SunScreen 3.2 Installation Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part No: 806–6345–10
December 2001

020110@3062

Contents

Preface

SunScreen™ 3.2 software is part of the family of SunScreen products that provide solutions to security, authentication, and privacy requirements for companies to connect securely and conduct business privately over an insecure public internetwork. Earlier SunScreen firewall products include SunScreen EFS 1.0, 2.0, 3.0, SunScreen 3.1 and SunScreen 3.1 Lite, SunScreen SPF-100 and SunScreen SPF-200, their respective Administration Stations, SunScreen packet filtering software, and SunScreen Simple Key-Management for Internet Protocols (SKIP) encryption software.

This *SunScreen 3.2 Installation Guide* contains the information necessary for you to install the SunScreen 3.2 software.

Who Should Use This Book

The *SunScreen 3.2 Installation Guide* is intended for system administrators responsible for the operation, support, and maintenance of network security. This manual assumes that you are familiar with UNIX® system administration, TCP/IP networking concepts, and your network topology.

Before You Read This Book

Before you install and administer your system, become familiar with the following SunScreen 3.2 manuals:

- *SunScreen 3.2 Release Notes* (PN 806–6350)
- *SunScreen 3.2 Installation Guide* (PN 806–6345)

- *SunScreen 3.2 Administrator's Overview* (PN 806–6347)
- *SunScreen 3.2 Administration Guide* (PN 806–6346)
- *SunScreen 3.2 Configuration Examples* (PN 806–6348)
- *SunScreen SKIP User's Guide, Release 1.5.1* (PN 806–5379)

How This Book Is Organized

The *SunScreen 3.2 Installation Guide* contains the following chapters and appendices:

- Chapter 1 covers the basic concepts of the SunScreen product, including operating system and hardware requirements and compatibility, product architecture, and modes of operation.
- Chapter 2 discusses installing SunScreen in routing mode with local administration.
- Chapter 3 discusses installing SunScreen in routing mode with remote administration using SKIP certificate technology.
- Chapter 4 discusses installing SunScreen in stealth mode using SKIP certificate technology.
- Chapter 5 discusses installing SunScreen in routing mode with remote administration using IKE certificate technology.
- Chapter 6 discusses installing SunScreen on a Trusted Solaris 8 system.
- Chapter 7 contains instructions for upgrading your system to SunScreen 3.2 from SunScreen EFS 1.1, 2.0, 3.0, SunScreen 3.1, SunScreen 3.1 Lite, or SunScreen SPF-200, including how to preserve your existing configurations, as well as how to upgrade your cryptographic modules.
- Chapter 8 describes how to convert to SunScreen 3.2 from FireWall-1, releases 2.1, 3.0, or 4.0.
- Chapter 9 details removing the SunScreen software.
- Appendix A documents the command-line interface for installing SunScreen in its various modes of operation.
- Appendix B contains worksheets for planning your security policy, as well as instructions for choosing your initial security level.

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://www1.fatbrain.com/documentation/sun`.

Accessing Sun Documentation Online

The docs.sun.com^{SM} 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 purchased this product from Sun Microsystems™ and require technical support, contact your Sun™ sales representative or Sun Authorized Reseller.

For information on contacting Sun, go to the URL:
`http://www.sun.com/service/contacting/index.html`.

For information on Sun's support, go to the URL:
`http://www.sun.com/service/support/index.html`.

Typographic Conventions

The following table describes the typographic changes used in this book.

TABLE P–1 Typographic Conventions

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.`
`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*.
AaBbCc123	Book titles, new words, or terms, or words to be emphasized.	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.

TABLE P–2 Shell Prompts

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 lists sources for background information on network security, cryptography, and SunScreen.

- Schneier, Bruce, *Applied Cryptography*, John Wiley & Sons, 1996, 2nd edition, ISBN 0471128457

- Chapman, D. Brent, and Elizabeth D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, 1995, ISBN 1565921240
- Walker, Kathryn M., and Linda Croswhite Cavanaugh, *Computer Security Policies and SunScreen Firewalls*, Sun Microsystems Press, Prentice Hall, 1998, ISBN 0130960150
- Cheswick, Bill, and Steve Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994, ISBN 201633574
- Black, Uyless D., *Internet Security Protocols: Protecting IP Traffic*, 1st Edition, Prentice Hall, 2000, ISBN: 0130142492
- Comer, Douglas E., *Internetworking with TCP/IP, Volume 1*, Prentice Hall, 1995, ISBN 0132169878
- Doraswamy, Naganand and Dan Harkins, *IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 1st Edition, Prentice Hall, 1999, ISBN: 0130118982
- Stallings, William, *Network and Internetwork Security Principles and Practice*, Institute of Electrical and Electronics, 1994, ISBN 078031108
- Kaufman, Charlie, and Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, 1st Edition, Prentice Hall, 1995, ISBN 0130614661
- Garfinkel, Simson, and Gene Spafford, *Practical UNIX and Internet Security*, O'Reilly & Associates, 2nd edition, 1996, ISBN 1565921488
- Stevens, W. Richard, *TCP/IP Illustrated, Volume 1: The Protocols*, Addison-Wesley, 1994, ISBN 0201633469
- Farrow, Rik, *UNIX System Security: How to Protect Your Data and Prevent Intruders*, Addison Wesley, 1994, ISBN 020163469

Sun Software and Networking Security: `http://www.sun.com/security/`

CHAPTER 1

Installation Overview

This chapter gives an overview of the SunScreen software installation.

Topics covered include:

What Is SunScreen?

SunScreen is a layered software security solution that is installed on Solaris™-based systems to enable companies to connect their departmental networks to public internetworks securely. Depending on the type of installation, SunScreen can function as both a firewall and router (in routing mode) or like a bridge for hosts on the network it protects (in stealth mode.)

The Screen is the firewall responsible for screening packets. An Administration Station can be used to define objects and rules that form the security policy and to administer the Screen remotely. Administration can be performed on the Screen itself or from a remote Administration Station. The number of Screens and Administration Stations

depends on your site's network topology and security policies. The SunScreen firewall and administration software can be installed on a single system or on separate systems when using an Administration Station to remotely administer the Screen.

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

For encryption, SunScreen supports Internet Protocol Security (IPsec) with manual keying (see "IPsec Key" in the *SunScreen 3.2 Administration Guide*). Solaris Internet Key Exchange (IKE) and SunScreen Simple Key Management for Internet Protocol (SKIP) (see "Certificate Objects" in the *SunScreen 3.2 Administration Guide* for information about IKE and SKIP). SunScreen can be configured to encrypt packets using IPsec with manual keying or IKE, as well as with SKIP. IKE and SKIP can be used on the same Screen but they cannot encrypt the same traffic.

Note – To communicate with the Screen using IKE, you must download the `SUNWcryr` and `SUNWcryrx` packages onto the Administration Station from: `http://www.sun.com/software/solaris/encryption/download.html`. This requirement applies in the case of Solaris 9 only if you need to use encryption other than DES or 3DES (which are included with the operating system).

SunScreen Operation Modes

You can install the SunScreen software in routing mode or in stealth mode.

It is possible to mix the two modes so that the interfaces protecting your system from the outside network are stealth and the interfaces to your internal network are routing. When mixing modes, install the Screen in routing mode first, then configure the stealth interfaces.

Caution – Mixing interface modes requires careful consideration. Before you attempt this configuration, refer to the *SunScreen 3.2 Administration Guide* and the *SunScreen 3.2 Configuration Examples* documents, the latter of which includes an example of a mixed mode configuration.

Routing Mode

Choose routing mode when you need to filter packets between multiple networks connected by a Solaris-based system. A system in routing mode acts as both a router and a firewall. To use proxies or to install additional network services on the Screen, the interfaces must be configure in routing mode. Routing mode requires at least two exposed IP interfaces.

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

- Solaris software provides IP routing for the Screen.
- As with any router, the Screen is situated between subnets.
- Adding a new router to your network can require a reorganization of your network and renumbering of your hosts.
- Solaris software IP stack on the Screen's filtering interfaces exposes an IP address, as opposed to a stealth configuration that does not.

Stealth Mode

Choose stealth mode to increase your defense against attacks and when routing functions are not needed. In stealth mode, your system behaves like a bridge in that no IP interfaces are exposed to the public or private network and packets are filtered by the Screen transparently. While operating in stealth mode, the Screen cannot be seen or detected through `traceroute` or similar network tools.

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

- Packets are not routed, instead the Screen behaves like a bridge.
- IP address renumbering on hosts is not required.
- Only when using remote administration does any network interface need to be configured.

Security Issues

The systems that are used as gateways, or that are in vulnerable positions on the network, need only have the minimum Solaris software packages installed, which reduces the number of potentially exploitable applications (see "Software and Hardware Requirements" in this manual.

When installing SunScreen in stealth mode, you are asked if you want to harden the Screen. Hardening is optional and if chosen, automatically removes any Solaris software files and packages that might otherwise make the Screen vulnerable to an attack (in accordance with the best practices as described in

`http://www.sun.com/blueprints/browsesubject.html#security`). Hardening in SunScreen 3.2 is based upon JASS (JumpStart Architecture and Security Scripts). More information regarding JASS is available at: `http://www.sun.com/blueprints`. The hardening process can be performed during installation or at a later time by running the script: `/usr/lib/sunscreen/lib/harden_os`. For more information on hardening, see the "Installing in Stealth Mode With Remote Administration Using IKE" and "Installing in Stealth Mode With Remote Administration Using SKIP" chapters in this manual.

Note – Do not harden your Screen if some of your interfaces are in stealth mode and other interfaces are in routing mode. See the chapter "Configuring a Stealth Mode Screen" in the *SunScreen 3.2 Configuration Examples* document for an example of a mixed-mode configuration.

Before You Install SunScreen

Before installing SunScreen, complete the following tasks:

- Be acquainted with the SunScreen documentation set, especially the SunScreen 3.2 Release Notes document, which gives the latest product information.
- Make a map of your network. See "Determining Your Security Policy" in this manual for worksheets and instructions to aid you in determining your network configuration and your desired security level.
- Ensure that the system you have identified to run the SunScreen software is secure.
- Consider reinstalling the Solaris software from CD-ROM to ensure its stability.
- If you are running the Solaris 8 software, install the recommended kernel and security patches from `http://sunsolve.sun.com`. In addition, make sure the following patches are installed.
  - For all installations:
    - SPARC™ 108528-06; Intel 108529-05: kernel update patch.
  - For systems with a `qfe` board installed:
    - SPARC 108806-02: Sun Quad Fast Ethernet `qfe` driver patch.
  - For systems running Trusted Solaris 8:
    - SPARC 110337-02: Security CIPSO TCP kernel support patch.
- When using SKIP CA-issued keys and certificates, make sure a set is available for each host.

After installing the SunScreen software, you begin to set up and implement your network's security policy. For administrative instructions, refer to the *SunScreen 3.2 Administration Guide*. For examples of security policy configurations, see the *SunScreen 3.2 Configuration Examples* document. For more information regarding the SunScreen product, see *SunScreen 3.2 Administrator's Overview* document.

Software and Hardware Requirements

The table below lists the installation requirements for SunScreen 3.2.

SunScreen includes HotJava™ 1.1, SunScreen SKIP for Solaris, and IKE software.

To read the SunScreen documentation from the administration GUI, you must have the Adobe Acrobat Reader plug-in installed on your system.

Note – Because of a limitation in SunScreen SKIP, release 1.5.1 for Solaris, the RC2 encryption algorithm is not available when running Solaris 8 in 64–bit mode.

TABLE 1–1 SunScreen 3.2 Installation Requirements

Requirement	Description
Operating environment	■ Solaris 9 (with IPv4 only) in either 32–bit or 64–bit mode for (SPARC systems only) ■ Trusted Solaris 8 (SPARC systems only)
Browsers supported:	■ A Java™-enabled Web browser compliant with JDK™, release 1.1.3 through 1.1.8 ■ HotJava™ 1.1 running on the SPARC platform ■ Internet Explorer 4.0 (with or without the Java plug-in) on the Windows platform ■ Netscape 4.0.1 or higher, can be used for all administrative functions except those requiring local file access. (See below for system requirements for Internet Explorer and Netscape to run Java plug-ins.) ■ Note that a Solaris platform with SKIP and/or IKE installed can be used as an Administration Station for command line-based remote administration.

TABLE 1–1 SunScreen 3.2 Installation Requirements *(Continued)*

Requirement	Description
Hardware	■ All SPARCstation™ workstations, UltraSPARC systems supported by the Solaris 9 operating environment. ■ All SPARCstations and UltraSPARC systems supported by Trusted Solaris 8.
Disk space	Minimum of 1 Gbyte (with at least 300 Mbytes unused). This space is needed for the following: ■ configuration database = `/etc/sunscreen` = 10 MB[1] ■ logs and temporary files = `/var/sunscreen` = 120 MB[2] ■ internal files = `/usr/lib/sunscreen` = 50 MB ■ man pages = `/usr/share/man` = 1 MB
Memory	■ For administration software installation: a minimum of 32 Mbytes is required and 64 Mbytes is *strongly* recommended. ■ For Screen–only software installation: a minimum of 32 Mbytes.
Network interfaces supported	For the Screen:[3] 1. For SPARC and UltraSPARC systems in routing mode: ■ 10–Mbps or 100–Mbps Ethernet interfaces (`le`, `qe`, `hme`, `be`, `qfe`, `pnet`) ■ Gigabit Ethernet (ge) interfaces ■ Token Ring interfaces (trp) ■ ATM (155 and 622 Mbps) in LAN emulation mode (lane) or classic IP mode (ba) ■ FDDI (nf), or PCI-based Ethernet cards 2. For SPARC and UltraSPARC systems in stealth mode: 10–Mbps, 100–Mbps, Fast Ethernet, or Gigabit Ethernet interfaces 3. High availability requires that the two machines be connected by means of a nonswitching hub.[4] For the Administration Station:[5] 1. For SPARC systems: 10–Mbps or 100–Mbps Ethernet interfaces (`le`, `qe`, `hme`, `be`, `qfe`), or FDDI, or PCI-based Ethernet cards. 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.
Media	CD-ROM drive (and a diskette drive, if you are using certain types of CA-issued certificates.

1. Can grow larger over the course of hundreds of policy or configuration changes
2. Can grow larger if the SunScreen log size parameter is increased from its default of 100 MB
3. The Screen can support up to 15 stealth interfaces at one time.

Stealth configurations do not support ATM, FDDI, token ring, or the use of proxies.

SunScreen HA in routing mode does not support FDDI, token ring, ATM, Gigabit Ethernet, or failover of IKE-based IPsec connections

4. Some switches, including Alteon, Radware's Fireproof, and Foundry's ServerIron, can be configured to work with SunScreen HA clusters. Each Screen is set up as an individual Screen, with different IP addresses, and no interconnect. You can use as many Screens as the switch supports. Note that because SunScreen is a stateful firewall, TCP connections do not failover.
5. 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).

Operating System Package Requirements

Ensure that the required Solaris software packages reside on the Screen and the Administration Station as described below.

Note – Install third-party content scanning products on a system separate from your SunScreen firewall to avoid possible security risks, as well as to avoid overloading your system when the content is large.

Solaris Software Packages for the Screen

When installing the SunScreen software on your Screen remotely from an Administration Station or if you choose to use the command-line interface instead of the administration GUI, install the Solaris Core Distribution software as well as the packages listed in the following table from your Solaris CD, if not already on your system.

Note – When installing only the Solaris Core Distribution software, either change your DISPLAY variable for using the installer to a windowing system or install SunScreen using the command-line installation procedure described in the "Command Line Installation" appendix in this manual.

When installing the SunScreen software on your Screen locally, install the Solaris End User Distribution software as well as the packages listed in the following table from your Solaris CD, if not already on your system.

TABLE 1–2 Solaris Packages for Screen System

Package Name	Description
SUNWlibc	Sun Workshop Compilers Bundled libC
SUNWlibms	Sun WorkShop Bundled shared libm
SUNWsprot	Solaris Bundled tools
SUNWxwplt	X Window System platform software
SUNWmfrun	Motif RunTime Kit
SUNWloc	System Localization
SUNWxwice	X Window System Inter-Client Exchange (ICE) Components
SUNWxwrtl	X Window System & Graphics Runtime Library Links in /usr/lib
SUNWtoo	Programming Tools
SUNWtoox	Programming Tools (64–bit)
SUNWeuluf	UTF-8 L10N For Language Environment User Files
SUNWeulux	UTF-8 L10N For Language Environment User Files (64-bit)
SUNWjvrt	JavaVM run time environment
For Trusted Solaris 8 only SUNWj2rt	JDK 1.2 run time environment
For Solaris 9 only SUNWj3rt	J2SDK 1.4 runtime environment
SUNWapchr	Apache Web Server (root)
SUNWapchu	Apache Web Server (usr)
SUNWeu8os	American English/UTF-8 L10N For OS Environment User Files
SUNWeu8osx	American English/UTF-8 L10N For OS Environment User Files (64-bit)
SUNWcryr	Cryptography packages for IKE. Optional for Solaris 9 unless AES or Blowfish is required. Required for Trusted Solaris.
SUNWcryrx	Cryptography packages for IKE(64–bit). Optional for Solaris 9 unless AES or Blowfish is required. Required for Trusted Solaris.

Solaris Software Packages for the Administration Station

When installing the SunScreen software remotely using the administration GUI, install the following packages on your Administration Station from your Solaris CD, if not already on your system.

TABLE 1–3 Solaris Packages for Administration Station

Package Name	Description
`SUNWjvrt`	JavaVM run time environment
`SUNWxwplt`	X Window System platform software
`SUNWmfrun`	Motif RunTime Kit
`SUNWcryr`	Cryptography packages for IKE. Optional for Solaris 9 unless AES or Blowfish is required. Required for Trusted Solaris 8.
`SUNWcryrx`	Cryptography packages for IKE(64–bit). Optional for Solaris 9 unless AES or Blowfish is required. Required for Trusted Solaris 8.

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

Additional Requirements and Restrictions

- Use the command-line interface to create IKE self-generated certificates.
- SunScreen 3.2 on the Solaris 8 operating environment supports IPv4 packets according to the policy but blocks IPv6 packets.
- A routing-mode Screen supports an unlimited amount of network interfaces, all of which must be configured in Solaris; while a stealth-mode Screen supports up to 15 network interfaces at one time, and only the network interface that is used for remote administration is configured in Solaris. See the documentation accompanying your Solaris software.
- The SunScreen CD includes the SunScreen SKIP, revision 1.5.1, software. The SunScreen SKIP version of Windows 95/98 and NT4.0 is available separately.

- A remote Administration Station connects directly to a Screen only through an Ethernet local area network (LAN) or a Fiber Distributed Data Interface (FDDI). Once connected directly to the network by way of an Ethernet or FDDI connection, it can connect to the Screen by an asynchronous transfer mode (ATM) or Token Ring LAN.

Encryption Requirements

ForTrusted Solaris 8, to use IPsec manual keying or IKE, you must download the `SUNWcryr` and `SUNWcryrx` encryption packages onto both the Screen and the Administration Station.

For Solaris 9, support for DES and 3DES is built into the operating system. You only need to download the encryption packages if you need support for AES or Blowfish.

In either case, to download the packages go to `http://www.sun.com/software/solaris/encryption/download.html`

Web Server Requirements

For downloading the Java applets used by the administration GUI, the the Solaris 8 and 9 software uses Apache Web Server.

Note – Web server onfiguration files are contained in `/etc/sunscreen/httpd/`.

Web Browser Requirements

SunScreen allows any system with a Java-enabled Web browser compliant with JDK 1.1.3 through 1.1.8 to function as an Administration Station. However, the version of the JVM™ or plug-in you are using with the browser dictates the operations you are able to perform on the Administration Station.

HotJava 1.1.5 is included on the SunScreen CD.

You can use any supported browser to look at status information and logs as well as modify and save policy configurations. However, some browser configurations do not support local system access.

Note – The Netscape Navigator™ default Java plug-in provided with the Solaris 8 software is not compatible with the SunScreen 3.2 administration applet. To save log files and load certificates using Netscape Navigator 4.5 or higher, you must install the older version (version 1.1.2, which is included in the SunScreen distribution) of the Java plug-in or use the HotJava browser (included).

How to install the Java plug-in, version 1.1.2, save the `identitydb.obj` file, and set the `NPX_PLUGIN_PATH` environment variable is described in"Administration GUI Browser Requirements" section of this chapter.

Trusted Solaris

You can install and use SunScreen 3.2 on systems running Trusted Solaris 8 . See "Installing on Trusted Solaris" in this manual for more information.

High Availability

High availability (HA) enables you to deploy groups of Screens together in situations in which the connection between a protected inside network and an insecure outside network is critical. For a detailed description regarding installing an HA cluster, see "Using High Availability" in the *SunScreen 3.2 Administration Guide*.

Upgrading Your System to SunScreen 3.2

The SunScreen CD includes software to upgrade to SunScreen 3.2 for the following:

- SunScreen 3.1 and SunScreen 3.1 Lite
- SunScreen EFS 1.1, 2.0, and 3.0
- SunScreen SPF-200

Detailed instructions for upgrading your SunScreen system are in "Upgrading to SunScreen 3.2" in this manual.

Converting From FireWall-1 to SunScreen

To use your existing FireWall-1 configurations for a similar security policy on SunScreen, you can either: Convert the FireWall-1 system to become the Screen or convert the FireWall-1 security policies and use them on a system running SunScreen. See “Converting FireWall-1 to SunScreen in Routing Mode” in this manual.

Links to Other SunScreen Features

SunScreen 3.2 includes:

- “Network Address Translation (NAT) Rules” in the *SunScreen 3.2 Administration Guide*
- “Virtual Private Network (VPN) Rules” in the *SunScreen 3.2 Administration Guide*
- “Setting Up and Using Proxies” in the *SunScreen 3.2 Administration Guide*
- “Configuring Centralized Management Groups” in the *SunScreen 3.2 Administration Guide*
- “Getting Status and Managing Logs” in the *SunScreen 3.2 Administration Guide*
- “Using the Command Line Interface” in the *SunScreen 3.2 Administration Guide*
- “About SunScreen Lite” in the *SunScreen 3.2 Administration Guide*
- “Quick Start Procedures” in *SunScreen 3.2 Administration Guide*

CHAPTER 2

Installing in Routing Mode With Local Administration

This chapter describes how to install SunScreen in routing mode on a locally administered Screen (the default method of installation). Choose this method when you need your system to function both as a router and as a firewall.

Topics covered include:

Installing the Screen with Local Administration

The Solaris Web Start installer guides you through installing both the administration and Screen software on a local system. Because a locally administered Screen does not send administrative commands over the network, it is not necessary to set up encrypted communication during installation. To use this type of installation, just accept all of the default selections given for a Typical installation which is a locally administered routing firewall that allows common services to pass.

Before you begin the installation:

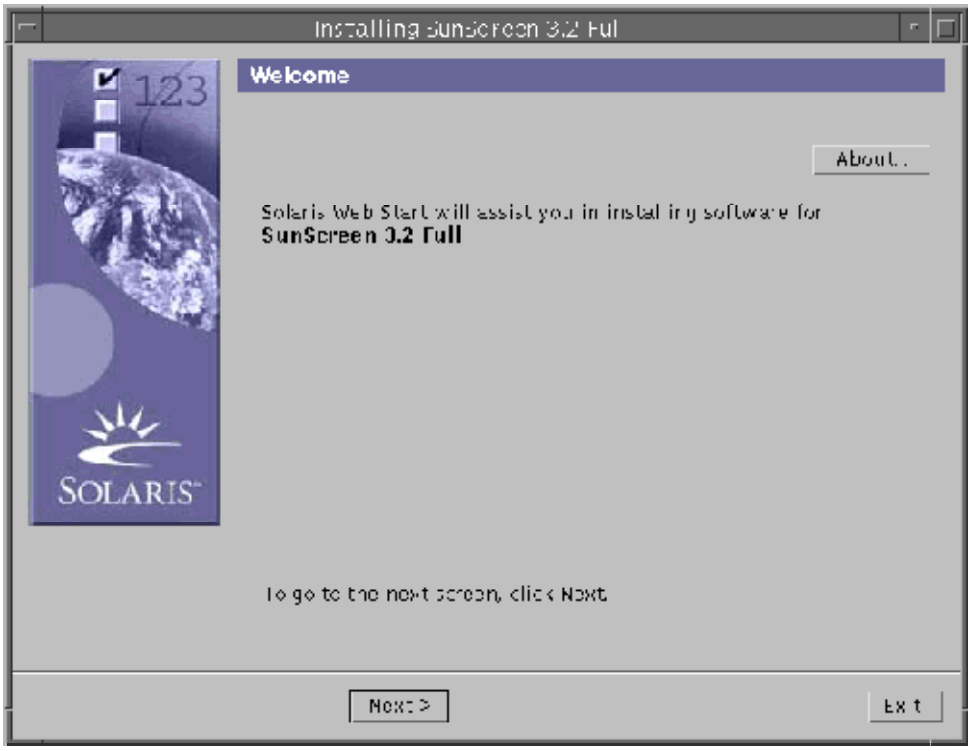
- Make sure your system is performing properly as a router.
- Review the *SunScreen 3.2 Release Notes* for the latest product information.
- Read all of the information in the "Installation Overview" chapter.
- Make a map of your network. See the "Determining Your Security Policy" appendix for worksheets and instructions to aid you in determining your network configuration and your desired security level.

