SunScreen™ 3.1 Lite Installation Guide

For the Solaris Operating Environment

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part No. 806-4970-05
June 2000, Revision A

Please
Recycle

Contents

Figures

Preface

This *SunScreen Installation Guide* provides all information necessary to install the SunScreen firewall from the Solaris 8 Early Access CD-ROM onto your network.

Who Should Use This Book

This manual is intended for SunScreen system administrators responsible for the operation, support, and maintenance of network security. It is assumed that you are familiar with UNIX system administration and TCP/IP networking concepts, and with your network topology.

How This Guide Is Organized

The *SunScreen Installation Guide* is organized into the following chapters:

Chapter 1, “Installation Overview” on page 1, introduces SunScreen concepts including product architecture, hardware, operating system, and browser requirements.

Chapter 2, “Installation Considerations” on page 11, covers choosing the level of security for SunScreen, and preparing for installation with either local or remote administration.

Chapter 3, “Installing Lite With Local Administration” on page 25, contains instructions for installing SunScreen in routing mode with local administration.

Chapter 4, “Installing Lite With Remote Administration” on page 37, contains instructions for installing a remotely administered SunScreen using self-generated or issued certificates.

Chapter 6 “Removing SunScreen” on page 61, explains how to remove the SunScreen 3.1 software.

Appendix A, “Command Line Installation” on page 63, shows examples of using the command line to install SunScreen 3.1 in routing mode with remote administration or in stealth mode.

Appendix B, “Upgrading Cryptography Modules” on page 77, explains how to add additional Cryptography modules to your SKIP configuration.

Ordering Sun Documents

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc. for a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at `http://www.fatbrain.com/doc`

Accessing Sun Documentation Online

The `docs.sun.com` Web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`.

Getting Support for SunScreen Products

If you require technical support, contact your Sun sales representative or Sun Authorized Reseller. See `http://sun.com/service/contacting/index.html` for information on contacting Sun and `http://internet.central.sun.com/service/support/index.html` for information on Sun’s support Services.

What Typographic Conventions Mean

The following table describes the type changes and symbols used in this book.

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. *machine_name%* `You have mail.` Type `su -` to become superuser.
`AaBbCc123`	What you type, contrasted with on-screen computer output	*machine_name%* **`su -`** Password:
AaBbCc123	Command-line placeholder; replace with a real name or value	To delete a file, type `rm` *filename.*
AaBbCcl123	Book titles, new words or terms, or emphasized words	Read Chapter 6 in *User's Guide.* These are called *class* options. You *must* be root to do this.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

Related Books and Publications

The following books may be useful or interesting when installing the SunScreen:

- *Applied Cryptography*
  Bruce Schneier,
  John Wiley & Sons, 1996, 2nd edition,
  ISBN 0-471-12845-7
- *Building Internet Firewalls*
  D. Brent Chapman and Elizabeth D. Zwicky
  O'Reilly &Associates, 1995, ISBN 1-56592-124-0
- *Computer Security Policies and SunScreen Firewalls*
  Kathryn M. Walker and Linda Croswhite Cavanaugh
  Sun Microsystems Press, 1998, ISSBN 0-13-096015-0
- *Firewalls and Internet Security*
  Bill Cheswick and Steve Bellovin
  Addison-Wesley, 1994, ISBN 0-201-63357-4
- *Handbook of Computer-Communications Standards*
  Volume 3: The TCP/IP Protocol Suite
  William Stallings, Macmillan, 1990
- *Internetworking with TCP/IP, Volume 1*
  Douglas E. Comer, Prentice Hall, 1995, ISBN 0-13-216987-8
- *Network and Internetwork Security Principles and Practice*
  William Stallings, Prentice Hall, 1995, ISBN 0-02-415483-0
- *Practical UNIX and Internet Security*
  Simson Garfinkel and Gene Spafford, O'Reilly & Associates, 1996, 2nd edition,
  ISBN 1-56592-148-8
- *TCP/IP Illustrated, Volume 1 The Protocols*
  W. Richard Stevens, Addison-Wesley, 1994,
  ISBN 0-201-63346-9
- *TCP/IP Network Administration*
  Craig Hunt, O'Reilly & Associates, 1992
- *Network Security*
  Charlie Kaufman, Radia Perlman, and Mike Speciner
  Prentice Hall, 1995
- *SKIP IP-Level Cryptography* [http://skip.incog.com/]
  Sun Software and Networking Security [http://www.sun.com/security]

CHAPTER 1

Installation Overview

This chapter introduces SunScreen installation concepts.

Topics covered include:

- What is SunScreen?
- Operating the firewall in routing mode
- Before installing SunScreen
- Security issues
- Software and hardware requirements
- Operating system package requirements
- Additional requirements and restrictions
- Web browser requirements

What is SunScreen?

SunScreen is a software security solution, which is installed on a Solaris®-based machine. It lets companies connect their departmental networks to public internetworks securely. Depending on how you install it, SunScreen can function as a firewall and router for hosts on the network it protects.

The Screen is the firewall responsible for screening packets. You use an Administration Station to define the objects and rules that form the security policy and administer the Screen. The number of Screens and Administration Stations depends on your site's network topology and security policies. You can install all of SunScreen on a single machine (local administration) or you can put the Administration software and the Screen software on different machines (remote administration).

You need a Screen at every point in the network where you want to restrict access. In the strictest sense, you need one Screen for each point in the network that has direct public access (usually one per site). One Administration Station can manage multiple Screens, although you can install more Administration Stations for redundancy and ease of access. Encryption and authentication protects access and limits management of a Screen to an authorized Administration Station.

Local Administration

With Local administration, you administer the Screen on the Screen itself (as shown in FIGURE 1-1.) Local administration does not require an encrypted connection as no network traffic is generated.

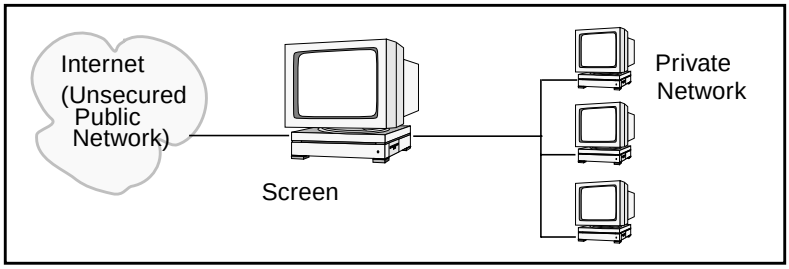

FIGURE 1-1 Example of a Locally Administered Screen

Remote Administration

With Remote administration, you use a separate machine called an Administration Station to administer the Screen (as shown in FIGURE 1-2.) Remote administration uses encrypted communication (using SKIP) between the Screen and Administration Station so the information about the security policy in place on the Screen can not be obtained by others. It is also possible to set up remote administration without using encryption between the Administration Station and the Screen. You should only use this feature when the network between the two components is secured as in the case where the Administration Station is behind the firewall.

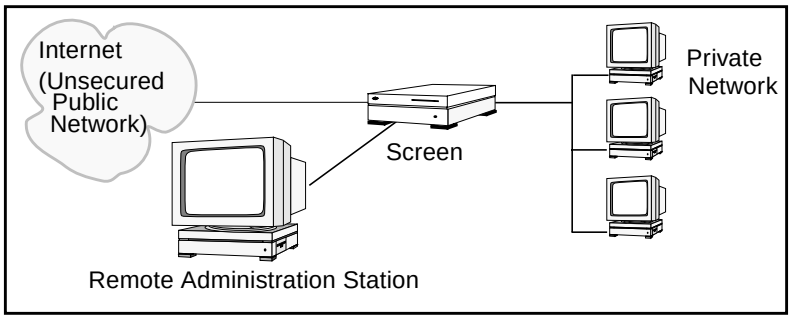

FIGURE 1-2 Example of a Remotely Administered Screen

Routing Mode

This Lite version of SunScreen 3.1 only operates in Routing mode (where the Screen performs routing as well as firewall functions).

Typically, you operate the Screen in Routing mode if you need a machine to act both as a router and a firewall. In this mode, you need at least two exposed IP interfaces, and a hop visible to `traceroute` and other network utilities.

Be aware of the following considerations when operating in Routing mode:

- The existing Solaris machine must be acting as a router. The Screen uses Solaris to provide IP routing.
- The Screen makes use of the Solaris IP stack on the filtering interfaces, so it does not possess stealth characteristics.
- You must divide up different networks as you would with any router.
- The addition of a SunScreen to your network may require re-numbering IP addresses on your hosts (if you did not already have a router where your SunScreen is being placed.)

Before You Install

Before you install SunScreen, you should complete the following tasks:

- Be acquainted with these documents:
  - *SunScreen Release Notes*

- *SunScreen SKIP 1.5.1 User's Guide*

- Ensure that the system that is to run SunScreen is secure—consider reinstalling the Solaris operating environment from CD-ROM to ensure that it has not been altered.
- If you are using issued keys and certificates, make sure a set of is available for each host.

After installing SunScreen, you are ready to set up and implement the security policy for your network. For instructions on administering your SunScreen, refer to the *SunScreen Administration Guide* for detailed examples of SunScreen configurations, please see the *SunScreen Configuration Examples* manual.

Upgrading to SunScreen

Upgrading to this Lite version of SunScreen 3.1 from previous versions of SunScreen EFS, SPF-200, or Firewall-1 is not supported. The Full version of SunScreen 3.1 will support these upgrades.

Security Issues

The machines that are used as gateways, or that are in vulnerable positions on the network, should have only the minimum Solaris packages installed. This action reduces the number of potentially exploitable applications.

Software and Hardware Requirements

TABLE 1-1 lists the minimum hardware and operating system requirements for installing SunScreen.

TABLE 1-1 SunScreen Installation Requirements

Requirement	Description
Operating Environment	• Solaris 8 (**with IPv4 only**) operating environment for SPARC™ and Intel platforms. • Requires a Java-enabled Web browser compliant with JDK™ 1.1.3 or later.
Hardware	All SPARC, UltraSPARC, and Intel platforms supported by the Solaris 8 operating environment.
Disk space	Minimum of 1 Gbyte. This space is needed to support the Solaris operating environment, the SunScreen product and sufficient space for storing of packet logs. SunScreen requirements alone are approximately 300 Mbytes.
Memory	• Administration Station: Minimum of 32-Mbytes, 64-Mbytes *strongly* recommended. • Screen: Minimum of 32–Mbytes.
Network interfaces	1. For SPARC and UltraSPARC systems in Routing mode: • 10 Mbps or 100 Mbps Ethernet interfaces (`le`, `qe`, `hme`, `be`, `qfe`) • Gigabit Ethernet interfaces • Token Ring interfaces • ATM (155 and 622 Mbps in LAN emulation mode or Classic IP mode) • FDDI, or PCI-based Ethernet cards. 2. For Intel-based systems: 10 Mbps or 100 Mbps Ethernet interfaces (`dnet`, `elxl`). See supported devices listed at: `http://access1.sun.com/drivers/hcl/hcl.html`
Media	CD-ROM drive (also a diskette drive if using issued certificates).

Operating System Package Requirements

You should ensure that the required Solaris packages reside on both the Screen and the Administration Station.

Screen Solaris Packages

If you do not plan on using the GUI on your Screen (either because you are doing Remote Administration or you have chosen to use only the command line interface for administration) you will only need to install the Core distribution of Solaris as well as the packages listed in this section.

Note – If you only install the Core Distribution of Solaris, you will either have to change your DISPLAY variable for using the installer to a machine with a windowing system or install using the command line installation procedure described in "Command Line Installation" on page 63

If you plan on using the GUI on your Screen itself, you will need to install the End User Distribution of Solaris, as well as the packages listed in this section.

TABLE 1-2 Screen Solaris Packages

Type of Package	Package Name	Description
system	SUNWeuluf	TF-8 L10N For Language Environment User Files
system	SUNWjvjit	Java JIT compiler
system	SUNWjvrt	JavaVM run time environment
system	SUNWlibC	SPARCompilers Bundled libC
system	SUNWlibms	SPARCompilers Bundled shared libm
system	SUNWsprot	SPARCompilers Bundled tools
system	SUNWtoo	Programming Tools

TABLE 1-2 Screen Solaris Packages

system	SUNWvolr	Volume Management (Root)
system	SUNWvolu	Volume Management (Usr)
system	SUNWxwice	ICE components
system	SUNWxwplt	X Window System platform software
system	SUNWxwrtl	X Window System & Graphics Runtime Library Links
system	SUNWmfrun	Motif RunTime Kit
system	SUNWloc	System Localization
system	SUNWdoc	Documentation Tools

Administration Station Solaris Packages

If you will be using a remote administration station, add the following packages to the Administration Station from your Solaris CD, if not already on your system:

Note – In addition to the patches provide by SunScreen, make sure you install all recommended security patches available for your operating environment. For security reasons,you should always keep your operating environment up to date with available patches.

TABLE 1-3 Administration Station Solaris Packages

Type of Package	Package Name	Description
system	SUNWjvrt	JavaVM run time environment
system	SUNWmfrun	Motif RunTime Kit
system	SUNWxwplt	X Window System Platform software

Additional Requirements and Restrictions

- SunScreen only supports IPv4 in the Solaris 8 operating environment.
- The Screen can support up to 2 network interfaces at one time.
- The SunScreen CD includes the SunScreen™ SKIP for Solaris software. The PC version of SKIP is available separately or as part of the Secure Net bundle.
- A remote Administration Station can connect directly to a Screen only through an Ethernet local area network (LAN) or a Fiber Distributed Data Interface (FDDI). An Administration Station can connect to the Screen by an Asynchronous Transfer Mode (ATM) or Token Ring LAN, but only after it is connected directly to the network by way of an Ethernet or FDDI connection first.
- Configure all network interfaces that will be used. See the documentation accompanying the Solaris operating environment, if needed.

