup directory....ok
Looking for existing RPM package.....ok
Removing GuiSvr files from default location.....ok
Installing GUI Server RPM.....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
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 GUI Server start script.....ok
Enabling HA Server start script.....ok
##### PERFORMING POST-INSTALLATION TASKS #####
Running nacnCertGeneration.....ok
Removing staging directory.....ok
Starting GUI Server.....ok
Starting Device Server.....ok
Starting HA Server.....ok
NOTES:

```

- Installation log is stored in
`/usr/netscreen/DevSvr/var/errorLog/netmgtInstallLog.20051026152408`
- This is the GUI Server fingerprint:
`B4:F4:62:A1:DE:20:12:94:E7:47:31:93:2C:EC:BC:CA:FA:E4:36:02`
You will need this for verification purposes when logging into the GUI Server. Please make a note of it.
- If you are managing ScreenOS 4.x devices, you need to install the `tftp-server` RPM on this system. The TFTP server is used by the management server to update firmware images on 4.x devices. The root directory for the TFTP server must be set to `'/usr/netscreen/DevSvr/var/cache'`.

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 6:00pm, 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.

Verifying the GUI Server Fingerprint

After installing the management system, be sure to note the GUI Server fingerprint. Distribute this information to all Admins who plan to use the UI. Instruct your Admins to verify the fingerprint when using the UI to connect to the GUI Server for the first time. If the fingerprint is not valid, have them contact the appropriate staff to investigate the issue.

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 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” on page 103 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 “System Requirements - User Interface” on page 4 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. Log in as an Administrator user on the computer where you are installing the UI.

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

2. Download the UI installer from the 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.

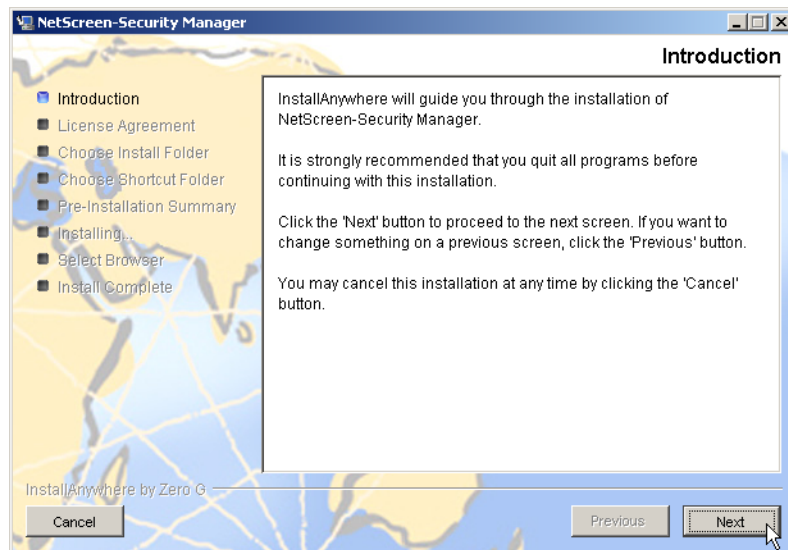
If you are installing the UI on a Linux-based computer, then launch it from a command line using the following command:

```
sh nsm2006.1_ui_linux_x86.bin
```

Alternatively, you can also run the following command:

```
chmod755 nsm2006.1_ui_linux_x86.bin  
./nsm2006.1_ui_linux_x86.bin
```

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, 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, 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.

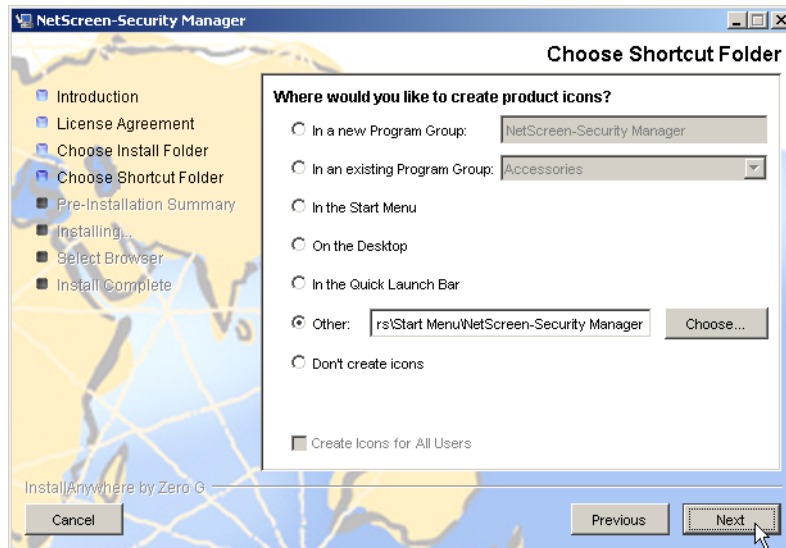


5. To accept the default install folder, click **Next**.

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.

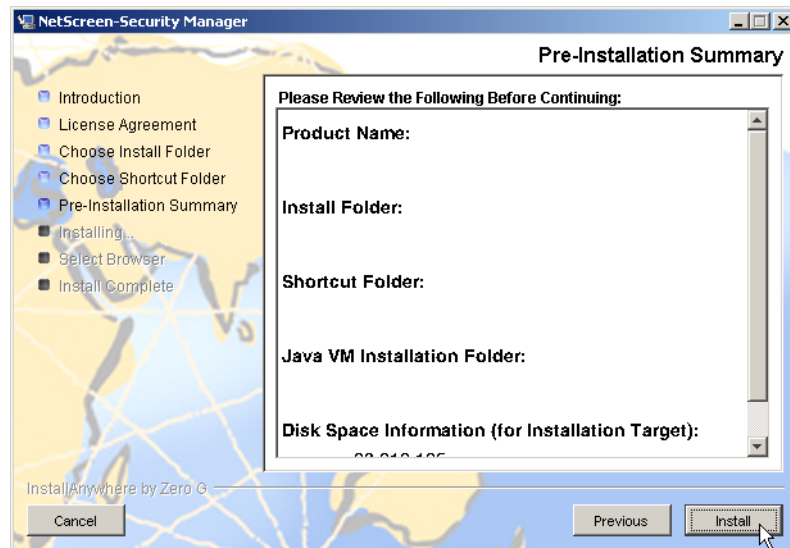
To specify a new or different folder location, click **Choose...** If you decide to accept the default install folder, then click **Restore Default Folder**.

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\\.nsm\`

For Linux-based computers:

`/<install_user_homedir>/.nsm/`

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

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

Running the User Interface

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, 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**.

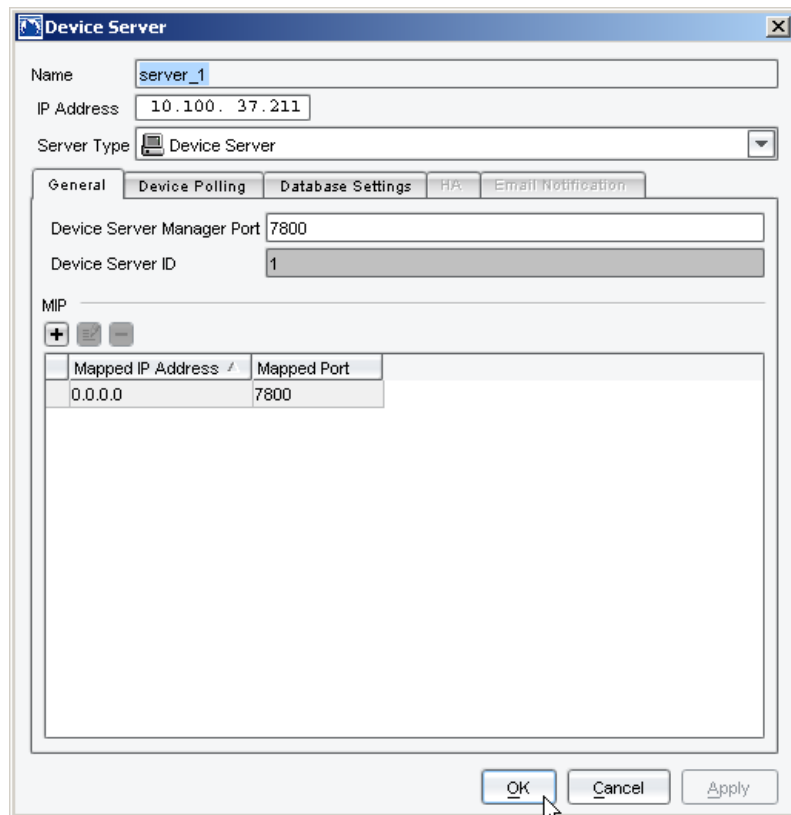
The UI appears indicating that the installation was successful.

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, 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 security 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 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 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 the Management System in a Distributed Configuration* for more information.

Chapter 3

Installing the Management System in a Distributed Configuration

In This Chapter:

- “Suggested Distributed Configuration Installation Order”
- “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.

Suggested Distributed Configuration Installation Order

Table 10 summarizes the process for installing the management system on separate servers.

Table 10: Installation Process for Distributed Configuration

Step	Description/Estimated Time to Complete
1	Define system parameters that you need to provide during the installation process.
2	Perform prerequisite steps.
3	Download the management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate web site.
4	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).
5	Install the User Interface.
6	Launch the User Interface, then connect it to the GUI Server. Add and configure the Device Server.
7	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).
8	Transfer certificate files from the server that you are installing the Device server to the server that you are installing the GUI Server.

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.

Table 11 identifies the system parameters that you need to identify.

Table 11: Distributed Configuration - System Parameters

Parameter	Description	Your Value
Device Server data directory	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: <code>/var/netscreen/DevSvr/</code>	
GUI Server data directory	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: <code>/var/netscreen/GuiSvr/</code>	
GUI Server database log directory	Directory location on the GUI Server where database logs are stored. Because the data on the GUI Server can grow to be very large, you may want to place this log data in another partition. 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: <code>/var/netscreen/GuiSvr/xdm/Log</code>	
Management IP address	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.	
Initial “super” user password	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.	
Local Database Backup directory	Directory location where local database backup data is stored. By default, the GUI Server stores local database backup data at: <code>/var/netscreen/dbbackup/</code>	
Path to the rsync utility executable	Path to the rsync utility executable. The default path is: <code>/usr/bin/rsync</code>	
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.	

Parameter	Description	Your Value
Hour of the Day to Start Local Database Backup	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 4:00am, type 04; if at 4:00pm, 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.	
Number of Local Database Backup Files Stored	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.	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 1800 seconds before timing out.	
Enable Logging	Enable logging related to local backup and HA.	
Device Server Database Parameters	Parameters required for the Postgres Database used for the Device Server. You must specify a port number, super username and password. By default, the Postgres Database uses port 5432; the super user is "netscreen".	
Device Server ID	Unique ID assigned when you add the Device Server.	
Password for GUI Server Connection	Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.	

Prerequisites

Perform the prerequisite steps described as if you were installing the management system on the same server. Refer to "Prerequisite Steps" on page 14 for more information.

Installing the GUI Server

The management system installer guides you through all the steps required to configure system parameters, 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 nsm2006.1_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2006.1_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 script then prompts if you want this machine to participate in an HA cluster.
 4. Type **n**, 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**, then press **< Enter >**. Refer to “High Availability Overview” on page 47 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 **< Enter >** to accept the default location `/var/netscreen/GuiSvr`.

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, then prompts you to try again.

- b. Type the directory location for storing the database files for the GUI Server or press <Enter> to accept the default location
/var/netscreen/GuiSvr/xdb/1og.

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, then prompts you to try again.

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

- c. 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 **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.

- 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 log into the system.

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

6. Type **n**, then press <Enter>, if you are not planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type **y**, 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 to restart the server processes automatically in case of a failure.

7. Type **y**, then press <Enter> if you want the server processes to be restarted automatically in case of failure. Type **n**, 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**, 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 (2:00am).
 - b. Type **n**, then press **< Enter >** so daily backups are not sent to a remote machine. If you select **y**, 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. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
 - e. Type **y** or **n** to enable logging.
 - f. Designate a directory location for locally storing the management system database backup. Press **< Enter >** to accept the default location `/var/netscreen/dbbackup`.
 - g. Type the full path where the rsync utility is located.

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

The script then prompts you to configure the Device Server database.

9. To configure the Device Server database:
 - a. Enter a port number for the Device Server database.
 - b. Enter a name for the database super user.
 - c. Enter a password for the database super user. Enter the password again for verification.

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

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

NOTE: When you restart your server, the GUI Server and HA Server processes start automatically.

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

11. Verify your settings, and if they are correct, type **y**, 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, 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 6:00pm, 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” on page 26 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 security 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 nsm2006.1_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2006.1_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 script then prompts you to specify if you want the machine to have HA cluster enabled.
4. Type **n**, 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**, then press **<Enter>**. Refer to “High Availability Overview” on page 47 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`.

The script then prompts you to enter parameters assigned by the UI to this Device Server.

- b. Type the Device Server ID. The script then prompts you to type the one time password for this Device Server.

- c. Type the One-Time Password for GUI Server connection. The One-Time Password must be a minimum of 8 characters.
 - d. 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.
 - e. Type the IP address of the running GUI Server.
 - f. 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 **y**, then press <Enter> if you want the server processes to be restarted automatically in case of failure. Type **n**, 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 **y**, then press <Enter> if you want the Device Server to perform a backup of the database locally. Type **n**, 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 (2:00am).
- b. Type **n**, then press <Enter> so daily backups are not sent to a remote machine. If you select **y**, 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. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- e. Type **y** or **n** to enable logging.

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

The script then prompts you to configure the Device Server database.

8. To configure the Device Server database:
 - a. Enter a port number for the Device Server database.
 - b. Enter a name for the database super user.
 - c. Enter a password for the database super user. Enter the password again for verification.

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

9. Type **y**, then press <Enter> to start the Device Server after the installer has completed the installation process. Type **n**, 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.

10. Verify your settings, and if they are correct, type **y**, then press <Enter> to proceed. If you type **n**, 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 security devices running ScreenOS versions 4.0.x appears. Refer to “Installing a tftp Server” on page 118 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
- Performs post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and security devices running ScreenOS 4.0.X (using NACN), removing the staging directory, and starting up the Device Server and HA Server.

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 103 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 security 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:

```
cacertificate_table.nml  
cr1_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 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 Online Help* for more task-specific information.