▼ To Install a Locally Administered Screen

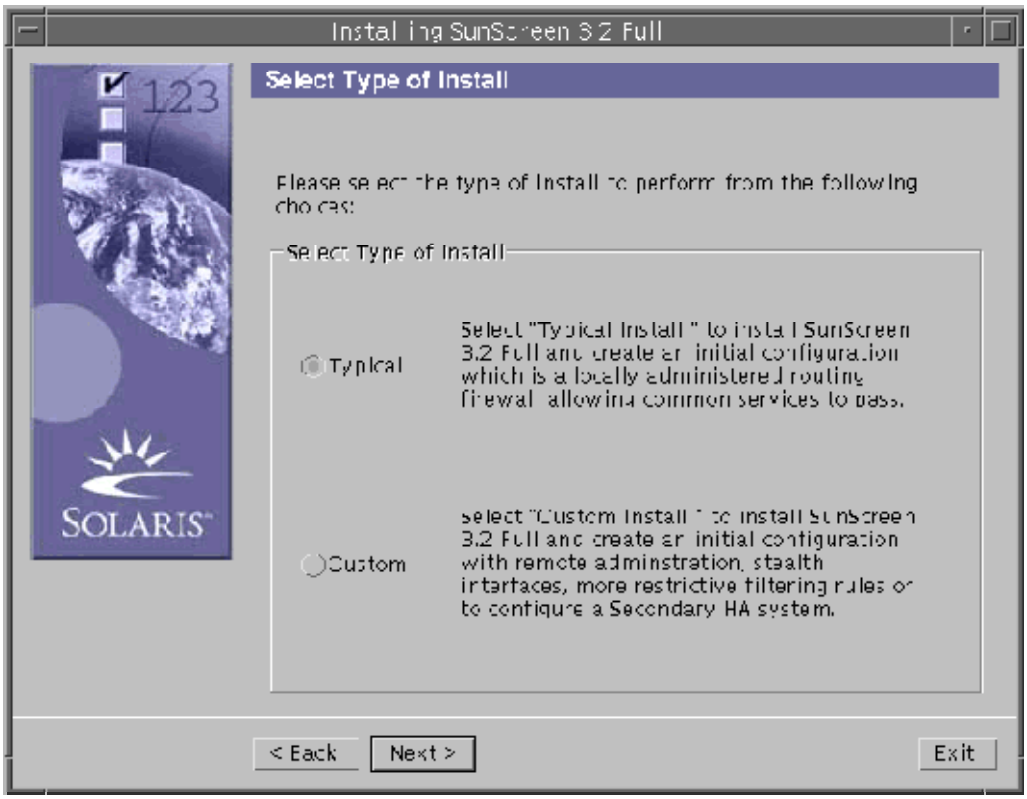
1. **Open a terminal window on your system and become root, if not already.**
2. **Insert the SunScreen CD into the CD-ROM drive.**
   A File Manager window appears listing the CD contents.
3. **Double-click the install icon to start the installation.**

Note – You are prompted to type the root password for your system if the installer is started as a user other than root.

The Welcome window appears.



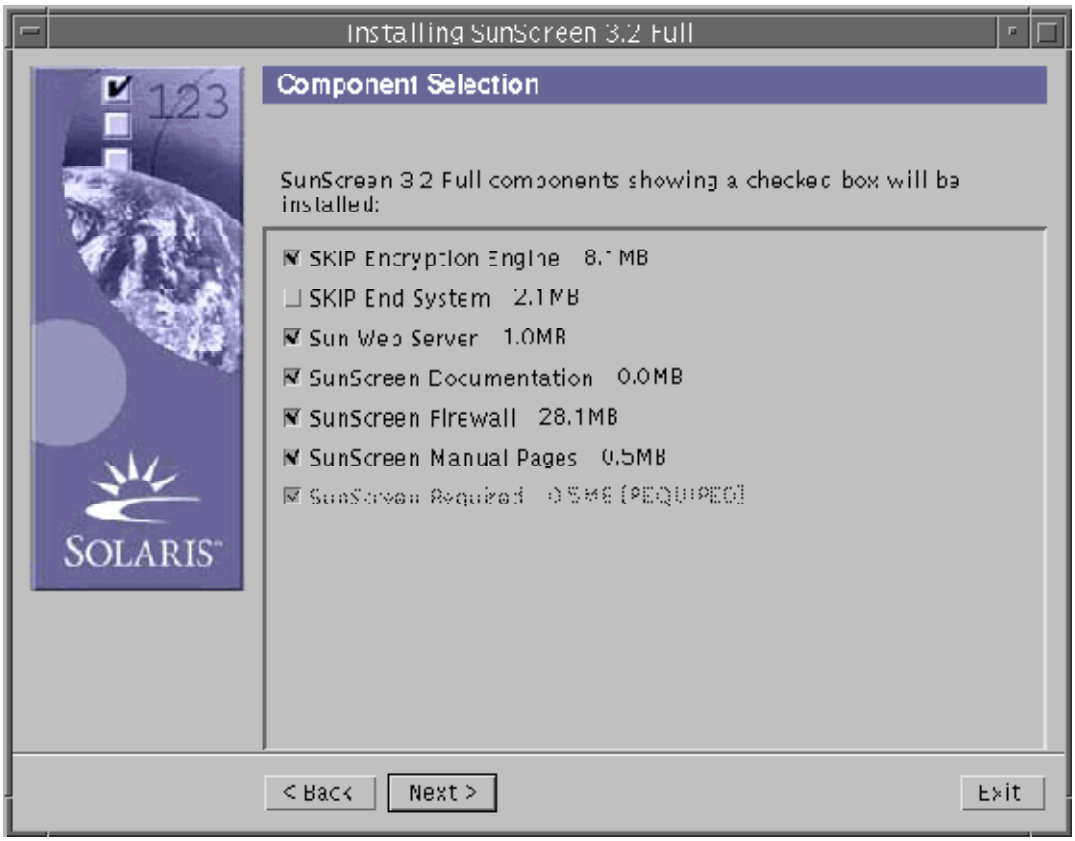
4. **In the Welcome window, click Next to continue.**
   The Select Type of Install window appears with Typical as the default entry.



5. **In the Select Type of Install window, accept the Typical default entry by clicking Next to continue.**

   A Typical installation installs SunScreen 3.2 and creates an Initial configuration, which is a locally administered routing firewall that allows common services to pass.

   The Component Selection window appears listing the components to be installed.



6. **In the Component Selection window, click Next to continue.**

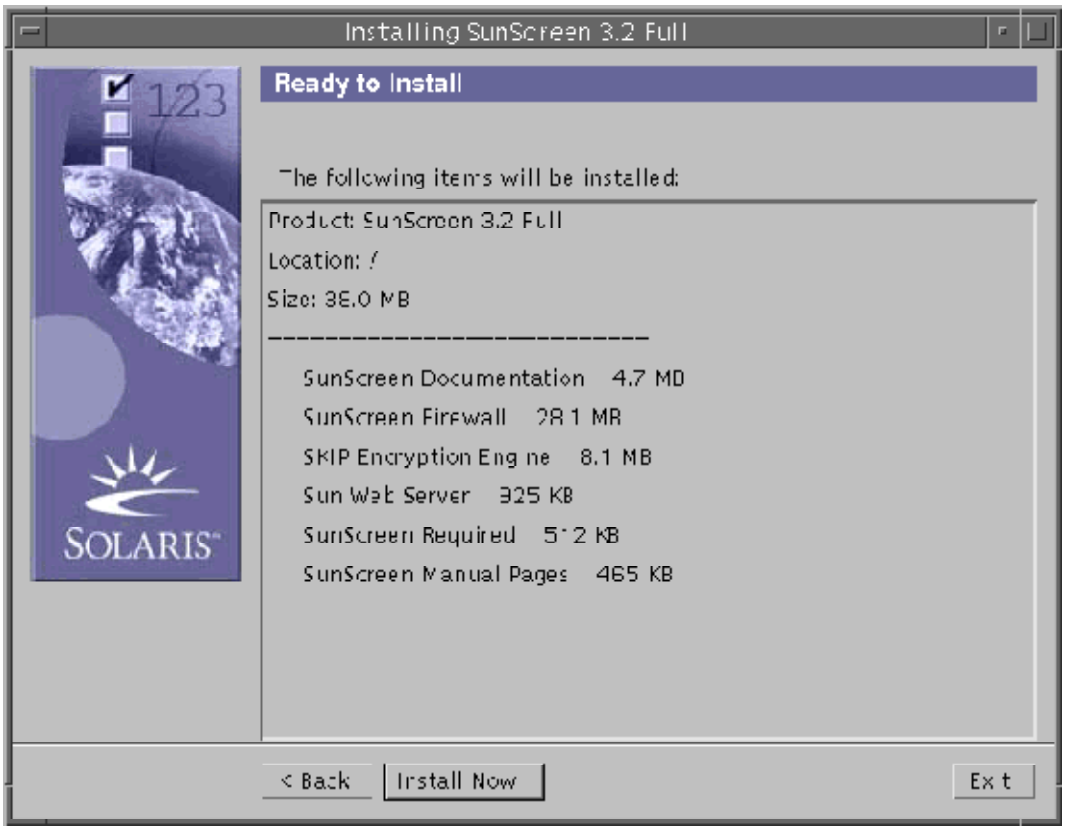
   The Checking System window appears and checks for any existing SunScreen configurations. If none are found, a message announces System check complete.

Note – If existing configurations are discovered, the Old Configurations window appears in which you are asked to select either Remove or Retain. The default is to Remove the existing configuration and create a new Initial configuration based on the set of inputs. Click Retain to keep the existing configurations and not create a new Initial configuration.

---

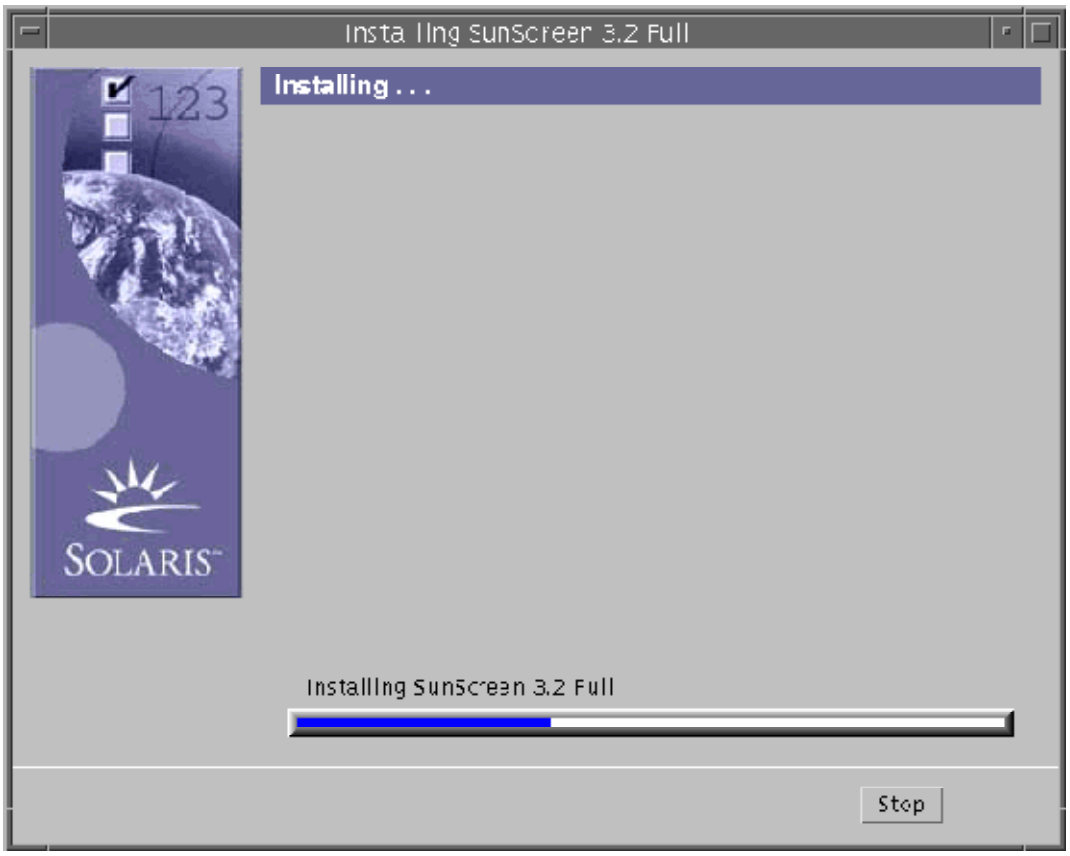
7. **In the Checking System window, click Next to continue**

   The Ready to Install window appears listing the items to be installed.

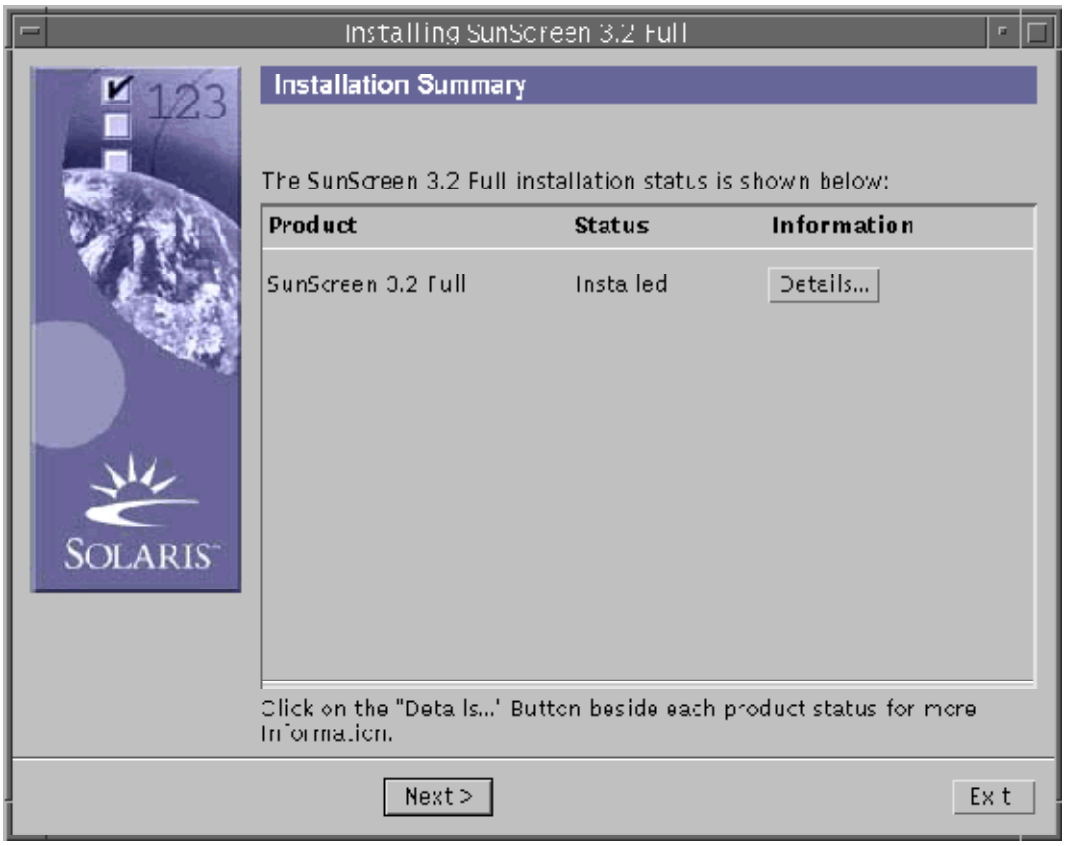


8. **In the Ready to Install window, verify that the correct items are listed, and click Install Now to continue.**

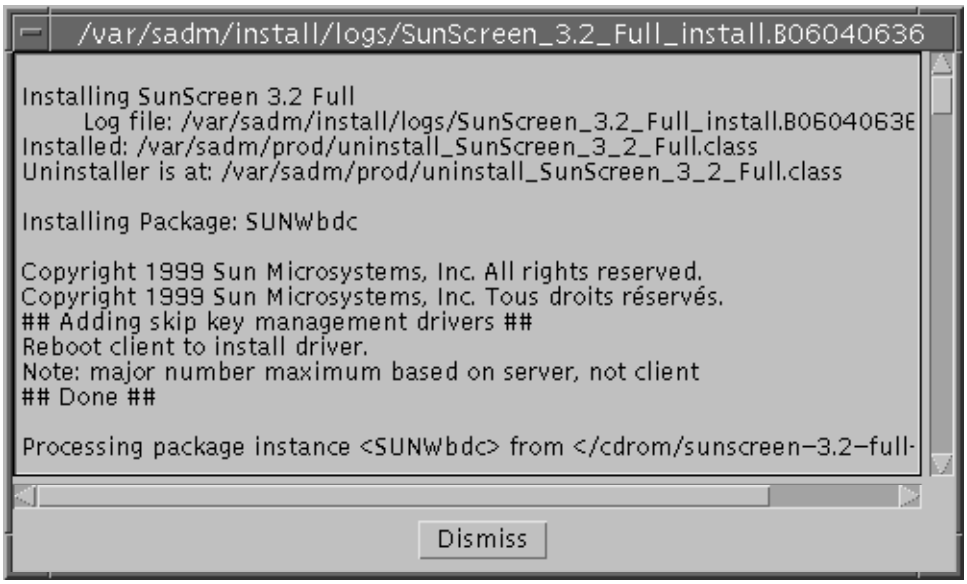
   The Installing window appears with a status bar showing the progress of the installation.



When the installation is complete, the Installation Summary window appears showing the product installed and its status.



For more information, click the Details button for a comprehensive list of the successfully installed packages and their locations.



The Checking System window appears and the installer verifies that all required Solaris and SunScreen software packages are installed.

- If the required packages are installed, a message appears announcing System check complete.
- If all required packages have not been installed, exit the installer, install the missing packages, and rerun the installer to complete the SunScreen configuration.

9. **In the Checking System window, click Next to continue.**

   The Verify Configuration Settings window appears showing the settings to be used for the Initial configuration. You have three options from which to choose: Back, Configure Now, or Exit.

10. **In the Verify Configuration Settings window, click Configure Now.**

    The Screen Configuration window appears showing that the Initial Configuration is generated based upon the Screen type, Administration type, certificate information, and security level.

    - If the configuration is successful, it announces that this configuration is compiled and activated.
    - If the configuration fails, an error message appears giving the results of the failure.

The Installation and Configuration Complete window appears and if successful, it announces that the installation and configuration of SunScreen 3.2 is complete. You can select Back to delay exiting the program, or you can select Exit to leave the program.

11. **To complete the installation, click System Reboot.**

    The installer is dismissed.

Note – To complete the installation process you must reboot the system at this time. If you do not wish to reboot your system, click Next instead of Reboot System.

Managing Your Firewall

Use the administration GUI to manage your SunScreen firewall. See the *SunScreen 3.2 Administrator's Overview* and the *SunScreen 3.2 Administration Guide* for more information.

▼ To Launch the Administration GUI

1. **Open a Java-enabled Web browser and launch the administration GUI by typing the URL:** `http://localhost:3852`**.**

   The administration GUI appears.

Note – When trying to launch the administration GUI, if you encounter the error: The requested item could not be loaded by the proxy, you must disable proxy usage by specifying localhost in the Don't Proxy list, and then try to launch the GUI again.

---

2. **To login, type the following user name and password, then click Login.**

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

Note – Change the default User Name and Password to something more secure.

CHAPTER 3

Installing in Routing Mode With Remote Administration Using SKIP

This chapter describes how to install the SunScreen software in routing mode with remote administration using SKIP encryption technology. This installation scenario is a three-step process that requires you to first install the appropriate software on an Administration Station, then install the software on the Screen, and last, establish encrypted communication between the Administration Station and the Screen.

Topics in this chapter include:

Note – This chapter describes installing the SunScreen software using the GUI installer; however, if you are installing on a system without a monitor, use the command-line installation described in "Command Line Installation" in the *SunScreen 3.2 Installation Guide*.

Before installing, review the *SunScreen 3.2 Release Notes* for the latest product information.

Note – Be sure to make a map of your network before you begin this installation. See "Determining Your Security Policy" in the *SunScreen 3.2 Installation Guide* appendix, which includes worksheets and instructions to aid you in determining your network configuration and your desired security level.

Supported Administration Station Configurations

The SunScreen CD includes SKIP for both SPARC and Intel platform editions. Using SKIP allows any hardware running the Solaris 2.6, Solaris 7, or Solaris 8 operating environments to be an Administration Station.

Any system operating Solaris 2.6, Solaris 7, or Solaris 8 with SunScreen and a Java-enabled Web browser compliant with JDK 1.1.3 through 1.1.8 that can connect securely to the Screen using SKIP can be used as an Administration Station.

Although systems operating Windows 95, Windows 98, or NT 4.x with PC SKIP, or Windows 2000 with IKE are supported platforms for an Administration Station, this chapter covers Solaris-based Administration Stations only.

Note – For details regarding SKIP, see either the *SunScreen SKIP User's Guide, Release 1.5.1*, or the *SunScreen SKIP User's Guide, Release 3.0.7, for the Microsoft Windows NT, Windows 95, and Windows 98 Operating Environments* documentation.

Routing Mode Installation Summary

The Solaris Web Start Wizards installer guides you through installing the SunScreen software on systems using SKIP UDH self-generated or SKIP CA-issued certificate technology for encryption.

Perform the installation in the following order:

1. On the Administration Station
   a. Install the administration software.
   b. Create the Administration Station's SKIP certificate.
2. On the Screen

a. Install the SunScreen software.

   This step requires the Administration Station's certificate ID.

b. Create the Screen's SKIP certificate.

3. On the Administration Station, install the Screen's certificate to begin encrypted communication.
4. Use the administration GUI on the remote Administration Station to manage your Screen.

The following sections describe the installation procedures for installing the SunScreen software and how to establish encrypted communication using SKIP certificate technology.

Do not begin this procedure until you have read the information in "Defining Security Policies" in the *SunScreen 3.2 Installation Guide*.

Installing the Administration Software on the Administration Station

1. **Open a terminal window on your system and become root, if not already.**
2. **Insert the SunScreen CD into the CD-ROM drive.**

   A File Manager window appears listing the CD contents.
3. **Double-click the install icon to start the installation.**

Note – You are prompted to type the root password for your system if the installer is started as a user other than root.

The Welcome window appears.

4. **In the Welcome window, click Next to continue.**

Note – The Welcome window includes an About button that you can click for information regarding the Web server used. Click the Dismiss button when done.

The Install Type window appears with Typical as the default entry.

5. **In the Install Type window, select Custom and click Next to continue.**

   The Functions window appears with both Screen and Administration selected as the default entry.

6. **In the Functions window, select Administration only by deselecting the Screen box, then click Next to continue.**

   The Component Selection window appears with all components except "Sun Web Server" and "SunScreen Firewall" selected as the default entry.

7. **In the Component Selection window, accept the default and click Next to continue.**

   The Install Verification window appears containing a list of components to be installed.

8. **After verifying that the list of components is correct, click Install Now to continue.**

   The Installation Summary window appears. Upon successful completion, the status reads "Installed."

Note – To see a list of the added components, click the Details button.

---

9. **In the Installation Summary window, click Next to continue.**

   The Checking System window appears. The installer verifies that all required Solaris software and SunScreen packages are installed.

   - If the required packages are installed, a message appears announcing System check complete.
   - If all required packages have not been installed, exit the installer, install the missing packages, and rerun the installer to complete the SunScreen configuration.

10. **In the Checking System window, if the required packages are installed, click Next to continue.**

    The Administration Station Configuration window appears and displays the results of the Administration Station's configuration.

11. **In the Administration Station Configuration window, click Next to continue.**

    The Installation and Configuration Complete window appears from which you must exit the installation to install the administration certificate.

12. **In the Installation and Configuration Complete window, click Exit to finish the installation.**

    The installer is dismissed.

    After installing the required software packages on the Administration Station, you continue the process by creating the Administration Station's SKIP certificate.

Note – Both the Administration Station and the Screen need certificates before encrypted communication can begin.

Creating the Certificate on the Administration Station

Use the command-line interface to create SKIP UDH self-generated certificates (the default) or to load SKIP CA-issued certificates on the Administration Station, as described in the following procedures.

▼ To Create the SKIP UDH Self-Generated Certificate on the Administration Station

1. **Open a terminal window and become root, if not already.**
2. **Create the required SKIP directories by typing:**

   ```
   # skiplocal -i
   ```

3. **Create the SKIP UDH certificate on the Administration Station by typing:**

   ```
   # skiplocal -k -f -V -m key_size
   ```

   Note – For *key_size*, you type either 512, 1024, 2048, or 4096 (the latter being the default for this release). Make sure that you use the same *key-size* when generating the Screen's certificate.

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

   Note – For export control regulatory assistance, consult the U.S. Department of Commerce, Bureau of Export Administration: `http://www.bxa.doc.gov`.

   ---

4. **Write down the certificate ID, which begins with '0x'.**

   This information is required when "Installing the SunScreen Software on the Screen" on page 45.

