SunScreen SKIP User's Guide

For the Microsoft Windows 95 Operating Environment

Part No.: 805-0966-10
Revision A, March 1997

Contents

Preface

This manual is designed to help you understand how to install and manage the SunScreen™ SKIP software on your personal computer.

Who Should Use This Book

This guide contains instructions for anyone responsible for installing, maintaining, or using the SunScreen SKIP software. It also contains background information to help you get the most out of the features offered by the software. This manual assumes that you are familiar with TCP/IP networking concepts and with public-key and shared-key cryptography.

How This Book Is Organized

This manual is divided into the following chapters:

Chapter 1, "Introduction," presents an overview of the features, benefits, and functions of your SunScreen SKIP software.

Chapter 2, "Installing SunScreen SKIP," describes how to install the SunScreen SKIP software on a personal computer running the Windows 95 operating system, and how to add the SunScreen SKIP network service to your Network Control Panel, how to install or generate your private key and public certificate, and how to set your SunScreen SKIP password.

Chapter 3, "Configuring SunScreen SKIP," describes how to enter settings in the Network Control Panel and the SunScreen SKIP Access Manager application to use the SunScreen SKIP software.

Chapter 4, "Administering SunScreen SKIP," presents an overview of security considerations and tips for administering key disks and your SunScreen SKIP software.

Chapter 5, "Troubleshooting SunScreen SKIP," offers suggestions for resolving problems that may arise when using SunScreen SKIP.

Appendix A, "How SunScreen SKIP Works," describes how the components of SunScreen SKIP interact to provide access control, encryption/decryption services, and authentication.

Appendix B, "Changes to System Files," describes changes made to Windows system files and to the Windows 95 Registry when you install the SunScreen SKIP software.

The **Glossary** defines terms and concepts used in the SunScreen SKIP software.

Related Sources of Information

You may want to refer to the following sources for background information on cryptography or SKIP.

Applied Cryptography
Bruce Schneier, John Wiley & Sons, 1994.

Building Internet Firewalls
D. Brent Chapman and Elizabeth D. Zwicky
O'Reilly and Associates, 1995.

Internetworking with TCP/IP, 3rd Edition
Douglas E. Comer, Prentice Hall, 1994.

SKIP Home Page
`http://skip.incog.com/`

1

Introduction

SunScreen SKIP is a security software application for Windows 95 and the Microsoft TCP/IP stack that uses the SKIP (Simple Key Management for Internet Protocol) key management system to provide access control, authentication, and privacy. Any two hosts running SunScreen SKIP (or compatible SKIP implementations, such as SunScreen™ SPF-100, SunScreen™ EFS 1.0, or SKIP for Solaris) can encrypt IP network communications passing between them. By providing efficient transparent encryption of any protocol within the TCP/IP protocol suite, SunScreen SKIP lets computers communicate privately and securely over non-secure public networks.

Because SunScreen SKIP operates at the network level, it is transparent to applications exchanging information over TCP/IP networks, including FTP, Telnet, and Web browsers. Consequently, SunScreen SKIP provides network security without restricting user activity.

SunScreen SKIP uses a number of terms that may be unfamiliar to you. You may find it helpful to refer to the glossary on page 1 for brief definitions of unfamiliar terms. Refer to “How SunScreen SKIP Works” on page 1 for a more complete explanation of SunScreen SKIP concepts and functions.

1.1 Features and Benefits of SunScreen SKIP

SunScreen SKIP provides the following features and benefits:

- Access control based on host address or network to protect corporate data resources from unauthorized use.
- Automatic packet encryption and decryption using industry-standard DES, RC2, and RC4 algorithms to ensure the confidentiality of information sent over the network.
- Optional authentication using the keyed MD5 algorithm to verify the source and integrity of information transferred over a network.
- Key and certificate management to provide efficient, cost-effective administration of the basic building blocks of your security policy.
- Support for the Certificate Discovery protocol.
- Support for multiple name space identifiers.
- Compatible with SKIP-compliant security solutions, including SunScreen SPF-100, SunScreen EFS, and SKIP for Solaris.

1.2 Export-Controlled and Global Versions of SunScreen SKIP

The SunScreen SKIP software is available in export-controlled and global versions. The two versions are identical in function except for the following:

- Key length – The export-controlled version of SunScreen SKIP uses a 1024-bit key to encrypt and decrypt data. The global version of SunScreen SKIP uses a 512-bit key for data encryption/decryption.
- Traffic encryption algorithms – The export-controlled version of SunScreen SKIP supports the DES, RC2, and RC4 algorithms for traffic encryption. The global version of SunScreen SKIP supports the RC2 and RC4 algorithms for traffic encryption.

Note that, because the two versions of SunScreen SKIP use keys of different lengths, they cannot interoperate.

1.3 How SunScreen SKIP Works — An Overview

SunScreen SKIP uses a combination of public-key and shared-key cryptography to protect network communications. Public-key cryptography uses a pair of complementary keys (a private key and a public key) to encrypt and decrypt messages. Each SunScreen SKIP host has a unique private key and a certificate that contains the public key corresponding to that unique private key. SunScreen SKIP hosts (and other systems running SKIP-compatible applications) keep their private keys secret but distribute their certificates to each other freely to exchange their public key values.

A SunScreen SKIP host uses its own private key value and the public key value of a remote host to calculate a *shared secret*, which only those two hosts know. This shared secret, which is computed using the Diffie-Hellman algorithm, is implicit, and is never communicated over the network.

When a SunScreen SKIP host wants to send a secure message to another host, it calculates a *session key* based on the shared secret known only to the two hosts and the current time/date. The host breaks the message into pieces (packets) and encrypts the data in each packet with a randomly generated *traffic key.* The sending host then uses the session key to encrypt the traffic key. Finally, SunScreen SKIP formats each packet with an IP header (which allows the packet to be routed to its destination), a SKIP header that identifies the encryption algorithms being used, the traffic key encrypted with the session key, and the message data encrypted with the traffic key.

When the destination host receives the packet, it finds the sender's certificate and retrieves or calculates their mutual shared secret. The destination host then calculates the same session key using the shared secret and the time/date provided by its system clock. The destination host uses the session key to decrypt and store the traffic key contained in each packet. The destination host then uses the traffic key to decrypt the message data. Finally, it compiles the packet data together to obtain the original message.

SunScreen SKIP changes the traffic key every 30 seconds or after a key has been used to encrypt 512K of data during a connection. SunScreen SKIP does this to prevent an unauthorized user from analyzing captured network traffic to calculate individual traffic keys.

After you install the SunScreen SKIP software on your computer, you set up an access control list, which specifies the hosts with which your computer is allowed to communicate. If you want to communicate securely with another host, which can be another SunScreen SKIP host or a SKIP-compliant device such as a SunScreen EFS, you install (or discover over the network) the remote host's certificate (and public key), and you specify how SunScreen SKIP should encrypt and authenticate messages to the host.

You can add hosts with which you want to communicate without encryption (in the clear) to your access control list. For example, you can identify the name servers, mail servers, proxy servers, authentication servers, and other hosts for which encrypted communications would not be appropriate. Similarly, you can specify that a designated host cannot communicate with your computer.

2

Installing SunScreen SKIP

Installing the SunScreen SKIP software on your computer consists of three activities:

- Copying the SunScreen SKIP software from a CD-ROM or network drive to your computer.
- Setting your SunScreen SKIP password.
- Adding your private key and its corresponding public certificate.

Each of these activities is described in the following sections.

2.1 Copying the SunScreen SKIP Software to Your Computer

Before you install the SunScreen SKIP software, you should identify the installation directory and the program folder you want the installation program to use. By default, the SunScreen SKIP files are installed in the *`C:\Program Files\SUNW`* directory.

1. **Insert the SunScreen SKIP CD-ROM into the CD-ROM drive.**
   If you want to copy the SunScreen SKIP software from a network drive, mount the drive you will use.

2. **Double-click the** *`setup.exe`* **icon to run the SunScreen SKIP installation program.**

3. **Click Next to step through the installation screens, answering each question as it appears.**
   The installation program copies files from the CD-ROM or network drive to your computer and enters information into system files.

2.2 Configuring the SunScreen SKIP Network Service

The SKIP Security for TCP/IP service is automatically added to the Network Control Panel when you install the SunScreen SKIP software. After you install SunScreen SKIP, you must set your SunScreen SKIP password and operating settings and add or generate your private key (and its corresponding public certificate). Each type of information is described in the following sections.

2.2.1 To Set Your SunScreen SKIP Password

Your SunScreen SKIP password prevents an unauthorized user from displaying your SunScreen SKIP settings or modifying your access control list. The SunScreen SKIP software asks you to enter this password whenever you enable SunScreen SKIP or make changes to your SunScreen SKIP settings.

You must set your SunScreen SKIP password before you can add certificates or run the SunScreen SKIP Access Manager. You can change your SunScreen SKIP password at any time. Setting your password automatically logs you in to the SunScreen SKIP Key Manager.

To set your SunScreen SKIP password:

1. **Open the Network Control Panel.**

2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network components list and click Properties.

3. **Click the General tab.**
   The General Properties page (Figure 2-1) opens.

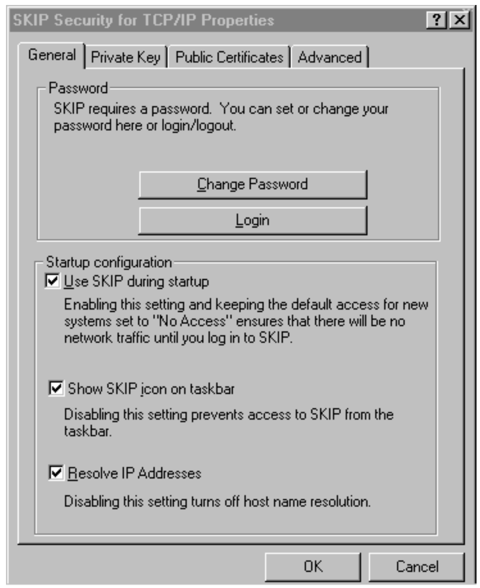

Figure 2-1 General Property Page

4. **Click Set Password.**
   If you are updating an existing password, click Change Password.

   The Set Password dialog box (Figure 2-2) opens.

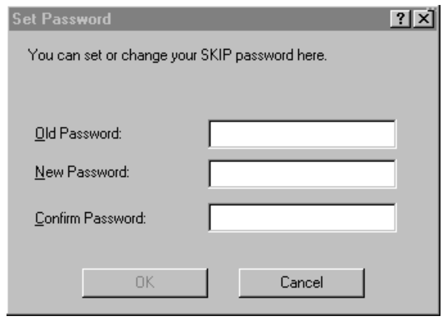

Figure 2-2 Set Password Dialog Box

5. **If you are changing your password, enter your current SunScreen SKIP password in the Old Password text field.**

6. **Enter your new SunScreen SKIP password in the New Password text field.**
   Passwords can be as many as 15 alphanumeric characters long. Passwords are case-sensitive.

7. **Enter the new SunScreen SKIP password again in the Confirm Password text field.**
   The password you enter in the Confirm Password text field must exactly match the password you entered in the New Password field.

8. **Click OK to save your changes and close the Properties panel.**

2.2.2 To Configure Operating Settings

1. **Open the Network Control Panel.**

2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list (Figure 2-3) and click Properties.