Chapter 4

Installing the Management System with High Availability

In This Chapter:

- “High Availability Overview”
- “High Availability Installation”
- “Suggested HA Installation Order”
- “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 HA Configuration”
- “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.

High Availability Overview

NetScreen-Security Manager 2006.1 enables you to install the management system and configure it for high availability. This configuration option involves installing two physical servers:

- 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.

HA Configuration Options

The management system can contain either a single Device Server or a Device Server Cluster (two Device Servers). It can also contain either a single GUI Server or GUI Server cluster. One combination that is not possible is the GUI Server and Device Server residing on the same machine with a single Device Server on standby. This is because the failure of the primary Device Server causes a shutdown of the primary GUI Server leaving only the standby Device Server running.

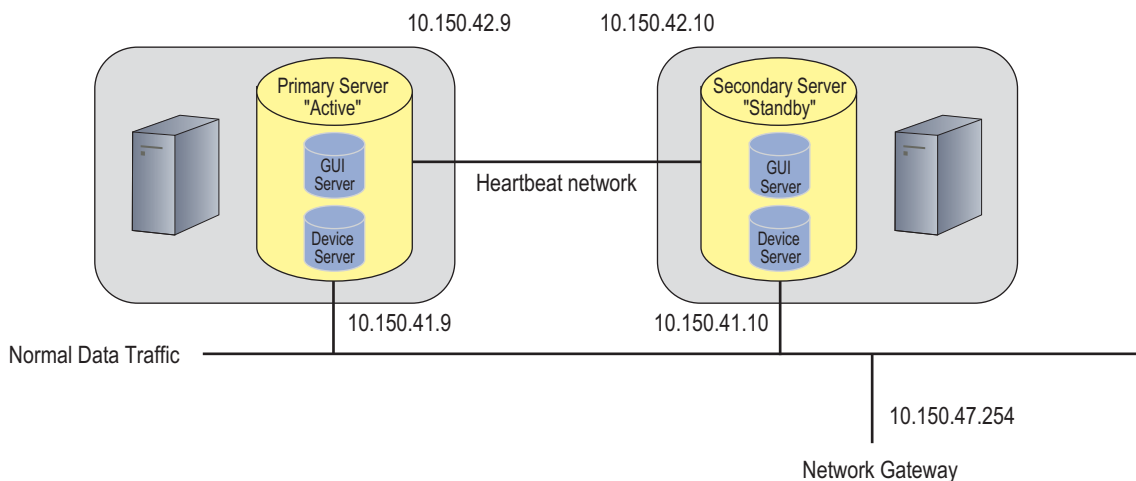
HA Requirements

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 servers can be geographically separate.

Figure 3 depicts the physical setup of the primary and secondary management systems:

Figure 3: Typical HA Management System Configuration



Inter-Server Communications

Communications from your security devices to the Device Server, Device Server to the GUI Server and GUI Server to NetScreen-Security Manager UI clients are all TCP based and make use of Juniper's proprietary SSP (Secure Server Protocol). This ensures that both AES encryption and certificate-based authentication is used throughout. There are some exceptions to this:

- management of security devices running ScreenOS 4.x and earlier
- certificate loading onto security devices running ScreenOS 5.0

- initial setup of all security devices to configure parameters on NetScreen-Security Manager using either Telnet or SSH

The system is designed in a tree structure. After installation, the security device always initiates the TCP session to the running Device Server on port 7800. The Device Server always initiates the TCP connection to the GUI Server on port 7801. The UI client works slightly differently. It attempts connection to the primary GUI Server using TCP port 7801. Upon failure, the UI automatically attempts to connect to the secondary GUI Server. This process is transparent to the Admin user. You may note however, that the IP address of the secondary GUI Server now appears in the bottom left of the main UI window, and in the Server Monitor.

In addition to the 78xx SSP connections, the Device Servers may require the use of legacy NetScreen-Global PRO protocols if communicating with security devices running ScreenOS 4.x and earlier (e.g. TCP 15400 & 11122). You will also see the use of UDP port 7802, which is used between servers of the same type to transmit heartbeat messages.

For more information on the communications between the components in your NetScreen-Security Manager system, refer to “Server Communications” on page 3.

HA Server

Each physical machine that is part of a cluster contains an additional service called the HA Server (HaSvr). The HA Server controls and detects failures in both the GUI Server and Device Server services (starts and stops services), as well as the inter-server data synchronization process. If you have installed the Device Server and GUI Server on a single server, one HA Server controls all services.

Data Synchronization

During normal HA operations, data is synchronized between the primary server and secondary server when they are in a cluster configuration. The HA Server controls this synchronization process. The HA Server makes use of rsync, a utility supplied by the operating system, to transfer files in each server’s data directory (`/var/netscreen` by default).

NOTE: During the installation process, you are required to provide the location of the rsync utility executable.

Objects such as PKI info and configuration data for the Device Server are synchronized. This allows the secondary Device Server to have the information it needs to accept connections from security devices and to create SSP connections to the GUI Server. Without the synchronization process, the secondary Device Server would not have the same private key as the primary (in this case, if it attempts a connection to the GUI Server, the SSP connection would be refused). This fact is important as it shows that a successful synchronization process must take place at least once after installation before the secondary Device Server can take over. A failover before the first synchronization (or before the first successful connection to the GUI Server) may cause serious problems. After the installation process, you must check that this has occurred.

Some directories are excluded from the synchronization process. For example, the directory on the Device Server where log data is stored is excluded because of the

potentially large size of your device log data, The complete list of directories that are excluded from the data synchronization process are listed in a text file called:

```
/usr/netscreen/HaSvr/var/exclude.rsnc
```

NOTE: There are no restrictions preventing you from editing this file to include the log directory. This is however, not at all recommended. 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.

The time it takes to complete each data synchronization process depends on the size of each data directory. If the number of security devices is not large, then the amount of data stored in the /var/netscreen/GuiSvr directory is small enough to be actively synchronized. This means that the rsync process can incrementally back it up on a regular basis. Conversely, if the number of security devices is large, or if the configurations on the few security devices are very large, then the rsync process will take a long time to complete and will use up system resources while doing so.

NOTE: The period between each data synchronization process is configurable within each server configuration file.

It is also important to note that during the synchronization process, the UI database is locked. During this time, you will not be able to access the database.

NOTE: if an Admin is currently logged in during the synchronization process, the UI saves all changes made during this time in cache. The UI then prompts the Admin to save or cancel these changes. If the Admin chooses to save changes, these are posted to the database when the synchronization process finishes.

If the synchronization process requires an extended period of time, the start of the next synchronization process may lock all Admins out for a period of time that may be considered unacceptable. In this case, it is recommended that you make use of a shared disk. In a four server, extended HA configuration, it is highly recommended that you make use of a shared disk for the Device Server data.

NOTE: Rsync utilizes a temporary SSH connection to the peer server to perform the incremental backups. If you are observing the open ports during the process, you will notice that there are two SSH connections open for the time it takes to complete the backup.

The data synchronization process is separate from the failover process. The HA Server does not consider a failed data sync to be reason to failover. This prevents failing over to a standby server that does not have all the information it requires.

Backup files are placed in the following directory (by default):

```
/var/netscreen/dbBackup/ha
```

These files remain unused on the standby server until failover occurs.

HA Failover

During normal operations, both the primary and secondary management systems monitor the health of the other using a series of heartbeat communications. The HA Server sends heartbeat messages over the UDP 7802 channel between itself and its peer. It also pings an external device (normally the IP address of the network gateway) that you configure during installation. This is in addition to monitoring the services running on itself. Based on information the HA Server gathers itself and peer, it starts or stops all the services that reside on that machine.

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 HA Server stops all services, and inform its peer of the problem. The peer HA Server then starts all its services. 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 Server1 are shutdown; and both the secondary GUI Server and Device Server on Server 2 start up.

NOTE: 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.

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 Server.

NOTE: It is very important that you do not start or stop the Device Server and GUI Server processes manually. The HA Server should always control these services.

During failover, a comparison is done of the time the backup occurred and the timestamp of the working files. Assuming that the backup file is newer, it is copied to the working directory (i.e., /var/netscreen/DevSvr in the case of the Device Server). It is because of this part of the process that you need to ensure that the two servers have their clocks in sync.

After the copy process is complete the HA Server starts the Device Server and GUI Server processes. It is important to recognize the order of events and the time they

occur. In the case where backup data is large, the entire failover process can take several minutes (e.g. if the GUI Server is managing 2000 devices, and there is a large amount of audit log data, all this might need to be copied to the working directory before services are started). During this time, logs may be lost in the case of a Device Server failover.

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.

The Device Server receives SSP and Global PRO DC connections from each security device it manages. All managed security devices are configured with both primary and secondary Device Server IP addresses. During failover, the device connection with the primary Device Server will time out. The security device will retry the connection, then attempt connection to the secondary Device Server.

The Device Server also has a connection to the active GUI Server. Like the security devices in your network, the Device Server is configured with the primary and secondary IP address of the GUI Server. Whenever a Device Server starts it will try to connect to the primary GUI Server, then to the secondary, then back to the primary until it is successful.

Using a Shared Disk

On systems which contain a Device Server cluster, it is strongly recommended that you use a shared disk (although this is not a minimum requirement). This is an additional server, often optimized for data storage. Since the management system refers to this store simply as a path (specified during installation) the mechanism of communication to the store (e.g. NFS relationship, SAN driver) and the type of media used is not relevant. It is also recommended that you create and test the shared disk prior to installation.

It should be noted that if an additional server is used as the shared data storage, a single point of failure is introduced. If you are using a shared disk setup, you need to ensure sufficient redundancy within the shared disk machine (e.g. RAID, dual power supplies...).

Creating a Trust Relationship Between Servers

Rsync is run automatically by the HA Server and should not require any manual interaction. Under normal circumstances when connecting via SSH to a server, you are required to authenticate. The need for authentication is obfuscated by creating a trust relationship between the two servers. You do this by creating a public/private RSA key on each server and copying the public key to the peer. For more information, refer to “Establishing an SSH Trust Relationship” on page 60.

It is highly recommended that you test the successful completion of this part of the installation process by attempting to SSH to the peer server.

Server Authentication

Communication between the Device Server and GUI Server uses a proprietary TCP based protocol called SSP. This uses AES encryption and is similar to an IPSEC VPN tunnel. The authentication is achieved via certificates. Each side of the SSP tunnel has a private and public key. The public keys are exchanged during the first time the Device Server connects to the GUI Server. This initial connection makes use of a OTP (one time password) which is configured on both Device Server and GUI Server during installation.

The GUI Server populates its shadow table with a single public key from the first Device Server that connects to it. Therefore it is essential that you allow the primary Device Server to connect to the primary GUI Server before failover occurs. After this, an HA Server data synchronization occurs. This transfers the Device Server configuration file (i.e., `devSvr.cfg`) and `shadow_table.nml` files to their appropriate peers. From that point on, each connection from either Device Server to GUI Server will make use of a single set of public/private keys. Failure to follow this order will result in the secondary Device Server not having the correct key information to connect to the running GUI Server.

