SunScreen 3.2 Configuration Examples

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

Part No: 806–6348
September, 2001

010910@2471

Contents

Preface

The SunScreen™ 3.2 software is part of the family of SunScreen products that provide solutions to security, authentication, and privacy requirements for companies to connect securely and conduct business privately over an insecure public internetwork. Earlier SunScreen firewall products include SunScreen EFS, SunScreen SPF-100, SunScreen SPF-100G and SunScreen SPF-200, their respective Administration Stations, SunScreen packet screen software, and SunScreen Simple Key-Management for Internet Protocols (SKIP) encryption software. This SunScreen product integrates the two SunScreen firewall technologies: SunScreen EFS and SunScreen SPF-200.

SunScreen 3.2 Configuration Examples contains detailed examples on how to use the SunScreen features. It does not offer recommendations for what security policy to implement.

Who Should Use This Book

SunScreen 3.2 Configuration Examples is intended for system administrators responsible for the operation, support, and maintenance of network security. It is assumed that you are familiar with UNIX™ system administration, TCP/IP networking concepts, and your network topology.

Before You Read This Book

You need to have the following tasks completed before you install and administer your SunScreen:

- Become familiar with the SunScreen guides:
  - *SunScreen 3.2 Release Notes*
  - *SunScreen 3.2 Installation Guide*
  - *SunScreen 3.2 Administration Guide*
  - *SunScreen 3.2 Administrators Guide*
  - *SunScreen SKIP User's Guide, Release 1.5.1*
- Ensure that your system is running one of the following operating environments: Solaris 2.6, Solaris 7, Solaris 8 (without IPv6), or Trusted Solaris 7 or 8.
- List the network services by location (configuration matrix) allowed and disallowed per location used to establish rules.

Tip – Keep your SunScreen guides available for reference because the information they contain is not duplicated in this document.

How This Book Is Organized

SunScreen 3.2 Configuration Examples contains the following chapters:

- Chapter 1 provides a brief overview of the SunScreen examples.
- Chapter 2 describes how to set up an Administration Station with a Screen using SKIP or IKE as encryption.
- Chapter 3 describes enabling network hosts to be routable or accessible on the Internet.
- Chapter 4 shows a stealth-mode Screen installation.
- Chapter 5 describes how to use traffic filtering encryption and VPN rules and also using tunneling to hide the internal topology of a network.
- Chapter 6 describes HA on two stealth Screens.
- Chapter 7 describes how configurations on a group of Screens are remotely administered simultaneously.
- Chapter 8 describes a Screen that is configured to be a stealth firewall and set up to provide user authentication using proxies.
- Chapter 9 details how you would set up a Screen and a Windows 2000 system to interoperate using IKE.

Related Books and Publications

You may want to refer to the following sources for background information on cryptography, network security, firewalls, and SKIP.

- Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, 1996, ISBN: 0471128457
- Chapman, D. Brent and Elizabeth D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates, 1995, ASIN: 1565921240
- Walker, Kathryn M. and Linda Croswhite Cavanaugh, *Computer Security Policies and SunScreen Firewalls*, Sun Microsystems Press, Prentice Hall, 1998, ISBN 0130960150
- Cheswick, William R. and Steve Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 1st edition, Addison-Wesley, 1994, ISBN 201633574
- Black, Uyless D., *Internet Security Protocols: Protecting IP Traffic*, 1st Edition, Prentice Hall, 2000, ISBN: 0130142492
- Comer, Douglas E., *Internetworking with TCP/IP*, 3rd Edition, Volume 1, Prentice Hall, 1995, ISBN 0132169878
- Doraswamy, Naganand and Dan Harkins, *Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, 1st Edition, Prentice Hall, 1999, ISBN: 0130118982
- Stallings, William, *Network and Internetwork Security: Principles and Practice*, Inst Elect, 1994, Product#: 0780311078
- Kaufman, Charlie and Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, 1st Edition, Prentice Hall, 1995, ISBN: 0130614661
- Garfinkel, Simson and Gene Spafford, *Practical Unix and Internet Security*, 2nd Edition, O'Reilly & Associates, 1996, ISBN: 1565921488
- Farrow, Rik, *UNIX System Security: How to Protect Your Data and Prevent Intruders*, Addison-Wesley, 1990, ISBN: 0201570300

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

Ordering Sun Documents

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at `http://www1.fatbrain.com/documentation/sun`.

Accessing Sun Documentation Online

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

Typographic Conventions

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

TABLE P–1 Typographic Conventions

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

Shell Prompts in Command Examples

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

TABLE P–2 Shell Prompts

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

Getting Support For SunScreen Products

If you require technical support, contact your Sun sales representative or Sun Authorized Reseller.

For information on contacting Sun, go to:

`http://www.sun.com/service/contacting/index.html`

For information on Sun's support services, go to:

`http://www.sun.com/service/support/index.html`

CHAPTER 1

Introduction

SunScreen 3.2 is dynamic, stateful, IP-packet filtering firewall software used to protect a host or a network of hosts by controlling packet flow to or through the machine on which it is installed. SunScreen uses ordered rules that restrict access based on IP addresses and network service ports. Using both SunScreen SKIP and IPSec IKE, you can configure SunScreen to encrypt IP packets between hosts or a network of hosts to prevent data compromise. SunScreen generally provides authentication of hosts using certificates but you can also use IKE manual or pre-shared keys for encryption with Packet Filtering rules.

SunScreen supports Network Address Translation (NAT) , High Availability (HA), and Centralized Management Groups (CMG). Also, SunScreen includes user-level proxies for application-level packet examination or user authentication through internal or external means.

The administration graphical user interface (GUI) works on any browser supporting JDK 1.1 (or compatible versions) and has end-system SKIP or IPSec IKE installed . The installer program adds the required SunScreen SKIP and IKE packages automatically by or you can install these packages using command line installation.

For detailed information on how SunScreen SKIP encryption works, refer to the *SunScreen SKIP 1.5.1 User's Guide*. You can find a description of SunScreen's IKE implementation in the *SunScreen Administrators Overview*.

What Is the Configuration Examples Manual?

This document is a collection of hypothetical network configurations using the SunScreen firewall. The examples are real-life examples that use the following features of this product.

- Remote administration of a Screen using an Administration Station. The administration GUI runs on the Administration Station but the configuration files it uses are stored on the Screen. One Administration Station can manage any number of Screens that have the access rules defined to grant administrative access.
- SunScreen supports Network Address Translation (NAT) and this manual contains an example of how you use both the STATIC and DYNAMIC NAT features with the firewall.
- Sunscreen has both Routing mode allowing normal routing of traffic and Stealth mode which makes the firewall invisible to the outside world. You can also configure SunScreen in a mixed mode where one interface of the firewall is stealth and other interfaces are routing. Examples using all three of these modes are included in this manual.
- SunScreen allows you to set up Virtual Private Networks (VPNs). This manual provides three examples that use encryption with Packet Filtering and VPN rules. The examples use both SKIP and IKE
- The High Availability (HA) feature lets you use a redundant machine to mirror all network traffic and firewall configurations. Should the active machine in the HA configuration fail for any reason, the passive partner takes over providing uninterrupted operation.
- The Centralized Management Group feature enables you to connect to one Screen that is designated as the primary Screen. You can manipulate policy there , and then push that changed policy to secondary Screens.
- Proxies allow for authentication of users before they access supported services. This manual includes a proxy example of a Screen supporting `FTP`, `telnet`, and `http` proxies.
- SunScreen 3.2 systems and Windows 2000 systems can interoperate using the IPSec IKE protocol. This manual provides you with the information you need to know to make this feature work properly.

While this manual contains detailed examples of how you might use SunScreen's features. It is beyond the scope of this manual to suggest any particular security policies.

To determine the policy you want to implement, you should first:

- Identify your own security requirements for protecting the integrity and accessibility of your corporate data and computer resources.
- Determine the services you want to support at your site for employees and customers.
- Define the layout for your network and then configure SunScreen to implement this policy.

How SunScreen Works

Figure 1–1 shows where the SunScreen software resides in relation to the network protocol stack. Packets can flow from the network to an application; they can flow through the screen (between segments); or flow out to the network from an application running on the screen. For a detailed description of how SunScreen does Packet Filtering, see the *SunScreen 3.2 Administrators Overview*

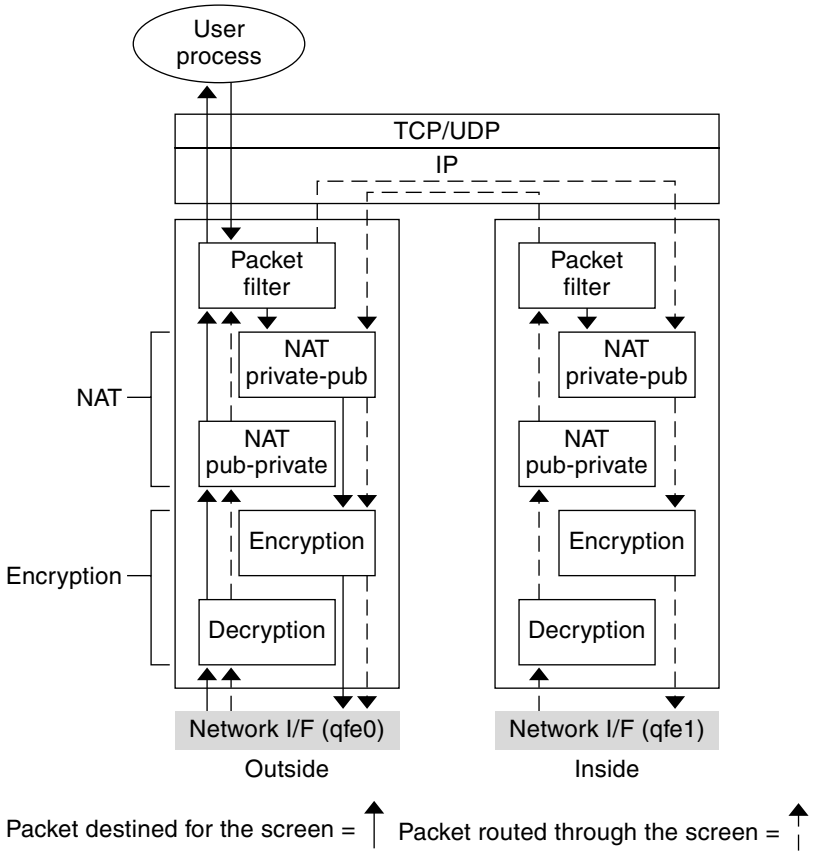
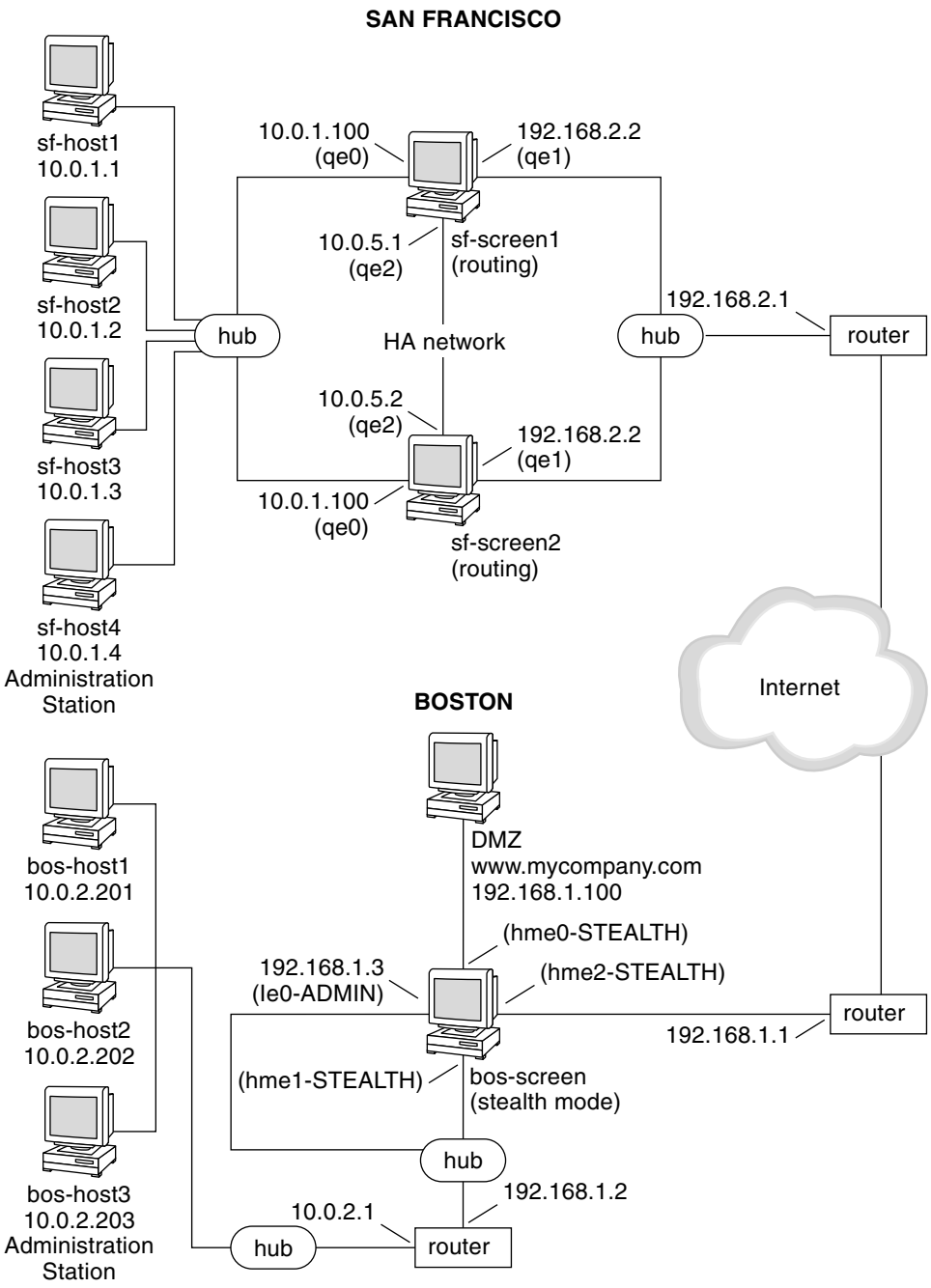
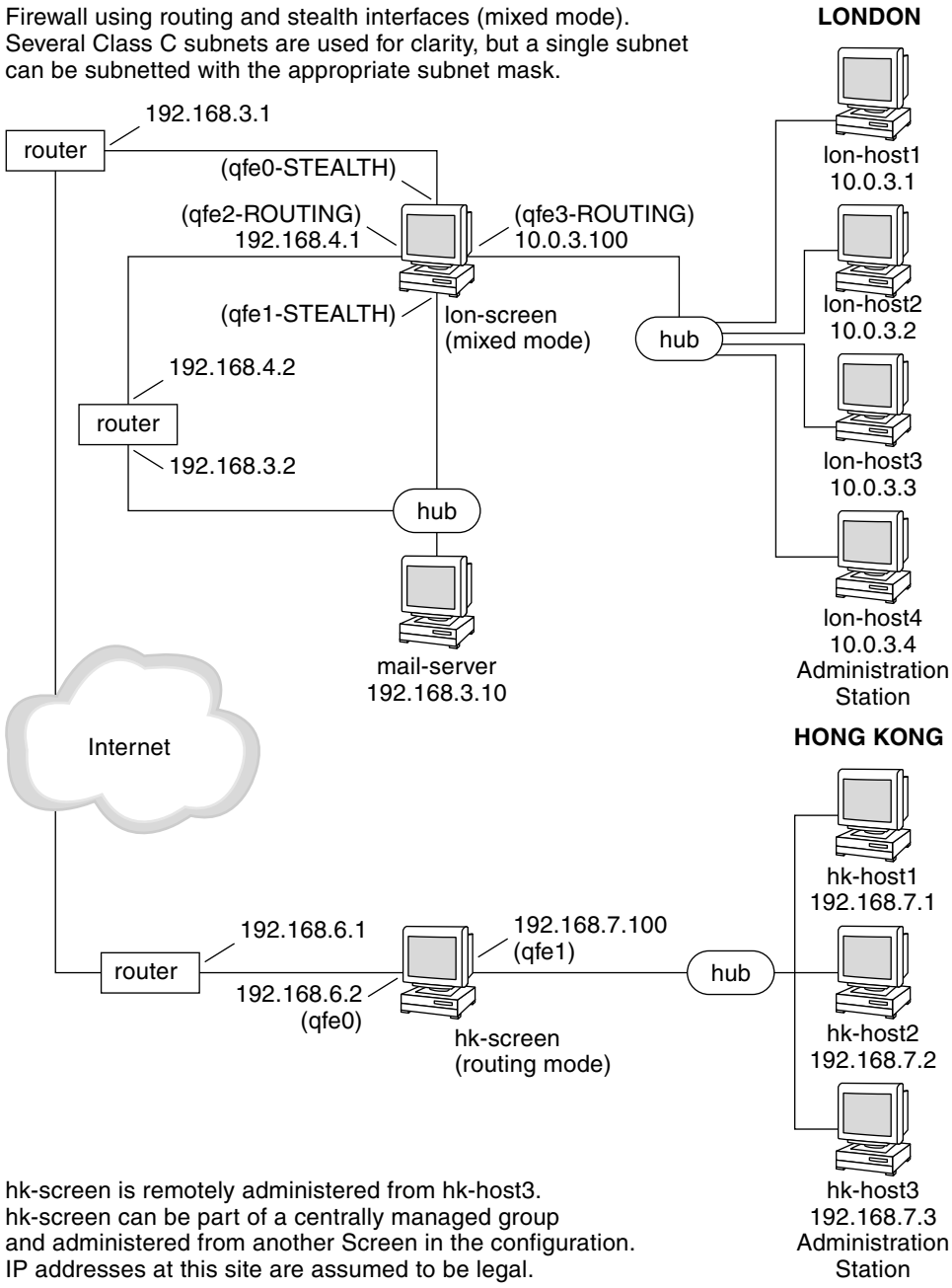


FIGURE 1–1 SunScreen Functions

Network Map

Segments of the sample company network shown in the following figures are used in the configuration examples described in this document.


SAN FRANCISCO
sf-host1
10.0.1.1
sf-host2
10.0.1.2
sf-host3
10.0.1.3
sf-host4
10.0.1.4
Administration
Station
10.0.1.100
(qe0)
192.168.2.2
(qe1)
10.0.5.1
(qe2)
sf-screen1
(routing)
hub
HA network
hub
192.168.2.1
router
10.0.5.2
(qe2)
192.168.2.2
(qe1)
10.0.1.100
(qe0)
sf-screen2
(routing)
Internet
BOSTON
bos-host1
10.0.2.201
bos-host2
10.0.2.202
bos-host3
10.0.2.203
Administration
Station
DMZ
www.mycompany.com
192.168.1.100
(hme0-STEALTH)
192.168.1.3
(Ie0-ADMIN)
(hme2-STEALTH)
router
192.168.1.1
(hme1-STEALTH)
bos-screen
(stealth mode)
hub
192.168.1.2
10.0.2.1
hub
router



The machines used in the examples are assumed to include any required patches or

plug-in software. In your own configurations, you should be familiar with the following topics and which prerequisite you need to satisfy. See the SunScreen manuals for specific information on:

- Using the Netscape Navigator™ browser for administration
- Preparing for installation
- Choosing a certificate
- Dedicating interfaces.

