



SunScreen 3.2 Administration Guide

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

Part No: 806-6346
September, 2001

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. Tous droits réservés

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



010907@2347



Contents

Preface	15
1 Starting the Administration GUI and Logging In	21
Terms Used in This Book	21
Administration GUI Browser Requirements	22
Accessing Local System Resources	23
▼ To Install the Java Plug-In on the Screen	23
▼ To Install on the Remote Administration Station.	24
▼ To Save the <code>identitydb.obj</code> File	24
▼ To Use the HotJava 1.1 Browser	25
Using the Administration GUI	26
▼ To Start the Administration GUI for Browsers Without the Java Plug-In	26
▼ To Start the Administration GUI for Browsers With the Java Plug-In	26
▼ To Log In to the Administration GUI	27
Administration GUI Navigation Bar and Buttons	29
Changing the Admin User Password	30
▼ To Change the Admin User Password	30
2 Working With Common Objects	35
Using the Policy Rules Page	37
▼ To Modify the Policies Associated with a Common Object	37
Policies List Page	39
Policies List Panel	40
Types of Policies	40
Policies List Page Action Buttons	41

Using Common Objects	43
The Screen Field and Common Objects	45
▼ To Add a Common Object	46
▼ To Search for a Common Object	46
▼ To Edit a Common Object	47
▼ To Edit a Common Object From the Policy Rules Table	49
▼ To Delete a Common Object	50
▼ To Rename a Common Object	51
Service and Service Group Objects	53
▼ To Add a Service	53
▼ To Add a Service Group	57
Address Objects	60
▼ To Add a Host Address	60
▼ To Add a Group of Addresses	62
▼ To Add a Range of Addresses	64
Certificate Objects	67
▼ To Generate an IKE Certificate	68
▼ To Export an IKE Certificate	70
▼ To Import an IKE Certificate	72
▼ To Associate an IKE Certificate	74
▼ To Generate SKIP UDHs Certificates	76
▼ To Load a SKIP Issued Public or Private Certificate	78
▼ To Associate SKIP Certificate	81
Certificate Groups	83
▼ To Add a Certificate Group	83
▼ To Work with IKE Certificate Groups	85
IPsec Key	88
▼ To Add an IPsec Key	88
Screen Objects	90
Screen Object Tabs	90
Miscellaneous Tab	90
SNMP Tab	92
Primary/Secondary Tab	95
Mail Proxy Tab	97
Adding a Screen Object	98
▼ To Add a Screen	98
SNMP Alert Receivers	99

▼ To Add an SNMP Alert Receiver	100
▼ To Delete an SNMP Alert Receiver	101
Interface Objects	103
▼ To Add or Edit Interfaces	105
▼ To Remove an Interface	107
▼ To Set up a Routing Interface	107
▼ To Set up a Stealth Interface	109
▼ To Change an Admin Interface From the Local Console	112
▼ To Change an Admin Interface From a Remote Console	115
Adding Jar Signatures and Jar Hashes	117
▼ To Add a Jar Signature	118
▼ To Add a Jar Hash	120
Proxy Users	121
Authentication	121
▼ To Add an Authorized User	123
Time Objects	125
▼ To Create Time Objects	125
3 Creating and Managing Rules	129
Packet Filtering Rules	130
▼ To Modify Rules	130
▼ To View and Edit the Details of an Object	133
▼ To Edit a Rule	133
▼ To Add a New Rule	135
▼ To Move a Rule	136
▼ To Delete a Rule	137
Administrative Access Rules	138
▼ To Add or Change an Administrative Access Rule for Local Administration	138
▼ To Add or Change an Administrative Access Rule for Remote Administration	140
▼ To Specify a SKIP/IPsec/IKE Action on a Remote Access Rule	145
Network Address Translation (NAT) Rules	150
NAT Mapping Overview	150
NAT Administration Page	151
Your NAT Scenario	152
▼ To Manually Add an ARP Entry	153

▼ To Define NAT Rules	153
▼ To Edit the NAT Rules	155
Example: Static NAT of a Host to a Host	157
Example: Reverse Rule	157
Example: Dynamic Translation of a Range Of Addresses to One Host	158
Virtual Private Network (VPN) Rules	159
Before You Begin	160
Configuring a VPN	160
▼ To Add a VPN Gateway Definition	160
▼ To Create Packet Filtering Rules for a VPN	164
4 Creating and Managing Policies	169
Working With Policies	170
▼ To Work with Policies	171
Editing Policies	172
▼ To Edit a Policy	172
▼ To Add a New Policy	173
▼ To Copy a Policy	174
▼ To Rename a Policy	175
▼ To Delete a Policy	176
▼ To Verify a Policy	177
▼ To Back Up All Policies	179
▼ To Restore All Policies	181
Working With Policy Locks	183
▼ To Leave an Administration Session	183
▼ To Unlock a Policy	183
▼ To Forcibly Clear the Lock	184
Activating Policies	184
▼ To Save Changes	184
▼ To Cancel Policy Changes	186
▼ To Activate a Policy	186
5 Using High Availability	187
Setting Up High Availability	188
HA Policy	189
Preparing to Install High Availability	189

Using the <code>/etc/hosts</code> File for Name Resolution	190
Defining HA	190
Modifying the HA Service Group	191
Using NAT With HA in Routing Mode	191
Installing High Availability	192
▼ To Edit the Policy	192
▼ To Install the SunScreen software in an HA Configuration	193
▼ To Install HA on the Secondary HA Screen	194
▼ To Define the HA Interface	199
▼ To Define the Screen Object for the HA Primary Screen	201
▼ To Initialize HA on the Primary HA Screen	203
▼ To Add the Secondary HA Screen to the Primary HA Screen	203
▼ To Allow Non-Administrative Traffic on an HA Network	205
Configuring Policies for an HA Cluster	208
Removing HA	209
HA Logging	210
6 Setting Up and Using Proxies	211
Matching Proxy Rules	212
Preparing to Use Proxies	212
Defining Proxy Data	213
Setting Up Proxy Users	213
▼ To Set up Basic Proxy Users	214
▼ To Add a Single Proxy User	215
▼ To Add a Proxy User Group	217
▼ To Add Spam Domains	218
▼ To Delete Spam Domains	221
Writing and Editing Policy Rules for Proxies	223
▼ Basic Steps for Writing Policy Rules for Proxies	224
▼ To Write Policy Rules for the Proxies	227
▼ To Define PROXY_FTP	228
▼ To Define PROXY_HTTP	230
▼ To Define PROXY_SMTP	231
▼ To Define PROXY_Telnet	232
Using the FTP Proxy	233
▼ To Use the FTP Proxy	233
Using the TELNET Proxy	235

▼ To Use the Telnet Proxy	235
Using the SMTP Proxy	236
▼ To Use the SMTP Proxy	236
Using the HTTP Proxy	236
▼ To Configure the Browser to Use the HTTP Proxy	237
Proxy Logging	238
7 Configuring Centralized Management Groups	241
CMG Overview	242
CMG Requirements	242
CMG Configuration Tasks	243
▼ Basic Centralized Management Procedure	243
▼ To Generate an IKE or SKIP Certificate on the Primary Screen	245
▼ To Associate the IKE or SKIP Primary Screen's Certificate with the Primary Screen Object	247
▼ To Put the IKE or SKIP Primary Screen's Certificate on the Secondary Screen	250
▼ To Add the IKE or SKIP Primary Screen Object to the Secondary Screen	252
▼ To Generate an IKE or SKIP Certificate for the Secondary Screen	254
▼ To Modify the IKE or SKIP Secondary Screen Object	254
▼ To Configure the Secondary Screen for Management by the Primary Screen	256
▼ To Add the Secondary Screen's Certificate ID to the Primary Screen	260
▼ To Add a Secondary Screen Object to the Primary Screen	261
▼ To Add a New Address Group to the Primary Screen	263
▼ To Define the Secondary Screen's Interfaces on the Primary Screen	265
▼ To Configure the Primary Screen to Manage the Secondary Screens	267
8 Adding Remote Administration Stations After Installation	271
Adding a Remote Administration Station	271
▼ To Set Up the Screen to Use the New Remote Administration Station	272
▼ To Inform the Screen About the New Remote Administration Station	272
▼ To Set Up the Access Control List on the New Remote Administration Station	277
9 Getting Status and Managing Logs	279
The Information Page	279

Status Information	280
▼ To View Status Information	280
Log Page	282
▼ To View the Log Page	282
284	
Setting a Log Viewing Filter	285
The Information Tab	288
Action Buttons	289
Statistics Page	290
▼ To View the Statistics Page	290
Viewing Statistics	293
▼ To See the SKIP Statistics	293
Viewing Logs	294
▼ To Set the Retrieval Mode	294
▼ To Set a Log Viewing Filter	296
Saving and Clearing the Log	298
▼ To Save the Log	298
▼ To Clear the Log	300
▼ To Save and Clear the Log	301
Changing the Size of the Log File	302
▼ To Change the Log File Size for a Specific Screen	303
Virus Scanning	304
10 Using the Command Line Interface	305
Command Summary	305
UNIX (shell) Commands	306
ssadm Command	306
▼ To Execute an ssadm Command on a Local Screen	307
▼ To Execute an ssadm -r Command on a Remote Administration Station	307
Logging In to and Out of SunScreen Remotely	308
▼ To Log In to and Out of SunScreen Remotely	308
ssadm Subcommand Summary	308
ssadm configure Command	310
Configuration Editor Subcommands	310
Using the Configuration Editor	312
▼ To Edit a Policy	312

Working With Policies	312
▼ To Create a New Policy	312
▼ To Copy a Policy	313
▼ To Rename a Policy	313
▼ To Delete a Policy	313
▼ To Verify a Policy	313
▼ To Activate a Policy	314
▼ To Back Up Your SunScreen Configuration	314
▼ To Restore Your SunScreen Configuration	314
Working With Services and Service Groups	314
▼ To Add a New Single Service	315
▼ To Add a New Service Group	315
▼ To Modify Service Groups	315
▼ To Rename a Service or Service Group	316
▼ To Rename References to a Service	316
▼ To Delete a Service or Service Group	316
▼ To Check References to a Service or Service Group	316
Addresses, Address Ranges, and Address Groups	317
▼ To Add a New Host Address	317
▼ To Add a Range of Addresses	317
▼ To Add an Address Group	318
▼ To Add an Address Range in CIDR Format	318
▼ To Delete an Address, Address Range, or Address List	318
▼ To Check References to a Deleted Address, Address Range, or Address List	319
▼ To Rename an Address, Address Range, or Address Group	319
Working With Certificates	319
▼ To Add Private Screen Certificates From a Diskette	320
▼ To Add Private Screen Certificates From a Directory	321
▼ To Add Screen Local Identities	321
▼ To Add Self-Generated Screen Certificates for Local Administration	322
▼ To Add Self-Generated Screen Certificates Using Remote Administration	323
▼ To Add Public Certificates from a Diskette or a File	325
Using Certificate Groups	326
▼ To Add Certificate Groups	326
▼ To Add a New Member to a Certificate Group	326
▼ To Remove a Member From a Certificate Group	326
▼ To Rename a Certificate or Certificate Group	327

▼ To Delete a Certificate or Certificate Group	327
▼ To Check References to a Deleted Certificate	327
▼ To Check References to a Deleted Certificate Group	328
IKE Policy Rule Syntax	328
▼ To Add Rules Using Keys Added on Both Screens	329
▼ To Work with IKE Rules with Pre-Shared Key	329
▼ To Work with IKE Rules with Self-Signed Certificates	330
▼ To Work with IKE Rules with Issued Certificates	332
Working With Screen Objects	333
▼ To Add a Screen	333
▼ To List the Screens	334
▼ To Add an SNMP Receiver to a Screen	334
▼ To Add Multiple SNMP Receivers to a Screen	334
▼ To Add a Time Status Indicator to a Screen	334
▼ To Remove SNMP Receivers From a Screen	334
▼ To Set a Screen to Stealth Mode	335
Interfaces	335
Overlapping Interfaces	335
▼ To Add Interfaces (in Routing Mode)	335
▼ To Add Interfaces (in Routing Mode) with a Detailed Log	336
▼ To Remove an Interface	336
Adding or Modifying an Authorized User	336
Configuration Editor authuser Subcommands	336
▼ To Add An Authorized User with Password Authentication	337
▼ To Add An Authorized User and SecurID Name	338
▼ To Display Authorized Users	338
▼ To Modify Authorized Users	338
▼ To Delete an Authorized User	339
Working With Policy Rules	339
▼ To Create a Packet Filtering Rule	339
▼ To Reorder the Rules	340
▼ To Delete a Rule	341
▼ To Edit Any Part of a Rule	341
Modifying Access Rules for GUI Local Administration	342
▼ To Add an Access Rule for GUI Local Administration	342
▼ To Edit an Access Rule for GUI Local Administration	342
▼ To Delete an Access Rule for GUI Local Administration	342

Modifying Access Rules for Remote Administration	343
▼ To Add an Access Rule for Remote Administration	343
▼ To Edit an Access Rule for Remote Administration	343
▼ To Delete an Access Rule for Remote Administration	344
Network Address Translation (NAT)	344
▼ To Add ARP Manually	344
▼ To Define NAT Mappings	345
▼ To Delete NAT Mappings	345
▼ To List the NAT Mappings	346
Virtual Private Network (VPN)	346
▼ To Add a VPN Gateway	346
▼ To Replace a VPN Gateway	347
▼ To Remove a VPN Gateway	347
Information, Statistics, and Logs	347
▼ To View the Information	347
▼ To View the Statistics	348
▼ To Set Logsize on a Screen	348
▼ To Set Up Packet Logging	348
▼ To Examine Packets	349
▼ To Display Packets in the Log File	349
▼ To View the Log	349
▼ To Save the Log	349
▼ To Clear the Log	349
▼ To Save and Clear the Log	350
Setting Up High Availability (HA)	350
▼ To Allow Non-Administrative Traffic on an HA Network	351
▼ To Remove an HA Screen	352
▼ To View HA Information	352
Centralized Management Groups (CMG)	353
▼ To Change a Screen Object to Put It in a Cluster	353
▼ To Remove a Screen from a Cluster	353
Getting Support for SunScreen Products	353
Gathering Data From the Screen	355
▼ To use the <code>ssadm lib/statetables</code> Command	355
▼ To Use the <code>ssadm lib/screeninfo</code> Command	355
▼ To Use the <code>ssadm lib/nattables</code> Command	356
▼ To Use the <code>ssadm lib/support</code> Command	356

▼ To Use the <code>ssadm lib/support help</code> Option	356
Troubleshooting	356
▼ To Use the <code>ssadm debug_level</code> Command	357
Installing and Configuring the Netscape Browser from the Command Line	357
▼ To Install and Configure the Netscape Browser	357
▼ To Save the <code>identitydb.obj</code> File	358
A About SunScreen Lite	361
Differences Between SunScreen and SunScreen Lite	361
Supported Features	361
Limitations	362
B Quick Start Procedures	363
Telnet Proxy Service Without Proxy User Authentication	363
▼ To Set Up the SunScreen Environment	364
▼ To Configure the Telnet Proxy Service	364
Telnet Proxy Service With Proxy User Authentication	365
▼ To Set Up the SunScreen Environment	366
▼ To Configure the Telnet Proxy Service	366
FTP Proxy Service Without Proxy User Authentication	368
▼ To Set Up the SunScreen Environment	369
▼ To Configure the FTP Proxy Service	369
▼ To Test the FTP Proxy Service	370
FTP Proxy Service With Proxy User Authentication	371
▼ To Set Up the SunScreen Environment	372
▼ To Configure the FTP Proxy Service	372
HTTP Proxy Service	374
▼ To Set Up the SunScreen Environment	375
▼ To Configure the HTTP Proxy Service	375
SMTP Proxy Service	376
▼ To Set Up the SunScreen Environment	376
▼ To Test Relay Blocking	378
Configuring RADIUS Authentication	380
▼ To Configure RADIUS Authentication	380
Telnet Proxy Service With RADIUS User Authentication	381
▼ To Configure the Telnet Proxy Service With RADIUS User Authentication	381

FTP Proxy Service With RADIUS User Authentication	382
▼ To Configure the FTP Proxy Service With RADIUS User Authentication	382
SecurID Clients Supported by SunScreen	383
▼ To Configure SecurID Authentication	384
Telnet Proxy Service With SecurID User Authentication	384
▼ To Set Up the Telnet Proxy Service With SecurID User Authentication	384
FTP Proxy Service With SecurID User Authentication	385
▼ To Set Up the FTP Proxy Service With SecurID User Authentication	385
Glossary	389
Index	401

Preface

SunScreen™ 3.2 for the Solaris™ operating environment is part of the family of SunScreen products that provide solutions for security authentication and privacy requirements. SunScreen enables companies to establish secure department networks that are connected to a public internetwork.

This *SunScreen 3.2 Administration Guide* provides all the information necessary to configure and administer SunScreen on your network. Other manuals in the SunScreen documentation set include:

- *SunScreen Installation Guide*
- *SunScreen 3.2 Administrator's Overview*
- *SunScreen 3.2 Configuration Examples*
- *SunScreen SKIP User's Guide, Release 1.5.1*

Who Should Use This Book

The *SunScreen 3.2 Administration Guide* is intended for SunScreen system administrators who are responsible for the operation, support, and maintenance of network security. In this guide, it is assumed that you are familiar with UNIX® system administration and TCP/IP networking concepts as well as with your network topology.

How This Guide Is Organized

The *SunScreen 3.2 Administration Guide* contains the following chapters and appendixes:

- Chapter 1 covers the basic concepts as well as the procedures for starting and configuring the Java™-based browser and logging in to the administration graphical user interface (GUI). It also shows how to define access levels for administrative users.
- Chapter 2 contains the procedures for using the administration GUI to add, delete, and rename common objects.
- Chapter 3 shows how to use packet filtering, administrative access rules, Network Address Translation (NAT), and virtual private networks (VPN).
- Chapter 4 explains how to create a policy file, which specifies how your SunScreen firewall will function. This chapter also contains many policy management procedures.
- Chapter 5 describes how to set up and manage a High Availability (HA) SunScreen configuration.
- Chapter 6 tells you how to use proxies to provide content filtering and user authentication.
- Chapter 7 describes how to set up multiple Screens to be managed from one location.
- Chapter 8 shows how to add additional remote Administration Stations to your network.
- Chapter 9 describes the information page in the administration GUI, how to view statistics and logs, and how to set the retrieval mode.
- Chapter 10 contains procedures for using the UNIX command line interface (CLI) to manage a SunScreen firewall.
- Appendix A describes the features and limitations SunScreen 3.2 Lite product, which is bundled with the current release of the Solaris operating environment.
- Appendix B contains detailed information about proxy services and SecurID and RADIUS authentication.

Related Books and Publications

You may want to refer to the following sources for background information on cryptography, network security, and SunScreen 3.2 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 Crosswhite 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.comSM Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is <http://docs.sun.com>.

Getting Support for SunScreen Products

If you require technical support, contact your Sun sales representative or Sun authorized reseller. See <http://www.sun.com/service/contacting/index.html> for information on contacting Sun and <http://www.sun.com/service/support/index.html> for information on Sun's support services.

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 <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% you have mail.</code>
AaBbCc123	What you type, contrasted with on-screen computer output	<code>machine_name% su</code> <code>Password:</code>

TABLE P-1 Typographic Conventions (Continued)

Typeface or Symbol	Meaning	Example
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	To delete a file, type rm <i>filename</i> .
<i>AaBbCc123</i>	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You must be <i>root</i> 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	#

Starting the Administration GUI and Logging In

This manual provides the information and instructions for configuration and management of the SunScreen firewall. The main part of the manual relies on the administrative graphical user interface (GUI). Chapter 10 describes how to configure and manage the firewall using the command line interface (CLI). The various features and theory behind SunScreen are discussed in the *SunScreen 3.2 Administrator's Overview*.

This chapter provides basic information you will use throughout the book. It assumes that you have already installed the Administration Station and Screen software using the information in the *SunScreen Installation Guide*.

After a brief discussion of SunScreen terminology, this chapter reviews basic browser requirements and shows how to use the administration GUI to perform basic tasks.

Terms Used in This Book

To manage the SunScreen firewall effectively, you need to understand certain terms, a few of which are defined below. Other terms are defined when they are first used. All terms can be looked up in the Glossary at the back of this manual.

The system running the firewall software is called a *Screen*. An *Administration Station* is a system used to configure and administer the Screen. An Administration Station can be located:

- At the local Screen
- At a remote location on your network
- At a remote location across the Internet

Use *common objects* to model your network configuration and topology. Common objects are the smallest units that you can define on a Screen. The addresses of networks and individual hosts, different services (network protocols), and the user names of people authorized to administer the Screen are examples of common objects.

Policy rules are the individual rules that implement a security *policy*. Policy rules describe the relationships between the common objects (for example, hosts that can communicate with each other). There are four types of policy rules:

- *Packet Filtering rules* describe network traffic flow policy.
- *Administrative Access rules* describe who can access the Screen and what they can do once they access it.
- *Network Address Translation (NAT) rules* describe network address translations.
- *Virtual Private Network (VPN) rules* describe the Screens that participate in a VPN and the hosts for which they provide the VPN.

A *policy* is a named set of policy rules. When you install SunScreen, an initial policy is created for you, based on the information you supply. The name of this policy is `Initial`.

New installations can be performed at three levels for routing mode (see “Deciding on Your Initial Security Level” in *SunScreen Installation Guide*). After a new “permissive” installation, the default policy rules leave everything “open”; in other words, there is no packet filtering or any other type of firewall activity until you specify it. New “secure” and “restricting” installations begin with different default levels of filtering in place.

For stealth mode, the installation comes up without any rules.

Administration GUI Browser Requirements

Using the Administration GUI, you can configure, administer, edit, and manage the Screen. You can use any browser that supports the Java™ platform and is compliant with JDK™ 1.1.3. You can use Netscape Navigator™, the HotJava™ browser, or Internet Explorer as long as the browser has the required Java support. The only restriction applies to accessing local system resources.