You can view the GUI Server public key in the Device Server configuration file (i.e., `/var/netscreen/DevSvr/devSvr.cfg`). You can also view the Device Server key in the bottom half of the following file:

```
/var/netscreen/GuiSvr/shadow_table.nml
```

NOTE: You can also view the OTP in these two files.

You can view the certificate information in the Device Server certDB directory located at:

```
/usr/netscreen/DevSvr/var/certDB/
```

If the connection fails, check the contents of each of these files.

Changing Permissions for Data Synchronization

The HA Server process itself must run as root. You cannot modify the HA Server user. You can however, run the synchronization between peer servers (using `rsync`) as the “nsm” user. The following script is provided to do this manually:

```
/usr/netscreen/HaSvr/utlils/setRsyncUser
```

For more information on changing permissions, open and view the following file:

```
/usr/netscreen/HaSvr/utlils/README.remote.replication.as.nonroot
```

After running the script, the HA Server process continues to run as root but the `rsync` process runs as the “nsm” user. Separate scripts exist for GUI Server and Device Server permissions (found in the respective `/utlils` directories). For more information, refer to “Changing Permissions To a Normal User” on page 110.

Checking HA Status

It is possible to get an accurate report on the state of the HA Server and its state using the following script:

```
/usr/netscreen/HaSvr/utlils/haStatus
```

An example of the output is provided below.

```
[root@NSM1 utlils]# ./haStatus

=====
H/A process status
=====
Retrieving status...
highAvail (pid 1681).....ON
highAvailSvr (pids 2161).....ON
=====
State of the local and peer H/A server
=====
Local Server:
  192.168.0.152 running network-up      db-repl:in-sync
Peer Server:
  0.0.0.0      timed-out(error)      network-down  db-repl:n/a
```

You can view the same information by opening the following text file:

```
/usr/netscreen/HaSvr/var/HaStatus.txt
```

Viewing HA Error Logs

You can also view error logs generated by the HA Server by opening the following file:

```
/usr/netscreen/HaSvr/var/errorLog
```

If the HA Server is in error mode, the script appends log messages from the /HaSvr/var/errorLog/highAvail.0 error log. You can use this script view error messages output for the server that the script is run in real time. If there is a problem preventing the status from being transmitted, observing the state from the UI only can be misleading.

High Availability Installation

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

- Installing the Management System - Simple Configuration With HA on page 52 - 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 53 - 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.

Suggested HA Installation Order

Table 12 summarizes the process for installing the management system to provide for high availability. In general, it is recommended that you install your primary servers first, test that they work properly, then install the secondary servers. The order in which the four servers is installed is critical to the success. In an Extended HA configuration (i.e., with four servers), the most important step is to ensure that the PKI information is shared correctly between the servers. A failure to do this step correctly may result in the Device Server-GUI Server connection failing.

Table 12: Suggested HA Configuration Installation Process

Step	Description
1	Define system parameters that you need to provide during the installation process.
2	Perform prerequisite steps.
3	Install the primary GUI Server. Install the primary Device Server.
4	Install the User Interface. Log into the primary GUI Server and test that the primary management system is installed and working properly.
5	Install the secondary Device Server. Test that a successful remote replication occurs. You can do this by checking that files are located in the secondary server's /var/netscreen/dbbackup directory). It is vital that the secondary Device Server remains the standby until after the first remote replication occurs. Failure to achieve this will result in the secondary Device Server using its own PKI information rather than that supplied by the primary Device Server. If this occurs, it will not have the correct private key to enable the SSP connection.
6	Allow the primary Device Server to failover. You can do this by stopping the primary DevSvr services or rebooting. This process may take several minutes because of the time taken to acknowledge failure, copy files from backup to active directories, then start the Device Server services. Use "tail -f " on the secondary server's HaSvr error log to view the progress.
7	Use the UI to test connectivity between secondary Device Server and the primary GUI Server.
8	Install the secondary GUI Server.
9	Test that a successful remote replication occurs. You can do this by checking that files are located in the secondary server's /var/netscreen/dbbackup directory. Again, it is important not to failover before a remote replication is successfully completed.
10	Allow the primary GUI Server to failover.
11	Restart the UI and verify the connection between the GUI Server and Device Server.
12	Allow the primary Device Server to failover to test that it can connect to the secondary GUI Server.
13	Add your security devices in the UI. Check the device connection to both Device Servers.

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.

Simple HA Configuration Parameters

Table 13 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 13: Simple HA Configuration - System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>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.</p> <p>By default, the Device Server stores data in:</p> <p><code>/var/netscreen/DevSvr/</code></p>	
GUI Server data directory	<p>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.</p> <p>By default, the GUI Server stores data in:</p> <p><code>/var/netscreen/GuiSvr/</code></p>	
GUI Server database log directory	<p>Directory location on the GUI Server where database logs are stored. Because the data on the GUI Server can grow to be very large, you may want to place this log data in another partition. If you decide to have data stored in an alternative location, then specify the new location during the install process.</p> <p>By default, the GUI Server stores data in:</p> <p><code>/var/netscreen/GuiSvr/xdm/Log</code></p>	
Management IP address	<p>The IP address and port used by the running GUI Server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
Initial “super” user password	<p>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.</p>	
Primary HA Server IP address	<p>IP address of the primary server participating in the HA cluster.</p>	
Secondary HA Server IP address	<p>IP address of the secondary server participating in the HA cluster.</p>	
HA replications	<p>Time interval with which you want the GUI Server to replicate the database.</p> <p>By default, the GUI Server replicates the database every 60 minutes.</p>	
Heartbeat links between primary and secondary machine	<p>Number of heartbeat communication paths between the primary and secondary machine.</p> <p>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.</p>	
Shared password for heartbeat authentication.	<p>This is the password that is required to authenticate heartbeat messages between the primary and secondary HA servers.</p>	

Parameter	Description	Your Value
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: <code>/var/netscreen/dbbackup/</code>	
Path to the rsync utility executable	Path to the rsync utility executable. The default path is: <code>/usr/bin/rsync</code>	
Path to the ssh utility executable	Path to the ssh utility executable. The default path is: <code>/usr/bin/ssh</code>	
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.	
Hour of the Day to Start Local Database Backup	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 4:00am, type 04; if at 4:00pm, 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.	
Number of Local Database Backup Files Stored	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.	
Rsync Backup Timeout	Time value (in seconds) that the rsync utility waits before timing out backup operations. By default, the rsync utility waits 1800 seconds before timing out.	

Parameter	Description	Your Value
Enable Logging	Enable logging related to local backup and HA.	
Device Server Database Parameters	Parameters required for the Postgres Database used for the Device Server. You must specify a port number, super username and password. By default, the Postgres Database uses port 5432; the super user is "netscreen".	

Extended HA Configuration Parameters

Table 14 describes additional system parameters that you need to identify to install HA with the Device Server and GUI Server on separate server machines:

Table 14: Extended HA Configuration - System Parameters

Parameter	Description	Your Value
Device Server ID	Unique ID assigned when you add the Device Server.	
Password for GUI Server Connection	Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.	

Shared Disk Parameters

If you are using a shared disk partition, the installer prompts you to configure additional information. Table 15 identifies the additional system parameters that you need to identify to install HA with access to a shared disk:

Table 15: Shared Disk System Parameters

Parameter	Description	Your Value
Command to mount the shared disk partition	The command to mount the shared data partition. The default command is: <code>/bin/mount /var/netscreen/DevSvr</code>	
Command to unmount the shared disk partition	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: <code>/bin/umount /var/netscreen/DevSvr</code>	
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: <code>/sbin/fsck</code>	
Directory path for the shared disk	Directory path of the shared disk mount point.	

Prerequisites

Perform the prerequisite steps described as if you were installing the management system using a standalone configuration. Refer to "Prerequisite Steps" on page 14 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
- Verifying that All Required System Binaries are Available
- Verifying that Clocks are Synchronized
- Establishing an SSH Trust Relationship

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/utl1s` 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 server:

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

NOTE: If prompted to enter a passphrase, leave the value blank.

The result of the process is the creation of a hidden directory called `.ssh` under `/root` which contains two text files (public and private key).

2. Run the following commands on the secondary server:

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

NOTE: If prompted to enter a passphrase, leave the value blank.

3. You then need to copy the public key called `.ssh/id_rsa.pub` to the peer server manually and place it in `.ssh/authorized_keys`. For example, you would run the following command:

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

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_keys
```

5. You should test connectivity via SSH from the primary server to the secondary 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 Server>
```

6. Validate that you do not receive a prompt to enter a password to access the secondary 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 115 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 nsm2006.1_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2006.1_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**, then press `<Enter>` to specify that you want to install the Device and GUI Servers on the same server. The script then prompts if you want this machine to participate in an HA cluster.
 5. Type **y**, 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**, 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:
 - a. Type **n**, then press <Enter> if you are not using a shared disk. Type **y**, 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 59 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**, then press <Enter> if you are not using a shared disk. Type **y**, 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 59 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`.
 - c. Type the directory location for storing the GUI Server database log files or press <Enter> to accept the default location `/var/netscreen/GuiSvr/xdb/log`.

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

- d. 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.

The script then prompts you to type a password for the “super” user account.

- e. 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 log into the UI.

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

9. Type **n**, then press < Enter >, if you are not planning on installing NetScreen-Statistical Report Server with NetScreen-Security Manager. Type **y**, 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. 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. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- m. Designate a directory location for locally storing the management system HA/database backup. Press **<Enter>** to accept the default location `/var/netscreen/dbbackup`.
- n. Type the full path where the rsync utility is located.
- o. 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**, 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 (2:00am).
 - b. Type **n**, 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.
- d. Type a number specifying how many seconds you want the management system to wait while performing backups until the process times out.
- e. Type **y** or **n** to enable logging.

The script then prompts you to start the HA daemon processes when installation is complete.