For the purpose of these configuration examples, addresses starting with `192.168` are considered legal, routable, IP addresses, while addresses starting with `10.0` are considered illegal IP addresses. All networks shown assume a class C (`255.255.255.0`) subnet mask. In a real-life configuration, you would replace these IP addresses with your own addresses.

CHAPTER 2

Setting Up Remote Administration in Routing Mode

Typically, you use SunScreen in routing mode if you need a machine to act as both a router and a firewall. In this mode, the interfaces have IP addresses and perform IP routing functions, while the SunScreen software restricts the packet flow between those interfaces. This example shows how you would set up a routing mode Screen and connect it to a remote Administration Station.

Network Example

The example in Figure 2–1 shows the Hong Kong segment of the network. A remotely administered Screen, `hk-screen`, is set up in routing mode with two interfaces (configured with IP addresses on separate subnets). In this example, traffic between the Screen and the Administration Station is encrypted using SKIP. You can find information about using IKE for encryption in Chapter 5 and in the *SunScreen 3.2 Administrators Overview*.

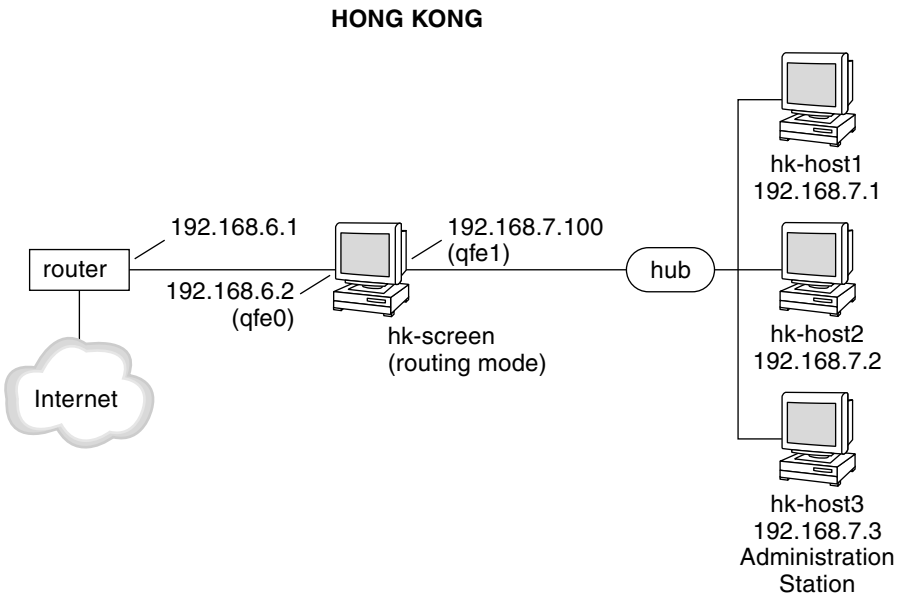


FIGURE 2–1 Hong Kong Segment of the Sample Company Network

Routing Prerequisites

Before you install SunScreen, make sure the machine can route traffic properly:

- Each interface connects to a different subnet
- Network traffic routes correctly between the individual subnets
- System can forward packets between interfaces
- Kernel global variable *ip_forwarding* is set to 1

To set this variable to 1, type:

```
# ndd -set /dev/ip ip_forwarding 1
```

See the `ip(7P)` Solaris man page for more details.

Note – If you are using SunScreen 3.2 Lite, you must set this variable to `0`, or your Screen will be limited to two routing interfaces.

Setting Up Remote Administration with SKIP

Before you begin, verify that the Administration Station can communicate with the Screen. After logging on as `root`, perform the following procedures:

Install the Administration Station Software

1. **On the Administration Station, install the SunScreen Administration Station software.**

   See the *SunScreen 3.2 Installation Guide* for complete information including command line installation. Also check the *SunScreen 3.2 Release Notes*, which may show additional installation issues.

2. **On Administration Station, generate a local certificate ID and set up SunScreen SKIP as follows:**

   a. **Initialize the SunScreen SKIP directories by typing:**

   ```
   #  skiplocal -i
   ```

   b. **Generate the certificate ID by typing:**

   ```
   # skiplocal -k
   ```

   Because the output of `skiplocal -k` is verbose, use the command shown in the next step, `skiplocal -l`, to list the certificate ID you just created in a more clearly understood format.

   c. **List the certificate ID you just created by typing:**

   ```
   # skiplocal -l
   ```

   d. **Write down the certificate ID for use when installing the SunScreen software on the Screen, for example:**

   ```
   c590723af78f869118cd35dee50680a6
   ```

   e. **Add SunScreen SKIP to all the interfaces by typing:**

   ```
   # skipif -a
   ```

   f. **Reboot the system.**

Install the Screen Software

1. **On the Screen, install the SunScreen Screen software.**

   Install the Screen with remote administration. If you use the command line to install the Screen software, make sure that you *do not install* End System SKIP (`SUNWes` and `SUNWesx`) on the Screen.

2. **Use the Administration Station's certificate ID, when prompted.**

3. **Write down the Screen's certificate ID for use in the next section.**

4. **Reboot the Screen upon completion.**

Enable Communication Between the Administration Station and the Screen

Return to the Administration Station and add an ACL using the `skiptool` GUI.

This action allows all hosts not specified by other ACL entries to communicate with the Administration Station system in the clear. Then, the only encrypted traffic will be between this system and the Screen.

Note – These steps can also be accomplished using the `skiphost` command as described in the file `/etc/opt/SUNWicg/SunScreen/AdminSetup.readme`.

---

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

   ```
   # skiptool
   ```

2. **Click the Add button under Host and choose Off.**

3. **Type 'default' as the hostname and click Apply.**

4. **Click the Add button under Host and choose SKIP.**

5. **Type the following information:**

   screenname as hostname (`hk-screen` in this example), `MD5` for Remote Key ID, the Screen's certificate ID for Local Key ID. Use the Administration Station's certificate ID for the local Key ID and the default values for key, traffic, and authentication algorithms

6. **Verify that Access Control is set to Enabled.**

7. **Choose Save from the File menu to make your changes permanent.**

   Enabling SunScreen SKIP allows the Administration Station to begin encrypted communication with the Screen.

8. **Continuing on the Administration Station, start a browser and verify that remote administration to the Screen is working by typing a URL like this one:**

   `http://hk-screen:3852`

   The SunScreen log-in screen for Screen `hk-screen` appears. For your own configuration, replace `hk-screen` with the name of you Screen.

Setting Up Remote Administration with IKE

The following section describes how you would set up a remote administration station using IKE instead of SKIP.

Installing a Remote Administration Station

These instruction apply to using SunScreen on a Solaris—based system only. Because the Solaris operating environment does not yet support IKE, there is no built-in facility for generating IKE certificates on a remote Administration Station. So, you must install the Screen packages as well as the administration packages on your system.

On the Screen

1. **Install the full Screen software. Create a self-signed Screen certificate using the GUI, or use the command line editor, as follows:**

   # **`ssadm certlocal -Iks -m`** *1024* **`-t`** *rsa-sha1* **`-D "C=`***US***`, O=`***Your_Org***`, CN=`***screen_name***`"`**

2. **Export the Screen certificate to a file using the GUI, or the command line editor:**

   # **`ssadm certdb -Ie "C=`***US***`, O=`***Your_Org***`, CN=`***screen_name***`" > /tmp/`***screen_cert***

3. **Import Administration Station certificate using the GUI, or the command line editor and add the Certificate objects into the SunScreen configuration:**

   # **`ssadm certdb -Ia < /tmp/`***admin_cert*

4. **Edit the SunScreen policy for certificates.**

```
# ssadm edit policyname
edit> add certificate admin_cert SINGLE IKE "C=US, O=YourOrg, CN=admin_name"
edit> add certificate screen_cert SINGLE IKE "C=US, O=YourOrg,CN=screen_name"
edit> add address admin_addr HOST ip.address
edit> add accessremote screen "screen_name" USER "admin"  "admin_addr" IPSEC ESP
 ("DES-CBC", "MD5") AH ("SHA1") IKE("DES-CBC", "MD5", 1,
RSA-SIGNATURES, "screen_cert") PERMISSION ALL SCREEN "screen_name"
edit> add screen "screen_name" ADMIN_IP "admin_addr" IKE(screen_cert) RIP
```

Note – The DN must be entered correctly including the space after the commas. Also, no packet filtering rule is required on the Screen.

---

5. **Save and activate policy.**

On the Remote Administration Station

1. **Install the full Screen software**
2. **Create a self-signed Screen Certificate:**

```
# ssadm certlocal -Iks -m 1024 -t rsa-sha1 -D "C=US, O=Your_Org, CN=admin_name"
```

3. **Export the Administration Certificate to a file using the GUI or use the command line editor as follows:**

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

4. **Import Screen Certificate using the GUI or command line editor:**

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

5. **Edit the SunScreen policy for certificates:**

```
# ssadm edit policyname
edit > add certificate admin_cert SINGLE IKE "C=US, O=YourOrg, CN=admin_name"
edit > add certificate screen_cert SINGLE IKE "C=US,O=YourOrg, CN=screen_name"
edit > add address admin_addr HOST ip.address
edit > add address screen_addr HOST ip.address
```

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

```
edit > add rule "remote administration" "admin_addr"
"screen_addr" IPSEC ESP("DES-CBC", "MD5") AH("SHA1") IKE("DES-CBC", "MD5",
 1, RSA-SIGNATURES, "admin_cert", "screen_cert") ALLOW
```

CHAPTER 3

Configuring Network Address Translation (NAT)

A Screen using network address translation (NAT) transparently maps an internal, unregistered IP address to an external, registered IP address. You can configure NAT on a Screen in stealth mode as well as in routing mode although `arp` entries are not needed on a stealth Screen.

Typically, you use NAT for the following situations:

- When adding a previously configured private network to the Internet, or when changing Internet service providers (ISPs).
- When you do not want to renumber all your unregistered addresses.
- To ensure that the internal unregistered addresses appear as public, registered IP addresses on the Internet.
- To hide the addresses of your current private network from the outside world.

There are two types of NAT address mappings, STATIC and DYNAMIC.

- A STATIC mapping sets up a one-to-one relationship between two addresses, and generally (though not exclusively) is used for publicly accessible servers that require direct inbound connections (initiated from outside the Screen).
- A DYNAMIC mapping uses a many-to-one or many-to-few relationship, and ensures that all traffic leaving the Screen appears to come from a single address or group of addresses. You generally use DYNAMIC NAT for outbound connections only (initiated from inside the Screen) but "reverse" NAT rules are allowed.

You should create a table of all addresses that require translation, and determine which addresses require STATIC or DYNAMIC address mappings. Use the worksheets in the *SunScreen 3.2 Installation Guide* to help organize your addresses.

The instructions in this section provide detailed steps about setting up NAT. For more NAT details, see the *SunScreen 3.2 Administrators Guide*; for background information on NAT, see the *SunScreen 3.2 Administrators Overview*.

Network Example

Figure 3–1 (and the instructions that follow) demonstrate how you can configure NAT on a Screen to make hosts on an internal network routable on the Internet.

Assume that host `sf-host1` is a company web server that requires access from the Internet. Use STATIC NAT to translate the private unregistered address to a public, registered address (from `10.0.1.1` to `192.168.2.101` for this example). Use dynamic NAT to translate all other addresses in the San Francisco network to a single, public registered address (`192.168.2.102` in this example).

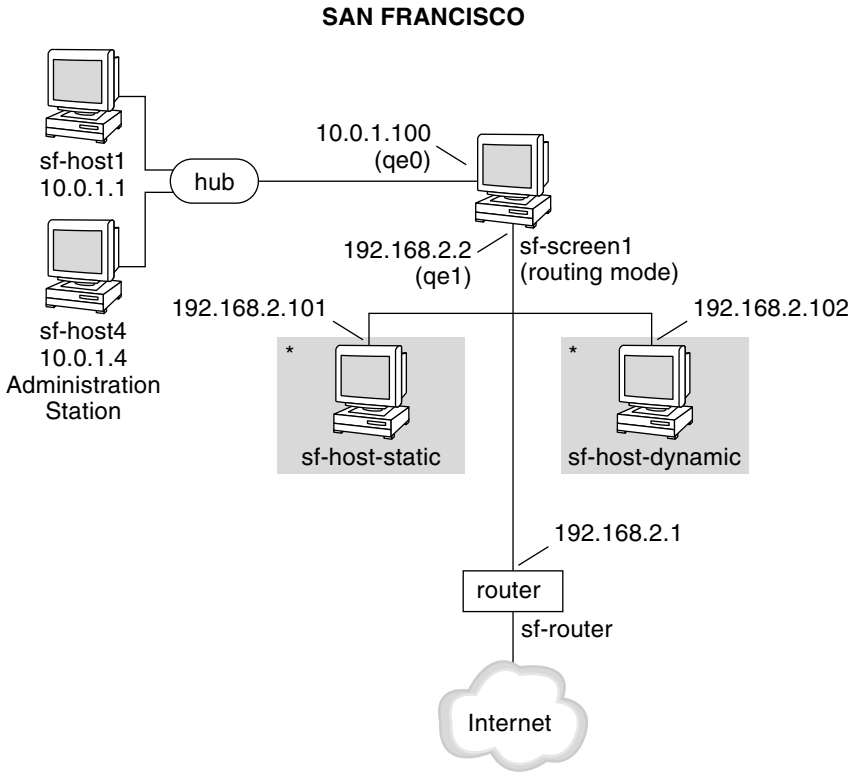


FIGURE 3–1 San Francisco Segment of the Sample Company Network

Static NAT Example

▼ Configure Static NAT

1. **Install and configure the Screen in either stealth or routing mode.**

   In our example, `sf-screen1` is configured in routing mode with `sf-host4` as a remote Administration Station. For instructions on configuring a Screen with remote administration, refer to "Setting Up Remote Administration with SKIP" on page 23.

2. **Create an Address HOST object for the private, unregistered host.**

   In this example, the unregistered host `sf-host1` is defined as `10.0.1.1`.

3. **Create an Address HOST object for the public, registered IP address and give it a name.**

   In this example, the you would name the address object `sf-host-static` and assign it an address of `192.168.2.101`.

4. **Create an Address GROUP object that contains everything but the Screen.**

   In this example this object is defined as `internet-static`. You would create this object by including `*` and excluding `localhost`(the Screen).

5. **Check that you created Packet Filtering rules to allow appropriate traffic to through the Screen.**

   In this example, you would allow http traffic from any host (*) to `sf-host1` through the Screen as shown in the following figure.

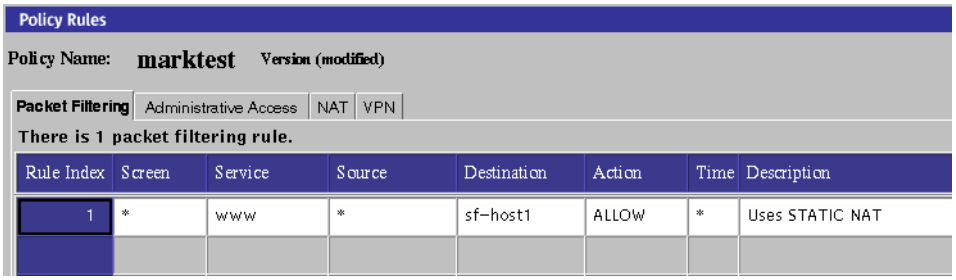


FIGURE 3–2 Rule for HTTP Traffic

6. **Create a STATIC NAT rule to translate the internal address to the legal address.**

   Rule 1 in Figure 3–3 maps internal address `sf-host1` to legal address `sf-host-static`. This rule enables the internal host to initiate connections to any host on the internet (provided they are allowed by packet filtering rules.)

   Because the SunScreen firewall keeps state information about NAT connections, return packets destined for the NAT address (`sf-host-static`) are translated back to the original internal address before entering the internal network

7. **Create a STATIC NAT rule to translate the legal address to the internal address.**

   Rule 2 in Figure 3–3 is needed for hosts on the internet to initiate connections to the internal host. The rule translates the legal address (`sf-host-static`) to the internal address (`sf-host1`) .

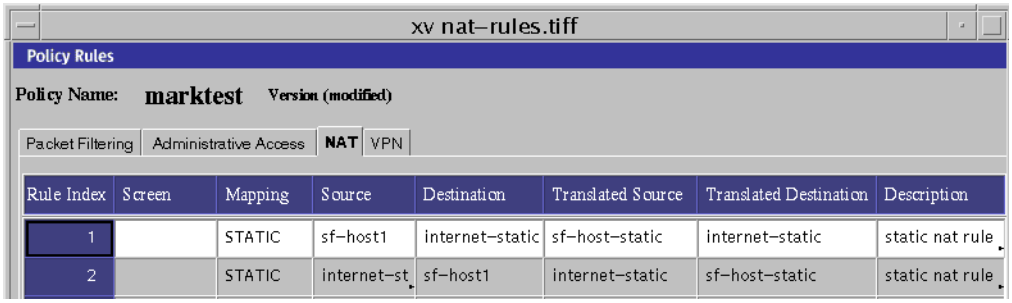


FIGURE 3–3 STATIC NAT Rules

8. **Add an `arp` entry on the Screen so it can respond to ARP requests from the external router.**

Note – If you configured the Screen in stealth mode, this step is not required.

Use the following command as a model.

```
# arp -s translated-ip-addr   screen-ethernet-addr pub
```

where *translated-ip-addr* is the public, registered IP address (`192.168.2.101` for this example) and *screen-ethernet-addr* is the Ethernet address of the external interface of the Screen (`qe1` in this example.)

Run this `arp` command for each legal IP address that the Screen uses for NAT .

Place this command in a start-up script to run each time the system boots because the `arp` entry is only valid until the Screen is rebooted.

The following shows an example of an `arp` start-up script used for STATIC and DYNAMIC NAT (see the following section on DYNAMIC NAT):

```
# /etc/rc2.d/S72sunscreenARP
#!/bin/sh
# startup script example to publish ARP entries
# for IP addresses sunscreen performs NAT on
#
# STATIC NAT mappings
arp -s 192.168.2.101 8:0:20:a3:ec:27 pub
# DYNAMIC NAT mappings
arp -s 192.168.2.102 8:0:20:a3:ec:27 pub
arp -s 192.168.2.103 8:0:20:a3:ec:27 pub
arp -s 192.168.2.104 8:0:20:a3:ec:27 pub
```

9. **Save and activate your policy.**

10. **Verify that connections work to and from the host being translated, and that the translation is actually taking place.**

    For example, run `snoop` both inside and outside the Screen and try a `ping` from the Screen to the router. If the configuration is set up correctly, the result should be that the router is alive, and the `snoop` output should look similar to the following examples:

    Inside the Screen:

```
sf-host1 -> sf-router     ICMP Echo request
sf-router -> sf-host1     ICMP Echo reply
```

    Outside the Screen:

```
192.168.2.101 -> sf-router     ICMP Echo request
sf-router -> 192.168.2.101     ICMP Echo reply
```

Dynamic NAT Example

▼ Configure Dynamic NAT

SunScreen also supports DYNAMIC NAT. In our example, the remaining hosts on the San Francisco network (those not already translated) need access to the internet. However, they do not need to allow inbound connections from the internet. Their source addresses can be translated to a single external legal addresses for this purpose.