Note – The Netscape Java Plug-In provided with the Solaris 8 software is not compatible with the Administration GUI applet. To save log files and load certificates using a Netscape browser, you must install the required version of the Netscape Java Plug-In, as documented in the following sections.

Accessing Local System Resources

Because Netscape Navigator and Internet Explorer do not support the Java mechanism for applet signing, browser security mechanisms prevent the administration GUI from accessing your system's local resources.

The operations that require access to your local system resources are:

- Exporting and importing IKE certificates
- Loading certificates from a diskette
- Backing up all policies
- Restoring all policies
- Saving log files
- Loading Jar signatures

If you do not need to perform any of these operations, you can go to “To Log In to the Administration GUI” on page 27. If you need to access local system resources, you should read the following sections.

To work around local access limitations, you can use the Java Plug-In or the HotJava browser version. You can find versions of the Netscape and HotJava browsers, as well as the required Java Plug-In, on the SunScreen CD-ROM.

Note – The SunScreen Administration GUI requires a Java plugin that supports Java 1.1 features. This dependency creates interaction problems when the Java plugin 1.2 (or later) is already present on the system. The fix for this problem is to remove the Java 1.2 plugin from the system.

▼ To Install the Java Plug-In on the Screen

The documentation for the Java Plugin is on the Sun Website at <http://java.sun.com/products/plugin/1.1.3/readme.html>.

1. **Issue the following command to remove the Java 1.2 Plugin:**

```
pkgrm SUNWj2pi
```

2. **Make sure the SunScreen CD-ROM is still in the CD-ROM drive.**

3. Become root, if you are not already root.

4. Install the Java Plug-In for use by a single screen, type the following:

```
# volcheck
$ cp /cdrom/cdrom0/javaplugins/* /usr/lib/sunscreen/admin/htdocs/plugin/plugins/.
```

If you plan on sharing the Java plugin with Administration Stations, use the following instructions:

5. Save the file `identitydb.obj` on a diskette (see below) and distribute it to all Administration Stations.

▼ To Install on the Remote Administration Station.

1. Open a Web browser window on the remote Administration Station.

2. Download the plugin from the Screen using one of the following links.

- Java plugin for SPARC system from
`http://localhost:3852//plugin/plugins/plugin-112i-solsparc.sh.`
- Java plugin for x86 system from
`http://localhost:3852//plugin/plugins/plugin-112i-solx86.sh.`
- Java plugin for Windows system from
`http://localhost:3852//plugin/plugins/plugin-112i-win32.exe.`

3. On the remote administration station, execute the shell script.

a. If your system is a Solaris operating environment, type the following command at the shell prompt:

```
# chmod a+x file_name.sh
# ./file_name.sh
```

b. If your system is a Windows system, make sure that you have permission to execute the program and then execute the program.

▼ To Save the `identitydb.obj` File

After you install the Java Plug-In, next you install the `identitydb.obj` file.

1. If administration is done from a Solaris operating environment (local or remote), place the `/usr/lib/sunscreen/admin/htdocs/plugin/plugins/identitydb.obj` file in the `$HOME` directory of the user on the machine they are using for administration.

2. If administration is done from a Windows system, Use the following procedure:

- a. Obtain a DOS formatted diskette
- b. Insert the DOS formatted diskette in the floppy drive on the Screen.
- c. On the Screen, copy the file `identitydb.obj` to the diskette:

```
% volcheck
% cp /usr/lib/sunscreen/admin/htdocs/plugin/plugins/identitydb.obj /floppy/floppy0
```

- d. Use the diskette you just created to copy the `identitydb.obj` file to the appropriate location:
 - C:\WINDOWS directory for Windows 95/98/2000 users
 - C:\WINDOWS\PROFILES*username* for multiuser Windows 95/98/2000 systems
 - C:\WINNT\PROFILES*username* for Windows NT systems
- e. If the file `identitydb.obj` already exists in these locations, add SunScreen as one of the accepted signers to the file `identitydb.obj`.

Note – The SunScreen GUI can use a signed Java applet to provide access to functions that are normally restricted by a web browser. These functions include saving or loading SunScreen configurations and certificates to files on the local computer.

To verify the Java applet's signature, the web browser needs a copy of the certificate that was used to sign the applet. A copy of this certificate is installed with the SunScreen administration software in `/usr/lib/sunscreen/etc/SunScreenEFS.x509`. This is a file that you copy to your workstation or PC where the web browser will be run and add to your browser's list of trusted signers. Refer to your browser's documentation for detailed instructions on Java applet security.

▼ To Use the HotJava 1.1 Browser

You can add the HotJava 1.1 browser from the SunScreen CD. The package name is `SUNWdthj`. If you use the HotJava 1.1 browser and want to access local system resources, the browser's preferences must allow medium security for unsigned applets. To set this level of security:

1. Go to the browser's Edit menu.
2. Choose Preferences.
3. Choose Applet Security.

4. Choose the Medium Security radio button from the Unsigned Applets column.
5. Choose Apply.

Using the Administration GUI

▼ To Start the Administration GUI for Browsers Without the Java Plug-In

1. To connect to a Screen with local administration, type:

`http://localhost:3852`

2. To connect to a Screen with remote administration, type:

`http://Screen_Name:3852`

where *Screen_Name* is the name of the machine running the SunScreen software.

▼ To Start the Administration GUI for Browsers With the Java Plug-In

1. To connect to a Screen with local administration, type:

`http://localhost:3852/plugin`

2. To connect to a Screen with remote administration, type:

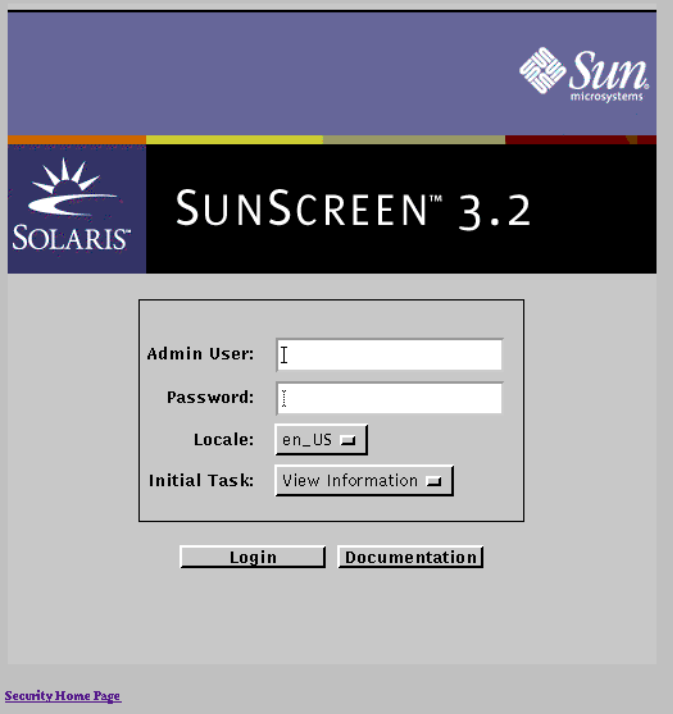
`http://Screen_Name:3852/plugin`

where *Screen_Name* is the name of the machine running the SunScreen software.

Note – HA Configurations Only: Use the name of the interface dedicated to high availability (HA) or to a dedicated Admin interface for all HA administration; otherwise, you will connect to the *currently active* HA host instead of the *primary* HA host.

▼ To Log In to the Administration GUI

You must log in with a user name and password every time you start the administration GUI. The initial user name and password are both `admin`.



The screenshot shows the SunScreen 3.2 administration GUI. At the top, there is a Sun Microsystems logo and the Solaris logo. The main title is "SUNSCREEN™ 3.2". Below the title, there is a login form with the following fields:

- Admin User:** A text input field.
- Password:** A password input field.
- Locale:** A dropdown menu showing "en_US".
- Initial Task:** A dropdown menu showing "View Information".

Below the form, there are two buttons: "Login" and "Documentation". At the bottom left, there is a link for "Security Home Page".

1. Type your Sunscreen Admin User name in the Admin User field.

The initial user name is `admin`. To change the Admin User, you can add another Authorized User and use that Authorized User name when you log into Sunscreen (see "To Add an Authorized User" on page 123).

2. Type your Sunscreen Admin User password in the Password field.

The default user password is admin. Change the password for the default login account as soon as possible to prevent unauthorized access to the Screen's policies. For a description on how to change passwords, see "Changing the Admin User Password" on page 30.

3. Select the locale.

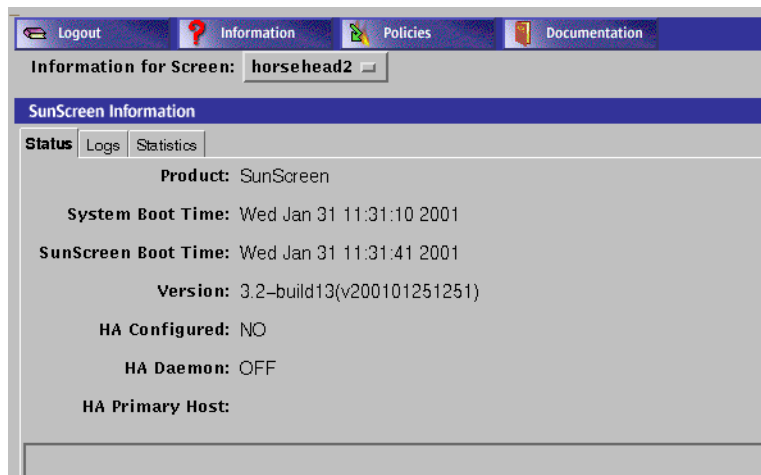
The default is en_US [English USA]. This also means that the libraries used to generate messages are in US English.

4. Select the initial task.

There are two choices for the initial task:

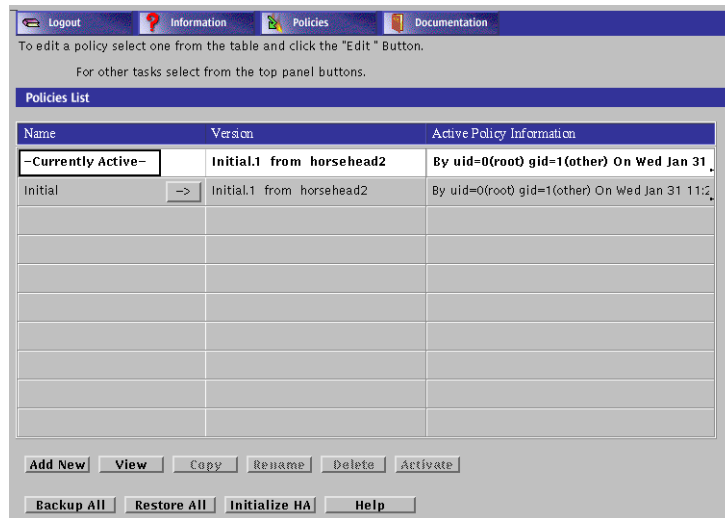
- **View Information**

The information page shows the current status of the Screen, enables you to view and manage the logs, and shows interface statistics.



- **Manage Policies**

The policies page enables you to create, edit, and manage SunScreen policies, policy rules, and common objects, including the Admin User IDs.



Once logged in, you can move between the Information and Policies pages by selecting the appropriate task from the administration GUI navigation buttons.

5. **Click the Login button to log in.**
Opens the page that you chose for the Select Task field after successful authentication.
6. **(Optional) Click the Documentation button to display online documentation.**
Click one of the links to open the appropriate documentation. You do not have to log in to look at the online documentation.

Administration GUI Navigation Bar and Buttons

The administration GUI navigation bar and navigation buttons, shown below, appear at the top of administration GUI pages. You should use these button for moving among the pages of the administration GUI.



If these buttons are missing from a page of the administration GUI, it means that you have unsaved changes from your editing session. Once you have saved your changes the buttons reappear.

The following table describes the administration GUI navigation buttons.

TABLE 1-1 Administration GUI Navigation Buttons

Control	Description
Logout	Logs out of the administration session, which clears any lock you may be holding.
Policies	Displays the Policies List page, where you add new policies. You can edit the policies for SunScreen on the Policy Rules page.
Information	Displays the Information page, where you can view the logs, product information, status of SunScreen, and the SKIP and IKE statistics.
Documentation	Displays the Documentation page, which contains links to the online SunScreen documentation.

Changing the Admin User Password

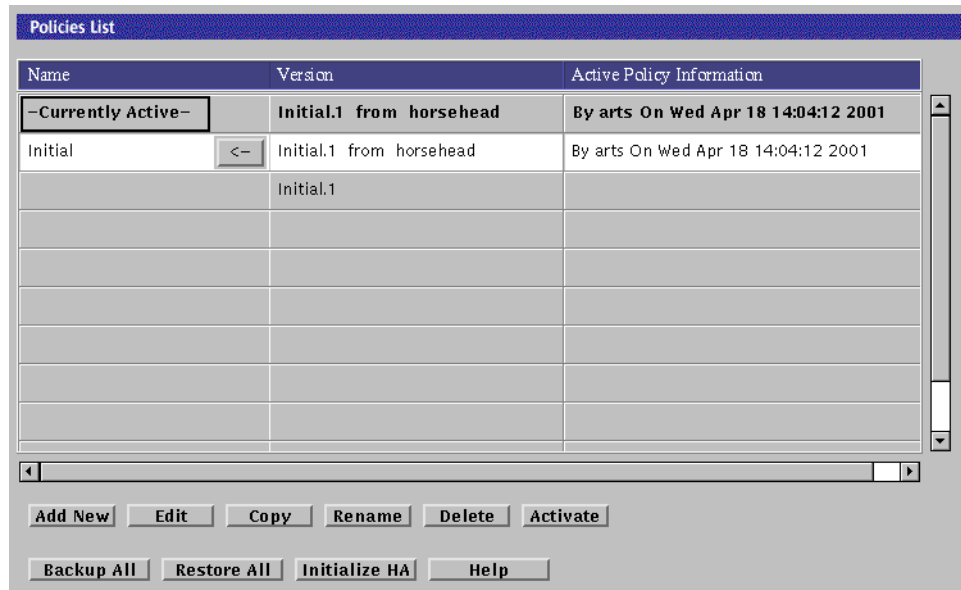
The security of the network relies on restricting the ability to change SunScreen rules to authorized people only, so changing the password for the admin user is extremely important.

▼ To Change the Admin User Password

1. **Log in to the Screen using the default admin user name and password if you have not already done so.**
2. **Select Manage Policies as the initial task.**
If you are already logged in, select Policies from the navigation buttons across the top of the page.
3. **Select the policy named Initial from the Policies List panel of the Policies List page.**

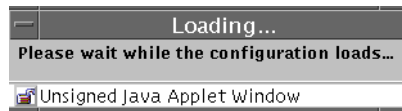
Note – Do not select the policy named Currently Active.

The Policy List page appears. The buttons below the policy list become active, and the Edit button changes from View to Edit.



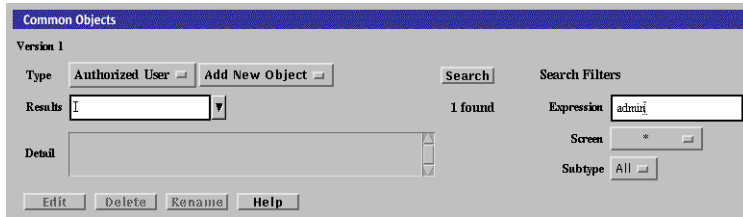
4. Click the Edit Button.

A *Please wait while the configuration loads...* warning window appears while the Policy Rules page is loading.



5. In the Common Objects panel, set the following variables:

- a. Select Authorized User for Type, and leave the action setting at Add New.
- b. Type admin in the Search String field.
- c. Select * for Screen.
- d. Leave Subtype setting at All.



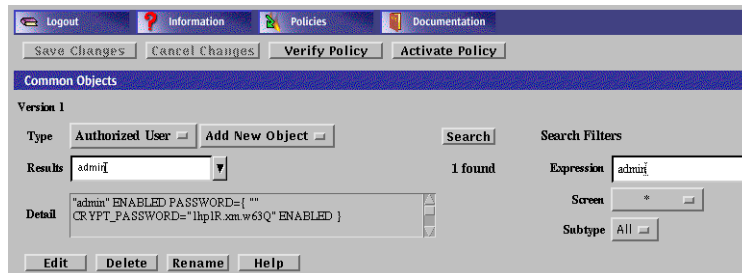
6. Click the Search button.

At the far right of the Results area, the text string 1 found appears.

7. Select admin in the Results area.

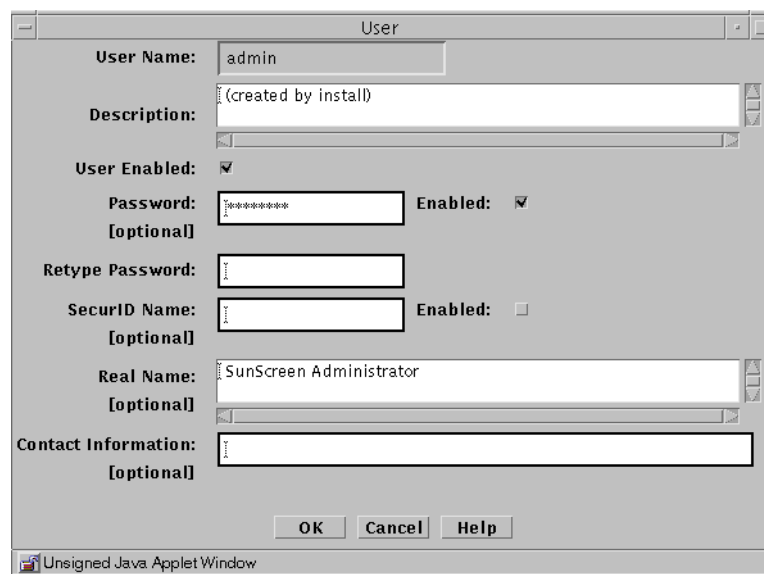
Note – You might have to scroll to see the admin setting in the Results area.

The **Detail** field displays the details of the admin, including the encrypted password.



8. Click the Edit button at the bottom part of the Common Objects panel.

The User dialog box appears.



9. **Deselect the User Enabled and Password Enabled check boxes, and type the new password twice.**
If you do not deselect the check boxes, you will not be able to edit the password.
10. **When you have finished typing and retyping the password, select the User Enabled and Password Enabled check boxes again, then click the OK button.**
If you do not select User Enabled and Password Enabled at this point, the admin user will not be active on the policies.
11. **Click Yes when asked to Activate the policy.**

Working With Common Objects

Common objects are the smallest building blocks you work with when managing your SunScreen. Common objects are used by (“common” to) all existing policies; any modification to these objects affects the operation of all policies.

This chapter describes:

- Using the Policy Rules page
- Adding, editing, deleting, renaming, and searching for common objects
- Viewing and editing details of a common object
- Adding services and service groups
- Adding host addresses, ranges, and groups of addresses
- Adding and deleting SNMP alert receivers
- Adding, generating, and loading SKIP UDHs
- Generating, importing, exporting and associating IKE certificates
- Adding a Screen
- Adding and editing interfaces
- Adding a time object

This chapter describes how to use the administration GUI to manipulate common objects. To perform the same tasks from the command line interface, refer to Chapter 10.

The following table provides a list of the procedures that are in this chapter.