12. Type **y**, then press < Enter > if you want to start the HA daemon processes. Type **n**, then press < Enter > if you to start the HA daemon processes manually. Refer to “Controlling the Management System” on page 103 for more information.
13. Verify your settings, and if they are correct, type **y**, then press < Enter > to proceed. If you type **n**, 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
- Performs post installation tasks such as generating the necessary certificates to enable encrypted communication between the Device Server and security 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, 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 6:00pm, then the installation log file would be named:

```
netmgmtInstallLog.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 103 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.

Other Useful Commands

Table 16 describes some useful commands which may assist in the installation and troubleshooting of your high availability configuration:

Table 16: Useful Installation and Troubleshooting Commands

Command	Description
less < filename >	This displays the contents of a text file. the up and down keys can be used to scroll. the letter q to quit.
netstat -n	This displays the current network connections without resolving any addresses
while sleep 1 ;do netstat -n grep 192.168.0.;done	This continually displays the command after the word do. useful if you are waiting for a server connection attempt of data sync.
clear	Clears the screen
vmstat 1	Gives a continuous output of system resource information. the figures at the end of the line give cpu stats.

Transferring Certificate Files (optional)

If you are using NetScreen-Security Manager to manage security 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
cr1_table.nml
nacncertificate_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: If you are using a shared disk, you must stop the primary server before installing the secondary server. The secondary server and primary server must also run on the same operating system and share the same directory structure for all NetScreen-Security Manager software and data.

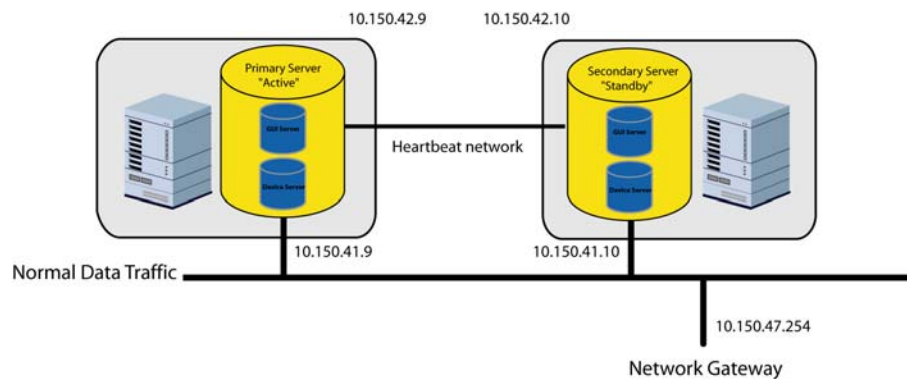
Example: Installing the Management System in an HA Configuration

For example, you want to install the management system in a simple 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

Figure 4 depicts the configuration example above.

Figure 4: HA Configuration Example



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
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]> 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]> y
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:
 D1:63:36:9E:C3:68:10:D7:13:64:3B:C0:36:C3:67:79:8A:AD:5B:CD
 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> 10.150.41.9
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 []> 10.150.42.10
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:
      D1:63:36:9E:C3:68:10:D7:13:64:3B:C0:36:C3:67:79:8A:AD:5B:CD
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 26 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 security devices in your network. In the event that the primary server becomes incapacitated, the managed security devices will re-attempt to connect to the management system using the Secondary Server IP Address.

To add the secondary server:

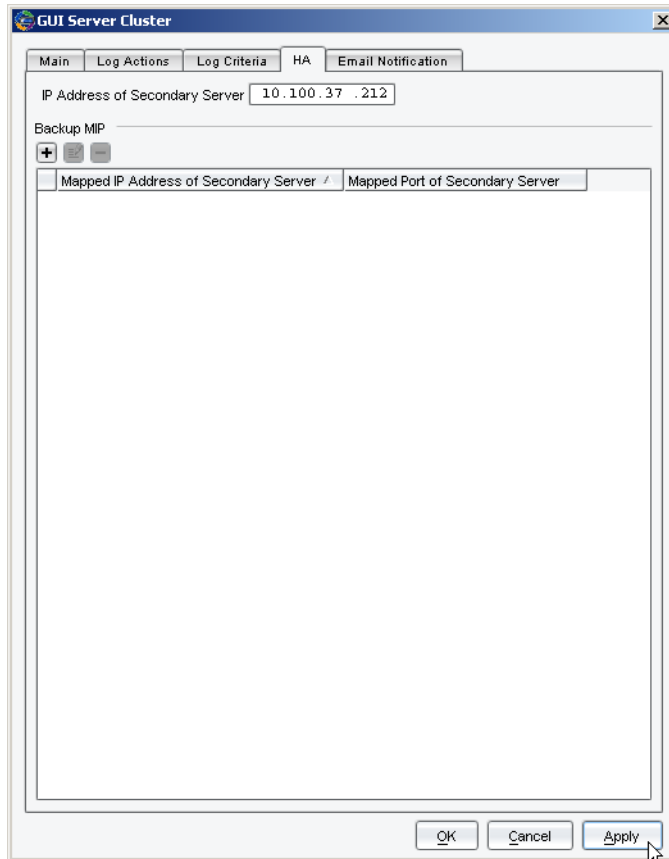
1. From the NetScreen-Security Manager UI, use **Server Manager > Server**.
2. In the Device Server area, click the + icon. The Device Server dialog box appears.
3. In the Name box, enter the name of the Device Server.
4. In the IP Address box, enter the IP address of the Device Server.

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 security 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)

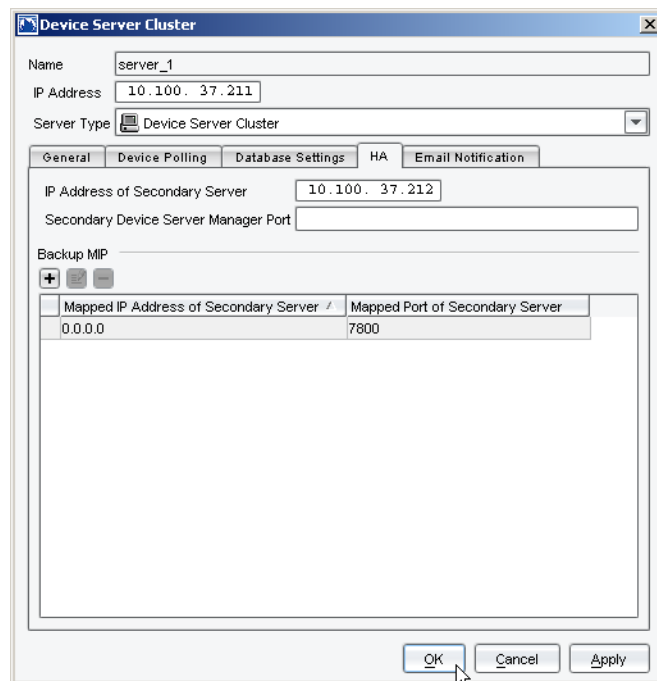
c. **Mapped IP Address** (if applicable)



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.

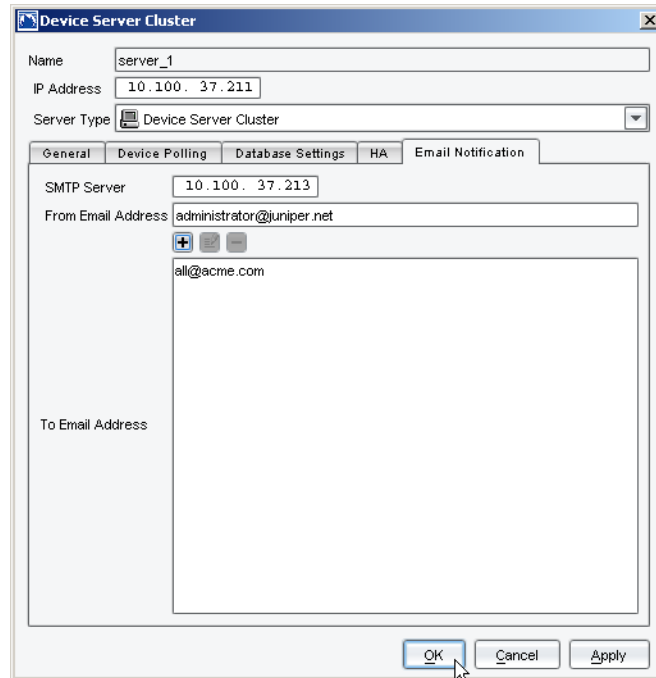
To configure the Device Server Cluster:

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. Log into 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. Log into the primary GUI Server and replicate the database. You can do so by running the following command:

```
/usr/netscreen/HaSvr/utlils/replicateDb ha
```

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

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

7. Verify that the command was successful.

Installing the Management System in an Extended HA Configuration

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: primary GUI Server, secondary GUI Server, primary Device Server, and secondary Device Server.

Use the system parameters referred to in “Extended HA Configuration Parameters” on page 59 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 59.

The process for installing the management system in an extended HA configuration is as follows:

1. Install the primary GUI Server; Start the HA Server process on the primary GUI Server.
2. Install the UI.
3. Login to the UI and add the primary Device Server.

Refer to “Installing the Management System in a Distributed Configuration” on page 33 for more information on installing the management system on separate servers. Refer to “Starting Server Processes Manually” on page 67 for more information on starting the HA Server process.

4. Install the primary Device Server; Start the HA Server process on the primary Device Server.
5. Install the secondary GUI Server and Device Server. Start the HA Server process on the secondary GUI and Device Server.
6. Perform a manual replication. Refer to “Testing the Initial HA Replication” on page 80 for more information on performing a manual replication.

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

The 192.168.0.x network is the operations LAN. The UI client does not need to be on the same network but must have a fast link to the active GUI Server. A Terminal Server could be used if this is not possible. The minimum speed is 384kbs although at this speed a large implementation will cause a slow user response.

The 1.1.1.x network is the management network. All communications to and from servers can use a single interface on each server. If using a shared disk, the host machine would also be placed on this network. The servers can be routed although LAN speed connections are recommended between. In the case of a UI client viewing continuously updating logs, large amounts of information will flow from the security device to the Device Server to the GUI Server to UI client in real time.

An optional second interface can be used to ensure heartbeat delivery and therefore avoid split brain situations. This is represented by the 2.2.2.x network.

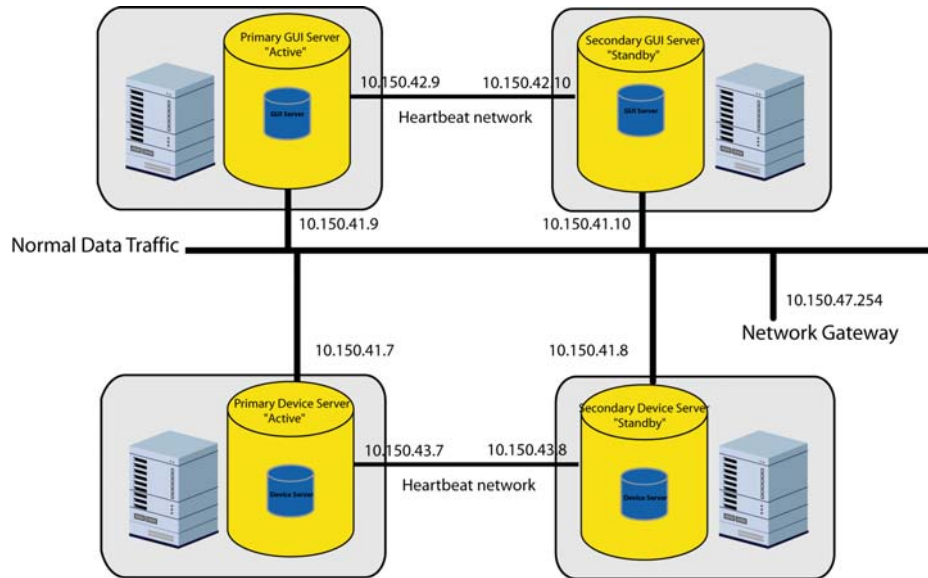
The following example illustrates a configuration which might be used for a similar situation to GuiSvr1 below. Note the Pingable IP address is the router. This ensures that if it cannot reach the router, it will failover.

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

Figure 5 depicts the configuration example above:

Figure 5: Extended HA Configuration Example



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 Administrator's Guide* and *Online Help* for information describing how to plan and implement NetScreen-Security Manager for your network.

Chapter 5

Upgrading to 2006.1

In This Chapter:

- “Upgrade Overview”
- “Defining System Parameters”
- “Prerequisite Steps”
- “Upgrading the Management System - Standalone Configuration”
- “Upgrading the User Interface”
- “Post Upgrade Steps: Migrating Domain Version Data”
- “Upgrading the Management System - Distributed 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 2006.1. This includes patching the management system, upgrading the User Interface on your Windows or Linux client, and validating that you have upgraded successfully.

Upgrade Overview

Table 17 summarizes the process for upgrading NetScreen-Security Manager for most typical cases.

Table 17: Upgrade Process

Step	Description/Estimated Time to Complete
1	Define system parameters that you need to provide during the installation process.
2	Perform prerequisite steps. It is highly recommended that you backup all your data files before beginning the upgrade process.
3	Download the NetScreen-Security Manager 2006.1 management system and User Interface installer software from the NetScreen-Security Manager installation CD or the Juniper Networks corporate Web site.
4	Run the NetScreen-Security Manager 2006.1 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.
5	Upgrade the User Interface.
6	Launch the User Interface, then connect it to the management system.
7	Validate that you have successfully installed the management system and User Interface.

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.

Standalone Configuration Parameters

Table 18 identifies the system parameters that you need to identify if you are upgrading a standalone configuration of the management system — both GUI Server and Device Server on the same server machine.

Table 18: Standalone Configuration - System Parameters

Parameter	Description	Your Value
Device Server data directory	<p>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.</p> <p>By default, the Device Server stores data in:</p> <p><code>/var/netscreen/DevSvr/</code></p>	
GUI Server data directory	<p>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.</p> <p>By default, the GUI Server stores data in:</p> <p><code>/var/netscreen/GuiSvr/</code></p>	
Management IP address	<p>The IP address used by the running GUI Server.</p> <p>The default is the IP address of the machine that you are installing on.</p>	
Initial “super” user password	<p>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.</p>	
Local database backup directory	<p>Directory location where local database backup data is stored.</p> <p>By default, the GUI Server stores local database backup data at:</p> <p><code>/var/netscreen/dbbackup/</code></p>	
Path to the rsync utility executable	<p>Path to the rsync utility executable.</p> <p>The default path is:</p> <p><code>/usr/bin/rsync</code></p>	
Remote Backup Machine IP Address	<p>IP address of the machine where remote backups are sent.</p> <p>By default, the installer sets this to the IP address of the secondary HA Server.</p>	
Hour of the Day to Start Local Database Backup	<p>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 4:00am, type 04; if at 4:00pm, 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.</p> <p>By default, the GUI Server performs the daily backup within an hour after 2am.</p>	
Number of Local Database Backup Files Stored	<p>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.</p> <p>By default, the GUI Server stores seven backup files.</p>	

Distributed Configuration Parameters

Table 19 describes additional system parameters that you need to identify if you are upgrading a distributed configuration of the management system — GUI Server and Device Server on separate server machines:

Table 19: Distributed Configuration - System Parameters

Parameter	Description	Your Value
Device Server ID	Unique ID assigned when you add the Device Server.	
Password for GUI Server Connection	Password assigned to the Device Server enabling it to authenticate with the GUI Server when attempting to connect.	

HA Configuration Parameters

Table 20 describes the system parameters that you need to identify if you are upgrading a standalone configuration of the management system with HA enabled:

Table 20: HA Configuration - System Parameters

Parameter	Description	Your Value
Primary HA Server IP address	IP address of the primary server participating in the HA cluster.	
Secondary HA Server IP address	IP address of the secondary server participating in the HA cluster.	
HA replications	Time interval with which you want the GUI Server to replicate the database. By default, the GUI Server replicates the database every 60 minutes.	
Heartbeat links between primary and secondary machine	Number of heartbeat communication paths between the primary and secondary machine. By default, there is only 1 communication link between the primary and secondary machine.	
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: <code>/var/netscreen/dbbackup/</code>	
Path to the rsync utility executable	Path to the rsync utility executable. The default path is: <code>/usr/bin/rsync</code>	
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.	

Parameter	Description	Your Value
Hour of the Day to Start Local Database Backup	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 4:00am, type 04; if at 4:00pm, 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.	
Number of Local Database Backup Files Stored	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.	

Shared Disk Parameters

Table 21 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

Parameter	Description	Your Value
Command to mount the shared disk partition	The command to mount the shared data partition. The default command is: <code>/bin/mount /var/netscreen/DevSvr</code>	
Command to unmount the shared disk partition	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: <code>/bin/umount /var/netscreen/DevSvr</code>	
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: <code>/sbin/fsck</code>	
Directory path for the shared disk	Directory path of the shared disk mount point.	

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. Log into 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, 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 110.

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 “*Hardware Sizing Recommendations*” on page 1 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 111 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 91 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 “Patching the Sun Solaris SSH Daemon” on page 92 for more information.
7. If you are installing the management system on Solaris 8 or 9, it is highly recommended that you increase the maximum size of your shared memory segment. Refer to “Increasing Shared Memory Segment Maximum Size” on page 93 for more information.

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.

NOTE: The NetScreen-Security Manager 2005.3 system update utility is compatible with Red Hat Enterprise Linux 3.0 Update 5 and Red Hat Enterprise Linux 4.0 Update 1.

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.

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

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 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. Log into 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.

Increasing Shared Memory Segment Maximum Size

If you are installing the management system on Solaris, it is highly recommended that you increase the maximum size of your shared memory segment.

To increase the maximum size of shared memory:

1. Open the `/etc/system` file in any text editor.
2. Edit the OS kernel parameters by adding the following lines.