1. **Define an Address GROUP object and add all the internal hosts that need to use DYNAMIC NAT to this group.**

   In our example, we define `sf-ten-net` as containing `sf-host2`, `sf-host3` and so forth.

2. **Define an Address HOST object for the private, unregistered hosts.**

   In this example `sf-host-dynamic` is defined as `192.168.2.102.`

Note – DYNAMIC NAT can use a group of addresses when needed. The `sf-host-dynamic` object could be a RANGE or GROUP object in such an instance.

---

3. **Create an Address GROUP object that contains every address that you want to use DYNAMIC NAT but excludes those systems which you do not want to use it.**

   In this example this object is defined as `sf-internal`. You would create this object by including `sf-ten-net` and excluding `localhost` and `sf-host1`.

4. **Create an Address GROUP object that represent systems outside your internal network.**

   In this example, you would create an Address group called `external` that includes `*` and excludes `localhost`, `sf-ten-net`, and `sf-host1`.

5. **Add an ARP entry on the Screen for the legal address, as described in the preceding STATIC example.**

Note – If you configured the Screen in stealth mode, this step is not necessary.

   In this example, `sf-host-dynamic` would need an ARP entry.

6. **Add a DYNAMIC NAT rule to translate the internal address group to the public, registered IP address.**

   In this example, `sf-internal` is translated to `sf-host-dynamic`. Refer to the following figure.

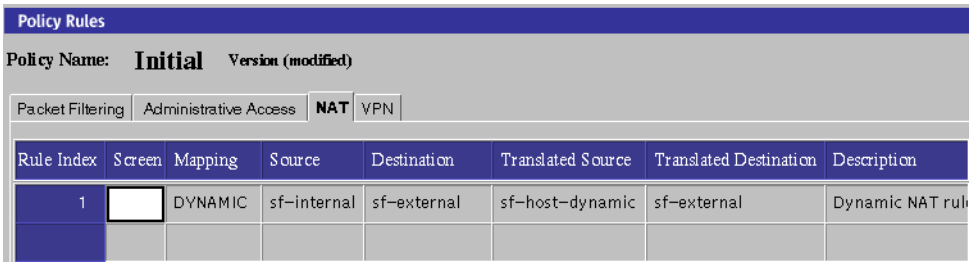


FIGURE 3–4 DYNAMIC NAT Rules

7. **Save and activate your policy**

8. **Verify that connections work from the internal host to the internet.**

   For details, refer to step 10 in "Static NAT Example" on page 29.

CHAPTER 4

Configuring a Stealth Mode Screen

A Screen running in routing mode filters packets passing between subnets on a Solaris system configured as a router. A Screen in stealth mode differs from routing mode in that it partitions a single subnet into two or more parts and filters packets passing between them.

Typically, SunScreen in stealth mode provides you with the following features:

- Filtering interfaces on stealth Screens do not have an IP address.

  Because no IP protocol stack is associated with the filtering interfaces, the Screen is invisible to the network. Therefore, it is very difficult for a potential attacker to know the firewall exists.

  Conceptually, a Screen running in stealth mode is like a bridge that filters IP addresses rather than media access control (MAC) addresses.

- Partitioning a single subnet.

  Each of the filtering interfaces has the identical IP subnet. Because a stealth Screen is not a router, it cannot connect to or pass packets between different subnets. Stealth mode uses Ethernet interfaces only.

  There is no need to reconfigure the hosts where the stealth Screen is inserted into a single subnet. The hosts on this subnet retain the same IP addresses they had before the stealth Screen was inserted.

- Optional hardening of the operating environment to increase the security on the system.

  Hardening of the operating environment removes packages and files from the Solaris operating environment that are not used by SunScreen. That is, hardening prevents network applications, such as `telnet`, from being configured.

Caution – Hardening the operating environment is not reversible. To reverse the hardening requires that you to reinstall both the Solaris operating environment and the SunScreen software.

Note – You should only plumb (configure) one network interface for use as the remote administration ADMIN interface. You set up your filtering interfaces as STEALTH type interfaces using SunScreen.

If you configure a network interface that you later set to stealth mode and the Screen hangs upon activation, reboot the Screen in single-user mode, remove the `/etc/hostname.`*interface_name* file (which unconfigures that interface), and reboot the Screen (follow the procedure for restoring proper operation as shown in the *SunScreen Administrator's Overview).*

Network Example

Figure 4–1 shows the Boston segment of the network. In this diagram, the administration interface is attached to the same subnet that the stealth Screen partitions (it can be attached to any subnet in the configuration). Screen, `bos-screen1`, does not pass packets between its filtering interfaces and the administration interface.

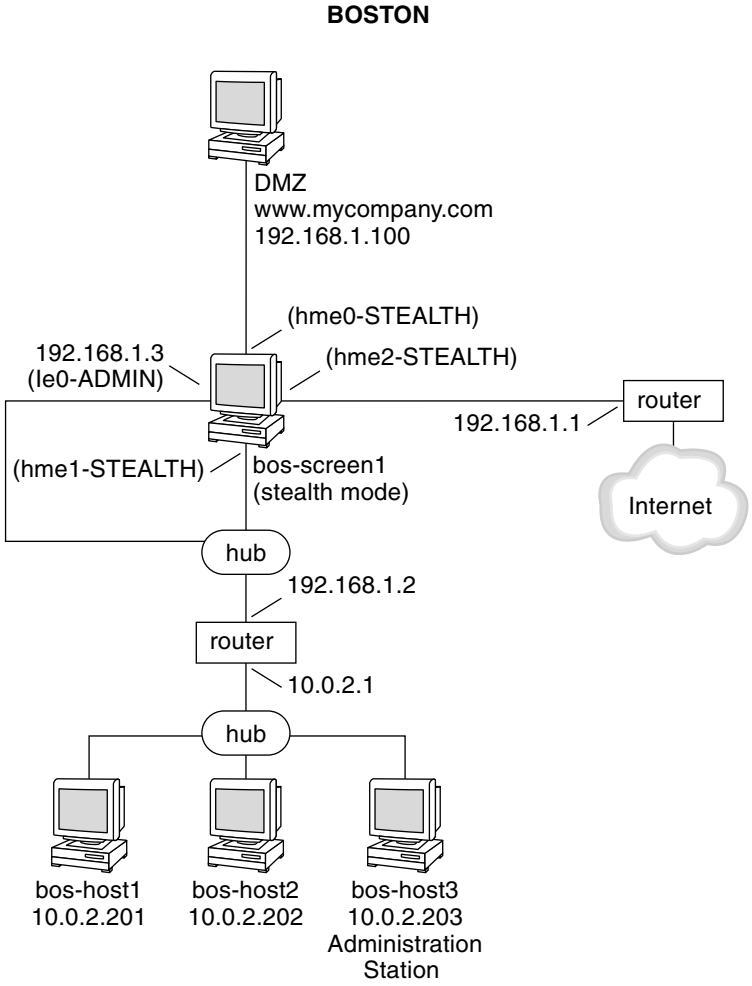


FIGURE 4–1 Boston Segment of the Sample Company Network

Stealth Mode Configuration

The stealth ADMIN interface is restricted to administration traffic over ports 3852 and 3953 only. Typically, this traffic is encrypted using SunScreen SKIP although it is also possible to use IKE. Either method requires the Screen and Administration Stations to have certificates. SunScreen supports:

- Self-signed certificates (that is, Unsigned Diffie-Hellman [UDH] SKIP certificates and X.509 IKE certificates.)
- Certificates signed by certification authority (CA).

See "Basic Encryption Configuration" on page 45 in this manual and also the *SunScreen 3.2 Administration Guide* for more information on generating and using certificates.

Administrative access to the Screen is restricted to systems in a remote access rule using the SunScreen SKIP or IKE identity of that system for authentication. For SKIP, this remote access rule is configured as part of the Custom installation process. For IKE, you must explicitly configure this rule, see "Setting Up Remote Administration with IKE" on page 25 for more information.

▼ Prepare the Screen Machine

1. **On the machine that will be the Screen, install the Solaris operating environment and configure a single interface to enable remote administration of the Screen from an Administration Station.**

   In this example, you would configure an interface named `le0` with the IP address of `192.168.1.3`.

   The Screen is only able to resolve IP addresses using the administration interface. Since the Screen only needs to resolve the IP address of the Administration Station and any SNMP trap receivers, consider configuring `/etc/nsswitch.conf` only to use files for name resolution.

2. **Install the recommended Solaris operating environment patches at this point, especially any Ethernet interface patches.**

▼ Set Up the Administration Station

- **On the Administration Station, install and configure the Administration Station software (For more details, see "Setting Up Remote Administration with SKIP" on page 23 and "Setting Up Remote Administration with IKE" on page 25.)**

▼ Install the Screen Software

1. **On the Screen, install the SunScreen software as stealth mode.**
2. **Harden the Solaris operating environment (optional).**
3. **SKIP Only — Add the Administration Station's certificate when prompted.**

▼ Finish the Administration Station

1. **On the Administration Station, set up communication with the Screen.**

   See "Enable Communication Between the Administration Station and the Screen" on page 24 for a SKIP example .

2. **Reboot the Administration Station and the Screen.**

Note – The Administration Station can only contact the Screen using the administration GUI or the command-line interface; you cannot use `ping` to test the connection to the Screen.

---

3. **On the Administration Station, start a browser and connect to the Screen URL.**

   In this example you would by type:

   ```
   http://192.168.1.3:3852
   ```

▼ Finish the Screen

1. **On the Screen, select the Screen object and define the network that the Screen partitions, as shown in Figure 4–2.**

Caution – Failure to do this step means the Screen will not work correctly.

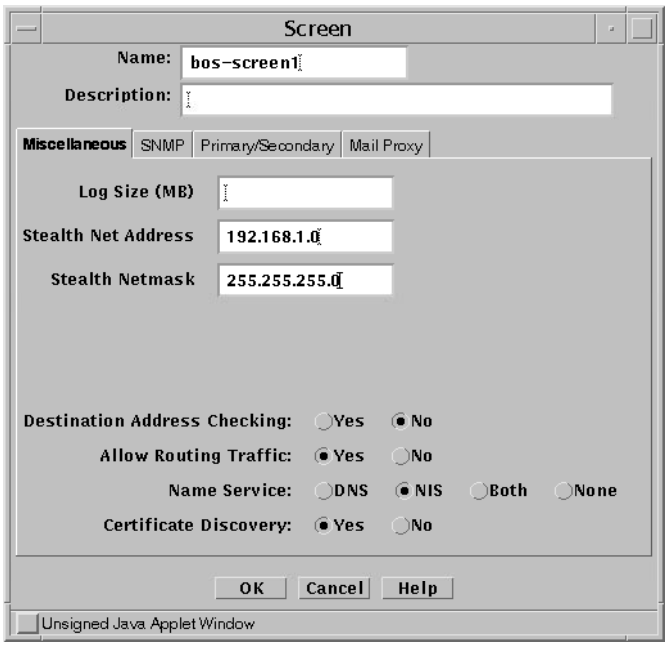


FIGURE 4–2 Network Address Used in the Example

2. **Define the address objects you need to construct your rules.**
   The network shown in this example requires the objects shown in the following table.

TABLE 4–1 Example Address Object Definitions

Name	TYPE	Details
`bos-ten-net`	Range	10.0.2.0 to 10.0.2.255
`DMZ`	Range	`192.168.1.100` to `192.168.1.100`
`192.168.1-private`	Range	`192.168.1.2 to 192.168.1.99`
`192.168.1-public`	Range	`192.168.1.1` to `192.168.1.1`
`Internal`	Group	Include: {`bos-ten-net 192.168.1-private`} Exclude: {}
`Internet`	Group	Include: {*} Exclude: {`Internal DMZ` }

TABLE 4–1 Example Address Object Definitions *(Continued)*

Name	TYPE	Details
`hme0_grp`	Group	Include: {`DMZ`}
		Exclude: {}
`hme1_grp`	Group	Include: {`Internal`}
		Exclude: {}
`hme2_grp`	Group	Include: {`Internet`}
		Exclude: {}

The empty curly braces ({}) mean you exclude nothing. The last three objects are called the Interface Groups. These should contain all the IP addresses of all the hosts that can be reached from that interface. The Screen uses these groups to determine which interface to use when passing a packet.

Note – Be sure the address groups do not overlap.

---

3. **Define the stealth interfaces.**

   In this example, you would define `hme0`, `hme1`, and `hme2` as stealth interfaces. The following figure is an example for `hme0`.

FIGURE 4–3 Stealth Interface Definitions

4. **Define policy rules.**

   These are the same type of Packet Filtering, NAT, and Encryption rules as you would use on a routing Screen.

5. **Save and activate the policy.**

CHAPTER 5

Creating a VPN

Typically, companies use a virtual private network (VPN) when they have offices with networks in more than one location. Usually, those companies want to use an encrypted tunnel through public networks for a secure connection between their own locations or to connect securely with partners. This strategy avoids the need for dedicated lines or any changes to user applications.

You can use a Screen as a VPN gateway on behalf of systems or networks that reside behind the firewall. The Screen then encrypts and encapsulates all packets before they are sent over the Internet. The content of each packet remains private until it arrives at the remote location. Anyone capturing packets between locations will only see encrypted, unreadable packets.

A VPN also enables a site to conceal the details of its own network topology by encrypting the original packets (including their IP headers) and creating new IP headers using addresses specified by the VPN gateway (called tunnel addresses). When these packets arrive at the remote location, the new IP headers are removed. Then, once decryption takes place, the original headers are restored so the packets can reach their intended destination.

SunScreen provides two options for creating a VPN gateway: Use the ENCRYPT action on Packet Filtering rules, or VPN action after defining VPN rules.

- Using the ENCRYPT action on Packet Filtering rules

  In this scenario, you define the encrypted tunnel endpoints as part of a regular Packet Filtering rule. The tunnel endpoints typically are single systems although you can define multiple endpoints using Address ranges and groups. This method provides an easy way to accommodate requests for encrypted access between a few systems. The limitations of this method are:

  - Your rulebase can become very complicated if you add many separate encryption rules.
  - If the systems referenced by these rules change in anyway, you might have to edit each Packet Filtering rule to accommodate the changes.

- Each Packet Filtering rule typically requires that you specify certificates for each system referenced by the rule. Certificate management can be a complex task if you are referencing more than a few systems.

This chapter provides two examples of a VPN created using Packet Filtering rule with the ENCRYPT action. In the first example, "Basic Encryption Scenario" on page 44, a simple VPN exists between two systems, each behind a routing Screen, over the Internet . The second example, "Advanced Encryption Scenario" on page 52, is a more elaborate scenario where one Screen is in stealth mode and the other is a routing mode Screen.

- Using VPN Action After Defining VPN rules

  VPN Rules are a convenience that allows you to easily define and reference a large number of systems or networks using a single VPN name. First, you create VPN rules which define your tunnel endpoints and give the definition for a VPN name. Then, you use the VPN name as part of a Packet Filtering rule. This method is particularly convenient where you are referencing groups of networks as opposed to groups of systems. Then, if the topographical details of a network changes, you only have to modify the related VPN rules and not the Packet Filtering rules. Since you only need one certificate for each VPN rule, certificate management is much easier.

  "VPN Rules Scenario" on page 62 is an example of a VPN using VPN rules. In this example, the Screens are running in routing mode.

Basic Encryption Scenario

This example shows how you would create an encrypted tunnel between two systems, each behind a routing Screen. Figure 5–1 shows a VPN connecting the San Francisco and Hong Kong segments of the network. In the diagram, an encrypted tunnel across the Internet exists between Screens `sf-screen` and `hk-screen`. The Screens encrypt and decrypt traffic on behalf of the systems behind them (`sf-host1` and `hk-host1` in this example).

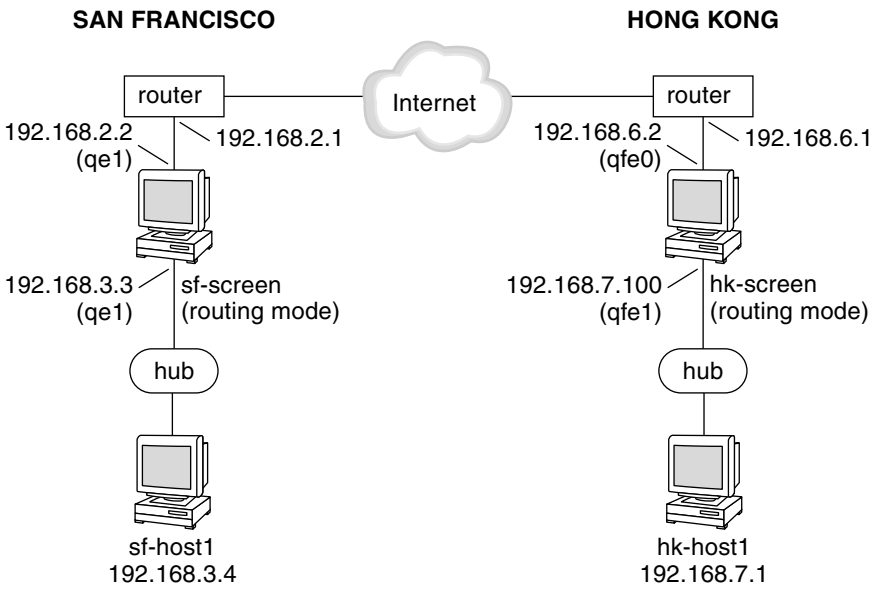


FIGURE 5–1 San Francisco and Hong Kong Segments of the Sample Company Network

Basic Encryption Configuration

This example presumes you have installed both screens in routing mode. The Screens used in this example are called `sf-screen` and `hk-screen`.

Note – The IKE portion of this example uses certificates but you could substitute IKE preshared keys if appropriate. See REFERENCE for an example of using preshared keys; the example uses a Screen and a Windows 2000 system but the Screen portion is the same.

▼ Create Address Objects on Both Screens

See the *SunScreen Administration Guide* for more information on creating Address objects.

1. **Define an Address object on each Screen for the other Screen**

   In this example, on `sf-screen` you would create an Address object to represent `hk-screen` and vice versa.

   In this example, both Screens are routing Screens, so the addresses of these objects are the IP addresses of their interfaces nearest the Internet (`192.168.6.2`) for `hk-screen` and `192.168.2.2` for `sf-screen`.

2. **Define Address objects on each Screen for the systems using encryption.**

   In this example, you would create Address objects named `sf-host1` and `hk-host1` on each Screen.

▼ Create a Certificate Object for Each Screen

1. **Creating a SKIP certificate – If you installed your Screen with Remote Administration, you already have a SKIP certificate. If not, see the following steps for details on creating SKIP Certificate objects.**

   a. **In the GUI Common Objects panel, select Certificate->Generate SKIP UDH. The Generate Certificate window appears.**

   b. **Fill in the required fields and generate the certificate as shown in the following figure. For details on the screen fields , see the** *SunScreen Administrators Guide* **or the window online help.**

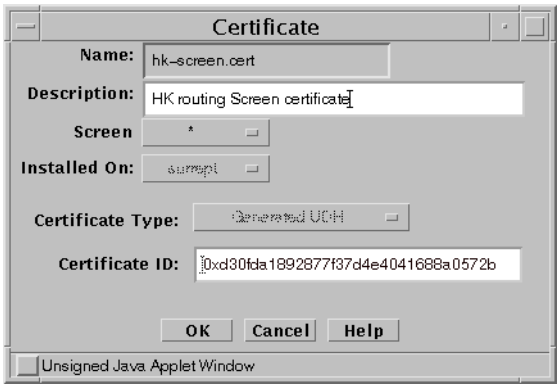


FIGURE 5–2 SKIP Generate Certificate window

2. **Creating an IKE certificate – use the following steps to generate an IKE Certificate object.**

   a. **In the GUI Common Objects panel, select Certificate->Generate IKE certificate. The Generate Certificate window appears.**

b. Fill in the required fields and generate the certificate as shown in the following figure. For details on the screen fields , see the *SunScreen Administrators Guide* or the window online help.