TABLE 2-1 Common Object Procedures

Object	Procedure
Common Objects	"To Add a Common Object" on page 46
	"To Search for a Common Object" on page 46
	"To Edit a Common Object" on page 47
	"To Edit a Common Object From the Policy Rules Table" on page 49
	"To Delete a Common Object" on page 50
	"To Rename a Common Object" on page 51
Service Objects	"To Add a Service " on page 53
	"To Add a Service Group" on page 57
Address Objects	"To Add a Host Address " on page 60
	"To Add a Group of Addresses" on page 62
	"To Add a Range of Addresses" on page 64
Certificate Objects	"To Generate an IKE Certificate" on page 68
	"To Export an IKE Certificate" on page 70
	"To Import an IKE Certificate" on page 72
	"To Associate an IKE Certificate" on page 74
	"To Generate SKIP UDHs Certificates" on page 76
	"To Load a SKIP Issued Public or Private Certificate" on page 78
Certificate Group	"To Associate SKIP Certificate" on page 81
	"To Add a Certificate Group" on page 83
Certificate Group	"To Work with IKE Certificate Groups" on page 85
	"To Add an IPsec Key" on page 88
IPsec Key Object	
Screen Objects	"To Add a Screen" on page 98
	"To Add an SNMP Alert Receiver" on page 100
	"To Delete an SNMP Alert Receiver" on page 101

TABLE 2-1 Common Object Procedures (Continued)

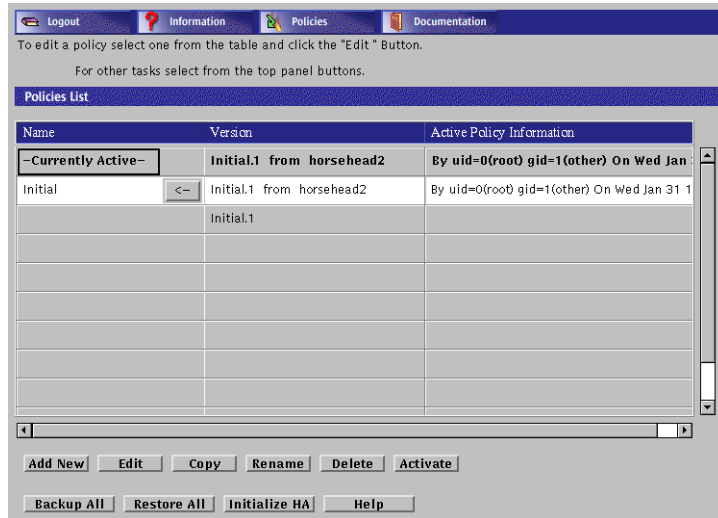
Object	Procedure
Interface Objects	"To Add or Edit Interfaces" on page 105
	"To Remove an Interface" on page 107
	"To Set up a Routing Interface" on page 107
	"To Set up a Stealth Interface" on page 109
	"To Change an Admin Interface From the Local Console" on page 112
	"To Change an Admin Interface From a Remote Console" on page 115
Jar Objects	"To Add a Jar Signature" on page 118
	"To Add a Jar Hash" on page 120
Authentication	"To Add an Authorized User" on page 123
Time Objects	"To Create Time Objects" on page 125

Using the Policy Rules Page

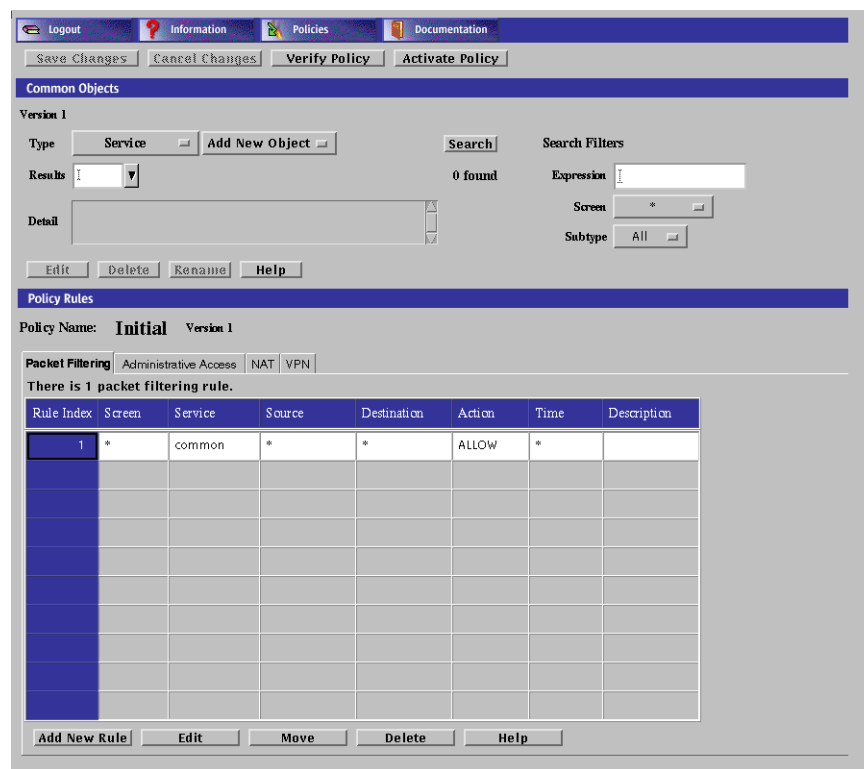
To add and modify the common objects, use the Policy Rules page of the administration GUI.

▼ To Modify the Policies Associated with a Common Object

1. Choose a policy in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.



Policies List Page

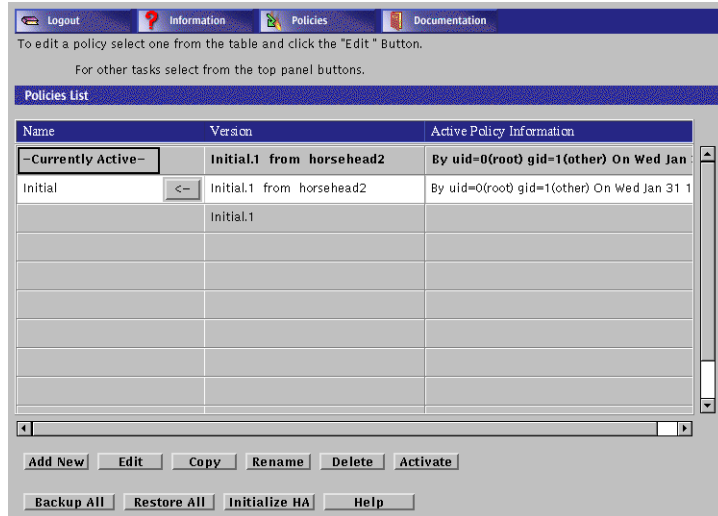
You reach the Policies List page by choosing Manage Policies for the Select Task field on the Login Page before you click the login button or by clicking the Policies button on the administration GUI's navigation bar.

You can move to the SunScreen Information page, display the online documentation, or log out by clicking the appropriate button on the administration navigation bar

The Policies List page allows you to add a new policy or to edit, copy, rename, delete, and backup a particular policy to a local file; to restore a policy from a local file; and to initialize HA.

The Policies List page identifies the policies that have been stored for a Screen. The List Policies page has two instructions under the top or navigation bar: "To edit a

policy select one from the table and click the 'Edit' button," and "For other tasks select from the top panel buttons."



Policies List Panel

Below the Policies List banner is a panel consisting of three columns that show:

1. The name – You must click a name of a policy that you want to edit in this column. The term “-Currently Active-” appears in this column for the active policy and the name and the version of the active policy appears in the version column.
2. The version (if present) – The version lists the versions of policies for your system.
3. The active policy information (if present).

The Policies List panel lists the policies that have been set up for a particular Screen. The active policy is the first policy in the list of policies and is automatically highlighted when you first come to this page. You can edit inactive Screen policies by clicking the name of an entry in the Policies List panel to highlight it, then click one of the controls at the bottom of the Policies List page.

Types of Policies

The types of policies are:

- Regular Policies – Policies that share common objects with other regular policies.

- Versioned Policies – A policy with a version number is displayed by clicking the button next to the regular policy name in the first column of Policies List Panel of the Policies List Page. Clicking the reverse arrow hides the versions of a policy. A policy with a version number contains a snapshot of the common objects that are embedded in the saved policy. The name of the policy contains a dot followed by an incremental number. The higher the number, the later the version. Versioned policies cannot be modified, but their rules can be extracted to a new policy.
- Currently Active Policy – This policy is extracted from the active policy. The currently active policy cannot be modified. If you click the currently active policy and highlight it, the edit button retains the (RO) designation to show that it is read only. A Save As button appears on the Policy Name line on the Packet Filtering tab of the Policy Rules panel. You can save any modifications to the currently active policy as a new policy. A Save As button appears on the Common Objects panel. You can save the common objects of this policy to replace the current common objects associates with regular policies.

This allows you to make the common objects embedded in this version of the policy the current common objects, overwriting the existing set of common objects.

This approach allows you to save only the rules part of the versioned policy so that:

- These rules become the current rules for this policy, for example the rules for policy Initial.10 can be made the rules for the current version of Initial.
- You can copy the rule to a new name.

Note – The rules created in this way are used with the current set of common objects. On verifying this policy, you may have to fix any inconsistencies.

The difference in behavior between Save As and Edit(RO) is that Save As affects the current policy only and Edit(RO) affects a policy version. With Edit(RO), you have the additional choice of making the rules the current rules for the policy.

Policies List Page Action Buttons

The following table describes the action buttons for the Policies List page.

TABLE 2-2 Action Buttons on the Policies List Page

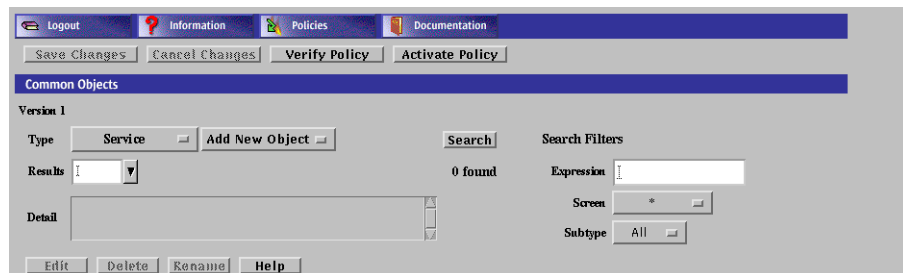
Control	Description
Add New button	Opens a dialog box that prompts you for the name of the policy that you want to add. The name for this new policy appears on the policies list panel. You add the rules for the new policy on the Policy Rules page.

TABLE 2-2 Action Buttons on the Policies List Page *(Continued)*

Control	Description
Edit button	Opens the Policy Rules page for the policy that you have highlighted and allows you to change the parameters. If the Edit button displays (RO), it means that the policy that you highlighted is read-only. The read-only mode applies only to the active policy and the policy versions in the version column: <ul style="list-style-type: none">■ You cannot modify an active policy.■ You must click the name (the first column of the policies list panel) to highlight the policy that you want to edit.
Copy button	Opens a dialog box that prompts you for the new name of the policy to which you want to copy the information from the policy that you highlighted on the Policies List panel.
Rename button	Opens a dialog box asking for the new name you want to assign to the selected policy on the Policies List panel.
Delete button	Opens a dialog box asking you to confirm you want to delete the selected policy on the Policies List panel.
Activate button	Activates the selected policy on the Policies List panel for the Screen. After you click the Activate button, the version and active policy information are updated in the highlighted row.
Backup All button	Opens the Backup All dialog box, which enables copying the policies to a file or diskette. You cannot use the Backup All button if you are using a browser whose security restrictions do not allow access to the file system from applets. Most browsers have plug-in modules that permit you to back up your policies to a local file or diskette. The backup medium contains copies of the local identities (the encryption keys and certificates) and must be stored securely and disposed of securely to avoid compromising your security.
Restore All button	Opens the Restore All dialog box, which enables restoring the policies from a file or diskette. The restore operation causes the information from the backup file to overwrite all current policy information. You cannot use the Restore All button if you are using a browser whose security restrictions do not allow access to the file system from applets.
Initialize HA button	Opens the Initialize HA dialog box. This dialog box contains the statements that you need to be connected to the HA primary to perform this operation and that you must select the interface you would like to be the HA interface for the primary. This dialog box presents a choice list of all the interfaces available.
Help button	Opens the online help.

Using Common Objects

Use the Common Objects area of the Policy Rules page to add common objects and construct policy rules. The changes you make to the common objects do not affect the currently active policy until you activate them.



The following table describes the information, controls, and the buttons in the Common Objects Panel.

TABLE 2-3 Common Object Information, Controls, and Buttons

Information	Control	Description
Version		The version of the registry of common objects that is being used in a policy. The latest version of the registry is used by all policies. If you edit the common objects (registry) the word “modified” appears after the number until you either cancel the changes or save the changes.
Type	Common Object Choice List	Displays the list of common objects available. You choose the common object that you want from this list.
	Subtype Choice List for Adding a New Common Object of Chosen Type	Displays the choice list of subtypes available for the common object that you selected. Each common object has its own set of subtypes and each subtype requires that you provide different information in a dialog box for that subtype for that common object.

TABLE 2-3 Common Object Information, Controls, and Buttons *(Continued)*

Information	Control	Description
Search	Search String	Enter the string for a particular subtype for a common object in this editable text field. When you click the Search button, all matching subtypes appear in the Results choice list. Leaving this field blank returns all entries defined for the selected subtype or local to the selected Screen. Selecting All in Search on Screens and Search Subtype Choice with the Search String field empty returns all entries defined.
	Search on Screen	Displays a choice list of the Screens that the Administration Station manages. Selecting a Screen from this list limits the search to common objects exclusive to that Screen.
	Search Subtypes	Display a choice list of the subtypes available for the selected common object.
	Search Button	Starts the search according to the criteria set.
	Results	Displays a choice list of available entries that match the criteria.
Found		Show the number of entries in the search that match the criteria.
Detail		Displays the description for the item chosen from the Results choice list.
	Edit Button	Displays the dialog box for the common object selected. Editing a common object is similar to adding a new one. The difference is that after you have chosen the common object that you want to edit and have clicked the Edit button, the dialog box for that common object contains all the information and you only need to modify the requisite information.
	Delete Button	Displays the Delete dialog box.
	Rename Button	Displays the Rename dialog box.
	Help Button	Displays online help.

The following table lists the common objects used in SunScreen.

TABLE 2-4 Common Object Descriptions

Common Object	Use
Address	Defines the network elements that make up the policy
Authorized User	Describes an administrator for your Screen administration
Certificate	Defines the certificates used for SKIP and IKE connections
Interface	Defines the Screen's network interface ports.

TABLE 2-4 Common Object Descriptions (Continued)

Common Object	Use
Jar Hash	The Java archive hash for HTTP proxy dialog filtering
Jar Signature	The Java archive signature for HTTP proxy dialog filtering
IPsec Key	For IPsec manual keys
Proxy User	Defines the proxy user name for an authorized user
Screen	Defines values and objects to a specific Screen
Service	Defines network protocols
Time	Defines time intervals for time-dependent rules

Some of these objects are saved automatically every time they are edited or new objects are added. Although the changes apply immediately and cannot be cancelled, they do not take effect until the policy is activated. The automatically saved objects are:

- Authorized user
- Jar hash
- Jar signature
- Proxy user

The Screen Field and Common Objects

The Screen field provides a way to define an object or rule for a specific screen in a scenario that utilizes multiple Screens, specifically when you use Centralized Management Groups. It has no effect on standalone Screen administration.

SunScreen allows you to use the same name for different common objects if you select different Screen objects for them. You may also define different parameters for these common objects; the Screens to which they refer then interpret them locally.

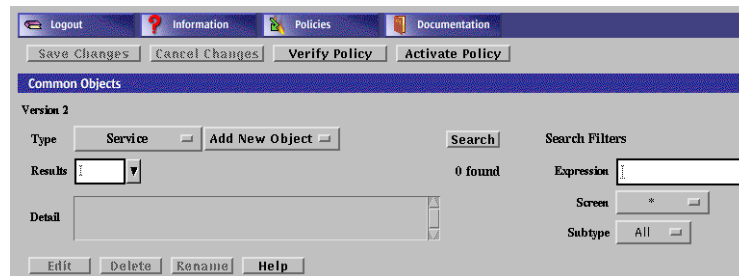
An object with "*" selected applies to all Screens. This is the default, and is recommended for all objects unless there is a need to use a single name more than once.

Rules whose Screen field is blank apply to all Screens. Rules with a specific Screen object selected apply only to that Screen.

▼ To Add a Common Object

You use the same steps to add all common objects. The dialog boxes vary according to the common object selected.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select the Common Object in the Type list.

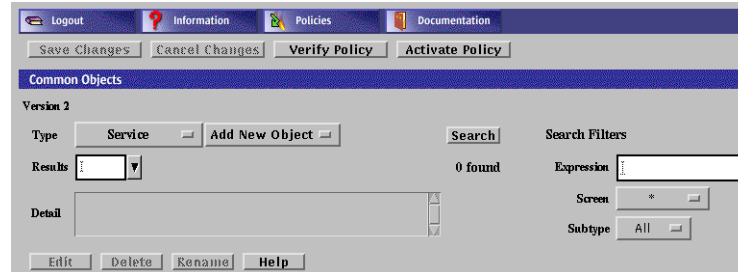


3. Click the Add New Object button to display the choices.
4. Type the necessary information in the dialog box.
5. Click the OK button.

▼ To Search for a Common Object

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Common Object in the Type list.



3. (Optional) Type or select values in the search filters.

The results depend on whether the common object matches one of the three search criteria for the selected type. The search criteria are:

- Expression This field restricts the search to names that match a specified character pattern. Leaving the field blank returns all names.
- Screen This field restricts the search to match a specified screen. Leaving the field an asterisk (*) returns all names.
- Subtype This field returns all objects when set to All. If you select a specific subtype, the search returns those objects that match the subtype.

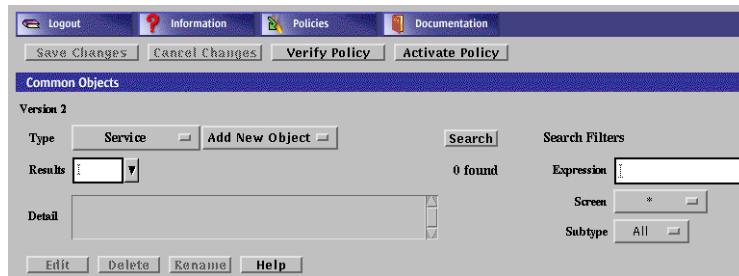
4. Click the Search button or press Enter in the Expression field.

5. Select a result from the Results area to retrieve and display its properties in the Detail field.

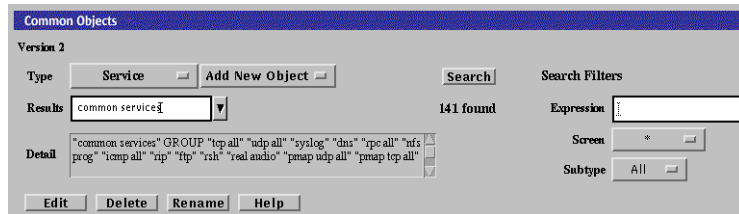
After you retrieve the common object, you can edit, rename, or delete it.

▼ To Edit a Common Object

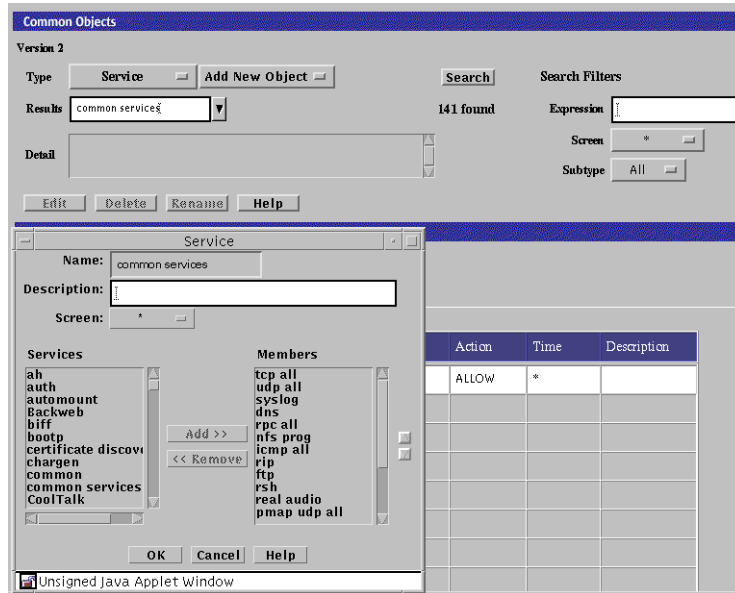
1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Common Object in the Type list.



3. (Optional) Select the search criteria.
4. Click the Search button.
5. In the Results area, select the name of the common object to edit.
The details for the selected common object are displayed.



6. Click the Edit button.
The dialog box for the object appears.



7. Make your changes in the dialog box.

8. Click the OK button.

▼ To Edit a Common Object From the Policy Rules Table

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Click once on the cell in the Policy Rules Table that contains the object to be viewed or edited.

The dialog box for the chosen object appears.



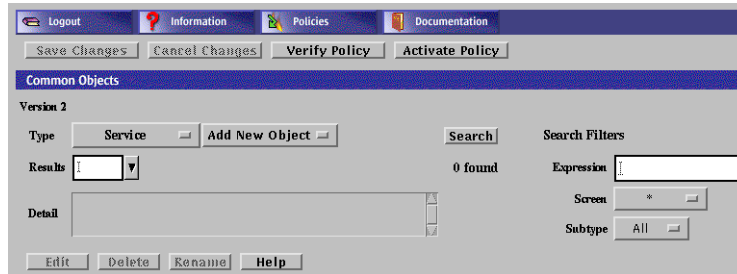
Note – If more than one common object uses a particular name, you may not be able to display the details for the object by clicking on the table cell. In such cases, you must search for desired object and select it.

3. Edit the object if necessary.
4. Click the OK button.

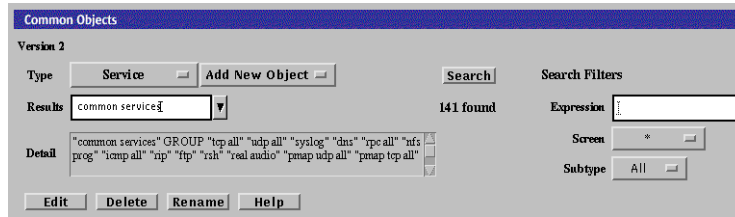
▼ To Delete a Common Object

If you delete a named common object (such as address, service, or certificate) that is being used in a policy object, SunScreen displays a warning message before it deletes the object.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Common Object in the Type list.



3. Select the search criteria.
4. Click the Search button.
5. From the Results area, select the name of the common object to delete.



6. Click the Delete button.
7. Click Yes in the Delete Rule dialog box.

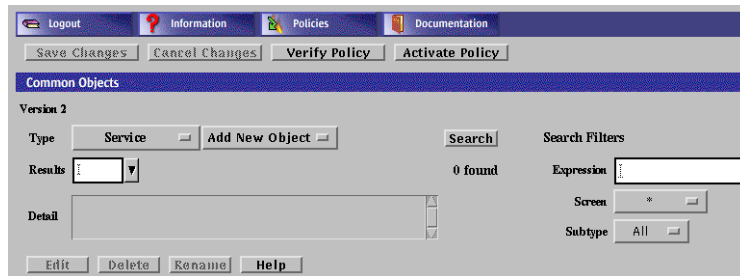


Note – Be careful not to remove your Administration Station’s address from its interface address group. If you do, you will be unable to administer your Screen after you activate the next policy.

▼ To Rename a Common Object

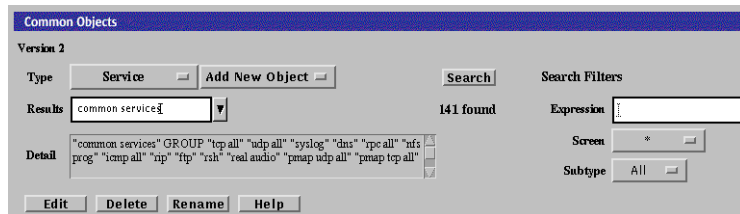
When you rename a common object with no Screen object, you also rename all references to the object in the current policy.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Common Object in the Type list.