Web Browser Requirements

SunScreen allows any machine with a Java-enabled web browser compliant with JDK 1.1.3 or later to function as as an Administration Station. But, the version of the JVM or plugin you are using with the browser dictates the operations you are able to perform on the Administration Station. For example, using any of the following browsers allows you to look at status information, logs, and policy configurations. However, some of the browser configurations do not support local file access.

To do mangement operations that require local disk access (like saving logs), you need to use the 1.1.2 version of the Java plugin that supports local file access.

Browsers With Local File Access

The following Web browsers support local file access using the required Java Plugin. SunScreen Lite provides the required Java plug-in (version 1.1.2) as part of its distribution. The plugin is located in the directory `javaplugins`.To install it, see "To Install the Solaris 8 Required Java Plugin" on page 9:

- Netscape Navigator™ 4.x with the Java™ plug-in.
- Internet Explorer (IE) 4.x with the Java plug-in on Windows 95/98 or NT only.

- HotJava Browser

Note – IE 5.0 with its own JVM, this configuration can read or write files but is not a supported configuration.

Browsers Without Local File Access

- Netscape Navigator 4.5, or higher, with its own Java VM has the limitation that you can not read or write files.
- IE 4.01 with its own JVM has the limitation that you can not read or write files.

Note – You can find compliant versions of the Netscape Navigator and HotJava browsers on the Solaris 8 Early Access CD in the SunScreen directory in package format.

Netscape Navigator on Solaris 8

The Netscape Navigator default Java plugin provided with Solaris 8 is not compatible with the SunScreen Aministration applet. To save log files and load certificates using Netscape Navigator 4.5 or 4.7, you must install the older version of the Java plugin that is included on the CD-ROM or use the HotJava browser (also included).

This procedure shows how to install the Java plugin 1.1.2, save the `identitydb.obj` file, and set the `NPX_PLUGIN_PATH` environment variable.

▼ To Install the Solaris 8 Required Java Plugin

1. **Ensure that the Solaris 8 early Access CD-ROM is inserted in the CD-ROM drive.**
2. **Navigate down the SunScreen directory structure to the plugin location**
3. **Install the Java plugin by typing:**

```
% cp plugin-112i-solsparc.sh /tmp
% cd /tmp
% sh plugin-112i-solsparc.sh
```

4. **Save the identitydb.obj file by typing:**

```
% cd /opt/SUNWicg/SunScreen/admin/htdocs/plugin/plugins/
% cp identitydb.obj $HOME
% cd
```

5. **Set the environment variable if using sh or ksh by typing:**

```
$ NPX_PLUGIN_PATH=$HOME/.netscape/plugins:$NPX_PLUGIN_PATH
$ export NPX_PLUGIN_PATH
or if using csh:
% setenv NPX_PLUGIN_PATH $HOME/.netscape/plugins:$NPX_PLUGIN_PATH
```

6. **Run the Netscape browser and use the URL for the plugin version of the GUI:**

```
 % netscape http://localhost:3852/plugin &
```

CHAPTER 2

Installation Considerations

This chapter describes the issues you should consider before installing SunScreen.

These issues include:

- Determining your security policy
- Mapping out your network configuration
- Deciding on your initial level of security
- Choosing which interfaces to use

Before installing, review the *SunScreen Release Notes* for the latest information about this product.

Determining Your Security Policy

Before installing the SunScreen software, you should first determine your network security policy. For a more thorough discussion of this topic, we suggest you read *Computer Security Policies and SunScreen Firewalls* by Kathryn M. Walker and Linda Croswhite Cavanaugh. Additional resources are listed in the Preface.

In brief, considerations when creating a security policy are:

- what services do employees need to access?
- what services do customers need to access?
- will you allow Internet access, and if so, what services do users need to access?
- what type of threat are you trying to protect your company from?
- Do you need to use Network Address Translation (NAT)?

Mapping Your Network Configuration

Prior to installing SunScreen, you should make a map of your network. This will help identify any potential security problems inherent in the way the network is currently connected. A diagram of your network will aid installation and should include:

- Routers to the Internet
- FTP, WWW or TELNET servers
- Application relay servers
- Remote networks
- Internal subnetworks

Deciding on Your Initial Security Level

You must determine your initial level of security. You have three possible security levels to choose. Each security level corresponds to a different set of network services permitted to, from, and through the Screen. If you are in doubt about which security level to select for the `Initial` configuration, use a more permissive security mode. You can always reconfigure it to be more secure by changing the rules using the Administration GUI.

Note – If you only install the Core Distribution of Solaris, you will either have to change your DISPLAY variable for using the installer to a machine with a windowing system or install using the command line installation procedure described in “Command Line Installation” on page 63

Security Levels

The security levels are:

- *Restrictive*—This level of security denies all traffic to, from, and through the Screen, except encrypted administration traffic. This level is best for deploying the Screen in a hostile network environment. It requires that static routing and the naming service have been configured on the host (that is, names must be resolved by means of a local `hosts` file).
- *Secure*—This level of security denies all traffic to and through the Screen, except encrypted administration traffic. It allows common services (like NFS) *from* the Screen, naming service selection (such as, DNS and NIS), and routing (RIP). This level is a good starting point to get a Screen up and running on a friendly network, where the Screen may not be a stand-alone machine and may depend on NIS, DNS, or NFS to function properly.
- *Permissive*—This level allows the same traffic as the Secure level and also allows inbound connections to the Screen itself and allows all traffic through the Screen. This security level is appropriate for installing the Screen on a machine that has multiple network interfaces and is acting as a router, or on a machine that is acting as a server (for example, for NFS, NIS, or HTTP).

Naming Services

You must also choose which naming service to use. You may choose one (NIS or DNS), both (NIS and DNS), or no naming service. Selection of NIS, DNS, or both NIS and DNS allows the name service packets to pass to the screen. To use a local host file, deselect both services.

Worksheets for Defining Security Policies

Here are directions and worksheets to help you analyze and define your company's security policy requirements. Once established, SunScreen controls access to the network through a set of rules and interface definitions that are created in the administration GUI. The information you accumulate in this section will be used to define your policies. See the *SunScreen Reference* manual for more information. You can also find some useful examples in the *SunScreen Configuration Examples* manual.

To begin the process, create a group of all the IP addresses that SunScreen needs to know. SunScreen identifies network elements—network, subnetworks, and individual hosts—by IP address. Before you can define the rule, you must define all the elements or parts that make up the rule. Several types of addresses need to be defined in SunScreen.

Creating Service Groups

Use TABLE 2-1 to assist you in creating service groups that use any combination of the individual network services. A useful group to define at many sites is an "internet services" group, consisting of public services, such as FTP, e-mail, and WWW. You might want to familiarize yourself with the set of pre-defined network services to avoid creating unnecessary duplicates.

TABLE 2-1 Services or Service Groups

Name	Definition

Addresses

SunScreen uses IP addresses to define the network elements that make up the configuration. These addresses are then used in defining the Screen's network interfaces and as the source and destination addresses for rules and NAT.

The address can be for a single computer, or it can be for a whole network or subnetwork. Additionally, addresses (individual and network) can be grouped together to form an address group. SunScreen allows you to define address groups that specifically *i*nclude or exclude other defined addresses (single IP hosts, ranges, or groups).

Table 2-2 Address Explanations

Host addresses	For individual elements, such as the router and individual computers, you need to know the IP address, in standard dotted Internet-address notation (w.x.y.z format), and the name of the host.
Address Ranges	For networks and subnetworks, you need to know the beginning and ending addresses of the network or subnetwork, both in standard dotted Internet-address notation (w.x.y.z format).
Address Groups	Groups of host addresses, network addresses, and other address groups can be combined to form logical groups of addresses that can then be manipulated as a *single* element. Groups may be inclusive or exclusive or a combination of both, but may not be cyclic as in cases where dress Group "A" includes (references) Address Group "B" which in turn includes Address Group "A".

The FIGURE 2-1 shows an example of various types of addresses and can be used as a reference when completing your own network map.

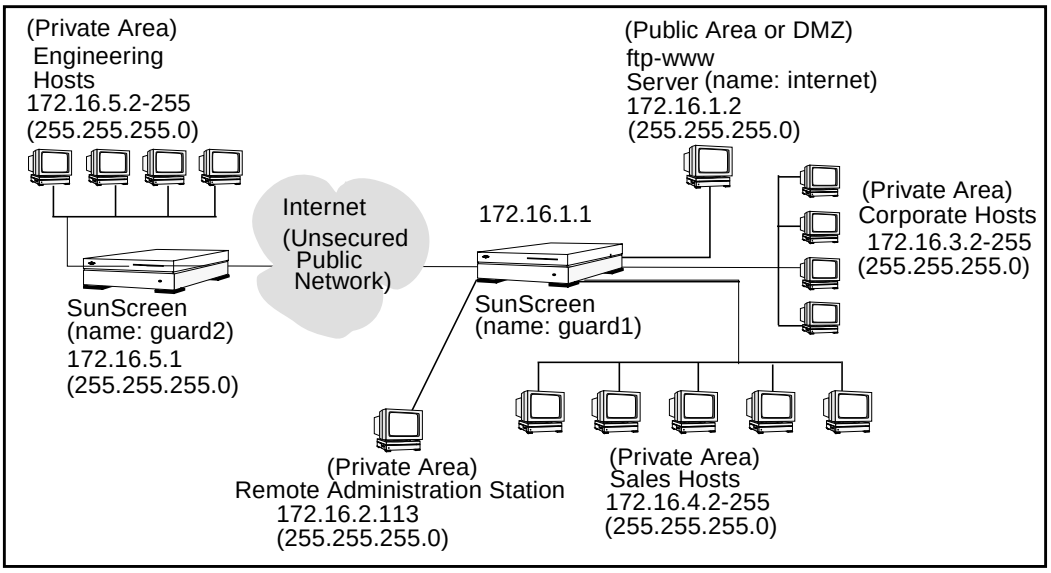

FIGURE 2-1 Example of a Network Map

In this figure, the following examples of different types of addresses can be seen:

- The ftp-www server is an example of a *single* host address (172.16.1.2).
- Corporate, sales, and the engineering hosts are examples of *ranges* of addresses. For example, the range of addresses in the engineering hosts, 172.16.5.2 with the netmask 255.255.255.0, is defined as a range of addresses from 171.16.5.2 to 172.16.5.255.

The Internet is an example of a *group* of addresses, in this case defined as *all*. The ftp-www server is an example of a single address. The corporate, sales, and engineering hosts are examples of ranges of addresses.

The following worksheets help you organize the IP addresses. Expand them as necessary. Group the IP addresses and names for the following network elements:

- A single computer, or a whole network or subnetwork.
- Additionally, addresses (individual and network) can be grouped together to form an address group.

Rules are used to control access to your computer network and to control encryption for access to your data. In preparing to implement rules, you have:

- Determined the overall services that are available on your network
- Determined the services available to a particular user or host and user groups over particular IP addresses
- Determined the correct action for the service and addresses for that user or host.

Note – By default, the Screen drops any packets that do not specifically match a rule. This makes it easier to create rules, since you only have to write a rule for the services you want to pass.

TABLE 2-3 Host Addresses

Name	IP Address

TABLE 2-4 Address Ranges

Name	Address	
	Beginning	Ending

TABLE 2-5 Address Group

Name	Address	
	Include	Exclude

NAT

NAT enables you to map from unregistered addresses to registered addresses allocated by your Internet service provider (ISP). The NAT function of SunScreen uses this translation to replace the IP addresses in a packet with other IP addresses. This allows you to use unregistered addresses to number your internal networks and hosts and yet have full connectivity to the Internet. With this Lite version, you can have up to 10 internal addresses that use NAT.

TABLE 2-6 NAT Map Table

Type	Address		Translated Address	
Static/Dynamic	Source	Destination	Source	Destination

Interfaces

This Lite version of SunScreen 3.1 only supports 2 routing interfaces.

TABLE 2-7 Screen's Interfaces

Type	Interface Name	Group Address	Logging Details		
			SNMP Alert	Logging	ICMP Reject

Administration Stations

Use this table to collect the information need to add Administration Stations.

TABLE 2-8 Administration Stations

Name of Certificate associated with Admin Station	Address of Admin Station	Key Algorithm	Data Algorithm	MAC Algorithm	Admin User Name	Access Level

Rules

Use the Rules worksheet to organize the individual rules you want to use. Space is provided for you to create your own service groups. Make copies of the worksheet, as necessary.

A filled-in sample of worksheet with the requisite services that you may want for a particular network.on and sales networks is shown in worksheet TABLE 2-10.

TABLE 2-9 Rules

Ordered Rule Index	Service or Service Group	Source Address	Destination Address	Action	Encryption	User or Groups of Users *Optional*	Time of Day *Optional*	Screen *Optional*

TABLE 2-10 Sample for “Rules” Worksheet

Ordered Rule Index	Service or Service Group	Source Address(es)	Destination Address(es)	Action	Encryption
1	ftp	Internal-net	Internet	ALLOW	NONE
2	ftp	*	ftp Server	ALLOW	NONE
3	ftp	Internet	Internal-net	DENY	NONE

Four Action Types

This section lists the available action types you use to construct ordered rules.

