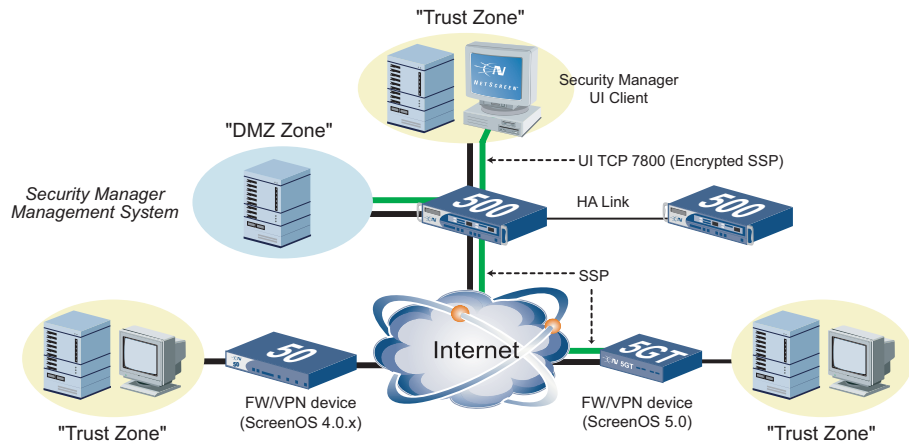




## NetScreen-Security Manager Getting Started Guide

Use the instructions in this Getting Started Guide to help you install a basic working configuration of NetScreen-Security Manager 2004. To do this, you need to install the Security Manager management system on a single server running either Red Hat Linux 8.0 or 9.0 or Solaris 8 or 9, and a User Interface (UI) client on a Windows-based PC. You can then connect the UI client to the management system. For more detailed information about installing Security Manager, or if you prefer to install the management system on two servers for increased performance, refer to the NetScreen-Security Manager 2004 Installer's Guide.



**Example topology of a typical NetScreen-Security Manager 2004 deployment.**



### Installation CD Contents

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

File / Folder	Description
<b>nsm2004_ui_win_x86.exe</b>	Installer for the Security Manager UI client.
<b>nsm2004_servers_linux_x86.sh</b>	Installer for the Security Manager management system for Linux.
<b>nsm2004_servers_sol_sparc.sh</b>	Installer for the Security Manager management system for Solaris.
<b>nsm2004_gpexport_sol_sparc.sh</b>	Installer for Global PRO export utility used to migrate data from Global PRO/Express into Security Manager.
<b>system_update_linux_x86.tar</b>	Linux system update utility. Linux users may need this file to update the RPM package, for certain versions of Linux (see Page 2, Step 4).
<b>/docs</b>	Folder containing all product documentation in .pdf format.



## Prerequisite Steps

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

### Step 1

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

```
su -
```

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

### Step 2

Partition your drives for sufficient disk space to accommodate your planned data requirements. (See *Installer's Guide* for more information.)

### Step 3

Create a normal user called "nsm". Create a group called "nsm", with the user nsm as the only member.

You can do this in Linux, by typing the following command:

```
useradd nsm
```

You can do this in Solaris, by typing the following commands:

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

The GUI Server and Device Server processes of the management system run as this user by default. It is recommended that you restrict this user account, so that the server runs as a non-privileged user.

### Step 4

If you are installing the management system on Linux, verify that you are running the correct version of RPM by running the following command:

```
rpm -qi rpm
```

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

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

If you are not running the correct version of RPM for the version of Linux that you are using, you must install it before proceeding. You can upgrade your version of RPM using the following procedure.

Untar the `system_update_linux_x86.tar` from the Installation CD (example command shown), or from the directory where it is saved, to a suitable directory on the server (/tmp is suggested).  
**tar xvf /mnt/cdrom/system\_update\_linux\_x86.tar /tmp**

Navigate to the resulting directory, `systemupdate`, where the update script is stored.

```
cd /tmp/systemupdate
```

Execute the below update script:

```
./update.sh
```

Let the script run to completion. This may take up to 20 minutes depending on the number of packages that must be installed.