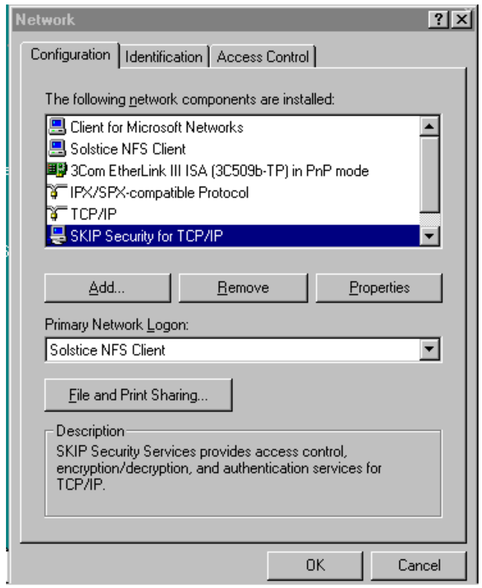

Figure 2-3 Network Control Panel – SKIP Security for TCP/IP Selected

3. **Click the General tab (Figure 2-1 on page 3).**

4. **If you want your computer to use its default SunScreen SKIP access setting until SunScreen SKIP is running, enable the Use SunScreen SKIP During Startup check box.**
   When your computer is turned on, it runs a series of diagnostics and startup routines. During this startup sequence, your computer can send and receive network traffic in the clear.

   - If you want your computer to use the default SunScreen SKIP access method (No Access, Ask for Confirmation, or Add Automatically) for network traffic until the SunScreen SKIP software is available to control host access, click the Use SunScreen SKIP During Startup check box.

- If you want your computer to accept network traffic during the startup sequence, clear the Use SunScreen SKIP During Startup check box.

See “To Configure the Default Host Access” on page 3 for information on setting the default SunScreen SKIP access method.

5. **If you want to display the SunScreen SKIP icon on your taskbar, select Show SunScreen SKIP Icon On Taskbar.** You can add the SunScreen SKIP icon to the Windows 95 taskbar to simplify running SunScreen SKIP Access Manager. You can double-click the SunScreen SKIP icon to run the SunScreen SKIP Access Manager application.

   If you do not want the SunScreen SKIP icon to appear on the taskbar, clear the Show SunScreen SKIP Icon On Taskbar check box. If the program icon does not appear in the taskbar, you can open the SunScreen SKIP Access Manager dialog box by running *SUNWSKIP.EXE* and double-clicking the SunScreen SKIP icon.

6. **If you want SunScreen SKIP to resolve host names to IP addresses, click Resolve IP Addresses.** If you do not use name services such as DNS or if you do not want SunScreen SKIP to resolve IP addresses, clear the Resolve IP Addresses check box.

7. **When you are finished, click OK to save your changes and close the Properties panel.**

2.3 Adding Your Private Key/Public Certificate

You must have a private key (and the certificate containing your corresponding public key) before you can exchange secure communications with other SKIP hosts. You can obtain a private key and a signed public certificate by installing it from a SunCA key diskette. Alternatively, you can generate a private key (and an unsigned certificate).

Note—Contact your Sun sales representative for information on purchasing signed Diffie-Hellman certificates.

You need a signed certificate to communicate with hosts using signed certificates, and you need an unsigned certificate to communicate with hosts using unsigned certificates. Your certificate must have a key with the same length as the key in the remote host's certificate.

If you install a signed certificate, you can assign it an alternative name space in order to provide yourself with an additional measure of security. See "Adding an Alternative Name Space for a Signed Certificate" on page 5 for more information on creating an alternate name space identifier for a signed Diffie-Hellman certificate.

2.3.1 To Install A Private Key/Public Certificate

1. **Insert the SKIP Key &Certificate diskette containing your private key in your diskette drive.**
2. **Run SunScreen SKIP Access Manager by double-clicking the SunScreen SKIP taskbar icon.**
   When the login dialog appears, enter your SunScreen SKIP access password and click OK.
3. **Open the Network Control Panel.**
4. **Open the Properties panel for the SunScreen SKIP Virtual Adapter.**
   Select the SunScreen SKIP Virtual Adapter entry in the network component list and click Properties.
5. **Click the Private Key tab.**
   The Private Key property page (Figure 2-4) opens.

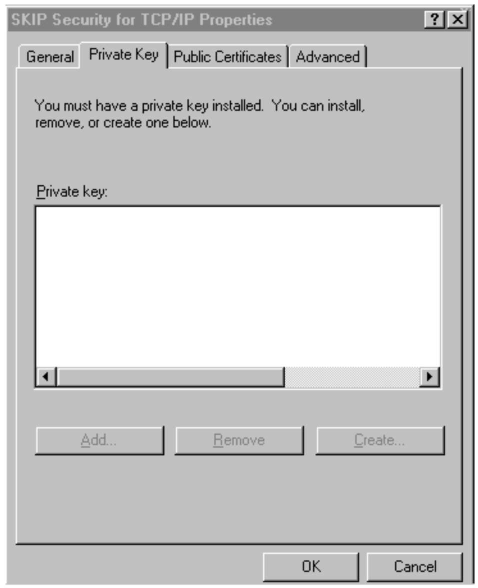

Figure 2-4 Private Key Property Page

6. **Click Add.**
   The File Open dialog box opens.

7. **Select the key you want to add for yourself and click Open.**
   Private keys have file names ending in `.key`; for example, `0a000123.key`.

8. **In the Private Key Information dialog box, enter a description for your key.**
   The description should consist of your name or other information indicating you are using the key (and its corresponding certificate).

9. **Use the Name Space drop-down list to select the name space you want to use.**
   - IPv4 Address – The 8-digit hexadecimal number used as the Distinguished Name in your signed public certificate.

- MD5 (DH Pub. Value) – The 16-digit MD5 hash value of your public key.

10. **Click OK.**
    The Private Key Information dialog box closes and the new private key appears in the Private Key list.

Note—An entry for the public certificate that corresponds to your private key appears in the Public Certificates list.

11. **Click OK to save your changes and close the Properties panel.**

12. **Remove your SKIP Key & Certificate diskette and store it in a secure location.**
    You must keep your SKIP Key + Certificate diskette in a physically secure location.

13. **Restart your computer.**

2.3.2 To Generate A Private Key/Public Certificate

As an alternative to installing a signed public certificate/private key, SunScreen SKIP lets you generate your own unsigned Diffie-Hellman (UDH) certificate and private key.

1. **Open the Network Control Panel.**

2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and click Properties.

3. **If you have not logged in to the SunScreen SKIP Key Manager, click the General tab, click Log In, enter your SunScreen SKIP password, and click OK.**

4. **Click the Private Key tab.**
   The Private Key property page (Figure 2-4 on page 8) opens.

5. **Click Create.**
   The Create Private Key dialog box (Figure 2-5) opens.

Figure 2-5 Create Private Key Dialog Box

6. **Type a description for your key in the Create Private Key dialog box.**
7. **Click OK to create your private key and unsigned Diffie-Hellman certificate.**
8. **Click OK to save your changes and close the Properties panel.**

2.3.3 To Delete Your Private Key

Because you can have only one private key at a time, you must delete the current key before you add a new private key. You will need to delete your private key if it expires, if you want to change computers, or if you are issued a new key.

SunScreen SKIP Access Manager deletes your password and clears its key cache when you delete your private key. Consequently, you must enter a new password before you can install a new private key, and all hosts with which you exchange secure communications must delete your old public certificate and install or discover your new public certificate.

When you replace your private key, all shared secrets calculated with your old key are invalid. Consequently, you should clear your SunScreen SKIP cache after you replace your private key. See "To Clear the SunScreen SKIP Key Cache" on page 6 for more information.

1. **Open the Network Control Panel.**
2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and click Properties.
3. **If you have not logged in to the SunScreen SKIP Key Manager, click the General tab, click Log In, enter your SunScreen SKIP password, and click OK.**
4. **Click the Private Key tab.**
5. **Click the entry for the private key currently installed on your system.**
6. **Click Remove.**
7. **Click OK to save your changes and close the Properties panel.**

3

Configuring SunScreen SKIP

After you have installed the SunScreen SKIP software and added your password and private key, you are ready to identify the remote hosts with which you want to communicate securely.

3.1 Using SunScreen SKIP Access Manager

You use the SunScreen SKIP Access Manager application to configure your SunScreen SKIP access control list, which identifies the hosts with which you want to exchange encrypted or unencrypted network communications. SunScreen SKIP Access Manager runs in the background automatically when you start your computer. You access the SunScreen SKIP Access Manager dialog box (Figure 3-1) by clicking the SunScreen SKIP icon on the Windows 95 taskbar.

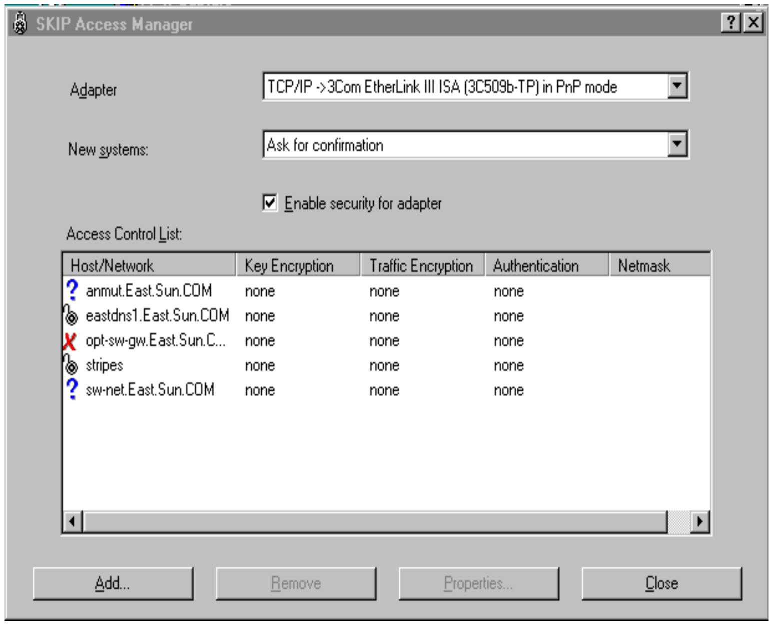

Figure 3-1 SunScreen SKIP Access Manager Dialog Box

3.1.1 To Enable SunScreen SKIP Security

You can enable or disable SKIP security selectively for each network interface on your computer. To enable or disable SKIP security for a network interface:

1. **Open the SunScreen SKIP Access Manager dialog box.**
   - If the SunScreen SKIP icon appears on the Windows 95 taskbar, double-click it.
   - If the SunScreen SKIP icon does not appear on the Windows 95 taskbar, run `SUNWSKIP.EXE` and then double-click the SunScreen SKIP icon.

2. **If you have more than one network interface, use the Adapter list to select the interface for which you want to enable or disable SunScreen SKIP.**

3. **Select or clear the SKIP Enabled check box to enable or disable SunScreen SKIP security.**

4. **When the SunScreen SKIP Login dialog box opens, enter your SunScreen SKIP password in the Password field and click OK.**

5. **Close the SunScreen SKIP Access Manager dialog box.**

3.1.2 To Configure the Default Host Access

You can configure SunScreen SKIP settings for each network interface you maintain on your computer. For example, if you are configuring SunScreen SKIP on a portable computer with Ethernet and serial interfaces, you can set up SunScreen SKIP settings separately for each interface.

1. **Open the SunScreen SKIP Access Manager dialog box.**
   - If the SunScreen SKIP icon appears on the Windows 95 taskbar, double-click it.
   - If the SunScreen SKIP icon does not appear on the Windows 95 taskbar, run *`SUNWSKIP.EXE`* and then double-click the SunScreen SKIP icon.

2. **Select the network interface for which you want to configure SunScreen SKIP.**
   SunScreen SKIP maintains a separate configuration for each network interface on your computer. Use the Adapter list to select the network interface you want to configure.