FIGURE 5–3 Generate IKE Certificate Window

3. (IKE Only) Export the IKE certificate.

a. In the GUI Common Objects panel, select Certificate, then click the Search button.

b. Select `hk-screen.cert` from the list of Certificate objects and click Edit

FIGURE 5–4 Export Certificate Window

c. When the Edit Certificate window appears, click Export Certificate

d. When the Export Certificate window appears, you have two choices:

- Select the window contents and paste them into either a file or a mail message.
- Save the contents into a file directly from this window. This method requires that you have a Java plug-in installed that supports local file operations.

e. Move the exported certificate file to the other Screen.

▼ Install Each Screen's Certificate Object on the Other Screen.

1. Installing SKIP certificates

a. In the GUI Common Objects panel, select Certificate->Associate->SKIP Certificate. The Associate SKIP Certificate window appears.

b. Specify a name for the certificate and specify the certificate's MKID.

See

Note – Make sure that CDP is enabled on each Screen object.

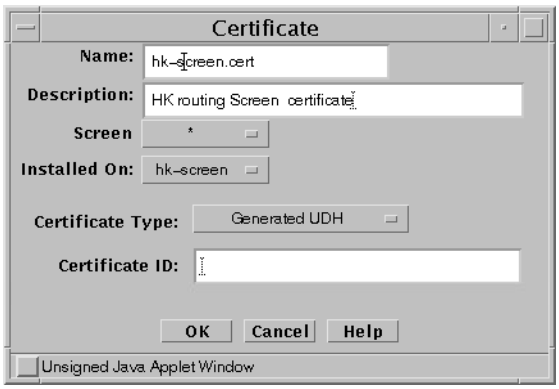


FIGURE 5–5 Associate SKIP Certificate Window

2. Installing IKE certificates

a. In the GUI Common Objects panel, select Certificate->Import IKE Certificate. The Import IKE Certificate window appears.

FIGURE 5–6 Import IKE Certificate Window

b. After filling in the Name field, you can either browse for the certificate file (requires Java plugin) or paste the file contents into the Screen.

c. When you have specified the file, click Install Certificate.

d. Add the new certificate to the appropriate verified IKE Certificates group.

There are reserved Certificate groups for trusted manually- generated (IKE manually verified certificates) and CA-generated IKE (IKE root CA certificates) certificates. This example uses manually-generated IKE certificates so you would add the IKE certificate on each Screen to the IKE manually verified certificates group as shown in the following figure.

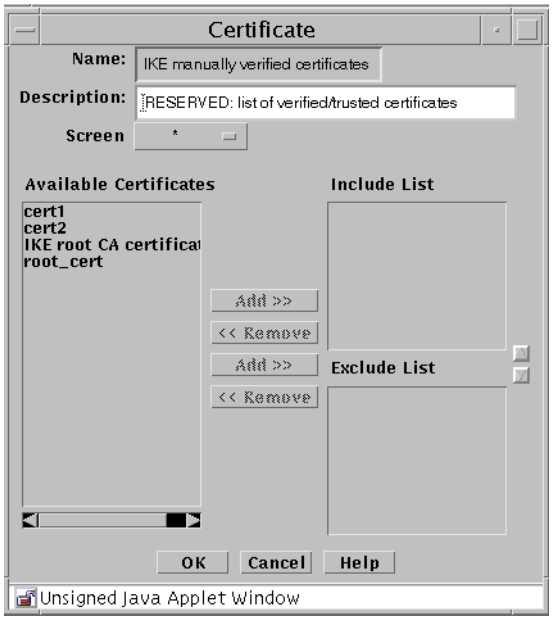


FIGURE 5–7 Adding IKE Certificate to Group

▼ Create Packet Filtering Rules with the ENCRYPT action

On each Screen, add a Packet Filtering rule to encrypt traffic between the two Screens; step 8 in the Advanced Encryption scenario shows you how to use the Rule Definition and Action Details windows. Note that one difference between the Advanced and Basic examples is that this Basic example does not use a tunnel address.

1. **On each Screen, edit the active policy or create a new policy.**

2. **Click Add New Rule.**

3. **When the Rule Definition window appears, specify the Service, Source Address, Destination Address, and Action (ENCRYPT).**

   Go to the Action Details screen appropriate for the encryption method (SKIP or IKE).

4. **When the Action Details window appears, choose the parameters that are appropriate for your encryption method (IKE or SKIP). These parameters must match on each Screen.**

   a. **Specify the Source and Destination Certificates.**

      For example, the `sf-screen` certificate is the Source Certificate on `sf-screen` and the Destination Certificate on `hk-screen`.

   b. **For SKIP – Specify the Key, Data, and MAC algorithms.**

      Also, specify source and destination tunnel addresses if you are using them (for a Stealth Screen for example).

   c. **For IKE – Specify the ESP and/or the AH. Also specify the Encryption Algorithm, Hash Algorithm, and Oakley Group (also known as the DH Group). Specify the Authentication Method and make sure that it matches the certificate Encryption Type.**

      For example, if you selected `rsa-sha1` or `rsa-md5` as the certificate Encryption type the select `RSA-SIGNATURES` as the Authentication Method. Similarly, if you chose `dsa-sha1` as the certificate Encryption type, use `DSS-SIGNATURES` as the Authentication Method.

   d. **For IKE — On the Option tab specify Mode and related parameters.**

      Your choices are Tunnel or Transport mode. Tunnel mode encapsulates and encrypts the entire packet including the IP header for maximum security. Transport mode encapsulates and encrypts only the data portion of the IP packet resulting in smaller packets and potentially better throughput as the Screen is relieved of the overhead of decrypting the IP header.

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

6. **On each Screen, save and Activate the policy.**

Note – SKIP Only – The Greenwich Mean Time (GMT as displayed by `env TZ=GMT date`) must be synchronized between SKIP peers. When Screens are located in different parts of the world, you should set the time for that part of the world. Also, set the TimeZone for that part of the world. That is, the local time that is corrected with the TimeZone must be the same on both machines. You can check the time using the `date -u` command.

Advanced Encryption Scenario

Figure 5–8 shows the Boston and Hong Kong segments of the network. In this example, a VPN will be configured between the Boston and Hong Kong offices. It shows tunnel addresses between the stealth Screen (`bos-screen`) and the routing Screen (`hk-screen`). SunScreen SKIP or IKE encrypts the entire original packet, including the IP header, and inserts a new IP header. The new IP header uses either the same addresses as the original packet or different (tunnel) addresses.

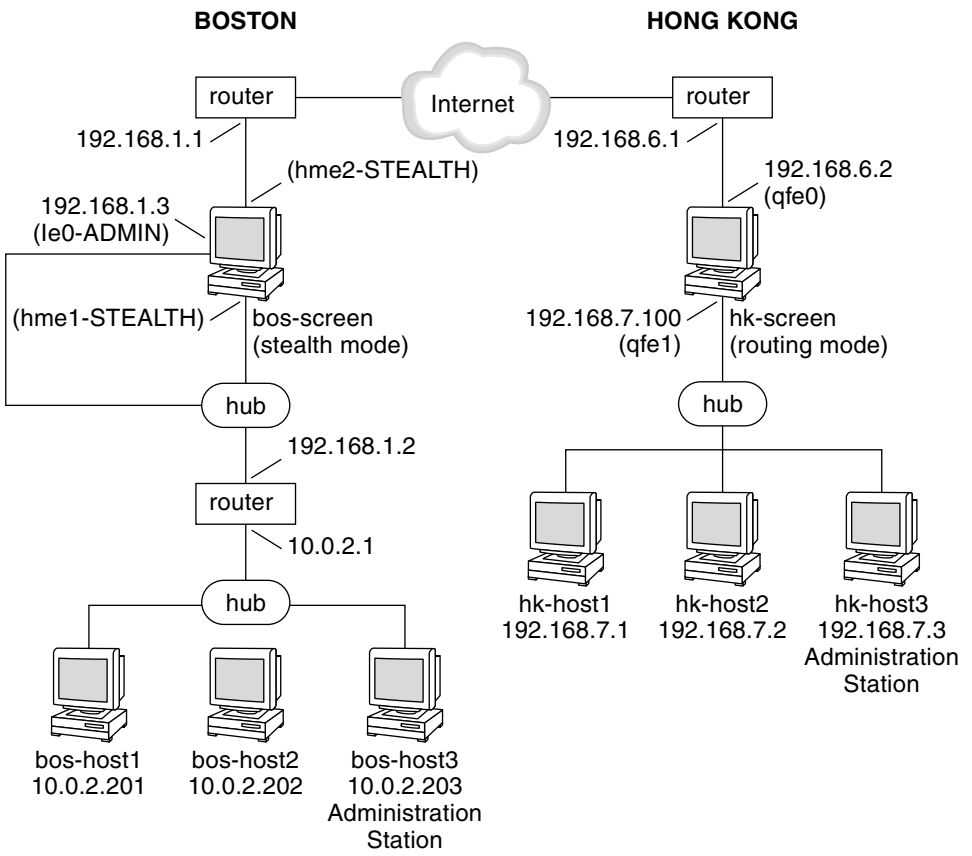


FIGURE 5–8 Boston and Hong Kong Segments

The hosts in Boston have non-routable addresses (`10.0.2.20x` in this example), so a tunnel address is used to hide these addresses. The stealth Screen in Boston (`bos-screen1`) has no IP addresses on its filtering interface so a tunnel address must be added to the `192.168.1.0` subnet. When the Screen in Hong Kong inserts a new IP header on packets destined for Boston, it uses this tunnel address on and routes the packet over the Internet to the Boston router. Although `bos-screen` does not have an IP address, it responds to ARPs from the Boston router for the tunnel address so the packets from `hk-screen` are passed to `bos-screen`. There, they are decrypted and, if the Packet Filtering Rules allow, are passed on to the Boston network.

Although the hosts in Hong Kong have routable addresses, a tunnel address is also used to hide the Hong Kong network topology. this example uses the IP address of the Screen network interface nearest the internet (192.168.6.2) as the tunnel address.

Encryption and decryption are done by both `hk-screen` and `bos-screen`. Thus, if some tool like `snoop` was used to show the packets on the Internet, only encrypted IP

packets would appear (Protocol 57 for SKIP, Protocol 50 for ESP and 51 for AH in IPSec) with the tunnel address as the source and the destination. If someone ran `snoop` or some tool to capture packets on the inside of either Screen they would find the packets unencrypted and using their original IP addresses.

Advanced Encryption Configuration

▼ Preliminary Steps

1. **Install the SunScreen software on the Screens.**

   In this example, you would install `bos-screen` as a stealth Screen (see Chapter 4) and `hk-screen` as a routing Screen. See the *SunScreen 3.2 Installation Guide* for installation details.

2. **Make sure both Screens have a local certificate of the same type (SKIP or IKE) and modulus. If they do not, generate a certificate.**

   In this example, both Screens were installed using remote administration, so the installation process generated SKIP certificates for them. The default name for this SKIP certificate is *screenname*`.admin` (For example: `bos-screen.admin`).

   If you need to generate an IKE certificate for a Screen, see step 2 in "Create a Certificate Object for Each Screen" on page 46 for an example.

3. **Set up an open policy on both Screens and confirm that they can communicate.**

▼ Configure the Stealth Mode Screen

In this example, the stealth Screen is `bos-screen`.

1. **Define the tunnel address of the Screen .**

   This address is the IP address used to send packets over the Internet. The tunnel address should be on the local network (`192.168.1.100` in this example). For this example, define an Address object on `bos-screen` called `bos-tunnel` and give it an IP address of `192.168.1.5`.

2. **Define an Address object for the other Screen in the VPN configuration .**

   In this example, `hk-screen` is a routing Screen, so the address of this object is the IP address of the interface nearest the Internet (`192.168.6.2`).

Note – Optionally, you can define a separate tunnel address for `hk-screen` as well.

3. **Define Address objects for the networks behind both Screens.**

   This example uses Address objects called `bos-net` and `hk-net`.

4. **Edit the Address GROUP object for the interface nearest the Internet and make sure that the definition contains the tunnel address object .**

   In this example, the interface nearest the internet is `hme2`. The Address GROUP object for that interface is `hme2-grp`. So, for this example, `hme2-grp` must contain `bos-tunnel`.

5. **SKIP Only – Edit the Screen object and make sure that Certificate Discovery is selected.**

6. **Edit the Interface object for the interface nearest the Internet (`hme2`.)**

   Fill in the Router IP Address field of the Interface definition for `hme2` with the address of a default router on this network (`192.168.1.1`) for this example. See Figure 5–9. The stealth Screen is actually generating packets with a source IP address set to the tunnel address, but it has no routing table (because it is not a router) . Therefore, it needs to send the packets to a router that knows the location of `hk-screen`.

FIGURE 5–9 Interface Definition Screen

7. **Add a Certificate object for the other Screen.**

   For this example, create a Certificate object `hk-screen.cert`.

8. **Add a rule to encrypt the traffic between the two Screens.**

   Define an ENCRYPT rule as shown in Figure 5–10 to encrypt traffic between the two networks (`bos-net` and `hk-net` in this example.)

   This example uses Common Services, but the actual services you use should reflect your own security policy.

FIGURE 5–10 Rule Definition Window

After selecting the ENCRYPT Action (or by clicking the Action Details button), the Action Details window appears. Figure 5–11 shows the default Action Details window which includes the parameters required to configure a SKIP tunnel.

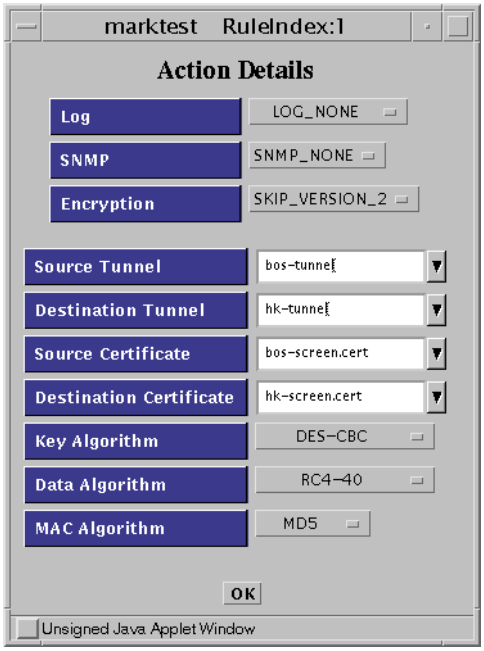


FIGURE 5–11 Rule Index, Action Details Window (SKIP)

To reach the IKE Action Details windows, you must choose IPSEC IKE from the Encryption list.

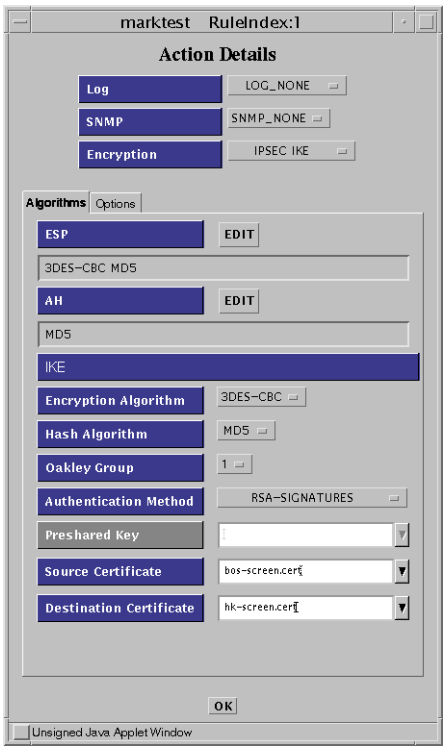


FIGURE 5–12 Rule Index, Action Details Window (IKE Algorithms)

Click on the Options tab to specify the certificates for the screens and the tunnels.

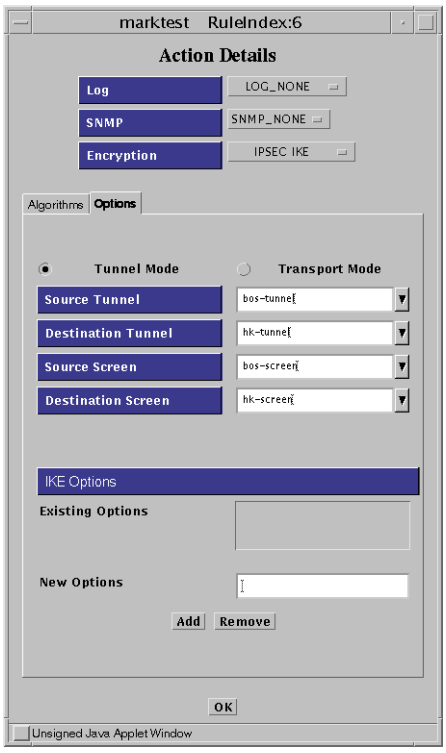


FIGURE 5–13 Rule Index, Action Details Window (IKE Options)

After you enter all the required parameters, click OK to save the information. This action returns you to the Rule Definition window.

9. **In the Rule Definition window, click OK to complete the addition of this rule.**

   Figure 5–14 shows two ENCRYPT rules. The first rule lets you initiate encrypted connections from `bos-net` to `hk-net` establish connections from `hk-net` to `bos-net`, you need to add a second rule. Be sure to reverse the source and destination addresses and the certificates.

10. **Save and activate the policy.**

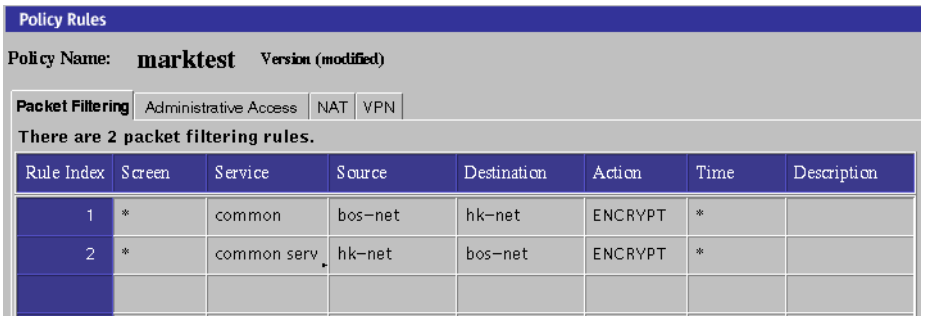


FIGURE 5–14 Encryption Configuration

Note – SKIP ONLY — The Greenwich Mean Time (GMT) (as displayed by `env TZ=GMT date`) must be synchronized between SKIP peers. When Screens are located in different parts of the world, you should set the time for that part of the world. Also, set the TimeZone for that part of the world. That is, the local time that is corrected with the TimeZone must be the same on both machines. You can check the time using the `date -u` command.