- ALLOW options:
  - LOG_NONE
  - LOG_SUMMARY
  - LOG_DETAIL
  - SNMP_NONE
  - SNMP

- DENY options:
  - LOG_NONE
  - LOG_SUMMARY
  - LOG_DETAIL
  - SNMP_NONE
  - SNMP
  - ICMP_NONE
  - ICMP_NET_UNREACHABLE
  - ICMP_HOST_UNREACHABLE
  - ICMP_PORT_UNREACHABLE
  - ICMP_NET_FORBIDDEN
  - ICMP_HOST_FORBIDDEN

- ENCRYPT options:
  - NONE
  - SKIP_Version_1 (for connection to a SunScreen SPF-100 *only*)
  - You must decide on:

  Key Algorithm list (depends on the SKIP version chosen: Domestic or Global)

  Data Algorithm list (depends on the SKIP version chosen: Domestic or Global)

  SKIP_Version_2 (for connection to all other SKIP-enabled devices)
  (Optional: Tunnel addresses are allowed.)

  You must decide on:
  - From Encryptor list
  - To Encryptor list
  - Key Algorithm list (depends on the SKIP version chosen: Domestic or Global)
  - Data Algorithm list (depends on the SKIP version chosen: Domestic or Global)

    - MAC Algorithm list (NONE or MD5)

- SECURE options:
    - This option is selected only when forming VPN rules using the VPN gateways previously defined

After you define and map out your network and decide on your policy, you use data objects, such as services and addresses, to configure SunScreen with the policy rules to control access to your network. When you installed SunScreen, you created a Policy named “Initial,” is created so you can connect to the Policy Edit page and build your own Security Policies.

CHAPTER 3

Installing Lite With Local Administration

This chapter explains how to install SunScreen in routing mode with local administration. In this configuration, the software is installed on a single machine and does not need to encrypt administration traffic. Use this installation method if you need SunScreen to function both as a router and a firewall and wish to administer on the firewall.

Topics covered include:

- Installation of the software on a single machine
- Setting of the PATH and installing SKIP upgrades
- Launching the Administration GUI

Before You Begin

Prior to installation, make sure the machine is performing properly as a router. Do not begin this procedure until you have read the information in Chapter 2.

Caution – The installation procedure requires that you reboot the machine when indicated. Do not perform any other tasks on the machine while installing the software, as a delay in rebooting the machine may affect installation and cause your system to hang.

▼ To Install SunScreen

The installation wizard guides you through this procedure. You must be on the machine you are installing on in order to use the wizard and must not telnet to the machine.

Note – This chapter documents a default installation so you should accept all defaults as given on the screens. If you want a different choice on any of the screens, quit the installation wizard and restart it using the appropriate installation procedure; see the Table of Contents to locate the types of installations.

---

7. **Insert the Solaris Early Access into the CD-ROM drive.**

   A File Manager screen appears listing the CD contents. Navigate down to the SunScreen directory.

8. **Start the installation by double-clicking on the SunScreen installer icon.**

   Enter the root password for your system when prompted. The Screen Installer's Welcome window appears (FIGURE 3-1).

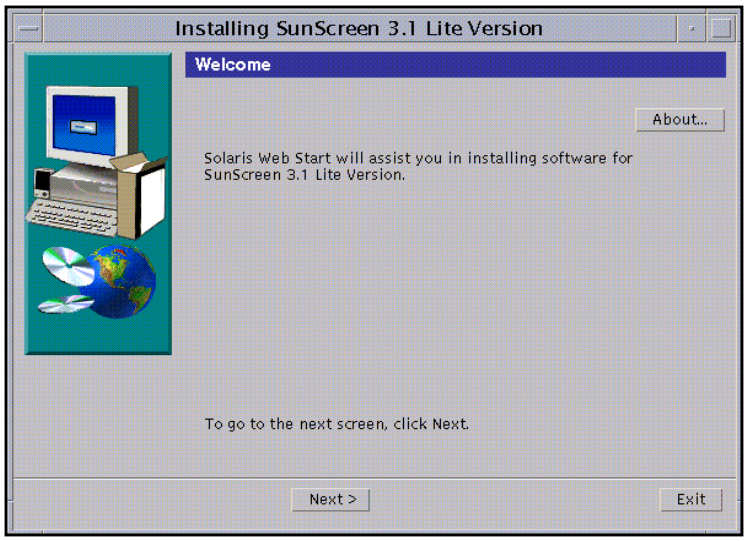

FIGURE 3-1 Screen Welcome Window

9. **Click Next to continue.**

   The Select SunScreen Components Window appears (FIGURE 3-2).

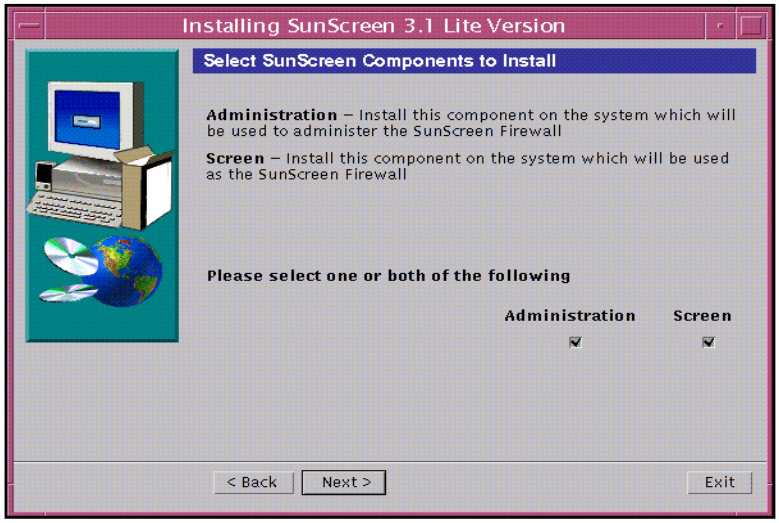

FIGURE 3-2 Select SunScreen Components Screen

Since this Screen is a local administration installation, you need both the Administration and Screen software.

10. **Make sure both Administration and Screen boxes are checked then click Next to continue.**

    The Checking System window appears (FIGURE 3-3), while a check is verifying that all the required Solaris packages are on your machine.

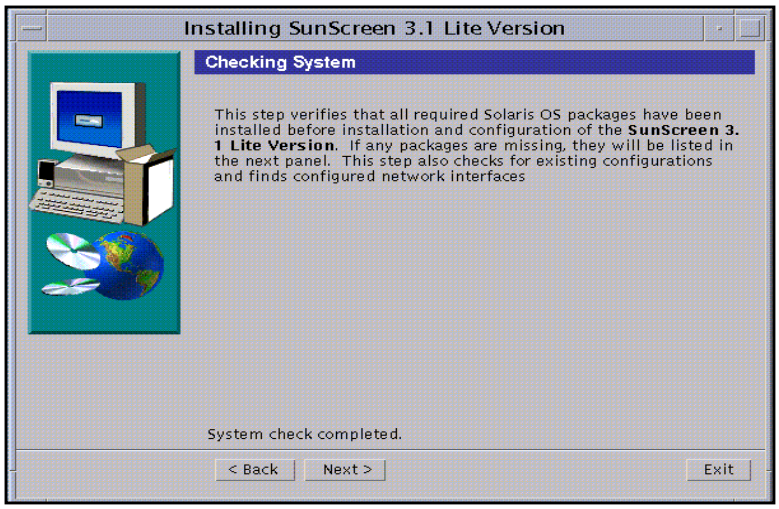

FIGURE 3-3 Checking Installed Solaris Packages Window

Note – If a list of missing required packages displays, exit the installation wizard now and install the required Solaris packages from your Solaris CD.

---

11. **Click Next to continue.**

    The Select Administration Type(s) window appears (FIGURE 3-4) with Local Administration as the default entry .

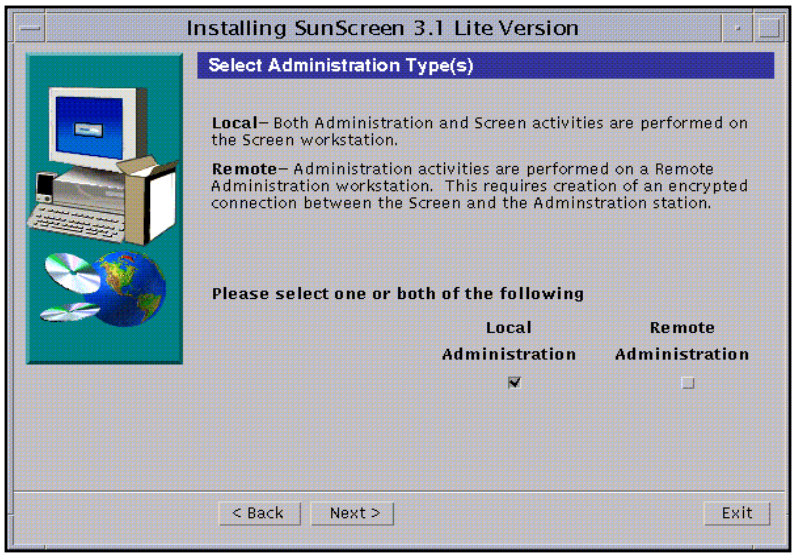

FIGURE 3-4 Select Administration Type(s) Window

12. **Click Next to continue.**

The Select Type of Install window appears (FIGURE 3-5). You have two choices: Typical Install or Custom Install.

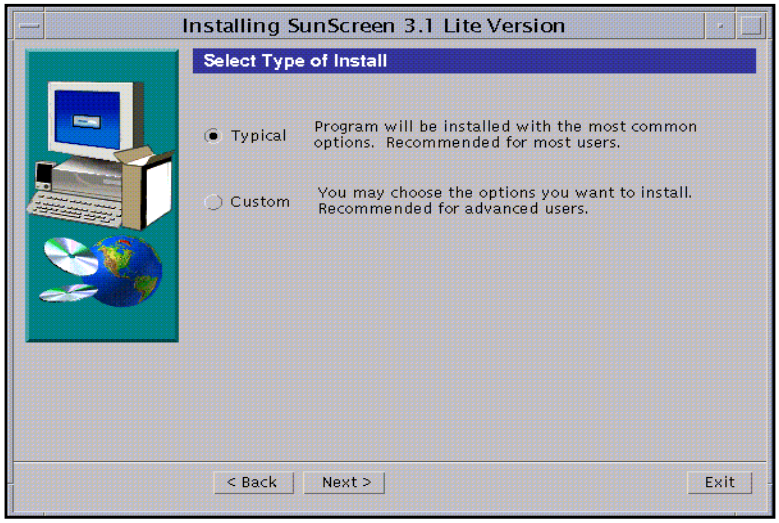

FIGURE 3-5 Select Type of Install Window

13. **Select the type of install desired, and click Next.**

    Next, the disk space on your machine is checked. An error message appears if you do not have enough disk space. If you have enough space, the Ready to Install window appears (FIGURE 3-6).

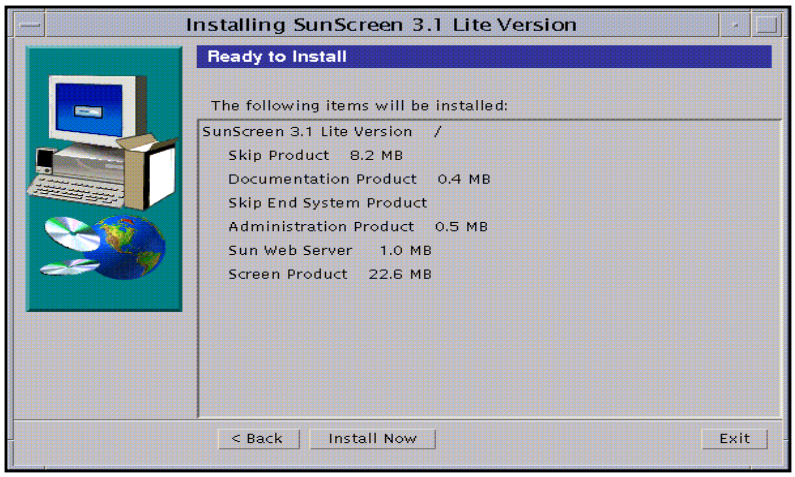

FIGURE 3-6 Ready To Install Window

14. **Click Install Now to continue.**

    The Installing window appears with a status bar showing the progress of the installation (FIGURE 3-7).

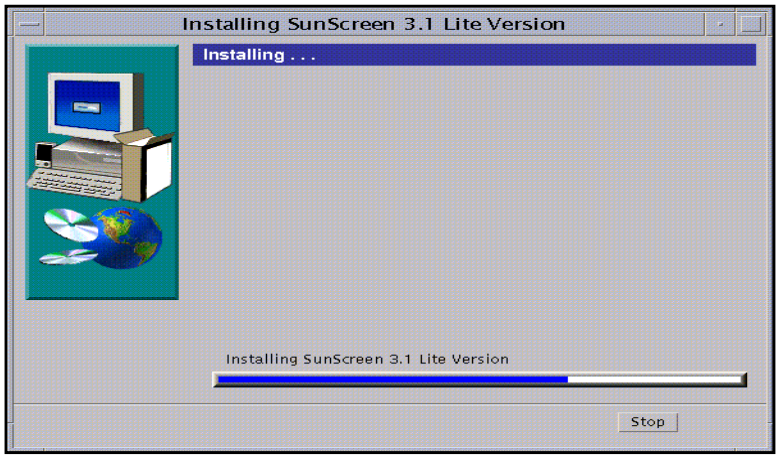

FIGURE 3-7 Installing Window

When it finishes, the Select Initial Security Level window appears (FIGURE 3-8.)