3. **Specify whether unknown systems can exchange network traffic with your computer.**
   Depending on security policies at your location, you can configure SunScreen SKIP to accept or refuse traffic from hosts that are not in your access control list. Use the New Systems list to specify how SunScreen SKIP should respond to communications from unauthorized hosts. You can choose one of the following:

   - No Access – Your computer refuses connections from the unknown host. The icon for hosts without access is a red X.

- Ask for Confirmation – Your computer refuses connections from the unknown host until you indicate whether connections from the unknown host should be accepted. The icon for hosts awaiting confirmation is a blue question mark.
- Add Automatically – Your computer adds the unknown host to your access control list and accepts connections from the newly added host. The icon for hosts with access is a open lock.

The icon for a host added to your access control list automatically is displayed with a plus sign (+) beside it.

4. **Close the SunScreen SKIP Access Manager dialog box.**

3.1.3 Maintaining Your Access Control List

You add hosts to your access control list to specify the hosts with which you want to exchange encrypted traffic and to identify the algorithms and settings you want to use to communicate. If you want to communicate securely with another host, you can choose SKIP security or SunScreen compatibility (which is an older version of the SKIP protocol).

If you want to communicate with a host without encryption or authentication, you must add the host to your access control list with Clear Access. For example, you should set up access control list entries for any servers you use, such as authorization servers, mail servers, or proxy servers. If you do not want to communicate with a host, you must add the host with Access Denied access.

You can add network numbers to your access control list if you want to communicate in the clear with all hosts on a particular subnetwork (or deny access to all hosts on the subnetwork).

To Add a SKIP Host to Your Access Control List

You must configure a remote host for SKIP communication before you can exchange encrypted traffic with that host. If you are not using certificate discovery, you must add the remote host's Diffie-Hellman certificate before you add the remote host to your access control list.

1. **Open the SunScreen SKIP Access Manager dialog box.**
   - If the SunScreen SKIP icon appears on the Windows 95 taskbar, double-click it.
   - If the SunScreen SKIP icon does not appear on the Windows 95 taskbar, run *`SUNWSKIP.EXE`* and then double-click the SunScreen SKIP icon.

2. **Click the Add button to open the Configure Access dialog box (Figure 3-2).**

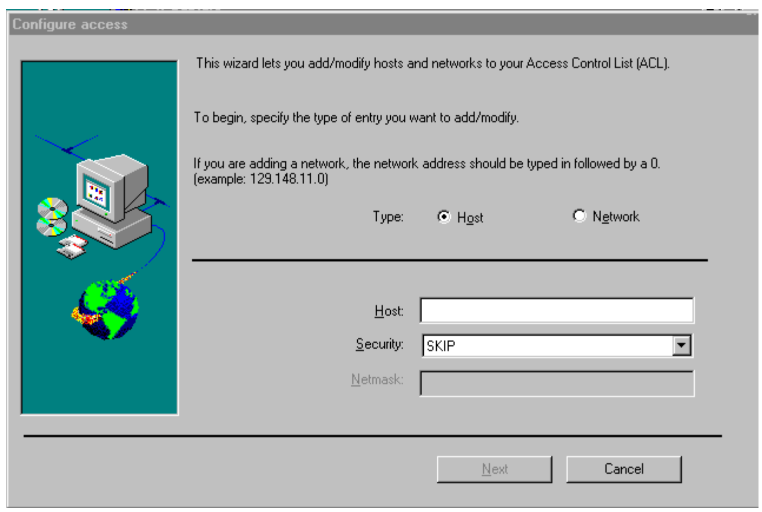

Figure 3-2 Configure Access Dialog Box

3. **Click Host to indicate you want to add a host to your access control list.**

4. **Enter the name or IP address of the host you want to add in the Host field.**
   If you enter a host name, your computer contacts your nameserver to resolve the name to an IP address. Note that you must have enabled the "Resolve IP Addresses" setting in the General panel (Step 6 on page 6) for SunScreen SKIP to resolve host names.

5. **Choose SKIP from the Security list to specify that you want to use SKIP security to communicate with the remote host.**

6. **Click Next.**
   The Add Host dialog box (Figure 3-3) opens.

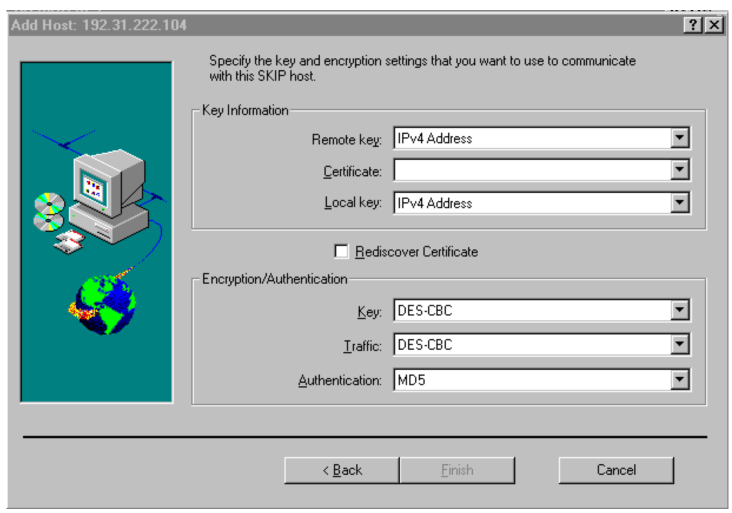

Figure 3-3 Add Host Dialog Box – SKIP

7. **Use the Remote Key ID list to select the name space used to identify the certificate for the remote host.**
   You can choose IPv4 Address or MD5/UDH.

8. **Select the public certificate associated with the host.**

- If the certificate for the remote host is installed on your computer, use the Certificate list to select the certificate you want.
- If the certificate for the remote host is not installed and if certificate discovery is enabled, enter the identifier of the certificate in the Certificate list box. SunScreen SKIP will then contact the remote host to obtain the identified certificate over the network.

  You can enter dashes (-) in an MD5-UDH certificate identifier to make the certificate name more readable.

9. **Use the Local Key ID list to select the name space used to identify the certificate on your computer.**
   You can choose IPv4 Address or MD5/UDH. The setting you choose must match the setting being used by the remote host.

10. **Use the Key Encryption list to select the algorithm you want to use to encrypt traffic keys between your computer and the remote host.**
    You can choose DES-CBC or RC2-40 as the key encryption algorithm. The setting you choose must match the setting being used by the remote host.

11. **Use the Traffic Encryption list to select the algorithm you want to use to encrypt traffic between your computer and the remote host.**
    You can choose DES-CBC (export-controlled version only), RC2-40, or RC4-40 as the traffic encryption algorithm. You can choose None if you want network traffic to be authenticated but not encrypted. The setting you choose must match the setting being used by the remote host.

12. **Use the Authentication list to specify whether you want traffic keys to be authenticated.**
    Choose MD5 to authenticate traffic keys or <none> to turn off keys authentication. The setting you choose must match the setting being used by the remote host.

13. **Click Finish.**

To Add a Network to Your Access Control List

You can add a network (or subnetwork) to your access control list to permit or refuse cleartext access between hosts on that network and your computer. When you add a network to your ACL, you specify whether hosts on that network can exchange cleartext communication with your computer. After you set access controls for a network, you can override those controls for specific hosts on the network by adding an entry for that host to your access control list.

1. **Run SunScreen SKIP Access Manager.**

2. **Click Add to open the Configure Access dialog box.**

3. **Click Network to indicate you want to add a network to your access control list.**
   The fields on the Configure Access dialog box (Figure 3-4) change to let you enter network information.

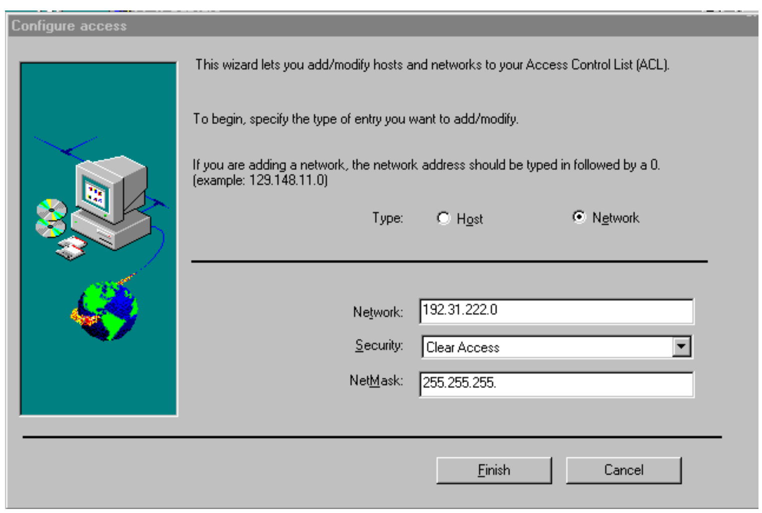

Figure 3-4 Configure Access Dialog Box – Network

4. **Enter the IP address of the network or subnet in the Network field.**
   For example, you would enter `192.33.222.` or `192.33.222.0` to indicate that all hosts on the 192.33.222.0 network should be given or denied access.

5. **Specify whether hosts on the specified network can access your computer by choosing Clear Access or Access Denied from the Security list.**

6. **Enter the subnet mask for the network IP address in the Netmask text field.**
   For example, you would enter `255.255.255.0` to indicate that you are communicating over a Class C IP network.

7. **Click Finish.**

To Add a SunScreen SPF-100 to Your Access Control List

Sun Microsystems offers a security product called SunScreen SPF-100 that uses an earlier version of the SKIP protocol. A host running SunScreen SKIP can communicate through a SunScreen SPF-100, provided both hosts have the proper certificates installed. Depending on your network requirements, you can configure two hosts running SunScreen SKIP to use SunScreen security to communicate securely.

Note—You must have a signed Diffie-Hellman certificate to communicate with a SunScreen SPF-100 (or a host using SunScreen security). The SunScreen SPF-100 does not support certificate discovery.

To add a SunScreen to the SKIP access control list:

1. **Run SunScreen SKIP Access Manager.**

2. **Click Add to open the Configure Access dialog box.**

3. **Click Host.**

4. **Enter the name or IP address of the remote host in the Host field.**
   Do not enter the name or IP address of the SunScreen SPF-100.

5. **Select SunScreen Compatibility from the Security list.**

6. **Click Next.**
   The Add Host dialog box for Sunscreen hosts (Figure 3-5) opens.

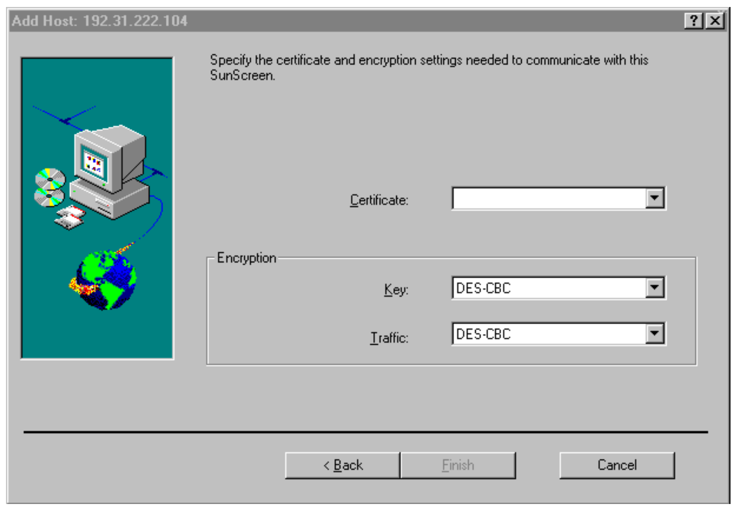

Figure 3-5 Add Host Dialog Box – SunScreen

7. **Use the Certificate list to select the public certificate that belongs to the SunScreen.**

8. **Use the Key list to select the algorithm you want to use to encrypt traffic keys traveling between your computer and the remote SunScreen.**
   You can choose DES-CBC or RC2-40 as the key encryption algorithm. This setting must match the setting entered on the SunScreen SPF-100.