▼ Configure the Routing Screen

In this example, `hk-screen` is the name of the routing mode Screen.

1. **Define an Address object for the other Screen in the configuration.**

   The other Screen (`bos-screen`) is a stealth Screen. Therefore, the address of this object is the tunnel address `bos-tunnel`. You have to create the same Address object here as exists on `bos-screen`.

2. **Define Address objects for the networks behind both Screens.**

   In this example, the objects would be `bos-net` and `hk-net`.

3. **SKIP ONLY — Edit the Screen object and make sure that Certificate Discovery is selected.**

4. **Add the Certificate object for the other Screen.**

   Create an Certificate object called `bos-screen.cert`. See "Create a Certificate Object for Each Screen" on page 46 for more information on creating certificates.

5. **Add a rule to the configuration to encrypt the traffic between the two Screens.**

   step 8 in the previous section shows the parameters used.

6. **Save and activate the policy.**

VPN Rules Scenario

Figure 5–15, shows a VPN connecting the San Francisco and Hong Kong segments of the network. In the diagram, an encrypted tunnel across the Internet exists between Screens `sf-screen` and `hk-screen`. The Screens encrypt and decrypt traffic on behalf of the systems behind them, for example `sf-host1` and `hk-host1`.

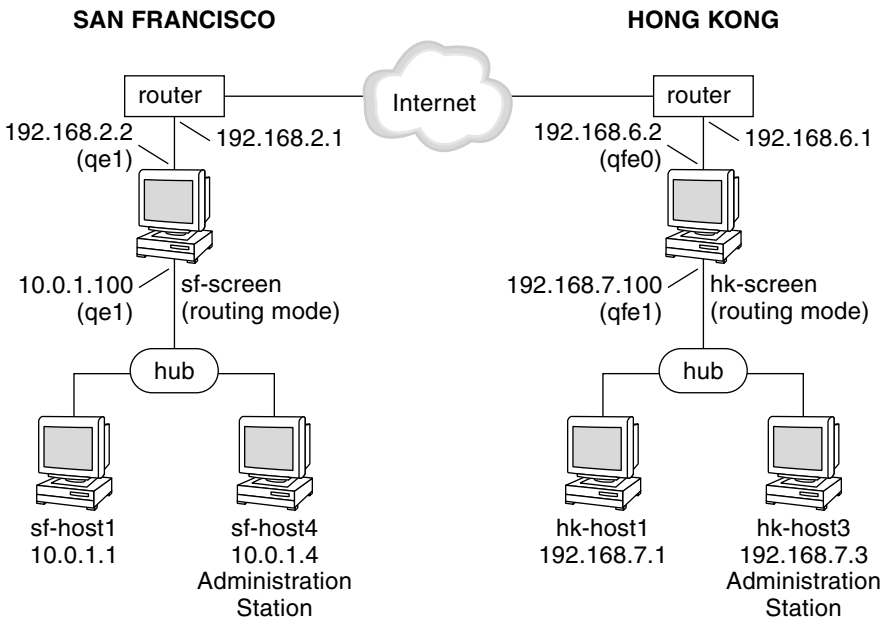


FIGURE 5–15 San Francisco and Hong Kong Segments of the Sample Company Network

This network diagram does not really illustrate a scenario where using of VPN rules would enhance convenience. Typically, a scenario including VPN rules would contain a much more complex set of networks on either side. For the sake of brevity, this example only contains two gateways, each with two systems behind them. The steps to create a VPN using VPN rules however would be similar for a VPN with a large number of Gateways and systems.

Using VPN Rules

▼ Configure the VPN

To configure a VPN like the preceding network example, use the following steps:

1. **Install the SunScreen software on both Screens .**

   The two routing-mode Screens in this example are named `sf-screen` and `hk-screen`.

2. **Add each Screen's certificate object to the other Screen**

   If the Screens were installed using the SunScreen Installer program, they should already have local SKIP certificates named `sf-screen1.cert` and `hk-screen1.cert`, generated when the Administration Stations were set up. If you are using a Screen that does not yet have a certificate, you need to manually generate a SKIP or IKE certificate using the Common Objects panel. See "Create a Certificate Object for Each Screen" on page 46 in "Basic Encryption Configuration" on page 45 for an example of creating certificates.

3. **Ensure that each Screen includes Address objects for the other Screens and systems.**

   In this example, you would need to create the following Address objects:

   - `hk-screen` (should be address for outside IP address of this Screen)
   - `sf-screen` (should be address for outside IP address of this Screen)
   - `hk-host1` (can be part of a group or range)
   - `sf-host1` (can be part of a group or range)

4. **Use the VPN Rules to add entries for the systems in your VPN.**

   Under Policy Rules, click the VPN tab and add entries for each host in your VPN. This example requires entries for `sf-host1` and for `hk-host1`). Figure 5–16 (SKIP) and Figure 5–17 (IPSEC/IKE) show what the VPN rule definition dialog box might look like when adding the entry for `sf-host1`.

   - SKIP VPN Definition

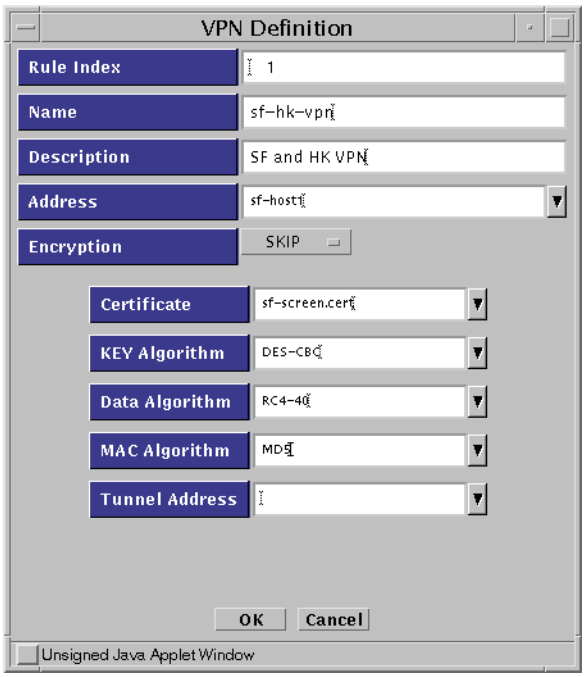


FIGURE 5–16 SKIP VPN Definition Dialog Box

Note – In this example, the entry in the Address field (`sf-host1`) is a single system. Typically, this entry would be either an address group or an address range defining all the systems on the San Francisco side of the gateway which are going to use encryption.

- IKE VPN definition

  The Name, Address, Encryption, Algorithms, Oakley Group, Authentication Method and Certificate are required for each entry. You specify tunnel addresses on the Options tab.

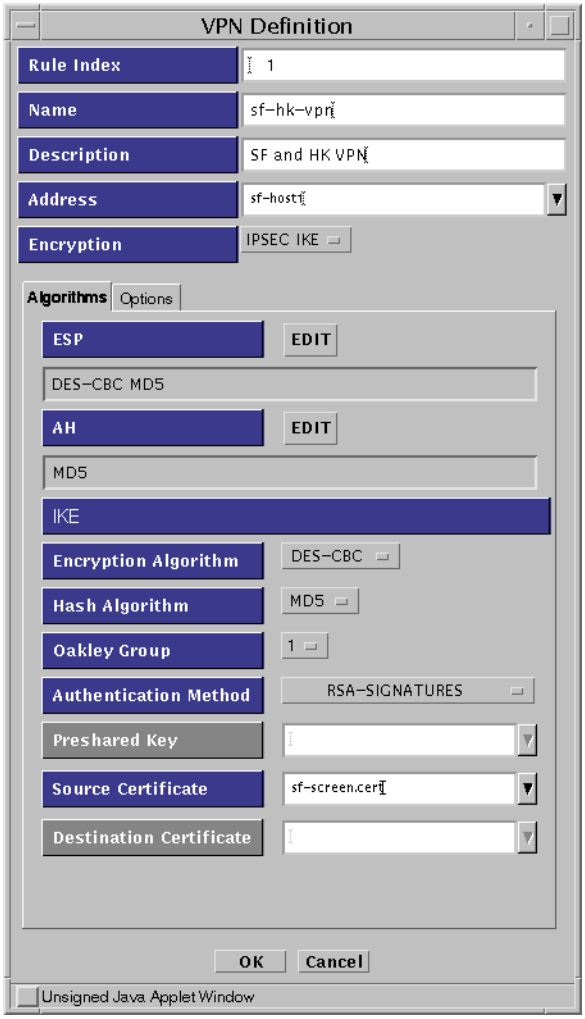


FIGURE 5–17 IKE VPN Definition Dialog Box

Once you complete the VPN definitions for `sf-host1` and `hk-host1`, the VPN tab (under the Policy Rules section of the administration GUI) should look like Figure 5–18. Note that the two entries contain the same name (`sf-hk-vpn` for this example).

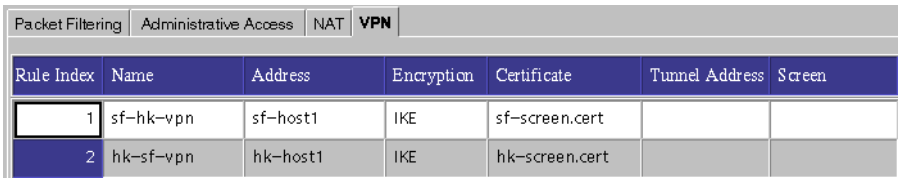


FIGURE 5–18 VPN Tab, Under Policy Rules

Note – All entries associated with a particular VPN must have the same VPN name. The VPN name is referenced again when you create the packet filtering rules. They only accept a packet if both addresses in the IP header are associated with the same VPN.

---

5. **Add a new Packet Filtering rule that uses the VPN name:**

   In this example, the following steps would occur on Screen `sf-screen1`.

   Complete the information as needed, and select VPN as the action.

Note – Use an "`*`" for the source and destination addresses (at least for testing). This enables any packet that reaches this rule, *and* has both source and destination in the specified VPN, to be securely sent to the remote site.

---

6. **The Action Details window appears and prompts you to supply a VPN.**

   Enter the VPN name you created in step 4 (`sf-hk-vpn`) as shown in the dialog window in Figure 5–19.

FIGURE 5–19 Initial Rule Index Dialog Box

7. **Save and activate the policy.**

8. **Repeat step 4, step 5, and step 7 on the other Screen (in this example `hk-screen`.)**

9. **Test the VPN Gateway.**

   You can easily test the configuration by creating a VPN packet-filtering rule that enables ICMP traffic to pass through the VPN, and then running a `ping` between protected hosts (`sf-host1` and `hk-host1`.)

   The following examples show the results of running `snoop` on the network in San Francisco, Hong Kong, and out on the Internet, the results would be as follows:

   Inside either the San Francisco or Hong Kong Screen:

   ```
   sf-host1 -> hk-host1   ICMP Echo request
   hk-host1 -> sf-host1   ICMP Echo reply
   ```

   Outside the Screen on the Internet:

   ```
   sf-screen -> hk-screen IP D=192.168.6.2 S=192.168.2.2 ...
   hk-screen -> sf-screen IP D=192.168.2.2 S=192.168.6.2 ...
   ```

CHAPTER 6

Using High Availability (HA)

This chapter provides step by step instructions for setting up SunScreen with High Availability (HA). You can configure SunScreen HA in either Stealth mode or Routing mode with the same level of redundancy. The steps to configure a Screen are nearly identical in either mode. For more details on using the GUI to configure HA, see the *SunScreen 3.2 Administration Guide*. For background technical information about HA, see the *SunScreen 3.2 Administrators Overview*.

Note – When configuring HA in routing mode, the machine designated as the secondary Screen should have it's screening interfaces physically disconnected from the network until after you configure HA on the primary Screen and activate its.

Network Example

Figure 6–1 shows the Boston segment of the network. In this diagram, two stealth-mode Screens, `bos-screen1` and `bos-screen2`, use HA. Figure 6–2 shows a network with two routing-mode Screens in an HA cluster.

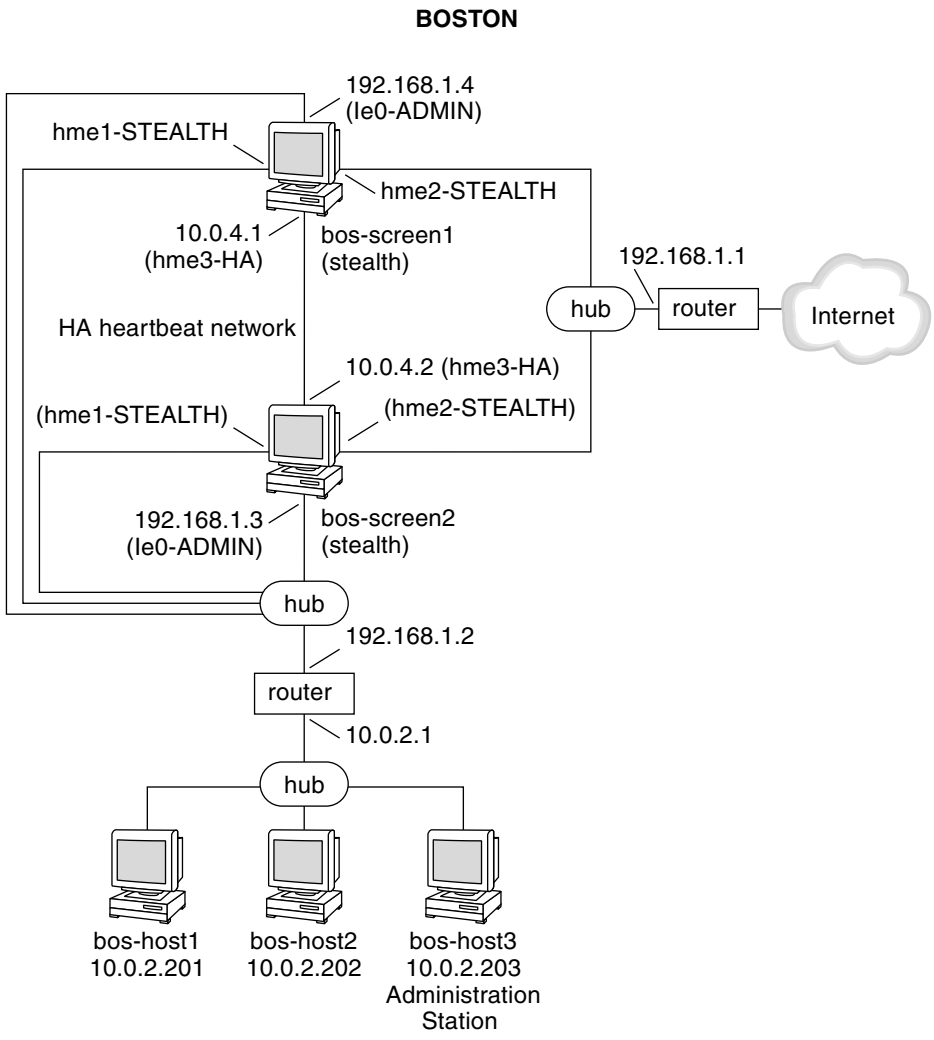


FIGURE 6–1 Stealth Mode HA Cluster

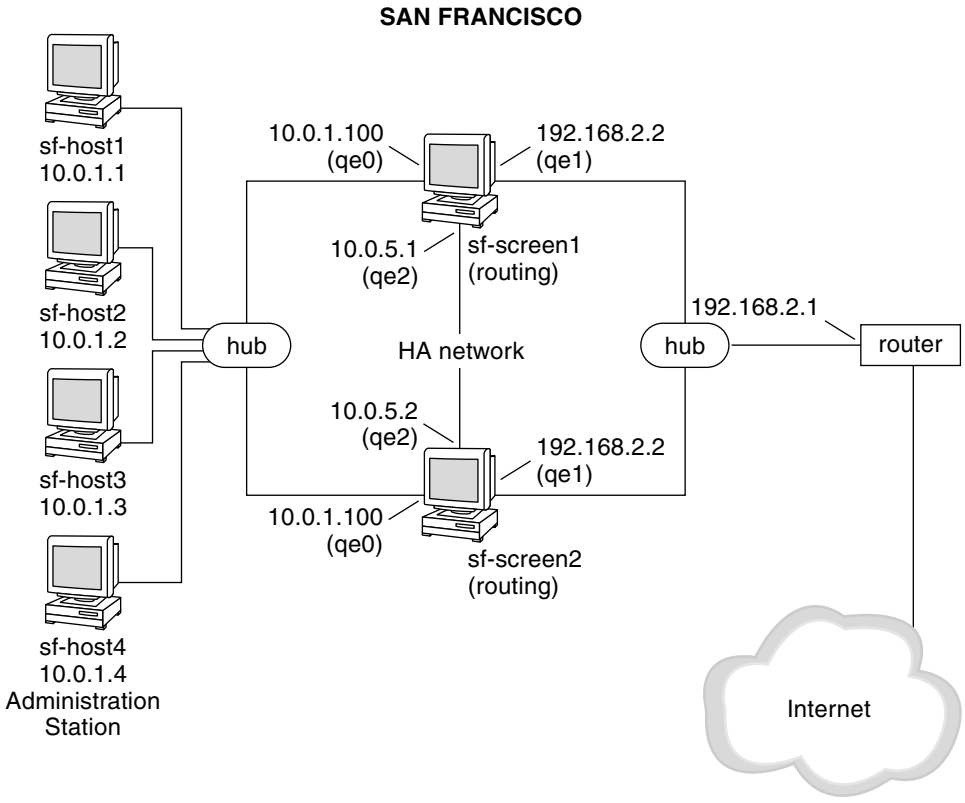


FIGURE 6–2 Routing Mode HA Cluster

Setting Up the HA Screens

This section explains how you prepare either stealth-mode or routing-mode Screens to run HA.

Note – The Screens in an HA cluster must have identical network interfaces. All Screens in the HA cluster must be the same type; either stealth or routing.

Preparing Stealth Mode Screens for HA

The first step when defining an HA cluster is to properly configure the necessary network interfaces and install the SunScreen software.

▼ Prepare the System

1. **Configure the interfaces on the Primary machine.**

   a. **If it does not already exist, configure the administration interface.**

      For bos-screen1 in this example, use the following command:

      ```
      echo "192.168.1.3" > /etc/hostname.le0
      ```

   b. **If it does not already exist, configure the HA heartbeat interface.**

      For `bos-screen1` in this example, use the following command:

      ```
      # echo "10.0.4.1" > /etc/hostname.le0
      ```

   c. **Reboot the Primary machine.**

2. **Install the SunScreen software on the Primary machine and verify that it is functions properly**

   Follow the instructions for the stealth mode example described in Chapter 4

3. **Prepare a Secondary machine to mirror the configuration of the Primary Screen.**

   This machine will be used as the secondary HA Screen. In this example, the second machine is named `bos-screen2`. The second machine (HA secondary) must be identical to the first machine (HA primary) in the following ways:

   - Solaris configuration
   - hardware (ideally)
   - Interface types

   The only configuration differences between the first and second machines are:

   - `/etc/`*nodename*
   - IP address of the administrative interface
   - IP address of the HA interface

4. **Configure the interfaces on the Secondary machine.**

   a. **If it does not already exist, configure the administration interface.**

      For `bos-screen2` in this example, use the following command:

      ```
      # echo "192.168.1.4" > /etc/hostname.le0
      ```

   b. **If it does not already exist, configure the HA heartbeat interface.**

      For `bos-screen2` in this example, use the following command:

      ```
      # echo "10.0.4.2" > /etc/hostname.le0
      ```

   c. **Reboot the Secondary machine.**

Your systems are now prepared to run HA in stealth mode. Continue with the configuration by going to "Configuring the HA Cluster" on page 74.