15. **Select the appropriate level of security.**

    This screen offers three levels of security with Permissive as your default initial security level. You can change this security level later as needed. See "Deciding on Your Initial Security Level" on page 12 if you need more information.

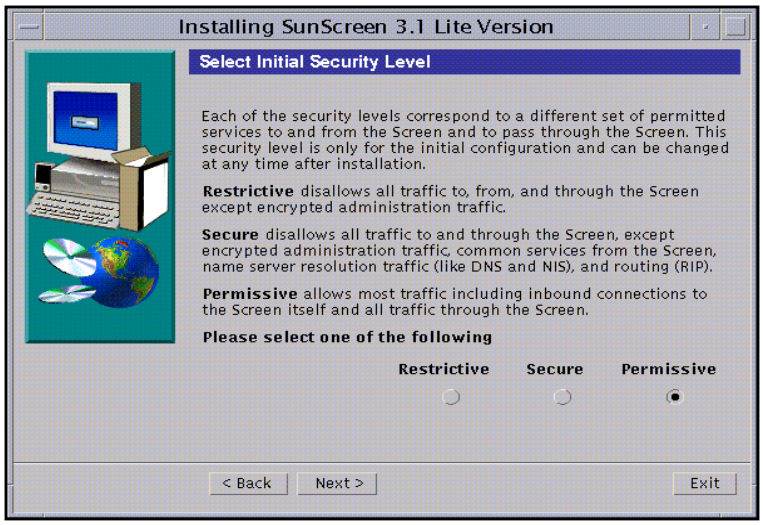

FIGURE 3-8 Select Initial Security Level Window

16. **Click Next to continue.**

    The Select Name Service(s) window appears (FIGURE 3-9.) The default entry specifies both NIS and DNS. You can deselect either one or if you do not want to use a name service, you can deselect both.

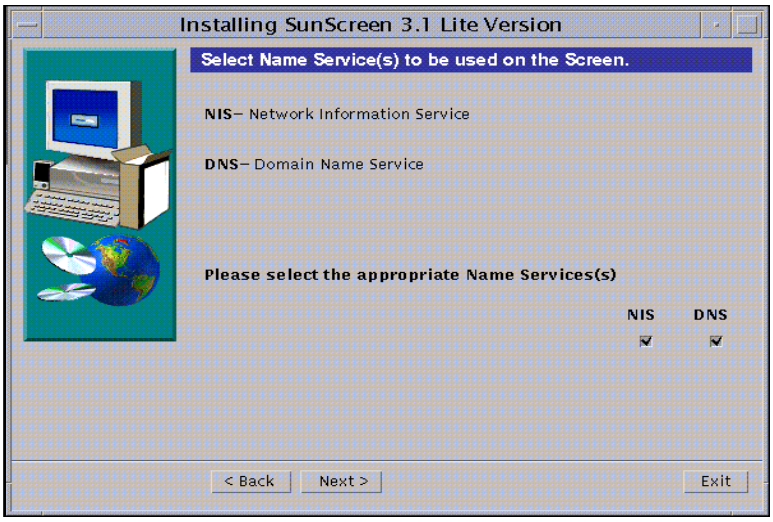

FIGURE 3-9 Select Name Service(s) Window

17. **Click Next to continue.**

    The Screen Configuration window appears with the message: `Configuring Screen`(FIGURE 3-10). A message appears once the Screen successfully configures.

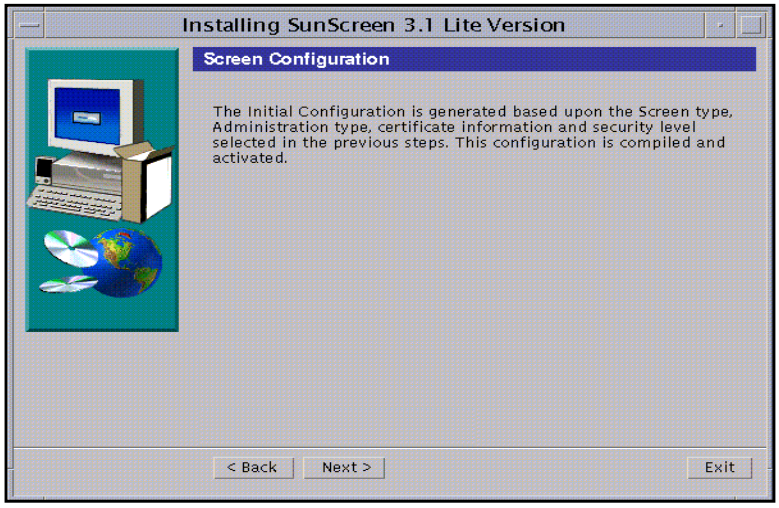

FIGURE 3-10 Screen Configuration Window

18. **Click Next to continue.**

    The Reboot Window appears (FIGURE 3-11).

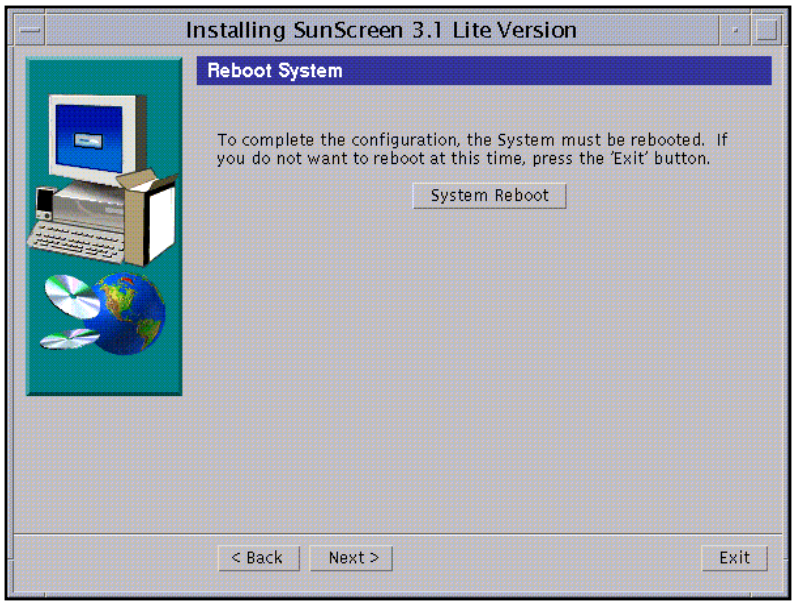

FIGURE 3-11 Reboot Window

19. **Click System Reboot to finish the installation.**

    The installation wizard disappears.

Note – You must reboot the machine at this time in order to complete the installation process. If you wish to delay rebooting your machine, click Next instead of Reboot System. An Installation Summary window appears from which you can exit the install.

Post Installation Tasks

After you install SunScreen, you should set the `PATH` and `MANPATH` so you can easily access the application and `man` pages.

Also, if you need to upgrade your Screen SKIP encryption keys, this would be an appropriate time to do it.

▼ To Set the PATH

1. **Open a terminal window and become root, if not already.**
2. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
export PATH
MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

▼ To Install SKIP Upgrades

While you are not required to use encryption on a locally administered Screen, you may want to use encryption for VPN communication over public and private networks. If you do want to use this feature, you may also want to upgrade the SKIP installation on your screen.

By default, SunScreen ships with the Global version of SKIP, which only supports the RC2, RC4(x), and DES(x) Cryptography modules and key lengths up to 1024 bits. If the security profile at your site requires additional cryptography packages and greater key lengths, you have to add these packages from the SunScreen SKIP 1.5.1 Domestic CD. For more information, see “Upgrading Cryptography Modules” on page 77.

Managing Your Configuration

Use the Administration GUI on the Remote Administration Station (or the Screen) to manage your Sunscreen firewall. See the *SunScreen Administration Guide* for more information.

By default there is a pre-defined rule to allow encrypted administration traffic between the Screen and the Administration Station. This is the only default rule so no other communication (like `ping` or `telnet`) is allowed between the two systems until you specifically define a rule to allow that service.

▼ To Launch the Administration GUI

To configure and manage your Screen, launch the Administration GUI from a Java-enabled web browser.

1. **Open a Java-enabled web browser and launch the Administration GUI by typing the following URL:**

```
http://localhost:3852
```

The Administration GUI appears (as shown in FIGURE 3-12.)

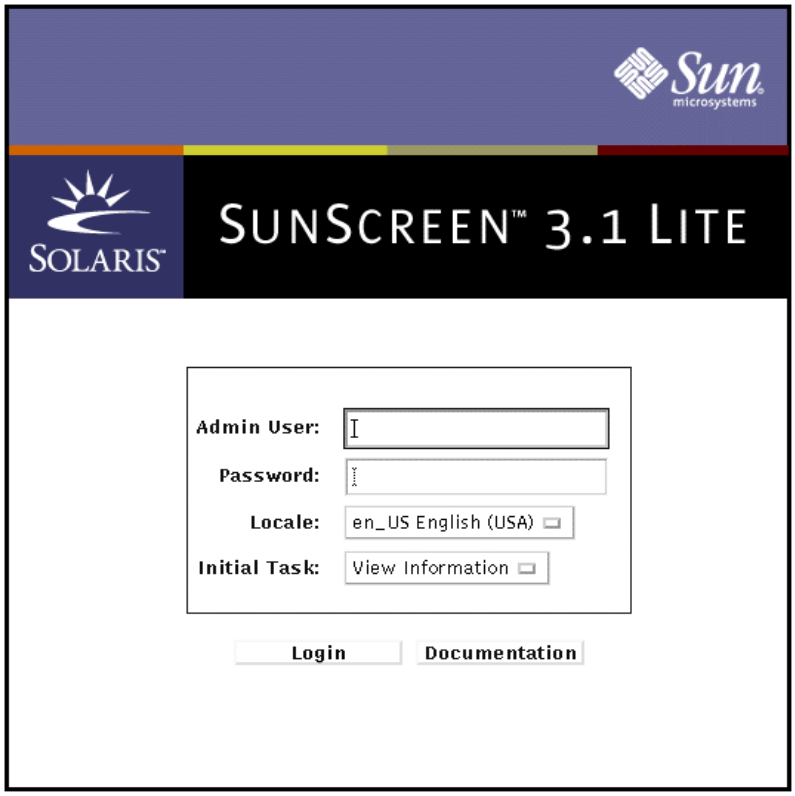

FIGURE 3-12 Administration GUI Login Page

2. **To login, type the following and Click Login:**

```
User Name: admin
Password: admin
```

You next configure and manage your SunScreen with the Administration GUI. See the *SunScreen Administration Guide* for further instructions

---

Note – One of your first administration tasks should be to change the default User Name and Password to something more secure so you can reduce the risk of compromising the administration traffic.

CHAPTER 4

Installing Lite With Remote Administration

This chapter explains how to install SunScreen on remotely administered Screen machines. This installation scenario is basically a three-step process. First you install the appropriate software on the Administration Station, next you install the software on the Screen, last you enable SKIP on the Administration Station.

You use SunScreen™ SKIP (Simple Key-Management for Internet Protocols) to enable encrypted communication between the Administration Station and the Screen. SunScreen includes and installs SunScreen SKIP. For general information regarding SKIP, refer to the *SunScreen SKIP 1.5.1 User's Guide.*

Topics in this chapter include:

- Supported configurations for the Administration Station
- Installation overview
- Installing the software on the Administration Station
- Installing certificates on the Administration Station
- Installing the software and certificates on the Screen
- Setting Up SKIP on the Administration Station

Note – If you are installing on a system without a monitor, use the command line installation discussed in "Command Line Installation" on page 63.

Supported Administration Station Configurations

You can use any machine with a Java-enabled web browser compliant with JDK 1.1.3 or later as an Administration Station, as long as it can connect securely to the Screen using SKIP. The SunScreen CD-ROM includes SunScreen SKIP for both SPARC and x86 platforms. This allows any hardware running the Solaris 2.6, Solaris 7, or Solaris 8 operating environment to be an Administration Station.

PCs operating Windows 95, Windows 98, or NT 4.x with SKIP are supported platforms as an Administration Station, using the Administration GUI. This chapter, however, covers Solaris-based Administration Stations only.

Installation Overview

This chapter explains how to install SunScreen in routing mode with remote administration, using either self-generated or issued certificate technology.

This is a multi-step installation which you should complete in the following order:

1. **On the Administration Station**

   Install the SunScreen Administration software. This step installs the required SunScreen and SKIP packages on the Administration Station (see "To Install the Software on the Administration Station" on page 39.)

2. **On the Administration Station**

   Install the Administration Station certificate (see "To Install a Self-Generated Certificate" on page 42 or "To Install an Issued Certificate" on page 43.)

3. **On the Screen**

   Install the SunScreen software. This procedure requires the Administration Station's certificate ID and installs the Screen's certificate (see"To Install Screen Software" on page 45.)

4. **On the Administration Station**

   - Install the Screen's certificate ID.
   - Start encrypted communication by enabling SKIP (see "To Set Up SKIP on the Administration Station" on page 54.

Note – The installation procedure requires that you reboot your machine when indicated. Do not perform any other tasks on the machine while installing the software, as a delay in rebooting the machine may affect installation and cause your system to hang.

Installing the Administration Software

▼ To Install the Software on the Administration Station

1. **Insert the SunScreen CD-ROM into the CD-ROM drive.**

   A File Manager screen appears listing the CD contents.

2. **Add the software by double-clicking on the installer icon.**

   Enter the root password for your system when prompted.