3. Click the Search button.

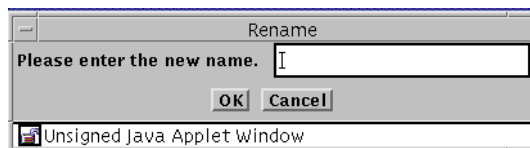
4. From the Results area, select the name of the common object to be renamed.



5. Click the Rename button.

The Rename dialog box appears.

6. Type the new name in the Please Enter the New Name field.



7. Click the OK button.

Service and Service Group Objects

When setting up your network security policy, you need to decide which network services to make available to hosts on your internal network and which services to make available to hosts on the external network. Most sites need to determine policy rules that govern basic services.

SunScreen provides many *predefined* network services and service groups, such as `www`, `http`, `ftp`, `telnet`, and `dns`. You can change the default values of a service or add a new service as needed. (See “Services and State Engines” in *SunScreen 3.2 Administrator’s Overview* for a list of services and service groups.)

You can define both single services and service groups (clusters of single services that you want to use together.) The services that are available for use in the policies are installed as part of the SunScreen software.

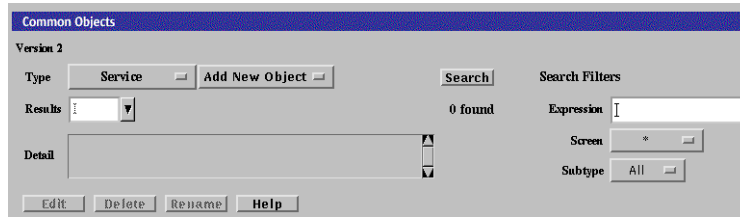
In addition to the basic services, every TCP/IP implementation provides services such as `echo`, `discard`, `daytime`, `chargen`, and `time`. For services such as `ftp`, you may want to allow anyone in the internal corporate network to send outbound traffic, but only allow inbound traffic in this protocol to go to the FTP server. This requires two rules: one for the outbound traffic and one for the inbound traffic going to the public server.

Each service uses a *state engine*, a sort of protocol checker. For example, the FTP state engine checks port numbers when the `ftp` service is being used. For more information on state engines, see “Services and State Engines” in *SunScreen 3.2 Administrator’s Overview*.

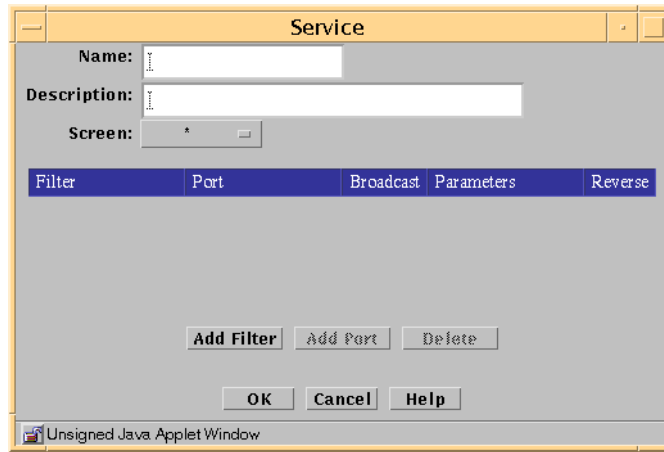
▼ To Add a Service

Note – Although you *can* change the default values for a service, the preferred method is to add a new service with the new values. This makes troubleshooting easier.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Service in the Type list.



3. Click **New Single** from the **Add New Object** list.
The **Service** dialog box appears.



The following table describes the controls in the Service dialog box for a single service.

TABLE 2-5 Controls for Service Dialog Box for Single Service

Control	Description
Name	Specifies the name of the service object.
Description	(Optional) Provides a brief description about the service object.
Screen	(Optional) Restricts the service so that it applies to the selected Screen only. The default (All) means that <i>all</i> Screens recognize this object unless an object exists that has been specifically defined for a particular Screen and has the same name as the Screen for which it is defined.
Filter Table Information	

TABLE 2-5 Controls for Service Dialog Box for Single Service (Continued)

Control	Description
Filter Table	Display the parameters for the single services. <ol style="list-style-type: none">1. The Add Filter button Adds a row to the filter table so that you can define additional forward filters for the service.2. The Add Port button adds ports for use by the forward filter. This field becomes active when you click the port field of the filter table.3. The Delete button the highlighted row in the table. You click a row in the table to highlight it.
Filter	Identifies the state engine.
Port	Identifies the port number, program number, or type used by the forward filter.
Broadcast	Determines whether the rules in which the service is used allows communication to broadcast or multicast addresses. If you want the service to work for nonbroadcast addresses, you must enter a separate table entries for broadcast and nonbroadcast entries
Parameters	Overrides the default values the selected packet-filter state engine. Each state engine has a set of parameters; refer to "Services and State Engines" in <i>SunScreen 3.2 Administrator's Overview</i> for default parameters values and their meaning.
Reverse	Determines whether the filter applies to packets originating from the host in the To address of a rule and going to the From address of a rule.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Displays the page of online help for this common object.

4. Type the name for this new service in the Name field.

For example: **ftp-34**

5. (Optional) Type a description for this service in the Description field.

For example: **Use ftp-34 instead of the supplied ftp service.**

The description appears in the Service Details field that displays when you choose a service or service group for a rule.

6. (Optional) Select a Screen from the Screen list.

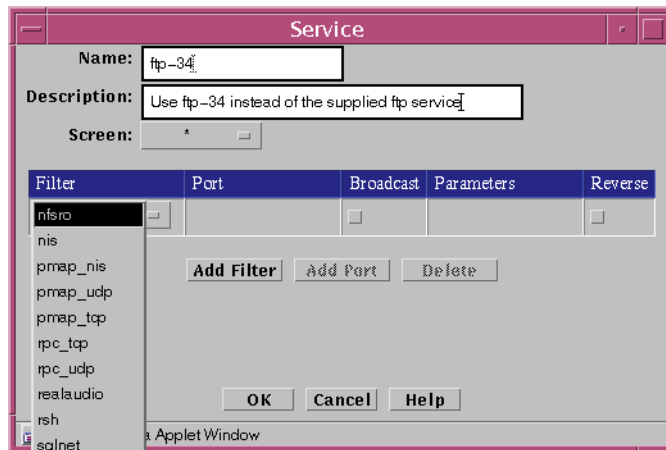
7. Click the Add Filter button.

This adds an entry to the filter list.

8. Select a filter from the list.

You can use the Add Filter button as necessary to select the filters that you need for a particular service.

9. (Optional) If you have too many filters:
 - a. Select the Parameters field to highlight the line that contains the unwanted filter.
 - b. Click the Delete button to delete the filter.
 - c. Repeat these steps until all unwanted filters are deleted.
10. Click the select box in the Filter field to display the list of service filter engines.



For each filter desired:

- a. Click the Select box under Filter.
 - b. Choose a filtering engine from the list displayed.
 - c. Click the Reverse box, if the service operates in the reverse direction.
Reverse is a seldom-used option for specifying asymmetric inbound traffic, such as traceroute and router discovery services.
11. Type the port number for the new service in the Port field.
You can use the Add Port button as necessary to add an additional set or sets of ports that you need for a particular filter. As a rule, you need to use the Add Port button only when you must specify a discontinuous set of port numbers, such as "1024-1028" + "1030-1048". If you have too many ports, follow the steps below to delete them:
 - a. Click the Add Port button to add the necessary ports.
 - b. Select the parameters field to highlight the line that contains the unwanted port.

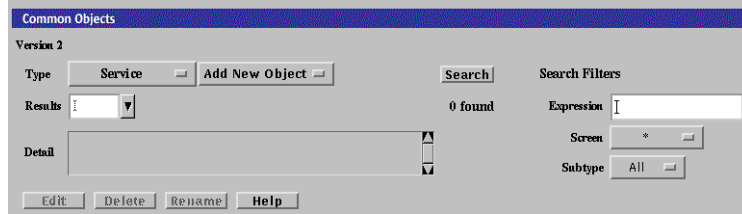
- c. Click the **Delete** button to delete the unwanted port.
12. **(Optional) To override the default values for the filter that you have selected, change the default values by typing the values that you want to use.**
13. **Click the Broadcast button if the service sends IP broadcast packets.**
If the service sends both broadcast and non-broadcast packets (for example, the standard `rip` service), you will need two ports: one with the broadcast box checked and one with the broadcast box unchecked.
14. **(Optional) If you want to override the default parameters for the filter that you have selected, type the required number of parameters, separated by spaces.**
You need to type in parameters only if you do not want to use the default values. For information about the default values for these fields, see “Services and State Engines” in *SunScreen 3.2 Administrator’s Overview*.
15. **Click the OK button to place this service definition in the policy file.**
The service `ftp-34` now appears in the list of services.
16. **Repeat the above steps until you have added all the services necessary for your policy.**

▼ To Add a Service Group

Note – Although you can modify the default services in service groups, the preferred method is to add a new service group that contains the services that you want. This makes troubleshooting easier.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Service in the Type list.



3. Select New Group from the Add New Object list.
The Service dialog box is displayed.



The following table describes the controls in the Service dialog box for service group.

TABLE 2-6 Controls for Service Group Service Dialog Box

Control	Description
<i>Name</i>	Specifies the name of the service object.

TABLE 2-6 Controls for Service Group Service Dialog Box (Continued)

Control	Description
<i>Description</i>	(Optional) Provides a brief description about the service object.
<i>Screen</i>	(Optional) Restricts this service group applies to the selected Screen only. The default (All) means that <i>all</i> Screens recognize this object unless an object exists that has been specifically defined for a particular Screen and has the same name as the Screen for which it is defined.
Services List	Identifies the services that do not belong to the service group. Refer to “Services and State Engines” in <i>SunScreen 3.2 Administrator’s Overview</i> for a description of services.
Members List	Identifies the services that belong to the service group.
Add Button	Moves the service selected in the Services list to the Members list, making the service a member of the specified service group.
Remove Button	Moves the service selected in the Members list to the Services list, removing the service from the specified service group.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. **Type the name for the new service group in the Name field in the Service dialog box.**
5. **(Optional) Type a description for this new service group in the Description field.**
The description appears in the Service Details field that displays when you choose a service or service group for a rule.
6. **(Optional) Choose a Screen from the Screen list.**
7. **Select the service or service group that you want to include in this new service group.**
8. **Click the Add button to move the chosen service or service group to the Members list.**
9. **Click the OK button.**
10. **Repeat the above steps until you have added all the service groups required.**

Address Objects

SunScreen identifies network elements—networks, subnetworks, and individual hosts—by mapping a named address *object* to one or more IP addresses. Address objects are used:

- To define the network elements that make up the policy
- To define the network interfaces
- As the source and destination addresses for policy rules and for NAT

Each rule must have a source address and a destination address.

An address object can represent a single computer or a whole network. You can gather address objects that represent individual and network addresses to form address groups. You may define address objects that specifically include or exclude other address objects (single IP hosts, ranges of contiguous IP addresses, or groups of discontinuous IP addresses). Some addresses are already defined.

An individual host is identified by linking its unique IP address to an address object. The address object can use the name or IP address of the host.

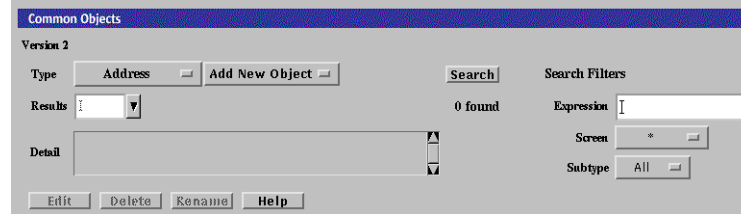


Caution – If you change the Admin address, the admin certificate, the local certificate, or the admin-group certificate, you risk losing connectivity from the Administration Station to the Screen. Reestablishing connectivity is difficult and requires you to log into the Screen directly or to use an Administration Station that is still working. It also requires exchanging encryption information.

▼ To Add a Host Address

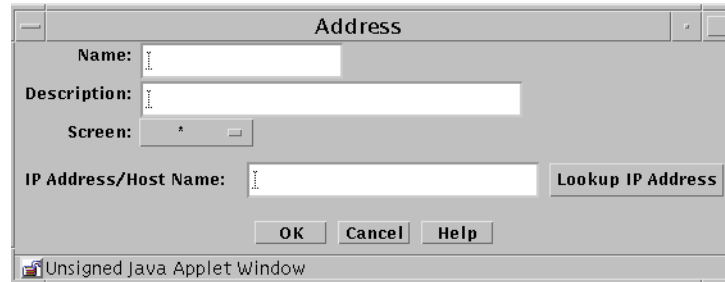
1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Address in the Type list.



3. Select New Host from the Add New Object list.

The Host Address dialog box appears.



The following table describes the controls in the Address dialog box for a new host.

TABLE 2-7 Controls for New Host Address Dialog Box

Control	Description
Name	Specifies the name for the address object.
Description Field	(Optional) Provides a brief descriptive note about the address object.
Screen	(Optional) Restricts this address so that it applies to the selected Screen only. The default (All) means that <i>all</i> Screens recognize this object unless an object exists that has been specifically defined for a particular Screen and has the same name as the Screen for which it is defined.
IP Address/Host Name	Specifies the IP address you want to associate with the address object identified in the Name list.
Lookup IP Address Button	If SunScreen has access to DNS or NIS, lets you look up host addresses by host name.

TABLE 2-7 Controls for New Host Address Dialog Box (Continued)

Control	Description
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type the name for this new address in the Name field.

For example: **NewAddr**

5. (Optional) Type a description in the Description field.

The description appears in the Address Details field that is displayed when you use the Rule Definition dialog box to choose an address or address group for a rule.

6. (Optional) Select a Screen from the Screen list.

7. Type the IP address in the IP Address/Host Name field.

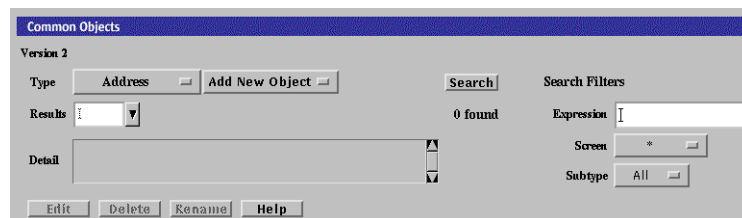
For example: **100.100.20.10**

8. Click the OK button.

▼ To Add a Group of Addresses

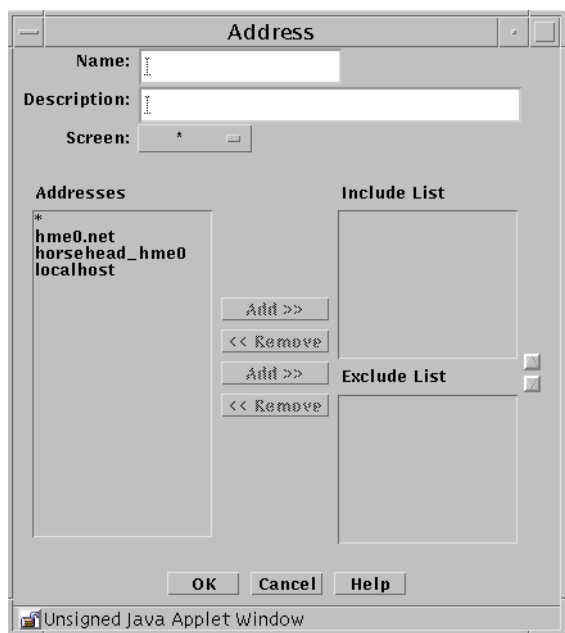
1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Address in the Type list.



3. Select New Group from the Add New Object list.

The Address dialog box appears.



The following table describes the controls for the Address dialog box for new group.

TABLE 2-8 Controls for the New Group Address Dialog Box

Control	Description
Name	Specifies the name for the address object.
Description	(Optional) Provides a brief description about the address object.
Screen	(Optional) Restricts this address group so that it applies to the selected Screen only. The default (All) means that <i>all</i> Screens recognize this object unless an object exists that has been specifically defined for a particular Screen and has the same name as the Screen for which it is defined.
Addresses	Displays the addresses objects that can to be used to create the address group.
Include List	Specifies the address objects that are currently included in the address group. Use the Add or Remove buttons to modify the list.
Exclude List	Specifies the address objects that are excluded from the address group. For example, you can create an address group that includes all addresses except as specified in the Exclude List. Use the Add or Remove buttons to modify the list.

TABLE 2-8 Controls for the New Group Address Dialog Box (Continued)

Control	Description
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type the name for this new address group in the Name field.

For example: **GroupName**

5. (Optional) Type a description in the Description field.

The description appears in the Address Details field that is displayed when you choose an address or address group for a rule using the Rule Definition dialog box.

6. (Optional) Select a Screen from the Screen list.

7. Select an address from the Addresses list.

8. Use the Add button to move the address to the Include list or to the Exclude list.

Use the corresponding Remove button to remove addresses from the lists.

9. Continue to build the intended address group by adding to the Include lists.

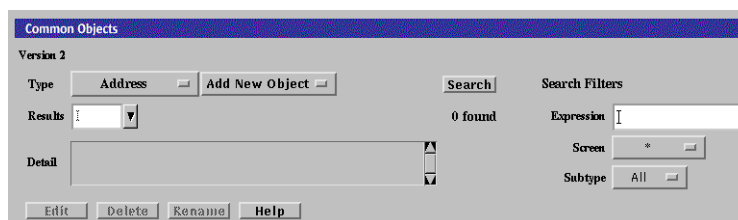
10. Click the OK button.

▼ To Add a Range of Addresses

An address range is a set of numerically contiguous IP addresses, identified by the starting and ending *addresses* or using the CIDR notation. Networks and subnetworks are typically identified by an IP *address range* name. You can set up an address object to represent an address range.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Address in the Type list.



3. Select New Range in the Add New Object list.

The Address dialog box appears.



The following table describes the controls for the Address dialog box for new range.

TABLE 2-9 Controls for New Range Address Dialog Box

Control	Description
Name	Specifies the name for the address object.
Description	(Optional) Provides a brief description about the address object.
Screen	(Optional) Restricts this range of addresses so that it applies to the selected Screen only. The default (All) means that <i>all</i> Screens recognize this object unless an object exists that has been specifically defined for a particular Screen and has the same name as the Screen for which it is defined.
Starting IP Address	Specifies the starting IP address in the range.
Ending IP Address	Specifies the ending IP address in the range.

TABLE 2-9 Controls for New Range Address Dialog Box *(Continued)*

Control	Description
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type the name for this new address range in the Name field.

For example: **AddrRange**

5. (Optional) Type a description in the Description field.

The description appears in the Address Details field that is displayed when you choose an address or address group for a rule using the Rule Definition dialog box.

6. (Optional) Select All from the Screen list.

7. If you are using the Range Syntax, type the Starting IP address in the Starting IP Address field.

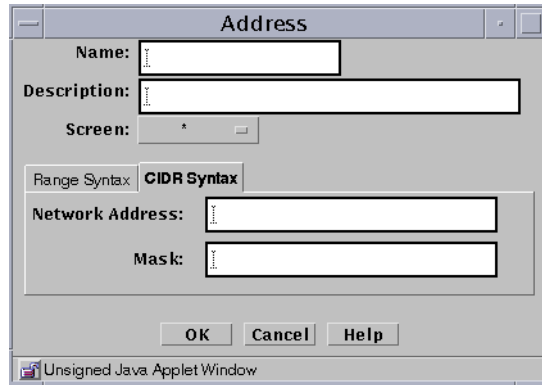
For example: **100.100.20.10**

8. If you are using the Range Syntax, type the Ending IP address in Ending IP Address field.

For example: **100.100.20.90**

9. Clicking the CIDR Syntax tab to use the CIDR Syntax for defining a Range of Addresses.

The CIDR Address dialog box appears



10. If you are using the CIDR Syntax tab, type the network address (for example, 10.100.20.0) and the network mask (for example, 255.255.255.0, or 24).

11. Click the OK button.

Certificate Objects

If you are using remote administration, the certificate for the Screen and the certificate for the remote Administration Station were created, and the hashes exchanged, during the installation procedure.

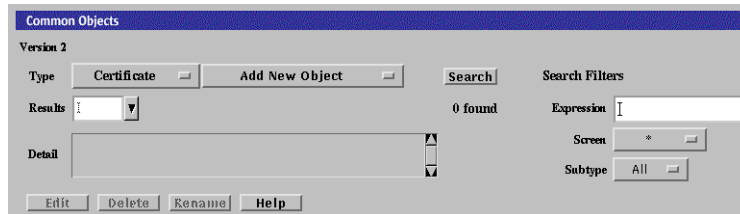
You can combine certificates into groups for ease of use and convenience.

Note – Store the diskette that contains the certificate safely and securely. It contains sensitive information that is *not* encrypted.

▼ To Generate an IKE Certificate

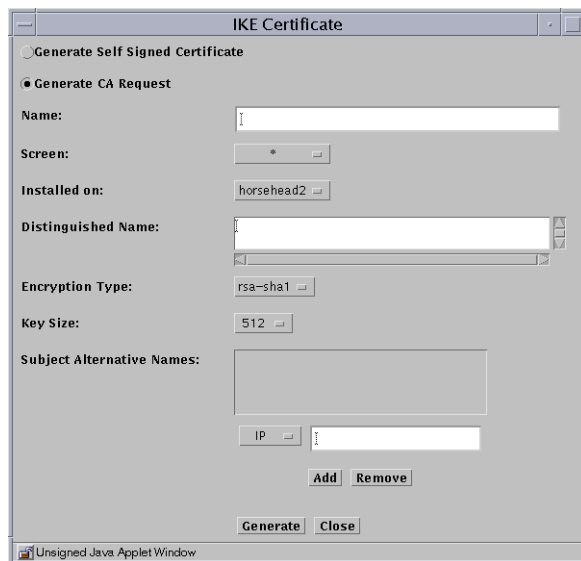
Unlike SKIP, installing a remote administration station does not automatically create an IKE certificate. Perform the following steps on the primary Screen to generate a new certificate:

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Certificate from the Type list.