Preparing Routing Mode Screens for HA

The first step when defining an HA cluster is to properly configure the necessary network interfaces and install the SunScreen software.

▼ Prepare the System

1. **Configure the interfaces on the Primary machine.**

   a. **If it does not already exist, configure the HA heartbeat interface.**

      For `sf-screen1` in this example, use the following command:

      ```
      # echo "10.0.5.1" > /etc/hostname.qe2
      ```

   b. **If they do not already exist, configure the filtering interfaces.**

      For `sf-screen1` in this example, you would use the following commands to configure the two screening interfaces:

      ```
      # echo "10.0.1.100" > /etc/hostname.qe0
      # echo "192.168.2.2" > /etc/hostname.qe1
      ```

   c. **Reboot the Primary machine.**

2. **Install the Screen software on the Primary machine and verify that it is functions properly.**

3. **Prepare a Secondary machine to mirror the configuration of the Primary.**

   This machine will be used as the secondary HA Screen. In this example, the second machine is named `sf-screen2`. The second machine (HA secondary) must be

identical to the first machine (HA primary) in the following ways:

- Solaris configuration
- hardware (ideally)
- Interface types

The only configuration differences between the first and second machines are:

- `/etc/`*nodename*
- IP address of the administrative interface (if a separate one exists)
- IP address of the HA interface

4. **Configure the interfaces on the Secondary machine**

   a. **If it does not already exist, configure the HA heartbeat interface.**

      For `sf-screen2` in this example, use the following command:

      ```
      # echo "10.0.5.2" > /etc/hostname.qe2
      ```

   b. **If they do not already exist, configure the filtering interfaces.**

      For `sf-screen2` in this example, you would use the following commands to configure the two filtering interfaces:

      ```
      # echo "10.0.1.100" > /etc/hostname.qe0
      # echo "192.168.2.2" > /etc/hostname.qe1
      ```

   c. **Reboot the Secondary machine.**

Note – Be sure to physically disconnect the screening interfaces before you reboot the system. These interfaces should not be reconnected until after the HA configuration is complete, and the policy has been activated on the Primary Screen.

Your systems are now prepared to run HA in Routing mode. Continue with the configuration by following the instructions in the "Configuring the HA Cluster" on page 74 section that follows.

Configuring the HA Cluster

▼ Modify the Primary Screen to Run in HA Mode

In this example, the primary Screen is name `bos-screen1`

1. **Create empty Address GROUP object for use in defining the HA heartbeat interface.**

   In this example, the Address Group would be called `ha_grp`.

2. **Define an Interface object of type HA using the interface group created in the previous step.**

   Enter the name of the interface you want as the HA heartbeat interface. Select HA as the Type and `ha_grp` in the Valid Address field.

   Note – Make sure that the Spoof Protection field specifies INCOMPLETE.

   ---

3. **Save, but do not activate, the policy.**

   If you activate now, an error message appears regarding an HA interface being defined but HA not being activated.

4. **In the administration GUI, under the Policies section, click the `Initialize HA` button.**

   Select the interface name you specified in the previous step and click OK.

5. **Save and activate the policy.**

▼ Install the HA secondary Screen

In this example, the secondary Screen is named `bos-screen2`.

- **Install the Screen software on the secondary machine and specify that it is a Secondary HA system.**

  When prompted, enter the interface name of the HA heartbeat interface, and specify the IP Address of the HA heartbeat interface of the Primary HA system. The installation program will then perform the necessary steps for the SunScreen HA configuration.

▼ Define the HA cluster

1. **Using the Administration GUI, connect to the HA primary Screen's administrative interface.**

   This can be done either locally on the Primary machine, or remotely from an administration station.

2. **Define a Screen object for the HA secondary Screen.**
   See Figure 6–3

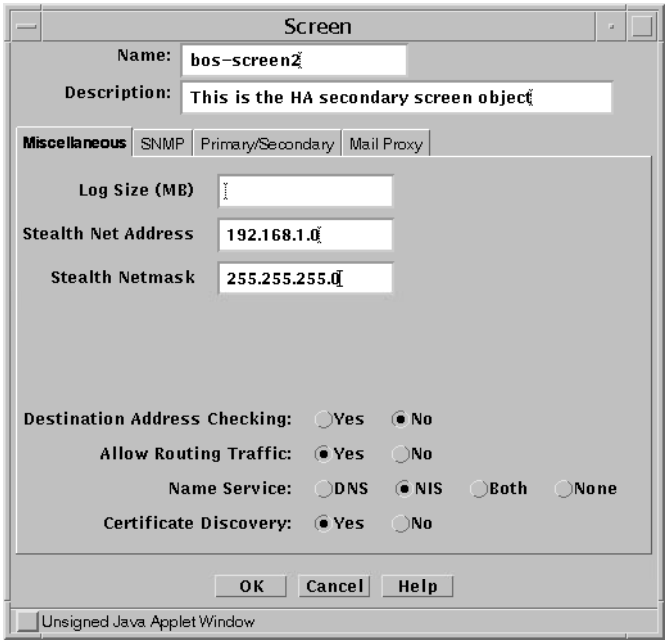


FIGURE 6–3 Screen Object Definition for HA Secondary Screen

   a. **Enter the name of the Secondary Screen in the name field.**

   b. **Select the Miscellaneous tab. Make sure that the information specified on this tab is identical to that of the Primary machine's Screen object.**

   c. **Select the Primary/Secondary tab. Specify the High Availability status (Secondary) and the HA Primary Screen. Finally, enter the High Availability IP Address (that of the Secondary's heartbeat interface).**
      See Figure 6–4for an example.

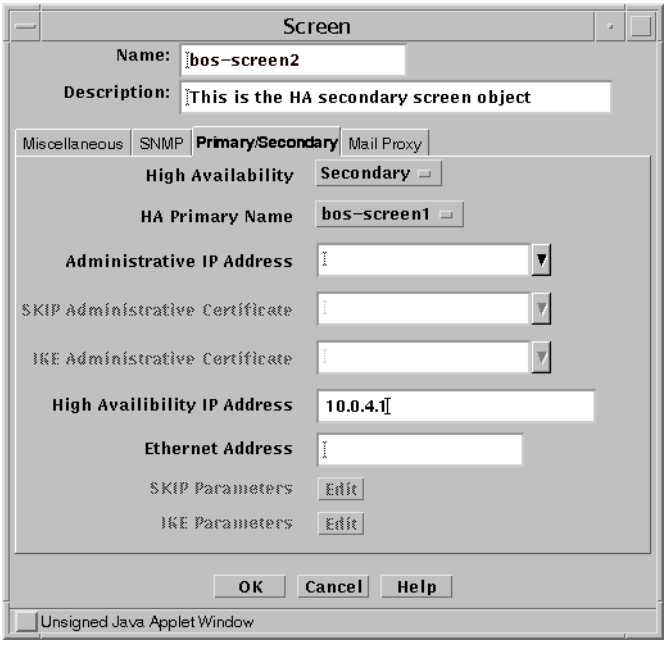


FIGURE 6–4 Secondary Screen Name and HA IP Address

3. **Save and activate the policy.**

Note – If the policy was activated successfully, and the Screens were configured in routing mode, the screening interfaces should be reconnected to the network at this point.

HA Notes

When administering an HA cluster, you usually contact only the primary Screen because it stores all the configuration information. If you need to administer the secondary Screen remotely, you must first have the Screen set up with an Administrative Interface (required in stealth mode). Then you need to add an access control list (ACL entry) on the Administration Station for the IP address of the secondary Screen's administrative interface using the same certificate names as those used by the primary Screen. The secondary and primary Screens have the same keys, which are copied across the HA interface during activation.

CHAPTER 7

Creating a Centralized Management Group

Typically, you use centralized management (CMG) to simultaneously administer configurations on a group of Screens. A CMG contains a primary Screen and some number of secondary Screens. Besides its firewall function, the primary Screen's main purpose is to push policy configurations to all of the secondary Screens in the CMG.

Note – Only a full function (non-Lite) routing-mode Screen can be a CMG primary. However, you can configure both stealth and routing-mode Screens as CMG secondaries.

Network Example

Figure 7–1 shows the San Francisco and Boston segments of the network. In this diagram, `sf-screen1` is the primary routing-mode CMG Screen and `bos-screen1` is the secondary CMG Screen (running in stealth mode.) You can add additional secondary CMG Screens by following this same procedure.

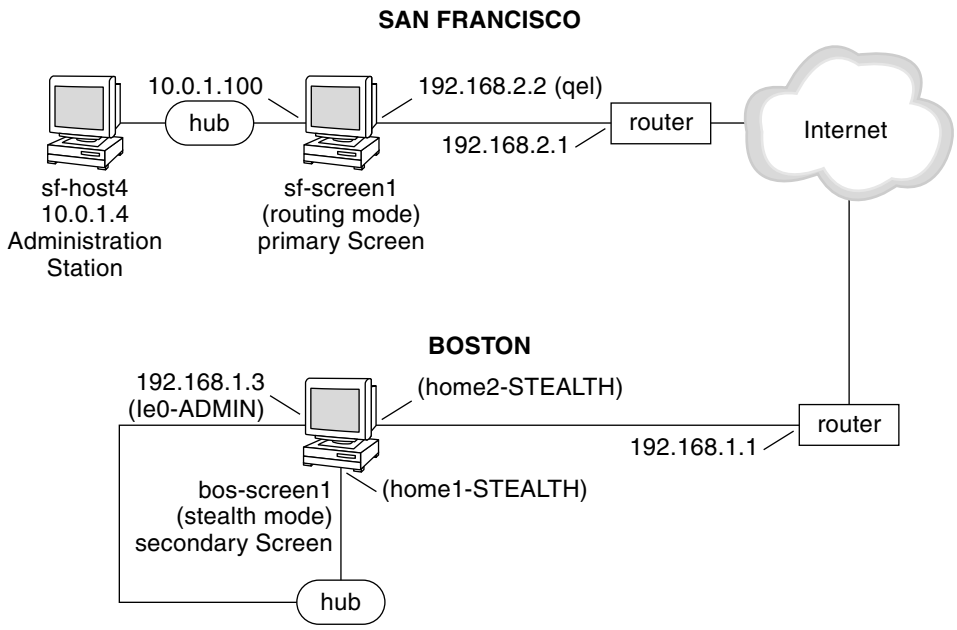


FIGURE 7–1 San Francisco and Boston Segments of the Sample Company Network

Centralized Management Group Configuration

▼ Install SunScreen on the Primary and Secondary Systems

1. **On the CMG primary system, install the Screen software in routing mode with remote Administration Station .**

   See Chapter 2 for installation information.

   In this example, the primary Screen is called `sf-screen1` and the Administration Station is named `sf-host4`. Be sure to write down the Screen's certificate ID for use in the next step. Refer to "Setting Up Remote Administration with SKIP" on page 23 for instructions on this step.

2. **On the CMG secondary system, install the Screen software in stealth mode.**

   See " Stealth Mode Configuration" on page 37 for installation information.

   In this example, the secondary Screen is called `bos-screen1`. Use the certificate generated in the previous step when prompted for the Administration Station's certificate ID. This certificate is given the name "remote" by default.

▼ Configure the CMG Secondary Screen

In this example the CMG secondary Screen is named `bos-screen1`.

1. **Configure the stealth mode Screen `bos-screen1` as a secondary Screen in the centralized management group.**

   Create the following objects to enable Screen `sf-screen1` to push the security policy to `bos-screen1`.

   - Create address objects (to enable definition of the stealth interfaces), screen objects, and policy rules shown in the following table.

   TABLE 7–1 Address Object Definitions

Name	Type	Address
`sf-screen1`	Host	`192.168.1.2`
`bos-screen1`	Host	`10.0.2.200`
`bos-ext-router`	Host	`192.168.2.1`
`bos-net-10`	Range	`10.0.2.0 - 10.0.2.255`
`bos-net-192`	Range	`192.168.2.0 - 192.168.2.255`
`bos-internal`	Group	Include: `bos-net-10`, `bos-net-192` Exclude: `bos-ext-router`, *
`bos-external`	Group	Include: *, `bos-ext-router` Exclude: `bos-net-10`, `bos-net-192`

   - Create a screen object for primary Screen containing the administrative IP Address and certificate under the Primary/Secondary Config Tab, shown in Figure 7–2.

     This secondary screen expects packets to originate from that Administrative IP address when the primary screen is in control. If the primary screen has more than

1 interface then activation may fail because the packets came from the wrong IP address. The Administrative IP address must be an address object in the Registry. It can also be a group object containing more than 1 IP address or *which means any address.

The Administration Certificate is the primary Screen's certificate. This could be any valid certificate on the primary Screen. You can create this certificate as part of the installation process or use this alternative method: Create a certificate object for the primary on the secondary using Associate MKID and give it a name like `sf-screen1.admin`. Then, make this certificate the Administration Certificate in the primary screen object.

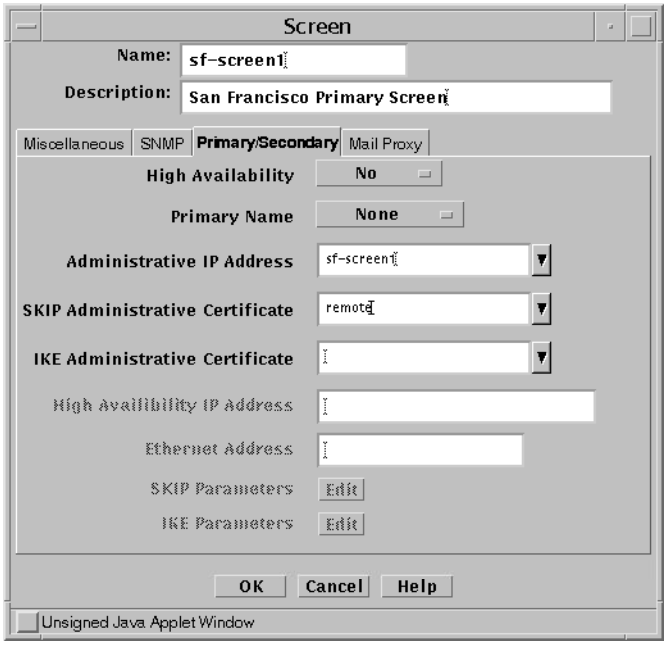


FIGURE 7–2 Screen Object for `sf-screen1`

- Create interface objects like the ones shown in the following table.

TABLE 7–2 Interface Object Definitions

Name	Screen	Type	Address Group
`qfe0`	`bos-screen1`	STEALTH	`bos-external`
`qfe1`	`bos-screen1`	STEALTH	`bos-internal`
`hme0`	`bos-screen1`	ADMIN	`bos-screen1_hme0` (created by default)

2. **Modify the Screen object and select the primary Screen as the Primary Name. Be sure you specify the correct the Administrative IP Address and Administrative Certificate, as shown in the following figure.**

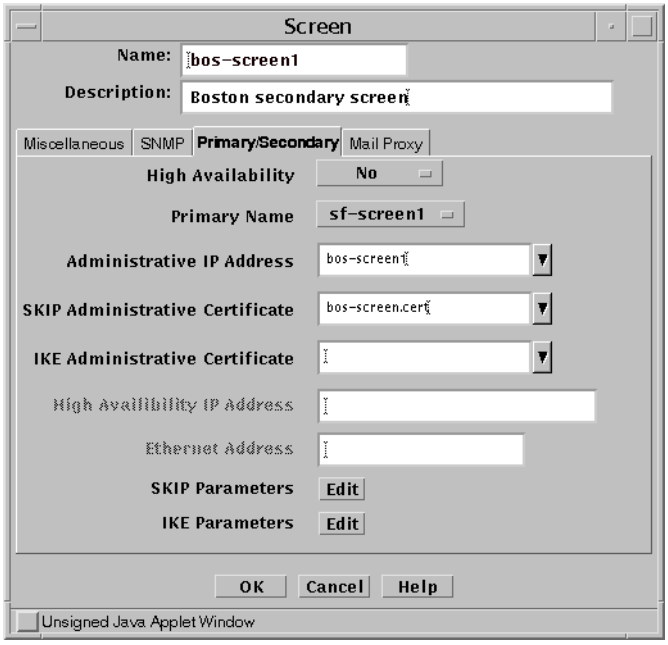


FIGURE 7–3 Screen Object for `bos-screen1`

3. **Create policy rules to enable SunScreen SKIP and CDP packets from the primary screen to pass through the Screen shown in the following figure.**

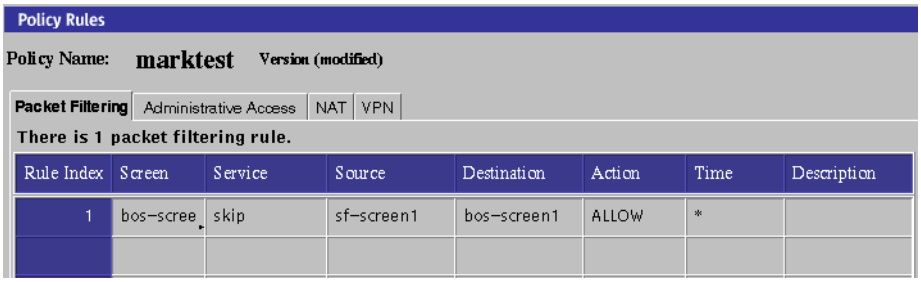


FIGURE 7–4 Policy Rules to Allow SunScreen SKIP and CDP Packet Flow

4. **Save and activate the policy on `bos-screen1`.**

▼ Configure the CMG Primary Screen

1. **On the primary Screen, create the objects needed to push the policy to secondary Screen**

   In this example, you would create the following objects:

   - These Address objects are needed for the example configuration.

     TABLE 7–3 Address Objects To Enable Configuration

Name	Type	Address
`sf-screen1`	Host	`192.168.1.2`
`bos-screen1`	Host	`10.0.2.200`
`bos-ext-router`	Host	`192.168.2.1`
`bos-net-10`	Range	`10.0.2.0 - 10.0.2.255`
`bos-net-192`	Range	`192.168.2.0 - 192.168.2.255`
`bos-internal`	Group	Include: `bos-net-10`, `bos-net-192`Exclude: `bos-ext-router`, *
`bos-external`	Group	Include: *, `bos-ext-router`Exclude: `bos-net-10`, `bos-net-192`

   - Create a Certificate object called `bos-screen1.admin` using the Associate MKID selection by choosing Certificate and then Add New in the Policy Objects area. Use the certificate ID that was generated previously.
   - Create a Screen object for `bos-screen1` containing `sf-screen1` as the primary Name, `bos-admin1` as the Administrative IP Address, and `bos-screen1.admin` as the Administrative Certificate.

   This looks the same as it did on the secondary Screen, as shown in Figure 7–3.