3. **After the Install Wizard's Welcome Window appears, click Next to continue.**

   The Select Secure Net Components Window appears (as shown in FIGURE 4-1). Make sure that you select the Administration box only.

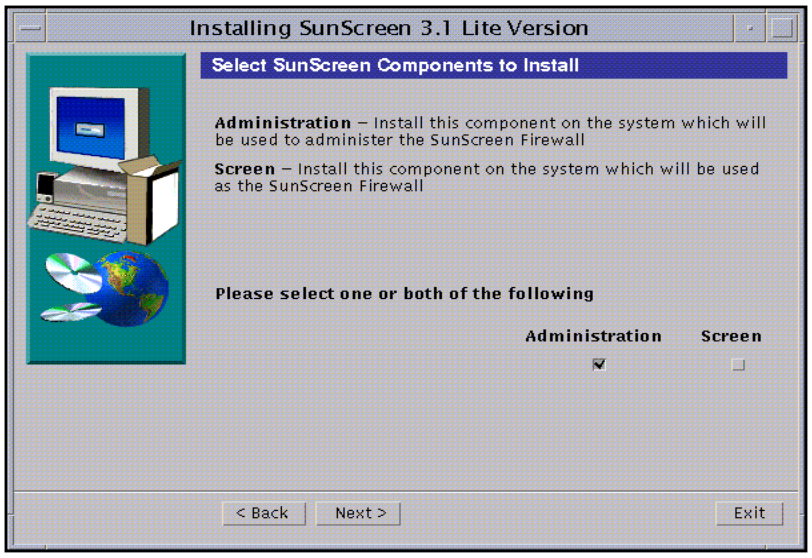

FIGURE 4-1 Select SunScreen Components Screen

4. **Click Next to continue.**

   The Select Type of Install window appears. You have two choices: Typical Install or Custom Install. You should use the Typical install.

5. **When the Ready to Install Window appears, click Install Now to continue.**

   The installation process continues until you see the Reboot Window.

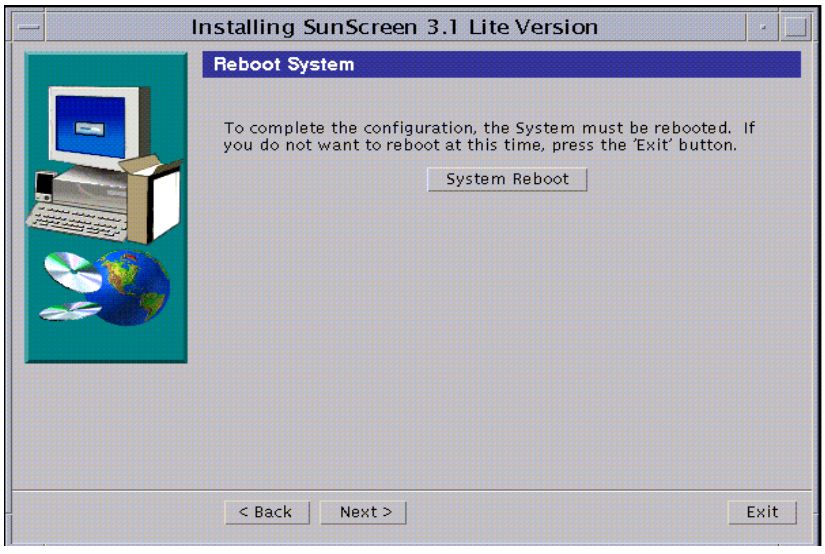

FIGURE 4-2 Reboot Window

6. **Select System Reboot to complete the installation process.**

   The installation wizard disappears.

7. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
export PATH
MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

▼ To Install SKIP Upgrades

By default, SunScreen ships with the Global version of SKIP, which only supports the RC2, RC4, and DES Cryptography modules and key lengths up to 1024 bits. If the security profile at your site requires additional cryptography packages and greater key lengths, you have to add these packages from the SunScreen Domestic CD. For more information, see "Upgrading Cryptography Modules" on page 77.

What is Next?

The required software packages have been installed. Now, you continue the installation process on the Administration Station by adding a certificate.

Installing Certificates on the Administration Station

You need to install certificates on both the Administration Station and the Screen before they can use encrypted communication. You can use either self-generated certificates or issued certificates.

- If you are using self-generated certificates, see "To Install a Self-Generated Certificate" on page 42.
- If you are using issued certificates, use "To Install an Issued Certificate" on page 43.

▼ To Install a Self-Generated Certificate

1. **Open a terminal window and become root.**
2. **create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Create the self-generated certificate on the Administration Station by typing:**

```
# skiplocal -k -f -V
```

The local certificate ID appears, as shown in FIGURE 4-3. It is the Administration Station's 32-character certificate ID (MKID).

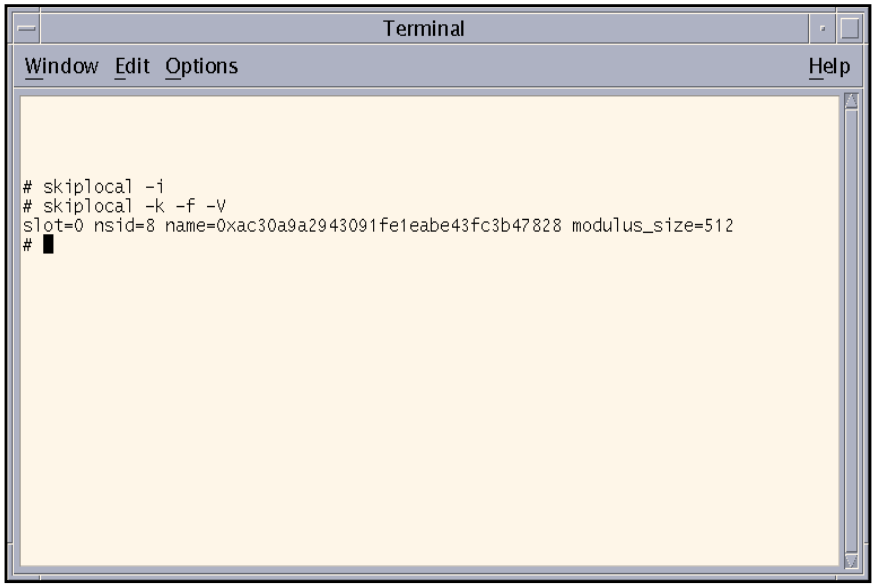

FIGURE 4-3 Administration Station's Self-Generated Certificate

4. **Write down the certificate ID, which begins with '0x'.**
5. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

6. **Reboot the Administration Station to complete the installation by typing:**

```
# sync; init 6
```

What is Next?

Now you need to install the SunScreen software on the Screen as described in, "Installing the Software on the Screen" on page 44.

▼ To Install an Issued Certificate

To do this procedure, you will need the Key and Certificate diskette.

1. **Open a terminal window on the Administration Station and become root.**
2. **Create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Insert the Key and Certificate diskette into the Administration Station's diskette drive.**
4. **Mount the diskette by typing:**

```
# volcheck
```

5. **Install the SKIP keys by typing:**

```
# install_skip_keys -icg /floppy/floppy0
```

6. **Start the SKIP daemon by typing:**

```
# skipd_restart
```

7. **Eject the Key and Certificate diskette by typing:**

```
# eject floppy0
```

8. **Write down the certificate ID, which is eight characters long.**
9. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

10. **Reboot the Administration Station to complete the installation by entering:**

```
# sync; init 6
```

What is Next?

The Administration Station's certificate ID has been installed. Now move to the Screen to install the SunScreen software.

Installing the Software on the Screen

The next step is to install the SunScreen software on the Screen. If you have a monitor and a keyboard attached to your Screen, you can use the installation wizard. If you are operating the Screen without a monitor, you must either temporarily attach a monitor, or install the software via the command line (see "Command Line Installation" on page 63.)

Note – Before starting this next step, make sure that all network interfaces you plan on using are configured. For details on Solaris network configuration, see the Solaris operating environment documentation.

▼ To Install Screen Software

Note – In this procedure, you need the Administration Station's certificate ID (MKID) from the "To Install a Self-Generated Certificate" on page 42.

1. **Insert the SunScreen CD-ROM into the Screen's CD-ROM drive.**

   A File Manager screen appears listing the CD contents.

2. **Add the software by double-clicking on the installer icon.**

   Enter the root password for your system when prompted.

3. **After the Install Wizard's Welcome Window appears, click Next to continue. If you are not logged on as `root`, you are prompted for the `root` password.**

4. **Proceed through the installation screens accepting the default choices, until the Select Administration Type Window appears.**

   In this window (FIGURE 4-4), you are given the choice of Local Administration or Remote Administration with Local Administration as the default. Select Remote Administration.

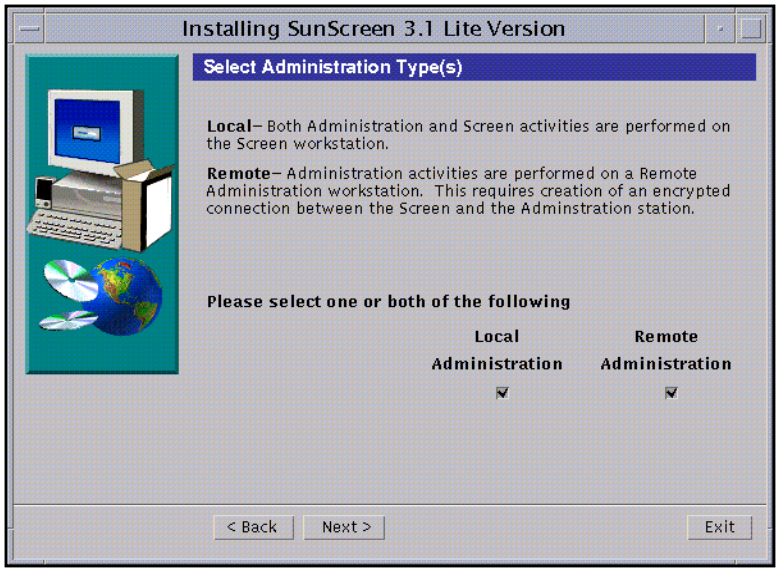

FIGURE 4-4 Select Administration Type(s) Window

5. **Select Remote Administration and click Next.**

   Click next to proceed through the installation until the Select Certificate Type window appears (FIGURE 4-5). Self-Generated Certificate is the default. You have to make a choice at this point whether you are going to use self-generated certificates or issued certificates

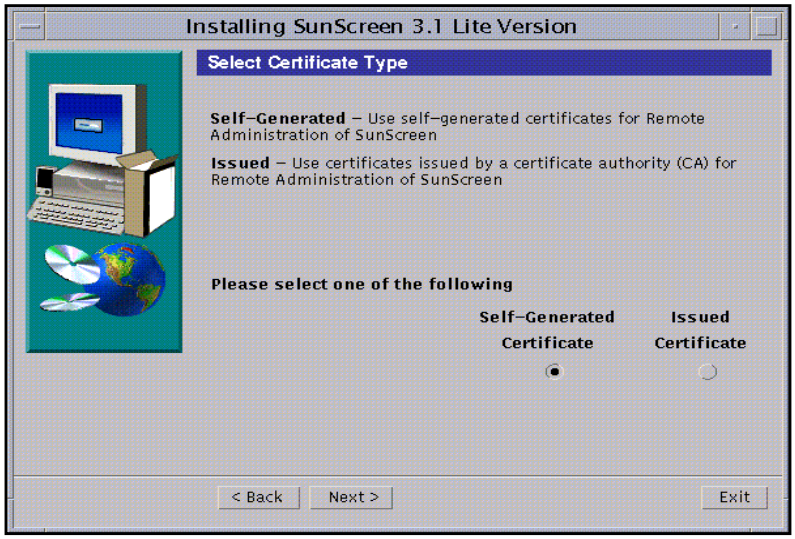

FIGURE 4-5 Select Certificate Type Window

6. **If you are using Self-Generated Certificates, follow instructions a-i through iii then go to Step 7. If you are using Issued Certificates, follow instructions b-i through iv then go to Step 7.**

   a. **Self-Generated Certificates Only**

      Accept the default (Self-Generated Certificate) and click Next.

      The Self-Generated Certificate ID window appears(FIGURE 4-6).

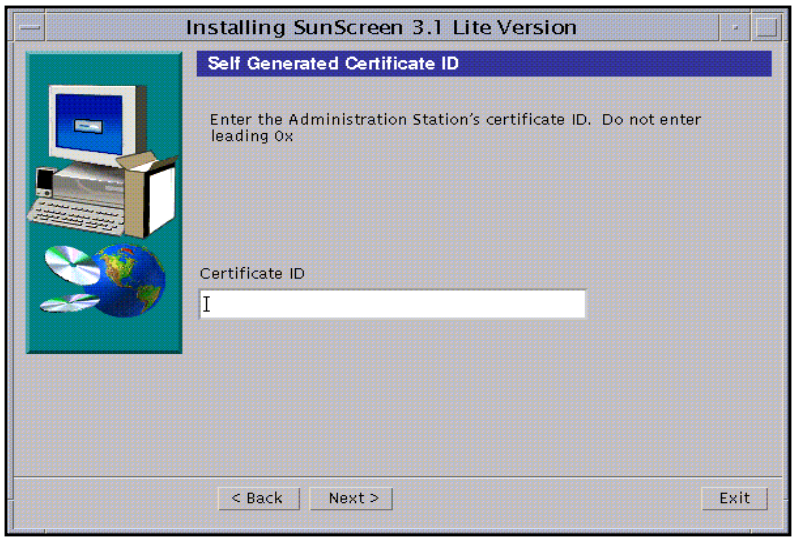

FIGURE 4-6 Self Generated Certificate ID Window

i. Enter the Administration Station's 32-character certificate ID (MKID), obtained in the previous procedure (FIGURE 4-3**). Do not enter the leading two characters: 0x. After you enter the ID, click Next.**

The Generate Screen Certificate window appears. Wait while the Screen's certificate ID generates. When completed, the Screen's 32-character certificate ID appears at the bottom of the window, as shown in FIGURE 4-7.