3. Select Generate IKE Certificate from the Add New list.

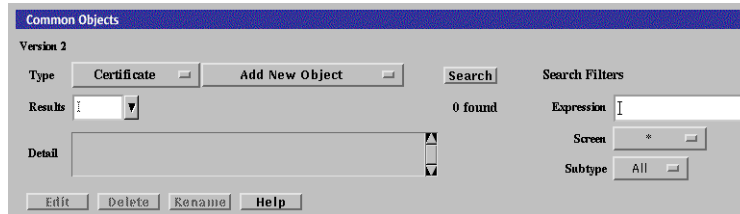
The certificate dialog box appears with options for the type of key to generate. The default value for the Encryption Type is rsa-sha1. The default Key Size is the lowest available.



4. Select if you want to use a self-generated certificate or a certificate request for a certificate authority to sign.
5. Type a name in the Name field.
6. (Optional) Type a description in the Description field.
7. (Optional) Select the Screen from the Screen list.
8. Select the Screen the certificate is installed on from the Installed On list.
9. Type an X.509 distinguished name for the certificate subject in the Distinguished Name field. The distinguished name typically has the form of C=Country, O=Organization, OU=Organizational_Unit, and CN=Common_Name.
10. Select the Encryption Type. You can select rsa-sha1, rsa-md5, or dsa.
11. Select the Key Size. The default is the lowest available.
12. Click the Generate button.
13. Click the OK button.

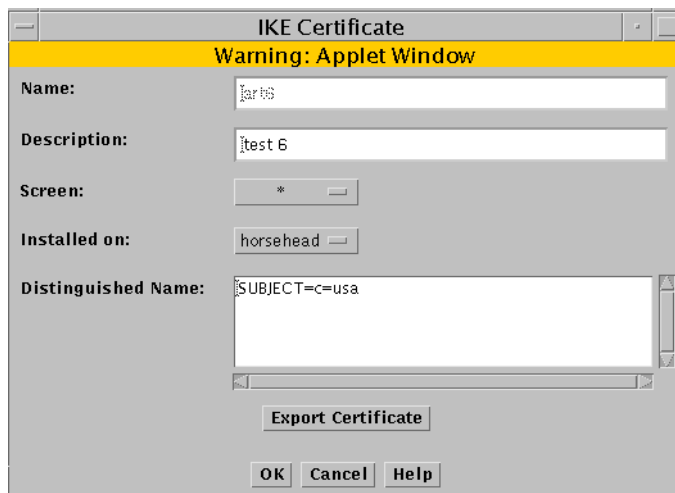
▼ To Export an IKE Certificate

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Certificate from the Type list.



3. Click Search.
4. Select the certificate you want to export from the list in the Results area.
5. Click the Edit button.

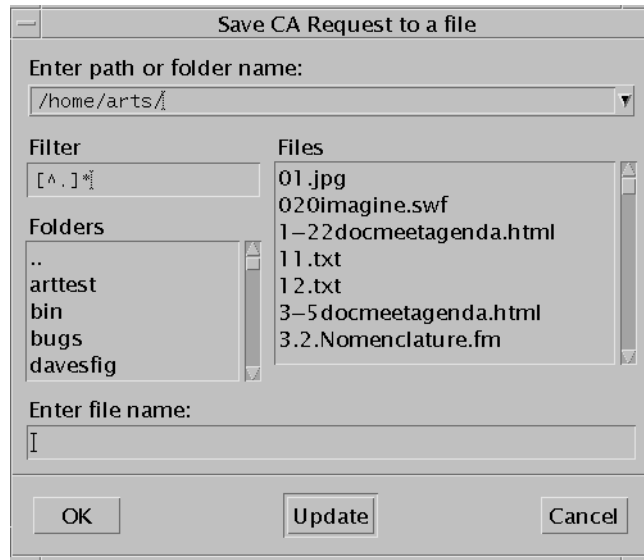
The export certificate panel appears



6. Click the Export Certificate button.
The Export Certificate panel appears

8. If you have the Java plugin loaded, you can click the Save button.

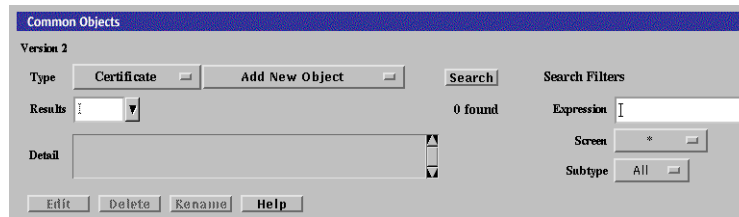
The Save CA request to a file panel appears. Type the file name for where to save the exported certificate.



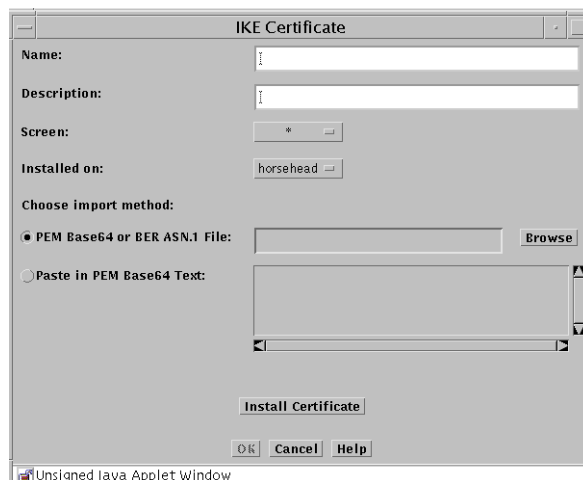
▼ To Import an IKE Certificate

When you import an IKE certificate, the process explicitly creates an object and associates that object with imported certificate. You do not need to manually do an associate for the imported IKE certificate. The procedure "To Associate an IKE Certificate" on page 74 is typically used when you have added an IKE certificate from the command line.

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Certificate from the Type list.



3. Select Import IKE Certificate from the Add New Object selection list.
4. The IKE Certificate panel appears.



5. Type a name in the Name field.
6. (Optional) Type a description in the Description field.
7. Select the Screen from the Screen list.
8. Select the machine where the certificate will be installed from the Installed on list.
9. If you have the Java plugin loaded, click the Browse button beside the PEM Base64 or BER ASN.1 File field to bring up a panel that you can use to navigate to the file that contains the certificate.
10. If you do not have the Java plugin loaded, click the radio button beside the Paste in PEM Base64 Text: which enables the area where you can paste in the certificate information that you have copied from another file.

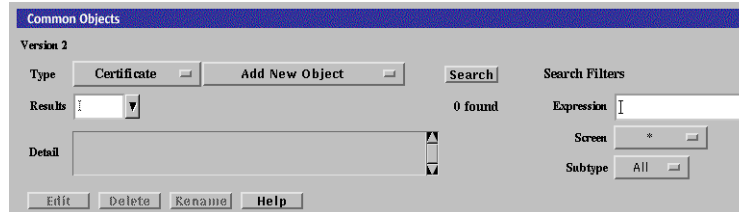
11. Click the **Install Certificate** button to import and install the certificate.
12. Go to **“To Work with IKE Certificate Groups”** on page 85 to add the IKE certificate to either an IKE root CA certificate group or to an IKE manually verified certificate group.

▼ To Associate an IKE Certificate

This procedure is typically used when you have added an IKE certificate using the command line interface.

1. Execute the steps in **“To Modify the Policies Associated with a Common Object”** on page 37.

2. Select Certificate from the Type list.



3. Select Associate IKE Certificate from the Add New Object selection list.

The associate IKE certificate panel opens.



4. Type a name in the Name field.

5. (Optional) Type a description in the Description field.

6. Select the Screen from the Screen list.

7. Select the machine where the IKE certificate will be installed from the Installed on list.

8. Type an X.509 distinguished name for the certificate subject in the Distinguished Name field. The distinguished name typically has the form of C=Country, O=Organization, OU=Organizational_Unit, and CN=Common_Name.

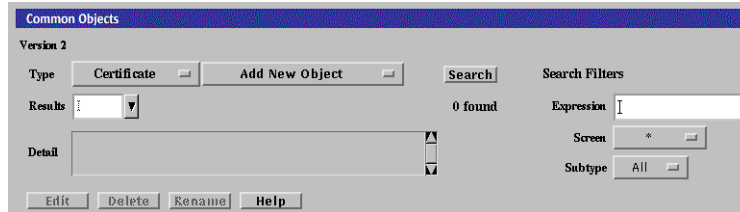
9. Go to "To Work with IKE Certificate Groups" on page 85 to add the IKE certificate to either an IKE root CA certificate group or to an IKE manually verified certificate group.

▼ To Generate SKIP UDHs Certificates

Note – Use the Installed On field in the Certificate dialog box to choose the Screen where you want to add the certificate to the SKIP database. The default choice is the Screen to which users are connected. This is the choice you should use if you are using centralized management groups.

Self-generated private keys use the SKIP NSID 8, signifying that the public value for that key has not been signed. To validate the public value, the hash of the public value associated with that private key is used as the certificate ID. When the certificate is added either manually or through Certificate Discovery Protocol (CDP), you can certify the public value by comparing the hash of the public value in the certificate to the certificate ID. Unsigned Diffie-Hellman certificates are described in the *SunScreen 3.2 Administrator's Overview*.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Certificate in the Type list.



3. Select Generate SKIP UDH in the Add New Object list.
The Certificate dialog box is displayed.



The following table describes the controls for the Certificate dialog box for generate Screen certificate.

TABLE 2-10 Controls for the Certificate Dialog Box for Generate Screen Certificate

Control	Description
Name	Specifies a name for the certificate.
Description	(Optional) Provides a brief description about the certificate object.
Screen	Specifies the Screen that recognizes the certificate object. The default is All.
Installed On	(Optional) Specifies the Screen on which the certificate is generated.
Radio buttons	Specifies the strength of encryption that the Screen uses.
Generate New Certificate	Generates the certificate. The Certificate ID field displays the certificate's certificate ID.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

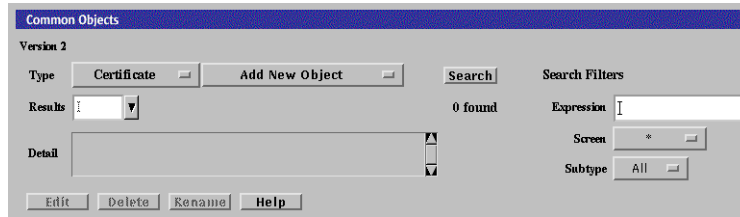
4. Type a name in the Name field.
5. (Optional) Type a description in the Description field.
6. (Optional) Select the Screen from the Screen list.
7. (Optional) Select the name of the Screen on which the Certificate is installed in the Installed On field.
8. Specify the level of encryption the Screen uses.
Available levels are:
 - Highest available
 - U.S. and Canada (4096)
 - U.S. and Canada (3072)
 - U.S. and Canada (2048)
 - Global (1024)
 - Global (512)
9. Click the Generate New Certificate button.
The Certificate ID field displays the Certificate ID.
10. Click the OK button.

▼ To Load a SKIP Issued Public or Private Certificate

Note – Because Netscape Navigator and Internet Explorer do not support the Java mechanism for applet signing, the administration GUI cannot access your system's local resources. (Browser security mechanisms prevent this type of access to local system resources.) See "Accessing Local System Resources" on page 23.

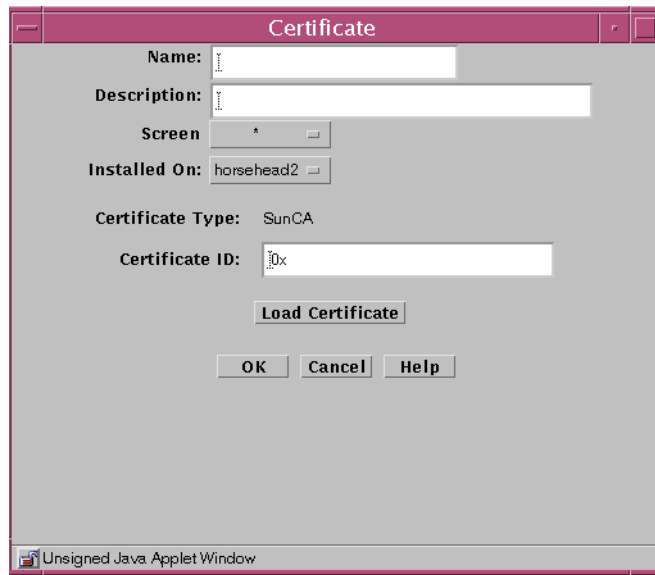
You can add new key pairs and local identities by using a SunScreen Key and Certificate diskette. This type of key and certificate is known as an *issued certificate*. Certificates are described in "Certificate Object" in *SunScreen 3.2 Administrator's Overview*. You also can add new private keys from a directory that contains only one set of private key and certificate files.

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Certificate in the Type list.



3. Select Load SKIP Issued Private key or Load SKIP Issued Public key from the Add New Object list.

The Certificate dialog box appears.



The following table describes the controls for the Certificate dialog box for generate Screen certificate.

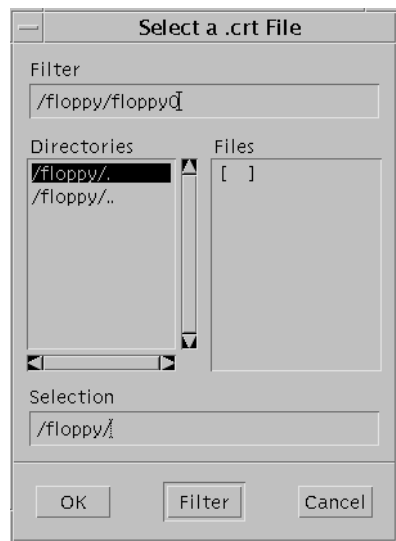
TABLE 2–11 Controls for the Certificate Dialog Box for Generate Screen Certificate

Control	Description
Name	Specifies a name for the certificate.
Description	(Optional) Provides a brief description about the certificate object.
Screen	Specifies the Screen that recognizes the certificate object. The default is All.

TABLE 2-11 Controls for the Certificate Dialog Box for Generate Screen Certificate
(Continued)

Control	Description
Installed On	(Optional) Specifies the Screen on which the certificate is generated.
Load Certificate	Brings up a selection panel where you can identify the location of the file that contains the certificate.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type a name in the Name field.
5. (Optional) Type a description in the Description field.
6. (Optional) Select the Screen from the Screen list.
7. (Optional) Select the Screen the certificate is installed on from the Installed On list.
8. Click the Load Certificate button.
9. In the File dialog box:



- a. Select the directory of the floppy that contains the certificate files.

b. Select a file with a .crt extension from the Files list.

c. Click the OK button.

The Certificate ID field contains the value.

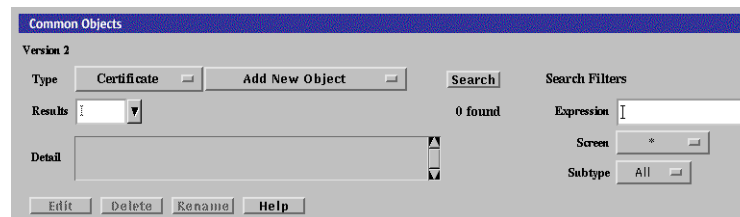
10. Click the OK button.

▼ To Associate SKIP Certificate

By associating a certificate, you can assign a name to a certificate that exists on another Screen. Associate a certificate ID when you want to encrypt communication between two Screens or between a Screen and an Administration Station.

Note – Self-generated certificates are validated by a telephone call between two people who know each other and recognize each other’s voice.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Certificate in the Type list.



3. Select Associate SKIP Certificate from the Add New Object list.
The Certificate dialog box appears.



The following table describes the controls for the Certificate dialog box for associate SKIP certificate.

TABLE 2-12 Controls for Associate SKIP Certificate Dialog Box

Control	Description
Name	Specifies the name for the certificate ID object.
Description	(Optional) Provides a brief description about the MKID or certificate ID object.
Screen	Specifies which Screen recognizes the certificate ID object. The default is All. Specifying a Screen allows you to define packet-filtering rules that encrypt traffic between any two machines, not just between an Administration Station and a Screen. Specify the Screen only if you are using Centralized Management. A common object or policy rule applies to all Screens unless you choose a specific Screen.
Installed On	(Optional) Used only if you later remove this certificate object from the common objects. At that time, the SKIP identity that is installed on the Screen will be removed from the parameter.
Certificate ID	Specifies the certificate ID (hash value) for the certificate that you generated on the other system.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type a name in the Name field.
5. (Optional) Type a description in the Description field.
6. (Optional) Select the Screen from the Screen list.
7. Select the Screen the certificate is installed on from the Installed On list.
8. Select the type of certificate from the Certificate Type list.
9. Type the Certificate ID (MKID) for the certificate.
10. Click the OK button.

Certificate Groups

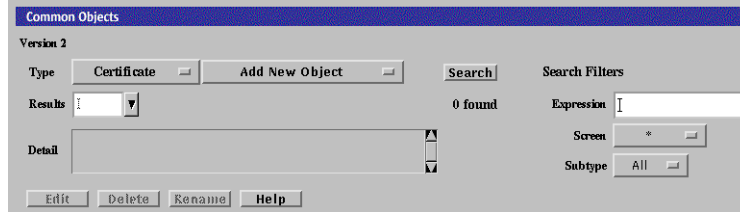
▼ To Add a Certificate Group

After you have named certificate, you can group them into logical groups, so that you can use a group instead of single names in a policy rule..

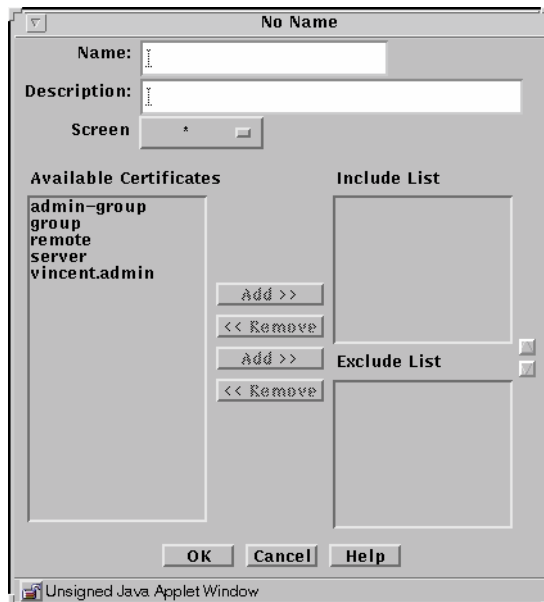
There are two special predefined IKE certificate groups. See “To Work with IKE Certificate Groups” on page 85 for the steps you need to follow to set up IKE certificate groups.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Certificate in the Type list.



3. Select New Group from the Add New Object list.
The Certificate dialog box appears.



The following table describes the controls in the Certificate dialog box for certificate group.

TABLE 2-13 Controls for Certificate Group Dialog Box

Control	Description
<i>Name</i>	Specifies the name of the certificate object.
<i>Description</i>	(Optional) Provides a brief description about the certificate object.

TABLE 2-13 Controls for Certificate Group Dialog Box (Continued)

Control	Description
Screen	Specifies which Screen recognizes the certificate object.
Available Certificate List	Identifies the certificates that do not belong to the certificate group. Refer to "Services and State Engines" in <i>SunScreen 3.2 Administrator's Overview</i> for a description of services.
Include List	Identifies the certificates that are to be included in the certificate group.
Exclude List	Identifies certificates that are to be excluded from the certificate group.
Add Button	Moves the certificate selected in the Available Certificates List to the Include or Exclude list, making the certificate a member of the specified service group.
Remove Button	Moves the certificate selected in the Group Members list to the Include or Exclude list, removing the certificate from the specified certificate group.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

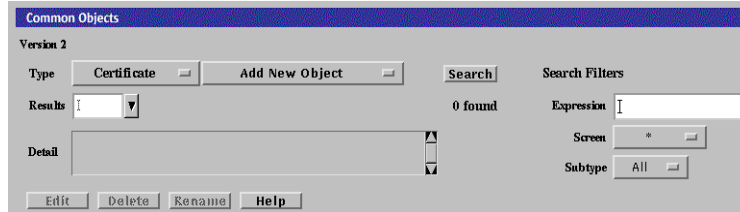
4. **Type a name in the Name field.**
5. **(Optional) Type a description in the Description field.**
6. **(Optional) Select a Screen from the Screen list.**
7. **Select an certificate from the Available Certificates list.**
8. **Use the Add button to move the certificate to the Include list or the Exclude list.**
Use the corresponding Remove button to remove certificates from the lists.
9. **(Optional) Continue to build the intended certificate group by adding to the Include lists.**
10. **Click the OK button.**

▼ To Work with IKE Certificate Groups

There are two special predefined IKE certificate groups:

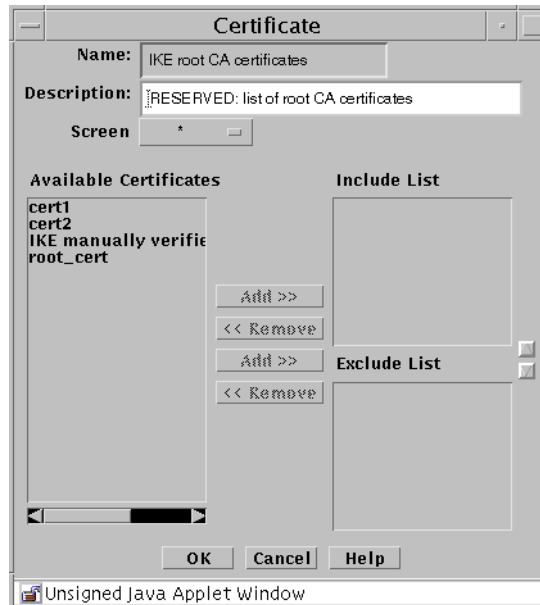
IKE manually verified certificates that hold trusted certificates used by IKE
IKE root CA certificates that hold root CA certificates used by IKE

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Certificate in the Type list.