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
   ```

Continue to the section "Installing the SunScreen Software on the Screen" on page 45.

▼ To load a SKIP CA-Issued Certificate on the Administration Station

1. **Open a terminal window and become root, if not already.**
2. **Load the required SKIP directories by typing:**

   ```
   # skiplocal -i
   ```

3. **Insert the SKIP CA-issued 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 SKIP CA-issued Key and Certificate diskette by typing:**

   ```
   # eject floppy0
   ```

8. **Write down the eight-character certificate ID.**

   This information is required when "Installing the SunScreen Software on the Screen" on page 45.

9. **Add SKIP to all the interfaces by typing:**

   ```
   # skipif -a
   ```

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

    ```
    # sync; init 6
    ```

    Continue to the following section "Installing the SunScreen Software on the Screen" on page 45.

Installing the SunScreen Software on the Screen

Note – Before proceeding, make sure that all network interfaces you plan on using are configured. Configured interfaces are those displayed with `# ifconfig -a`. For details on the Solaris network interface configuration, see your Solaris software documentation.

After adding SKIP certificates on the Administration Station, you install the SunScreen software on the Screen. This procedure requires the Administration Station's SKIP certificate ID (MKID).

You can use the installer if a monitor and a keyboard are attached to your Screen. If you are operating the Screen without a monitor, you must either temporarily attach a monitor or install the software through the command line (see "Command Line Installation" in the *SunScreen 3.2 Installation Guide*).

▼ To Install the Software on the Screen

1. **Open a terminal window on your system and become root, if not already.**
2. **Insert the SunScreen CD into the Screen's CD-ROM drive.**
   A File Manager window appears that lists the contents of the CD.
3. **Double-click the install icon to invoke the SunScreen installer, which brings up the Welcome window.**

Note – You are prompted to type the root password for your system if the installer is started as a user other than root.

---

4. **In the Welcome window, click Next to continue.**
   The Install Type window appears with Typical selected as the default entry.
5. **Select Custom in the Install Type(s) window and click Next to continue.**
   The Functions window appears with both Screen and Administration selected as the default entry.
6. **In the Functions window, accept the default entry and click Next to continue.**
   The Component Selection window appears with all components except "SKIP End System" selected as the default entry.

Note – Never add the end-system SKIP packages `SUNWes` and `SUNWesx` to the Screen.

7. **In the Component Selection window, accept the default entry and click Next to continue.**

   The Checking System window appears and lists any existing SunScreen configurations found by the installer.

8. **In the Checking System window click Next to continue.**

   - If an existing configuration was found, the Old Configurations window appears. Select Remove or Retain, as appropriate, and click Next to continue.
     - If Retain is selected, the Ready To Install window appears, and you can go to Step 10.
     - If Remove is selected, the Secondary HA window appears with No selected as the default entry.
   - If no existing configurations were found, the Secondary HA window appears with No selected as the default entry.

9. **In the Secondary HA window, accept the No default entry and click Next to continue.**

   The Screen Type window appears with Routing selected as the default entry.

10. **In the Screen Type window, accept the default entry and click Next to continue.**

    The Administration Type window appears with Local Administration selected as the default entry.

11. **In the Administration Type window, select Remote Administration and click Next to continue.**

    The Ready to Install window appears and lists the components for you to verify.

12. **After you verify that the components shown in the list are correct, click Install Now to continue.**

    The Installation Summary window appears and shows the status of the installation, which upon a successful completion, reads “Installed.”

Note – To see a list of the added components, click the Details button.

13. **In the Installation Summary window, click Next to continue.**

    The Checking System window appears wherein the installer verifies that all required Solaris software and SunScreen packages are installed.

    - If the required packages are installed, a message appears announcing System check complete.

- If all required packages have not been installed, exit the installer, install the missing packages, and rerun the installer to complete the SunScreen configuration

14. **In the Checking System window, click Next to continue.**

    The Select Certificate Type window appears with UDH self-generated certificates selected as the default entry. The following section describes how to create the SKIP certificate on the Screen.

Creating the SKIP Certificate on the Screen

After installing the required software packages on the Screen, you continue the process by creating the Screen's SKIP certificate, as described in the following procedures

---

Note – Both the Administration Station and the Screen need certificates before encrypted communication can begin.

▼ To Create the SKIP UDH Self-Generated Certificate on the Screen

1. **In the Select Certificate Type window, accept the default entry and click Next to continue.**

   The Self Generated Certificate ID window appears.

2. **In the Self Generated Certificate ID window, type the Administration Station's certificate ID (do not type the leading 'Ox') in the text entry field and click Next to continue.**

   The Select Administration SKIP Key Length window appears with 4096–bit key length as the default.

Note – The Screen's key length must match the UDH self-generated certificate key length you created previously for the Administration Station (see "Creating the Certificate on the Administration Station" on page 43). You must specify the Administration Station's key in the SKIP Key Length window if it is less than the 4096–bit default key length.

---

3. **After selecting the appropriate key length, click Next to continue.**

The Generate Screen Certificate window appears and displays the Screen's generated SKIP certificate key ID.

4. **In the Generate Screen Certificate window, click Next to continue.**

   The Security Level window appears with Permissive as the default entry.

Note – The security levels are: Permissive, the default, allows almost all traffic through; Secure restricts access to the Screen but allows connections from the Screen; and Restrictive only allows encrypted administration traffic to the remote Administration Station. You can change an initial security level later, as needed. See "Defining Security Policies" in the *SunScreen 3.2 Installation Guide*.

---

5. **After selecting the appropriate security level, click Next to continue.**

   The Name Service window appears with both NIS and DNS name services selected as the default.

6. **After selecting the appropriate name services, click Next to continue.**

   The Verify Configuration window appears.

7. **After verifying that the information is correct, click Configure Now to continue.**

   The Screen Configuration window appears and instructs you, upon a successful configuration, to consult the `/etc/sunscreen/AdminSetup.readme` file on the Screen for instructions on completing the Administration Station setup.

8. **In the Screen Configuration window, click Next to continue.**

   The Installation and Configuration Complete window appears and prompts you to reboot your system.

9. **In the Installation and Configuration Complete window, click Reboot Now to complete the installation.**

   The installer is dismissed.

Note – To complete the installation process you must reboot the system at this time. If you do not wish to reboot your system, click Next instead of Reboot System.

You are now ready to complete the installation on the Administration Station as described in "Completing the SKIP Certificates Installation Procedure" on page 50.

▼ To Load the SKIP CA-Issued Certificate on the Screen

1. **Select SKIP CA-Issued Certificate from the Select Certificate Type window (the default is SKIP UDH Certificate) and click Next to continue.**

The Issued Certificate Key Diskettes window appears.

2. **Insert the Administration Station's Key and Certificate diskette into the diskette drive and click Read Diskette.**

   Wait until the SKIP CA-issued certificate ID appears at the bottom of the window.

3. **Write down the Administration Station's eight-character certificate ID and click Next to continue.**

   This certificate ID is required to complete the Administration Station installation.

4. **Insert the Screen's Certificate ID diskette into the diskette drive and click Read Diskette.**

   The SKIP CA-issued certificate ID for the Screen appears at the bottom of the window.

5. **Write down the Screen's eight-character certificate ID and continue to the Select Initial Security Level window.**

Note – The security levels are: Permissive, the default, allows almost all traffic through; Secure restricts access to the Screen but allows connections from the Screen; and Restrictive only allows encrypted administration traffic to the remote Administration Station. You can change an initial security level later, as needed. See "Defining Security Policies" in the *SunScreen 3.2 Installation Guide*.

---

6. **After selecting the appropriate security level, click Next to continue.**

   The Name Service window appears .

7. **After selecting the appropriate name services, click Next to continue.**

   The Screen Configuration window appears and instructs you, upon a successful configuration, to consult the `/etc/sunscreen/AdminSetup.readme` file on the Screen for instructions on completing the Administration Station setup.

8. **In the Screen Configuration window, click Next to continue.**

   The Reboot System window appears.

9. **To complete the installation, click System Reboot.**

   The installer is dismissed.

Note – To complete the installation process you must reboot the system at this time. If you do not wish to reboot your system, click Next instead of Reboot System.

To complete the installation and establish encrypted communication between the Administration Station and the Screen using SKIP certificate technology, you load the Screen's SKIP certificate information on the Administration Station, as described in the following procedure.

Completing the SKIP Certificates Installation Procedure

After installing the SunScreen software and the SKIP certificates on the Screen, the Screen's certificate information must be loaded onto the Administrating Station to complete the installation. This information is located on the Screen in the `/etc/sunscreen/AdminSetup.readme` file.

The following procedure explains how to display this file.

▼ To Display the `/etc/sunscreen/AdminSetup.readme` File

1. **Display the `/etc/sunscreen/AdminSetup.readme` file by typing:**

   ```
   # more /etc/sunscreen/AdminSetup.readme
   ```

   The `AdminSetup.readme` file contains the Screen's certificate ID as well as the command run to give the Administration Station the Screen's certificate ID.

   This command adds the Screen to the ACL with the necessary encrypting parameter settings. If it executes successfully, then the configuration is complete, and you can go to "To Configure the Administration Station to Communicate With the Screen Using SKIP" on page 50.

2. **Write down the command, which begins with `skiphost -a`, that is requried in the next procedure.**

Note – You can use ftp to copy the `/etc/sunscreen/AdminSetup.readme` file onto the Administration Station if you trust that the network between the Screen and Administration Station is secure. Otherwise, display the file and write down the information for use in the next section.

Instructions for using SKIP from the command line are in the "Using the Command-Line Interface" in *SunScreen SKIP User's Guide, Release 1.5.1.*

▼ To Configure the Administration Station to Communicate With the Screen Using SKIP

The following steps describe how to load the SKIP encryption software onto the Administration Station.

If the `AdminSetup.readme` file was not copied to the Administration Station using `ftp` (or if the `skiphost -a` command fails), execute the following steps using the information obtained from that file.

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

2. **Launch the `skiptool` GUI by typing:**

```
# skiptool &
```

Note – To set SKIP parameters on a network interface other than the default interface, type: **`skiptool -i`** *name_of_interface* (such as `qe3`).

The main window of the `skiptool` GUI appears.

3. **Next, add a default access control list (ACL) to communicate unencrypted to all hosts.**

   a. **Click the Add button and, under Host, choose the Off security option.**
   The Add Host properties window appears.

   b. **In the Add Host Properties window, type `default` as the Hostname, as shown in the following figure, and click Apply.**

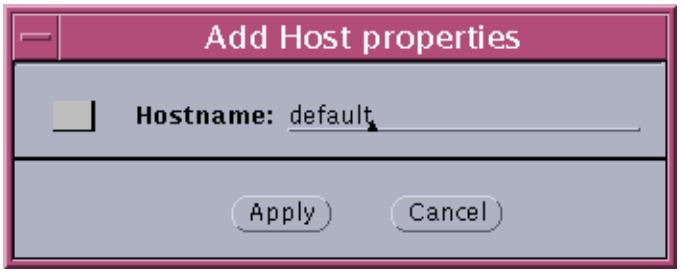


FIGURE 3–1 `skiptool` With Add Host Properties Window Completed

4. **Next, add an ACL entry for the Screen.**

   a. **Click the Add button and, under Host, choose the SKIP security option.**
   The Add SKIP Host Properties window appears, as shown in the following figure.

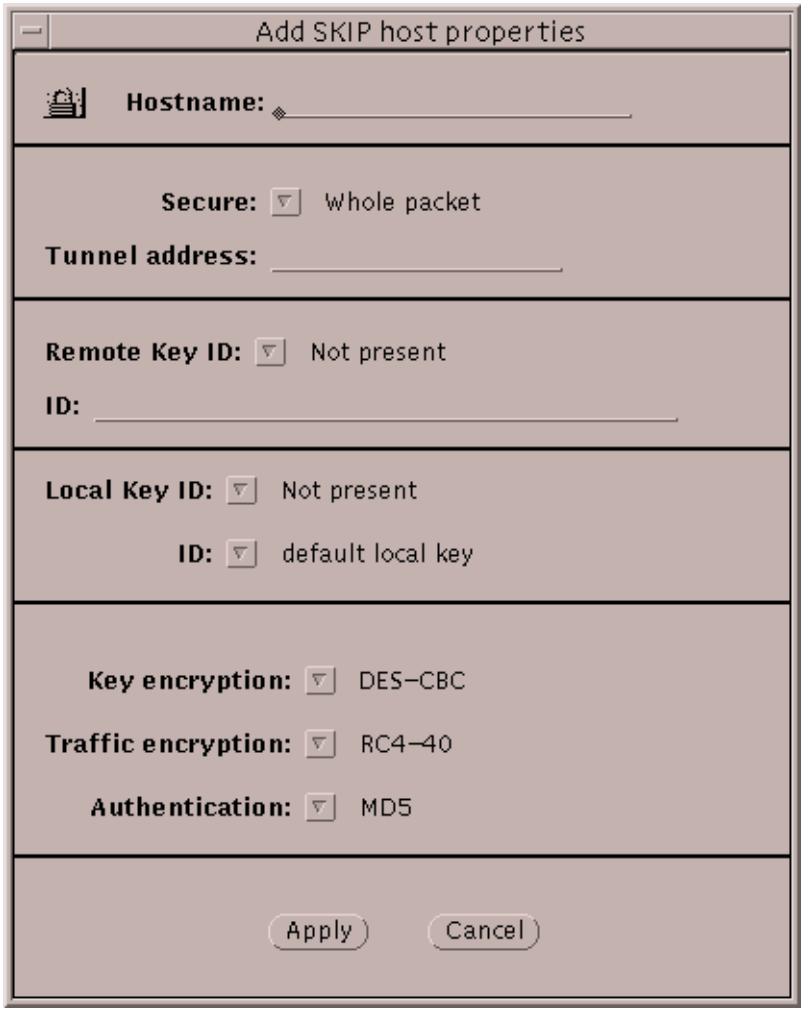


FIGURE 3–2 Add SKIP Host Properties Window

b. Use the information contained in the Screen's `AdminSetup.readme` file to complete the following fields:

- Type the name of the Screen in the Hostname field.
- Select Whole Packet in the Secure field.
- Make the appropriate selection in the Remote Key ID field.

  For UDH self-generated certificates on the Administration Station, select MD5 (DH Public Value). For CA-issued certificates, select IPv4.
- Type the Screen's MKID in the ID: field.

The correct Remote Key ID is found in the `AdminSetup.readme` file.

- Make the appropriate selection in the Local Key ID field.

  For UDH self-generated certificates on the Administration Station, select MD5 (DH Public Value). For CA-issued certificates, select IPv4.
- Select the Administration Station's MKID in the ID: field.
- Select the appropriate Key encryption, Traffic encryption, and Authentication algorithms for this connection.

  These algorithms must match those specified for the Screen in the `AdminSetup.readme` file.

5. **Click Apply to load your entry into the list.**
6. **Select enabled from the pull-down menu for "Access control is," which is located at the top of the `skiptool` window.**

Note – When you select enabled, a window appears when you save the configuration. To prevent these acquired systems, which are part of the default configuration, from showing up in the Authorized Systems window, click Cancel.

---

7. **In the `skiptool` window, select Save from the File 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 Firewall

To manage your Screen, use the administration GUI on the remote Administration Station.

Note – There is a predefined rule to allow encrypted administration traffic between the Screen and the Administration Station. Thus, no other communication (like `ping` or `telnet`) is allowed between the two systems until you specifically define a rule to allow such a service. See the *SunScreen 3.2 Administration Guide* for instructions on defining rules.

▼ To Launch the Administration GUI

1. **To configure and manage your Screen, open a Java-enabled Web browser and launch the administration GUI by typing the following URL:**

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

   The administration GUI appears.

Note – When trying to launch the administration GUI, if you encounter the error: The requested item could not be loaded by the proxy, you must disable proxy usage by specifying localhost in the Don't Proxy list, and then try to launch the GUI again.

---

2. **To login, type the following default user name and password, then click Login:**

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

Note – Change your default User Name and Password to something more secure.

See the *SunScreen 3.2 Administration Guide* for further instructions on using the administration GUI to configure and manage your Screen.

CHAPTER 4

Installing in Stealth Mode With Remote Administration Using SKIP

This chapter describes how to install the SunScreen software in stealth mode with remote administration using SKIP encryption technology. This installation scenario is a three-step process that requires you to first install the appropriate software on an Administration Station, then install the software on the Screen, and last, establish encrypted communication between the Administration Station and the Screen.

Note – Installing a locally administered Screen in stealth mode is not supported because a method for retrieving debug information is not available.

A system operating SunScreen in stealth mode behaves much like a bridge in that no IP interfaces are exposed to the public or private network and packets are filtered by the Screen transparently.

Topics in this chapter include:

Note – This chapter describes installing the SunScreen software using the Solaris Web Start Wizards installer; however, if you are installing on a system without a monitor, use the command-line installation described in "Command Line Installation" in the *SunScreen 3.2 Installation Guide*.

Before installing, review the *SunScreen 3.2 Release Notes* for the latest product information.

Note – Be sure to make a map of your network before you begin this installation. See "Determining Your Security Policy" in the *SunScreen 3.2 Installation Guide* appendix for worksheets and instructions to aid you in determining your network configuration and your desired security level.

Supported Administration Station Configurations

Any system operating Solaris 8 with SunScreen and a Java-enabled Web browser compliant with JDK 1.1.3 through 1.1.8 that can connect securely to the Screen using SKIP can be used as an Administration Station.

The SunScreen CD includes SKIP for both SPARC and Intel platform editions. Using SKIP allows any hardware running the Solaris 2.6, Solaris 7, or Solaris 8 operating environments to be an Administration Station.

Although systems operating Windows 95, Windows 98, or NT 4.x with PC SKIP, or Windows 2000 with IKE are supported platforms for an Administration Station, this chapter covers Solaris-based Administration Stations only.

Note – For details regarding SKIP, see either the *SunScreen SKIP User's Guide, Release 1.5.1*, or the *SunScreen SKIP User's Guide, Release 3.0.7, for the Microsoft Windows NT, Windows 95, and Windows 98 Operating Environments* documentation.

Stealth Mode Installation Summary

The installer guides you through installing the SunScreen software on systems using SKIP UDH self-generated or SKIP CA-issued certificate technology for encryption.

Perform the installation in the following order:

1. On the Administration Station
    a. Install the SunScreen administration software.
    b. Create the Administration Station's SKIP certificate.
2. On the Screen
    a. Install the SunScreen software.

This step requires the Administration Station's certificate ID and installs the Screen's certificate.

b. Create the Screen's SKIP certificate.

3. On the Administration Station install the Screen's certificate to begin encrypted communication.
4. Use the administration GUI on the remote Administration Station to manage your Screen.

Caution – If you configure a network interface as routing and later set it to stealth mode, the Screen will hang upon activation. If this happens, you must reboot the Screen in single user mode; remove the file `/etc/`*hostname.interface_name*, which unconfigures that interface; and reboot again.

The following sections describe the installation procedures for installing the SunScreen software in stealth mode and how to establish encrypted communication using SKIP certificate technology to remotely administer the stealth Screen.

Do not begin this procedure until you have read the information in "Defining Security Policies" in the *SunScreen 3.2 Installation Guide*.

Installing the Administration Software on the Administration Station

This procedure describes installing the administration software on the Administration Station.

▼ To Install the Administration Software on the Administration Station

1. **Open a terminal window on your system and become root, if not already.**
2. **Insert the SunScreen 3.2 CD into the CD-ROM drive.**
   A File Manager window appears that lists the contents of the CD.
3. **Double-click the install icon to start the installation.**

Note – You are prompted to type the root password for your system if the installer is started as a user other than root.

The Welcome window appears.

4. **In the Welcome window, click Next to continue.**

Note – The Welcome window includes an About button that you can click for information regarding the Web server used. Click the Dismiss button when done.

The Install Type window appears with Typical as the default entry.

5. **In the Install Type window, select Custom and click Next to continue.**

   The Functions window appears with both Screen and Administration selected as the default entry.

6. **In the Functions window, select Administration only by deselecting the Screen box, then click Next to continue.**

   The Component Selection window appears with all components except "Sun Web Server" and "SunScreen Firewall" selected as the default entry.

7. **In the Component Selection window, accept the default and click Next to continue.**

   The Install Verification window appears, containing a list of components to be installed.

8. **After verifying that the list of components is correct, click Install Now to continue.**

   The Installation Summary window appears. Upon successful completion, the status reads "Installed."

Note – To see a list of the added components, click the Details button.

---

9. **In the Installation Summary window, click Next to continue.**

   The Checking System window appears. The installer verifies that all required Solaris software and SunScreen packages are installed.

   - If the required packages are installed, a message appears announcing System check complete.
   - If all required packages have not been installed, exit the installer, install the missing packages, and rerun the installer to complete the SunScreen configuration.

10. **In the Checking System window, if the required packages are installed, click Next to continue.**

The Administration Station Configuration window appears and displays the results of the Administration Station's configuration.

11. **In the Administration Station Configuration window, click Next to continue.**

    The Installation and Configuration Complete window appears from which you must exit the installation to install the administration certificate.

12. **In the Installation and Configuration Complete window, click Exit to finish the installation.**

    The installer is dismissed.

After installing the required software packages on the Administration Station, you continue the process by creating the Administration Station's SKIP certificate.

Note – Both the Administration Station and the Screen need certificates before encrypted communication can begin.

Creating the Certificate on the Administration Station

Use the command-line interface to create SKIP UDH self-generated (the default) or SKIP CA-issued certificates on the Administration Station, as described in the following procedures.

▼ To Create the SKIP UDH Self-Generated Certificate on the Administration Station

1. **Open a terminal window and become root, if not already.**
2. **Create the required SKIP directories by typing:**

   ```
   # skiplocal -i
   ```

3. **Create the SKIP UDH certificate on the Administration Station by typing:**

   ```
   # skiplocal -k -f -V -m key_size
   ```

Note – For *key_size*, you type either 512, 1024, 2048, or 4096 (the latter being the default for this release). Make sure that you use the same *key-size* when generating the Screen's certificate.

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

Note – For export control regulatory assistance, consult the U.S. Department of Commerce, Bureau of Export Administration: `http://www.bxa.doc.gov`.

4. **Write down the certificate ID, which begins with '0x'.**

   This information is required when "Installing the SunScreen Software on the Screen" on page 61.

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
   ```

   Continue to the section "Installing the SunScreen Software on the Screen" on page 61.

▼ To load a SKIP CA-Issued Certificate on the Administration Station

1. **Open a terminal window on the Administration Station and become root, if not already.**

2. **Load the required SKIP directories by typing:**

   ```
   # skiplocal -i
   ```

3. **Insert the SKIP CA-issued 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 SKIP CA-issued Key and Certificate diskette by typing:**

```
# eject floppy0
```

8. **Write down the eight-character certificate ID.**

   This information is required when "Installing the SunScreen Software on the Screen" on page 61.

9. **Add SKIP to all the interfaces by typing:**

```
# skipif -a
```

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

```
# sync; init 6
```

    Continue to the following section "Installing the SunScreen Software on the Screen" on page 61.

Installing the SunScreen Software on the Screen

Note – Before proceeding, make sure the network interface you plan on using for administration is configured. For details on the Solaris network interface configuration, see your Solaris software documentation.

After adding certificates on the Administration Station, you install the SunScreen software on the Screen. This procedure requires the Administration Station's SKIP certificate ID (MKID).

You can use the installer if a monitor and a keyboard are attached to your Screen. If you are operating the Screen without a monitor, you must either temporarily attach a monitor or install the software through the command line (see "Command Line Installation" in the *SunScreen 3.2 Installation Guide*)..

▼ To Install the Software on the Screen

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

   A File Manager window appears that lists the contents of the CD.

2. **Double-click the install icon to invoke the SunScreen installer, which brings up the Welcome window.**

Note – You are prompted to type the root password for your system if the installer is started as a user other than root.

---

3. **In the Welcome window, click Next to continue.**

   The Install Type window appears with Typical selected as the default entry.

4. **Select Custom in the Install Type(s) window and click Next to continue.**

   The Functions window appears with both Screen and Administration selected as the default entry.

5. **In the Functions window, accept the default entry and click Next to continue.**

   The Component Selection window appears with all components except "SKIP End System" selected as the default entry.

Note – Never add the end-system SKIP packages `SUNWes` and `SUNWesx` to the Screen.

---

6. **In the Component Selection window, accept the default entry and click Next to continue.**

   The Checking System window appears and lists any existing SunScreen configurations found by the installer.

7. **In the Checking System window, click Next to continue.**

   - If an existing configuration was found, the Old Configurations window appears. Select Remove or Retain, as appropriate, and click Next to continue.
     - If Retain is selected, the Ready To Install window appears, and you can go to Step 10.
     - If Remove is selected, the Secondary HA window appears with No selected as the default entry.
   - If no existing configurations were found, the Secondary HA window appears with No selected as the default entry.

8. **In the Secondary HA window, accept the No default entry and click Next to continue.**

   The Screen Type window appears with Routing selected as the default entry.

9. **In the Screen Type window, select the Stealth entry and click Next to continue.**

   The Ready To Install window appears and lists the components for you to verify.

10. **After you verify that the components shown in the list are correct, click Install Now to continue.**

The Installation Summary window appears and shows the status of the installation, which upon a successful completion, reads “Installed.”

Note – To see a list of the added components, click the Details button.

---

11. **In the Installation Summary window, click Next to continue.**

    The Checking System window appears wherein the installer verifies that all required Solaris software and SunScreen packages are installed.