9. **Use the Traffic list to select the algorithm you want to use to encrypt packets between your computer and the remote SunScreen.**
   You can choose DES-CBC (export-controlled version only), RC2-40, or RC4-40 as the traffic encryption algorithm.

   This setting must match the setting entered on the SunScreen SPF-100.

10. **Click Finish.**
    After you configure SunScreen SKIP to communicate with a SunScreen SPF-100, you must configure the SunScreen SPF-100 to communicate with your computer. See "SunScreen SPF-100" on page 7 for information on how to configure a SunScreen SPF-100 to communicate with a computer running SunScreen SKIP.

3.2 Maintaining Public Certificates

Public certificates contain the Diffie-Hellman public key for remote hosts with which you exchange encrypted messages. You must have a public certificate for a remote host before you can add that host to your access control list. You can either install a public certificate from a diskette or discover (retrieve) a certificate from a remote host over a network.

Note—You must install a signed certificate to communicate with a SunScreen SPF-100. You must install a SunCA global certificate to communicate with a SunScreen SPF-100 G.

3.2.1 To Install a Public Certificate

1. **Insert the diskette containing the public certificate in your diskette drive.**

2. **Open the Network Control Panel.**

3. **Select the SKIP Security for TCP/IP entry in the network component list and click Properties.**

4. **In the Properties page for the SunScreen SKIP network service, click the Public Certificates tab.**
   The Public Certificates property page (Figure 3-6) opens.

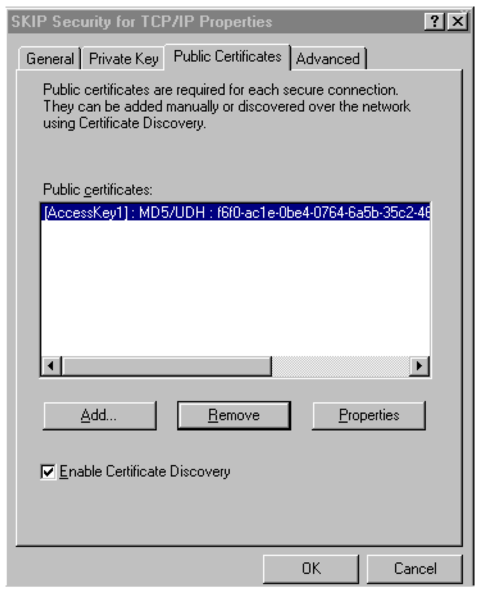

Figure 3-6 Public Certificates Property Page

5. **Click Add.**

6. **Use the Open File dialog box to select the public certificate you want to add. Click Open.**

7. **When the Public Certificate Information dialog box (Figure 3-7) opens, enter a description of the certificate you are adding.**
   For example, you might enter the name of the remote user associated with the public certificate to simplify maintenance of your access control list.

Figure 3-7 Public Certificate Information Dialog Box

8. **Use the Name Space list to specify the type of identifier you want to use to communicate with the remote host:**
   - IPv4 Address – Use the Class A IP address specified as the Distinguished Name in the certificate to identify the public certificate.
   - MD5 (DH Pub. Value) – Use the MD5 hash value of the remote host's public key to identify the public certificate.

9. **Click OK.**
   The Private Key Information dialog box closes and the new public certificate appears in the Public Certificates list on the Public Certificates tab.

10. **Click OK to save your changes and close the Properties panel.**

3.2.2 *To Enable Certificate Discovery*

1. **Open the Network Control Panel.**

2. **Select the SKIP Security for TCP/IP entry in the network services list and click Properties.**

3. **In the Properties page for the SunScreen SKIP network service, click the Public Certificates tab.**

4. **When the Public Certificates property page (Figure 3-6 on page 12) opens, use the Enable Certificate Discovery check box to enable or disable certificate discovery.**

5. **Click OK to save your changes and close the Properties panel.**

3.2.3 To Display the Contents of a Public Certificate

You can display a summary of the contents of any of the public certificates stored in SunScreen SKIP's cache, including your own.

1. **Open the Network Control Panel.**

2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and click Properties.

3. **Click the Public Certificates tab.**

4. **Click the entry and then click Properties or double-click the entry for the public certificate you want to display.**
   The Certificate Contents window lists information about the public certificate, such as its public key and its expiration date.

5. **When you are finished, click OK.**

3.2.4 To Delete a Public Certificate

1. **Open the Network Control Panel.**

2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and click Properties.

3. **Click the Public Certificates tab.**

4. **Click the certificate you want to delete from the Public Certificates list.**

5. **Click Remove.**

6. **When you are finished, click OK to save your changes and close the Properties panel.**

4

Administering SunScreen SKIP

4.1 General Security Notes

- Computer security begins with physical security. An unauthorized user who has physical access to a computer you want to protect can modify or delete files, including files needed by the SunScreen SKIP software.
- SunScreen SKIP encrypts only TCP/IP traffic. Other protocols, such as NetBEUI or IPX, are not encrypted.
- Users should be discouraged from selecting the Add Automatically option for default host connection attempts.
- Users requiring high levels of security must balance performance against security. Strong encryption algorithms, such as DES-CBC, may be somewhat slower, but they offer much stronger levels of protection.

4.2 Administering Key Diskettes

At sites using signed Diffie-Hellman certificates, each user must install a private key in order to exchange encrypted traffic with other hosts. The diskettes on which these keys are delivered must be secured at all times, since an unauthorized user with access to a key diskette can pretend to be the key's rightful owner.

You should examine each key package you receive to verify that it is sealed. If the seal is broken, the private key may have been copied or compromised. If you believe that a private key may have been copied, do not issue the key package and contact the certification authority.

Key packages issued by SunCA, Sun's certification authority, contain two diskettes:

- The SKIP Key & Certificate diskette contains the user's Diffie-Hellman private key in clear text. This diskette must be kept physically secure when it is not being used. This diskette should never be given to anyone other than its assigned user to avoid compromising SKIP security protection.

  The Key-and-Certificate diskette contains 10 files:

  - `<Key-ID>.crt` – For example, `0a0002a1.crt`. This file contains your certified Diffie-Hellman public key in the form of an X.509 certificate signed using an RSA signature.
  - `<Key-ID>.dsa` – Identical to the `<Key-ID>.crt` file, except that it is signed using a DSA signature.
  - `dh.crt` – This file is identical to the `<Key-ID>.crt` file.
  - `<Key-ID>.key` – For example, `0a0002a1.key`. This file contains your Diffie-Hellman private key in clear text.
  - `dh.key` – This file is identical to the `<Key-ID>.key` file.
  - `dh_param` – This file contains the Diffie-Hellman g and p parameters.
  - `secret_i` – This file contains your private value (that is, i in $g^i \; mod \; p$).
  - `sunicg_c` – This file contains SunCA's (the issuing Certification Authority) self-signed certificate using RSA.
  - `sunicg.dsa` – This file contains SunCA's (the issuing Certification Authority) self-signed certificate using DSA.
  - `icg_keys.sh` – This file contains a UNIX SHELL script used for installing the `dh_param` and `sunicg_c` files for your SunScreen SKIP software. Consult Technical Support before using this file.

- The Public Certificate diskette contains two files:
  - `<Key-ID>.crt` contains your certified Diffie-Hellman public key in the form of an X.509 certificate, signed using RSA. This file is identical to the `<Key-ID>.crt` file on the SKIP Key & Certificate diskette.
  - `<Key-ID>.dsa` – Identical to the `<Key-ID>.crt` file, except that it is signed using the DSA digital signature algorithm. This file is identical to the `<Key-ID>.dsa` file on the SKIP Key & Certificate diskette.

You can copy the Public Certificate diskette to distribute your public certificate to other SKIP users.

4.3 *Adding the SunScreen SKIP Network Service*

1. Open the Network Control Panel (Figure 4-1).

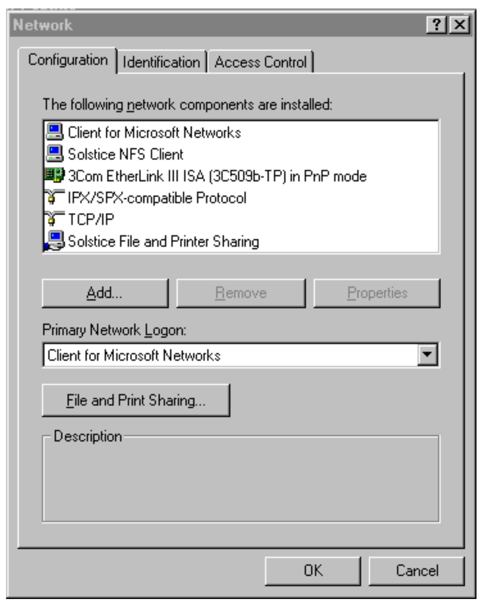

Figure 4-1 Network Control Panel

2. **Click Add. When the Select Network Component Type dialog box (Figure 4-2) opens, select Service and then click Add.**

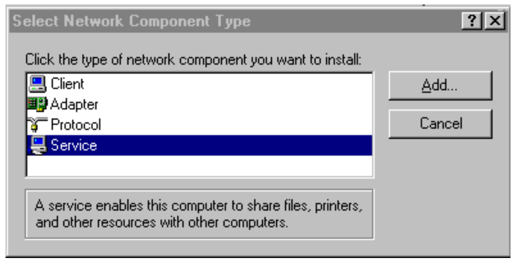

Figure 4-2 Select Network Component Type Dialog Box

3. **When the Select Network Service dialog box (Figure 4-3) opens, select SunSoft from the Manufacturers list. Select SKIP Security for TCP/IP from the Network Service List.**

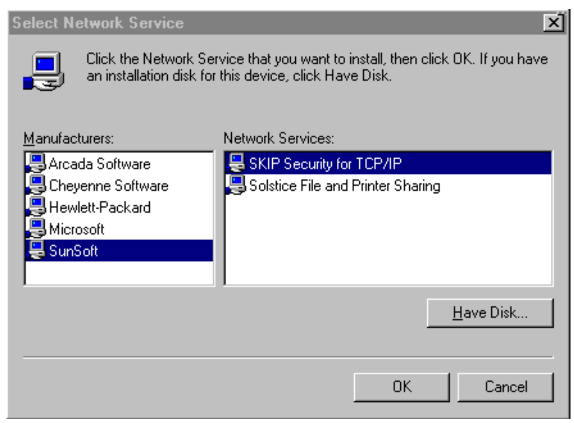

Figure 4-3 Select Network Service Dialog Box

4. **Click OK to close the Select Network Service dialog box. Click OK again to close the Network Control Panel.**

4.4 Adding an Alternative Name Space for a Signed Certificate

If you have installed a signed Diffie-Hellman certificate for yourself, you can create an alternate name space for your public certificate. Adding an additional name space for your public certificate lets you identify it in one way to one group of users and in another way to a different group of users, which increases your security.

1. **Open the Network Control Panel.**
2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and click Properties.
3. **If you have not logged in to the SunScreen SKIP Key Manager, click the General tab, click Log In, enter your SunScreen SKIP password, and click OK.**
4. **Click the Private Key tab.**
5. **Click the entry for the private key you installed previously.**
6. **Click Create.**
7. **Enter a description for the selected key in the Create Private Key dialog box.**
8. **Click OK to close the Create Private Key dialog box.**
   The alternate name for your private key/public certificate appears in the list of private keys.
9. **Click OK to save your changes and close the Properties panel.**

4.5 Administering the SunScreen SKIP Key Cache

The SunScreen SKIP key cache contains the shared secrets SunScreen SKIP generates. Having a cache decreases the time required to decrypt packets. After you clear the SunScreen SKIP key cache, the SunScreen SKIP Key Manager recalculates its shared secrets immediately.