```
set shmsys:shminfo_shmmax=0x2000000  
set shmsys:shminfo_shmmi=1  
set shmsys:shminfo_shmmni=256  
set shmsys:shminfo_shmseg=256  
set semsys:seminfo_semmap=256  
set semsys:seminfo_semmni=512  
set semsys:seminfo_semns=512  
set semsys:seminfo_semmsl=32
```

3. Save the file.
4. Restart your system.

Upgrading the Management System - Standalone 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 - Distributed Configuration” on page 99.

To upgrade the management system on a standalone system:

1. Load the NetScreen-Security Manager 2006.1 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 nsm2006.1_servers_linux_x86.sh
```

On Solaris, run the following command:

```
sh nsm2006.1_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 upgrade both the Device Server and GUI Server.

4. Type **2** to specify that you want to upgrade both the Device Server and GUI Server.

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

The installer next prompts you to configure additional options specific to your installation during the upgrade. This can include:

- configuring High Availability
 - migrating versioned domains
 - configuring interoperability with NetScreen-Statistical Report Server
 - configuring backup options
5. If applicable, follow the installer prompts to configure these options. Refer to “Configuration Options” on page 6 for more information. The script next prompts if you want to restart the server(s) when finished.
 6. Type **y**, then press < Enter > to restart the server(s) when finished. Type **n**, then press < Enter > , if you do not want to restart server processes.

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.

7. Verify your settings, and if they are correct, type **y**, then press < Enter > to proceed. If you type **n**, 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 and decompresses 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, then exits.

After the installation script finishes, it generates a log file with the output of the installation commands for troubleshooting purposes. The installer indicates the name of the installation log file and the directory location where it is saved. This file is saved by default in the `tmp` subdirectory.

An example of the output is as follows:

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

For example if you ran the installer on June 1, 2005 at 6:00pm, then the installation log file would be named: `netmgtInstallLog.20050601180000`.

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:

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

2. Run the following command:

```
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:

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

2. Run the following command:

```
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:

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

2. Run the following command:

```
sh devSvr.sh status
```

Refer to “Controlling the Management System” on page 103 for more information on manual commands that you can send to the management system.

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 “Installing the User Interface” on page 26 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 security 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.

Post Upgrade Steps: Migrating Domain Version Data

Users of previous versions of NetScreen-Security Manager may note that each time you update a device configuration on a security device using NetScreen-Security Manager, a new version of the device domain is automatically created. NetScreen-Security Manager archives the previous domain version and stores it on the GUI Server.

During the upgrade process, you are given the option of migrating data about your versioned domains. Because the number and size of the data in domain versions can grow to be quite large, it can take an extraordinary amount of time to migrate this data. For your convenience, a note appears in the installer script warning that the domain version migration can take an extremely long time to complete, depending upon the size of the domain version data. 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.

If you choose not to migrate data about your versioned domains as part of the upgrade process, a tool is provided in the NetScreen-Security Manager utility package enabling you to migrate the data manually.

To migrate your domain version data manually:

1. Stop all server processes—first the HA Server, the Device Server, then the GUI Server.
2. Log into the GUI Server.
3. Run the following command specifying the domain name and the domain version number:

```
/usr/netscreen/GuiSvr/utils/sh migrateDomainVersion.sh <domain name>  
<domain version #>
```

The domain version migration tool migrates one domain version at a time.

4. Repeat the command for all domain names and versions.
5. Restart all server processes — first the HA Server, the GUI Server, then the Device Server.

Validate that the domain version data migrated successfully.

Upgrading the Management System - Distributed Configuration

The process for upgrading the management system on separate servers (i.e., in the distributed configuration) is as follows:

1. Perform the pre-requisites steps described as if upgrading the management system in a standalone 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 15. 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**, then press <Enter> when prompted if this machine will participate in an HA Cluster
 - Type **y**, then press <Enter> when prompted if this machine is the primary server for the HA Cluster
 - Type **y**, then press <Enter> if the Device Server data directory is located on a shared disk partition. Type **n**, then press <Enter>, if you are not using a shared disk partition for the Device Server.
 - Type **y**, then press <Enter> if the GUI Server data directory is located on a shared disk partition. Type **n**, 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 97 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 "High Availability Overview" on page 47 for more information.
11. Test HA replication. Refer to "Testing the Initial HA Replication" on page 80 for more information.

Upgrading the Database Backup Files

If you have implemented your previous installation of NetScreen-Security Manager with high availability, and upgraded to NetScreen-Security Manager 2006.1, 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 115 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. 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 121 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 “Archiving and Restoring Logs and Configuration Data” on page 111 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 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”
- “Configuring Server Options”
- “Archiving and Restoring Logs and Configuration Data”
- “Configuring High Availability Options”
- “Relocating the Database”
- “Installing a tftp Server”
- “Modifying the Bulk CLI Status Timeout Value”
- “Downgrade Procedures”
- “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 an tftp server (required if you are managing security 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, 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:

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

2. Run the following command:

```
./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:

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

2. Run the following command:

```
./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:

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

2. Run the following command:

```
./haSvr.sh
```

Common Management System Commands

Table 22 describes the commands that the management system supports.

Table 22: Management System Commands

Command	Action
reload	Sends a hangup signal to the management system process, then instructs the process to reload its configuration and start again.
restart	Stops the management system process for two seconds, then restarts the process.
start	Starts the management system process.
stop	Stops the management system process.
status	Provides a status of the management system process.
version	Lists the current version of the management system.

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:

```
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
```

Configuring Server Options

The following procedures are provided for your reference:

- Changing the Management System IP Address on page 120
- Changing the Device Server IP Address on page 121
- Changing the GUI Server IP Address on page 122
- Configuring Disk Space Management on page 108
- Configuring Connection Timing on page 109
- Changing Permissions To a Normal User on page 123

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 security devices to connect to it at its new location.

To change the management system IP address:

1. Update the Device Server IP on each security device or set the secondary management server IP to the new IP address.
2. Log into the server that is running the Device Server as **root**.

3. Navigate to `usr/netscreen/DevSvr/var`
4. Open the Device Server configuration file (`devSvr.cfg`) in any text editor.
5. Edit the values for the `guiSvr.addr` and `guiSvr.port` variables using the new IP address and port number.
6. Save the Device Server configuration file.
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, 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 security devices to connect to it at its new location.

To change the Device Server IP address:

1. Update the Device Server IP on each security device or set the secondary management server IP to the new IP address.
2. Log into 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.
6. Save the `server_table.nml` file.
7. Restart the GUI Server.

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. Follow the procedures to edit the Device Server configuration file (called `devSvr.cfg`).

2. 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.
3. Log into the server that is running the GUI Server as root.
4. Navigate to `usr/netscreen/GuiSvr/var`
5. Open the `server_table.nml` file in any text editor.
6. Edit the values for the IP Address in the GUI Server section only.
7. Save the `server_table.nml` file.
8. Restart the GUI Server, then restart the Device Server.

Configuring Disk Space Management

The Device Server maintains a minimum of 1000Mb (by default) of disk space available, primarily for the storage of log records. When the available disk space reaches this minimum, it sends an email alerting you of the situation. In the event that disk space on the Device Server reaches a minimum of 500Mb, the Device Server attempts to free the disk space by purging log records beginning with the oldest records on file. The Device Server stops purging log records when the 1000Mb minimum disk space is restored. If for any reason, the Device Server is not able to restore 500Mb of disk space, the Device Server will automatically shut down. If the Device Server fails to restart for this reason, an error message appears in the console window indicating that there is not enough disk space on the server machine, and that you must either backup your data or free up additional disk space in order to start the server again.

If you want to change the parameters for managing disk space on the Device Server, you can edit the Device Server configuration file.

To configure disk space management:

1. Log into 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 value (in megabytes) for the `storageManager.threshold` parameter. This parameter sets the minimum threshold at which the Device Server begins purging log records. The Device Server purges log records when disk space reaches 500Mb by default.
5. Edit the value (in megabytes) for the `storageManager.minimumFreeSpace` parameter. This parameter indicates that 1000Mb disk space need to be free up if the Device Server starts to purge log records after crossing `storageManager.threshold`.

6. Edit the value (in megabytes) for the `storageManager.alert` parameter. This parameter sets the minimum threshold for available disk space at which the Device Server sends you an email alert. The Device Server sends an email alert when disk space reaches 1000Mb by default.

NOTE: Use the Server Manager node in the NetScreen-Security Manager UI to configure email notification. Refer to the *NetScreen-Security Manager Administrator's Guide* for more information.

7. Save the file.
8. Restart the Device Server.

Disk Space Management on the GUI Server

Disk space management occurs in the same manner on the GUI Server except that there is no log record purging on the GUI Server side. When the GUI Server reaches the minimum disk space threshold, it automatically shuts down. You will not be able to restart the GUI Server until you restore the minimum disk space.

The GUI Server also performs a checks for sufficient i-nodes. I-nodes are data structures that contain information about files in a Unix file system. Each file has an inode that is identified by an inode number (i-number) in the file system where it resides. There are a set number of inodes, which indicates the maximum number of files the system can hold. If the required minimum i-nodes is not available, the GUI Server shuts down automatically. The default threshold is 10% of the total i-nodes remaining. You will not be able to restart the GUI Server until you reclaim required minimum i-nodes. For your convenience, a shell script is provided enabling you to reclaim i-nodes. This script is located in the utilities directory on the GUI Server (i.e., `/usr/netscreen/GuiSvr/util`). The script first archives the old domain versions into a compressed tar file before removing them to reclaim i-nodes. The archive file is stored in:

```
/usr/netscreen/GuiSvr/var/global/oldDomainVersion.MM-DD-YYYY-HH-MM.tar.gz
```

You can configure disk space management on the GUI Server by editing the values for the parameters listed previously in the GUI Server configuration file (called `guiSvr.cfg`). If you are running the Device Server and GUI Server on the same machine, it is recommended that you set the `storageManager.threshold` on the Device Server to a value that is higher than that on the GUI Server. By doing this, the GUI Server will not shut down as the Device Server attempts to free up some disk space by purging logs. You can also configure the minimum i-node threshold by editing the `storageManager.inodeThres` variable.

Configuring Connection Timing

To configure connection timing with the managed devices in your network:

1. Follow the procedures to edit the Device Server configuration file (called `devSvr.cfg`).

2. 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 security devices running ScreenOS 4.x. The `devSvrDirectiveHandler.fastCli.timeout` parameter determines the amount of time that the Device Server waits for a CLI response from a security device running ScreenOS 4.x before it disconnects the connection. By default, the Device Server waits 40 seconds before disconnecting the connection.
3. Save the file.
4. Restart the Device Server.

Changing Permissions To a Normal User

In Linux/Solaris systems, services and scripts are run by a particular user, whether automatically or manually at a command prompt. All files and directories on the system have an associated permission. For example, if you log in with a non-root user you will receive an error message if you attempted to run a script which was associated with the root user.

The NetScreen-Security Manager management system runs by default as the root user. If your organization has a policy which does not permit processes to be run as root, you have the option of running some parts of the system as a non-root user. The management system makes use of a user called “nsm” in the group “nsm”. This must be created prior to installation (if you want to change permissions from root) on each system using the following commands:

```
groupadd nsm
useradd -g nsm -s /bin/bash -d /home/nsm nsm
```

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

If after installation, you decide that you want to change permissions, a shell archive script called “`setperms.sh`” is included for both the Device Server and GUI Server that automatically changes the `setuid.user` value.

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, 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.

NOTE: If you run the management system in an HA configuration as a normal user, you need to enable the remote replication utility to also run as a non-root user. Refer to “Running the Remote Replication Utility as a Non-Root User” on page 115 for more information.

Setting Core File Naming on Solaris

If you are running the management system on Solaris, you can configure the file naming used for core files to indicate the executable file and process ID generating the core file. This also ensures that Solaris does not overwrite the names of multiple core files.

To set core file naming on Solaris:

1. Log into the GUI Server computer as root.
2. Run the following command:

```
coreadm -i core.%f.%p
```
3. Restart the server.

Future core files will indicate the executable file name and process id generating the core file. For example, if the core file “core.a.out.8855” appears, the file name indicates that the core file was generated by an executable named “a.out”, running process id “8855”.

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; 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.

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>
bi
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, then the Device Server.

Restoring Logs and Configuration Data

To restore log and configuration data:

1. Stop the HA Server, Device Server, 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, 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 Options

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:

```
cd /usr/netscreen/HaSvr/var/
```

2. Open the High Availability configuration file (`haSvr.cfg`) in any text editor.
3. Configure the following parameters:

```
highAvail.isHaEnabled=y  
highAvail.isWatchdogEnabled=n
```

4. Save the file.
5. Restart the HA Server process. To do this, you must send a HUP signal to the `highAvail` daemon. For example, type the following command:

```
kill -HUP <process id>
```

NOTE: You can run an `haStatus` command to identify the `highAvail` daemon process ID.

NOTE: By sending a HUP signal to the `highAvail` daemon, you no longer need to restart the HA Server process.

To disable high availability, follow the above procedures to High Availability configuration file, configure the following parameter, and save the file:

`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 HA Server process. To do this, you must send a HUP signal to the `highAvail` daemon. For example, type the following command:

`kill -HUP <process id>`

NOTE: You can run an `haStatus` command to identify the `highAvail` daemon process ID.

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 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.
3. Navigate to the HA Server utilities subdirectory (`/usr/netScreen/HaSvr/utils` by default).

4. Run the database restore shell archive script and specify the number day of the week for the backup file that you want to restore from (N = backup day of the week). You can do so by running the following command:

```
restoreDbFromBackup.sh N
```

For example, to restore the backup file from Friday:

```
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.

Changing the HA Server IP Address

If for any reason you are required to change the IP address of either the primary or secondary HA Server, note that you must manually re-import or update the IP Address on the device.

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 2005.x). 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 “Installing the Management System in a Standalone Configuration” on page 11 for more information on installing the management system on the same server machine.

Refer to “Installing the Management System in a Distributed Configuration” on page 33 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. (Optional) If you are using NetScreen-Security Manager to manage IDP sensors, you must also copy /usr/netscreen/DevSvr/var/certDB/ to the new server. This is required to enable IDP sensors to connect back via TLS to the Device Server.
5. 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 security 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 security 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:

```
service tftp
{
  socket_type = dgram
  protocol = udp
  wait = yes
  user = root
  server = /usr/sbin/in.tftpd
  server_args = -s /usr/netscreen/DevSvr/var/cache
  disable = no
  per_source = 11
  cps = 100 2
}
```

4. Restart the `xinetd` service. You can do so by running the following command:

```
service xinetd restart
```

Installing a tftp Server on Solaris

By default, Solaris installs the tftp service on your machine but leaves it disabled.

To configure and enable the tftp service on Solaris:

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

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

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

```
/etc/init.d/inetd stop
/etc/init.d/inetd start
```

Modifying the Bulk CLI Status Timeout Value

By default, the bulk command line interface (CLI) timeout value is 40 minutes. You can modify this value to be from 1 to 39 minutes.

1. Stop the Device Server and any High Availability processes by entering the following commands:

```
/etc/init.d/haSvr stop
/etc/init.d/devSvr stop
```

2. Open the following file in a text editor:

```
/var/netscreen/DevSvr/be/cfg/devCommProp.cfg
```

3. Locate the following line:

```
:bulk-cli-final-status-timeout (40)
```

4. Change the “40” to a value from 1 to 39.
5. Start the Device Server and verify that 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
```

Downgrade Procedures

If you upgrade to NetScreen-Security Manager 2006.1, then decide to downgrade back to NetScreen-Security Manager 2005.3, then you need to reinstall NetScreen-Security Manager 2005.3, and restore your old data. Before you upgrade

to NetScreen-Security Manager 2006.1, verify that you have made a backup copy of all of your existing data from NetScreen-Security Manager 2005.3.

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 NetScreen-Security Manager 2006.1 to NetScreen-Security Manager 2005.3:

1. Make a backup copy of all your existing data.
2. Remove the management system. Refer to “Removing the Management System” on page 121 for more information.
3. Install NetScreen-Security Manager 2005.3.
4. Restore your backup database. Refer to “Restoring the Database” on page 115 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. For systems running Linux:

- a. 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
```

- b. Navigate to the `/var` subdirectory, and remove all the files in the `netscreen` subdirectory.

```
rm -rf netscreen
```

5. For systems running Solaris:

- a. Locate and remove all packages related to NetScreen-Security Manager in the `netscreen` subdirectory. For example, run the following commands:

pkginfo | grep -i netscreen

```
application NSCNhasv      NetScreen-Security Manager HA Server
application NSCNguisv     NetScreen-Security Manager GUI Server
application NSCNdevsv     NetScreen-Security Manager Device Server
```

root# pkgrm -R / NSCNdevsv

```
The following package is currently installed:
NSCNdevsv      NetScreen-Security Manager Device Server
(sparc) 1.3.2
```

Do you want to remove this package? [y,n,?,q] y

```
## Removing installed package instance <NSCNdevsv> ## Verifying
package dependencies.
## Processing package information.
## Removing pathnames in class <none>
/usr/netscreen/DevSvr/utills/setperms.sh
/usr/netscreen/DevSvr/utills/policy_compiler
/usr/netscreen/DevSvr/utills/nacnUpdateCANm1
/usr/netscreen/DevSvr/utills/nacnLoadPKCS12
...
/usr/netscreen/DevSvr/bin/.devSvrDataCollector
/usr/netscreen/DevSvr/bin
/usr/netscreen/DevSvr <non-empty directory not removed> ## Updating
system information.
Removal of <NSCNdevsv> was successful.
```

- b. Repeat this step for each package.
- c. Remove the `netscreen` subdirectory.
- d. Remove the startup script links. For example, run the following commands:

```
cd /etc/rc3.d
/etc/rc3.d root# ls *Svr
S32haSvr S33guiSvr S34devSvr

/etc/rc3.d root# rm -f *Svr
/etc/rc3.d root#
```

- e. Remove the actual scripts. For example, run the following commands:

```
cd ../init.d
etc/init.d root# ls *Svr
devSvr guiSvr haSvr

etc/init.d root# rm -f *Svr
etc/init.d root#
```

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, 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 security 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 Security Devices

Figure 6: NetScreen-Security Manager Architecture



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 security 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.

Figure 7: 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 including all device configuration information, audit log data (i.e., versioning), and almost all other information pertinent to the system except log data sent by the security device.

NOTE: The GUI Server can accommodate no more than 20 UI clients 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 the security devices in your network. The Device Server stores this data, primarily traffic logs generated by a security device, in a local data store.

NOTE: The Device Server can accommodate no more than 6000 security devices connected to it at any time. This is the maximum number of security 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 Administrator's Guide* or the *Online Help* included in the UI for more information about the NetScreen-Security Manager UI.

About Managed Security Devices

The managed security devices that you have implemented in your network are the lowest tier of the NetScreen-Security Manager management architecture.

You need to enable each security device to communicate and work with NetScreen-Security Manager. Refer to the *ScreenOS Concepts and Examples Guide* for more information describing how to enable management on your security devices.

Once enabled, each security 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 security devices provide the firewall and VPN services required to secure your network environment.

Server Communications

As you plan your installation, it helps to understand how NetScreen-Security Manager establishes communication between the UI, Management System, and security 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 security devices and two outbound TCP ports used to establish communication with security devices running ScreenOS 4.0.X.

Table 23 summarizes the port that is open on the GUI Server.

Table 23: GUI Server Communication Port

Port	Protocol	Direction	Description
7801	TCP	INBOUND	<p>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).</p> <p>This communication session uses an <i>encrypted</i> 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.</p>

Table 24 summarizes the ports that are open on the Device Server.

Table 24: Device Server Communication Ports

Port	Protocol	Direction	Description
7800	TCP	INBOUND	Listens for incoming connection requests from security device(s) running ScreenOS 5 + . Used to establish encrypted communication sessions with the GUI Server and security devices (running ScreenOS 5 +).
15400	TCP	INBOUND	Listens for incoming Report Manager NetScreen protocol (NSP) connection requests from security device(s) using ScreenOS 4.0.x. Used to establish communication session with security devices running ScreenOS 4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.
11122	TCP	INBOUND	Listens for incoming NACN connection requests from security device(s) using ScreenOS 4.0.x. Used to establish communication session with security devices running ScreenOS 4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.
69	UDP	INBOUND	Listens for incoming tftp connection requests from security device(s) using ScreenOS 4.0.x. Used to establish communication session with security devices running ScreenOS 4.0.x. These sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections.
22/23	TCP	OUTBOUND	Sends outbound Telnet/SSH connection requests to security device(s) using ScreenOS 4.0.x. Used to establish communication sessions with security devices running ScreenOS 4.0.x. While SSH sessions are encrypted, Telnet sessions are not encrypted. To secure the data transfer, it is highly recommended that you run a VPN tunnel for each pair of connections. It is not recommended that you use a Telnet session to communicate between devices because it is insecure. If your devices are running with ScreenOS 4.0.x, then use a SSH connection.
7803	TCP	INBOUND	Listens for Intrusion Detection and Prevention (IDP) connection requests by default.

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 security 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 security 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 security devices managed in your network. You must also configure firewalls between the GUI Server and UI clients to permit TCP port 7801.

Table 25 lists and describes the ports used specifically in communications between NetScreen-Security Manager and ScreenOS 5.0 devices.

Table 25: Management System Communications With Devices Running ScreenOS 5.x

Server Component	Port	Description
Device Server	Inbound TCP: 7800	Accepts incoming ScreenOS 5.0 device connections.
Device Server	Outbound TCP: 7801	On a separated install, used to communicated with GUI server.
Device Server	Outbound TCP: 22/23	SSH/Telnet to import initial configs of devices running ScreenOS 5.0.
GUI Server	Inbound TCP: 7801	Accepts communication from the Device Server and UI.

NOTE: The Device Server can use port 22 (SSH) to perform an initial connection to security 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. Security devices running ScreenOS 5.0 also support SSH v2.

Communicating With Devices Running Screen 4.x and Earlier

Security 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 security devices running 4.x and earlier is strongly recommended.

Table 26 lists and describes the ports used specifically in communications between NetScreen-Security Manager and ScreenOS 4.x and earlier devices.

Table 26: Management System Communications With Devices Running ScreenOS 4.x and Earlier

Server Component	Port	Description
Device Server	Outbound TCP: 22/23	SSH/Telnet to manage security devices running ScreenOS 4.0.x.
Device Server	Inbound TCP: 15400	Management for security devices running ScreenOS 4.0.x.
Device Server	Inbound UDP: 69	tftp server for updating security devices running ScreenOS 4.0.x.
Device Server	Inbound TCP: 11122	Accepts incoming NACN requests for security devices running ScreenOS 4.0.x.