    - If the required packages are installed, a message appears announcing System check complete.
    - If all required packages have not been installed, exit the installer, install the missing packages, and rerun the installer to complete the SunScreen configuration.

12. **In the Checking System window, click Next to continue.**

    The Select Certificate Type window appears with UDH self-generated certificates selected as the default entry. The following section describes how to create the SKIP certificate on the Screen.

Creating the Certificate on the Screen

After installing the required software packages on the Screen, you continue the process by creating the Screen’s SKIP certificate, as described in the following sections

---

Note – Both the Administration Station and the Screen need certificates before encrypted communication can begin.

▼ To Create the SKIP UDH Self-Generated Certificate on the Screen

1. **In the Select Certificate Type window, accept the default entry and click Next to continue.**

   The Self Generated Certificate ID window appears where you type the Administration Station’s certificate ID.

2. **In the Self Generated Certificate ID window, type the Administration Station’s certificate ID (do not type the leading ’Ox’) in the text entry field and click Next to continue.**

The Select Administration SKIP Key Length window appears with 4096–bit key length as the default.

Note – The Screen's key length must match the UDH self-generated certificate key length you created previously for the Administration Station (see "Creating the Certificate on the Administration Station" on page 59). You must specify the Administration Station's key in the SKIP Key Length window if it is less than the 4096–bit default key length.

---

3. **After selecting the appropriate key length, click Next to continue.**

   The Generate Screen Certificate window appears and displays the Screen's generated SKIP certificate key ID.

4. **In the Generate Screen Certificate window, click Next to continue.**

   The Select Administrative Interface window appears listing the configured interfaces available for administration.

5. **After selecting the appropriate administrative interface, click Next to continue.**

   The Name Service window appears with both NIS and DNS name services selected as the default.

6. **After selecting the appropriate name services, click Next to continue.**

   The Verify Configuration window appears.

7. **After verifying that the information is correct, click Configure Now to continue.**

   The Screen Configuration window appears and instructs you, upon a successful configuration, to consult the `/etc/sunscreen/AdminSetup.readme` file on the Screen for instructions on completing the Administration Station setup.

8. **In the Screen Configuration window, click Next to continue.**

   The Screen Hardening window appears.

Caution – Once you harden your Screen, it becomes a dedicated firewall and cannot be used for another purpose without first reinstalling the Solaris software. Hardening automatically removes files and packages that might otherwise make the Screen vulnerable to an attack.

Clicking Next completes the installation without hardening your Screen. Optionally, to harden your Screen, click the Harden Screen button.

Note – The hardening process can be done later by running the script: `/usr/lib/sunscreen/lib/harden_os`.

9. **In the Screen Hardening window, click Next to continue.**
   The Installation and Configuration Complete window appears and prompts you to reboot your system.
10. **In the Installation and Configuration Complete window, click Reboot Now to complete the installation.**
    The installer is dismissed.

Note – To complete the installation process you must reboot the system at this time. If you do not wish to reboot your system, click Next instead of Reboot System.

You are now ready to complete the installation on the Administration Station as described in "Completing the SKIP Certificates Installation Procedure" on page 66.

▼ To Load the SKIP CA-Issued Certificate on the Screen

1. **Select SKIP CA-Issued Certificate from the Select Certificate Type window (the default is SKIP UDH Certificate) and click Next to continue.**
   The Issued Certificate Key Diskettes window appears.
2. **Insert the Administration Station's Key and Certificate diskette into the diskette drive and click Read Diskette.**
   Wait until the SKIP CA-issued certificate ID appears at the bottom of the window.
3. **Write down the Administration Station's eight-character certificate ID and click Next to continue.**
   This certificate ID is required to complete the Administration Station installation.
4. **Insert the Screen's Certificate ID diskette into the diskette drive and click Read Diskette.**
   The SKIP CA-issued certificate ID for the Screen appears at the bottom of the window.
5. **Write down the Screen's eight-character certificate ID and continue to the Screen Configuration window.**
6. **To complete the installation, click System Reboot.**
   The installer is dismissed.

Note – To complete the installation process you must reboot the system at this time. If you do not wish to reboot your system, click Next instead of Reboot System.

You are now ready to complete the installation on the Administration Station as described in "Completing the SKIP Certificates Installation Procedure" on page 66.

Completing the SKIP Certificates Installation Procedure

After installing the SunScreen software and the SKIP certificates on the Screen, the Screen's certificate information must be loaded onto the Administrating Station to complete the installation. This information is located on the Screen in the `/etc/sunscreen/AdminSetup.readme` file.

The following procedure explains how to display this file.

▼ To Display the `/etc/sunscreen/AdminSetup.readme` File

1. **Display the `/etc/sunscreen/AdminSetup.readme` file by typing:**

   ```
   # more /etc/sunscreen/AdminSetup.readme
   ```

   The `AdminSetup.readme` file contains the Screen's certificate ID as well as the command run to give the Administration Station the Screen's certificate ID.

   This command adds the Screen to the ACL with the necessary encrypting parameter settings. If it executes successfully, then the configuration is complete, and you can go to "To Configure the Administration Station to Communicate With the Screen Using SKIP" on page 50.

2. **Write down the command, which begins with `skiphost -a`, that is requried in the next procedure.**

Note – You can use ftp to copy the `/etc/sunscreen/AdminSetup.readme` file onto the Administration Station if you trust that the network between the Screen and Administration Station is secure. Otherwise, display the file and write down the information for use in the next section.

Instructions for using SKIP from the command line are in the "Using the

Command-Line Interface" in *SunScreen SKIP User's Guide, Release 1.5.1.*

▼ To Configure the Administration Station to Communicate With the Screen Using SKIP

The following steps describe how to set up SKIP encryption software on the Administration Station.

If the `AdminSetup.readme` file was not copied to the Administration Station using ftp (or if the `skiphost -a` command fails), execute the following steps using the information obtained from that file.

1. **Open a terminal window and become root, if not already.**
2. **Launch the `skiptool` GUI by typing:**

```
# skiptool &
```

Note – To set SKIP parameters on a network interface other than the default interface, type: **`skiptool -i`** *name_of_interface* (such as `qe3`).

The main window of the `skiptool` GUI appears.

3. **Next, add a default access control list (ACL) to communicate unencrypted to all hosts.**

   a. **Click the Add button and, under Host, choose the Off security option.**
   The Add Host properties window appears.

   b. **In the Add Host Properties window, type `default` as the Hostname, as shown in the following figure, and click Apply.**

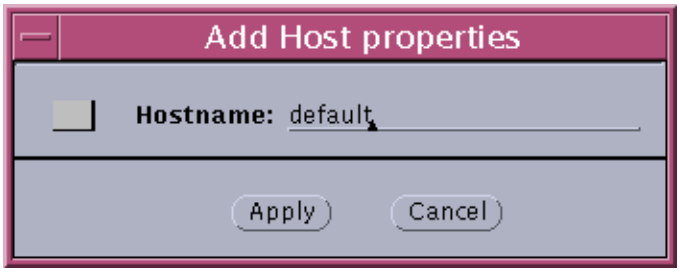


FIGURE 4–1 `skiptool` With Add Host Properties Window Completed

4. **Next, add an ACL entry for the Screen.**

a. **Click the Add button and, under Host, choose the SKIP security option.**
The Add SKIP Host Properties window appears, as shown in the following figure.

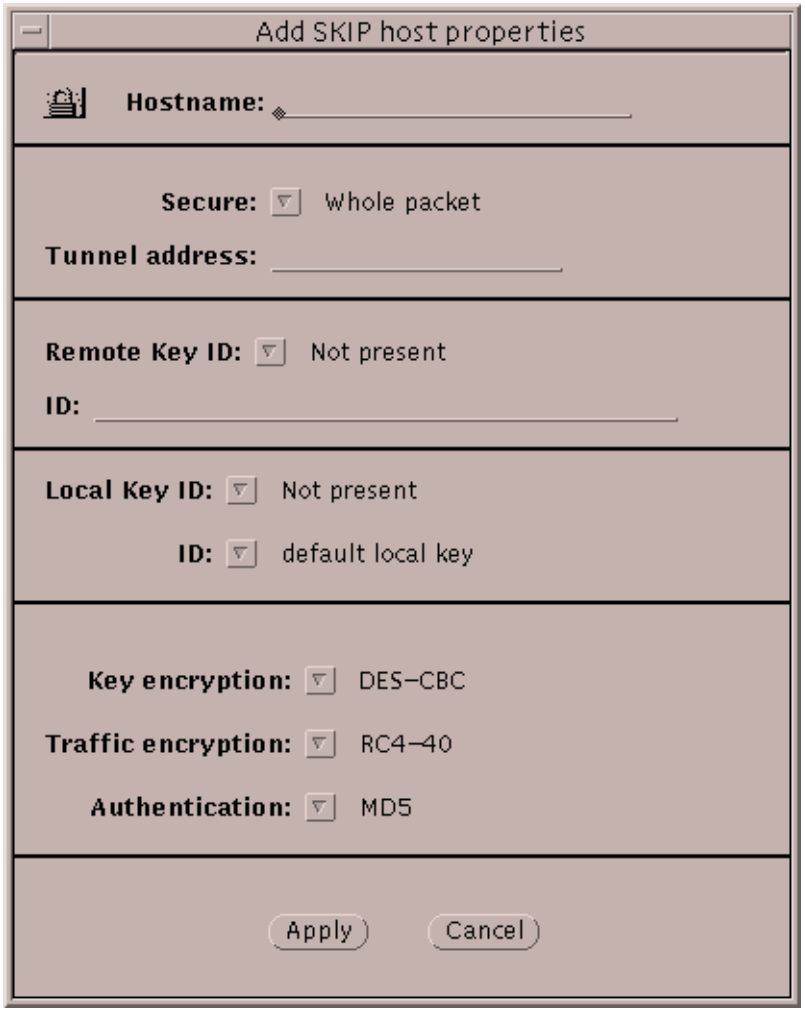


FIGURE 4–2 Add SKIP Host Properties Window

b. **Use the information contained in the Screen's `AdminSetup.readme` file to complete the following fields:**

- Type the name of the Screen in the Hostname field.
- Select Whole Packet in the Secure field.
- Make the appropriate selection in the Remote Key ID field.

For UDH self-generated certificates on the Administration Station, select MD5 (DH Public Value). For CA-issued certificates, select IPv4.

- Type the Screen's MKID in the ID: field.

  The correct Remote Key ID is found in the `AdminSetup.readme` file.
- Make the appropriate selection in the Local Key ID field.

  For UDH self-generated certificates on the Administration Station, select MD5 (DH Public Value). For CA-issued certificates, select IPv4.
- Select the Administration Station's MKID in the ID: field.
- Select the appropriate Key encryption, Traffic encryption, and Authentication algorithms for this connection.

  These algorithms must match those specified for the Screen in the `AdminSetup.readme` file.

5. **Click Apply to load your entry into the list.**
6. **Select enabled from the pull-down menu for "Access control is," which is located at the top of the `skiptool` window.**

Note – When you select enabled, a window appears when you save the configuration. To prevent these acquired systems, which are part of the default configuration, from showing up in the Authorized Systems window, click Cancel.

---

7. **In the `skiptool` window, select Save from the File 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 Firewall

To manage your Screen, use the administration GUI on the remote Administration Station.

Note – There is a predefined rule to allow encrypted administration traffic between the Screen and the Administration Station. Thus, no other communication (like `ping` or `telnet`) is allowed between the two systems until you specifically define a rule to allow such a service. See the *SunScreen 3.2 Administration Guide* for instructions on defining rules.

▼ To Launch the Administration GUI

1. **To configure and manage your Screen, open a Java-enabled Web browser and launch the administration GUI by typing the following URL:**

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

   The administration GUI appears.

   Note – When trying to launch the administration GUI, if you encounter the error: The requested item could not be loaded by the proxy, you must disable proxy usage by specifying localhost in the Don't Proxy list, and then try to launch the GUI again.

2. **To login, type the following default user name and password, then click Login:**

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

   Note – Change your default User Name and Password to something more secure.

   See the *SunScreen 3.2 Administration Guide* for further instructions on using the administration GUI to configure and manage your Screen.

CHAPTER 5

Installing With Remote Administration Using IKE

This chapter describes how to install the SunScreen software in routing and stealtgh mode with a remote administration using IKE encryption technology. The configuration steps are almost identical whether you are installing your Screen in routing mode or in Stealth mode.

For Trusted Solaris 8, there is no built-in facility for generating IKE certificates on a remote Administration Station like there is when using SKIP encryption. Instead, you employ a second Screen (known as an administrative Screen) for remote administration. Solaris 9 has native IKE support and only requires the administration software.

This installation example uses self generated certificates but it is also possible to use CA signed certificates. In fact, in the case of using a Windows 2000 system as a remote Administration Station, you must used CA signed certificates.

For an example of an installation using IKE encryption technology with Windows 2000, see the *SunScreen 3.2 Configuration Examples* document.

Topics in this chapter include:

Before installing, review the *SunScreen 3.2 Release Notes* for the latest product information.

Note – Be sure to make a map of your network before you begin this installation. See "Determining Your Security Policy" appendix, which includes worksheets and instructions to aid you in determining your network configuration and your desired security level.

Supported Administration Station Configurations

For IKE administrative traffic, systems using Solaris 9 and Trusted Solaris 8 (with Screen software installed), or Windows 2000 with IKE (using CA signed certificates) are supported platforms for an Administration Station.

Routing and Stealth Mode Installation Summary

Although you can use the installer to guide you through the installation, this chapter covers installing the SunScreen software through the command-line interface on systems using IKE with self-generated certificates for encryption.

For Trusted Solaris 8, there is no built-in facility for generating IKE certificates on a remote Administration Station like there is when using SKIP encryption. Instead, you employ a second Screen (known as an administrative Screen) for remote administration. Solaris 9 has native IKE support so you only need to install the Administration packages.

Perform the installation in the following order:

1. On the Administration Station:
    a. Install the administration software. In the Solaris 9 case, you only install the administration package. In the Trusted Solaris 8 case, you install both the administration and Screen packages.
    b. Create the Administration Station's IKE certificate. Export it to a file, then transfer the file to the firewall Screen system.
2. On the firewall Screen
    a. Install the Screen and the administration software.

This step requires the Administration Station's certificate ID.

b. Create the Screen's IKE certificate. Export it to a file, then transfer the file to the Administration Station.

c. Import the Administration Station's IKE certificate.

d. Mark the certificate as trusted.

e. Create an address object for the Administration Station.

f. Create an Admin Acess rule allowing communication bewteen the Administration Station and the Screen.

g. Edit the Screen object to specify the Administration Station's IP address.

3. On the Administration Station

a. Import the Screen's certificate.

b. Mark the certificate as trusted.

c. Set up encrypted communication between the Administration Station and the Screen. In the Solaris 9 case, this means editing the IKE configuration files. In the Trusted Solaris 8 case, you must create certificate and address object then use these objects to create a packet filtering rule allowing communication between the two systems.

The following sections describe the installation procedures for installing the SunScreen software and how to establish encrypted communication using IKE certificate technology.

Installing the Screen and Administration Station

Note – Before proceeding, make sure that all network interfaces you plan on using are configured. Configured interfaces are those displayed with `# ifconfig -a`. For details on the Solaris network interface configuration, see your Solaris software documentation.

This procedure describes installing the required SunScreen 3.2 Screen and administration packages using `pkgadd` to install the software. Use this procedure to install the Screen and administration packages on the firewall Screen as well as on the Administration Station. You can also use this procedure on the firewall Screen itself for a local installation.

▼ To Install the Software

Use this procedure on both systems.

1. **Open a terminal window on one of the systems and become root, if not already.**
2. **Insert the SunScreen 3.2 CD into that Screen's CD-ROM drive.**
3. **Add the software by typing:**

   ```
   # pkgadd  /cdrom/cdrom0/sparc
   ```

   A list of available packages appears.

   - For Trusted Solaris 8:

     For a Screen, specify: 1-9 and 13-31. For a Remote Administration Station, specify: 1-11, 14-24, 28, and 31.

   - For Solaris 9

     For a Screen, specify: 2-7 and 13-31. For a Remote Administration Station, specify: 2-7, 10-11, 14-24, 28, and 31.

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

   The answers you provide determine whether this will be a routing mode or a stealth mode Screen. When completed, you return to the same menu of packages.

5. **Type `q` to quit** `pkgadd`**.**
6. **Complete the installation by activating your policy configuration.**

   Type: `ssadm configure`

   Answer the questions that appear.

7. **Eject the CD by typing:**

   ```
   # eject cdrom0
   ```

8. **Reboot by typing:**

   ```
   # sync; init 6
   ```

   After installing the appropriate software on both the Screen and Administration Station, you create the IKE self-generated certificates on the systems and set up encrypted communications, as described in the following procedure.

Note – The Adminstration Station and the firewall Screen need both their own certificates and each other's certificates installed before encrypted communication can begin.

Setting Up a Remote Administration Station Using IKE

The following procedure describes using the command-line interface to create the IKE self-generated certificates on the Administration Station and firewall Screen. In the case of Trusted Solaris 8, the Administration Station is also a Screen.

Create an IKE Certificate on the Administration Station

The first step ijn this process is to create an IKE certificate on the remote Administration Station and to export it to a file.

▼ To Create the Certificate on a Trusted Solaris 8 Administrative Screen

1. **Open a terminal window and become root, if not already.**
2. **Create the IKE self-generated certificate.**

   ```
   # ssadm certlocal -Iks -m 512 -t rsa-md5 -D "C=US,
   O=YOUR_ORG, CN=admin_name"
   ```

3. **Export the Administration Station's certificate to a file.**

   ```
   # ssadm certdb -I -e "C=US, O=YOUR_ORG,
   CN=admin_name" > /tmp/admin_cert
   ```

4. **Set up the Screen.**

▼ To Create the Certificate on a Solaris 9 Administration Station

1. **Open a terminal window and become root, if not already.**
2. **Create the IKE self-generated certificate.**

   ```
   # ikecert certlocal  -ks -m 512 -t rsa-md5 -D "C=US,
   O=YOUR_ORG, CN=admin_name"
   ```

3. **Export the Administration Station's certificate to a file.**

```
# ikecert certdb  -e "C=US, O=YOUR_ORG,
CN=admin_name" > /tmp/admin_cert
```

4. **Set up the Screen.**

Setting Up the Screen

This section describes how you set up a Screen to use IKE to communicated with a remote Administration Station. Much of the instructions are given using command line examples while others use the administration GUI. In each case, the easiest method of performing the required task was chosen.

If you need further instructions on how to perform a specific task, try looking at the *SunScreen Administration Guide* and also the *SunScreen Configuration Examples* for detailed instructions.

▼ To Set Up IKE on the Firewall Screen

After adding certificates on the administrative Screen or Administration Station, you create the IKE certificate on the firewall Screen.

1. **Create the IKE self-generated certificate.**

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D
"C=US, O=YOUR_ORG, CN=screen_name"
```

2. **Export the firewall Screen's IKE certificate to a file by typing.**

```
# ssadm certdb -I -e "C=US, O=YOUR_ORG,
CN=screen_name" > /tmp/screen_cert
```

3. **Import the administrative Screen's certificate by typing.**

```
# ssadm certdb -I -a < /tmp/admin_cert
```

4. **Create certificate objects for the certificates**

```
# ssadm edit PolicyName
then using ssadm edit
edit> add certificate admin_cert SINGLE IKE "C=US,
O=SUN, CN=admin_name"
edit> add certificate screen_cert SINGLE IKE "C=US,
O=SUN, CN=screen_name"
```

5. **Mark the imported certificate as trusted.**

```
Using ssadm edit
edit>add member certificate "IKE manually
verified certificates" "admin_cert"
```

6. **Start the Administration GUI.**

From this point on, it is easier to use the administration GUI to do the remaining steps.

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

After you log in, edit the appropriate policy then continue with the following steps.

7. **Add the Administration Station's IP address as an `address` object.**
8. **Add the Administration Station as a `screen` object and allow routing traffic and naming service.**
9. **Edit the firewall Screen's `screen` object by selecting the primary/secondary tab and establishing the Administration Station's IP address as the administrative IP address in the IKE administrative certificate field, and add the firewall Screen's certificate.**
10. *Stealth Mode Only* **– Return to the miscellaneous tab and make sure routing traffic and name service are No or None (certificate discovery is on).**
11. **From a command line, mark the administrative certificate as trusted by typing:**

```
# ssadm edit PolicyName
then, using ssadm edit
edit>add member certificate "IKE manually
verified certificates" "admin_cert"
```

12. **From th GUI, add a remote access rule by selecting the administrative access tab and under the Access rules for remote administration table, click the add new rule button.**

```
screen: screen name
address object: remote admin address
user: admin
access level: all
encryption: IPSEC IKE
```

13. **Select the one algorithm that matches the packet filtering rule on the firewall Screen's source certificate: `screen cert`.**
14. **Click on the Options tab, source screen: screen name.**

    When done, you have a remote access rule like the following:

```
1 SCREEN "screen_name" USER "admin" "admin_addr"
IPSEC ESP("DES-CBC", "MD5") AH("SHA1") IKE("DES-CBC", "MD5",
1, RSA-SIGNATURES, "screen_cert") PERMISSION ALL
```

15. **Activate the policies.**
16. **Finish the Administration Station.**

Finish the Administration Station

▼ Finishing a Trusted Solaris 8 Administration Station

1. **Import the firewall Screen's certificate.**

   ```
   # ssadm certdb -I -a < /tmp/screen_cert
   ```

2. **Create certificate objects for the certificates.**

   ```
   # ssadm edit PolicyName
   edit> add certificate admin-cert SINGLE IKE "SUBJECT=C=US, O=SUN,
   CN=admin_DN"
   edit> add certificate screen-cert SINGLE IKE "SUBJECT=C=US, O=SUN,
   CN=screen_DN"
   ```

3. **Mark the imported certificate as trusted.**

   ```
   Using ssadm edit
   edit>add member certificate "IKE manually
   verified certificates" "screen_cert"
   ```

   Note – The Group name "IKE manually verified certificates" is reserved for a trusted Certificate Group.

   ---

4. **Create an address object for the Screen.**

   ```
   Using ssadm edit
   edit>add address nameofscreen ipaddressofscreen
   ```

5. **Add a packet filter rule like the following:**

   ```
   1 "remote administration" "admin_address"
   "screen_address" IPSEC ESP("DES-CBC", "MD5") AH("SHA1")
   IKE("DES-CBC", "MD5", 1, RSA-SIGNATURES, "admin_cert",
   "screen_cert") ALLOW
   ```

   See "Packet Filtering Rules" in the *SunScreen 3.2 Administration Guide*.

6. **Activate the policies.**

▼ Finishing a Solaris 9 Administration Station

1. **Import the firewall Screen's certificate.**

   ```
   # ikecert certdb  -a < /tmp/screen_cert
   ```

2. **Set Up the IKE rules.**

   You have to edit the IKE configuration files to set up encrypted communication between the Administration Station and the Screen. For information on editing these files, see the Solaris 9 IKE documentation.

a. **Edit the** `/etc/inet/ipsecinit.remote` **file.**

The following file provides an example of how you would set up communication between an Administration Station with an IP address of 172.16.2.3 and a Screen's administrative interface with an address of 172.16.2.1

```
{sport 500} bypass {dir out}
{dport 500} bypass {dir in}
{saddr 172.16.2.3 daddr 172.16.2.1} apply {encr_algs des encr_auth_algs sha1 sa shared}
{saddr 172.16.2.1 daddr 172.16.2.3} permit {encr_algs des encr_auth_algs sha1 sa shared}
```

b. **Edit the** `/etc/inet/config` **file.**

This file contains instructions to amrk the Screens certificate as trusted as well as encryption parameters.