   - Create Interface objects as shown in the following table:

     TABLE 7–4 Interface Objects for `bos-screen1`

Name	Screen	Type	Address Group
qfe0	bos-screen1	STEALTH	bos-external
qfe1	bos-screen1	STEALTH	bos-internal
hme0	bos-screen1	ADMIN	bos-screen1_hme0 (created by default)

Be sure that all interface definitions for the primary Screen contain `sf-screen1` in the Screen field.

2. **Add policy rules to enable SunScreen SKIP and CDP packets from `sf-screen1` to pass through Screen `bos-screen1`, as shown in Figure 7–4 .**

   Be sure that each rule has an entry in the Screen object field to tell it which Screen is to implement the particular rule.

3. **Save and activate the policy on `sf-screen1`.**

   Your centralized management group is now configured, and is ready for you to implement your full security policy.

   In the network diagram, Figure 7–1, the primary routing-mode Screen `sf-screen1` is shown in an HA cluster configuration. You can configure your primary, centrally managed Screen with HA if you desire. However, you should first follow the steps to get your centralized management group working, then follow the procedure for adding the secondary HA Screen into the configuration.

CHAPTER 8

Using Proxies in Mixed-Mode

This configuration example shows how to use proxies in mixed-mode. In mixed-mode, one interface on the Screen is configured as in stealth-mode and the others are configured in routing-mode. You are not required to use mixed-mode in order to use proxies; you can also use proxies on a Screen in routing mode.

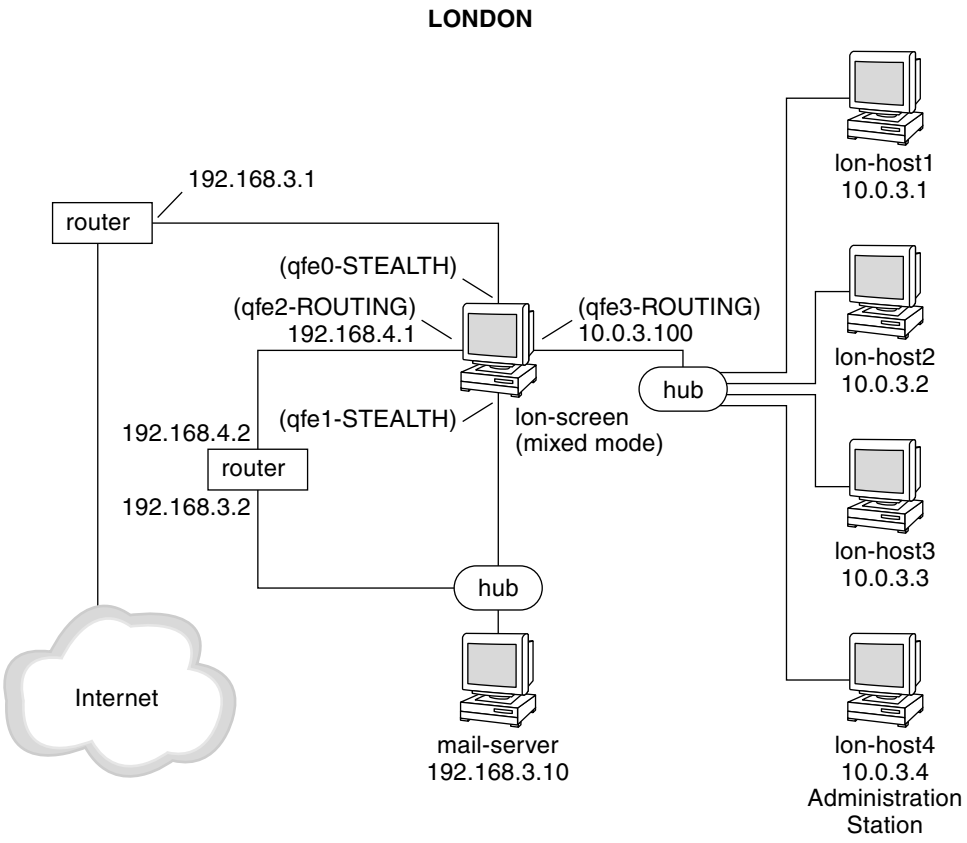
Typically, you use SunScreen in a mixed-mode configuration to provide the advantages of stealth to the subnet it partitions without the additional cost of a second Screen. The subnet is not visible outside of the network and can be added to a network without changing IP addresses.

Network Example

Figure 8–1 shows the London segment of the network example. In this diagram, a mixed-mode Screen, (`lon-screen1`) provides stealth protection on interfaces facing the internet and routing interfaces on the internal network. The stealth interfaces give the DMZ stealth protection for the mail server and the routing interfaces enable proxy user authentication to the internal network. The routing interfaces also allow internal access to the mail server and also internet access.

In this configuration, the hosts protected by the Screen have illegal IP addresses that give them web access to the Internet. The Screen also acts as an HTTP proxy and performs NAT for these hosts as well.

Note – Use care when designing the security policy for the routing interfaces. An open policy on a routing interface (like `qfe2` in this example), can expose the Screen to attacks, and can affect the stealth operation as well as negate the advantage of the stealth interface.



Firewall using routing and stealth interfaces (mixed mode). Several Class C subnets are used for clarity, but a single subnet can be subnetted with the appropriate subnet mask.

FIGURE 8–1 London Segment of the Sample Company Network

Configuration Considerations

The following parameters are used to implement this example:

- Two interfaces are set up in stealth mode
- Two interfaces are set up in routing mode

Note – The routing and stealth interfaces *must* be on different subnets, and separated by an external router.

- User authentication is provided for `telnet` access from the Internet to the internal network (`lon-host1`, and so forth)
- Anonymous FTP access is provided using the FTP proxy to `lon-host2` (ftp-server)
- Rules are added to only ALLOW SMTP access to mail-server
- Rules are added to only ALLOW authenticated `telnet` and FTP to the `qfe2` interface of `lon-screen1`
- The HTTP proxy is used to provide web access to the Internet

  All proxies are accessed through the transmission control protocol (TCP), and therefore can only run on systems configured in routing mode.

Mixed-Mode Limitation

Because NAT has a single state table only, NAT cannot be used to translate the IP addresses of the internal network in this mixed-mode configuration. You can, however, use NAT on the routing interfaces and on the stealth interfaces on a mixed-mode Screen provided that the packets only pass through the Screen once.

NAT is not required because the proxies that provide the `telnet/ FTP/HTTP` connections between the Internet and the internal network use the IP address of the Screen and not the illegal IP address of the host. Therefore, only the Screen needs to be able to resolve the host's IP address.

For example, the `mail-server` can have its address translated when packets pass to the Internet because the packets only pass through the stealth interfaces once. This is true of any host on the private part of the network (`192.168.3.0` in this example) or on the `192.156.4.0` network.

Using DYNAMIC NAT

The following steps outline how DYNAMIC NAT is used to translate the source IP addresses of hosts on the network (`10.0.3.0` in this example) to a legal address (`192.168.3.100` in this example).

- Add rules to ALLOW hosts on the `10.0.3.0` network free access to the Internet.
- Add rules to only ALLOW SMTP access to `mail-server`.
- Add rules to only ALLOW authenticated `telnet` and `FTP` to the `qfe3` interface of `lon-screen1`.

Note – The routing and stealth interfaces *must* be on different subnets, and separated by an external router.

Mixed-Mode Configuration

▼ Performing Preliminary Steps

The following steps illustrate what you would have to do to create a network like the one in the example. Your own configuration may differ significantly but the general steps would still apply.

1. **Configure the routing interfaces with the correct IP addresses.**

   In this example, the routing interfaces are named `qfe2` and `qfe3`

2. **Confirm that the Screen can contact the addresses of both the internal router and the internal hosts.**

   Make sure to use the correct routing and netmasks.

3. **Install the Screen in routing-mode with remote administration.**

   Use the steps described previously in “Setting Up Remote Administration with SKIP” on page 23 Select "routing mode" when installing the firewall software even though this Screen has both stealth- and routing-mode interfaces. In this example, `lon-host4` is the remote Administration Station.

4. **After rebooting the Screen, start a browser on the Administration Station and log into the Screen.**

5. **Define the Address objects that reflect the topology of your network.**

   For this example, you would create the Address objects shown in the following table

TABLE 8–1 Address Objects

Name	Type	Details
external-router	HOST	192.168.3.1
168.3-private	RANGE	192.168.3.2 to 192.168.3.254
mail-server	HOST	192.168.3.10
168.4-net	RANGE	192.168.4.1 to 192.168.4.254
10.0.3-net	RANGE	10.0.3.1 to 10.0.3.254
ftp-server	HOST	10.0.3.3
qfe3_grp	GROUP	Include {10.0.3-net} Exclude {}
qfe2_grp	GROUP	Include {*} Exclude {10.0.3-net}
qfe1_grp	GROUP	Include {168.3-private 168.4-net 10.0.3-net} Exclude {}
Internet	GROUP	Include {*} Exclude {qfe1_grp}
qfe0_grp	GROUP	Include {Internet} Exclude {}

Note – The address groups (for example, qfe1_grp) must contain all the IP addresses that can be reached from that interface.

6. **Verify that the routing interfaces were defined by the installation procedure.**

   In this example, the routing interfaces are qfe2 and qfe3. They must have the interface groups qfe2_grp and qfe3_grp assigned to them, respectively.

7. **Add INTERFACE objects for the stealth interfaces.**

   In this example, you would define qfe0 and qfe1 as using the address groups qfe0_grp and qfe1_grp. These interfaces must be defined as TYPE: STEALTH.

8. **Edit the Screen object ensuring that the STEALTH SUBNET/NETMASK are defined.**
   In this example, the values would be `129.168.3.0` and `255.255.255.0`.
9. **Install an open, or a test, policy.**
10. **Save and activate the policy.**
11. **Verify that the configuration works.**
    In this example, you would try to `ping` the `mail-server` from an external host. Verify that this host can `ping` the Screen's external routing interface `qfe2`.

Configuring Proxies for User Authentication

In Figure 8–1, `telnet` access is required to the hosts on the `10.0.3.0` network from unspecified hosts on the Internet. To give access to your trusted users only, implement user authentication.

▼ Set Up Telnet User Authentication

This example shows six user names that need access to the `10.0.3.0` network: Mathew, Mark, Luke, and John.

1. **Define each of your users as an Authenticated User, as shown in the following figure:**

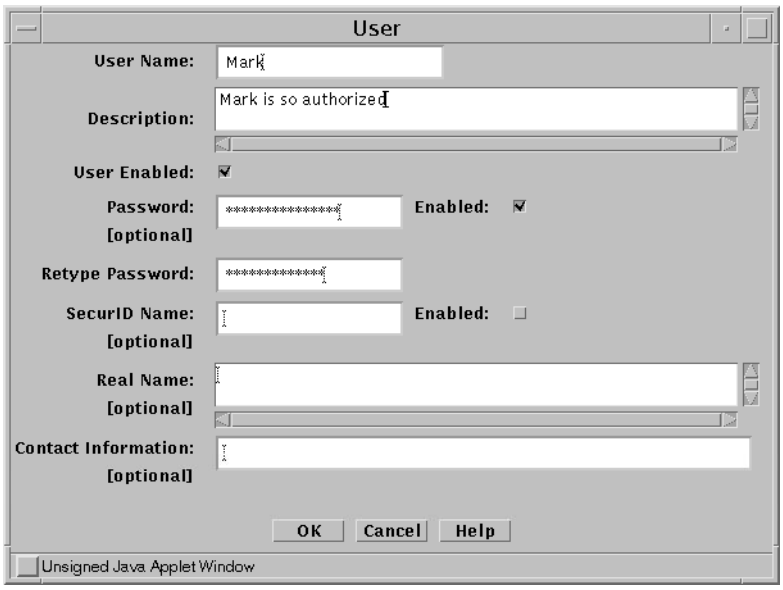


FIGURE 8–2 Authenticated User Definition

2. **Define each of your users as a Proxy User, as shown in Figure 8–3.**
   Define only those users who are qualified to use the proxy for authentication.

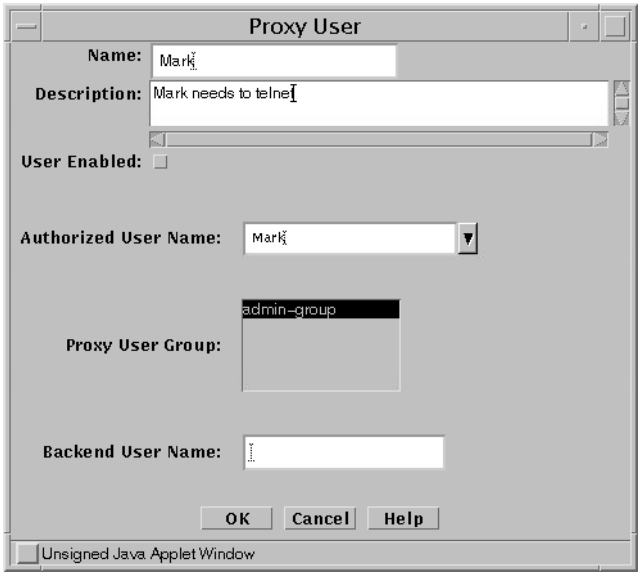


FIGURE 8–3 Proxy User Definition

3. **Create a rule to ALLOW proxy access that references either a single Proxy User, or, more usually, a GROUP of Proxy Users, as shown in the following figure.**

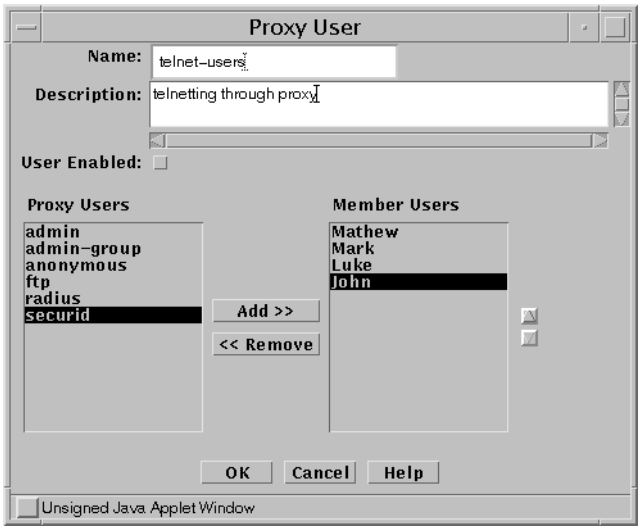


FIGURE 8–4 Proxy User Name Used in the Rule

4. **Define a Proxy User GROUP with all your users.**

5. **Add a rule to ALLOW `telnet` with Proxy AUTHENTICATION, as shown in the following figure.**

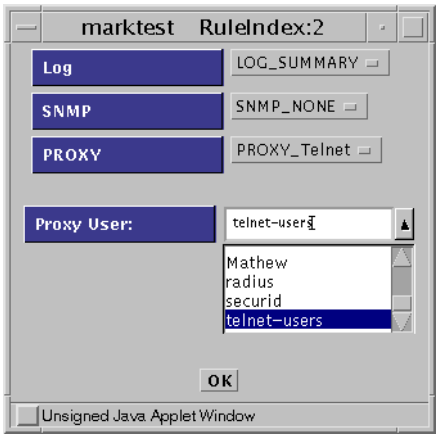


FIGURE 8–5 ALLOW telnet Rule

6. **Save and activate the configuration.**

▼ Set Up `FTP` Authentication

Another requirement is to ALLOW `anonymous FTP` to the server `lon-host3` using the FTP Proxy. Because this is `anonymous FTP`, you do not have to create an Authenticated User. Use the predefined Proxy Users for `ftp` and `anonymous` for this purpose.

The advantage of using the FTP Proxy to ALLOW `anonymous FTP` access over a regular packet filter rule in this configuration is that the outside world does not need to know which system is the FTP server. Because the FTP connection is made from the firewall, only the firewall needs to know how to resolve the name `ftp-server` to an IP address. The firewall can use a simple alias in its hosts file and can be changed to another server without having to tell your users. In this example, the FTP server `lon-host3` has an illegal IP address, which is enabled because the firewall can contact it.

Note – Using NAT with a conventional packet filtering rule requires you to add a DNS entry for this host.

1. **Define a Proxy User Group that contains the users who can use FTP, as shown in the following figure.**

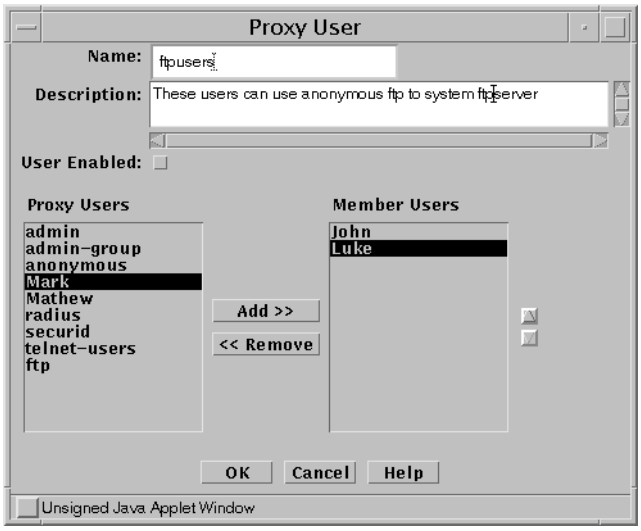


FIGURE 8–6 Proxy User Group Definition

2. **Define a rule to ALLOW FTP access, as shown in the following figure.**

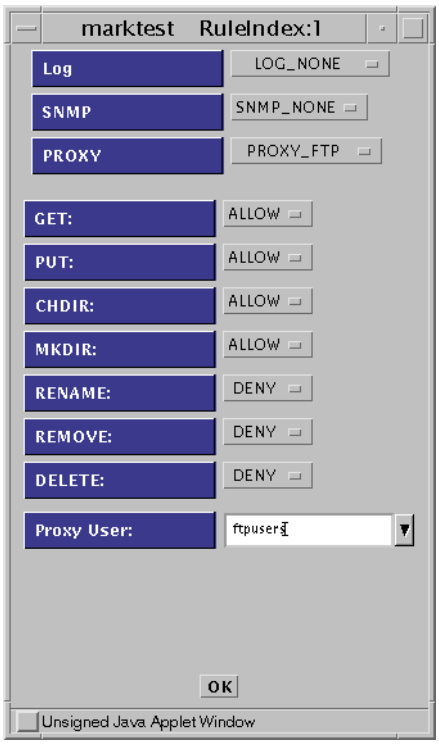


FIGURE 8–7 ALLOW FTP Access Rule Definition

3. **Save and activate the policy.**

▼ Set Up HTTP the Proxy

Because the users behind the firewall have illegal IP addresses and NAT cannot be used in a mixed-mode configuration, the HTTP proxy can be used to provide Internet access for your internal users.

1. **Add a rule to ALLOW Internet access, as shown in the following figure.**

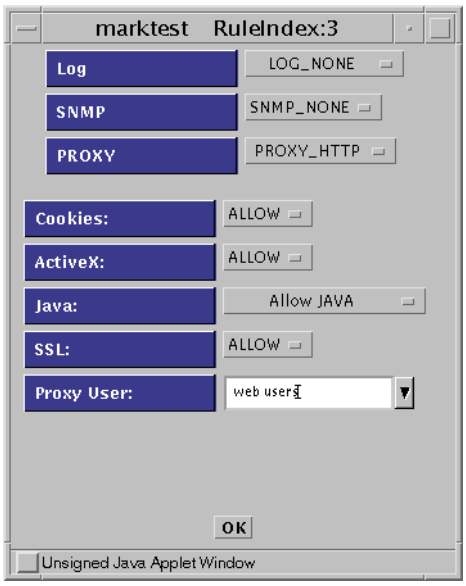


FIGURE 8–8 Rule Definition: Initial Window

2. **Save and activate the policy.**

   The internal hosts must set the Proxy Address of their browsers to the internal IP address of the firewall (`10.0.3.100` in this example).