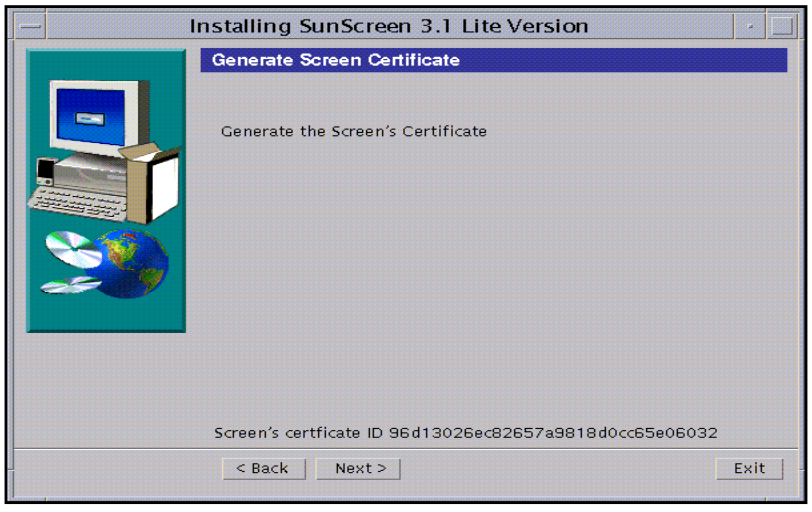

FIGURE 4-7 Generate Screen Certificate Window With Screen's Certificate ID

ii. Write down the Screen's 32-character certificate ID (MKID) that appears at the bottom of the window. You need this ID is required to complete the Administration Station installation.

iii. Go to Step 7.

b. Issued Certificates Only

From the Select Certificate Type window, select Issued Certificate and click Next. The Issued Certificate Key Diskettes window next appears (FIGURE 4-8).

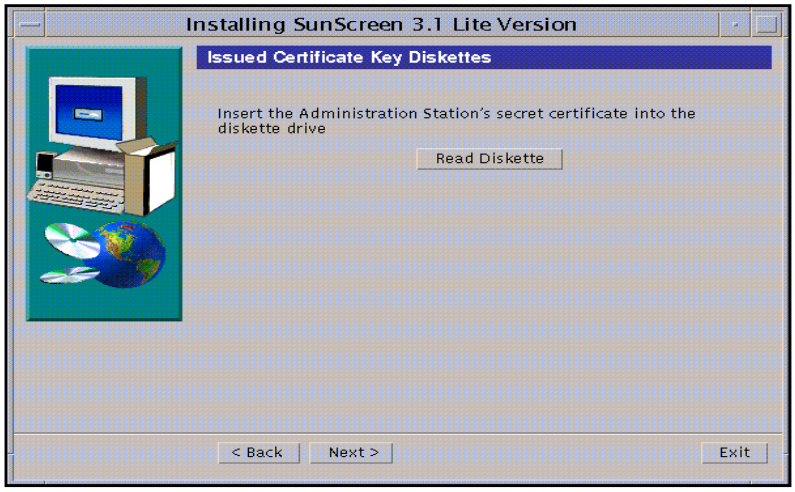

FIGURE 4-8 Issued Certificate Key Diskettes Window

i. Insert the Administration Station's Key and Certificate diskette and click Read Diskette. Wait until the issued certificate ID appears at the bottom of the window (FIGURE 4-9**).**

FIGURE 4-9 Issued Certificate Key Diskettes Window With Issued Certificate ID

ii. Write down the Administration Station's eight-character certificate ID, and click Next.

The Issued Certificate Key Diskettes window re-appears, and prompts you to use the Screen's certificate ID diskette.

iii. Insert the Screen's Certificate ID diskette into the floppy drive and click Read Diskette.

The Issued Certificate ID for the Screen appears at the bottom of the window.

iv. Write down the Screen's eight-character certificate ID then go to Step 7.

7. Click Next to continue.

The Select Initial Security Level window appears (FIGURE 4-10).

8. Select the level of security you want.

When in doubt, select Permissive as your initial security level. You can change this level later as needed. See "Deciding on Your Initial Security Level" on page 12 if you need more information.

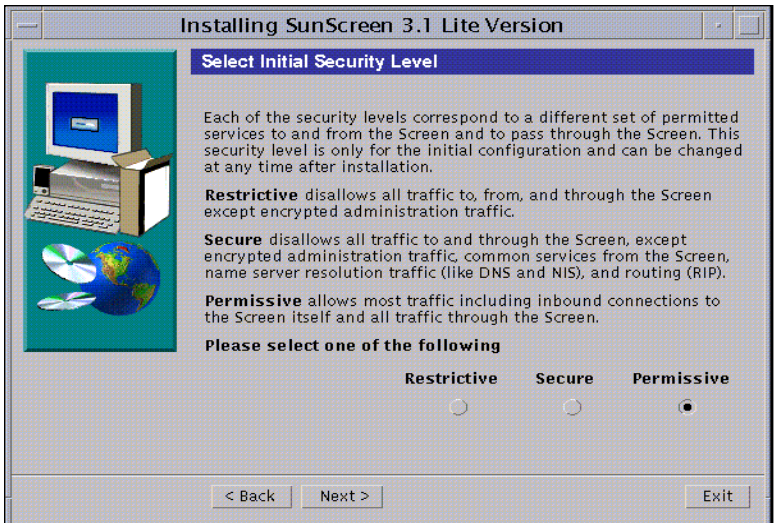

FIGURE 4-10 Select Initial Security Level Window

9. **Click Next.**

   The Select Name Service(s) window appears (FIGURE 4-11). The default entry is to use both NIS and DNS. You can deselect either one or if you do not want to use a name service, you can deselect both.

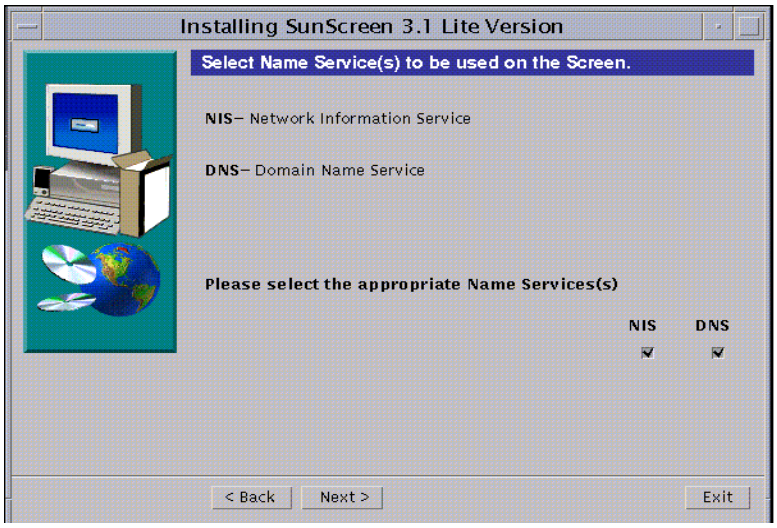

FIGURE 4-11 Select Name Service(s) Window

10. **Select the appropriate Name Service(s), and click Next.**

The Screen Configuration window appears with the message: `Configuring Screen`. The message changes when the Screen successfully configures.

11. **Click Next to continue.**

    The Reboot Window appears (FIGURE 4-12).

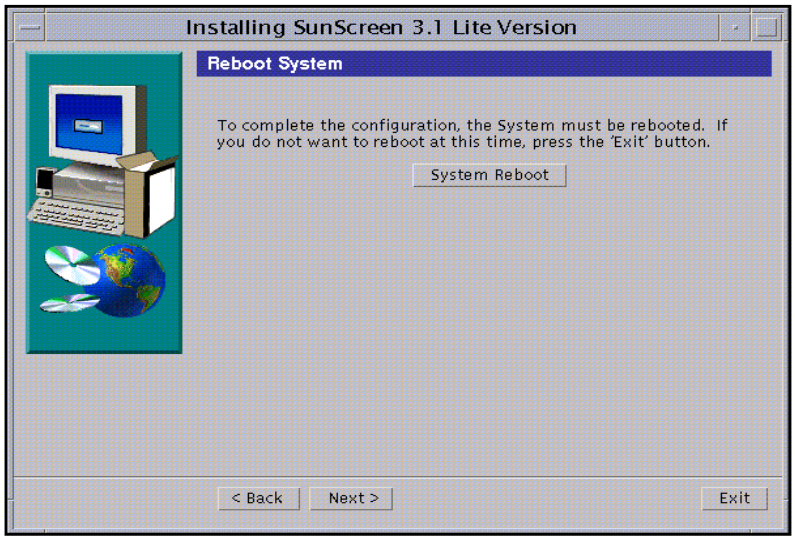

FIGURE 4-12 Reboot Window

12. **Click System Reboot to finish the installation.**

    The installation wizard disappears.

Note – You must reboot the machine at this time in order to complete the installation process. If you wish to delay rebooting your machine, click Next instead of Reboot Screen. An Installation Summary window appears from which you can exit the install.

Finishing the Installation

The software is installed on the Screen. To finish the installation you need to:

- Set the PATH.
- Install SKIP Upgrades (if needed)
- Display the `AdminSetup.readme` File

▼ To Set the PATH

1. **On the Screen, open a terminal window and become root, if not already.**
2. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
export PATH
MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

▼ To Install SKIP Upgrades

By default, SunScreen ships with the Global version of SKIP, which only supports the RC2, RC4, and DES Cryptography modules and key lengths up to 1024 bits. If the security profile at your site requires additional cryptography packages and greater key lengths, you have to add these packages from the SKIP Domestic CD. For more information, see "Upgrading Cryptography Modules" on page 77.

▼ To Display the AdminSetup.readme File

- **To display the `AdminSetup.readme` file, in a terminal window type:**

```
# more /etc/opt/SUNWicg/SunScreen/AdminSetup.readme
```

The `AdminSetup.readme` file contains the Screen's certificate ID as well as the command you run in order to give the Administration Station the Screen's certificate ID, (FIGURE 4-13). Write the command down for later use, which begins with `skiphost -a`.

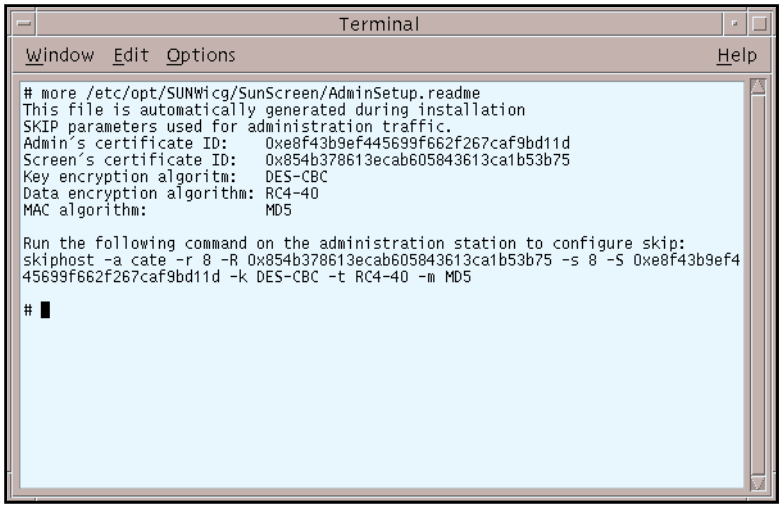

FIGURE 4-13 `AdminSetup.readme` file

Note – If you trust that the network between the Screen and the Administration Station is secure, you can ftp the AdminSetup.readme file from the Screen to the Administration Station. This saves you the task of writing down the information which is required in the next procedure.

What is Next?

You now return to the Administration Station to complete SKIP configuration. Proceed to "Completing SKIP Setup on the Administration Station" on page 53.

Completing SKIP Setup on the Administration Station

You complete this installation by establishing encrypted communication between the Administration Station and the Screen. This step involves enabling SunScreen SKIP on the Remote Administration Station. In this procedure, you tell the Administration Station which encryption algorithms to use when communicating with the Screen. For more information regarding SunScreen SKIP for Solaris, see the *SunScreen SKIP 1.5.1 User's Guide*.

Requirements

To configure the Administration Station to communicate with the Screen, you must know:

- Which access control list (ACL) parameters to set to match the Screen's encryption settings.
- The Screen's certificate ID.
- This is where you use the command obtained from the `AdminSetup.readme` file in "To Display the AdminSetup.readme File" on page 52.

Note – Instructions for using SKIP from the command line are in "Command Line Installation" on page 63

▼ To Set Up SKIP on the Administration Station

1. **Open a terminal window and become root.**
2. **Launch the skiptool GUI by typing:**

```
# skiptool
```

Note – You may need to use `skiptool -i` *name_of_interface* (such as qe3) if you wish to set SKIP parameters on a network interface other than the default interface.

The main window of the `skiptool` GUI appears (FIGURE 4-14).