```
# Example remote admin config file
 # IKE manually verified self-signed certs
cert_trust "SUBJECT=CN=DNofScreensCert-rsa-sha1-4096, O=Sun, C=US"
# Outgoing IKE rule for remote admin
{label "outgoing"
local_id_type DN
local_id "SUBJECT=CN=RemoteAdminCert-rsa-sha1-4096, O=Sun,
C=US"
remote_id "SUBJECT=CN=ScreenCert-rsa-sha1-4096, O=Sun, C=US"
local_addr 172.16.2.3
remote_addr  172.16.2.1
p1_xform {auth_method rsa_sig oakley_group 1 auth_alg sha1 encr_alg des }
}
```

3. **Reload IKE and it's associated components.**

Issue commands similar to the following:

```
# pkill iked
# ipsecconf -f
# ipseckey flush # ipsecconf -a /etc/inet/ipsecinit.remote
# /usr/lib/inet/in.iked -f /etc/inet/ike/config.remote
```

The remote Administration Station is now ready to communicate with the Screen.

Managing Your Firewall

To manage your firewall Screen, use the administration GUI on the remote administrative Screen.

Note – There is a predefined rule to allow encrypted administration traffic between the firewall Screen and the administrative Screen. Thus, no other communication (like `ping` or `telnet`) is allowed between the two systems until you specifically define a rule to allow such a service. See "Administrative Access Rules" in the *SunScreen 3.2 Administration Guide*.

▼ To Launch the Administration GUI

1. **To configure and manage your firewall Screen, open a Java-enabled Web browser and launch the administration GUI by typing the following URL:**

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

   The administration GUI appears.

   Note – When trying to launch the administration GUI, if you encounter the error: The requested item could not be loaded by the proxy, you must disable proxy usage by specifying localhost in the Don't Proxy list, and then try to launch the GUI again.

2. **To login, type the following user default name and password, then click Login:**

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

   Note – Be sure to change your default User Name and Password to something more secure.

   See "Using the Administration GUI" in the *SunScreen 3.2 Administration Guide* for further instructions on configuring and managing your firewall Screen.

CHAPTER 6

Installing SunScreen on Trusted Solaris 8

This chapter describes how to install the SunScreen software on a system running the Trusted Solaris™ 8 operating environment. Installing SunScreen on a system running Trusted Solaris is different than installing SunScreen on a regular Solaris software system because of the built-in security features. Trusted Solaris is an extension of the Solaris operating environment. Although these systems are similar, there are many differences that can thwart the efforts of an experienced Solaris software systems administrator. The following procedures show you how to prepare and configure a Trusted Solaris system to run the SunScreen firewall software. For more information regarding Trusted Solaris, see *Trusted Solaris 8 Reference Manual*. For the latest product information, see *Trusted Solaris 8 Release Notes*.

Note – Be sure to make a map of your network before you begin this installation. See "Determining Your Security Policy" in *SunScreen Installation Guide* appendix for worksheets and instructions to aid you in determining your network configuration and your desired security level.

Topics covered include:

Overview

The following information specifically applies when SunScreen 3.2 is used on a system running the Trusted Solaris 8 operating environment (for more information regarding installing and configuring Trusted Solaris, see *Trusted Solaris Installation and Configuration*.)

Note – Do not use the command line interface to install SunScreen 3.2 on Trusted Solaris 8 as it does not work. Use the File Manager with the `admin` role as described in "Installing SunScreen on Trusted Solaris" in the *SunScreen 3.2 Installation Guide*.

- SunScreen 3.2 is supported on Trusted Solaris 8, but not on the previous versions, Trusted Solaris 7 or Trusted Solaris 2.5.1.
- Use only the File Manager (see "To Install the Software on the Screen" on page 83) to install the software on your system.
- Packets with TSOL, CIPSO, and UNLABELED templates work. While other templates may work, no others were verified.
- When two Trusted Solaris systems using the TSOL protocol talk to each other using the TSOL networking protocol, they typically use rpc program 110002 to exchange process attributes for peer processes. The entry in `/etc/rpc` is: `tsolpeerinfo 110002 rpc.getpeerinfo peerinfod`.

  Services between two Trusted Solaris systems do not work if this service is blocked. You must allow the `tsolpeerinfo` service through your firewall, and the rule base must allow this service to be initiated from both ends of a connection.

  This service works with STATIC NAT when `tsolpeerinfo` is allowed through in the rule base, however, it does not work with DYNAMIC NAT.

Every process in Trusted Solaris has privileges associated with it (called effective privileges). These effective privileges fall into the following categories:

- Some privileges
- All privileges
- No privileges

A Trusted Solaris file also has a set of privileges called the *allowed* privileges. When you execute a Trusted Solaris file (to create a process), the resulting processes' effective privileges are the intersection of the file's allowed privileges and your privileges as defined in your users rights.

Therefore, all SunScreen executable files must have their allowed privileges set to all. This action is performed during installation of the SunScreen software through `pkgadd`.

This action is performed by the `/usr/lib/sunscreen/lib/pkgadd` shell script. When you use the installer, this script is automatically invoked.

A Trusted Solaris system needs the latest revision of the following patches installed from: `http://sunsolve.Sun.COM/pub-cgi/show.pl`.

- 110739
- 110337
- 110771

Refer to the README file included with the download for instructions.

Installing the SunScreen Software

The SunScreen software is installed by an administrative role. The `admin` role as described in the Trusted Solaris documentation can be used, or any role, that has the Software Installation rights.

The Screen's and Administration Station's software is installed by `admin` user.

▼ To Install the Software on the Screen

1. **Assume the `admin` role.**
2. **From the front panel, choose Allocate Device, then select and mount the CD-ROM device and wait for the File Manager to appear.**

Note – If the File Manager does not appear presently after allocating and mounting the CD-ROM, start the File Manager manually and select the `/cdrom/cdrom0` directory.

---

3. **In the File Manager, select View Hidden Objects from the View menu.**
4. **Double click on `.install`.**
5. **Double click on `install.class`.**

   The rest of the installation steps are the same as a regular SunScreen installation. Refer to the appropriate chapter in this book for further instructions on your particular installation.

▼ To Install the Software on the Administration Station

1. **Assume the `admin` role.**
2. **From the front panel, choose Allocate Device, then select and mount the CD-ROM device and wait for the File Manager to appear.**
3. **In the File Manager, select View Hidden Objects from the View menu.**
4. **Double click on `.install`.**
5. **Double click on `install.class`.**

   The rest of the installation steps are the same as a regular remote SunScreen installation. Refer to the appropriate chapter in this book for further instruction on your particular installation.

Note – If you choose to install the SunScreen software on an Administration Station manually, after adding the `sunscreen` role, run the `/usr/lib/sunscreen/lib/ts_setup` command as the `sunscreen` role.

For a more detailed explanation of trusted networking, see the following URL by typing: .

`http://www.sun.com/software/solaris/trustedsolaris/trustedsolaris.html`

▼ To Add the `sunscreen` Role

Note – You must create the `sunscreen` role to administer SunScreen (see "Assuming a Role and Working in a Role Workspace" in *Trusted Solaris Administrator's Procedures*.

- **Create a role named `sunscreen` using the Solaris Management Console as described in the Trusted Solaris documentation.**

  You can choose any UID and any GID, but you must assign the following rights:

  - SunScreen -- This is the list of commands needed to administer SunScreen.
  - Outside Accred -- This is the authorization needed to work at an administrative label.

Note – By default, Trusted Solaris assigns the Basic Solaris User rights to all users. If you have modified your `policy.conf` file to exclude this right, you can either add this right manually to the `sunscreen` role or assign the Basic Commands and Basic Actions rights to the `sunscreen` role. This allows the `sunscreen` role to perform normal command line operations with no additional privilege.

If you choose to allow the `sunscreen` role to allocate devices, you must assign Convenient Authorizations rights to the role.

The `sunscreen` role must have a minimum label of ADMIN_LOW. The clearance can be assigned to ADMIN_HIGH, although this is not required.

For example, the `sunscreen` role is assigned a UID of 121, if not already in use, and a GID of 10. The SunScreen and Outside Accred rights are assigned to the role, and the minimum label is set to ADMIN_LOW. Make certain to assign a password.

Assign the `sunscreen` role to the user or users who administer SunScreen.

CHAPTER 7

Upgrading Your System

This chapter explains how to upgrade your system to SunScreen 3.2 from prior releases of SunScreen, as well as how to upgrade cryptographic modules.

Topics covered include:

Before You Upgrade

Caution – The upgrade script removes and adds packages as needed. To avoid corruption of your existing configurations, do not attempt to remove or add packages manually.

Before installing SunScreen, complete the following tasks:

- Since SunScreen 3.2 is only supported on the SPARC versions of Trusted Solaris 8 and Solaris 9, upgrade your operating system to the required level.
- Ensure that the system you have identified to upgrade is secure.
- When running the Solaris 8 software, install the recommended kernel and security patches from `http://sunsolve.sun.com`. In addition, make sure the following patches are installed:

- To upgrade a SunScreen EFS 3.0, revision A, system to SunScreen 3.2, you must first install the SunScreen EFS 3.0, revision A, patch that is available at: `http://www.sun.com/software/securenet/securenet3/install.html`.
  - SPARC: 108156 patch
  - Intel: 108157 patch

  Note – This patch is *only* required for SunScreen EFS 3.0, revision A. Refer to the README for instructions on installing the patch.

- For all installations:
  - SPARC 108528-06; Intel 108529-05: kernel update patch.
  - SPARC 109279-08; Intel 109280-08: `/kernel/drv/ip` patch.
- For systems with a `qfe` board installed:
  - SPARC 108806-02: Sun Quad Fast Ethernet `qfe` driver patch.
- For systems running Trusted Solaris 8:
  - SPARC 110337-02: Security CIPSO TCP kernel support patch.

- Review custom scripts from SunScreen EFS 3.0 or SunScreen 3.1 because the directory structure has been changed in SunScreen 3.2.
- Upgrading a SunScreen SPF-200 stealth system is performed differently than other SunScreen upgrades. (See "Upgrading From SunScreen SPF-200" on page 100.)

  To reduce network downtime consider transferring your SunScreen SPF-200 configurations to a new system and performing the upgrade on the new system. See "Upgrading From SunScreen SPF-200" in the *SunScreen 3.2 Installation Guide*.

Note – After completing the upgrade from SunScreen EFS 1.1, 2.0, or from SunScreen SPF-200, you must review your packet filtering rules to verify the filtering order because SunScreen 3.2 uses ordered packet filtering rules and ordered NAT mappings. Also, be aware that NAT mappings changed considerably in SunScreen EFS 3.0 from the NAT mappings used in prior releases of SunScreen. See "Packet Filtering" and "Network Address Translation" in *SunScreen 3.2 Administrator's Overview* for details on packet filtering rules and NAT mappings.

The order in which you install the upgrade software is different from an initial installation. Upgrading requires that you first install it on the Screen and then on the Administration Station. This order prevents damage to the existing policies and makes communication easier between the Administration Station and the Screen.

Caution – To retain your existing SunScreen policy configuration files, you must take special care when upgrading to SunScreen 3.2. Do not remove your existing software packages unless you are instructed to do so.

Before installing the SunScreen software, review the *SunScreen 3.2 Release Notes* for the latest product information.

Upgrading to SunScreen 3.2

The following includes overview information as well as instructions for upgrading to SunScreen 3.2 from SunScreen EFS 1.1, 2.0, and 3.0, and from SunScreen 3.1 and SunScreen 3.1 Lite.

If you are upgrading from SunScreen EFS 1.1 or 2.0, your system upgrades to SunScreen 3.2 in routing mode. If you are upgrading from SunScreen EFS 3.0, SunScreen 3.1, or SunScreen 3.1 Lite, the current mode of your system is preserved.

The upgrade procedure automatically backs up your previous SunScreen policies, certificates, and packages in case the upgrade fails. It does not, however, save your existing log files, thus, before beginning the upgrade procedure, save your existing log files according to your specific SunScreen EFS 1.1, 2.0, or 3.0, or SunScreen 3.1 documentation, if needed. Also at this time, make any other system backups according to your standard Solaris backup procedures, if needed. Next, the program automatically removes your old SunScreen software packages and installs the SunScreen 3.2 software packages.

Note – For the commands you use to back up this information, refer to the documentation that accompanied your release of SunScreen.

The following procedures describe how to upgrade both locally and remotely administered Screens.

Caution – To retain your existing policies and SKIP keys and certificates (including your system's SKIP local identities) between software upgrades, do not remove `/etc/opt/SUNWicg`. Also, to retain your old remote administration rules, backup your `/etc/skip` directory, which contains all of your local keys, ACLs, and `skipd.conf`.

The following describes how to prepare to upgrade both locally and remotely

administered systems:

Note – If you use the command line, check the man pages and "Migrating From Earlier SunScreen Firewall Products" in the *SunScreen 3.2 Administrator's Overview* document for information regarding any commands or arguments that were removed or added since prior releases of SunScreen.

The following describes how to prepare both locally and remotely administered systems for upgrading.

Before proceeding, verify that all the software packages required for your operating environment are installed. That is, in addition to the Solaris Core Distribution software, and the Solaris End User Distribution software when using the administration GUI locally on the Screen itself, there are additional Solaris software packages required prior to installing the SunScreen 3.2 software, if not already on your system (see "Operating System Package Requirements" in the *SunScreen 3.2 Installation Guide*).

Caution – Do not *reinstall* the Solaris Core Distribution software group when upgrading your system to SunScreen 3.2.

SunScreen 3.2 runs on Solaris 2.6, Solaris 7, and Solaris 8 operating environments for SPARC and Intel platform editions, as well as on Trusted Solaris 8. To upgrade your system, it must be running at least the Solaris 2.6 software because Solaris 2.5.1 or earlier software releases are not supported.

▼ To Install the Prerequisite Solaris Packages and Kernel Patches on the Screen

1. **Add the packages to the Screen from your Solaris software CD, if not already on your system.**

   For your locally-administered Screen to use the SunScreen administration GUI, you must install the End User Distribution of Solaris, as well as the following packages.

Caution – Never install the End-System SKIP packages (SUNWes or SUNWesx) on a Screen.

---

2. **If you are using Solaris 2.6 software, add the following patches in the following order, if not already on your system, by typing:**

```
For SPARC platform edition systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
```

```
# patchadd 105181-11
# patchadd 105284-15
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For Intel platform edition systems:
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105182-13
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

3. **Reboot by typing:**

```
# sync; init 6
```

▼ To Install the Solaris Packages on the Remote Administration Station

1. **Add the packages to the Administration Station from your Solaris software CD, if not already on your system.**

2. **If you are using Solaris 2.6 software, add the following patches, if not already on your system, by typing:**

```
For SPARC platform edition systems:
# cd /cdrom/cdrom0/sparc/Patches
# patchadd 106125-06
# patchadd 105284-15
# patchadd 105490-04
# patchadd 106040-10
# patchadd 106409-01

For Intel platform edition systems:
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105285-15
# patchadd 105491-04
# patchadd 106041-10
# patchadd 106410-01
```

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

Upgrading a Screen

The following procedures explain how to upgrade a Screen to SunScreen 3.2 from SunScreen EFS 1.1, 2.0, 3.0, as well as from SunScreen 3.1 and SunScreen 3.1 Lite.

Note – The upgrade software automatically backs up your previous SunScreen policies, certificates, and packages in case the upgrade fails. If you need to do other system backups or save other files, such as log files, do so now before upgrading your system to SunScreen 3.2. For the commands you use to back up this information, refer to the documentation that accompanied your release of SunScreen.

▼ To Upgrade a Locally-Administered Screen

Caution – To avoid corrupting your existing policies during an upgrade, do not run the SunScreen installer, which is run only for an initial installation.

1. **Open a terminal window and become root, if not already.**
2. **Insert the SunScreen CD into the CD-ROM drive.**
3. **When the File Manager window appears, click the upgrade icon.**
   - The software automatically removes the existing SunScreen SKIP and SunScreen software packages.
   - No confirmations are needed or accepted. The file and package names appear as output on your monitor. Wait until this completes.
   - The SunScreen software is automatically installed and the file and package names appear as output.
   - Your existing SunScreen policies are automatically converted to SunScreen 3.2 policies.
   - If there are any conversion errors, they are itemized and appear on your monitor. Wait until this completes.
4. **Reboot by typing:**

```
# sync; init 6
```

5. **Open a terminal window and become root, if not already.**
6. **List the policies that have been converted by typing:**

```
# ssadm policy -l
```

Note – After completing the upgrade from SunScreen EFS 1.1, or 2.0, you must review your packet filtering rules to verify the filtering order because SunScreen 3.2 uses ordered packet filtering rules and ordered NAT mappings. Also, be aware that NAT mappings changed considerably in SunScreen EFS 3.0 from the NAT mappings used in prior releases of SunScreen. See the SunScreen 3.2 Administrator's Overview for details on packet filtering rules and NAT mappings. See the *SunScreen 3.2 Administrator's Overview* for more details on packet filtering and ordered rules.

---

7. **Choose the one policy that you want to activate by typing:**

```
# ssadm activate configuration_name
```

8. **To launch the SunScreen administration GUI, run a Java-enabled Web browser compliant with JDK 1.1.3 or later, and type the following URL:**

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

If you were upgrading your remotely-administered Screen and have completed the procedure for upgrading a locally-administered Screen, return to "To Upgrade a Remotely-Administered Screen" on page 93.

For management information, see the *SunScreen 3.2 Administration Guide*.

▼ To Upgrade a Remotely-Administered Screen

The following procedures explain how to upgrade a remotely-administered Screen to SunScreen 3.2 from SunScreen EFS 1.1, 2.0, 3.0, as well as from SunScreen 3.1 and SunScreen 3.1 Lite. Upgrading requires that for remote administration you install the upgrade software on the Screen first and then on the Administration Station.

- **To upgrade your remotely-administered Screen, use the same instructions as explained in "To Upgrade a Locally-Administered Screen" on page 92.**

▼ To Upgrade the Remote Administration Station

Note – Perform this procedure manually. Do not run the upgrade script on the Administration Station.

---

1. **Open a terminal window on the Administration Station and become root, if not already.**

2. **Remove each SunScreen EFS 1.1, 2.0, 3.0, SunScreen 3.1, or SunScreen 3.1 Lite package individually by typing:**

```
For SunScreen EFS 1.1:
# pkgrm SUNWicgSA

For SunScreen EFS 2.0:
# pkgrm SUNWicgSA SUNWicgSD SUNWicgSM SUNWHJicg

For SunScreen EFS 3.0, SunScreen 3.1, and SunScreen 3.1 Lite:
# pkgrm SUNWicgSA SUNWicgSD SUNWicgSM SUNWicgSS
SUNWdthj SUNWhttp
```

Note – If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

---

3. **Follow the program prompts and answer all the questions with `y`.**

   The `pkgrm` program ends with the statement: `Removal of` *name_of_package* `was successful.`

4. **Remove the SKIP software packages by typing:**

```
For SunScreen EFS 1.1 and 2.0:
# pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg
SICGkisup SICGbdcdr

For SunScreen EFS 3.0:
# pkgrm SUNWbdc SUNWbdcx SUNWrc2 SUNWrc4
SUNWrc4x SUNWes SUNWesx SUNWkeyman SUNWkisup

For SunScreen 3.1 and SunScreen 3.1 Lite:
# pkgrm SUNWbdc SUNWbdcx SUNWbdes SUNWbdesx
SUNWrc2 SUNWrc4 SUNWrc4x SUNWes SUNWesx SUNWkeyman SUNWkisup
```

Note – If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

---

5. **This next step applies to SunScreen EFS 1.1 and 2.0 systems only. (Any SunScreen EFS 3.0 or SunScreen 3.1 cryptography upgrades can be left on your system.)**

Remove any SKIP cryptography upgrades by typing:

```
# pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup SICGkusup
```

Note – If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

---

6. **Reboot the system by typing:**

   ```
   # sync; init 6
   ```

7. **Insert the SunScreen 3.2 CD into the Administration Station's CD-ROM drive.**

8. **Add the SunScreen 3.2 packages by typing:**

   ```
   For SPARC platform edition systems:
   # pkgadd  -d /cdrom/cdrom0/sparc

   For Intel platform edition systems:
   # pkgadd  -d /cdrom/cdrom0/i386
   ```

9. **Follow the program prompts, answering all the questions with `y`.**
   When completed, you return to the same menu of packages.

10. **Type `q` to quit** `pkgadd`**.**

11. **(For SunScreen EFS 1.1 and 2.0 systems only) Move the SKIP keys by typing:**

    ```
    # cp -rp /etc/opt/SUNWicg/skip/* /etc/skip/
    ```

    a. **Eject the CD-ROM by typing:**

       ```
       # eject cdrom0
       ```

    b. **Reboot to complete the upgrade by typing:**

       ```
       # sync; init 6
       ```

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

    d. **Type `q` to quit** `pkgadd`**.**

12. **(For SunScreen EFS 1.1 and 2.0 systems only) Move the SKIP keys by typing:**

    ```
    # cp -rp /etc/opt/SUNWicg/skip/* /etc/skip/
    ```

    a. **Eject the CD-ROM by typing:**

       ```
       # eject cdrom0
       ```

    b. **Reboot to complete the upgrade by typing:**

       ```
       # sync; init 6
       ```

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

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

`http://`*name_of_screen*`:3852`

Upgrading a High Availability System

High availability (HA) enables you to deploy groups of Screens together in situations in which the connection between a protected inside network and an insecure outside network is critical. At any time, one member of the HA cluster is the active Screen while the other members are passive. The passive Screens generate the same state as the active Screen but they do not forward traffic. When an active Screen fails, the passive Screen that has been running the longest takes over as the active Screen within 15 seconds. During the 15 seconds, no traffic goes through the HA cluster. An active Screen can be either a secondary Screen or a primary Screen, which administers the secondary Screens. (See "Using High Availability" in *SunScreen 3.2 Administration Guide* for details regarding creating an HA cluster.)

The actual upgrade procedure is run on the HA primary Screen, only. Before proceeding, manually remove any previously installed SunScreen software from the HA secondary Screens.

The general steps needed to upgrade an HA system running SunScreen EFS 2.0, 3.0, or SunScreen 3.1 are described as follows:

▼ To Upgrade an HA System

1. **Backup your SunScreen and SKIP configurations and logfiles.**

   For the commands you use to back up this information, refer to the documentation that accompanied your release of SunScreen.

2. **On the HA secondary Screen:**

   a. **Manually remove the SunScreen EFS 2.0, 3.0, or SunScreen 3.1 software packages, certificates, policies, and log files.**

   b. **Run the SunScreen HA command to initialize the secondary.**

3. **On the HA primary Screen:**

   a. **Run the upgrade program.**

b. **Complete the primary upgrade.**

4. **Complete the upgrade:**

   a. **If upgrading from SunScreen EFS 2.0, define a `screen` object for each upgraded HA secondary Screen (see "Working With Screen Objects" in the *SunScreen 3.2 Administration Guide*).**

   b. **Activate the desired policy.**

▼ To Upgrade the HA Secondary Screen

1. **Before proceeding, remove any previously installed SunScreen software from the secondary Screen, manually.**

2. **On the secondary Screen, determine the name and HA network interface of the primary Screen's HA interface that is running the upgrade program by typing:**

```
# ssadm edit Initial
edit> list interface
```

3. **On the primary Screen, determine the IP address of the primary Screen's HA interface by typing:**

```
# ifconfig -a
```

   This command lists all of the Solaris plumbed network interfaces. The IP address of the primary Screen's HA interface is listed with the HA network interface you determined previously.

▼ To Remove the SunScreen Software

The following steps describe how to manually remove the SunScreen EFS 2.0, 3.0, or SunScreen 3.1 software packages, certificates, policies, and log files:

1. **On the secondary Screen, open a terminal window and become root, if not already.**

2. **Remove the SunScreen software packages by typing:**

   a. **For SunScreen EFS 2.0:**

```
# pkgrm SUNWicgSS SUNWicgEF SUNWicgSM SUNWHJicg
SUNWicgSD SUNWicgSA SUNWfwcnv
```

   b. **For SunScreen EFS 3.0:**

```
# pkgrm SUNWicgSS SUNWicgSA SUNWicgSD SUNWicgSM
SUNWdthj SUNWfwcnv SUNWhttp
```

   c. **For SunScreen 3.1:**

```
# pkgrm SUNWicgSF SUNWicgSS SUNWicgSA SUNWicgSD
SUNWicgSM SUNWdthj SUNWfwcnv SUNWhttp
```

Note – If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

---

3. **Remove any SKIP software packages by typing:**

   a. **For SunScreen EFS 2.0:**

   ```
   # pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg
   SICGkisup SICGbdcdr
   ```

   b. **For SunScreen EFS 3.0:**

   ```
   # pkgrm SUNWbcd SUNWbdcx SUNWrc2 SUNWrc4
   SUNWrc4x SUNWes SUNWesx SUNWkeyman SUNWkisup SUNWsman
   ```

Note – SunScreen 3.2 uses the same SKIP modules, plus a few additional packages, that were used by SunScreen 3.1.

---

4. **For SunScreen EFS 3.1, if needed, remove any SKIP cryptography upgrades by typing:**

   ```
   # pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup SICGkusup
   ```

Note – Leave any cryptography upgrades for SunScreen EFS 3.0 and SunScreen 3.1 on your system.

---

5. **Remove all previously installed SunScreen EFS certificates, configurations, and log files by typing:**

   ```
   # rm -rf /var/opt/SUNWicg /etc/opt/SUNWicg /etc/skip
   ```

Note – After you reboot your system, physically remove the secondary node from the network to avoid leaving it unprotected. Only leave the HA network connected.

---

6. **Reboot your system to complete the removal of the previously installed SunScreen software by typing:**

   ```
   # sync; init 6
   ```

▼ To Install the Software on the HA Secondary Screen

- **Follow the procedure as described in "To Install HA on the Secondary HA Screen" in Chapter 5, "Using High Availability," in the** *SunScreen 3.2 Administration Guide***.**

▼ To Upgrade the HA Primary Screen

1. **Follow the procedure "To Upgrade a Locally-Administered Screen" on page 92, then return to this section to complete the HA system upgrade.**
2. **For SunScreen EFS 2.0, when upgrading you must define the Screen's HA interface.**
   Before proceeding, you must know the following information:
   - The machine name of the HA primary Screen
   - The IP addresses on your dedicated HA network (for example `10.0.4.0 to 10.0.4.255`)
   - The network interface to be used for HA communication (for example `qfe0`)
   - The name of the active policy configuration (for example `Initial`)

   a. **On the HA primary Screen, open a terminal window and become root, if not already.**

   b. **The following is an example of what to type to define the primary Screen's HA interface:**

```
# ssadm edit Initial
      edit> add address qfe0 RANGE 10.0.4.0 10.0.4.255
      edit> delete interface qfe0
      edit> add interface SCREEN haprimary qfe0 HA qfe0
      edit> save
      edit> quit
```

▼ To Complete the HA Upgrade

1. **For SunScreen EFS 3.0 or SunScreen 3.1:**

   a. **On the primary Screen, activate the policy configuration by typing a command similar to the following:**

```
# ssadm activate Initial
```

   Note – It is now safe to reconnect your HA systems to the network.