Figure 8: NetScreen-Security Manager Communications



Creating a Separate Management Network

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

If you are deploying NetScreen-Security Manager in a network with security 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.

Appendix B

Hardware Sizing Recommendations

This appendix lists guidelines for NetScreen-Security Manager hardware sizing. System requirements for each NetScreen-Security Manager component vary by use. We recommend that you discuss your current and projected device management requirements with a Juniper Systems Engineer to ensure that your needs are met by the hardware you select.

Formulas and Guidelines

Four basic elements determine sizing:

- type of installation: standalone or distributed
- memory
- storage capacity
- processor speed

Specific requirements for each system vary, but you can apply some general rules and formulas.

Standalone or Distributed System for GUI Server and Device Server

The GUI Server and Device Server are the two components of the management system. The GUI Server stores all configuration data and manages the UI connections. The Device Server stores logs and maintains connectivity to your managed devices.

If you are managing more than 1000 devices, it is recommended that you use two Network Interface Cards (NIC) for both GUI Server and Device Server systems. One of the NIC cards is dedicated for the connection between GUI Server and Device Server. The other NIC card is used for GUI connections and device connections for GUI Server and Device Server respectively.

Configuring Multiple Network Interface Cards

The process of configuring multiple Network Interface Cards (NICs) with NetScreen-Security Manager is as follows:

1. Before installing NetScreen-Security Manager, enable one NIC only.
2. Install NetScreen-Security Manager management system and User Interface.
3. Enable the second NIC.
4. Log into the UI as a super user.
5. Select Server Manager > Servers.

6. Edit the Device Server. Under the section MIP, add the IP Address of the second interface.
7. When you add a device, use the MIP Address for the devices to connect to the Device Server.

The GUI Server and Device Server may be combined if you have fewer than 200 devices, small device configuration sizes (e.g. large number of NS-5GTs with a few larger systems), and fewer than 1000 logs per second from all devices. Add at least 1GB RAM to the recommended GUI Server RAM to support this configuration.

Memory Requirements

This section details memory requirements on the GUI Server and Device Server.

GUI Server

Many factors are involved in determining the memory requirements for a given system, however the biggest factor is device configuration size.

First, make note of the number and type of devices that will be managed by NetScreen-Security Manager, and their configuration sizes. Configuration sizes can vary widely based on the number of rules in a policy and the number of VPN tunnels. To determine configuration size for a device look at the first line of the output of get config on the CLI. This is the size of the configuration for a device in bytes. Take the sum of the configuration sizes to be managed and refer to Table 27 to determine the estimated RAM required:

Table 27: GUI Server RAM Requirements

Total Config Size	GUI Server RAM Required
Less than 2 MB	512MB
Between 2 and 10 MB	3 GB
Between 10 and 50 MB	4 GB
More than 50 MB	8GB

Device Server

The key factor in determining the memory requirements for the Device Server is the number of devices you are managing. Use Table 28 to determine the requirements for a given deployment size if the Device Server is managing firewall/VPN devices only

Table 28: Device Server RAM Requirements for firewall/VPN devices

Number of Devices	Device Server RAM Required
Less than 200	1 GB
More than 200	2 GB
More than 500	4 GB

Use to determine the requirements for a given deployment size if the Device Server is managing IDP standalone devices that are performing profiling operations.

Table 29: Device Server RAM Requirements for IDP standalone devices running Profiler

Number of Profiling Devices	Device Server RAM Required
1-2	1 GB
3-8	2 GB
9-20	8 GB

UI Client

For managing more than 1000 devices, it is recommended to use PCs with 1 GB of RAM. In addition, it is recommended that you make the following change in the NSM.lax file in the C:\Program Files\NetScreen-Security Manager directory on the client machines:

Change:

```
tax.nl.java.option.java.heap.size.max=384m  
to:  
tax.nl.java.option.java.heap.size.max=512m
```

Storage Space Requirements

This section details storage space requirements on the GUI Server and Device Server.

GUI Server

Beyond the storage space required for the device configurations, there are additional items to be considered in sizing storage space. The GUI Server binaries and libraries require less than 100 MB.

Other key components that are disk space intensive are:

- Audit Log
- Error Log
- Device configuration database
- Nightly backup

The storage space requirements for each component are described in more detail below.

Audit Log

The Audit log has a large impact on disk space depending on how the audit log detail option is configured. You can configure the following options in the guiSvr.cfg file located in /usr/netscreen/GuiSvr directory:

```
guiSvrManager.auditlog_flag
```

1. Audit log is completely disabled if set = 0

guiSvrManager.auditlog_detail_flag

2. Audit summary only is enabled if set = 0

Table 30: Audit Log Details

Operation	Audit Log Detail OFF	Audit Log Detail ON
Update Device 10K	408 bytes	40 KB
Update Device 30K	408 bytes	60 KB
Update Device 300K	456 bytes	240 KB
Add Device	6K	5 KB
Login in/out	540 bytes	180 bytes
Save Policy 25 rules	144 bytes	.01 MB
Save Policy 100 rules	192 bytes	0.5 MB
Save Policy 250 rules	1536 bytes	0.75 MB
Save Policy 1000 rules	3072 bytes	5 MB
Save Policy 5000 rules	6144 bytes	15 MB

For example, in a system with 100 devices with 10 KB configuration size per device and 1000 rules, 100 device updates and 5 policies saves uses $(100 * 40 \text{ KB} + 5 * 5 \text{ MB} = 29 \text{ MB})$ 29 MB with the audit log detail option on. With the audit log details turned off, it takes only $(100 * 408\text{bytes} + 5 * 1 \text{ KB} = 45\text{KB})$ 45 KB of disk space.

The GUI Server also requires 2 GB for the database transaction log.

Error Log

The `/var/netscreen/GuiSvr/errorLog` directory keeps error log files (guidaemon.0). It stores up to 25 files before the oldest log files are overwritten. Each day's file may be up to 5 MB in size. Based on these default settings, error logs can consume up to 125MB (or 250 MB if GUI Server and Device Server are on the same server).

Device Configuration Database

The size of the Device Configuration database can vary based on number of devices and types of configuration used. For every 1 MB of aggregate device configuration, NetScreen-Security Manager may need 200 MB disk space.

For example, 100 devices with 10 KB configuration may need $(10 \text{ KB} * 100) * 200 = 200 \text{ MB}$ of disk space.

Nightly Backup

Nightly backup will maintain 7 copies of the GUI Server database if the default installation option is selected. The disk space requirement should be $7 * (\text{device configuration database size calculated above})$.

Device Server Requirements

Storage capacity requirements are determined by the following equation:

$(\text{Retention period in days} * \text{Events per day} * 200 \text{ bytes}) / 1,000,000,000 = \text{storage size in GB.}$

Log events average around 200 bytes each. Table 31 lists some examples for a Device Server managing just firewall/VPN devices based on a retention period of 30 days:

Table 31: Storage Requirements for Device Server Managing Firewall/VPN Devices

Events Per Day	Storage required
1,000,000	6 GB
10,000,000	60 GB
25,000,000	150 GB
50,000,000	300 GB

Table 32 lists some examples for a Device Server managing just IDP stand-alone devices running profiler based on a retention period of 30 days:

Table 32: Storage Requirements for Device Server Managing IDP (w/Profiler) Devices

Number of Profiling Devices	Storage required
1-2	8 GB
3-8	12 GB
9-20	24 GB

If traffic logs are turned on, they generally comprise about 2/3 of all logs; so turning off traffic logs can result in a large savings in storage space.

In NetScreen-Security Manager, logs are stored in /var/netscreen directory of the Device Server by default. Always mount the /var directory on a separate partition or drive from / to avoid log files filling up your root partition and crashing your server. In situations calling for high volume logging, it is recommended you mount /var on a locally attached high speed SCSI drive or similar performance storage solution. You can specify the path for log storage during initial installation.

In addition to regular logs, error logs may consume up to 125MB of storage space on the Device Server.

Processor Speed Requirements

This section details requirements for CPU on the GUI Server and Device Server.

GUI Server

A faster CPU in the GUI Server provides for a more responsive Log Viewer, and a faster feeling system overall. It is recommended that you focus on a system that supports your storage and memory needs first, and get a mid-range to high-end processor for it. Dual processors have a negligible performance benefit for NetScreen-Security Manager, but may have additional performance benefits with future releases.

Device Server

In internal testing, CPU speed had an impact on scalability on the Device Server in regard to sustained logging rates. A modern Intel or AMD CPU (i.e. 2.4GHz) or an UltraSparc III (1.2 GHz) is capable of handling sustained log rates in excess of 20,000 logs per second, while the SPARC processors in the Netra X1 used as a Global Pro Express appliance are able to handle fewer than 1900 logs per second.

A fast CPU on the Device Server is recommended for environments with high log volumes. For deployments using ScreenOS 4.0, maximum logging rates are approximately 1,900 events per second. For deployments using ScreenOS 5.0, maximum logging rates are approximately 20,000 events per second.

Device Server Managing IDP Standalone Devices Running Profiler

Multiple CPUs are recommended if you the Device Server is managing IDP standalone devices running profiler.

Table 33: CPU Requirements for Device Server Managing IDP (w/Profiler) Devices

Number of Profiling Devices	CPUs
1-2	1
3-8	2
9-20	4

Recommendations for Large Scale Installations

The following recommendations apply for large scale installations of NetScreen-Security Manager:

- Install Red Hat Enterprise Linux ES4 - Update 1 w/2.6.9-22 kernel (this kernel was introduced in ES4 update 2)). Linux is significantly faster than Solaris in our testing.
- Install Linux ext2 filesystem for maximum performance. Note that without journaling, crash recovery will not be robust. Regular backups mitigate that risk.
- Disable atime filesystem feature by mounting the noatime option.
- Use secondary 7200 RPM or better SATA hard drive for /var/netscreen on both the GUI Server and Device Server.
- For maximum server capacity and performance, use a high performance RAID controller such as the Adaptec 2410SA with striping across 2 or more 10K RPM drives. Avoid LSI MegaRAID based adapters (commonly shipped with Dell servers) since these have performed poorly in our internal testing.
- The Device Server must have at least enough space in /var/netscreen for 1 day of logs. Make sure that the storage manager parameters in devSvr.cfg are adjusted to cover 1 full day's worth of logs. You should set values in both the storageManager.minimumFreeSpace and storageManager.alert parameters to the same value (in Mbytes). In the maximum capacity scenario, you should set this value to 250GB. Recommended is 2 or more days' space for logs.

Migration to NetScreen-Security Manager from NetScreen-Global PRO or NetScreen-Global PRO Express

Are there any configurations of NetScreen-Global PRO or NetScreen-Global PRO Express that prevent migration to NetScreen-Security Manager?

You may experience problems if your LDIF file (Global PRO configuration) is over 8MB. Problems include extremely long export times during migration, or even inability to complete the export or import process. LDIF files containing large numbers of rules in policies are more likely to cause problems.

LDIF file sizes over 2MB indicate that a RAM upgrade is needed before a successful migration can occur.

Can I install NetScreen-Security Manager on my existing NetScreen-Global PRO or NetScreen-Global PRO Express appliance?

Yes, your existing appliance may be used as part of your NetScreen-Security Manager deployment if supported by your number of devices, number of rules in policies, and device configuration sizes. The two management server components of NetScreen-Security Manager (GUI Server and Device Server) may be installed on one server or two, with your Global PRO appliance as part of this configuration.

In most cases, RAM will need to be upgraded according to the sizing guidelines and formulas above.

Installing NetScreen-Security Manager on your Global PRO or Global PRO Express appliance is recommended for smaller deployments only.

Appendix C

Profiler Performance Tuning Recommendations

This appendix provides performance tuning guidelines for running the Profiler when managing IDP standalone sensors in NetScreen-Security Manager.

Performance Tuning Recommendations

The following performance tuning recommendations are based on the number of IDP standalone sensors that you have configured to perform Profiling activities:

- Low-End Configuration (1-2 profiling devices)
- Medium-Sized Configuration (3-8 profiling devices)
- High-End Configuration (9-20 profiling devices)

Recommendations for Low-End Configurations:

Table 34 describes recommendations for optimum performance when managing 1-2 profiling devices.