To Clear the SunScreen SKIP Key Cache

1. **Open the Network Control Panel.**
2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SKIP Security for TCP/IP entry in the network component list and then click Properties.
3. **Click the Advanced tab.**
4. **Click Clear Cache.**
5. **When SunScreen SKIP displays a dialog indicating that the cache has been cleared, click OK.**
6. **Click OK to close the SunScreen SKIP network service window.**
7. **Click OK to close the control panel.**

4.6 SunScreen SKIP and Security Gateways

SunScreen SKIP interoperates with SunScreen SPF-100, SunScreen EFS, and Solaris SKIP.

Note that you must use the same type of certificate/key on both systems (for example, signed keys or unsigned keys of the same length) and specify the same encryption algorithms for both ends of a secure connection.

4.6.1 SunScreen SPF-100

SunScreen SPF-100 is a dedicated hardware security device that acts as a communications gateway between external (untrusted) systems and trusted hosts on its own subnetwork. SunScreen SPF-100 functions as a SKIP proxy, receiving and decrypting packets coming from the outside and forwarding them to the appropriate host on its subnet.

When SunScreen SKIP is configured to emulate a SunScreen SPF-100 (SunScreen mode), a remote computer, such as a home PC, sends packets encrypted with an older version of the SKIP protocol to the SunScreen, which decrypts and forwards them to the appropriate internal host.

Setting Up SunScreen SKIP

1. **Install the SunScreen SKIP software.**

2. **Install your private key and public certificate.**

3. **Install the public certificate of the SunScreen through which you will communicate.**

4. **Add the host served by the SunScreen SPF-100 to the SunScreen SKIP access control list, selecting the appropriate encryption algorithms and specifying that SunScreen SKIP will use the certificate of the SunScreen to communicate with the remote host.**
   See "To Add a SunScreen SPF-100 to Your Access Control List" on page 9 for more information.

Setting Up Your SunScreen SPF-100

1. **Add your computer's IP address definition to the SunScreen SPF-100.**

2. **Use the Certificate Manager to identify your computer as a SunScreen SPF-100, entering its IP address and selecting the same encryption algorithms you specified when you added the SunScreen SPF-100 to your access control list.**

3. **Install your public certificate on the SunScreen SPF-100.**
4. **Configure one or more SunScreen actions to use the appropriate public certificates for encrypting and decrypting communications between your computer and the SunScreen SPF-100.**
5. **Create a PASS rule on the SunScreen to permit communications between your computer and the internal host for a specific service (such as PING or TELNET) or a range of services (such as TCP ALL).**
6. **Download the updated configuration to the SunScreen SPF-100.**
7. **Activate the new link in the SunScreen SPF-100.**

5

Troubleshooting SunScreen SKIP

Troubleshooting SunScreen SKIP can be difficult, because even when your network connection is functioning and packets are traveling from one computer to the other, a mismatch in configurations causes SunScreen SKIP to drop packets silently.

If you encounter problems running SunScreen SKIP:

- Verify your SunScreen SKIP installation and configuration
- Test your network connection
- Examine packets transmitted by your computer
- Use the Network Event Log to record network traffic information

5.1 Verifying Your Installation and Configuration

If you are encountering problems exchanging encrypted traffic with a host on your access control list, check the following:

- *Is SunScreen SKIP enabled on both systems?*

  Open the SunScreen SKIP Access Manager dialog box and verify that the SunScreen SKIP Enabled check box is enabled.

- *Do you have the correct certificate?*

  Verify that a certificate exists for the remote host in your access control list. Verify that your certificate is correct in the access control list on the remote host. If necessary, reinstall or rediscover certificates on both ends.

- *Is the SunScreen SKIP key cache obsolete or corrupted?*

  If necessary, clear the key cache. This causes the key manager to purge its list of shared secrets and recalculate them using installed or discovered certificates.

- *Are you using the correct name space?*

  Verify that both ends of the SKIP link are using the same name space for their certificates.

- *Are you behind a firewall?*

  If you are behind a firewall that blocks traffic to UDP port 1640 or port 1641, SunScreen SKIP's Certificate Discovery mechanism will fail. In such cases, try installing certificates from a diskette (if you are using signed certificates) or modifying the firewall to permit clear traffic on UDP ports 1640 and 1641.

- *Are the system clocks on both computers set correctly?*

  Because SunScreen SKIP uses the time and date specified by the system clock to generate session keys, an incorrect date or clock setting will cause a session key mismatch, resulting in the failure of secure communications. Verify that the time, date, and time zone settings on both hosts are configured correctly.

- *Do both hosts have stable IP addresses?*

  Because SunScreen SKIP identifies hosts by IP address, computers running the SunScreen SKIP software must have stable IP addresses. If your site uses the Dynamic Host Configuration Protocol (DHCP) to allocate IP addresses, you should assign static IP addresses or dynamic IP addresses with long lease terms to SunScreen SKIP hosts.

- *If a host has more than one network interface, is SunScreen SKIP configured for all interfaces?*

  If a computer has more than one network interface (such as a LAN interface and a serial interface), the Microsoft TCP/IP stack routes packets over whichever interface it considers the more efficient path to the specified destination host. If a destination host can be reached through more than one interface and if you have configured SunScreen SKIP differently for each interface, SunScreen SKIP will use different settings to encrypt/decrypt and authenticate network traffic.

5.2 Testing Your Network Connection

If the configuration on both hosts appears correct, you need to verify that packets are traveling from one host to the other. Disable SunScreen SKIP on both hosts and use a utility such as PING to test the network connection between the hosts. If the two hosts cannot see each other, the problem may be caused by a network cable or router.

If you can ping one host from the other with SunScreen SKIP disabled, try enabling SunScreen SKIP and using the PING utility to send encrypted ICMP packets between the hosts.

5.3 Examining SunScreen SKIP Packets

If two hosts are unable to use SunScreen SKIP to communicate securely, you may find it useful to determine whether the problem lies with the sender or the destination host. Use a packet capture utility to display the contents of packets being sent from one host to the other. If the captured packets are encrypted (that is, if the data portion of the packet that would normally be readable is not), try capturing packets traveling in the other direction. If packets traveling in one direction are not encrypted, verify that SunScreen SKIP is enabled and configured correctly on the sending host. If packets traveling in both directions are encrypted, you should verify that the SunScreen SKIP settings for the two hosts are consistent.

5.4 Using the Network Event Log

The Network Event Log monitors the operation of many network functions, including SunScreen SKIP, and records diagnostic and error messages as they occur. Using the Network Event Log, you can create an audit trail of the transactions and messages SKIP generates as it communicates with other hosts.

You can configure the Network Event Log to display messages, save messages to a text file, or send messages to a syslog host. For each location, you determine the severity of the messages and errors logged. You can also direct the Network Event Log to mark the log at specific intervals. Enable the mark function to assure yourself that the Network Event Log is monitoring operations, when few or no messages or errors occur.

Logged information includes the date and time of the message or error, the source, and a brief description of the message or error. When output is directed to a remote host, the name of the remote host to which the information is being forwarded is also included in the message or error log entry.

5.4.1 To Use the Network Event Log

1. **Open the Network Control Panel.**
2. **Open the Properties panel for the SunScreen SKIP network service.**
   Select the SunScreen SKIP Security for TCP/IP entry in the network component list and then click Properties.
3. **Click the Advanced tab.**
4. **Specify the minimum severity level for which you want SunScreen SKIP messages logged.**
   SunScreen SKIP sends messages with a severity level equal to or greater than the level you specify to the Network Event Log utility. Message severity levels are:
   - Emergency – Not used.

- Alert – Not used.
- Critical – Not used.
- Error (default) – General system errors.
- Warning – Unusual but non-harmful situations.
- Notice – Important traffic information.
- Informational – Detailed traffic information.
- Debug – Dump of internal data structures.

Note that using severity settings below Error will cause performance problems and may result in lost network packets.

5. **Click View Log.**
   The Network Event Log opens.

6. **Configure the Network Event Log utility to display messages with the severity level you specified in Step 4.**
   Choose Configure from the Display menu and click the appropriate severity level in the Window list box. The Network Event Log utility begins displaying messages as they are received.

Note—You can configure the Network Event Log to display messages, save messages to a text file, or send messages to a `syslog` host. See the on-line help for Network Event Log for information on configuring and using the application.

A

How SunScreen SKIP Works

SunScreen SKIP provides several network security services:

- **Access control** to protect corporate data resources from unauthorized use.
- **Encryption and decryption services** to ensure the confidentiality of information sent over the network.
- **Authentication** to ensure the integrity of the information transferred from one group to another within your corporation.

Each of these services is described separately below.

A.1 Access Control

Use access control on your network to limit and control who uses your host systems and applications through your communications links. Each entity with which you communicate must be identified by name, IP address, or network so that access to your system is controlled. Once communication is established, your computer can exchange encrypted or unencrypted data with the remote host.

The SunScreen SKIP access control list (ACL) specifies whether remote hosts or networks are authorized to communicate with your computer. Each entry in your access control list identifies a specific host (by name or IP address) or network (by network number and subnet mask). You use SunScreen SKIP Access Manager to maintain your access control list.

SunScreen SKIP's access control is based on the requesting system's IP address. When a system tries to connect to a host running SunScreen SKIP, the application searches for an ACL entry as follows:

1. SunScreen SKIP searches for an ACL entry for the remote host. If the entry exists, SunScreen SKIP uses it to determine access permissions (which can be Clear Access, Encrypted Access, or No Access) and encryption information (if any).

2. If an entry for the host does not exist, SunScreen SKIP searches for an ACL entry for the network to which the remote host belongs. If the entry exists, SunScreen SKIP uses it to determine access permission (which can be Clear Access or No Access).

3. If SunScreen SKIP cannot find an ACL that pertains to the remote host, it uses the default system entry, which is configured by the user to allow or deny access to unknown hosts, or to request user intervention before access is given.

A.2 Encryption/Decryption

Encryption is the process by which a readable message is converted to an unreadable form to prevent unauthorized parties from reading the message. *Decryption* is the process of converting an encrypted message back to its original (readable) format. The original message is called the *plaintext message*. The encrypted message is called the *ciphertext message*.

Digital encryption algorithms work by manipulating the digital content of a plaintext message mathematically using an encryption algorithm and a digital key to produce a ciphertext version of the message. The sender and recipient can communicate securely if the sender and recipient are the only ones who know the key.

A.2.1 Shared Key Encryption and Public Key Encryption

SunScreen SKIP uses a combination of *shared key cryptography* and *public key cryptography* to protect messages sent between hosts. Shared key cryptography uses traffic keys that change frequently to encrypt data sent from one host to another. Public key cryptography uses hosts' implicit shared secrets to encrypt the traffic keys, keeping network communication secure.

Shared Key Encryption

Shared key encryption uses one key to encrypt and decrypt messages. For shared key cryptography to work, the sender and the recipient of a message must both have the same key, which they must keep secret from everybody else. The sender uses the shared key to encrypt a message (Figure A-1) and then sends the ciphertext message to the recipient.

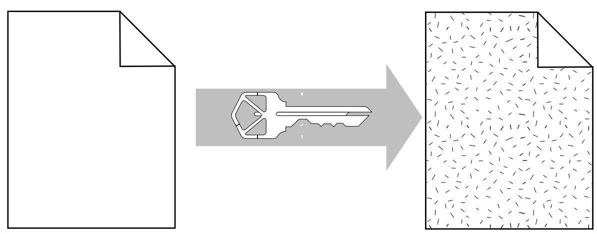

Figure A-1 Sender Uses Key to Encrypt Plaintext to Ciphertext

When the ciphertext message arrives, the recipient uses the identical shared key to decrypt the message (Figure A-2).