2. **For SunScreen EFS 2.0:**

The remaining steps are performed on the upgraded primary Screen. These steps include initializing the primary interface, adding the HA secondary IP address, and activating the configuration.

a. Initialize the primary network interface by typing a command similar to the following:

```
# ssadm ha init_primary qfe0
```

b. Add the IP address of the secondary HA Screen by typing a command similar to the following:

```
# ssadm ha add_secondary 10.0.4.2
```

c. On the primary Screen, activate the policy configuration by typing a command similar to the following:

```
# ssadm activate Initial
```

Note – It is now safe to reconnect your HA systems to the network.

Upgrading From SunScreen SPF-200

The upgrade from SunScreen SPF-200 to SunScreen 3.2 requires a unique set of steps and can cause significant network downtime To reduce the downtime, consider transferring your SunScreen SPF-200 configurations to a new system and performing the upgrade on the new system.

Note – Have your original SunScreen SPF-200 installation diskette nearby in the event that the upgrade procedure fails and you need to return your Screen to its original SunScreen SPF-200 configuration.

▼ To Backup SunScreen SPF-200 and Install Patches

1. Backup the SunScreen SPF-200 Screen, referring to your SunScreen SPF-200 documentation, if needed.

The medium used for backing up your software and policies contains unencrypted, sensitive information. Store it in a secure location.

Note – Save your existing log files according to your documentation because they are not backed up automatically.

2. **Backup the SunScreen SPF-200 Administration Station, following regular Solaris software procedures.**

   The medium used for backing up your software and policies contains unencrypted, sensitive information. Store it in a secure location

3. **Install Patch 105047-21 on the Administration Station and Screen, if not already installed.**

   This patch is available through Sun Service.

4. **Mount the CD-ROM by typing:**

   ```
   # volcheck
   ```

5. **From the Administration Station, install a special SunScreen SPF-200 patch on the Screen, by typing:**

   ```
   # ss_client Name_of_Screen ss_patch install noreboot <
   /cdrom/cdrom0/sparc/Patches/spfUpgradePatch.tar.Z
   ```

Note – Install this patch only on the Screen. Do not install this patch on the Administration Station itself or on any other system. Also, do not reboot your system at this time.

▼ To Install the Software on the SunScreen SPF-200 Screen

1. **On the Administration Station, insert the SunScreen CD into the CD-ROM drive.**

2. **From the Administration Station, run a special script to gather the SunScreen SPF-200 Screen's configurations by typing:**

   ```
   # ss_client Name_of_Screen config2 > 200config.tar
   ```

Note – Do not change the name of the `200config.tar` file.

Caution – This file contains sensitive information. Do not send this file over insecure lines. To move this file, use a diskette or a secured connection only.

3. **Obtain your Administration Station's SKIP certificate ID by typing:**

```
# skiplocal list
```

A list of SKIP encryption certificate IDs displays. The SKIP connection creates secure, encrypted communication between the Administration Station and the Screen.

4. **Write down the correct SKIP certificate ID for your Administration Station.**
5. **On the Screen, reinstall your Solaris 2.6 , Solaris 7, or Solaris 8 software, following the instructions accompanying your Solaris CD.**

Note – You must reinstall the Solaris software because the version used with the SunScreen SPF-200 cannot be upgraded. You can now use a separate system to upgrade to.

---

6. **On the Administration Station, verify that your operating environment is at least the Solaris 2.6 version.**
7. **On the Screen, using the same interface ID that the SunScreen SPF-200 used as its administration interface (for example, `le0`), configure that interface only.**

   See your Solaris software documentation, if necessary.
8. **Remove the old SunScreen SPF-200 administration software by typing:**

```
# pkgrm SUNWicgSA
```

Note – If you did not originally install this package, do not run the `pkgrm` command.

---

9. **Remove the old SKIP packages from the Administration Station by typing:**

```
# pkgrm SICGcrc2 SICGcrc4 SICGes SICGkeymg
SICGkisup SICGbdcdr

To remove any SKIP cryptographic upgrades:
# pkgrm SICGcdes SICGc3des SICGcsafe SICGkdsup
SICGkusup
```

Note – If you did not originally install any of these packages, omit them from the string or else remove the packages one at a time.

▼ To Install the SunScreen 3.2 Software and Verify Installation

To prevent damage to the existing policies and make communication easier between the Administration Station and the Screen, upgrading requires you to first install the SunScreen software on the Screen and then on the Administration Station.

1. **On the Screen, install the SunScreen software according to the instructions in "Installing in Stealth Mode With Remote Administration Using SKIP" in the** *SunScreen 3.2 Installation Guide***.**

2. **On the Administration Station, install the SunScreen software according to the instructions in "Installing in Stealth Mode With Remote Administration Using SKIP" in the** *SunScreen 3.2 Installation Guide***.**

3. **On the Administration Station, move the SKIP keys by typing:**

```
# cp -rp /etc/sunscreen/skip/* /etc/skip/
```

4. **Reboot the Administration Station by typing:**

```
# sync; init 6
```

To enable remote administration between the Screen and Administration Station, you must create a new access control list (ACL) using the same SKIP MKID that was used by the SunScreen SPF-200 as its administration interface and a new Screen MKID.

Note – For the new ACL to take affect, it is important that you follow the exact instructions for the remote Administration Station referenced by the administration GUI in the `/etc/sunscreen/AdminSetup.readme` file.

---

5. **Replace the old ACL on the Administration Station with the new ACL using the existing key.**

Note – Ensure that your administration interface is the default because it is assumed by the `skiphost` commands. Specify a non-default interface.

---

6. **Make sure that the date on the Screen and the Administration Station are synchronized.**

▼ To Verify Remote Administration and Convert Policies On the Screen

1. **On the Administration Station, create a session on the Screen by typing:**

```
# SSADM_TICKET_FILE=$HOME/.ssadmticket
# export SSADM_TICKET_FILE
# touch $SSADM_TICKET_FILE
# chmod go= $SSADM_TICKET_FILE
# ssadm -r Name_of_Screen login admin admin
```

2. **On the Administration Station, verify that you are able to remotely administer the upgraded Screen by typing:**

```
# ssadm -r Name_of_Screen active
```

3. **On the Administration Station, begin the conversion of the SunScreen SPF-200 configurations to SunScreen 3.2 policies on the Screen by typing:**

```
# ssadm -r Name_of_Screen spf2efs < 200config.tar
```

4. **Verify your migrated configuration before activating it. To view and update the migrated configurations, open a Java-enabled Web browser and launch the SunScreen administration GUI by typing:**

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

See "Using the Administration GUI" in the *SunScreen 3.2 Administration Guide* for instructions on using the administration GUI.

Note – After completing the upgrade from SunScreen SPF-200, you must review your packet filtering rules to verify the filtering order because SunScreen 3.2 uses ordered packet filtering rules and ordered NAT mappings. Also, be aware that NAT mappings changed considerably in SunScreen EFS 3.0 from the NAT mappings used in prior releases of SunScreen. See the *SunScreen 3.2 Administrator's Overview* for more details on ordered rules and NAT mappings.

---

5. **On the Administration Station, activate your migrated configuration by typing:**

```
# ssadm -r Name_of_Screen activate Name_of_Configuration
```

Upgrading Cryptography Modules

U.S. export laws now allow the SunScreen Global default key size to be 4096 bit.

For the most current information regarding U.S. export laws, go to the Web site for The Bureau of Export Administration, U.S. Department of Commerce, at the following URL: `http://www.bxa.doc.gov/`.

Note – When you upgrade the Administration Station, the former 512-bit SKIP MKID key and certificate is installed in the administration GUI. Because the administration GUI is not aware of the key size, you must check for this situation and create a new 4096–bit key on the Administration Station. Then, during installation, use the 4096–bit key as the administration certificate identifier.

CHAPTER 8

Converting FireWall-1 to SunScreen in Routing Mode

This chapter explains how to convert from FireWall-1 (Release 3.0, 4.0, or 4.1) to a SunScreen system in routing mode.

Topics covered include:

Before installing the software, review the *SunScreen 3.2 Release Notes* for the latest information about this product.

Preparing Your FireWall-1 Configuration

Before you convert your FireWall-1 system, read this section carefully. There are certain limitations that you must address before running the conversion utility. You can experience unrecoverable errors that require restarting the migration. Your existing FireWall-1 configurations are not modified by this tool. You must first review your existing FireWall-1 configurations and modify those that will not convert directly to SunScreen rules. This section lists these known limitations.

Check your FireWall-1 configuration files and edit any that contain:

- Reserved characters in comments and object names
- Reserved words used for object names

If any of the following reserved characters or words are used, you need to remove or replace them.

Known FireWall-1 Reserved Characters

‘ ‘ (space)	‘+’
‘*’	‘?’
‘)‘	‘)’
‘{‘	‘}’
‘[‘	‘]’
‘!’	‘#’
‘<‘	‘>’
‘=’	‘,’ (comma)
‘:’ (colon)	‘:’ (semicolon)
‘’’ (quote)	‘`’ (back quote)
‘””’ (double quote)	‘/’ (slash)
‘\’ (back slash)	‘\t’ (tab)

Known FireWall-1 Reserved Words

The following are known reserved words that must not appear in the FireWall-1 object names, and must be edited prior to conversion:

“accept”	“fwrule”	“netof”
“and”	“gateways”	“nets”
“black”	“get”	“nexpires”
“blue”	“gold”	“not”
“broadcasts”	“gray 101”	“or”
“call”	“green”	“orange”
“cyan”	“if”	“origdst”
“dark green”	“ifaddr”	“origsport”
“dark orchid”	“ifid”	“origsrc”
“date”	“in”	“other”
“day”	“inbound”	“outbound”
“define”	“interface”	“packet”
“delete”	“interfaces”	“packetid”
“direction”	“ipsecdata”	“pass”
“do”	“ipsecmethods”	“r_arg”
“domains”	“hold”	“r_cdir”
“drop”	“host”	“r_cflags”
“dst”	“hosts”	“r_ckey”
“dynamic”	“kbuf”	“r_connarg”
“expcall”	“keep”	“r_ctype”
“expires”	“limit”	“r_entry”
“firebrick”	“log”	“r_proxy_action”
“foreground”	“magenta”	“r_tab_status”
“forest”	“medium slate”	“r_xlate”
“forest green”	“medium slate blue”	“record”
“format”	“modify”	“red”
“from”	“navy blue”	“resourceobj”
“fwline”	“netobj”	“refresh”

“reject”	“static”	“wasskipped”
“routers”	“sync”	“xlatedport”
“servers”	“targets”	“xlatedst”
“servobj”	“to”	“xlatesport”
“set”	“tod”	“xlatesrc”
“sienna”	“tracks”	“xor”
“skippeer”	“ufp”	“yellow”
“src”	“vanish”	

What Configurations Convert From FireWall-1

The following limitations apply when converting FireWall-1 configurations to SunScreen. Some object-types and rules migrate with no difficulty, while others do not. FireWall-1 rules that do not migrate, contain an operation (on the Source, Destination, or Service) that SunScreen does not support. The following table lists what will and what will not migrate from FireWall-1 to SunScreen.

TABLE 8–1 What Converts From FireWall-1

Does Convert	Does Not Convert
Host objects	Resources
Group objects	NAT mappings
Network objects	Gateway objects
Most rules	Encryption and authentication information and rules
	Domain objects
	Router objects
	Switch objects
	Logical objects
	FW-1 services or user defined services
	Install objects
	Rules containing any object or service that will not migrate
	Using an object type as an object name

SunScreen Conversion Utility

The following procedures explain how to install, generate, and run the conversion utility.

▼ To Install the Conversion Utility

1. **Open a terminal window and become root on the FireWall-1 system.**
2. **Insert the SunScreen CD-ROM into the CD-ROM drive.**
3. **Add the software by typing:**

```
For SPARC platform edition systems:
# pkgadd -d /cdrom/cdrom0/sparc SUNWfwcnv

For Intel platform edition systems:
# pkgadd -d /cdrom/cdrom0/i386 SUNWfwcnv
```

4. **Continue the installation when prompted by pressing Return.**

   The various files in `SUNWfwcnv` are displayed as they are installed. The installation ends with the following message: `Installation of SUNWfwcnv was successful.`

   The SunScreen conversion utility is now installed in `/opt/SUNWfwcnv/bin`.

Generating Conversion Files

The following procedures explain how to generate conversion files.

The `fwconvert` utility (located in `/opt/SUNWfwcnv/bin`) generates files that create the SunScreen configuration from the original FireWall-1 configuration. `fwconvert` examines the rules and objects in your FireWall-1 security policy and generates new configuration files with commands for configuring SunScreen.

`fwconvert` uses the following FireWall-1 configuration files:

- *policyname*`.W`, for FireWall-1, Release 2.1, files
- *policyname*`.pf`, for FireWall-1, Release 3.0 and later files
- `objects.C`, for FireWall-1, Releases 3.0, 4.0, and 4.1 files, where *policyname* is either `default` or the name you have given your policy. These files are located in the `/opt/SUNWfw/conf` directory.

Verify the location of these files and the name of the policy file (indicated by the `.pf` or `.W` extension) before you run `fwconvert`.

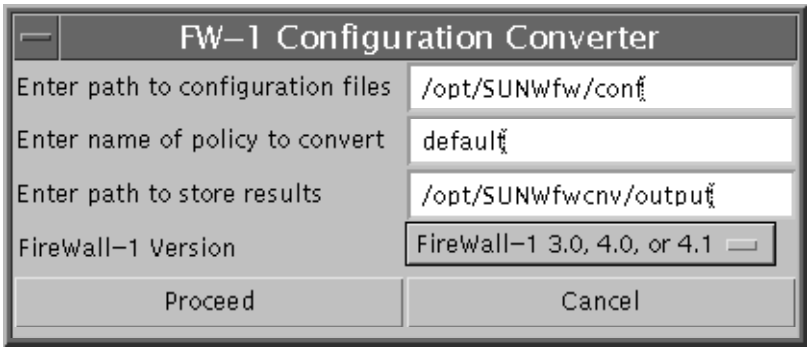
Note – You must run the conversion utility on the FireWall-1 system even if you are configuring SunScreen on a different system.

▼ To Run the Conversion Utility

1. **Open a terminal window and become root on the FireWall-1 system.**
2. **Run the conversion utility by typing:**

   ```
   # /opt/SUNWfwcnv/bin/fwconvert &
   ```

   `fwconvert` displays the FW-1 Configuration Converter dialog box with the default values already inserted.



3. **Type the path name where the FireWall-1 conversion files are located, or accept the default, if appropriate.**
4. **Type the name of the policy file you want to convert, if different from the default.**

Note – Do not type the `.pf` or `.W` extension.

---

5. **Type the name of the directory where you want to store the new configuration files. Make sure the directory actually exists before you proceed. Otherwise, accept the `/opt/SUNWfwcnv/output` default.**
6. **Choose the release number of your FireWall-1 software from the Version menu, or accept the default, if appropriate.**
7. **Click Proceed to begin the conversion.**

`fwconvert` reads the file *policyname*`.pf` (or *policyname*`.W`) and the `objects.C` files and generates the files used to create the SunScreen configuration.

When `fwconvert` completes successfully, the FireWall-1 Configuration Converter dialog box displays a DONE button.

8. **Click DONE to exit `fwconvert`.**

9. **Verify the converted rules.**

   For more information, see "Verifying the Converted Rules."

   After the conversion completes, the generated configuration files are located in the directory you specified in the FireWall-1 Configuration Converter dialog box (`/opt/SUNWfwcnv/output` by default). The *policyname*`_Objects` and *policyname*`_Rules` files must reside in the same directory as *policyname*`_sscfg` before you can run the *policyname*`_sscfg` generation program. Look at these files to confirm that the information converted correctly.

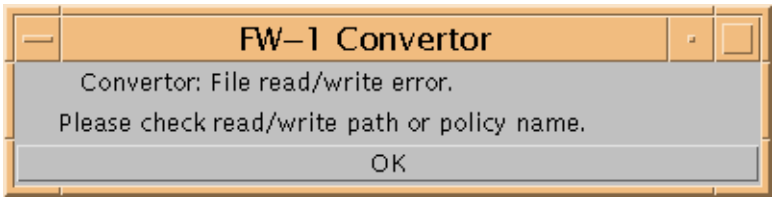
Troubleshooting the `fwconvert` Utility

The following describes how to troubleshoot the `fwconvert` utility.

The following conditions can cause the conversion to fail:

- You do not have permission to read files in `/opt/SUNWfw/conf` or the directory you specified as the location of the FireWall-1 configuration files.
- You do not have permission to write files into the directory that you specified for storing the results of `fwconvert`.
- The path names that you specified to the Converter are incorrect.
- The policy name that you specified is incorrect.
- One of the FireWall-1 configuration files you need to convert is missing.

When `fwconvert` encounters these conditions, it displays an error message in the FW-1 Converter dialog box, as shown in the following figure.



Note – When data cannot be parsed, this error is displayed on the terminal window and not in the FW-1 Converter dialog box.

▼ To Clear Conversion Errors (Except Parse Errors)

1. **Click the OK bar to clear the error message in the FW-1 Converter dialog box.**
2. **Change permissions on the affected directories, if applicable.**
3. **Fill in the corrected information in the `fwconvert` FW-1 Converter dialog box, making sure you have the accurate path names and file names that you need to specify.**
4. **Click the Retry button.**

   When it completes successfully, the FireWall-1 Configuration Converter displays the DONE button.
5. **Click DONE to exit `fwconvert`.**

   `fwconvert` creates a set of files that are used to generate the SunScreen 3.2 configuration.
6. **Verify the converted rules.**

   For more information, see "Verifying the Converted Rules" in *SunScreen Installation Guide*.

   After the conversion completes, the generated configuration files are located in the directory you specified in the FireWall-1 Configuration Converter dialog box, (`/opt/SUNWfwcnv/output` by default). The *policyname*`_Objects` and *policyname*`_Rules` files must reside in the same directory as *policyname*`_sscfg` before you can run the *policyname*`_sscfg` generation program. Look at these files to confirm that the information was correctly converted.

▼ To Clear Parse Errors

Note – The most common parse error is caused by the use of a reserved character (such as a ' ' space) in an object name.

1. **Edit the line containing the error manually.**
2. **Restart `fwconvert`.**

   See the procedure "To Install the Conversion Utility" in *SunScreen Installation Guide*, if needed.

Verifying the Converted Rules

`fwconvert` creates three types of files from the FireWall-1 configuration files: command, executable, and log files. See the following table for a complete list.

TABLE 8–2 Generated Configuration Files

File Type	File Name	Description
Data file	*policyname*_Objects	Contains the commands for configuring the SunScreen objects.
Data file	*policyname*_Rules	Contains the commands for adding SunScreen rules that use the generated objects.
Executable script	*policyname*_sscfg	Generates a SunScreen configuration from the commands in *policyname*_Objects and *policyname*_Rules.
Log file	*policyname*_Obj.log	Contains the objects from FireWall-1 that are not supported by SunScreen.
Log file	*policyname*_Rule.log	Contains the rules from FireWall-1 that could not be added. The rule is shown as a SunScreen rule command with an explanation of the reason why the rule is not supported.
Log file	*policyname*_Unused.log	Lists the FireWall-1 objects that cannot be used in SunScreen.

Command and Executable Files

When you create the new SunScreen configuration, you run the configuration program, which then executes the command files. You do not need to take further action on the command and executable files.

The following shows examples of these files.

EXAMPLE 8–1 *policyname*_Objects File

```
# The address commands may contain other addresses
which need to be created.
# These objects are logged in the policyname_Obj.log file
 add_nocheck Address  "mailhost-INT" HOST 205.167.60.6
COMMENT "Object from FW-1"
 add_nocheck Address  "mailhost-EXT" HOST 207.82.121.5
COMMENT "Object from FW-1"
 add_nocheck Address  "localnet" NETWORK 205.167.60.00
255.255.255.00  COMMENT "Object from FW-1"
```

EXAMPLE 8–1 *policyname*_Objects File *(Continued)*

```
 add_nocheck Address  "talon" HOST 205.167.60.200
COMMENT "Object from FW-1" add_no

check Address  "exosecure-alc" HOST 207.82.121.254
COMMENT "Object from FW-1" save
```

EXAMPLE 8–2 *policyname*_Rules File

```
add_nocheck Rule "ip all" "*" "*" ALLOW LOG SUMMARY save
```

EXAMPLE 8–3 *policyname*_sscfg File (where *policyname* is 4complex)

```
#!/bin/csh
setenv PATH .:/usr/bin:/usr/sbin:/bin:/usr/sbin
echo Creating Policy: 4complex
ssadm policy -a 4complex
echo Adding Policy Addresses
/usr/sbin/ssadm edit -P 4complex < 4complex_Objects
echo Adding Policy Rules
/usr/sbin/ssadm edit -P 4complex < 4complex_Rules
echo Finished!
```

Log Files

The log files describe instances where fwconvert could not directly convert your FireWall-1 policy to an equivalent SunScreen policy. After conversion, you should review the contents of the log files to see what else you may need to do to the new SunScreen configuration.

*policyname*_Obj.log

The *policyname*_Obj.log file lists objects found in your FireWall-1 security policy that were not directly supported in SunScreen 3.2. The following table lists the FireWall-1 objects and shows whether they were converted to SunScreen 3.2.

TABLE 8–3 How Conversion to SunScreen 3.2 Affects FireWall-1 Objects

FireWall-1 Object	SunScreen Equivalent	Conversion Status
Host	Host	Yes.
Network	Range	Yes.

TABLE 8–3 How Conversion to SunScreen 3.2 Affects FireWall-1 Objects *(Continued)*

FireWall-1 Object	SunScreen Equivalent	Conversion Status
Router	None	No. See the *policyname*_Obj.log file for details.
Switch	None	No. See the *policyname*_Obj log file for details.
Domain	None	No. See the *policyname*_Obj log file for details.
Group	Group	Yes.
Gateways	None	No. However, they are logged in the *policyname*_OBJ.log file. Gateways require more configuration within SunScreen to assure that the IP addresses of the gateway are correct. See the *SunScreen 3.2 Administration Guide* for more information.

The following figure shows a sample *policyname*_Obj.log file, similar to the file that you can generate from your FireWall-1 policy.

EXAMPLE 8–4 *policyname*_Obj.log File

```
/***** SunScreen: Firewall-1 conversion log *****/
/***** @(#)ObjStore.java    3.7 99/11/09 Sun Microsystems, Inc. *****/

Objects of type: gateway, need some user decisions
You had a gateway with name "skil" ipaddr 205.167.60.13
If this is the gateway on which SunScreen is being installed
please refer to the 'ssadm edit' command to enable the interfaces
```

*policyname*_Rule.log

This file shows rules generated from FireWall-1 rules that cannot be used in the SunScreenenvironment without modification. The *policyname*_Rule.log file explains why these rules were not added to the SunScreen firewall, for example:

- Source, Destination, or Installed on objects are of a type not supported by SunScreen
- FireWall-1 Service is of a type not supported by SunScreen
- FireWall-1 Action is not supported by SunScreen

SunScreen does not support FireWall-1 encryption, user authentication, or client authentication. Encryption in SunScreen is accomplished through SunScreen IKE or SunScreen SKIP, as explained in the *SunScreen 3.2 Administrator's Overview*. For more information regarding SKIP, see the *SunScreen SKIP User's Guide, Release 1.5.1*.

Caution – All FireWall-1 rules are generated during the conversion. You must remove any rules that you do not need manually.

The following shows a sample *policyname*_Rule.log file that might be generated after the FireWall-1 to SunScreen conversion.

EXAMPLE 8–5 *policyname*_Rule.log File

```
/***** SunScreen: Firewall-1 conversion log *****/
/***** @(#)RuleStore.java    3.6 99/11/09 Sun Microsystems, Inc. *****/

Rule below not added as the action Encrypt is configured differently
in SunScreen.
 add_nocheck Rule  "smtp" "aiims" "*" Encrypt

Rule below not added as the action Encrypt is configured differently
in SunScreen.
 add_nocheck Rule  "echo" "aiims" "*" Encrypt

Rule below not added as the action User Authentication is not valid
in SunScreen.
 add_nocheck Rule  "ftp" "*" "aiims" User

Rule below not added as the action Client Encryption/Authentication
is not valid in SunScreen.
 add_nocheck Rule  "dns" """ "*" Client
```

*policyname*_Unused.log

The following figure lists FireWall-1 objects encountered in your policy that are not supported by SunScreen.

EXAMPLE 8–6 *policyname*_Unused.log File

```
#Invalid Objects from FW-1
#Wed Mar 31 17:40:23 PST 1999
invalidobj1=gateway skil
```

Creating the SunScreen Configuration

The following procedures explain how you prepare for and generate the new SunScreen configuration.

Choosing which of the next two procedures to follow depends on whether you plan to run SunScreen on the former FireWall-1 system or on a new system. Option 1 discusses preparing the FireWall-1 system to become a SunScreen system. Option 2 discusses preparing a new system to run the converted FireWall-1 configurations.

Note – Choose only one of the four options.