Proxy Considerations

Ensure that the rules do not open a back door into the Intranet that bypasses the proxy rules (for example, a rule that enables `telnet` directly to a host).

Adding a rule that explicitly drops `telnet/FTP` *after* the proxy rules does this as shown in Figure 8–9.

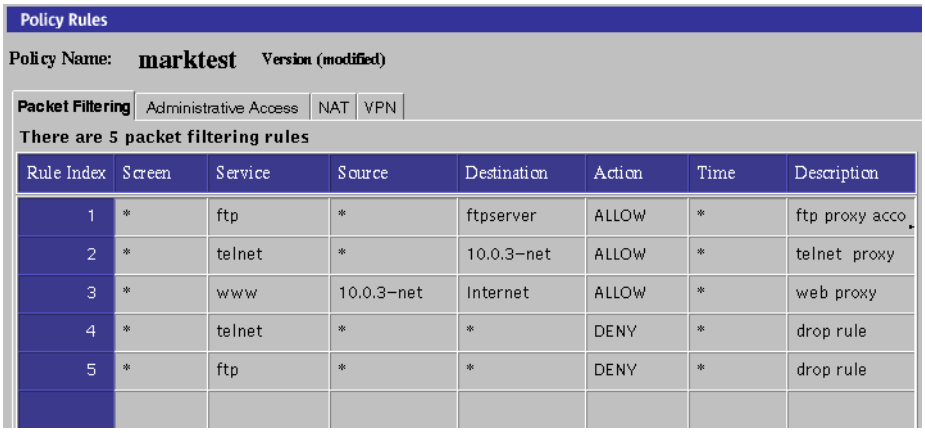


FIGURE 8–9 Add a Rule to Drop telnet or FTP After the Proxy Rules

Your user must `telnet/ FTP` to the firewall to be authenticated. The proxy connects the user to the target system (even though the rule has the destination address as the target host).

After configuring a proxy rule, you may need to reboot or rule this script to start the proxy by typing:

```
# /etc/rc2.d/S79proxy start
```

You can verify that the proxies are running by typing:

```
# ps -ef
```

which gives results like those shown in the following table:

TABLE 8–2 Proxies

root 4820	1 0 15:25:47?	0:00 /opt/SUNWicg/SunScreen/proxies/ftpp	
root 4819	1 0 15:25:47?	0:00 /opt/SUNWicg/SunScreen/proxies/telnetp	
root 4818	1 0 15:25:47?	0:00 /opt/SUNWicg/SunScreen/proxies/httpp	

The common objects, authorized user, administrative user, and proxy user that appear in the administration GUI are automatically saved when they are edited or new objects are added. You do not need to save these objects. Changes made to them apply immediately and cannot be reversed; however, they do not take effect until a policy is activated. To install the new objects and to propagate these changes to secondary Screens, activate your system configuration.

Note – The Save button is grayed out to show that it is inactive.

See the *SunScreen 3.2 Administrators Overview* for more information regarding authentication.

CHAPTER 9

SunScreen and Windows 2000 IKE Interoperability

This chapter provides some examples of how you can make a SunScreen firewall and a machine running Windows 2000 communicate with each other using IKE. SunScreen 3.2 and Windows 2000 each support the following IKE features:

- Preshared Keys – These keys act like a password to authenticate the communicating endpoints during IKE negotiation.
- Signed X.509 Certificates – These are certificates signed by a Certificate Authority (CA) as opposed to the self-signed Diffie-Hellman certificates supported by SunScreen (but not Windows 2000).

This chapter provides examples that illustrate the use of both interoperabilty features. You can find command line examples of using IKE in the IKE Policy Rule Syntax section of the Command Line Interface chapter of the *SunScreen 3.2 Administrators Guide*.

Network Example

Figure 9–1 shows a SunScreen communicating with a Windows 2000 systems over the Internet. The Screen is using IKE preshared keys and also using signed certificates. Some of the CAs supported by Windows 2000 are also shown. SunScreen does not restrict the use of CAs to these authorities.

In this example, the Screen is communicating with one Windows 2000 system using an IKE preshared key and is also communicating with another system using CA signed certificates.

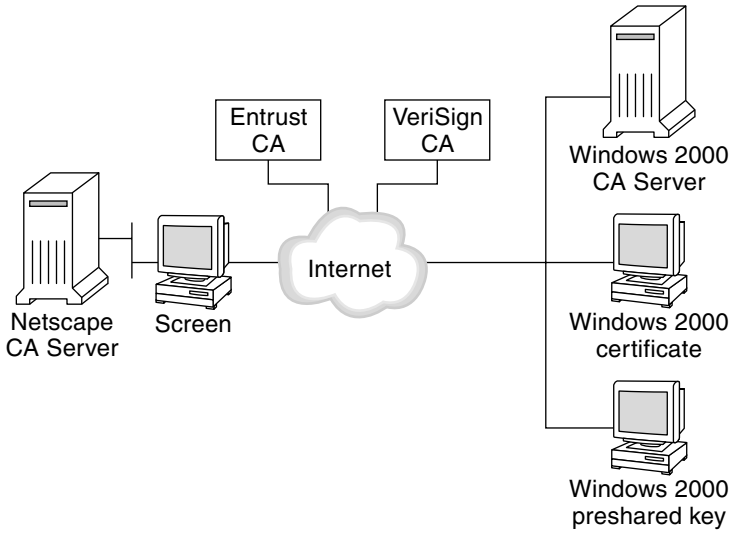


FIGURE 9–1 Windows 2000–SunScreen Interoperability

Using Preshared Keys

Preshared keys function as a type of password which authenticates each side of a communications channel during IKE negotiation. The actual preshared key (an ASCII text string) is not sent over the wire but a hash of it is used instead. Once the IKE parameters are successfully negotiated, regular secure communications can proceed. While this authentication method is simple to set up, it typically does not scale well.

Note – Certain SunScreen features like remote administration require the use of certificates. So, you cannot use a Windows 2000 system to remotely administer a Screen using preshared keys.

Configuring the Screen to Use Preshared Keys

This sections describes how you set up SunScreen to use IKE preshared Keys.

▼ Set Up the Screen

1. **Select and edit the appropriate policy.**
2. **Define an IPsec Key Common Object.**

Note – This is an optional step as you can also enter a preshared key directly into a field on the Rule Definition Action Details window.

In the Common Object panel select IPsec Key and New; the IPsec Key dialog appears (see Figure 9–2).

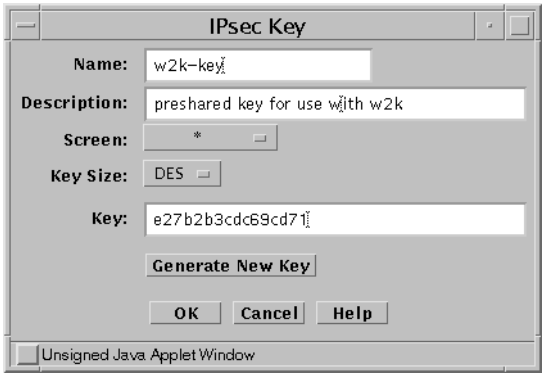


FIGURE 9–2 IPsec Key Dialog Window

3. **Fill in the required fields**

   Provide a Name and Description for the object as well as selecting the desired key size from the Key Size list. If you were using a preshared key generated by another system, you could type the key into the Key field. If you were using SunScreen to generate the key, you would click the Generate New Key button. The key does not have to be numeric, so you could for instance use a phrase.

4. **Define the required Address objects.**

   In this example, you would define HOST type Address objects for the following systems: `bos-host5`, `sf-w2kremote`, and `sf-w2k1`.

5. **Create a Packet Filtering rule that allows encrypted communication between the systems using the IKE preshared key.**

   In this example, `telnet` is the required service but it could be any service. The way you define the rule is similar to other IKE encryption rules except that the Authentication Method is PRE-SHARED (for more details on defining Packet Filtering IKE rules, see "Create Packet Filtering Rules with the ENCRYPT action" on page 50.)

See Figure 9–3 for an example of what the Rule Definition and Action Details windows would look like.

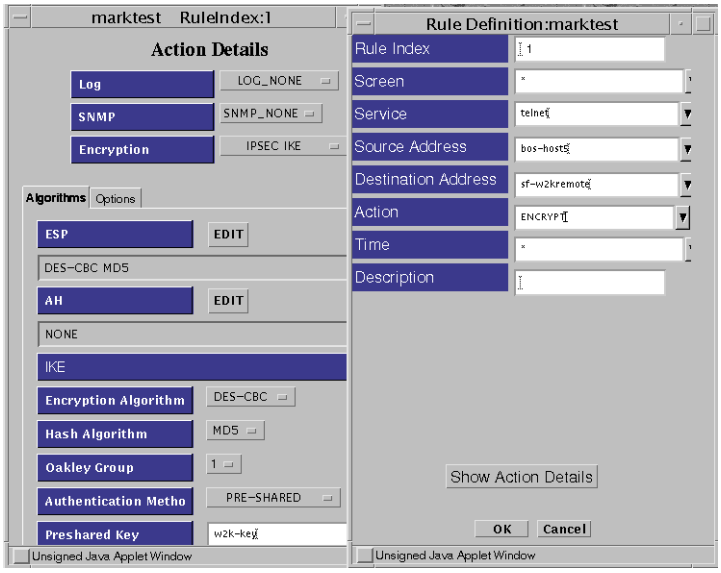


FIGURE 9–3 Rule Definition Windows for PreShared Key

Note – The Oakley Group field on the Screen and the DH Group field on the Windows 2000 system must use the same value.

---

6. **Click the Options tab and select the IKE mode.**

   Your choices are Tunnel or Transport mode. Tunnel mode encapsulates and encrypts the entire packet including the IP header for maximum security. Transport mode encapsulates and encrypts only the data portion of the IP packet resulting in smaller packets and potentially better throughput as the Screen is relieved of the overhead of decrypting the IP header. SunScreen and Windows 2000 both support IKE Transport and Tunnel modes.

   If you choose Tunnel mode, you can supply the Source and Destination Tunnel addresses. You can also supply Source and Destination Screens. If you choose Transport mode, you can only specify Source and Destination Screens.

   If the Source Address is the Screen, specify the Screen object in the Source Screen field. If the Destination Address is the Screen, specify the Screen object in the Destination Screen field.

7. **Save and activate the policy.**

Configuring the Windows 2000 System to Use Preshared Keys

See the Windows 2000 online help for specific instructions on how to create a Security Policy with an IKE filter that uses preshared keys. You can also refer to the Microsoft White Paper *How to Configure IPSec Tunneling in Windows 2000* which is available from their web site.

When you create the Security Policy, make sure all the IKE parameters on the Windows system match the IKE parameters on the Screen, including:

- ESP and/or AH
- Encryption Algorithm
- Hash Algorithm
- Authentication Method

Make sure he the DH Group value is the same as the Oakley Group value on the Screen. Lastly, use the same preshared key as the key used on the Screen.

Note – Windows 2000 uses an ACSII character string to specify the preshared key. SunScreen uses an ASCII hexidecimal string for the same purpose. For example, if you specified the preshared key as *ABC* on the Windows 2000 system, you would specify the same key as *414243* on the SunScreen system.

Using CA Signed Certificates

A more secure method than using preshared keys is using CA signed X.509 certificates. These certificates must be digitally signed by a Certificate Authority (CA) supported by both the Windows 2000 system and the SunScreen system. Currently, Microsoft supports certificates signed by its own Windows 2000 Server CA as well as a number of public CA authorities (see the Trusted CA Authorities list on Windows 2000, all of these vendors qualify as Root CAs). You can also use non-public CA's like Netscape Certificate server, if you import the CA's root Ccertificate into the Windows 2000 Trusted Root Certificate store. Self signed certificates are not supported by Microsoft

Each side must be able to follow each signed certificate up its certificate chain to the Root CA. They accomplish verification by having the Root CA's certificate in a special certificate store (the `IKE root CA certificates` GROUP certificate object on the Screen and the Trusted Root Certificate store on the Windows 2000 system). Because both systems must use certificates signed by a CA common to both systems, you cannot use self signed DH certificates to interoperate with Windows 2000.

Note – Certificates are necessary in order to have a Windows 2000 system act as a remote Administration Station managing a Screen.

Configuring the Screen to Use CA Signed Certificates

The following sections describe how you would set up the Screen and the Windows 2000 system to interoperate.

▼ Set Up the Screen

1. **Generate a Certificate Signing Request**

   a. **From the Common Objects panel, select Generate IKE Certificate**

b. When the IKE Certificate dialog appears, click the Generate CA Request button; see Figure 9–4

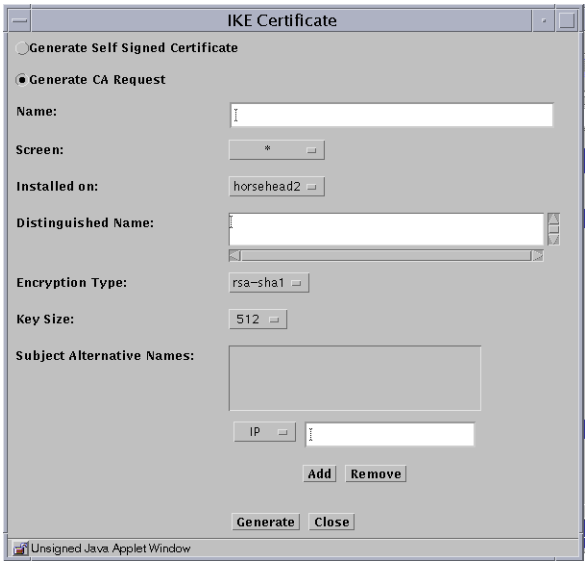


FIGURE 9–4 Generate CA Signing Request

c. Fill in the required fields.

Type in a Distinguished Name and make sure that the Encryption Type and Key Size match the related parameters used by the Windows 2000 system for its own certificate.

d. Click the Generate button.

SunScreen generates a Certificate Signing Request (CSR) and also creates and stores a private key. The following figure shows the CSR.

FIGURE 9–5 IKE CA Certificate Signing Request

You can copy the text or save into a file for use in your signing request.

2. **Present the CSR to the CA.**

   Have the certificate signed and acquire the new certificate.

3. **Import the CA signed certificate into the Screen**

   a. **From the common Objects panel, choose Import IKE Certificate. The Import IKE Certificate screen appears**

   b. **Specify a name and description.**

   c. **Choose an import method**

      Click the appropriate button and then either specify a file to import or paste the signed certificate into the text area.

   d. **Click the Install Certificate button.**

4. **Add the IKE Root CA Certificate to the Screen.**

   You accomplish this task by adding the Root CA certificate to the `IKE root CA Certificates` GROUP object.

   a. **Acquire the Root CA certificate and import it into the Screen's certificate store.**

   b. **After you finish the import, in the Common Objects panel, search for the `IKE root CA certificates` object.**

      When you find the object, select it and click the edit button. The Certificates object dialog appears. See Figure 9–6.

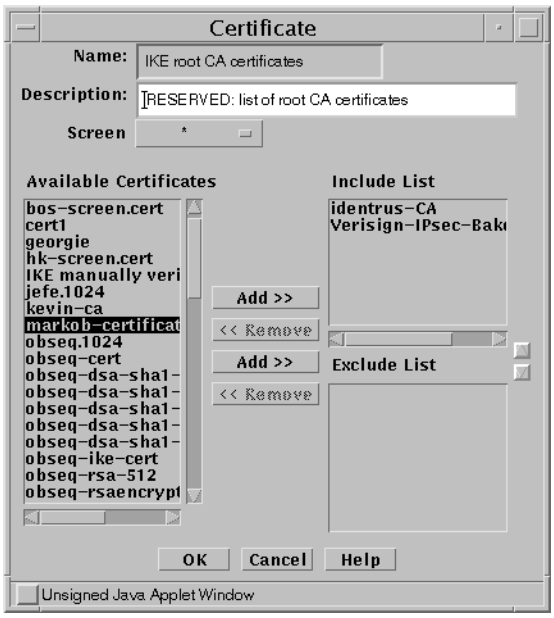


FIGURE 9–6 Import Root CA

c. Select the Root CA certificate you want and add it to the Include List.

d. Click OK to finish the task.

5. Edit the Root CA certificate object.

A requirement of Windows 2000 for IKE interoperability is that you must specify the Root CA certificate by its ISSUER Distinguished Name.

a. Search for the Root CA certificate object.

When you find the correct object click the Edit button.

b. Edit the Distinguished Name.

In the Distinguished Name, change the first qualifier from `SUBJECT` to `ISSUER`. Keep the value of the qualifier the same, only change the handle.

Configuring Windows 2000 to Use CA Signed Certificates

The following section describes in general terms how you would set up a Windows 2000 system to interoperate with a Screen. This section only provides general steps.

For specific instructions on setting up the Windows 2000 system see the Windows 2000 online help and also refer to these White Papers which are available on the Microsoft web site.

- *How to Configure IPSec Tunneling in Windows 2000*
- *How to Install a Certificate for Use with IP Security*
- *Step-by-Step Guide to Internet Protocol Security IPSec*

▼ Set Up the Windows 2000 System

1. **Obtain a private key and certificate signed by the same CA used by the Screen with whom you wish to communicate.**
2. **Make sure that the CA Root certificate is in the Trusted Root CA Certificate store.**
3. **Create an IPSec security policy.**

   Create an IKE rule that allows communication between the Screen and the Windows 2000 system.
4. **Be aware of the following interoperability requirements:**
   - The Authentication Method should be Certificate Authority and the Root CA list must contain the common Root CA certificate.
   - The filter action should be Negotiate Security and it should only specify one security method.

Using the Encryption Action on the Screen

To set up a packet filtering rule on the Screen use the same procedure as would be used with any IKE encryption rule. However, you must be aware of the following interoperability requirements:

- The ESP and AH values must match those specified in the Filter Action on the Windows 2000 system.
- The encryption Algorithm must be either DES or 3DES.
- The Authentication Method must be RSA-SIGNATURES
- The Oakley group must be consistent with the DH values used by the Windows 2000 system during IKE negotiation. You are restricted to those values supported by the Windows 2000 system. For example, Windows 2000 does not support Oakley group 5. The following table shows the *default* Oakley Group values used by Windows 2000. If someone on the Windows 2000 side changes these default values (unlikely based on how far down they are buried in the GUI) , you would have to use a value that matches their new value.

Encryption Algorithm	Hash Algorithm	Oakley Group Value
3DES	SHA1	2
3DES	MD5	2
DES	SHA1	1
DES	MD5	1

- If the rule permits traffic from the Windows 2000 system to the Screen, the Source Certificate must be the Root CA certificate and the Destination Screen is the Screen object.
- If the rule permits traffic from the Screen to the Windows 2000 system, the Destination Certificate must be the Root CA certificate and the Source Screen is the Screen object.