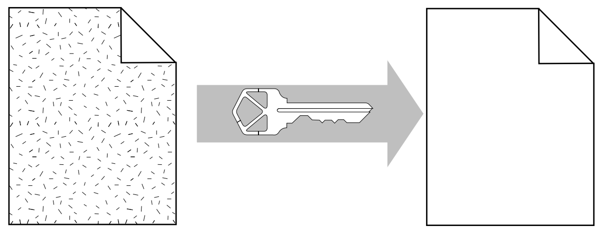

Figure A-2 Recipient Uses Key to Decrypt Ciphertext to Plaintext

Shared key encryption/decryption is relatively fast. However, since anyone with the shared key can decrypt the information, shared key encryption requires that only the sender and recipient have access to the shared key. SunScreen SKIP uses shared key algorithms to encrypt packets sent between hosts. SunScreen SKIP protects the security of encrypted information by generating new traffic keys frequently during a communication session, making acquisition of any one traffic key useless.

Public Key Encryption

Public key encryption uses a pair of complementary keys (a *public key* and a *private key*) to encrypt and decrypt messages (Figure A-3). The two keys (called a Diffie-Hellman key pair, after the inventors of the public key encryption algorithm) are mathematically related such that a message encoded with one key can only be decoded with the other key. Although a user's public and private keys are mathematically related, knowledge of a public key does not make it possible to calculate the corresponding private key.

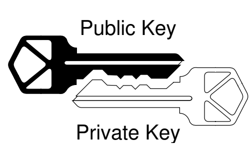

Figure A-3 Complementary Public and Private Keys

In public key encryption systems, users make their public key available to anyone and keep their private key secret. When one user wants to send a private message to another user, the sender looks up the recipient's public key and uses it to encrypt a message (Figure A-4) before sending it to the recipient.

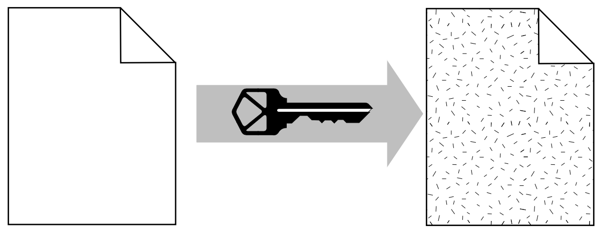

Figure A-4 Sender Uses Recipient's Public Key to Encrypt Message

When the encrypted message arrives, the recipient uses his private key to decrypt the message (Figure A-5). Since the recipient's private key is known only to the recipient, both the sender and recipient can safely assume that no one other than the recipient could read the message.

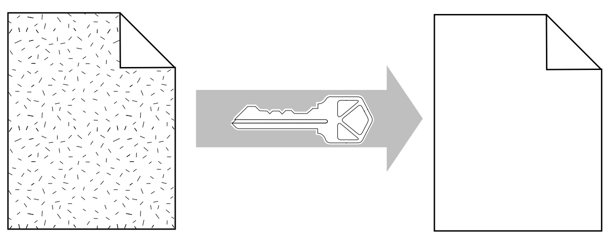

Figure A-5 Recipient Uses Private Key to Decrypt Message

Public key cryptography solves the problem of securely distributing keys by removing the need to transmit secret keys. Only users' public keys need to be exchanged.

Public key encryption algorithms are mathematically more complex than shared key encryption algorithms. As a result, public key encryption is significantly slower than shared key encryption. Consequently, SunScreen SKIP uses public key encryption to create a shared secret between two users, and then uses shared key encryption to encrypt traffic traveling between the two hosts.

A.2.2 Encryption Algorithms

Table A-1 lists the traffic encryption algorithms supported by SunScreen SKIP.

Table A-1 Encryption Algorithms

Encryption Algorithm	Description	Efficiency	Security
Data Encryption Standard (DES)	DES uses cipher block chaining (CBC) and a 56-bit key to encrypt 64-bit blocks of plaintext in multiple iterations.	Moderate	Excellent
RC-2	RC-2 uses cipher block chaining (CBC) and a variable-size key to encrypt 64-bit blocks of plaintext.	Good	Good
RC-4	RC-4 uses a 40-bit key to encrypt data in a continuous stream.	Excellent	Moderate

A.2.3 Diffie-Hellman Certificates

Diffie-Hellman certificates are the means by which a user distributes public key information. A Diffie-Hellman certificate is a digital document that contains a user's Distinguished Name, the public key associated with that Distinguished Name, and the time interval for which the certificate is valid. You can distribute your public certificate to other users, who extract and use your public key to encrypt messages they want to send you. Users can distribute their certificates freely to other SKIP users on diskette, via a certificate server, or over a network.

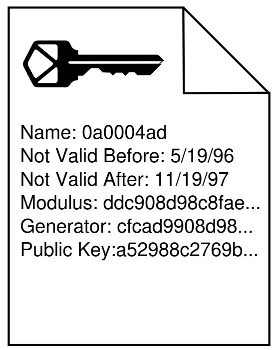

Figure A-6 Diffie-Hellman Certificate Contents

Diffie-Hellman certificates can be *signed* or *unsigned*:

- **Signed Diffie-Hellman certificates** must be obtained from a Certification Authority, which is an entity trusted to create and assign Diffie-Hellman certificates. In addition to the information described above, a signed certificate contains the name of the certification authority responsible for issuing the certificate and the MD5 hash of the certificate's public key. The CA's digital signature lets anyone who receives the certificate validate its contents and verify that an unauthorized user is not impersonating you.

  Signed certificates can be stored in directory servers, transmitted by means of non-secure message exchanges, or distributed by other means that make certificates easily accessible to users, such as diskette exchange.

- **Unsigned Diffie-Hellman (UDH) certificates** are generated on demand by the user. A user's unsigned certificate can be distributed only through certificate discovery (which is described on page 9). Unsigned Diffie-Hellman certificates can offer several advantages over signed certificates:

- When a user generates her own public certificate, she also generates her own private key. This private key never leaves the user's machine, meaning that a network administrator does not need to order, distribute, or protect key diskettes.
- Since UDH certificates are not registered by a certification authority, they do not need to be formally revoked. If a user or administrator suspects that a key has been compromised, she can generate a new key/certificate and distribute the new certificate to other users.

The decision whether to use a signed or unsigned Diffie-Hellman certificate depends on the type of hosts with which you want to exchange encrypted traffic. Table A-2 lists the type of certificate you need for various SKIP-compatible hosts. Refer to "SunScreen SKIP and Security Gateways" on page 6 for information on configuring SunScreen SKIP to work with other SKIP-compliant security gateways.

Table A-2 Diffie-Hellman Certificate Requirements

If you want to communicate with:	You must use:
SunScreen SKIP host using a signed certificate	Signed certificate
SunScreen SKIP host using an unsigned certificate	Unsigned certificate
SunScreen EFS 1.0 using a signed certificate	Signed certificate
SunScreen EFS 1.0 using an unsigned certificate	Unsigned certificate
SunScreen SPF-100 or SPF-100G	Signed certificate
SKIP for Solaris host using a signed certificate	Signed certificate
SKIP for Solaris host using an unsigned certificate	Unsigned certificate

A.2.4 Certificate Discovery

Certificate discovery lets a host running SunScreen SKIP retrieve a public certificate from another SKIP host over a network or serial connection. Certificate discovery is required when hosts use unsigned Diffie-Hellman (UDH) certificates, and is available as an alternative to direct installation of signed certificates. Certificate discovery works as follows:

1. You verify that certificate discovery is enabled on your computer and on the remote host.
2. You obtain the identifier and name space of the certificate you want to discover from a remote user by means of a channel that lets you authenticate the other user's identity. For example, you might call a user with whom you want to send encrypted traffic to exchange certificate identifiers and name spaces, relying on recognition of the other user's voice to authenticate the user's identity.
3. You enter the identifier of the remote certificate in SunScreen SKIP Access Manager.
4. You tell SunScreen SKIP to use certificate discovery to retrieve the specified certificate.
5. Your computer sends a Certificate Discovery Protocol request to the remote computer in clear text on UDP port 1640 asking for a specific certificate using the designated name space.
6. The remote computer sends back the requested information in clear text on UDP port 1641.
7. SunScreen SKIP adds the certificate for the remote host to its certificate database.
8. SunScreen SKIP uses the public key information contained in the remote host's certificate to generate a unique shared secret.

A.2.5 Name Spaces

Name spaces let users identify certificates in more than one way. For example, a user might use the IPv4 address assigned to her certificate to identify it to one user and use the MD5 hash of the certificate's public key to identify it to another user. By making certificate identification flexible, name spaces help protect certificates from unauthorized users.

Name space identifiers (NSIDs) identify the type of keys being used. SunScreen SKIP supports the following NSIDs:

- NSID 1, which is the IPv4 address assigned to the certificate by a certification authority.
- NSID 8, which is the MD5 hash of the certificate's Diffie-Hellman public key

When one host requests a certificate from another host, it must provide a NSID/KEYID pair. The NSID value specifies the type of identifier it is using, and the KEYID value specifies the identifier for the requested certificate.

Note—The IP address used for NSID 1 does not correspond to the IP address used by your computer. Rather, it is an eight-byte hexadecimal number assigned to the certificate by the certification authority to bind a unique Distinguished Name to the certificate contents.

A.3 Authentication

Authentication is the process of verifying that the person requesting access or sending a message is who they say they are. You can authenticate messages for two reasons: to ensure that a message received from another host has not been modified in transit and to verify the identity of the person sending the message.

SunScreen SKIP uses the Keyed MD5 algorithm to implement authentication. The MD5 message digest algorithm takes a message of any length and produces a 16-byte digest (the hash value). This message digest serves as a "thumbprint" of the original file when you want to authenticate a document. The original message cannot be derived from the message digest.

The process by which SunScreen SKIP signs a message with a message digest follows.

1. The sender and destination host agree to use authentication as part of their secure communication process.
2. The sender creates a message and indicates it can be sent to the destination host.
3. SunScreen SKIP encrypts the message using the specified encryption algorithm.
4. SunScreen SKIP creates a digest of the message using a keyed MD5 message digest algorithm and encrypts the message digest with the sender's private key.
5. SunScreen SKIP adds the encrypted digest to the authentication header for the message.
6. SunScreen SKIP sends the message to the destination host.
7. The destination host receives and decrypts the encrypted message, which includes the message digest.
8. The destination host uses the sender's public key to decrypt the message digest.
9. The destination host creates its own message digest of the message it received, using the same keyed MD5 algorithm the sender used.
10. The destination host compares the message digest it created from the original message with the one that came with the message. If the two message digests match, the destination

host knows that the text of the message has not been modified and that the person claiming to be the sender was actually the sender.

Figure A-7 illustrates how a destination host would calculate its own MD5 digest of the message, decrypt the digest sent with the message, and compare the two digests to authenticate the integrity and source of the message.

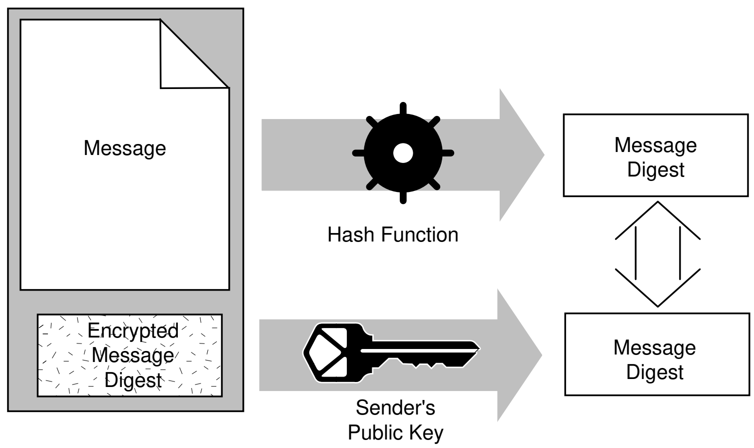

Figure A-7 Authenticating a Message

Authentication provides a "digital signature" that proves the identity of the sender. If the message digest could be decrypted with the sender's public key, the destination host knows it was encrypted with the sender's private key. Since the sender's private key is known only to the sender, the destination host can be confident of the message's source as well as of its integrity.