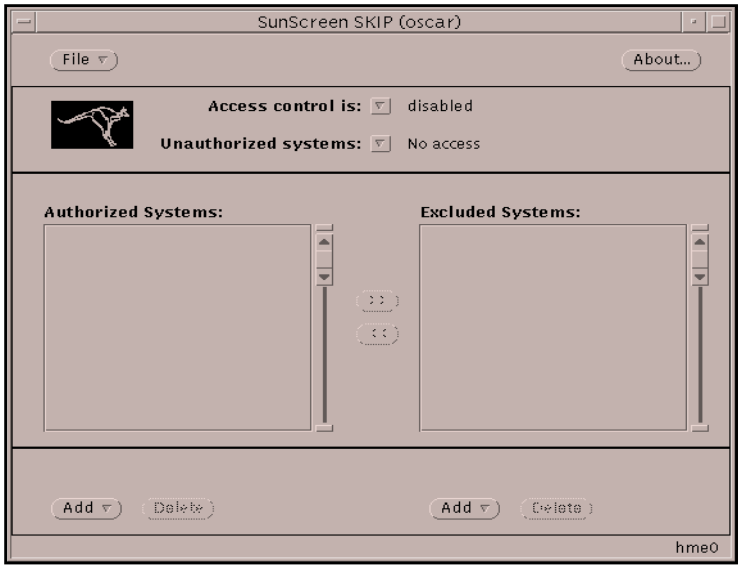

FIGURE 4-14 `skiptool` Main Window

Next, you add a default ACL to talk unencrypted to all hosts.

3. **Click the Add button, and under Host, choose the Off security option.**
   The Add Host properties window opens(FIGURE 4-15).

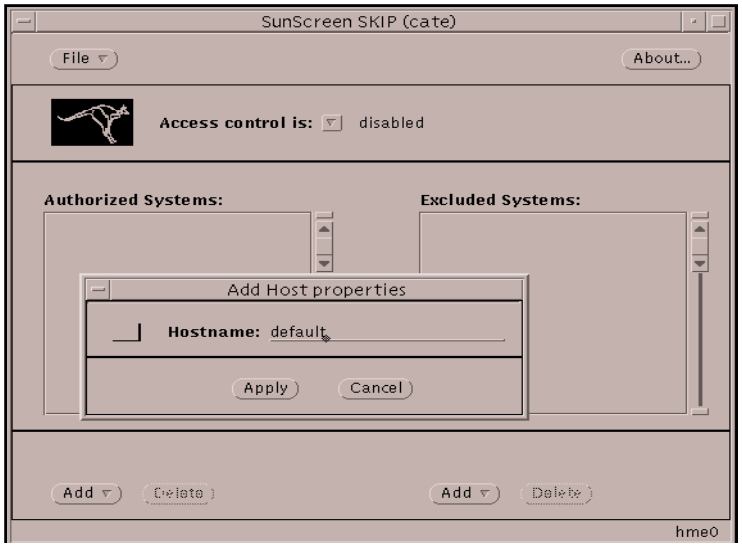

FIGURE 4-15 Skiptool With Add Host Properties Window Completed

4. **Type ‘default’ as the Hostname and Click Apply.**

   Next, you add an ACL entry for the Screen.

5. **Click the Add button, and under Host, choose the SKIP security option.**

   The Add Skip host properties window appears (FIGURE 4-16).

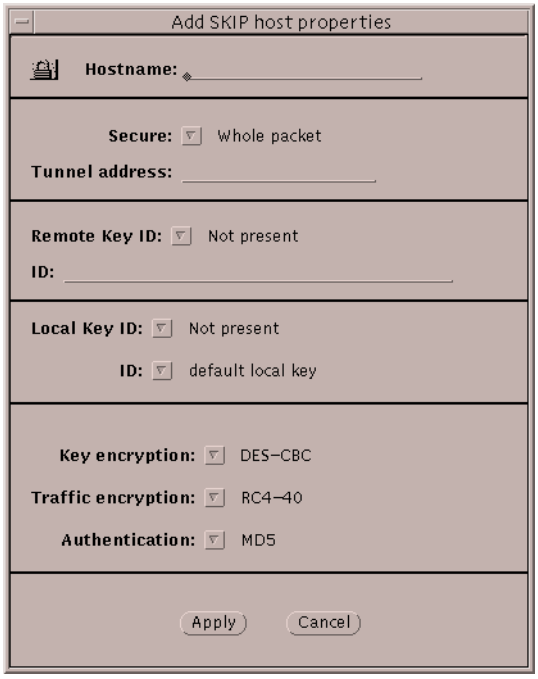

FIGURE 4-16 Add SKIP Host Properties Window

Use the information contained in the `AdminSetup.readme` file (see “To Display the AdminSetup.readme File” on page 52) to complete the fields.

6. **Type the name of the screen in the Hostname field.**

7. **In the Secure field, select Whole Packet from the drop-down list.**

8. **In the Remote Key ID, make the appropriate selection from the drop-down list.**

   Refer to the `AdminSetup.readme` file to select the correct Remote Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4. See FIGURE 4-17 for a sample of the Add SKIP Host Properties window completed.

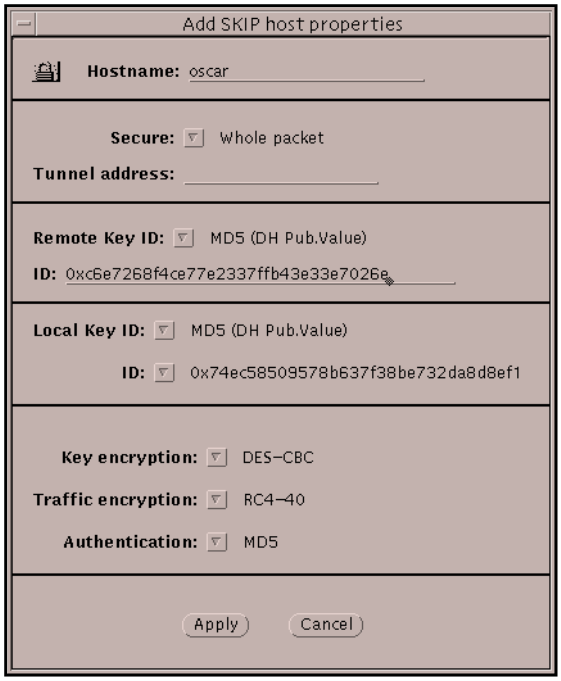

FIGURE 4-17 Add SKIP Host Properties Completed

9. **In the Local Key ID, make the appropriate selection from the drop-down list.**

   Refer to the `AdminSetup.readme` file to select the correct Local Key ID. For self-generated certificates on the Administration Station, select MD5 (DH Public Value). For issued certificates, select IPv4. The ID value is filled in automatically.

10. **Turn SKIP on. From the pulldown menu for "Access control is:", located at the top of the `skiptool` window, select 'enabled'.**

Note – When you select enabled from the pulldown menu, a window appears when you save the configuration. Click Cancel to prevent these required systems, which are part of the default configuration, from showing up in the Authorized Systems window

---

11. **Select Save from the File pulldown menu**

Note – After configuring SKIP, check that the encryption parameters and the certificate ID (MKID) values match on both the Administration Station and the Screen.

Managing Your Configuration

Use the Administration GUI on the Remote Administration Station (or the Screen) to manage your firewall. See the *SunScreen Administration Guide* for more information.

By default there is a pre-defined rule to allow encrypted administration traffic between the Screen and the Administration Station. This is the only default rule so no other communication (like `ping` or `telnet`) is allowed between the two systems until you specifically define a rule to allow that service.

▼ To Launch the Administration GUI

1. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser, and type the following URL:**

```
http://Name_of_Screen:3852/
```

The Administration GUI appears (FIGURE 4-18).

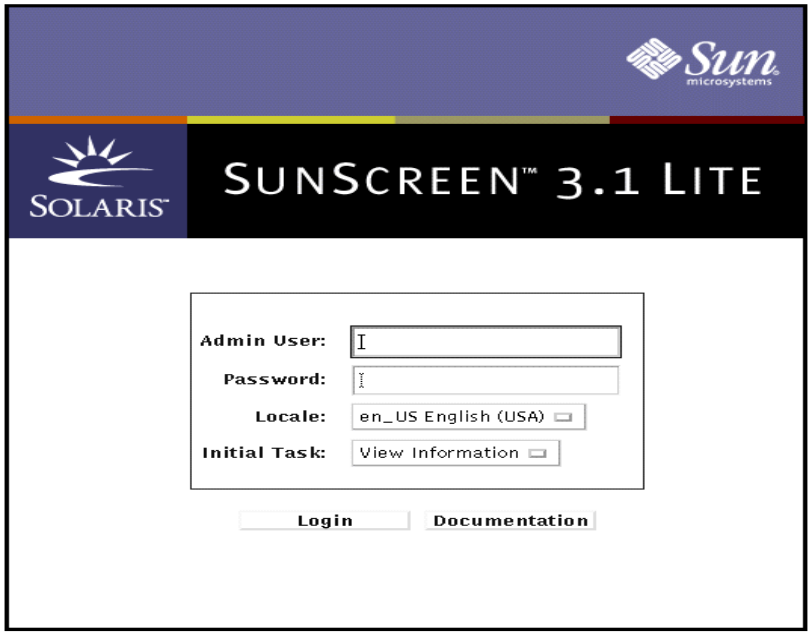

FIGURE 4-18 Administration GUI Login Page

2. **To login, type the following and Click Login:**

```
User Name: admin
Password: admin
```

You next configure and manage your SunScreen with the Administration GUI. See the *SunScreen Administration Guide* for further instructions.

Note – One of your first administration tasks should be to change the default User Name and Password to something more secure so you can reduce the risk of compromising the administration traffic.

CHAPTER 5

Removing SunScreen

This chapter explains how to remove the SunScreen software.

▼ To Remove SunScreen

1. **Use `pkgrm` to remove the software packages originally installed on the machine. See "To Install the Software on the Administration Station" on page 63 or "To Install the Screen" on page 70 for a list of the software packages to remove.**
2. **To remove the configurations and log files, you must remove these files:**
   - `/var/opt/SUNWicg` and its descendants, which contains the SunScreen packet logfiles.
   - `/etc/opt/SUNWicg` and its descendants, which contains the SunScreen configurations and policies.
   - `/etc/skip` and its descendants, which contains the SKIP keys and certificates.

Note – These three sets of files are not removed as part of the pkgrm command. Therefore, you must remove these files manually, if you are done with them.

If you do not remove these files and reinstall the software, the old configurations and rules are retained, in addition to the `Initial` policy. You may end up with unwanted duplicates. You can delete these using the Administration GUI.

If you do not remove the old SKIP keys and certificates, when the software is reinstalled multiple Screen identities will be created. To remove the SKIP identities completely, read more about `skiplocal` and `skipdb` in the *SunScreen SKIP 1.5.1 User's Guide*.

APPENDIX **A**

Command Line Installation

This Appendix contains procedures for installing using the command line. You can use these procedures when installing SunScreen

An expert system administrator can use command line installation as an alternative to the installation wizard. Before installing, review the *SunScreen Release Notes* for the latest information about this product.

Installing the Administration Station

You can install the required SunScreen packages on the Administration Station using `pkgadd` to install the software. After you install the Administration packages, you must set up your certificate environment.

▼ To Install the Software on the Administration Station

1. **Open a terminal window on the Administration Station and become root.**
2. **Insert the Solaris 8 Early Access CD-ROM into the Administration Station's CD-ROM drive.**

3. **Add the software by typing:**

```
For SPARC systems:
# pkgadd -d cdrom/Solaris_8/EA/products/SunScreen_3.1_Lite/sparc

For Intel systems:
# pkgadd -d cdrom/Solaris_8/EA/products/SunScreen_3.1_Lite/i386
```

For SPARC systems, you are prompted with a menu of packages to install:

```
The following packages are available:
  1  NSCPcom       Netscape Communicator
                   (sparc) 20.4.70,REV=1999.08.20.17.43
  2  SUNWbdc       SKIP Bulk Data Crypt
                   (sparc) 1.5.1
  3  SUNWbdcx      SKIP Bulk Data Crypt (64-bit)
                   (sparc) 1.5.1
  4  SUNWdes       SKIP DES Crypto Module
                   (sparc) 1.5.1
  5  SUNWdesx      SKIP DES Crypto Module (64-bit)
                   (sparc) 1.5.1
  6  SUNWdthj      HotJava Browser for Solaris
                   (sparc) 1.1.5,REV=1998.12.03
  7  SUNWdtnsc     Netscape Componentization Support for CDE
                   (sparc) 1.0,REV=1999.06.14.15.50
  8  SUNWes        SKIP End System
                   (sparc) 1.5.1
  9  SUNWesx       SKIP End System (64-bit)
                   (sparc) 1.5.1
 10  SUNWfwcnv     SunScreen Firewall conversion
                   (sparc) 3.1
11  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (sparc) 2.0
 12  SUNWicgSA     SunScreen Administration Software
                   (sparc) 3.1
 13  SUNWicgSD     SunScreen online documentation
                   (sparc) 3.1
 14  SUNWicgSM     SunScreen man pages
                   (sparc) 3.1
 15  SUNWicgSS     SunScreen Firewall
                   (sparc) 3.1
 16  SUNWkeymg     SKIP Key Manager Tools
                   (sparc) 1.5.1
 17  SUNWkusup     SKIP U-Support module
                   (sparc) 1.5.1
 18  SUNWrc2       SKIP RC2 Crypto Module
                   (sparc) 1.5.1
 19  SUNWrc4       SKIP RC4 Crypto Module
                   (sparc) 1.5.1
 20  SUNWrc4x      SKIP RC4 Crypto Module (64-bit)
                   (sparc) 1.5.1
21  SUNWsman      SKIP Man Pages
                   (sparc) 1.5.1
```