▼ Option 1: To Prepare the FireWall-1 System to Run SunScreen

1. **Open a terminal window and become root, if not already.**
2. **Save the existing FireWall-1 configuration files located in the** `/opt/SUNWfw/conf` **directory as a backup.**
3. **Use the** `pkgrm` **command to remove the** `SUNWfw` **package by typing:**

   ```
   # pkgrm SUNWfw
   # pkgrm SUNWwfwvpn
   # pkgrm SUNWwfwdes
   ```

4. **Upgrade to at least the Solaris 2.6 operating environment (if not already done).**

   See your Solaris documentation for instructions, if necessary.

5. **Install the additional Solaris software packages and kernel packages required as listed in "Installation Overview" in** *SunScreen Installation Guide* **(if not already done).**

   Note – Prior to installing the SunScreen software, make sure that the system is performing properly as a router.

   ---

6. **Install the SunScreen software as described in "Installing in Routing Mode With Local Administration" in** *SunScreen Installation Guide***.**

   Continue to the section, "To Generate the New SunScreen Configuration" on page 117.

▼ Option 2: To Prepare a New SunScreen System to Run the Converted FireWall-1 Configuration

---

Note – Prior to installing the SunScreen software, make sure that the system is performing properly as a router.

---

1. **Open a terminal window and become root, if not already.**
2. **Upgrade to at least the Solaris 2.6 operating environment (if not already done).**
   See your Solaris operating environment documentation for instructions, if necessary.
3. **Install the additional Solaris software packages and kernel packages required as listed in "Installation Overview" in** *SunScreen Installation Guide* **(if not already done).**
4. **Copy the generated configuration files to a directory on the new SunScreen system.**
5. **Install the SunScreen software as described in "Installing in Routing Mode With Local Administration" in** *SunScreen Installation Guide***.**

   Continue to the section, "To Generate the New SunScreen Configuration" on page 117.

▼ To Generate the New SunScreen Configuration

1. **Open a terminal window and become root, if not already.**
2. **Change to the directory where the conversion files were saved and make the** *policyname*`_sscfg` **file executable by typing:**

   ```
   # chmod 544policyname_sscfg
   ```

3. **Verify that the commands in the generated file are accurate by typing:**

   ```
   # ./policyname_sscfg
   ```

   policyname`_sscfg` creates the new SunScreen configuration from the FireWall-1 configuration, which is similar to the FireWall-1 policy.

   See the *SunScreen 3.2 Administration Guide* for instructions on activating the configuration.

CHAPTER 9

Removing SunScreen Software

This chapter describes how to remove the SunScreen software.

Topics covered in this chapter:

The following procedure describes how to remove the SunScreen software.

Removing the SunScreen Software

The following procedure describes how to remove the SunScreen software.

▼ To Remove the SunScreen Software

If you remove SunScreen packages from a Screen when the active configuration includes rules that use proxies, the disabled Solaris services, such as the standard FTP daemon, are not reinstated.

To ensure that they are reinstated, perform the following steps before removing the SunScreen packages:

Note – Remove the Screen from the managed group, if it is a secondary Screen. Use the instructions in the Section, "To Remove a Member From a Certificate Group" in the *SunScreen 3.2 Administration Guide*.

---

1. **If you used the SunScreen GUI-based installer to install the SunScreen software**

and the product registry was present:

a. **When running the Solaris 8, update 3 or newer, software, remove the SunScreen software through the product registry by typing:**

```
# /usr/bin/prodreg
```

SunScreen appears as an installed component, which you can select and remove by clicking the "uninstall" button.

b. **When running a release lower than the Solaris 8, update 3, software, execute the GUI-based uninstaller directly by typing:**

```
# cd /var/sadm/prod
# java uninstall_SunScreen_3_2_Full
```

2. **To verify that the SunScreen packages were removed, type:**

```
# pkginfo SUNWsfwau
```

This package should no longer be installed on the system if the GUI uninstaller was successful in removing SunScreen.

3. **If you used** `pkgadd` **to install the SunScreen software, use** `pkgrm` **to remove the software packages originally installed on the system.**

For a list of the software packages to remove see "Command Line Installation" in the *SunScreen 3.2 Installation Guide*.

4. **To remove the configurations and log files, delete the following:**

- `/var/sunscreen` and its descendants, which contain the SunScreen packet logfiles.
- `/etc/sunscreen` and its descendants, which contain the SunScreen configurations and policies.
- `/etc/skip` and its descendants, which contain the SKIP keys and certificates.

Note – Because these three sets of files are not removed as part of the `pkgrm` command, 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 your initial policy. Use the administration GUI to delete unwanted duplicates.

If you do not remove the old SKIP keys and certificates, when the software is reinstalled multiple Screen identities are created. To remove the SKIP identities completely, see the *SunScreen SKIP User's Guide, Release 1.5.1*, for more information about `skiplocal` and `skipdb`.

5. **Reboot to complete the removal of the SunScreen software by typing:**

```
# sync; init 6
```

Note – Reboot is required to remove the packet filtering modules to be unloaded.

The following procedure describes how to remove the SunScreen software when using proxies.

▼ To Remove SunScreen When Using Proxies

1. **If you have used proxies in your configuration: Remove all rules that use proxies (or else instantiate a policy that uses no proxies) to restore the `sendmail` and `inetd` daemons to their original Solaris functionality. On configurations with a number of centrally managed Screens, it may be simpler to restore these daemons manually:**

   a. **If the FTP or telnet proxy is in use, remove the `#efs#` prefix that comments them out in `/etc/inet/inetd.conf`. For example:**

   ```
   # efs#ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd

   # efs#telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd
   ```

   b. **If the SMTP proxy is in use, the command that invokes `sendmail` as a listening daemon was altered. For example:**

   ```
   # /usr/lib/sendmail -q15m & #efs{-bd}
   ```

   Move the commented {`-bd`} option back into its original location:

   ```
   # /usr/lib/sendmail -bd -q15m &
   ```

2. **Stop the current proxies in one of the following two ways:**

   a. **Activate a policy that does not contain proxy rules.**

   b. **Deactivate the proxies manually using the command line, as root, by typing:**

   ```
   # rm /etc/opt/SUNWicg/SunScreen/.active/*.conf# /etc/init.d/proxy stop
   ```

Note – This method is specific to SunScreen 3.2, as it uses path names and interfaces that are not guaranteed to exist in future releases.

The original daemons (that is, `sendmail`, `telnetd`, and `ftpd`) are reinstated.

APPENDIX **A**

Command Line Installation

This appendix contains SunScreen 3.2 installation procedures performed using the command line. You can use these procedures when installing SunScreen 3.2 in routing or stealth modes.

Topics covered include:

Expert system administrators can use the command-line installation as an alternative to using the installer. Before installing the software, review the *SunScreen 3.2 Release Notes* for the latest information about this product.

Note – Be sure to make a map of your network before you begin this installation. See "Determining Your Security Policy" in the *SunScreen 3.2 Installation Guide* appendix for worksheets and instructions to aid you in determining your network configuration and your desired security level.

The following procedures describing how to install the software and create the certificates use the same order as demonstrated in "Installing in Routing Mode With Remote Administration" in the *SunScreen 3.2 Installation Guide* and in "Installing in Stealth Mode With Remote Administration" in the *SunScreen 3.2 Installation Guide*. The installation scenario is a three-step process that requires you to first install the appropriate software on the remote administrative Screen or Administration Station, then install the appropriate software on the Screen designated as the firewall, and last, establish encrypted communication between the remote administrative Screen and the firewall Screen using IKE or between the Administration Station and the Screen using SKIP.

Note – Command line procedures for upgrading your system to SunScreen 3.2 from SunScreen SPF-200, SunScreen EFS 1.1, 2.0, 3.0, SunScreen 3.0, SunScreen 3.1, SunScreen 3.1 Lite, and SunScreen 3.2 Lite are in "Upgrading Your System" in this manual.

Routing and Stealth Mode Installation Summary

See "Routing and Stealth Mode Installation Summary" on page 72 for information on an IKE and SKIP routing mode installation and "Routing Mode Installation Summary" on page 40 for a SKIP routing mode installation. Also, "Stealth Mode Installation Summary" on page 56 for a SKIP stealth mode installation.

When installing a Screen in stealth mode, when asked if you want to harden the Screen, understand that hardening is an option and if chosen automatically removes any Solaris software files and packages that might otherwise make your system vulnerable to an attack. The hardening process can be performed during installation or at a later time by running the script on the command line: `/usr/lib/sunscreen/lib/harden_os`.

Caution – Once you harden your Screen, it becomes a dedicated firewall and cannot be used for any other purpose without first reinstalling the Solaris software.

Required SunScreen Software Packages

The following list shows the SunScreen packages followed by the numbers of the requires SunScreen packages.

For a list of the available packages, type:

```
# pkgadd -d /cdrom/cdrom0/sparc

  1  NSCPcom       Netscape Communicator
                   (sparc) 20.4.70,REV=1999.08.20.17.43
  2  SUNW3des      SKIP 3DES Crypto Module
                   (sparc) 1.5.1
  3  SUNW3desx     SKIP 3DES Crypto Module (64-bit)
```

```
                    (sparc) 1.5.1
  4  SUNWbdc        SKIP Bulk Data Crypt
                    (sparc) 1.5.1
  5  SUNWbdcx       SKIP Bulk Data Crypt (64-bit)
                    (sparc) 1.5.1
  6  SUNWdes        SKIP DES Crypto Module
                    (sparc) 1.5.1
  7  SUNWdesx       SKIP DES Crypto Module (64-bit)
                    (sparc) 1.5.1
  8  SUNWdthj       HotJava Browser for Solaris
                    (sparc) 1.1.5,REV=1998.12.03
  9  SUNWdtnsc      Netscape Componentization Support for CDE
                    (sparc) 1.0,REV=1999.06.14.15.50
 10  SUNWes         SKIP End System
                    (sparc) 1.5.1

... 21 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:

 11  SUNWesx        SKIP End System (64-bit)
                    (sparc) 1.5.1
 12  SUNWfwcnv      SunScreen tools for migration from Firewall-1
                    (sparc) 3.2,REV=40
 13  SUNWhttp       Sun WebServer daemon and supporting binaries
                    (sparc) 2.0
 14  SUNWkdsup      SKIP D-Support module
                    (sparc) 1.5.1
 15  SUNWkeymg      SKIP Key Manager Tools
                    (sparc) 1.5.1
 16  SUNWrc2        SKIP RC2 Crypto Module
                    (sparc) 1.5.1
 17  SUNWrc4        SKIP RC4 Crypto Module
                    (sparc) 1.5.1
 18  SUNWrc4s       SKIP RC4-128 Crypto Module
                    (sparc) 1.5.1
 19  SUNWrc4sx      SKIP RC4-128 Crypto Module (64-bit)
                    (sparc) 1.5.1
 20  SUNWrc4x       SKIP RC4 Crypto Module (64-bit)
                    (sparc) 1.5.1

... 11 more menu choices to follow;
<RETURN> for more choices, <CTRL-D> to stop display:

 21  SUNWsafe       SKIP SAFER Crypto Module
                    (sparc) 1.5.1
 22  SUNWsafex      SKIP SAFER Crypto Module (64-bit)
                    (sparc) 1.5.1
 23  SUNWsfwau      SunScreen Administrative Software
                    (sparc) 3.2,REV=40
 24  SUNWsfwd       SunScreen Online Documentation
                    (sparc) 3.2,REV=40
 25  SUNWsfwf       SunScreen Full Functionality
                    (sparc) 3.2,REV=40
 26  SUNWsfwg       SunScreen Administrative GUI
                    (sparc) 3.2,REV=40
```

```
 27  SUNWsfwi      SunScreen Interim IKE Software
                   (sparc) 3.2
 28  SUNWsfwm      SunScreen On-Line Manual Pages
                   (sparc) 3.2,REV=40
 29  SUNWsfwr      SunScreen Firewall, (Root)
                   (sparc) 3.2,REV=40
 30  SUNWsfwu      SunScreen Firewall, (Usr)
                   (sparc) 3.2,REV=40

... 1 more menu choice to follow;
<RETURN> for more choices, <CTRL-D> to stop display:

 31  SUNWsman      SKIP Man Pages
                   (sparc) 1.5.1
For SPARC Platform Edition Systems: Select the package(s) you wish to process (or 'all' to process
```

Note – Never add the end-system SKIP packages `SUNWes` and `SUNWesx` to the Screen.

- For Trusted Solaris 8:

  For a Screen, specify: 1-9 and 13-31. For a Remote Administration Station, specify: 1-11, 14-24, 28, and 31.

- For Solaris 9

  For a Screen, specify: 2-7 and 13-31. For a Remote Administration Station, specify: 2-7, 10-11, 14-24, 28, and 31.

Installing a Default Installation Through the Command Line

The following describes installing the SunScreen default installation through the command line.

▼ To Install the SunScreen Software Locally in Routing Mode Through the Command Line

Note – For the following procedure to work, you *must* have already installed the prerequisite Solaris packages; added the SunScreen packages, and rebooted your system.

1. **To begin the installation after rebooting your system, as root, type the following:**

```
# ssadm configure
```

A message appears: Checking for required packages.

2. **Press ENTER to continue if the prerequisite Solaris packages were installed, the SunScreen packages added, and you rebooted your system; otherwise, press Control-C to abort the installation.**

   You are asked which type of Screen you want to install: 1 (routing, the default entry) or 2.

3. **Specify 1, Routing, as the Screen Type.**

   The Screen can be set up as a router or as a bridge providing stealth. Which type of Screen you employ affects how the interfaces are initialized. For routing Screens, each interface is set up as a routing interface. For a stealth Screen, there is only one interface available, which is dedicated to Screen administration.

   You are asked which type of administration you want to install: 1 (routing, the default entry) or 2.

4. **Specify 1, Local administration.**

   When using (1) local administration, all administration is performed on the Screen itself. When administering the Screen from a (2) remote Administration Station, you need to install the SunScreen administration packages, IKE or SKIP certificates, and a local key onto the Administration Station before continuing. When appropriate, you can also specify both Local and Remote.

   You are asked which level of security you want to install.

5. **Specify 3, Permissive, as the security level.**

   There are three possible security levels and each security level corresponds to a different set of permitted services to, from, and through the Screen. The permissive security level is the default and can be used for the initial configuration and changed at any time after installation.

   The security levels are as follow:

   1. Permissive - This level allows most traffic, including inbound connections to the Screen itself and all traffic through the Screen. This security level is for installing the Screen onto a host that has multiple network interfaces and that acts as a router, or on a host that is acting as a server (for example, for NFS, NIS, or WWW).
   2. Restrictive - This level of security disallows all traffic to, from, and through the Screen, except for encrypted administration traffic. This level is best for deploying the Screen in an unsecured network environment. It requires that static routing and name resolution are configured on the host.
   3. Secure (routing Screens only) - This level disallows all traffic to and through the Screen, except for encrypted administration traffic, common services from the Screen, name server resolution traffic (like DNS and NIS), and routing (RIP). This level is a good starting point for getting a Screen up and running on a secure network, where the Screen cannot be a standalone system and depends on NIS, DNS, or NFS to function properly.

Note – With the exception of the Restrictive security level, no IP spoofing protection is provided until the system is properly configured.

A message appears: The following name resolution method was detected on this machine: None or Static name resolution from the `/etc/hosts` file.

6. **Specify 1, YES, to accept the Name Resolution as detected, if this is the name service that you want to use on this machine.**

Note – Make sure this is the name service that you want to use on this system (see "Preparing to Install High Availability" in *SunScreen 3.2 Administration Guide*).

7. **When the system configuration completes, reboot the system for your changes to take effect.**

Installing the Administration Packages

When installing the administration packages, the following limitations and requirements are present

The following is a list of limitations and requirements:

- To correct a known problem on the `screen address` object in the administration GUI, use the command line to revise the `addr`.
- Remote administration is affected by a known fragmentation problem on locally generated packets. To correct this problem, change the `screen admin` interface `mtu` to 1400.
- You must use the command-line interface to create IKE self-generated certificates on an administrative Screen.
- Due to a known problem in stealth mode in a temporary `kmcookies` file that causes the compiler to not create an `ike config` file, you must manually create an `ike config` file.
- If you are using SKIP CA-issued certificates for encryption, you need all of your certificate diskettes.
- Before proceeding, clean the state on both systems using the `-f` and `-fs` statetables.

▼ To Install the Administration Packages

1. **Open a terminal window on your system and become root, if not already.**
2. **Insert the SunScreen 3.2 CD into your system's CD-ROM drive.**
3. **Add the software by typing:**

   ```
   # pkgadd -d /cdrom/cdrom0/sparc
   ```

4. **Follow the program prompts, answering all the questions with `y`.**
   When completed, you return to the same menu of packages.
5. **Type `q` to quit** `pkgadd`**.**
6. **Complete the installation by activating your policy configuration.**
7. **Answer the questions that appear.**
   The questions and text are similar to those that appear when installing using the installer. Review the procedures for installing the software on the Screen in "Installing in Routing Mode With Remote Administration" in *SunScreen Installation Guide* or "Installing in Stealth Mode" in *SunScreen Installation Guide* if more details are needed.
8. **Eject the CD by typing:**

   ```
   # eject cdrom0
   ```

9. **Reboot by typing:**

   ```
   # sync; init 6
   ```

   After installing the software packages, set up encrypted communication between the Administration Station and the Screen.

Note – Both the Administration Station and the Screen need certificates before encrypted communication can begin.

Creating Encryption Certificates

This section describes how to set up encrypted communication between the Administration Station and the Screen.

The following is a list of limitations and requirements:

- There is a GUI problem on the `screen address` object that causes the `remote admin` rule to use the wrong address, which forces you to fix the `addr`.

- There is a fragmentation issue on locally generated packets that also affects the remote administrative Screen or remote Administration Station, which forces you to change the `screen admin` interface `mtu` to `1400`.
- Clean the state using `statetables -f, -fs` on both systems.
- When temporary `kmcookies` files are touched, the compiler used in a stealth system does not generate the IKE configuration, which forces you to manually create an IKE configuration file.

After installing the appropriate software on both systems, create the IKE self-generated certificates on the systems as described in the following sections.

▼ To Create Certificates on the Administration Station

1. **When using IKE self-generated certificates, after installing the appropriate SunScreen software on both Screens, create the certificates on the systems (see "To Create SKIP UDH Key and Certificates" on page 141).**
2. **When using SKIP UDH keys and certificates to encrypt the communication between the Administration Station and the Screen (see "To Create SKIP UDH Key and Certificates" on page 141).**
3. **When using SKIP CA-issued private keys and certificates (see "To Load SKIP CA-Issued Private Key and Certificates" on page 142).**

▼ To Create Remote Administration Screen IKE Self-Generated Certificates

1. **On the Remote Administrative Screen, create the IKE self-generated certificate by typing:**

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D "C=US,
O=YOUR_ORG, CN=admin_name"
```

2. **Export the administrative Screen's certificate to a file by typing:**

```
# ssadm certdb -I -e "C=US, O=YOUR_ORG,
CN=admin_name" > /tmp/admin_cert
```

3. **Import the firewall Screen's certificate by typing:**

```
# ssadm certdb -I -a < /tmp/screen_cert
then, using ssadm edit
edit > add certificate admin_cert SINGLE IKE "C=US, O=SUN,
CN=admin_name"
edit > add certificate screen_cert SINGLE IKE "C=US, O=SUN,
```

CN=*screen_name***"**

4. **Add a packet filter rule like the following:**

```
1 "remote administration" "admin_address" "screen_address"
IPSEC ESP("DES-CBC", "MD5") AH("SHA1") IKE("DES-CBC", "MD5",
1, RSA-SIGNATURES, "admin_cert", "screen_cert") ALLOW
```

See "Packet Filtering Rules" in *SunScreen 3.2 Administration Guide*.

5. **Mark the Screen's certificate as trusted by typing:**

```
> add member certificate "IKE manually verified certificates"
"screen_cert"
```

6. **Activate the policies.**

▼ To Create the Firewall Screen's IKE self-Generated Certificate

1. **On the firewall Screen, create the IKE self-generated certificate by typing:**

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D
"C=US, O=YOUR_ORG, CN=screen_name"
```

2. **Export the firewall Screen's IKE certificate to a file by typing.**

```
# ssadm certdb -I -e "C=US, O=YOUR_ORG,
CN=screen_name" > /tmp/screen_cert
```

3. **Import the administrative Screen's certificate by typing.**

```
# ssadm certdb -I -a < /tmp/admin_cert
then using ssadm edit
edit > add certificate admin_cert SINGLE IKE
"C=US, O=SUN, CN=admin_name"
edit > add certificate screen_cert SINGLE IKE
"C=US, O=SUN, CN=screen_name"
```

4. **Add the administrative Screen's IP address to `address` object.**

5. **Add the administrative Screen as a `screen` object and allow routing traffic and naming service.**

6. **Edit the firewall Screen's `screen` object by selecting the primary/secondary tab and making the remote administrative Screen's IP address the administrative IP address in the IKE administrative certificate field, and add the firewall Screen's certificate.**

7. **Mark the administrative certificate as trusted by typing:**

```
> add member certificate "IKE manually verified certificates"
"admin_cert"
```

8. **Add a remote add rule by selecting the administrative access tab and under Access rules for remote administration table, click the add new rule button.**

```
screen: screen name
address object: remote admin address
user: admin
access level: all
encryption: IPSEC IKE
```

9. **Select the one algorithm that matches the packeting filtering rule on the remote firewall Screen's source certificate:** `screen cert`**.**

10. **Click on the Options tab, source screen: screen name.**

    When finished, you should have a remote access rule like the following:

```
1 SCREEN "screen_name" USER "admin" "admin_addr"
IPSEC ESP("DES-CBC", "MD5") AH("SHA1") IKE("DES-CBC", "MD5",
1, RSA-SIGNATURES, "screen_cert") PERMISSION ALL
```

Note – No packet filtering rule is required on the firewall Screen.

---

11. **Activate the policies.**

    The following command-line interface examples demonstrate how to use the SunScreen command line to use IKE in this release:

    - To find instructions on adding an IPsec key, see "IPsec Key" in the *SunScreen 3.2 Administration Guide*.
    - To find instructions on creating, importing, and exporting IKE certificates and pre-shared keys, see "Certificate Objects" in the *SunScreen 3.2 Administration Guide*.
    - Also, to find an example of an encryption scenario that uses IKE, see "Setting Up Remote Administration with IKE" in the *SunScreen 3.2 Configuration Examples* manual.

▼ To Use IPses Manual Keying

The following is an example of adding manual IPsec rules:

1. **Add manual keys on both Screens using** `ssadm edit` **or the administration GUI.**

```
edit> add key "key_des" SINGLE "1234567812345678"
edit> add key "key_ah" SINGLE "1234567890abcdef1234567890abcdef"
```

2. **Add rules like the following using keys added on both Screens.**

   a. **On Screen1:**

```
1 "telnet" "screen1_host" "screen2_host" IPSEC ESP(0x123, "DES-CBC",
"key_des") AH(0x345, "MD5", "key_ah") SOURCE_SCREEN "screen1" ALLOW
```

```
2 "telnet" "screen2_host" "screen1_host" IPSEC ESP(0x123, "DES-CBC",
"key_des") AH(0x345, "MD5", "key_ah") DESTINATION_SCREEN "screen1" ALLOW
```

b. On Screen2:

```
1 "telnet" "screen2_host" "screen_host1" IPSEC ESP(0x123, "DES-CBC",
"key_des") AH(0x345, "MD5", "key_ah") SOURCE_SCREEN "screen2" ALLOW
2 "telnet" "screen1_host" "screen2_host" IPSEC ESP(0x123, "DES-CBC",
"key_des") AH(0x345, "MD5", "key_ah") DESTINATION_SCREEN "screen2" ALLOW
```

The hex values `0x123`, `0x345` are spi values and are between 0x000 and 0xFFF. If you choose different algorithms like 3DES-CBC or SHA1, you must define manual keys of the proper length. In hex strings, the lengths are respectively.

- DES-CBC 16
- 3DES-CBC 48
- MD5 32
- SHA1 40

3. Save and activate the policy.

▼ To Use IKE Rules With Pre-Shared Key

1. Add the pre-shared secret key on both Screens.

```
edit> add key "shared-secret" SINGLE "shared_secret"
```

2. Add rules like the following using keys added on both Screens.

- On Screen1:

```
1 "telnet" "screen1_host" "screen2_host"
IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, PRE-SHARED,
"shared-secret") SOURCE_SCREEN "screen1" ALLOW
2 "telnet" "screen2_host" "screen1_host" IPSEC IPSEC
ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, PRE-SHARED,
"shared-secret") DESTINATION_SCREEN "screen1" ALLOW
```

- On Screen2:

```
1 "telnet" "screen2_host" "screen1_host"
IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, PRE-SHARED,
"shared-secret") SOURCE_SCREEN "screen2" ALLOW
2 "telnet" "screen1_host" "screen2_host"
IPSEC IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, PRE-SHARED,
"shared-secret") DESTINATION_SCREEN "screen2" ALLOW
```

3. Save and activate policy.

▼ To Use Windows 2000 to Communicate With Solaris SunScreen Using an IKE Pre-Shared Key

The following procedure describes how to configure IPSEC and IKE on a windows 2000 system.