A.4 How SunScreen SKIP Calculates Key Values

When SunScreen SKIP (or a certification authority) generates a private key/public key pair, it starts by generating a random 512- or 1024-bit number, which serves as the private key value. It then calculates the public key value by using the formula g^x

$mod\ p$, where x is the private key value and g and p are fixed values. Once the private and public keys have been calculated, SunScreen SKIP formats the user's public certificate, which contains the public key value, the g and p values used to compute the public key, and other information, such as the period for which the certificate is valid.

SunScreen SKIP hosts exchange their public certificates with one another freely. When two hosts wish to communicate securely, each host calculates a mutually authenticated shared secret based solely on knowledge of its private key and the other host's public key.

For example, assume that a SKIP host (I) has a private key i and a public key $g^i\ mod\ p$. This public key is distributed in the form of a signed or unsigned Diffie-Hellman certificate. Similarly, another SKIP host (J) has a private key j and a public key $g^j\ mod\ p$. I and J can independently calculate their mutually authenticated secret ($g^{ij}\ mod\ p$) based on knowledge of their own private key value and the other host's public key value. This shared secret is implicit and does not need to be communicated between the two hosts. This mutually authenticated long-term secret is used to derive a long-term secret key, which is denoted K_{ij}. This key is derived from the low-order bits of $g^{ij}\ mod\ p$.

SunScreen SKIP uses the current date and time as a counter value (n), which changes each time I and J open a communication session. SunScreen SKIP uses the long-term secret key K_{ij} and the date/time value n to create a unique session key K_{ijn}. This session key, which changes for each communication session between I and J, is used to encrypt traffic keys. Since I and J can calculate K_{ij} based on their implicitly authenticated shared secret, the two computers can calculate the same value for K_{ijn} if their system clocks are synchronized.

Note—Because SunScreen SKIP relies on the system clock value to calculate session keys, users should verify that the system clock on their computers are configured with the correct time, date, and time zone. Users should never change the time or date setting on their computer during a SKIP session.

When I wants to send a secure message to J, I uses a randomly generated traffic key K_p to encrypt the packet data, which carries the contents of the message. The traffic key K_p is in turn encrypted using K_{ijn}. SunScreen SKIP then constructs a series of packets, each containing the IP header information needed to route the packet to its destination, the traffic key encrypted with the session key K_{ijn}, and the packet data encrypted with the traffic key K_p. Figure A-8 shows an encrypted IP packet, using the two-step encryption procedure described above.

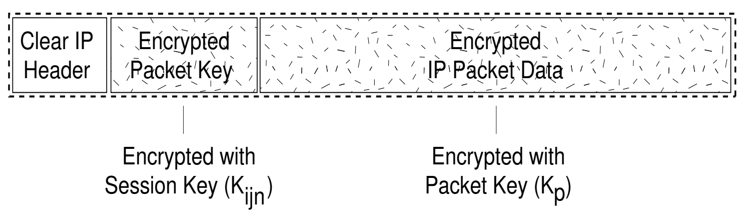

Figure A-8 Encrypted IP Packet

When the destination host receives this encrypted packet, it looks up the sender's certificate. Using the long-term secret key K_{ij}, the session counter value n, and the current date/time, the destination host computes the same K_{ijn} value used by the sender. Using K_{ijn}, the destination host decrypts the traffic key K_p, and then use the traffic key to decrypt the packet data.

Since K_{ijn} can be cached for efficiency, SunScreen SKIP can change traffic keys very rapidly without incurring the computational overhead of a public key operation. SunScreen SKIP changes traffic keys after 30 seconds or after they have been used to encrypt 512K of data.

A.5 SunScreen SKIP Components

The three main components of the SunScreen SKIP architecture are:

- The **key manager** (nfswkmgr.exe), which maintains a database of certificate information about peers. The key manager automatically runs in the background after you install SunScreen SKIP. The key manager is responsible for calculating and caching the Diffie-Hellman long-term secret used to derive K_{ij}, the master or key-encrypting key for each peer. The key manager also works in conjunction with the SunScreen SKIP kernel to generate the packet encryption key K_p.
- The **bulk data crypt engine**, which, in conjunction with the key manager, offers bulk data encryption and decryption services to kernel clients. The bulk data crypt engine uses kernel modules to perform packet encryption using DES-CBC, RC2-40, or RC4-40 algorithms.
- The **streams module**, which is a client of the bulk data crypt engine. This is inserted between the Windows TCP/IP stack and the network interface. Using an access–control list based on the peer's IP address, packets are either passed in the clear, dropped, or sent to the bulk data crypt engine for encryption or decryption.

Figure A-9 presents an overview of the relationships of the SunScreen SKIP components.

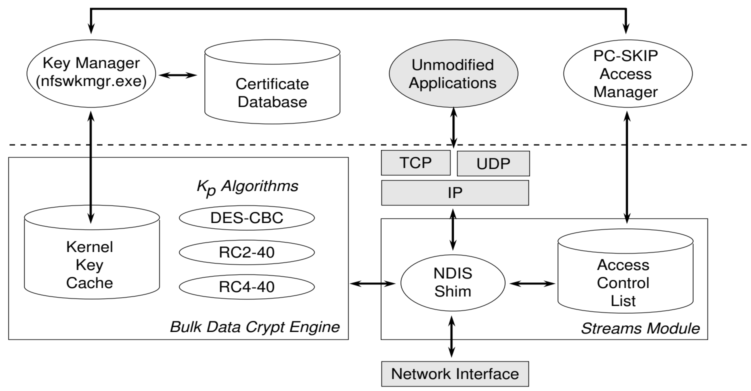

Figure A-9 SunScreen SKIP Components

A.6 How the SunScreen SKIP Components Interact

SunScreen SKIP works without modification to existing applications or to your Windows 95 system software. When you start your computer, SunScreen SKIP inserts an NDIS shim between the network interface and the IP layer of the Microsoft TCP/IP protocol stack. The NDIS shim lets SunScreen SKIP intercept all packets entering and leaving the IP layer.

If SunScreen SKIP determines that a packet needs to be encrypted, SunScreen SKIP passes the packet to the bulk data crypt engine. The bulk data crypt engine accepts a buffer containing the plaintext packet and a buffer containing the encrypted packet and the K_{ijn} key encryption algorithm, the K_p packet encryption algorithm, and the peer certificate information required to encrypt the packet.

If this is the first time the system is communicating with the peer, the bulk data crypt engine sends a message to the key manager requesting a packet encryption key (K_p). The key manager calculates K_{ijn} and caches the result. The key manager generates a traffic key K_p, encrypts K_p in K_{ijn}, and returns the traffic key to the bulk data crypt engine.

When the key manager responds with the message containing K_p and encrypted K_p, the SKIP engine calls the appropriate cryptographic algorithm with K_p as a parameter, and then writes a SKIP header containing encrypted K_p to the output buffer. The packet is then encrypted and written to the output buffer. The information about the peer is cached in the bulk data crypt engine. Subsequent packets to the same peer can be encrypted and sent without further assistance from the key manager.

SunScreen SKIP counts the number of bytes encrypted using a traffic key and requests a new key when a traffic key has been used to encrypt `512K` of data. The SKIP engine continues to use the old key while it waits for the key manager to deliver the new traffic key, and then purges the old traffic key from its buffer.

Packets are decrypted in a similar fashion. The SKIP module accepts an encrypted packet and passes it to the engine. The first time a system receives a packet from a peer, the SKIP protocol header is decoded, retrieving the encrypted K_p, the peer identifier, and algorithm information. A message containing this information is sent to the key manager with a request for the plaintext version of K_p. The key manager calculates the session key K_{ijn} and caches the result. The key manager then uses K_{ijn} to decrypt the packet encryption key K_p and returns the result to the bulk data crypt engine. While these calculations are taking place, the key manager stores the packet (and any subsequent packets from the same peer with the same encrypted K_p and algorithm information).

When the key manager responds with the message containing the plaintext K_p, the bulk data crypt engine calls the appropriate cryptographic algorithm with K_p as a parameter, and then decrypts the waiting packets using the appropriate cryptographic algorithm.

The information about the peer is cached in the bulk data crypt engine. The bulk data crypt engine can decrypt subsequent packets from the same peer with same encrypted K_p and algorithm information without further assistance from the key manager. The cached information is automatically removed after a specified period of nonuse. When the sender changes traffic keys, the old cached key entry is retained for a short time. This lets SunScreen SKIP deal efficiently with out-of-order IP packets as traffic keys change.

A.7 IP Fragmentation

Because of the overhead of the SKIP header information and the padding required by a block cipher, encrypted datagrams are larger than the original packets. SunScreen SKIP typically requires an additional overhead of 48 bytes (20 bytes for the new IP header plus 28 bytes for the SKIP ESP header. Since the resulting datagram could exceed the network interface's maximum transmission unit (MTU) size, the NDIS shim inserted by SunScreen SKIP between the Microsoft TCP/IP protocol stack and the network interface artificially reduces the interface's advertised MTU. This prevents unnecessary fragmentation of encrypted IP datagrams by the local host.

B

Changes to System Files

This appendix describes changes made to the Windows 95 Registry and to Windows system files by installing SunScreen SKIP software.

B.1 Windows 95 Registry

The SunScreen SKIP installation program adds the changes listed in Table B-1 to the *HKEY_LOCAL_MACHINE\SOFTWARE\SUNW\CC\1.0\SUNWSKIP* key in the Windows 95 Registry.

Table B-1 Windows 95 Registry Entries for SunScreen SKIP

Name	Valid Values	Default
Access Mode	Ask, Add Automatically, No Access	No Access
Bin Dir	<*INSTALLDIR*>*SKIP*	None
CD Enabled	True/False	True
Debug Level	1, 2, 3, 4, 5	3
KeyInfo Dir	<*INSTALLDIR*>*SKIP*	None
Last Protocol		None
Resolve Name	True/False	True
Show Icon	True/False	True
Start Secure	True/False	False

B.2 Windows 95 System Files

SunScreen SKIP installs a number of files on your computer. Once installed, the directory structure and files listed in Table B-2 constitute the SunScreen SKIP product.