Table 34: Performance Tuning Recommendations for Low-End Configurations

Component	Recommended	Value
Server Setup	GUI Server and Device Server (Profiler DB) running on the same machine	N/A
	Physical Memory Required	1 GB
	CPU	1 Fast
	Disk space reserved for Profiler	8 GB
UI System Preferences	Purge profiler database if size exceeds (in MB)	1000
	Max profiler database size after purging (in MB)	750
PostgreSQL Settings	shared_buffers	1000 (for Linux) 700 (for Solaris)
	work_mem	16384
	maintenance_work_mem	8192
	max_fsm_pages	20000
	checkpoint_segments	64
	checkpoint_timeout	600
Device Server	profilerMgr.receiver.maxParallelConns	Reduce from 3 to 1

Refer to “System Components for Improving Profiler Performance” for more information on recommended settings.

Medium-Size Configuration (3-8 IDP profiling devices):

Table 35 describes recommendations for optimum performance when managing 3-8 profiling devices.

Table 35: Performance Tuning Recommendations for Medium-Sized Configurations

Component	Recommended	Value
Server Setup	GUI Server and Device Server (Profiler DB) running on the same machine	N/A
	Physical Memory Required	2 GB
	CPU	2 Fast
	Disk space reserved for Profiler. *High end SCSI drives preferred	12 GB
UI System Preferences	Purge profiler database if size exceeds (in MB)	3000
	Max profiler database size after purging (in MB)	2200
PostgreSQL Settings	shared_buffers	32768
	work_mem	32768
	maintenance_work_mem	32768
	max_fsm_pages	200000
	checkpoint_segments	64
	checkpoint_timeout	600
Device Server	profilerMgr.receiver.maxParallelConns	Reduce from 3 to 1

Refer to “System Components for Improving Profiler Performance” for more information on recommended settings.

High end configuration (9-20 IDP profiling devices):

Table 36 describes recommendations for optimum performance when managing 9-20 profiling devices.

Table 36: Performance Tuning Recommendations for High-End Configurations

Component	Recommended	Value
Server Setup	GUI Server and Device Server (Profiler DB) running on the separate machines	N/A
	Physical Memory Required	8 GB
	CPU	4 Fast
	Disk space reserved for Profiler. *High end SCSI drives preferred	24 GB
UI System Preferences	Purge profiler database if size exceeds (in MB)	8000

Table 36: Performance Tuning Recommendations for High-End Configurations

Component	Recommended	Value
	Max profiler database size after purging (in MB)	6000
PostgreSQL Settings	shared_buffers	262143
	work_mem	512000
	maintenance_work_mem	32768
	max_fsm_pages	2000000
	checkpoint_segments	128
	checkpoint_timeout	3600

Refer to “System Components for Improving Profiler Performance” for more information on recommended settings.

System Components for Improving Profiler Performance

Additional information on recommended settings is provided for the following system components to improve the performance of the Profiler when managing IDP standalone sensors in NetScreen-Security Manager:

- User Interface (UI) System Preferences
- PostgreSQL Server
- Operating System Shared Memory Requirements
- Device Server

UI System Preferences

From the UI, use **System Preferences > Profiler Settings** to configure settings on the Profiler to improve performance. Table 37 describes settings that you can configure to improve performance from the UI.

Table 37: Profiler Settings in UI System Preferences

Parameter	Description	Default Value
DB Max Size - Purge Profiler Database if size exceeds (in MB)	A background Auto Purge is triggered if the Profiler database size exceeds this limit.	3000 MB
DB Max Size After Purge	Auto Purge attempts to bring down the Profiler database size to less than this limit.	2200 MB
Profiler Query Timeout (in seconds)	The SQL query timesout when this interval is elapsed, irrespective of whether the entire database is searched or not. In the event of a timeout, the result available so far is returned.	120 seconds

Table 37: Profiler Settings in UI System Preferences

Parameter	Description	Default Value
Hour of day to perform database optimization (local time)	Database optimization is an expensive operation. It occurs at or around the specified hour of day. It is recommended that you set this setting to an hour of the day when user activities are at a minimum, such as midnight local time. The time is displayed as local time of the NSM UI client. If you have multiple clients operating at varying time-zones, you must set this value to minimize the effect of the optimization operation.	7 GMT

PostgreSQL Server

You can also configure settings on the PostgreSQL server to improve the performance of the Profiler DB. These settings appear in the following file on the Device Server:

`$NSRROOT/DevSvr/var/pgsql/data/postgresql.conf`

Most of the changes to improve PostgreSQL performance will increase the shared memory requirement described in the next section.

Table 38 describes parameters in the postgresql.conf file that affect Profiler performance.

Table 38: PostgreSQL Server Settings

Parameter	Description	Default Value
shared_buffers	Sets the number of shared memory buffers (each 8 KB) used by the database server. Minimum is 2 X max_connections	1000 KB
work_mem	Specifies the amount of memory to be used by internal sorts and hashes before switching to temporary disk files. The value is specified in kilobytes.	16384 KB
maintenance_work_mem	Specifies the maximum amount of memory to be used in maintenance operations, such as VACUUM. The value is specified in kilobytes.	8192 KB
max_fsm_pages	Sets the maximum number of disk pages for which free space is tracked in the shared free-space map. Six bytes of shared memory are consumed for each page slot.	20000
checkpoint_segments	Maximum distance between automatic checkpoints maintained by postgresql, in log file segments.	64
checkpoint_timeout	Maximum time between automatic checkpoints, in seconds.	600 seconds

The defaults mentioned here are configured by NetScreen-Security Manager during initial installation. In some cases, the actual PostgreSQL default values are not indicated.

Operating System

When you configure the PostgreSQL server to perform better with more shared memory, the devSvrDbSvr (postmaster) process may not come up if the system does not support it. In such cases, after a failed run of devSvrDbSvr, you can identify the actual memory requirement from the following file:

```
$NSROOT/DevSvr/var/pgsql/data/psql.log file
```

The error appears as follows:

```
"Failed system call was shmget(key=5432001, size=145408000, 03600)"
```

Note that size specifies the required shared memory. You can then update the shared memory requirement.

On Solaris systems, add/update the following line in /etc/system:

```
set shmsys:shminfo_shmmax=<required shared mem>'
set shmsys:shminfo_shmmni=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256
set semsys:seminfo_semmmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmns1=32
```

On Linux systems, add/update the following line in /etc/sysctl.conf:

```
kernel.shmmax=<required shared mem>'
```

After updating the shared memory requirements, you must restart the system.

Device Server

You can also configure settings on the Device Server to improve the performance of the Profiler DB. Table 39 describes parameters in the Device Server configuration file (devSvr.cfg) that affect performance.

Table 39: Device Server Settings

Parameter	Description	Default Value
profilerMgr.printLevel	For debugging, info is most useful, but will potentially generate lots of logs.	Notice
profilerMgr.receiver.pktIntTimeoutInSec	A profiler session times out of time exceeds this configured value.	300 seconds

Table 39: Device Server Settings

Parameter	Description	Default Value
profilerMgr.receiver.saveFailedData	Profiler Data of a profiler session is stored temporarily in the folder \$NSROOT/DevSvr/var/profiler_data/ < domainId > . < deviceId > . < sessionId > . If a session completes successfully this folder is cleaned up. Otherwise, the folder is cleaned up unless this setting is 'YES'.	NO
profilerMgr.receiver.maxParallelConns	Specifies maximum number of concurrent profiler sessions.	3
profilerMgr.receiver.minPollTimeInSec	Two consecutive profiler sessions for the same device is spaced apart by at-least this interval.	300 seconds
profilerMgr.receiver.vacuumCostDelay	The length of time, in milliseconds, that the vacuum process will sleep when the vacuumCostLimit has been exceeded.	0 msec
profilerMgr.receiver.vacuumCostLimit	The accumulated cost that will cause the vacuuming process to sleep.	200 msec
profilerMgr.receiver.minVacuumInterval	Minimum time interval between two consecutive vacuums.	300 seconds
profilerMgr.receiver.performVacuumFull	If this setting is 'YES', VACUUM FULL is performed during optimization otherwise skipped.	NO
profilerMgr.receiver.optimizationWindow	This specifies the time window in hours from the 'hour to perform optimization' setting of GUI- > System Preferences- > Profiler Settings. Optimization would be triggered only during this window.	3 hours
profilerMgr.profilerQuerier.profilerQueryTimeoutInterval	A GUI query session is timed out if there is no activity for this interval.	600 seconds

NSM Generated Logs Impact on Performance

If you notice “Could not write the whole buffer to FIFO” entries in the deviceDaemon log files, it is recommended that you turn off NSM generated logs by unchecking the “New Host”, “New Protocol”, and “New Port” detected check boxes in the IDP device editor, and saving the data. Excessive messages indicating “Could not write the whole buffer to FIFO” could indicate that Device Server performance is affected by these NSM generated logs.

Index

A

adding, Device Server 41

B

bulk cli timeout 120

C

certificates

files 45, 68

transferring 45, 68

changing

default user management system runs as 110

configuration options

database backup 6

high availability 8

installing management system on same server

(typical) 6

installing management system on separate servers

(extended) 8

Statistical Report Server 7

configuring

Device Server data directory 19, 63

Device Server ID 42

HA Cluster 76–80

high availability 113–116

management system IP addresses 107

password for GUI Server connection 43

password for super user 20, 64

CPU

requirements on management system, same

server 3

requirements on management system, separate

servers 4

customer support x

D

data directory

for Device Server, described 13, 35, 57, 87

for GUI Server, described 13, 35, 57, 87

database

backup options 6

replicating 115

restoring 115

defining system parameters 12, 34, 56, 86

Demo Mode 32

Device Server

adding 41

data directory, configuring 19, 63

installing 42–45

starting 105

stopping 106

Device Server ID

configuring 42

described 36, 59, 88

disk storage

requirements on management system, same

server 3

requirements on management system, separate

servers 4

downgrading 120

E

establishing

SSH trust relationship 60

extended configuration option 8

G

GUI Server

installing 36–40

starting 105

stopping 105–106

H

HA Cluster

configuring 76–80

HA Server

starting 104

stopping 106

heartbeat communications

described 51

heartbeat links

described 57

high availability

configuring manually 113–116

installing 55–??

overview 8

I

installation

CD 2

files 3

log file for management system 25, 40, 66

log file for UI 29

package 2

installing

configuration options 5

Device Server 42–45

GUI Server 36–40

management system on same server	11–25
management system on separate servers	33–45, 55–68
management system with high availability ...	61–81
management system with high availability - separate servers	81–??
prerequisite steps	14
TFTP server on Linux	119
TFTP server on Solaris	119
UI	26–29
L	
log file	
management system install	25, 96
UI installation	29
logging in to the UI	30
logs	
restoring	113
M	
management IP address	
for GUI Server, described	13, 35, 57, 87
management system	
changing default user	110
commands	103
installation process	1
installing on same server	11–25
installing on separate servers	33–45, 55–68
restarting	104
starting	104
status	104
stopping	104
uninstalling	121
upgrading	85–97
memory requirements	
for UI	5
management system on same server	3
management system on separate servers	4
minimum system requirements	
described	3–5
for UI	4
management system	3–4
N	
network connection	
requirements for UI	5
requirements on management system, same server	3
requirements on management system, separate servers	4
O	
operating system	
requirements for management system	3
requirements for UI	5
P	
password	
super user, configuring	20, 64
Password for GUI Server connection	
configuring	43
described	36, 59, 88
patching	
Sun Solaris SSH daemon	16–17, 92–93
prerequisites before installing	14
prerequisites before upgrading	90
process	
for installing management system	1
for installing UI	2
R	
replicating	
database	115
restarting management system	104
restoring	
database	115
logs and configuration data	113
root user	
changing user that management system runs as ...	110
rsync	
using with database backup	7
running	
UI	30
UI, in Demo Mode	32
S	
SSH trust relationship	
establishing	60
starting	
Device Server	105
GUI Server	105
HA Server	104
management system manually	104
Statistical Report Server	
installing with NetScreen-Security Manager	7
stopping	
Device Server	106
GUI Server	105–106
HA Server	106
management system manually	104
Sun Solaris SSH daemon	
patching	16–17, 92–93
super user	
password, configuring	20
password, described	13, 35, 57, 87
swap space	
requirements on management system, same	

server.....	3
requirements on management system, separate	
servers.....	4
system parameters.....	12, 34, 56, 86
system update utility	
described.....	3
running.....	15-16, 91-92

T

testing	
initial HA replication.....	80
TFTP server	
installing on Linux.....	119
installing on Solaris.....	119
timeout	
bulk cli modification.....	120
typical configuration option.....	6

U

UI	
installation process.....	2
installing.....	26-29
running.....	30
uninstalling.....	123
upgrading.....	97
uninstalling	
UI.....	123
upgrading	
management system.....	85-97
management system on separate servers.....	99
prerequisite steps.....	90
UI.....	97

V

validating	
database recovery.....	116
management system installation.....	30
management system status.....	26, 45, 67, 96
management system upgrade.....	97
viewing management system commands.....	103