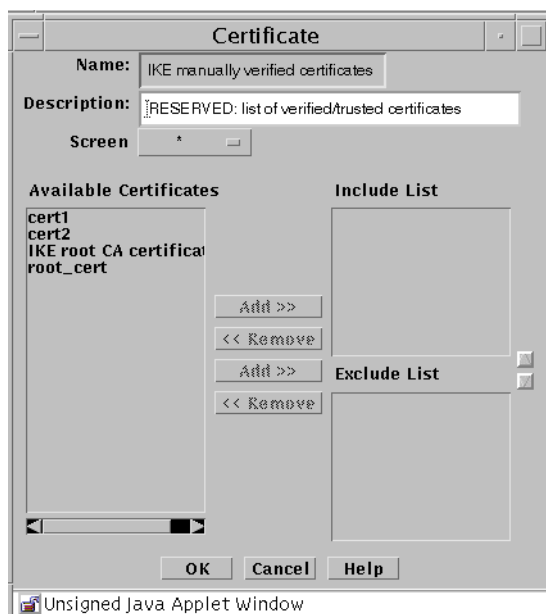
3. Click the Search button.
4. Select either the IKE root CA certificate or the IKE manually verified certificate from the results field.
5. Click the Edit button.

6. (For IKE root CA certificate) The IKE root CA certificate panel appears.



7. (For IKE root CA certificate) Select the IKE root CA certificate from the Available Certificates and click the ADD button to add it to the Include List

8. (For IKE manually verified certificate) The IKE manually verified certificate panel appears.



9. (For IKE manually verified certificate) Individually select the certificates that have been manually verified and click the Add button for each to add them to the Include List

IPsec Key

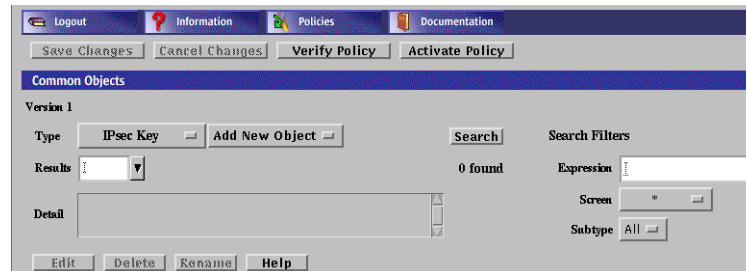
The IPsec Key (also referenced as manual keying) dialog allows you to generate an IPsec key by either manually typing the key value or to use a random number generator to generate the key. The key that is generated by the random number generator is determined by the algorithm used.

Note – IPsec Key cannot be used for remote administration or VPN.

▼ To Add an IPsec Key

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select IPsec Key from the Type list.



3. Select NEW from the Add New Object list.

The IPsec Key dialog appears.



4. Type the name for the IPsec key in the Name field.

5. (Optional) Type a brief description for the IPsec key.

6. Select which Screen recognizes the IPsec key. The default is all.

Note – Typing a Screen name allows you to define packet filter rules that encrypt traffic between any two machines, not just between an Administration Station and a Screen.

7. Select the Key size. The Hex string values you can select are:

DES-CBC 16

3DES-CBC 48

MD5 32
SHA1 40

8. **Manually type a key value to be used for the IPsec key. You should use the above hex values for proper security. If you type additional hex characters, they are discarded and the maximum value listed above is used.**
9. **Alternatively, click the Generate New Key to use the random generator to create the IPsec key.**
10. **Click the OK button**

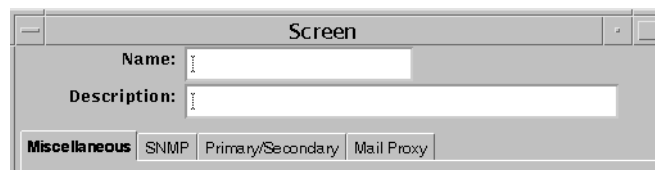
Screen Objects

If you are configuring high availability (HA) or centralized management groups (CMG), you need to add a Screen. For the standalone configuration, you may edit the Screen for adding SNMP or modifying miscellaneous properties.

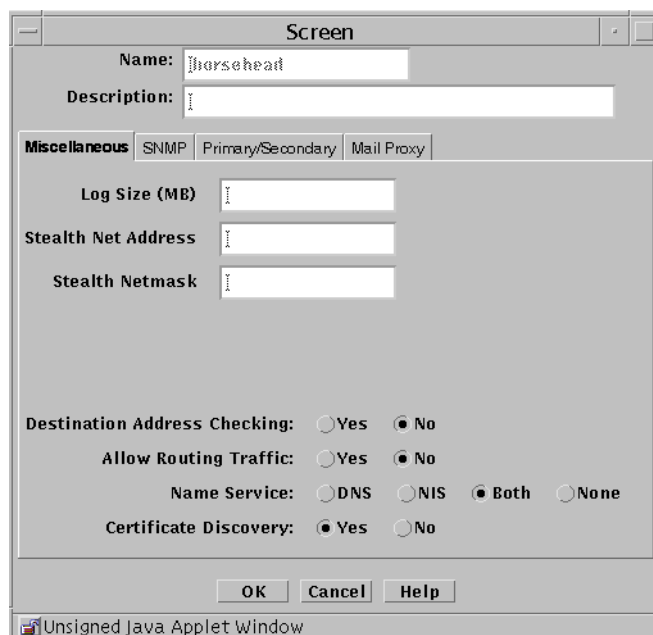
If you are running in stealth mode or mixed mode (a mix of routing and stealth interfaces), you must modify the Screen object in order to define the stealth network and netmask for the network the Screen is subdividing.

Screen Object Tabs

Most of the work with Screen Objects is done using the 4 tabs on the Screen dialog box.



Miscellaneous Tab



The following table describes the controls for the Miscellaneous tab of the Screen dialog box.

TABLE 2-14 Controls for the Miscellaneous Tab of the Screen Dialog Box

Control	Description
Name	Specifies a name for the screen object.
Description	(Optional) Provides a brief description of the screen object.
Log Size	Sets the size of the log in megabytes.
Stealth Network Address	Specifies the network address for interfaces that are used as stealth interfaces. Set this parameter if you have used the interface object to designate any Screen interfaces as stealth interfaces.
Stealth Netmask	Specifies the netmask for interfaces that are used as stealth interfaces. Set this parameter if you have used the interface object to designate any Screen interfaces as stealth interfaces.
Allow Routing Traffic	Specifies whether the Screen sends or receives updates to the routing table using the RIP protocol.
Name Service	Specifies the name service (DNS, NIS, Both, or None) that the Screen will use.

TABLE 2-14 Controls for the Miscellaneous Tab of the Screen Dialog Box *(Continued)*

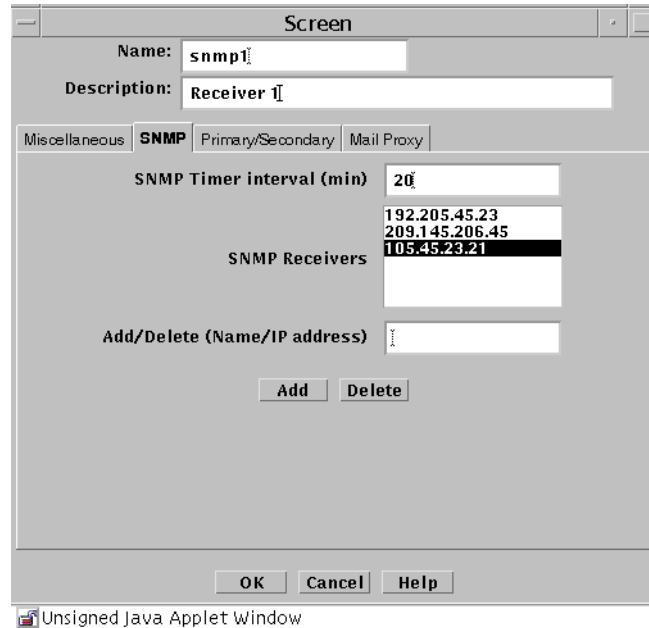
Control	Description
Certificate Discovery	Specifies whether the Screen uses Certificate Discovery.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

SNMP Tab

The SNMP tab specifies the interval for SNMP timed status indicator traps and you can add, edit, or delete SNMP trap receivers.

Note – Use the Action field of the packet-filtering Rule Definition dialog box to specify actions that generate SNMP alerts. The machine that receives SNMP trap alerts must not be a remote Administration Station.

The following shows the SNMP tab of the Screen dialog box.



The following table describes the controls for the SNMP tab on the Screen dialog box.

TABLE 2-15 Controls for the SNMP Tab of the Screen Dialog Box

Control	Description
Name	Specifies a name for the Screen object.
Description	(Optional) Provides a brief description of the Screen object.
SNMP timer interval (in minutes)	Specifies in minutes when an SNMP trap is emitted. Specifying a time here turns on the timed status indicator. Specify the time in 1-minute increments. If you do not set the interval as part of the screen object's <code>SNMP_TIMER</code> , these traps are not sent. You cannot configure this trap.
SNMP Receivers	Displays the list of SNMP receivers. You are limited to five receivers.

TABLE 2-15 Controls for the SNMP Tab of the Screen Dialog Box *(Continued)*

Control	Description
Add/Delete (Name/IP address)	<ol style="list-style-type: none"> 1. Specifies the name or the IP address of the SNMP receiver that you want to add to list when you click the Add button. 2. Specifies the name or the IP address of the SNMP receiver that you want to delete when you click the Delete button.
Add	Adds the SNMP receiver specified in the Add/Delete (Name/IP address) field to the list of SNMP receivers shown in the SNMP Receivers field.
Delete	<ol style="list-style-type: none"> 1. Deletes the SNMP receiver specified in the Add/Delete (Name/IP address) field from the list of SNMP receivers shown in the SNMP Receivers field. 2. Deletes the SNMP receiver highlighted in the SNMP Receivers field.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information
Help Button	Calls up the page of online help for this common object.

The following SNMP traps are supported:

- As an action on a packet that matches a particular rule
- As a default drop action on an interface
- Time status indicator traps

The first two types include the following data:

- `interface` – The SunScreen network interface number on which the packet was received.
- `interfaceName` – The SunScreen network interface name on which the packet was received.
- `errorReason` – The reason the alert was generated. (See the `sunscreen.mib` file for a complete list of reasons.)
- `packetLength` – The actual length of the packet in bytes.
- `lengthLogged` – The length of the data logged in bytes.
- `packetData` – The packet data.

The SNMP timed status indicator trap uses the same receivers database as other types of SNMP traps. There is only one database with a maximum of five receivers. These receivers are specified as variable to the screen object.

To activate the timed status indicator traps, set the SNMP timer interval.

The following data are in the SNMP timed status indicator. These data cannot be modified and new data cannot be added:

- `cpuUsage` – Average percentile CPU usage
- `memoryAvail` – Current swap space available, in kilobytes
- `swapIn` – Current swap ins
- `swapOut` – Current swap outs
- `scanRate` – Current scan rate
- `tcpUsage` – Current number TCP connections in the SunScreen state table
- `ipUsage` – Current number IP connections in the SunScreen state table
- `udpUsage` – Current number UDP connections in the SunScreen state table
- `rootUsage` – Disk usage of the `root` partition, /
- `varUsage` – Disk usage of the `var` partition, /var
- `etcUsage` – Disk usage of the `etc` partition, /etc
- `tmpUsage` – Disk usage at the `tmp` partition, /tmp

Only these SNMP traps are supported. No `get` or `set` operations are supported.

Primary/Secondary Tab

The Primary/Secondary tab associates a certificate object with a Screen that is part of an HA cluster or a CMG. The High Availability choice (No, Primary, or Secondary) and the Primary Name choice determine the role a Screen has within an HA cluster and centralized management group (CMG). The settings you choose determine which other controls on the Primary/Secondary tab are active.



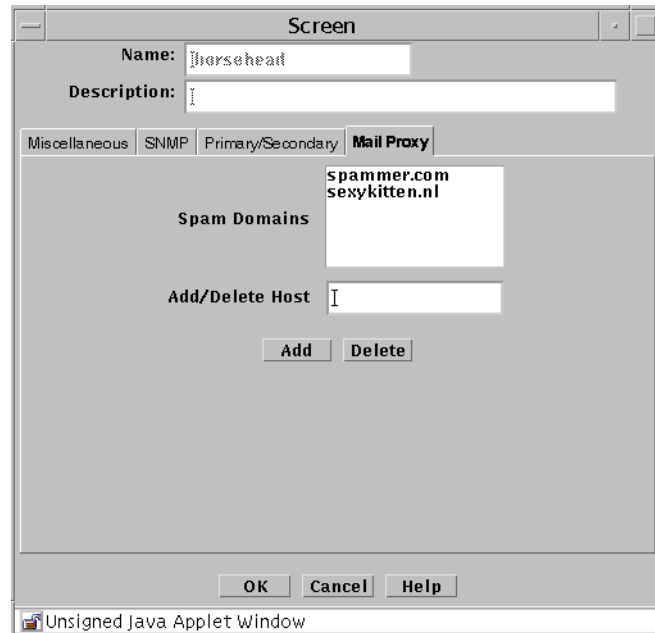
The following table describes the controls for the Primary/Secondary tab.

TABLE 2-16 Controls for the Primary/Secondary Tab of the Screen Dialog Box

Control	Description
Name	<p>Specifies a name for the Screen object.</p> <ol style="list-style-type: none"> 1. The entry in the Name field must be the same as the entry that exists in the <code>nameservice</code> lookup or in the <code>/etc/hosts</code> file. The IP address associated with this name must match the IP address of the administrative interface. 2. The type of interfaces must be the same on all the machines in the HA cluster. This interface must be dedicated on each machine in the HA cluster with a dedicated network connection. For reasons of security, the HA network should not be connected to any other network. The HA primary Screen is always the Screen you administer whether it is the active or passive Screen.
Description	(Optional) Provides a brief description of the Screen object.
High Availability	Specifies whether the Screen is used for HA. If you are using it for HA, you can specify whether the Screen is a primary HA Screen or a secondary HA Screen.
Primary Name	Specifies the name of the primary Screen. This is the primary of this Screen if this Screen is an HA secondary, or the primary of a centralized management group if you want this Screen to be a CMG secondary.
Administrative IP	IP address of the Screen that is used for administration. This is the IP address or an address group that contains all interface addresses of the Screen.
Administration Certificate	Specifies the name of the Screen's Administration certificate (SKIP/IKE).
High Availability IP Address	Specifies the IP address of the HA interface.
Ethernet Address	Generated by the system.
SKIP Parameters	■ Specifies SKIP Key, Data, and MAC algorithms.
IKE Parameters	■ Specifies IPSEC, AH, and ESP algorithms along with IKE options and algorithms.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

Mail Proxy Tab

The Mail Proxy tab allows adding, editing, or deleting domains known to distribute unsolicited electronic mail (spam). You can define spam domains if you use an SMTP proxy.



The following table describes the controls for the Mail Proxy tab of the Screen dialog box.

TABLE 2-17 Controls for the Mail Proxy Tab of the Screen Dialog Box

Control	Description
Name	Specifies a name for the Screen object.
Description	(Optional) Provides a brief description of the Screen object.
Spam Domains	Lists the domains that are distributing unsolicited electronic mail.
Add/Delete Host	<ol style="list-style-type: none">1. Specify the domain that you want to add to the Spam Domains list when you click the Add button.2. Specify the domain that you want to delete from the Spam Domains list when you click the Delete button.

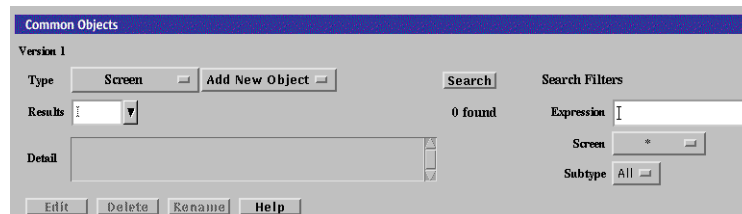
TABLE 2-17 Controls for the Mail Proxy Tab of the Screen Dialog Box (Continued)

Control	Description
Add	Adds the domain specified in the Add/Delete Host field to the list of spam domains shown in the Spam Domains field.
Delete	1. Deletes the domain specified in the Add/Delete Host field from the list of domains shown in the Spam Domains field. 2. Deletes the domain highlighted in the Spam Domains field.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

Adding a Screen Object

▼ To Add a Screen

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Screen in the Type list.



3. Select New from the Add New Object list.
The Miscellaneous area in the Screen dialog box appears.
4. In the Name field, type the name of the Screen as it appears in the naming service or the host file.
5. Type a number in the Log Size (MB) field, to set the total size for log files (the default is 100 Mbytes).

6. The **Stealth Network Address** and **Stealth Netmask** (of the network the Screen partitions) fields apply only if the Screen has stealth interfaces.
7. Click the **Yes** or **No** radio button to allow or deny **Destination Address Checking**. **Destination Address Checking** is used for anti-spoofing protection.
8. Click the **Yes** or **No** radio button to allow or deny routing traffic (**RIP**).
9. Click a **Name Service** radio button to choose the name service that the Screen will rely on to define the host address.
You can also use both DNS and NIS or no name service at all.
10. Click the **Yes** or **No** radio button for **Certificate Discovery (SKIP only)**.
This determines whether the Screen itself is to participate in a certificate discovery exchange. Selecting **Yes**, however, does *not* allow CDP traffic to go *through* the Screen.
11. Click the **OK** button.

SNMP Alert Receivers

You set actions that generate SNMP alerts as part of a security policy. Use the **SNMP** tab in the Screen dialog box to:

- Add an SNMP trap receiver
- Delete an SNMP trap receiver
- Set the timer for the timed status indicator

A management information base (MIB) that describes the SNMP trap is included with the SunScreen CD-ROM, as part of the `SUNWSfwau` package. It is installed as: `/usr/lib/sunscreen/Admin/etc/sunscreen.mib`. Load this MIB into your SNMP manager to enable it to use the SNMP trap generated by the Screen.



Caution – The machine that you want to receive SNMP trap alerts must not be a remote Administration Station. SNMP alert packets are sent *in the clear*, and the communication between the remote Administration Station and Screen is encrypted; any packets sent in the clear are dropped.

The recipients of SNMP messages are controlled on a Screen-by-Screen basis. The Screen object has a place for an optional list of IP addresses, which are the hosts to which it sends the SNMP packets.

There are two ways to send SNMP packets:

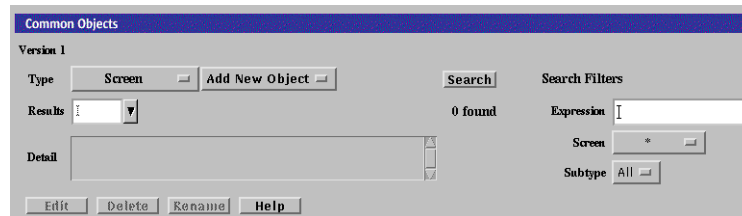
- Set SNMP in a Packet Filtering rule's Action
- Specify it in the default Reject Action of an interface object

SNMP alerts are described in “Screen Object” in *SunScreen 3.2 Administrator’s Overview*.

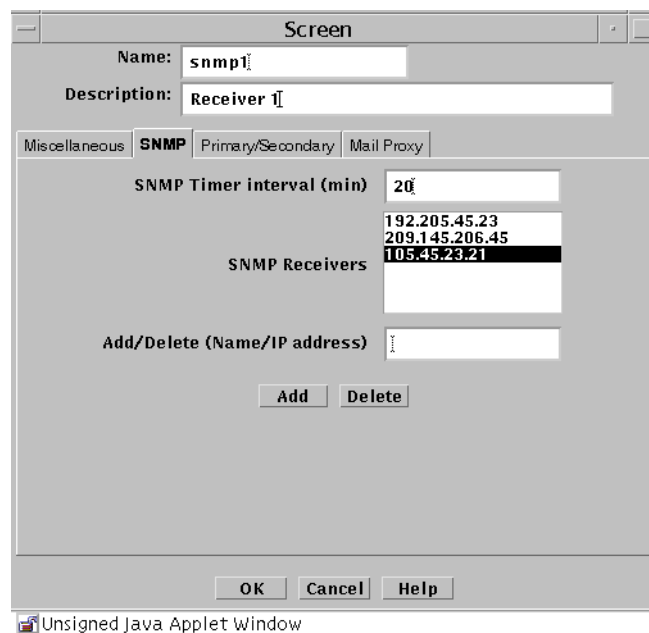
The following information describes using the administration GUI. For the command line interface, see Chapter 10.

▼ To Add an SNMP Alert Receiver

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Screen in the Type list.



3. Select New from the Add New Object list.
4. Click the SNMP tab in the Screen dialog box.
The SNMP area is displayed.



5. Type the name or IP address of the recipient of the SNMP trap in the Name field.
6. Click the Add button.
A list of SNMP alert receivers appears. You can define up to five receivers. SunScreen sends each generated alert to all receivers.
7. Click the OK button when you are finished.

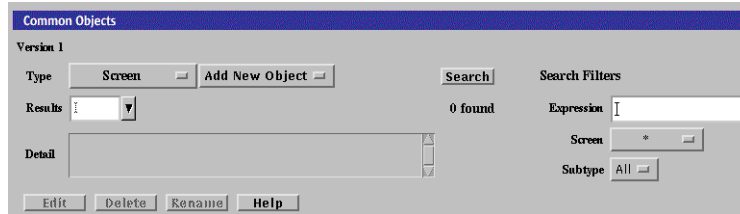
Note – You use the SNMP Timer Interval field in the SNMP tab to specify the time interval, in minutes, between the health-update packets that are emitted by the Screen. If you do not specify any Alert receivers, no health-update packets are issued.