1. **Start MMC console: start, run, and type mmc.**
   MMC console menu appears.
2. **Select Add/Remove snap-in (`Ctrl+m`).**
3. **Under Add/Remove snap-in window, click on Add.**
4. **Scroll down and select IP Security Policy Management, and click on Add.**
   The Select Computer window appears.
5. **In the Select Computer window, click Finish, then click Close to close the Add standalone snap-in window.**
6. **On the Add/Remove snap-in window, click OK to close it.**
   The original Console Root window reappears.
7. **In the Console Root window, select IP Security Policies on Local Machine.**
8. **Click the menu (right) mouse button to bring up a menu where you select Create IP Security Policy.**
   The IP Security Policy Wizard window appears.
9. **In the IP Security Policy Wizard window, click Next to continue.**
   The IP Security Policy Name window appears.
10. **In the IP Security Policy Name window, fill in the name of the policy you want, and click Next to continue.**
    The Request for Secure Communication appears.
11. **In the Request for Secure Communication window, click Next to continue.**
    The Default Response Rule Authentication Method window appears.
12. **In the Default Response Rule Authentication Method window, select Use this string ... and enter 'ABCEFGHI' in the field, and click Next, then click Finish.**
    The Mypolicy Properties with the Rules panel appears.

    Note – The pre-shared key used on SunScreen is 4142434445464748, hence on windows it maps to 'ABCEFGHI.'

    ---

13. **In the Mypolicy Properties window, click on Add.**

The Security Rule Wizard window appears.

14. **In the Security Rule Wizard window, click Next to continue.**
    The Tunnel Endpoint window appears.
15. **Do not change the Tunnel Endpoint window, except to click on Next to continue.**
    The Network Type window appears.
16. **Do not change the Network Type window, except to click on Next to continue.**
    The Authentication Method window appears.
17. **In the Authentication Method window, select Use this string ... and enter 'A' in the field, and click Next to continue.**
    The IP Filter List window appears.
18. **In the IP Filter List window, click Add to bring up the next window in which you enter the name of the filter.**
19. **Under the Name field, enter the name of the IP filter you want and click Add.**
    The IP Filter Wizard window appears. Click Next.
20. **In the IP Filter Wizard window, click Next to continue.**
    The IP Traffic Source window appears.
21. **Leave the IP Traffic Source window set to 'my IP address,' and click Next to continue.**
    The IP Traffic Destination window appears.
22. **In the IP Traffic Destination window, select a specific IP address from the pull-down menu and fill in the IP address of the host with which you want to establish a transport path, and click Next to continue.**
    The IP Protocol Type window appears.
23. **Do not change the IP Protocol Type window, except to click on Next to continue.**
24. **Then, in the IP Protocol Type window, click Finish.**
25. **Then, in the IP Protocol Type window, click Close.**
    The IP Filter List window appears with the filter you just added listed.
26. **In the IP Filter List window, enter the name of the IP filter you want and click Next to continue.**
    The Filter Action window appears.
27. **In the Filter Action window, select Require Security and click Next to continue.**
    The last window of the Security Rule Wizard appears. Click Next
28. **In this last window of the Security Rule Wizard, click Next to continue.**

The Mypolicy Properties window appears with both myfilter and Dynamic selected under the IP Filter List.

29. **In the Mypolicy Properties window, deselect Dynamic and click Close.**
    The original Console Root window appears.

30. **In the Console Root window, select the entry IP security on Local Machine showing on the left panel under the console root tree.**

31. **Select the mypolicy entry that shows in the right side of the window.**
    Right Click. And Select Assign. Now the policy will become assigned. On window 2K, only one policy can be assigned at one time.

    The above completes setting up an IPSEC policy on win2K, using IKE with pre-shared key 'A' to setup an transport mode protected path between win2K machine, and SunScreen protected machine.

▼ To Generate IKE Rules With Self-Generated Certificates

1. **Generate certificates or private keys on both Screens using** `ssadm certlocal`**:**

   a. **On Screen1:**

   ```
   # ssadm certlocal -Iks -m 512 -t rsa-md5 -D
   "C=US,O=YourOrg, CN=screen1_name"
   ```

   b. **On Screen2:**

   ```
   # ssadm certlocal -Iks -m 512 -t rsa-md5 -D
   "C=US,O=YourOrg, CN=screen2_name"
   ```

2. **Export the certificates to the other Screen.**

   a. **On Screen1:**

   ```
   # ssadm certdb -I -e "SUBJECT=C=US,
   O=YourOrg, CN=screen1_name" > /tmp/cert1
   ```

   b. **On Screen2:**

   ```
   # ssadm certdb -I -e "SUBJECT=C=US,
   O=YourOrg, CN=screen2_name" > /tmp/cert2
   ```

3. **Securely transport the file** `/tmp/cert1` **to the Screen1 and** `/tmp/cert2` **to Screen2.**

4. **Import the exported certificate to the Screen certificate database.**

   a. **On Screen2:**

   ```
   # ssadm certdb -I -a < /tmp/cert1
   ```

b. **On Screen1:**

```
# ssadm certdb -I -a < /tmp/cert2
```

5. **Add Certificate objects on both systems:**

```
> add certificate "screen1_cert" SINGLE IKE "C=US,
O=YourOrg,CN=screen1_name"
> add certificate "screen2_cert" SINGLE IKE "C=US,
O=YourOrg,CN=screen2_name"
```

6. **Mark the certificate you imported in Steps 3 and 4 as trusted on both systems using** `ssadm edit`**:**

a. **On Screen1:**

```
> add member certificate "IKE manually verified
certificates" "screen2_cert"
```

b. **On Screen 2:**

```
> add member certificate "IKE manually verified
certificates" "screen1_cert"
```

Note – The Group name "IKE manually verified certificates" is reserved for a trusted Certificate Group.

---

7. **Add Packet Filtering rules on both Screens.**

a. **On Screen1:**

```
1."telnet" "screen1_host" "screen2_host"
IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES,
"screen1_cert", "screen2_cert") ALLOW
2 "telnet" "screen2_host" "screen1_host"
IPSEC IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES,
"screen2_cert", "screen1_cert") ALLOW
```

b. **On Screen2:**

```
1."telnet" "screen2_host" "screen1_host"
IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES,
"screen2_cert", "screen1_cert") ALLOW
2 "telnet" "screen1_host" "screen2_host" IPSEC
IPSEC ESP("DES-CBC") IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES,
"screen1_cert", "screen2_cert") ALLOW
```

8. **Save and activate the policy.**

Refer to the man page of `ssadm-certlocal(1M)` and `ssadm-certdb(1M)` for more information.

▼ To Generate IKE Rules With Issued Certificates

1. **Generate keys and certificate requests on each Screen.**

   a. **On Screen1:**

   ```
   # ssadm certlocal -Ikc -m 512 -t rsa-md5 -D
   "C=US, O=YourOrg,CN=screen1_issued"
   ```

   b. **On Screen2:**

   ```
   # ssadm certlocal -Ikc -m 512 -t rsa-md5 -D
   "C=US, O=YourOrg,CN=screen2_issued"
   ```

2. **Bring the requests to a certificate server and have them signed. You receive three certificate files from the CA:**

   - screen1_issued.cert: screen1's cert
   - screen2_issued.cert: screen2's cert
   - root.cert: the CA's cert

   Further detailed instructions on this step depends on your certificate server.

3. **Securely transport the files to each machines under** `/tmp` **and import them. Import three certificates on each Screen:**

   ```
   # ssadm certdb -I -a < /tmp/screen1_issued.cert
   # ssadm certdb -I -a < /tmp/screen2_issued.cert
   # ssadm certdb -I -a < /tmp/root.cert
   ```

   In this example, assume you are using a certificate server with CA 's subject DN = "C=US, O=YourOrg.com, OU=sunscreen, CN=Certificate Manager".

4. **Add Certificate objects on each Screen and mark the root CA as trusted. On each Screen:**

   ```
   edit> add certificate root_cert SINGLE IKE "C=US,
   O=YourOrg.com, OU=sunscreen, CN=Certificate Manager"
   edit> add certificate screen2_issued_cert SINGLE IKE "C=US,
   O=YourOrg, CN=screen2_issued"
   edit> add certificate screen1_issued_cert SINGLE IKE
   "C=US, O=YourOrg, CN=screen1_issued"
   edit> add_member certificate "IKE root CA certificates" root_cert
   ```

   Note – The Group name "IKE root CA certificates" is reserved for a trusted Certificate Group.

   ---

5. **Add Packet Filtering rules on both Screens.**

   a. **On Screen1:**

   ```
   1."telnet" "screen1_host" "screen2_host" IPSEC ESP("DES-CBC")
   IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES, "screen1_issued_cert",
   "screen2_issued_cert") ALLOW
   ```

```
2 "telnet" "screen2_host" "screen1_host" IPSEC IPSEC ESP("DES-CBC")
IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES, "screen2_issued_cert",
"screen1_issued_cert") ALLOW
```

b. On Screen2:

```
1."telnet" "screen2_host" "screen1_host" IPSEC ESP("DES-CBC")
IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES, "screen1_issued_cert",
"screen2_issued_cert") ALLOW
2 "telnet" "screen1_host" "screen2_host" IPSEC IPSEC ESP("DES-CBC")
IKE("DES-CBC", "MD5", 2, RSA-SIGNATURES, "screen2_issued_cert",
"screen1_issued_cert") ALLOW
```

6. Save and activate the policy.

▼ To Install a Remote Administration Station Using IKE

These instruction apply to using SunScreen on a Solaris-based system only. Because the Solaris operating environment does not yet support IKE, there is no built-in facility for generating IKE certificates on a remote Administration Station. So, you must install the Screen packages as well as the administration packages on your system.

1. On the Screen

a. Install the full Screen software Create self-generated screen certificate using the GUI, or use the command line editor, as follows:

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D
"C=US, O=YOUR_ORG, CN=screen_name"
```

b. Export the Screen certificate to a file using the GUI, or the command line editor:

```
# ssadm certdb -Ie "C=US, O=YOUR_ORG,
CN=screen_name" > /tmp/screen_cert
```

c. Import Administration Station certificate using the GUI, or the command line editor and add the Certificate objects into the SunScreen configuration:

```
# ssadm certdb -Ia < /tmp/admin_cert
```

d. Mark the administrative certificate as trusted and edit the SunScreen policy for certificates.

```
# ssadm edit
edit> add certificate admin_cert SINGLE IKE
"C=US, O=YourOrg, CN=admin_name"
edit> add certificate screen_cert SINGLE IKE
"C=US, O=YourOrg, CN=screen_name"
edit> add member certificate "IKE manually verified certificates"
"admin_cert"
```

```
edit> add address admin_addr HOST
edit> add accessremote USER "admin" "admin_addr"
IPSEC ESP ("DES-CBC", "MD5") AH ("SHA1") IKE("DES-CBC", "MD5",
1, RSA-SIGNATURES, "screen_cert") PERMISSION ALL
SCREEN "screen_name"
edit> add screen "screen_name" ADMIN_IP
"admin_addr" IKE(screen_cert) RIP
```

Note – No packet filtering rule is required on the Screen.

---

e. **Save and activate policy.**

2. **On the Remote Administration Station**

   a. **Install the full Screen software**

   b. **Create a self-generated Screen Certificate:**

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D
"C=US, O=YOUR_ORG, CN=admin_name"
```

   c. **Export the Administration Certificate to a file using the GUI or use the command line editor as follows:**

```
# ssadm certdb -Ie "C=US, O=YOUR_ORG,
CN=admin_name" > /tmp/admin_cert
```

   d. **Import Screen Certificate using the GUI or command line editor:**

```
# ssadm certdb -I -a < /tmp/screen_cert
```

   e. **Edit the SunScreen policy for certificates:**

```
# ssadm edit
edit> add certificate admin_cert SINGLE IKE
"C=US, O=YourOrg, CN=admin_name"
edit> add member certificate "IKE manually verified certificates"
"admin_cert"
edit> add certificate screen_cert SINGLE IKE
"C=US, O=YourOrg, CN=screen_name"
edit> add address admin_addr HOST
edit> add address screen_addr HOST
```

   f. **Add a packet filter rule like the following:**

```
edit> add rule "remote administration" "admin_addr"
"admin_addr" IPSEC ESP("DES-CBC", "MD5") AH("SHA1") IKE("DES-CBC",
"MD5", 1, RSA-SIGNATURES, "admin_cert",
"screen_cert") ALLOW
```

   g. **Save and activate the policy.**

   Unless you have just done a fresh SunScreen install, clear the state and SADB using `ssadm lib/statetables -fs` on both systems.

Note – There is a problem on stealth Administration Stations using IKE where the compiler does not generate the IKE configuration, which forces you to manually create an IKE configuration file.

▼ To Create SKIP UDH Key and Certificates

Note – The SKIP command to run on the Administration Station is displayed at the end of the `AdminSetup.readme` file, which is found in the `/etc/sunscreen` directory. 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 use ftp to send the `AdminSetup.readme` file, which contains the `identitydb.obj` file, from the Screen to the Administration Station. This saves you the task of writing down the information that is required in the next procedure. To find information regarding creating SKIP UDH key and certificates, see "To Distribute the `identitydb.obj` File" in the *SunScreen 3.2 Administration Guide*.

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

   ```
   # skiplocal -i
   ```

2. **Create the SKIP UDH key and 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 SunScreen 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 3.2 software.

▼ To Load SKIP CA-Issued Private Key and Certificates

Note – The SKIP command to run on the Administration Station is displayed at the end of the `AdminSetup.readme` file, which is found in the `/etc/sunscreen` directory. 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 use ftp to send the `AdminSetup.readme` file, which contains the `identitydb.obj` file, from the Screen to the Administration Station. This saves you the task of writing down the information that is required in the next procedure. (See "To Distribute the `identitydb.obj` File" in *SunScreen 3.2 Administration Guide*.

For this procedure, you need your SKIP CA-Issued Private Key and Certificate diskette.

1. **Open a terminal window on your system and become root, if not already.**
2. **Load the required SKIP directories by typing:**

   ```
   # skiplocal -i
   ```

3. **Insert the SKIP CA-Issued Key and Certificate diskette into your system'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 SKIP CA-Issued 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 typing:**

   ```
   # skipif -a
   ```

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

   ```
   # sync; init 6
   ```

   The Administration Station's certificate ID has been installed. You next move to the Screen to install the SunScreen 3.2 software.

▼ To Complete the Installation When Using SKIP

To complete the installation when using SKIP for encryption, perform the following steps 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_ssadm_configure*

   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 User's Guide, Release 1.5.1* for more information on operating SunScreen 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 Screen 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 3.2 Administration Guide* for instructions on how to use the administration GUI.

Using IKE With SunScreen

The following information describes the IKE syntax and options as well as providing command line examples of policy rules that use IKE. You can also find administration GUI instructions for using IKE in the SunScreen 3.2 Administration Guide. Additionally, see the *SunScreen 3.2 Configuration Examples*manual for examples of using IKE for encryption.

IKE usage within SunScreen has three components:

- The authentication header (AH)
- The encryption header (ESP)

Note – Either the AH or ESP option can be omitted, but at least one must be present that has within it an authentication option (called a combined transform)

  In addition, the ESP header has within it an authentication option (called a combined transform).

- (Required) The IKE negotiation

  Possible combinations are:

  - IPSEC AH(`authalg1`) IKE(...)
  - IPSEC ESP(`encralg1`) IKE(...)
  - IPSEC ESP(`encralg1`, `authalg2`) IKE(...)
  - IPSEC AH(`authalg1`) ESP(`encralg1`) IKE(...)
  - IPSEC AH(`authalg1`) ESP(`encralg1`, `authalg2`) IKE(...)

Note – Unlike SKIP syntax, the IPsec and IKE parameter lists use parentheses to contain them.

The possible values for `authalgN` and `encralgN` are:

For `authalg`*:

- MD5
- SHA1

For `encralg`*:

- DES-CBC
- 3DES-CBC
- AES
- BLOWFISH
- NULL

The NULL algorithm is generally only used for testing because it exercises most of the normal code paths. However, it does not obscure the data; that is, NULL allows what is inside to be easily seen.

The `AH` and `ESP` options control the cryptographic means that are used to protect the DATA portions of network traffic. They are functional equivalents of the DATA and MAC algorithms used in SKIP.

The IKE option performs the functional equivalent of the rest of the options in SKIP, including the KEY algorithm and the naming of the certified cryptographic data to be used for configuring and securing the traffic.

APPENDIX **B**

Defining Security Policies

Once established, SunScreen controls access to the network through a set of rules and interface definitions that you create in the administration GUI. This appendix describes issues to consider before installing SunScreen. Included are directions and worksheets to help you analyze and define your company's security policy requirements. See the *SunScreen 3.2 Administrator's Overview* manual for more information. See the *SunScreen 3.2 Configuration Examples* document to better understand what you need to define for your security policy.

Topics covered include

Before installing SunScreen, review the *SunScreen 3.2 Release Notes* for the latest product information.

Determining Your Security Policy

Before installing the SunScreen software, determine your network security policy. For a more thorough discussion of this topic, read *Computer Security Policies and SunScreen Firewalls* by Kathryn M. Walker and Linda Croswhite Cavanaugh from Sun Microsystems Press, Prentice Hall, 1998, ISBN 0130960150. This book and additional resources are listed in the Preface.

General 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)?
- Do you need to use proxies?

Mapping Your Network Configuration

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

- Routers to the Internet
- FTP, WWW or TELNET servers
- Remote networks
- Internal subnetworks
- Your high availability (HA) configuration
- Proxy services you plan to run

The following figure is an example of various types of addresses that you can use as a reference when completing your own network map.

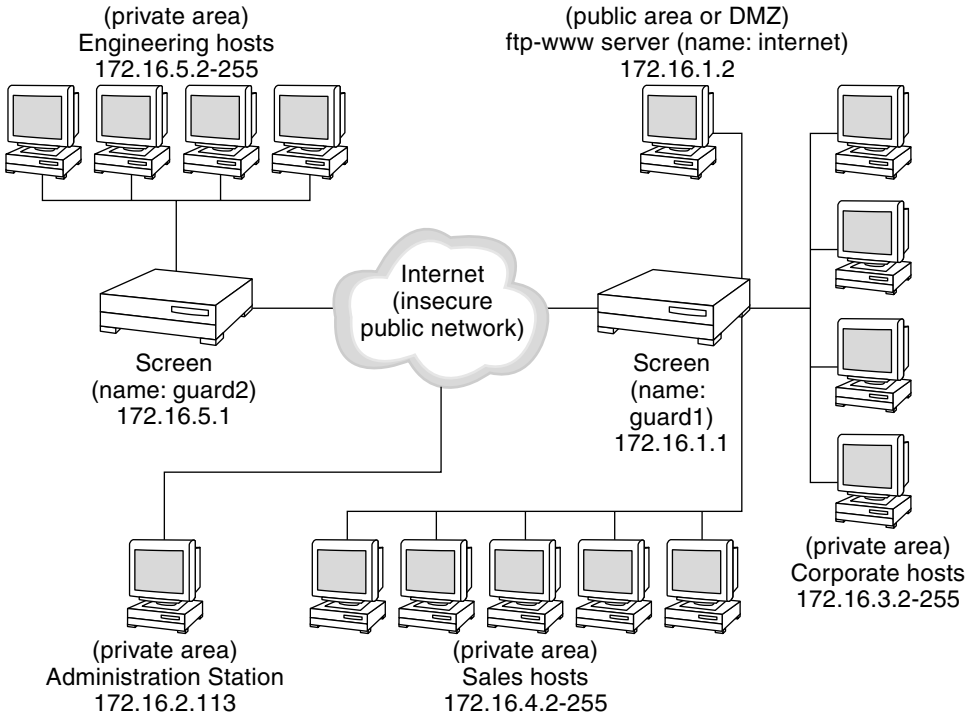


FIGURE B–1 Example of a Network Map

This figure includes the following examples of different types of addresses:

- 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 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.

Deciding on Your Initial Security Level

You must determine your initial level of security. There are three possible security levels when installing SunScreen in routing mode. (Installation in stealth mode automatically uses the Restrictive security level.) 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 use the administration GUI to change the rules to be more secure later.

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. Static routing and the naming service must be 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 standalone system and may depend on NIS, DNS, or NFS to function properly.
- Permissive - This level allows the same traffic as the Secure level. It 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 system that has multiple network interfaces and is acting as a router, or on a system that is acting as a server (for example, for NFS, NIS, or HTTP). Permissive is the default level.

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.

Interfaces

In routing mode, SunScreen automatically configures all plumbed interfaces to filter. In stealth mode, only the administrative port is plumbed and after installation, you must configure all filtering interfaces using the SunScreen administration GUI. Stealth interfaces must not be configured in the Solaris operating environment.

Once the following preparation criteria are met, continue to the appropriate chapter for your particular installation.

Worksheets for Defining Your Security Policy

This section contains directions and worksheets to help you analyze and define your security policy requirements.

See the *SunScreen 3.2 Administrator's Overview* manual for more information. You can also find useful examples in the *SunScreen 3.2 Configuration Examples*.

To begin the process, create a group of all the IP addresses of which the SunScreen software needs to be aware. SunScreen identifies network elements--network, subnetworks, and individual hosts--by IP address. Before you can define a rule, you must define all the elements or parts that make up the rule.

Addresses

The following types of addresses need to be defined in SunScreen:

- Host addresses
- Address ranges
- Address groups

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 filtering rules and NAT.

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

Use the following worksheets to help you organize your IP addresses. Reproduce them as necessary. Group the IP addresses and names for the following network elements:

- A single system, or a whole network or subnetwork
- Addresses (individual and network) grouped to form an address group

Host Addresses

Use the Host Addresses worksheet to list your host addresses. For individual elements, such as the router and individual systems, you need to know the IP address, in standard dotted Internet-address notation (w.x.y.z format), and the name of the host.

Name	Definition

Address Ranges

Use the Address Ranges worksheet to list your 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).

Name	Address	
	Beginning	Ending

Address Group

Use the Address Group worksheet to list your address group. 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 can be inclusive or exclusive or a combination of both, but cannot be cyclic, as in cases where address group A includes (references) address group B, which in turn includes address group A.

Name	Address	
	Include	Exclude

NAT

Network address translation (NAT) enables you to map from unregistered addresses to registered addresses allocated by your Internet service provider (ISP). The NAT function in 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. Using this approach with a small Class C network, which supports only 254 hosts (externally), you can use a private Class B network, which supports as many as 65,000 hosts or 255 networks of 254 hosts (internally).

The following worksheets include:

- NAT map
- Screen's interfaces
- Authorized users
- Administration Stations

NAT Map

Use the NAT Map worksheet to list type, address, and the translated address.

- Type, either static or dynamic
- Address, both source and destination
- Translated address, both source and destination

Type	Address		Translated Address	
Static Dynamic	Source	Destination	Source	Destination

Screen Interfaces

Use the Screen Interfaces worksheet to list:

- Type
- Interface name
- Group address
- Logging details, including SNMP alerts, logging, and ICMP rejects

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

Authorized Users

Use the Authorized Users worksheet to list:

- Name
- Authorized user
- Details

Name	Authorized User	Details

Administration Stations

Use the Administration Station Interface worksheet to list:

- Name of certificate associated with Administration Station
- Address of the Administration Station
- Key algorithm
- Data algorithm
- MAC algorithm
- Admin user name
- Access level

Name of Certificate Associated With Admin Station	Address of Admin Station	Key Algorithm	Data Algorithm	MAC Algorithm	Admin User Name	Access Level

Rules

You use rules to control access to your computer network and to control encryption for access to your data. In preparing to implement rules, you must determine:

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

---

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

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.

Following the Rules worksheet is a completed sample of a worksheet that includes the requisite services that you may want for a particular network.

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)

Ordered Rule Index	Service or Service Group	Source Address	Destination Address	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

The following shows the four action types: ALLOW, DENY, ENCRYPT, and SECURE.

- ALLOW options:
  - LOG_NONE
  - LOG_SUMMARY
  - LOG_DETAIL
  - SNMP_NONE
  - SNMP
  - A proxy type can be chosen if the service can be proxied by one of the SunScreen proxies.
- 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 system *only*)

    You must decide on:

    - Key Algorithm list
    - Data Algorithm list
  - 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
- Data Algorithm list
- MAC Algorithm list (NONE or MD5)

- Manual IPsec
  - Forward ESP
  - Forward AH
  - Reverse ESP
  - Reverse AH

Note – Forward and Reverse can be set the same or different. This is designated on the administration GUI by the Asymmetric and Symmetric options.

  - Transport or Tunnel Mode
  - Optional:
    - Source Screen (object)
    - Destination Screen (object)
    - Source Tunnel
    - Destination Tunnel
- Solaris IKE
  - ESP
  - AH
  - Encryption Algorithm
  - Hash Algorithm
  - Oakley Group
  - Authentication Method
  - Pre-Shared or Source Certificate
  - Destination Certificate
  - Transport or Tunnel Mode
  - Optional:
    - Source Screen (object)
    - Destination Screen (object)
    - Source Tunnel
    - Destination Tunnel

- VPN options:

This option is selected only when forming VPN rules using the previously defined VPN gateways.

After you define and map out your network and decide on your security policy, use data objects, such as services and addresses, to configure SunScreen with the policy rules to control access to your network. At installation, the SunScreen software automatically creates a policy named Initial that you can use to build your own security policies.

Additional information on creating security policies can be found at:
`http://www.sun.com/software/white-papers/wp-security-devsecpolicy/`