For Intel systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  NSCPcom       Netscape Communicator
                   (i386) 20.4.70,REV=1999.08.20.17.56
  2  SUNWbdc       SKIP Bulk Data Crypt
                   (i386) 1.5.1
  3  SUNWdes       SKIP DES Crypto Module
                   (i386) 1.5.1
  4  SUNWdthj      HotJava Browser for Solaris
                   (i386) 1.1.5,REV=1998.12.03
  5  SUNWdtnsc     Netscape Componentization Support for CDE
                   (i386) 1.0,REV=1999.06.14.15.53
  6  SUNWes        SKIP End System
                   (i386) 1.5.1
  7  SUNWfwcnv     SunScreen Firewall conversion
                   (i386) 3.1
  8  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (i386) 2.0
  9  SUNWicgSA     SunScreen Administration Software
                   (i386) 3.1
 10  SUNWicgSD     SunScreen online documentation
                   (i386) 3.1
11  SUNWicgSM     SunScreen man pages
                   (i386) 3.1
 12  SUNWicgSS     SunScreen Firewall
                   (i386) 3.1
 13  SUNWkeymg     SKIP Key Manager Tools
                   (i386) 1.5.1
 14  SUNWkusup     SKIP U-Support module
                   (i386) 1.5.1
 15  SUNWrc2       SKIP RC2 Crypto Module
                   (i386) 1.5.1
 16  SUNWrc4       SKIP RC4 Crypto Module
                   (i386) 1.5.1
 17  SUNWsman      SKIP Man Pages
                   (i386) 1.5.1
```

4. **For SPARC systems, enter: 2, 3-5, 8-9, 12, 14, 16-21**
   For x86 systems, enter: 2-3, 6, 9, 11, 13 -17

5. **Follow the program prompts, answering all the questions with y.**

   When completed, you return to the same menu of packages.

6. **Enter q to quit** `pkgadd`**.**

7. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

   a. Set the `PATH` for the Bourne shell by typing:

   ```
   PATH=/opt/SUNWicg/SunScreen/bin:$PATH
   export PATH
   ```

   b. Set the `MANPATH` for the Bourne shell by typing:

   ```
   MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
   export MANPATH
   ```

8. **Eject the CD-ROM from the CD-ROM drive by typing:**

   ```
   # eject cdrom0
   ```

9. **Install any SKIP upgrades (see "Upgrading Cryptography Modules" on page 77).**

10. **Reboot by typing:**

    ```
    # sync; init 6
    ```

    The software packages have been installed. You continue the installation process on the Administration Station.

Installing Administration Station Certificates

To obtain encrypted communication between the Administration Station and the Screen, certificates must be installed on both machines. This can be done by either using self-generated certificates or by installing issued certificates. Both methods are done on the Administration Station.

▼ To Create a Self-Generated Certificate on the Administration Station

1. **Open a terminal window and create the required SKIP directories by typing:**

```
# skiplocal -i
```

2. **Create the self-generated certificate on the Administration Station by typing:**

```
# skiplocal -k -f -V
```

   The local certificate ID appears. It is the Administration Station's 32-character certificate ID (MKID).

3. **Write down the certificate ID, which begins with 'Ox'.**
4. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

5. **Reboot to complete the installation by typing:**

```
# sync; init 6
```

   The Administration Station's certificate ID has been generated. You next move to the Screen to install the SunScreen software.

▼ To Install an Issued Certificate on the Administration Station

To do this procedure, you will need the Key and Certificate diskette.

1. **Open a terminal window on the Administration Station and become root.**
2. **Create the required SKIP directories by typing:**

```
# skiplocal -i
```

3. **Insert the Key and Certificate diskette into the Administration Station's diskette drive.**

4. **Install the SKIP keys by typing:**

```
# install_skip_keys -icg /floppy/floppy0
```

5. **Start the SKIP daemon by typing:**

```
# skipd_restart
```

6. **Eject the Key and Certificate diskette by typing:**

```
# eject floppy0
```

7. **Write down the certificate ID, which is eight characters long.**

8. **Add SKIP to all the interfaces by entering:**

```
# skipif -a
```

9. **Reboot to complete the installation by entering:**

```
# sync; init 6
```

The Administration Station's certificate ID has been installed. You next move to the Screen to install the SunScreen software.

Installing the Screen

You can install the required SunScreen packages on the Screen using `pkgadd` to install the SunScreen software using the following instructions.

▼ To Install the Screen

1. **Open a terminal window on the Screen and become root.**
2. **Insert the Solaris Early Access CD-ROM into the Screen's CD-ROM drive.**
3. **Add the software by typing:**

```
For SPARC systems:
# pkgadd -d /cdrom/Solaris_8/EA/products/SunScreen_3.1_Lite/sparc

For Intel systems:
# pkgadd -d /cdrom/Solaris_8/EA/products/SunScreen_3.1_Lite/i386
```

For SPARC systems, you are prompted with a menu of packages to install:

```
The following packages are available:
  1  NSCPcom       Netscape Communicator
                   (sparc) 20.4.70,REV=1999.08.20.17.43
  2  SUNWbdc       SKIP Bulk Data Crypt
                   (sparc) 1.5.1
  3  SUNWbdcx      SKIP Bulk Data Crypt (64-bit)
                   (sparc) 1.5.1
  4  SUNWdes       SKIP DES Crypto Module
                   (sparc) 1.5.1
  5  SUNWdesx      SKIP DES Crypto Module (64-bit)
                   (sparc) 1.5.1
  6  SUNWdthj      HotJava Browser for Solaris
                   (sparc) 1.1.5,REV=1998.12.03
  7  SUNWdtnsc     Netscape Componentization Support for CDE
                   (sparc) 1.0,REV=1999.06.14.15.50
  8  SUNWes        SKIP End System
                   (sparc) 1.5.1
  9  SUNWesx       SKIP End System (64-bit)
                   (sparc) 1.5.1
 10  SUNWfwcnv     SunScreen Firewall conversion
                   (sparc) 3.1
11  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (sparc) 2.0
 12  SUNWicgSA     SunScreen Administration Software
                   (sparc) 3.1
 13  SUNWicgSD     SunScreen online documentation
                   (sparc) 3.1
 14  SUNWicgSM     SunScreen man pages
                   (sparc) 3.1
 15  SUNWicgSS     SunScreen Firewall
                   (sparc) 3.1
 16  SUNWkeymg     SKIP Key Manager Tools
                   (sparc) 1.5.1
 17  SUNWkusup     SKIP U-Support module
                   (sparc) 1.5.1
 18  SUNWrc2       SKIP RC2 Crypto Module
                   (sparc) 1.5.1
 19  SUNWrc4       SKIP RC4 Crypto Module
                   (sparc) 1.5.1
 20  SUNWrc4x      SKIP RC4 Crypto Module (64-bit)
                   (sparc) 1.5.1
21  SUNWsman      SKIP Man Pages
                   (sparc) 1.5.1
```

For Intel systems, you are prompted with a menu of packages to install:

```
The following packages are available:
1  NSCPcom       Netscape Communicator
                   (i386) 20.4.70,REV=1999.08.20.17.56
  2  SUNWbdc       SKIP Bulk Data Crypt
                   (i386) 1.5.1
  3  SUNWdes       SKIP DES Crypto Module
                   (i386) 1.5.1
  4  SUNWdthj      HotJava Browser for Solaris
                   (i386) 1.1.5,REV=1998.12.03
  5  SUNWdtnsc     Netscape Componentization Support for CDE
                   (i386) 1.0,REV=1999.06.14.15.53
  6  SUNWes        SKIP End System
                   (i386) 1.5.1
  7  SUNWfwcnv     SunScreen Firewall conversion
                   (i386) 3.1
  8  SUNWhttp      Sun WebServer daemon and supporting binaries
                   (i386) 2.0
  9  SUNWicgSA     SunScreen Administration Software
                   (i386) 3.1
 10  SUNWicgSD     SunScreen online documentation
                   (i386) 3.1
11  SUNWicgSM     SunScreen man pages
                   (i386) 3.1
 12  SUNWicgSS     SunScreen Firewall
                   (i386) 3.1
 13  SUNWkeymg     SKIP Key Manager Tools
                   (i386) 1.5.1
 14  SUNWkusup     SKIP U-Support module
                   (i386) 1.5.1
 15  SUNWrc2       SKIP RC2 Crypto Module
                   (i386) 1.5.1
 16  SUNWrc4       SKIP RC4 Crypto Module
                   (i386) 1.5.1
 17  SUNWsman      SKIP Man Pages
                   (i386) 1.5.1
```

4. **For SPARC systems, enter: 2-5, 8-9, 11-21**
   For x86 systems, enter: 2-3, 6, 8, 9-17

5. **Follow the program prompts, answering all the questions with y.**

   When completed, you return to the same menu of packages.

6. **Enter q to quit** `pkgadd`**.**

7. **Set the `PATH` and `MANPATH` by editing your shell initialization file (such as `.profile` or `.login` file).**

```
PATH=/opt/SUNWicg/SunScreen/bin:$PATH
export PATH
MANPATH=$MANPATH:/opt/SUNWicg/SunScreen/man
export MANPATH
```

8. **Eject the CD-ROM from the CD-ROM drive by typing**

```
# eject cdrom0
```

9. **Install any SKIP upgrades (see "Command Line Installation" on page 63)**

10. **Reboot by typing:**

```
# sync; init 6
```

11. **Open a terminal window and become root, if not already.**

12. **Complete installation by typing:**

```
# ss_install
```

Answer the questions that appear. The questions and text are similar to the panels that appear when installing using the installation wizard. Review the procedures for installing the software on the Screen in Chapter 3 or 4 if more detail is needed.

If you are using issued certificates, you need your all your certificate diskettes.

Note – The SKIP command to run on the Administration Station is displayed at the end. It is contained in the `AdminSetup.readme` file, found in the directory `/etc/opt/SUNWicg/SunScreen`. Write this command down for use in the following procedure.

If you trust that the network between the Screen and the Administration Station is secure, you can ftp the `AdminSetup.readme` file from the Screen to the Administration Station. This saves you the task of writing down the information which is required in the next procedure.

---

13. **Reboot by typing:**

```
# sync; init 6
```

▼ To Use Command-Line SKIP on the Administration Station

1. **On the Administration Station, open a terminal window and become root.**
2. **To enable unencrypted communication from the Administration Station to all hosts other than the Screen, type:**

```
# skiphost -a default
```

3. **Add a rule so that encrypted communication is possible between the Administration Station and the Screen by typing:**

```
# skiphost command_from_ss_install
```

This command is in the `AdminSetup.readme` file. The command is in the following form, which has been divided into lines for readability:

skiphost -a *name_of_Screen* -r *NSID_type*

-R *Screen's_certificate_ID* -s *NSID_type*

-S *Administration_Station's_certificate_ID*

-k *key_encryption_algorithm*

-t *data_encryption_algorithm* -m *MAC_algorithm*

4. **Turn on SKIP by typing:**

```
If Screen has only one interface:
# skiphost -o on
If Screen has more than one interface, for each interface:
# skiphost -i name_of_interface -o on
```

Note – To display the interfaces, type `ifconfig -a`

---

5. **Save the SKIP settings by typing:**

```
# skipif -i all -s
```

6. **Restart the SKIP daemon by typing:**

```
# skipd_restart
```

Refer to the *SunScreen SKIP 1.5.1 User's Guide* for more information on operating SKIP, if needed.

Note – After configuring SKIP, check that the encryption parameters and 32-character certificate ID (MKID) values match on both the Administration Station and the Screen.

---

7. **To configure and manage your SunScreen from your Administration Station, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and launch the Administration GUI by typing the following URL: .**

```
http://Name_of_Screen:3852/
```

See the *SunScreen Administration Guide* for instructions on how to use the Administration GUI.

APPENDIX **B**

Upgrading Cryptography Modules

By default, SunScreen ships with the Global version of SunScreen SKIP, which only contains the RC2 , RC4(x), and DES(x) Cryptography modules and key lengths up to 1028 bits. To add additional modules (for example 3DES) and support for greater key lengths (up to 4096 bits), you must add packages from the SunScreen Domestic release CD. Use the following table when you want to add additional Cryptography modules to your SKIP configuration.

Note – You must take some care to install only the packages you need. The End System SKIP modules (`SUNWes` and `SUNWesx`) should not be added to a Screen.

▼ To Install SKIP Upgrades

1. **If you have a Global version of SKIP and you want to upgrade to the Domestic Use Only version, use `pkgadd` to install these packages from the Domestic SKIP CD-ROM.**
   - `SUNWkdsup` -- SKIP D-Support module
   - `SUNW3des` -- SKIP 3DES Crypto Module
   - `SUNW3desx` -- SKIP 3DES Crypto Module (64-bit in SPARC only)
   - `SUNWrc4` -- SKIP RC4-128 Crypto Module
   - `SUNWrc4x` -- SKIP RC4-128 Crypto Module (64-bit in SPARC only)
   - `SUNWsafe` -- SKIP SAFER Crypto Module
   - `SUNWsafex` -- SKIP SAFER Crypto Module (64-bit in SPARC only
2. **After you install a SKIP upgrade, reboot by typing:**

```
# sync; init 6
```

Index

F

G

H

I

J

K

L

M

N

P

R

S