If you set the SNMP Timer Interval field to zero (or leave it empty) and there are Alert receivers, no health-update packets are issued, although other SNMP alerts are sent to the Alert receivers.

▼ To Delete an SNMP Alert Receiver

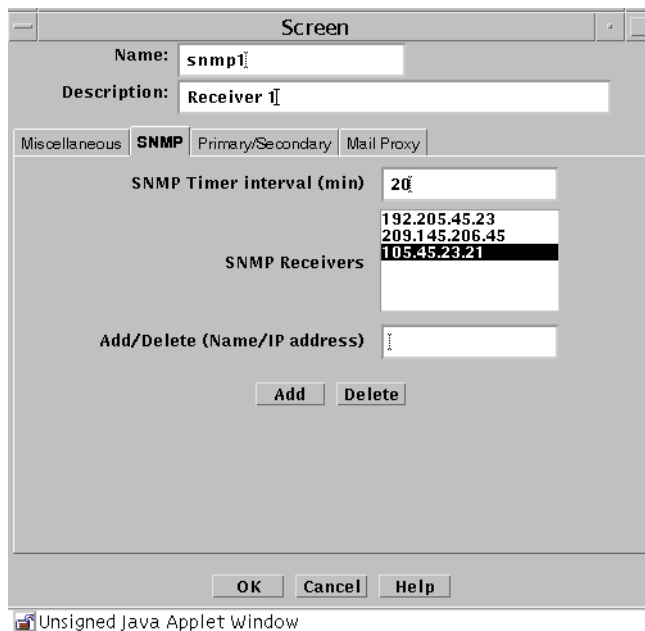
1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.

2. Select Screen in the Type list.



3. Select New from the Add New Object list.

4. Click the SNMP tab in the Screen dialog box for the Screen.
The SNMP area appears.



5. Select an entry in the SNMP Receivers field.

If the name of the SNMP Receiver to delete is not listed (that is, only the IP address is listed), type the name in the Add/Delete field.

6. Click the Delete button.

7. Click the OK button when you are finished with this Screen object.

Interface Objects

An Interface Object represents a network interface that makes one or more IP addresses accessible to a Screen. Empty address groups for all available network interfaces are defined during installation in *routing mode*. After you complete the installation, you can add and remove interfaces, redefine the addressees for the network interfaces, and set up high availability. For an interface to be able to reach a desired set of addresses, you must define one or more address groups and specify which address group each interface will use.

Note – If the user wants to use spoof detection, they will need to associate accurate address groups with each interface.

For Routing interfaces, there are two types of spoof detection : Complete and Incomplete. On the Interface Definition panel (see “To Add or Edit Interfaces” on page 105), you can set the spoof detection by clicking on the “Spoof Protection” pulldown and making the selection (see “Interface Object” in *SunScreen 3.2 Administrator’s Overview* for information on Complete and Incomplete spoof detection).

For Stealth interfaces, the type of spoof detection is always set to Complete and is not modifiable.

The maximum number of stealth interfaces per Screen is 15; however, the number of routing interfaces is virtually limitless.

The following table describes the controls for the Interface Definition dialog box.

TABLE 2-18 Controls for the Interface Definition Dialog Box

Control	Description
Interface	Specifies the interface.
Type	Specifies the type of interface. The options are: <ul style="list-style-type: none">■ ROUTING■ ADMIN■ DISABLED■ HA■ STEALTH
Screen	Specifies the Screen on which this interface physically resides. If you are using centralized management, you must complete this field.
Valid Address	Specifies the source IP addresses for this interface.

TABLE 2-18 Controls for the Interface Definition Dialog Box (Continued)

Control	Description
Spool Protection	Specified the level of spoof protection. For Routing interfaces, there are two types of spoof detection : Complete and Incomplete (see "Interface Object" in <i>SunScreen 3.2 Administrator's Overview</i> for information on Complete and Incomplete spoof detection).
Logging	Identifies the disposition of a packet, when a packet received on the interface does not match any rule. The options are: <ul style="list-style-type: none">■ NONE – Do not log packets.■ SUMMARY – Record the first 40 bytes of the packet in the log.■ DETAIL – Record the complete packet in the log. If a packet matches a rule, it is disposed of according to the action for the rule it matches.
SNMP Alerts	Specifies whether the Screen should issue an SNMP alert message when a packet received on an interface does not match a rule. The options are: <ul style="list-style-type: none">■ SNMP_NONE – Do not send an SNMP alert message. (This is the default.)■ SNMP – Send an SNMP alert message when a packet received on this interface is rejected. If a packet matches a rule, it is disposed of according to the action for the rule it matches.
ICMP Action	Identifies the ICMP rejection message that is issued if a packet received on the interface is rejected. In most cases, the Screen rejects packets by sending an ICMP Destination Unreachable packet with the reject code set as specified in the ICMP action on the interface. The one exception is the PORT_UNREACHABLE ICMP action. In this case, the Screen rejects TCP packets by sending a TCP RESET packet and other packets by sending an ICMP Destination Unreachable (Port Unreachable) message. The options for the actions are: <ul style="list-style-type: none">■ NONE■ NET_UNREACHABLE■ HOST_UNREACHABLE■ PORT_UNREACHABLE■ NET_FORBIDDEN■ HOST_FORBBIDEN. If a packet matches a rule, it is disposed of according to the action for the rule it matches.
Comment	(Optional) Provides a descriptive note about the Interface object.

TABLE 2-18 Controls for the Interface Definition Dialog Box (Continued)

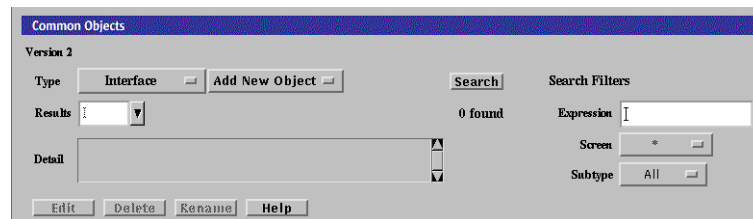
Control	Description
Router IP Address	(Optional) Specifies the router's IP address when the type of interface is STEALTH. This allows packets that have had their destination address changed, for example NAT or tunnelling, to be sent to a router. You can specify as many as five router IP addresses. If you have stealth interfaces, define the router that does the routing for the subnet for at least one of them.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

▼ To Add or Edit Interfaces

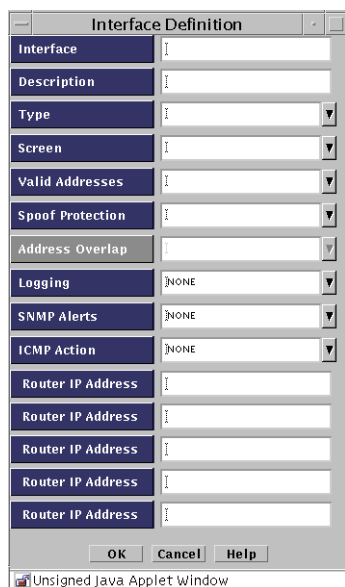
Before adding a new interface, you must define the address group that the interface will use in the policy.

Note – Any added interfaces, or edits to interfaces, take effect only when you activate the policy rule that includes those interfaces.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Interface in the Type list.



3. Select New from the Add New Object list beside the Interfaces area. The Interface Definition dialog box appears.



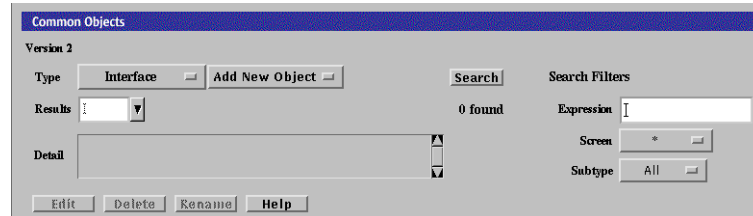
4. Type the name of the interface, such as hme0 or qfe1.

Note – Virtual interfaces are not configured in SunScreen. On the physical interface (qe1) needs to be defined, and all associated virtual (logical) interfaces will be protected.

5. Select the type of interface you want to add, such as ROUTING, ADMIN, DISABLED, HA, or STEALTH, from the Type list.
6. (Optional) Select the name of the Screen you want to add from the Screen list.
7. Select the name of the valid addresses you want to add from the Valid Addresses list.
8. (Optional) Select the type of logging you want to use from the Logging list.
9. (Optional) Select which SNMP alert to use, if any, from the SNMP Alert list.
10. (Optional) Select the name of the Reject Action you want to use from the ICMP Action list.
11. Click the OK button to save your interface definition.
12. (Optional) Repeat the steps above until you have added all the interfaces you require.

▼ To Remove an Interface

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Interface in the Type list.



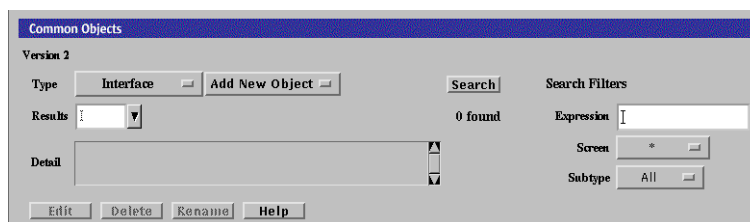
3. Select the name of the interface you want to delete from the Type list.
The Detail text area displays information about the interface.
4. Select the name of the Screen from which you want to remove the interface.
5. Click the Delete button.

Note – Any interfaces that you remove with this procedure remain active until you activate the policy rule that formerly included them. Routing interfaces must be removed from the operating system, otherwise they will be unprotected on the network.

▼ To Set up a Routing Interface

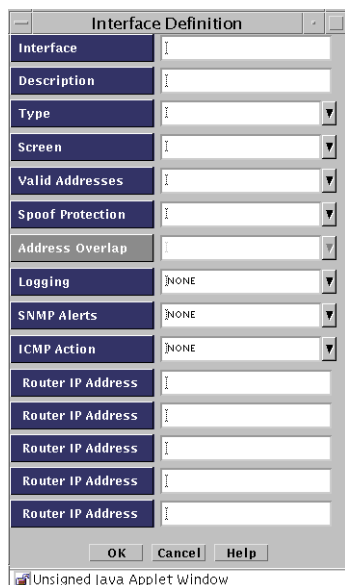
Note – *In Routing Mode only*, before you can configure a new routing interface, you must first configure it on your system. (Use the documentation for your operating system.) *Do not* try to do this for stealth interfaces.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Interface in the Type list.



3. Select New in the Add New Object list.

The Interface Definition dialog box appears.

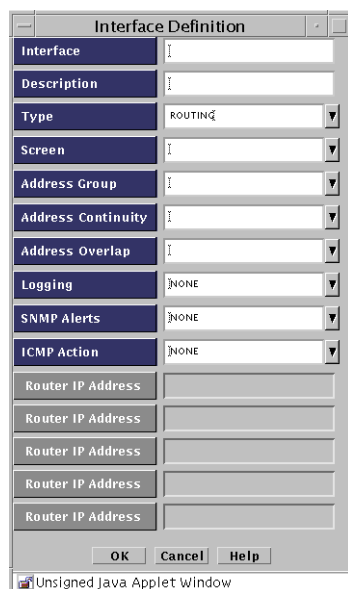


4. Type the name for the interface in the Interface field.

5. (Optional) Type a brief description for the interface.

6. Select ROUTING in the Type field list.

The Interface Definition dialog box changes and the Routing IP Address fields are disabled and the Address Overlap field is enabled.



7. Type the remainder of the information in the fields.
8. (Optional) Select the name of the Screen you want to add from the Screen list.
9. Select the name of the valid addresses you want to add from the Valid Addresses list.
10. (Optional) Select the type of logging you want to use from the Logging list.
11. (Optional) Select which SNMP alert to use, if any, from the SNMP Alert list.
12. (Optional) Select the name of the reject action you want to use from the ICMP Action list.
13. Click the OK button when finished.
14. Click Save Changes.

▼ To Set up a Stealth Interface

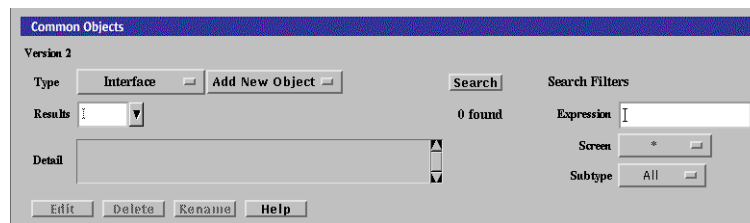
The stealth interfaces have optional **router entries**. Use these entries to define all accessible routers on your subnet that can be reached from this interface. These routers are *required* if your policy uses NAT or tunneling, and recommended otherwise.

You need to create address groups that accurately reflect all the hosts available from each stealth interface, and you must associate these address groups with stealth interfaces when you define them.

For additional information, see “Routing and Stealth Mode Interfaces” in *SunScreen 3.2 Administrator’s Overview*.

Note – Do not configure any interfaces at the operating system for use as stealth interfaces with the following exception. Configure one interface for use as an Admin Interface for Remote Administration.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Interface in the Type list.



3. Select New in the Add New Object list.
The Interface Definition dialog box appears.



4. Type the name for the interface in the **Interface** field.
5. (Optional) Type a brief description for the interface.
6. Select **STEALTH** in the **Type** field list.
The Interface Definition dialog box changes and the Address Overlap field is disabled.

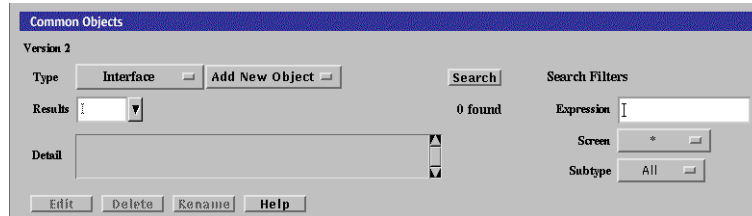


7. Select the name of the Screen you want to add from the Screen list.
8. Select the name of the valid addresses you want to add from the Valid Addresses list.
9. Select the type of logging you want to use from the Logging list.
10. Select which SNMP alert to use, if any, from the SNMP Alert list.
11. Select the name of the reject action you want to use from the ICMP Action list.
12. Type the Router IP Addresses
13. Click the OK button when finished.
14. Click Save Changes.

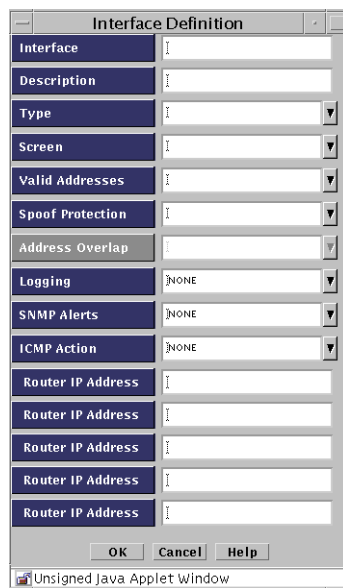
▼ To Change an Admin Interface From the Local Console

If you want to upgrade an existing admin interface or if an existing admin interface is defective, you can change the admin interface on the local console as follows:

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Interface in the Type list.



3. Select New from the Add New Object list
The Interface Definition dialog box appears.



4. Fill in the information making sure to select Admin in the Type field.
5. Click OK.
6. Select Screen from the Type List
7. Click Search to see the list of screens

8. Select the screen and click Edit.

The screen dialog box appears.

The screenshot shows a dialog box titled "Screen" with the following fields and options:

- Name:** horsehead
- Description:** (empty)
- Tabs:** Miscellaneous (selected), SNMP, Primary/Secondary, Mail Proxy
- Log Size (MB):** (empty)
- Stealth Net Address:** (empty)
- Stealth Netmask:** (empty)
- Destination Address Checking:** Yes No
- Allow Routing Traffic:** Yes No
- Name Service:** DNS NIS Both None
- Certificate Discovery:** Yes No
- Buttons:** OK, Cancel, Help

Unsigned Java Applet Window

9. Select Primary/Secondary.

The screenshot shows the same "Screen" dialog box, but with the "Primary/Secondary" tab selected. The fields and options are:

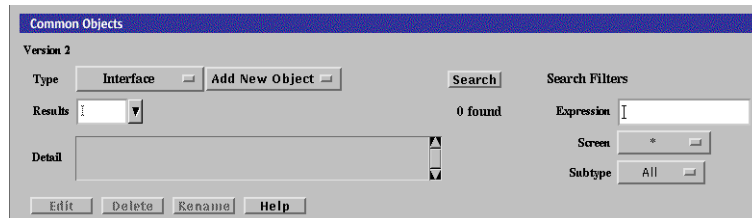
- Name:** boss
- Description:** primary screen
- Tabs:** Miscellaneous, SNMP, Primary/Secondary (selected), Mail Proxy
- High Availability:** Secondary
- HA Primary Name:** horsehead
- Administrative IP Address:** (empty)
- SKIP Administrative Certificate:** (empty)
- IKE Administrative Certificate:** (empty)
- High Availability IP Address:** 260.100.30.3
- Ethernet Address:** (empty)
- SKIP Parameters:** Edit
- IKE Parameters:** Edit
- Buttons:** OK, Cancel, Help

Unsigned Java Applet Window

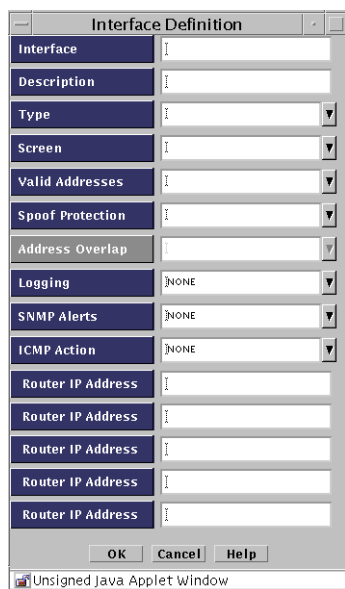
10. In the Administration IP Address field, either select "*" or the name of the address object. The address object is set by selecting Address in the Type list and then selecting New Host and filling in the IP address for the address object.
11. Save and activate the changes.
12. Thoroughly test the new admin interface.
13. Follow the steps in "To Remove an Interface" on page 107 to remove the old admin interface once you are satisfied with the new admin interface.
14. Save and activate the changes.

▼ To Change an Admin Interface From a Remote Console

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Interface in the Type list.



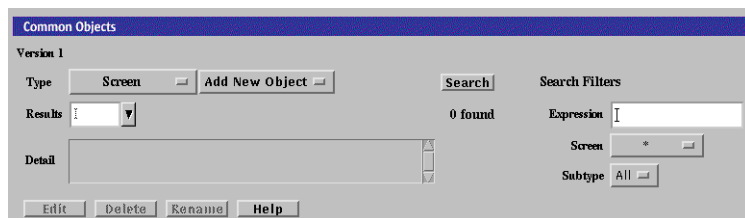
3. Select New from the Add New Object list
The Interface Definition dialog box appears.



4. Save and activate the changes.

5. Select Screen in the Type list.

The Screen panel appears.

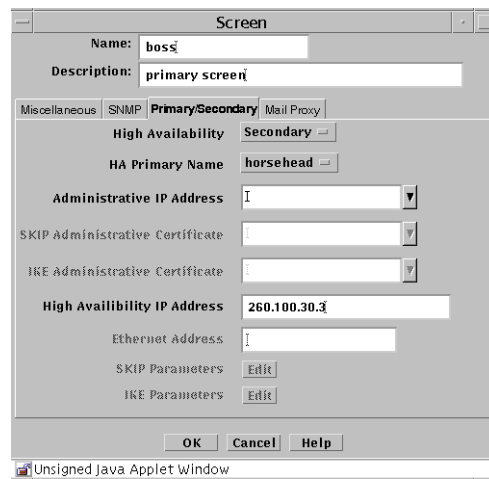


6. Click Search and then select the screen for which you are changing the admin interface

7. Click Edit

8. Select Primary/Secondary in the Screen dialog box.

The Primary/secondary panel appears.



9. Select "*" for the Administration IP Address to allow for testing.
10. Save and activate the changes.
11. Thoroughly test the new admin interface.
12. Reselect Screen from the Type list
13. Select Primary/Secondary in the Screen dialog box.
14. Fill in the fields making sure to select the address object for the new admin interface. The address object is set by selecting Address in the Type list and then selecting New Host and filling in the IP address for the address object.
15. Save and activate the changes.
16. Thoroughly test the new admin interface.
17. After you are satisfied that the new admin interface is working correctly, follow the steps in "To Remove an Interface" on page 107 to remove the old admin interface.

Adding Jar Signatures and Jar Hashes

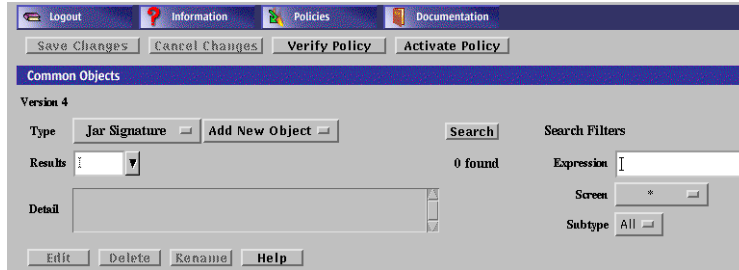
You administer the Screen through any browser that supports the Java platform and is compliant with Java Developers Kit (JDK) 1.1. Because Netscape Navigator and Internet Explorer do not support the Java mechanism for applet signing, the

administration GUI cannot access your system's local resources. (Browser security mechanisms prevent this type of access to local system resources.) See "Administration GUI Browser Requirements" on page 22 for more information.

Jar Signatures and Jar hashes are described in the *SunScreen 3.2 Administrator's Overview*.