## Installing the Management System Software

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

### Step 1

Load the installer software listed below onto the server which will function as the management system. The installers can be run directly from the NetScreen-Security Manager Installation CD, or copied to the server from the Installation CD, or downloaded from the NetScreen Customer Services Online website.

For Linux:

```
nsm2004_servers_linux_x86.sh
```

For Solaris:

```
nsm2004_servers_sol_sparc.sh
```

### Step 2

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

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

```
sh nsm2004_servers_linux_x86.sh
```

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

```
sh nsm2004_servers_sol_sparc.sh
```

The installation begins automatically.

### Step 3

Enter selection 3 to specify that you want to install the Device Server and GUI Server. The script then prompts you to specify where you want to store the Device Server data files.

### Step 4

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

### Step 5

Enter the management IP address for the server. This should be the same IP address of the serv-

er that you are installing on. It sets the GUI Server port to 7800 by default.

### Step 6

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

Enter a text string for the password (minimum length of five characters, case-sensitive). Enter the password again for verification. Make a note of the password that you have set for the super user account. You will need this when you first login to the UI.

### Step 7

The script next prompts you if you want to start both servers once it has completed installation. Enter y and then press ENTER to start both servers once the installer has completed the installation process.

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

### Step 8

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

The installation proceeds automatically. It runs for several minutes, and then exits. After installation is complete, the installer displays additional important information - take note of this for later use.

## 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 Device Server and GUI Server to confirm that all services are up and running.

### To check the status of the GUI Server:

Navigate to the GUI Server bin subdirectory (i.e., /usr/netscreen/GuiSvr/bin) and run the following command:

```
sh guiSvr.sh status
```

### To check the status of the Device Server:

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

```
sh devSvr.sh status
```



## Installing a TFTP Server - Linux

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

Before installing the TFTP server on your Red Hat Linux server, you should first check to see if it is already installed. To verify if the TFTP server is already installed on your Linux server, run the following command:

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

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

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

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

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

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

### To configure and enable the TFTP server on Linux:

#### Step 1

Open the /etc/xinetd.d/tftp file in any text editor.

#### Step 2

Edit the lines that start with "server\_args" and "disable" so that they appear as in the following example file:

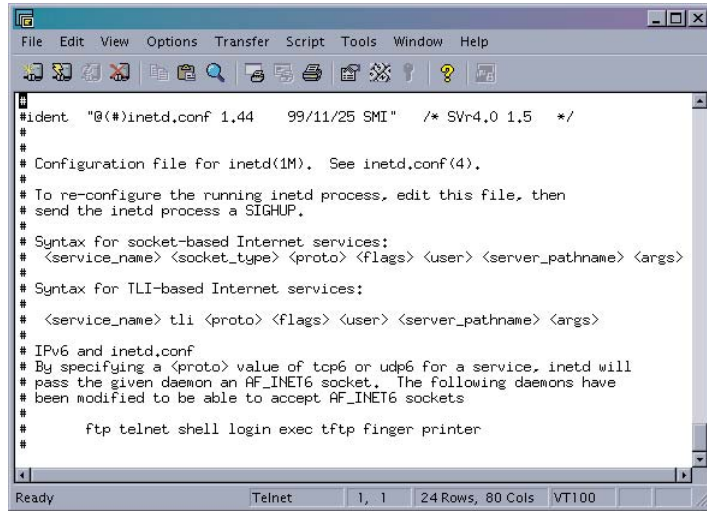
```
service tftp
{
    socket_type = dgram
    protocol = udp
    wait = yes
    user = root
    server = /usr/sbin/in.tftpd
    server_args = -s /usr/netscreen/DevSvr/var/cache
    disable = no
    per_source = 11
    cps = 100 2
}
```

#### Step 3

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

```
service xinetd restart
```