Table B-2 SunScreen SKIP Files

File Name and Default Path Name	File Description
C:\WINDOWS\SYSTEM\SUNWSKIP.EXE	Configuration application
C:\WINDOWS\SYSTEM\NFSWKMGR.EXE	Key Manager
C:\WINDOWS\SYSTEM\SUNWSYSLOGD.EXE	Error logger
C:\WINDOWS\SYSTEM\SUNWSC.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\SUNWSC32.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\SUNWSKIP.VXD	Virtual device driver
C:\WINDOWS\SYSTEM\KMAPI32.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\LKMAPIW.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\MSVCRT40.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\MFC40.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\SUNWLIC.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\SUNWCLS.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\LMGR324A.DLL	Dynamic link library

Table B-2 SunScreen SKIP Files

File Name and Default Path Name	File Description
C:\WINDOWS\SYSTEM\NFSWLIC.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\SKIP16.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\WINSOCKX.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\LMGR164A.DLL	Dynamic link library
C:\WINDOWS\SYSTEM\MFC250.DLL	Dynamic link library
C:\WINDOWS\HELP\SUNWSKIP.HLP	SunScreen SKIP Help file
C:\WINDOWS\HELP\SUNWSKIP.CNT	SunScreen SKIP Help contents
C:\WINDOWS\HELP\SUNWNFS.HLP	Post-installation Help file
C:\WINDOWS\HELP\SUNWSYSLOGD.HLP	Error logger Help file
C:\WINDOWS\HELP\SUNWSYSLOGD.CNT	Error logger Help contents
C:\WINDOWS\HELP\PRODSUPP.HLP	Product Support Help file

Table B-2 SunScreen SKIP Files

File Name and Default Path Name	File Description
C:\WINDOWS\INF\SUNWSKP.INF	
<INSTALLDIR>\BIN\SUNWINF.EXE	Device information file
<INSTALLDIR>\README.TXT	SunScreen SKIP release notes

Glossary

access control list (ACL)

The list of hosts with which your computer is authorized to communicate. Your access control list should identify hosts with which you want to communicate in the clear as well as hosts with which you want to exchange encrypted traffic.

address

In networking, a unique code that identifies a *node* to the *network*.

Address Resolution Protocol (ARP)

Protocol that translates Internet addresses to Ethernet addresses, and Ethernet addresses to Internet addresses.

algorithm

A sequence of steps designed to solve a problem or execute a process such as drawing a curve from a set of control points, or encrypting a block of data.

attack

An attempted *cryptanalysis* or an attempt to compromise system security.

authentication

Process used to verify that data received from another user was generated by the expected source and that the data has not been modified in transit.

block

Groups of bits are called blocks.

block cipher or block algorithm

An encryption algorithm that encrypts while blocks at once. (See *stream ciphers*)

broadcast

A *packet* delivery system where a copy of a given packet is given to all hosts attached to the network.

cache

A buffer of high-speed memory used to store frequently accessed memory or values. A cache increases effective memory transfer rates and processor speed.

CBC

Cipher block chaining (see also DES). A mode used to chain a feedback mechanism, which essentially means the previous block is used to modify the encryption of the next block.

CDP

Certificate discovery protocol. A request/response protocol used by two parties to transfer certificates.

CD-ROM

Compact disc, read-only memory. A form of storage characterized by high capacity (roughly 600 megabytes) and the use of laser optics rather than magnetic means for reading data.

certificate

Digital document that contains a user's public key and other identification information. SunScreen SKIP users must exchange certificates before they can communicate securely.

certification authority (CA)

An entity trusted to create and assign Diffie-Hellman certificates. A certification authority provides a digital signature that lets anyone who receives the certificate validate its contents and verify that it is being used by the authorized user.

certificate ID

The number identifying a user's certificate. Certificates using Name Space ID 1 (NSID 1) have an identifier consisting of eight hexadecimal digits, such as `0a00f123`. Certificates using Name Space ID 8 (NSID 8) have an identifier consisting of 16 hexadecimal digits. A signed certificate can use more than one name space, meaning that it can have more than one identifier.

cipher

A cryptographic algorithm used for encryption or decryption.

ciphertext

An encrypted message.

confidentiality

The property of communicating such that the intended recipients know what is being sent, but unintended parties cannot determine what is sent.

cryptanalysis

The art and science of breaking *ciphertext*.

cryptography

The art and science of keeping messages secure.

datagram

A packet containing enough information to be routed to a destination. It usually contains a complete source and destination address in addition to its data.

decryption

Process by which encrypted (unreadable) data is converted back into readable data through use of a key.

Diffie-Hellman encryption algorithm

A classic cryptographic construction that uses exponentiations over a prime field. Used as the basis of public key cryptography. Named after its developers.

encapsulation

The technique used by layered protocols in which a layer adds header information to the protocol data unit from the layer above. In Internet terminology, for example, a packet would contain a header from the physical layer, followed by a header from the network layer (*IP*), followed by a header from the transport layer (*TCP*), followed by the application protocol data.

encryption

Process by which a message is converted into an unreadable format using a series of calculations and a key.

export-controlled

Version of the SunScreen SKIP certificate software that uses 1024-bit keys and allows users to select DES, RC2, or RC4 for traffic encryption. Compare *Global*.

firewall

A network security and access control system that prevents hosts outside a site from accessing hosts or services inside the site

fragmentation

The process of dividing a packet into multiple smaller packets so that they can be sent over a communication link that only supports the smaller size.

FTP

File Transfer Protocol.

global

Version of the SunScreen SKIP certificate software that uses 512-bit keys and allows users to select RC2 or RC4 for traffic encryption. Compare *Export-Controlled*.

hash value

Digital “fingerprint” of a file or data sequence derived by submitting the information to a one-way hash algorithm. The same file or data sequence always produces the same hash value. The original file or data sequence cannot be derived from its hash value.

integrity

The property of ensuring that data are transmitted from the source to destination without undetected alteration.

IP

Internet Protocol. The low-level network protocol within the TCP/IP protocol suite that describes how Internet nodes are identified to the network.

kernel

The core of the operating system software. The kernel manages the hardware and supplies fundamental services such as filing that the hardware does not provide.

Key and Certificate Diskette

Diskettes that contain both the private key and the certificate containing the public key. The identifier for this certificate is on the label. The information is extremely sensitive and should be kept secure.

MD5

Message digest algorithm that creates a 128-bit hash from a message of any length.

modulus

An arithmetic operation used in programming whose result is the remainder of a division operation. The plural is moduli.

MTU

Maximum transmission unit

name space identifier (NSID)

Type of identifier used to identify a Diffie-Hellman certificate. SunScreen SKIP supports two name spaces: NSID 1 (IPv4 address) and NSID 8 (MD5 hash of certificate's public key). A signed Diffie-Hellman certificate can be identified by an NSID 8 identifier as well as an NSID 1 identifier. An unsigned Diffie-Hellman (UDH) certificate must be identified by an NSID 8 identifier.

network adapter

Hardware component that receives and sends packets on the network.

Network Device Interface Specification (NDIS)

A standard for device drivers for communication controllers, such as Ethernet and Token-Ring adapters. It was developed by Microsoft Corporation and 3Com Corporation. NDIS drivers support multiple protocols (for example, NetBIOS and TCP/IP). Use an NDIS driver for compatibility with other networking products such as Windows for Workgroups.

nonrepudiation

The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent these data.

one-way hash

A cryptographically secure hash function that cannot be reversed. See *MD5*.

packet

A single network message with an associated header, addressing information, data, and optional trailer.

packet key

A randomly generated key used to encrypt the data portion of a network packet. The packet key is updated every 30 seconds or after being used to encrypt 512K of data. The packet key is encrypted with the session key and included in each packet to which it is relevant. Also known as a *traffic key*.

peer

Any functional unit in the same layer as another *entity*.

peer-to-peer communication

Interaction between devices that operate on the same communications level on a network based on a layered architecture.

PFS

Perfect forward secrecy. Ephemeral Diffie-Hellman key exchange used in conjunction with the SKIP key distributions protocol provides PFS where required.

PGP

Pretty Good Privacy. A public-domain encryption program that uses *IDEA* for data encryption, *RSA* for key management, and *MD5* as a one-way hash function.

ping

Packet Internet groper. A program used to test reachability of destinations by sending them an *Internet control message protocol (ICMP)* echo request and waiting for a reply.

plaintext

An unencrypted message.

Point-to-Point Protocol (PPP)

A protocol that enables you to create a serial communications link between your PC and a server. This link may either be a direct link or by modem and telephone line.

port number

The number of a port or logical communication channel on the network. Many services take advantage of well known ports for their activity.

private key

The secret key that corresponds to a user's public key in a Diffie-Hellman key pair.

property sheet

Dialog box listing the attributes of a software component that can be changed.

protocol

A set of conventions governing communication between network components. Examples of protocols are TCP, UDP, NFS, NIS, and FTP.

proxy agent

A software program that forwards information from one location to another.

pseudo-random

Something that is statistically random.

Public Certificate Diskette

Contains only the certificate containing the public key. The identifier for this certificate is on the label.

public key

The encryption key a user makes public through distribution of the user's Diffie-Hellman certificate. Corresponds to the user's private key.

public key cryptography

Encryption method requiring two complementary keys: a private key and a public key. Messages encrypted with a user's private key can be decrypted only with the user's public key. Messages encrypted with a user's public key can be decrypted only with the complementary private key.

RC2 and RC4

RC2 and RC4 are variable-key-size encryption algorithms designed by Ron Rivest for RSA Data Security, Inc. Apparently, "RC" stands for "Ron's Code." RC2 is a variable-key-size block *cipher*, designed to be a replacement for *DES*. RC4 is a variable-key-size stream cipher that is, according to the company, ten times faster than DES. Both algorithms are quite compact, and their speed is independent of the key's size. It is notable, however, that neither RC2 nor RC4 has survived the 20 years of intense *cryptanalysis* that DES has. See *DES*.

RC2-40 and RC4-40

A globally exportable encryption algorithm from RSA, Inc.

robust

Reliable or dependable. Not prone to error. Usually used in reference to an application program.

routing

The path of datagrams targeted at networks other than the local network. The datagrams are forwarded to the gateway system that is selected when the Solstice software starts.

session key

Key used to encrypt the packet key for each packet sent during a single communication session. The session key is independently calculated by both the sender and the destination host based on their shared secret and the time and date of the system clock.

shared key cryptography

Encryption method that uses the same key to encrypt and decrypt messages. Packet keys (traffic keys) use shared key encryption, since both the sender and the receiver use the same key to encrypt and decrypt data.

shared secret

A unique number generated using a local host's private key and a remote host's public key. The Diffie-Hellman public key algorithm assures that the remote host will calculate the same value using its private key and the local host's public key.

signed Diffie-Hellman certificate

Certificate issued by a certification authority, such as SunCA, that contains a user's public key.

stream algorithm or stream cipher

A symmetric algorithm that operates on the *plaintext* a single bit (or byte) at a time. (See *block cipher*)

subnet

IP subnetting lets an organization partition one physical IP network into two or more logically separate networks. A subnet address is an extension of the Internet addressing scheme that enables a site to use a single Internet address for multiple physical networks.

subnet mask

Specifies which bits of the 32-bit IP address represent network information. The subnet mask, like an IP address, is a 32-bit binary number: a 1 is entered in each position that will be used for network information and a 0 is entered in each position that will be used as node number information.

SunCA

The certification authority operated by Sun Microsystems.

system files

Configuration files that are created by the installation and configuration programs, Windows, and certain applications.

TCP/IP

The Transmission Control Protocol/Internet Protocol, developed by the United States Department of Defense. It provides a set of standards for computer communications, including routing traffic across networks.

traffic key

A randomly generated key used to encrypt the data portion of a network packet. The packet key is updated every 30 seconds or after being used to encrypt 512K of data. The packet key is encrypted with the session key and included in each packet to which it is relevant. Also known as a *packet key*.

Tunnel

Logical connection between a PC-SKIP host and a remote gateway responsible for decrypting and forwarding packets to a remote destination host.

UDH

Unsigned Diffie-Hellman. The UDH public value can only be used when entities are named using the message digest (*hash*) of their DH public value, and these names are securely communicated.

UDP

User datagram protocol. All CDP communication uses UDP.

unsigned Diffie-Hellman certificate

Certificate generated by a user (instead of by a certification authority) that contains the user's public key.

Virtual Device Driver (VxD)

A virtual device driver is a 32-bit program that is part of the Windows kernel. VxDs are often used to control input/output devices such as ports or video. Many software products use VxD architecture to enable communication between the network and the Windows applications running on the PC.

Index

A

B

C

D

E

G