This completes the procedures required to install the Security Manager management system on Red Hat Linux. You can now proceed to install the User Interface (continue on Page 6).



```

ident  "@(#)inetd.conf 1.44  99/11/25 SMI" /* SVr4.0 1.5 */
#
#
# Configuration file for inetd(1M).  See inetd.conf(4).
# To re-configure the running inetd process, edit this file, then
# send the inetd process a SIGHUP.
# Syntax for socket-based Internet services:
# <service_name> <socket_type> <proto> <flags> <user> <server_pathname> <args>
#
# Syntax for TLI-based Internet services:
#
# <service_name> tli <proto> <flags> <user> <server_pathname> <args>
#
# IPv6 and inetd.conf
# By specifying a <proto> value of tcp6 or udp6 for a service, inetd will
# pass the given daemon an AF_INET6 socket.  The following daemons have
# been modified to be able to accept AF_INET6 sockets
#
#      ftp telnet shell login exec tftp finger printer
#

```



## Installing a TFTP Server - Solaris

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

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

### To configure and enable the TFTP service on Solaris:

#### Step 1

Open the `/etc/inetd.conf` file in any text editor.

#### Step 2

Edit the line that begins with the word "tftp" or "#tftp" so that it appears as follows:

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

#### Step 3

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

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

This completes the procedures required to install the Security Manager management system on Solaris. You can now proceed to install the User Interface.



## Installing the User Interface

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

### Step 1

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

### Step 2

Download the UI installer (nsm2004\_ui\_win\_x86.exe) from the Security Manager installation CD, or from the NetScreen Customer Service Online website, to the computer where you are installing the UI.

### Step 3

Run the UI installer. An Introduction screen for the InstallAnywhere wizard appears. Follow the wizard through all the steps required to configure and install the UI.

### Step 4

Click Next to continue the installation. The License Agreement screen appears. Review the license agreement. If you choose to accept the terms of the license agreement, click the button next to the appropriate statement. If you choose to not accept the terms of the license agreement, you will not be able to proceed with the installation.

### Step 5

If you accepted the License Agreement, the Choose Install Folder screen appears. Click Next to accept the default install folder and continue. To specify a new or different folder location, click Choose....

Note: The installer saves the UI software files in C:\Program Files\NetScreen-Security Manager by default.

The Choose Shortcut Folder appears.

### Step 6

Select where you would like to create the Security Manager product icons. Click Next to continue. The Pre-Installation Summary screen appears.

### Step 7

When the installation is complete, a screen indicating "Install Complete" appears. Click Done to exit the installation program.



## Connecting the UI to the Management System

Once you have completed installing the UI, you can launch the application and verify that you can connect to the management system. The first time you open the UI, you need to specify the host name (or IP address) of the management system that you want to connect to, a user name, and password. The default user name for new installations is `super`; the default password is the password you specified when configuring the management system. *Note: Passwords and user names are case-sensitive.*

### Step 1

Run the Security Manager UI (from the Start menu, select Programs>NetScreen-Security Manager>NetScreen-Security Manager or double-click on the Security Manager icon on your desktop). The Login window appears.

### Step 2

Login to management system.

- a) Verify that the user name in the Login field provided is the initial admin user called "super". If not, enter "super" in the Login field.

- b) Enter the password that you specified when you installed the management system in the Password field provided.
- c) Enter the IP address you assigned to the GUI Server in the Server field provided. If you have enabled DNS-lookup, you can enter the host name instead of the IP address.

### Step 3

Click OK. The UI appears indicating that the installation was successful.

*To receive important news on product updates and to gain access to online product support, please visit our website at [www.netscreen.com](http://www.netscreen.com) and register your product.*

Copyright © 2003 NetScreen Technologies Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, NetScreen-Security Manager, NetScreen-Remote, NetScreen ScreenOS and the NetScreen logo are trademarks and registered trademarks of NetScreen Technologies, Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective companies.