▼ To Add a Jar Signature

1. Execute the steps in "To Modify the Policies Associated with a Common Object" on page 37.
2. Select Jar Signature from the Type list.



3. Select New from the Add New list.
The Jar Signature dialog box appears.



The following table describes the controls for the JAR signature dialog box.

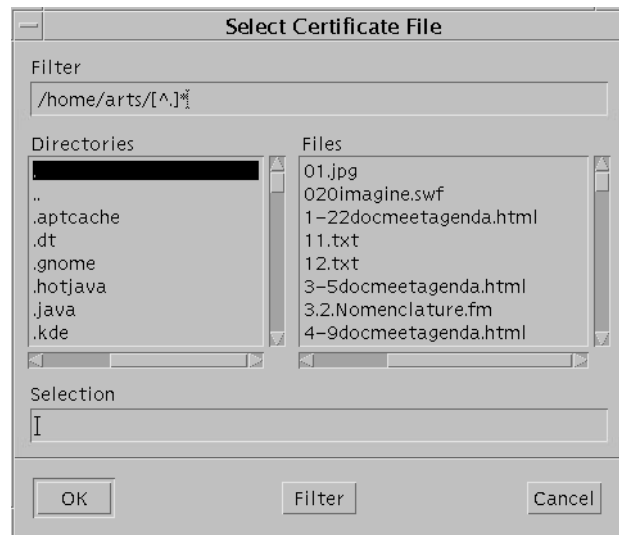
TABLE 2-19 Controls for the Jar Signature Dialog Box

Control	Description
Name	Identifies the name of the certificate.
Master Key ID	Identifies the certificate ID.
Load Jar Certificate Button	Loads the certificate used to authenticate the Java archive. This procedure requires that your browser can allow local access to files.
OK Button	Stores the new or changed information.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type a name in the Name field.

5. Click the Load Jar Certificate button.

A dialog box appears. Navigate through the paths to find the certificate used to sign the Java archive.



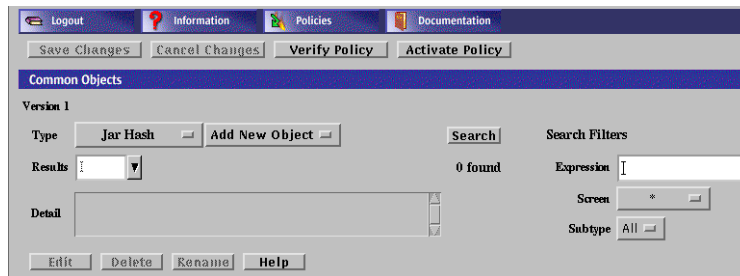
6. Select on the Certificate file.

7. Click the OK button.

▼ To Add a Jar Hash

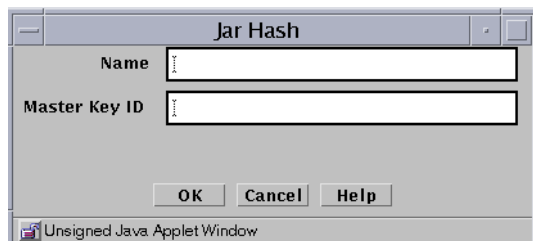
You can set up the HTTP proxy to filter Java applets based on the hash value of the Jar file. The Jar hash object is automatically saved when it is edited or when a new Jar hash object is added. Changes apply immediately and cannot be cancelled.

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Jar Hash from the Type list.



3. Select New from the Add New button.

The Jar Hash dialog box appears.



The following table describes the controls for the Jar hash dialog box.

TABLE 2–20 Controls for the Jar Hash Dialog Box

Control	Description
Name	Identifies the name of the certificate.
Master Key ID	Identifies the certificate ID.
OK Button	Stores the new or changed information.

TABLE 2-20 Controls for the Jar Hash Dialog Box (Continued)

Control	Description
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type the name for this certificate in the Name field.
5. Type the MD5 hash of the Jar archive in the Master Key ID field.
6. Click the OK button.

Proxy Users

Proxy users are discussed in Chapter 6.

Authentication

Authorized User is a Common Object that provides a way for you to specify which users are allowed to use the Telnet, HTTP, and FTP proxy.

The proxy users database depends on information in the authorized users database. To take full advantage of the user authentication feature of the FTP, HTTP, and Telnet proxies, you must create entries for both authorized users and proxy users. Define a user in the Authorized User area in the Policy Rules page before defining that user as a proxy user. See “Authentication” in *SunScreen 3.2 Administrator’s Overview* for information on the proxy database and the authorized user database.

Also see *SunScreen 3.2 Configuration Examples* for an example that uses Authorized User and Proxy User.

Note – You can define authorized and proxy user objects with identical names. Choose a naming strategy for each set that reflects naming systems already in use. For example, you might choose to name authorized users by employee identities, such as surname or employee number, and proxy users by their login names.

The proxy user database contains the mapping information for users of SunScreen proxies. FTP, HTTP, and Telnet rules reference the proxy user entries. Additionally, a user connecting through either of these proxies will often be configured to require authentication by using an authorized user identity. Users logging in with a Telnet proxy are authenticated through the authorized user identity.

You can also use external authentication mechanisms, such as RADIUS or SecurID, to enable user authentication by using *special* proxy user entries, which create a translation.

By referencing these *special* mechanisms directly in rules, or by adding references to other proxy user groups, you can allow users authenticated by those mechanisms to behave as authenticated users in the referenced contexts.

Names of proxy users must not contain the following characters: !, @, #, \$, %, ^, &, *, {, }, [,], <, >, ", \, \, or ?, nor may they contain a NULL character.

The following table describes the controls for the Authorized User dialog box for an authorized user object.

TABLE 2-21 Controls for the User Dialog Box for an Authorized User Object and an Administrative User Object

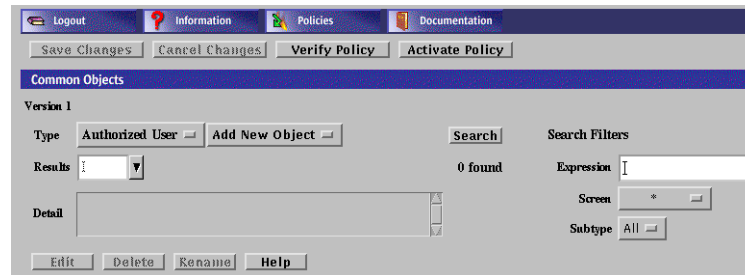
Control	Description
User Name	Specifies the login name of the authorized user.
Description	(Optional) Provides a brief description about the authorized user.
User Enabled	Controls whether the user can log into the Screen's proxy. This function permits the administrator to refuse login privileges to someone who previously could log in without having to remove that person from the list of proxy users.
Password	Specifies the login password for the authorized user.
Retype Password	Specifies the login password for the authorized user. The password typed in this field must exactly match the password you typed in the Password field.
SecurID Name	(Optional) Specifies the user's login name for SecurID authorization.
Real Name	(Optional) Identifies the real name of the authorized user.

TABLE 2-21 Controls for the User Dialog Box for an Authorized User Object and an Administrative User Object (Continued)

Control	Description
Contact Information	(Optional) Displays information on how to contact the specified user.
OK Button	Stores the new or changed information.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

▼ To Add an Authorized User

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Authorized User from the Type list.



3. Select New from the Add New button.
The User dialog box appears.

The screenshot shows a 'User' dialog box with the following fields and controls:


- User Name:** A text input field.
- Description:** A multi-line text area.
- User Enabled:** A checked checkbox.
- Password:** A text input field with '[optional]' below it. To its right is an unchecked 'Enabled:' checkbox.
- Retype Password:** A text input field.
- SecurID Name:** A text input field with '[optional]' below it. To its right is an unchecked 'Enabled:' checkbox.
- Real Name:** A text input field with '[optional]' below it.
- Contact Information:** A text input field with '[optional]' below it.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom.
- Window Title:** 'User'.
- Status Bar:** 'Unsigned Java Applet Window'.

4. Type the user name in the User Name field.
5. (Optional) Type a description in the Description field.
6. Click the User Enabled button.
7. Define the authorization method by either assigning a password or choosing a SecureID name.
 - a. (Assign Password) Type a password in the Password field.
If you do this step, you also need to retype the password to confirm it.
 - b. (SecureID name) Type a SecureID name in the SecurID field.
8. Select the Enabled check box.
9. (Optional) Type a name in the Real Name field.
10. (Optional) Type an email address in the Contact Information field.
11. Repeat these steps until you have added all the authorized users.
12. Click the OK button.
All changes apply immediately.

Time Objects

You can control the time of day when rules are in effect by defining time objects for them.

For instance, the following graphic shows use of the time object in a rule that allows all “www” service traffic during the “day” time (where “day” has been defined in the Time dialog box in “To Create Time Objects” on page 125). This rule is applicable only for the time defined, in this case the time specified in a predefined time object.



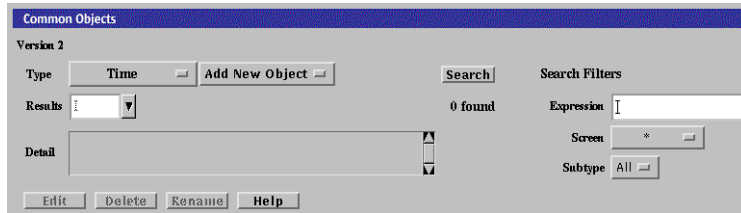
The screenshot shows a dialog box titled "Rule Definition:Initial". It contains several fields and dropdown menus:

Rule Index	2
Screen	*
Service	www
Source Address	*
Destination Address	*
Action	ALLOW
Time	day
Description	

At the bottom of the dialog box, there are buttons for "Show Action Details", "OK", and "Cancel". The window title bar indicates it is an "Unsigned Java Applet Window".

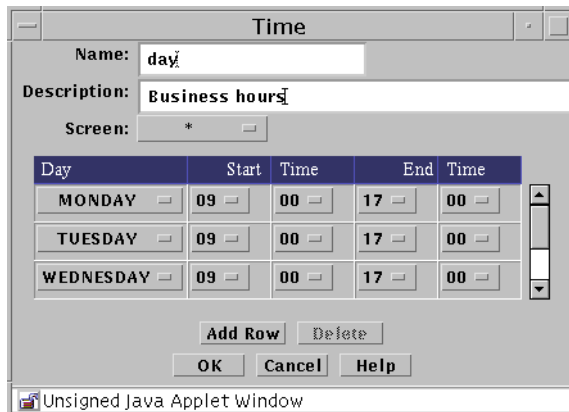
▼ To Create Time Objects

1. Execute the steps in “To Modify the Policies Associated with a Common Object” on page 37.
2. Select Time in the Type list.



3. Select New from the Add New Object list.

The Time dialog box appears.



The following table describes the controls in the Time dialog box.

TABLE 2-22 Controls for the Time Dialog Box

Control	Description
Name	Specifies a name for the time object.
Description	(Optional) Adds a descriptive note about the time object.
Screen	Specifies the Screen that recognizes the time object.

TABLE 2-22 Controls for the Time Dialog Box (Continued)

Control	Description
Table for the Time Parameters	Sets the time of day and the day of the week for this time object. Use the Add button to add a row to the table and the Delete button to remove a row to the table <ol style="list-style-type: none">1. Day column contains a choice list of the days of the week plus EVERYDAY and *.2. Start Time column contains a choice list of the hours in a day using the 24-hour clock with midnight denoted as 00.3. Time Start column contains a choice list of the minutes in an hour in 5-minute increments.4. End Time column contains a choice list of the hours in a day using the 24-hour clock with midnight denoted as 00.5. End Time column contains a choice list of the minutes in an hour in 5-minute increments.
Add Row Button	Adds a row to the table so that you can set time parameters for this time object. To cover more than one day, but less than everyday, add a row for each day and choose the day that you want for each row
Delete Button	Deletes a highlighted entry in the table.
OK Button	Stores the new or changed information and makes the Save Changes command button active.
Cancel Button	Cancels any new or changed information.
Help Button	Calls up the page of online help for this common object.

4. Type a name in the Name field.

For example: **day**

5. (Optional) Type a description in the Description field.

For example: **Business hours**

6. (Optional) Select a Screen from the Screen list.

7. Click Add Row.

8. Set the following:

- Day of the week
- Start Time (hr, min)
- End Time (hr, min)

9. Click the OK button.

Creating and Managing Rules

This chapter describes:

- Packet filtering rules
- Viewing and editing the details of an object in the packet filtering table
- Adding, editing, deleting, and reordering rules
- Administrative access rules
- Network Address Translation (NAT)
- Virtual private networks (VPN)
- Verifying a policy

The following information describes the administration GUI. Chapter 10 contains information about the command line interface.

The following table lists the procedures in this chapter.

TABLE 3-1 Procedures for Managing Rules

Rule	Procedure
Packet Filter Rules	"To View and Edit the Details of an Object" on page 133
	"To Edit a Rule" on page 133
	"To Add a New Rule" on page 135
	"To Move a Rule" on page 136
	"To Delete a Rule" on page 137

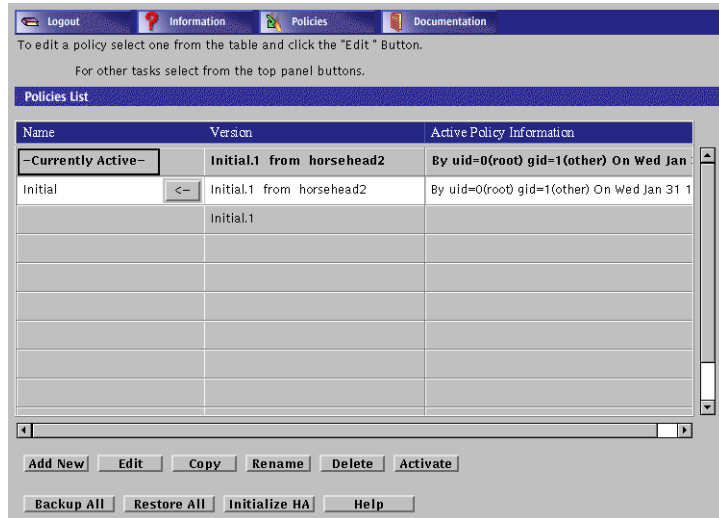
TABLE 3-1 Procedures for Managing Rules (Continued)

Rule	Procedure
Administrative Access Rules	"To Add or Change an Administrative Access Rule for Local Administration" on page 138
	"To Add or Change an Administrative Access Rule for Remote Administration" on page 140
	"To Specify a SKIP/IPsec/IKE Action on a Remote Access Rule" on page 145
NAT Rules	"To Manually Add an ARP Entry" on page 153
	"To Define NAT Rules" on page 153
	"To Edit the NAT Rules" on page 155
VPN Rules	"To Add a VPN Gateway Definition" on page 160
	"To Create Packet Filtering Rules for a VPN" on page 164

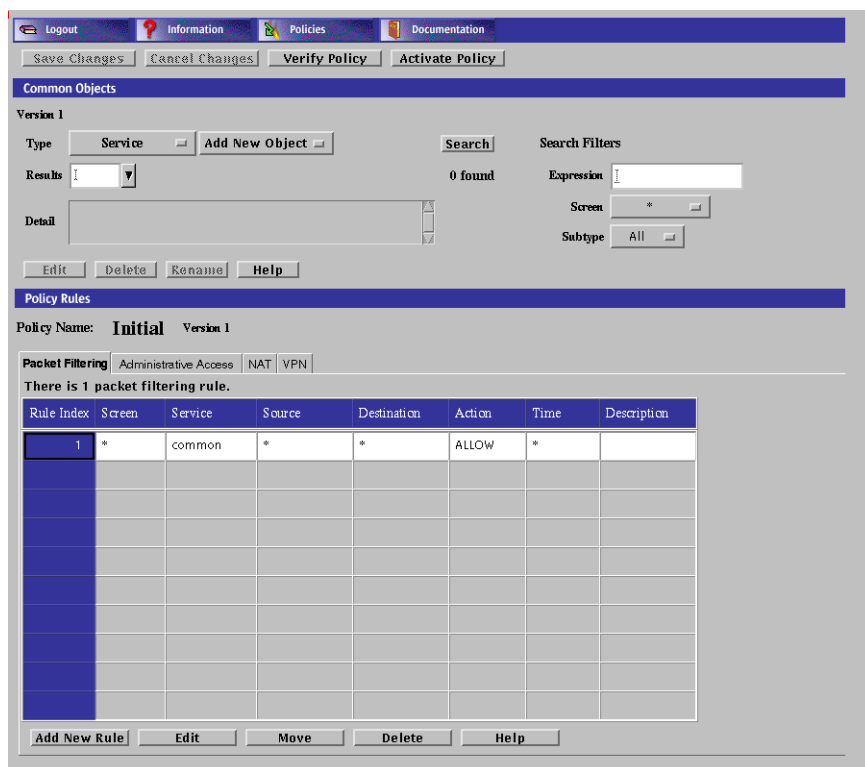
Packet Filtering Rules

▼ To Modify Rules

1. Choose a policy in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.



To display the controls on a tab, click the tab header. The following table describes the tabs that are available from the Policy Rules panel.

TABLE 3-2 Policy Rules Panel Tabs

Tab	Description
Packet Filtering	Shows the packet filtering rule or rules.
Administration Access	Defines access rules for local administration and remote Administration Stations through the administration GUI or the command line (see Chapter 10).
NAT (Network Address Translation)	Maps private network addresses to public network addresses.
VPN (Virtual Private Network)	Maps name, address, certificate, issued certificate (key) algorithm, data algorithm, MAC algorithm, tunnel address, and description.

▼ To View and Edit the Details of an Object

1. Execute the steps in “To Modify Rules” on page 130.
2. In the packet filtering table, click on the cell that contains the object you want to view or edit.

The dialog box for the chosen object appears.



Policy Rules

Policy Name: **Initial** Version 2

Packet Filtering | Administrative Access | NAT | VPN

There is 1 packet filtering rule.

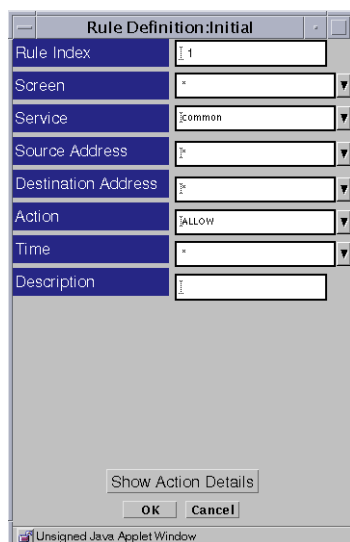
Rule Index	Screen	Service	Source	Destination	Action	Time	Description
1	*	common	*	*	ALLOW	*	

Note – The packet filtering table does not allow you to click and get a popup menu; you get a pulldown where you can select another value.

▼ To Edit a Rule

1. Execute the steps in “To Modify Rules” on page 130.
2. Click the Packet Filtering tab in the Policy Rules area.
3. Select the rule to edit.
4. Click the Edit button.

The Rule Definition dialog box for the selected policy appears.



5. Edit each field by clicking the down arrow to display the list.

You can add a new address, range of addresses, or list of addresses for both the Source and Destination addresses.

- | | |
|-------------|--|
| Rule Index | Assigns a number to a rule. When editing or adding a new rule, by default, this field displays a number one greater than the last rule (indicating this rule will be placed at the bottom of the list). If you type a lower number, the new rule is inserted into the specified position in the list, and the rules currently in the configuration are renumbered. |
| Screen | (Optional) Specifies the Screen for which you want the rule to apply. Select a specific Screen name in this field if you use centralized management and want a rule to apply to a specific Screen. |
| Service | Identifies the network service or service group to which this rule applies. |
| Source | The value to which the source address of a packet is compared. If an asterisk (*) appears, any source address meets the criteria of the rule. |
| Destination | The value to which the destination address of a packet is compared to determine whether the rule should apply. If an asterisk (*) appears, any destination address meets the criteria of the rule. |
| Action | Displays the action for the rule and permits setting the logging behavior. The options are ALLOW , DENY , ENCRYPT , and VPN . |
| Time | Specifies the time object which restricts the applicability of the rule. If an asterisk (*) appears, the rule applies at all times. |

Description (Optional) Provides a brief description of the Administrative Access rule.

6. Click the OK button in the Rule Definition dialog box when you have finished editing the rule.
7. (Optional) Click the Verify Policy button at the top of the Policy Rules page to ensure that you have created a valid policy.
8. Click the Save Changes button to be sure the changes are saved.

Note – Each Save creates a version.

Note – If a filtering rule fails to detect any issued certificate (key) encryption algorithms, it may display the following error message:

An error occurred in detecting the Encryption algorithms.
Please check if skipd process is running.

If this occurs, restart the SKIP daemon process with the `skipd_restart` command. See the “Configuration Editor Reference” in *SunScreen 3.2 Administrator’s Overview* for more information on the `skipd_restart` command.

▼ To Add a New Rule

1. Execute the steps in “To Modify Rules” on page 130.
2. Click the Add New Rule button in the Policy Rules area.
The Rule Definition dialog box for the selected policy appears.

Field	Value
Rule Index	2
Screen	*
Service	
Source Address	
Destination Address	
Action	
Time	*
Description	

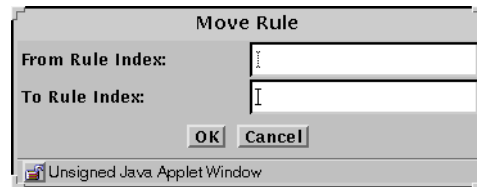
3. Edit each field by clicking the down arrow to display the list.
4. Click the OK button in the Rule Definition dialog box when you have finished editing the rule.
5. (Optional) Click the Verify Policy button at the top of the Policy Rules page to ensure that you have created a valid policy.

▼ To Move a Rule

1. Execute the steps in "To Modify Rules" on page 130.
2. Select the policy rule to be moved.

3. **Click the Move button.**

The Move Rule dialog box appears.



4. **Type the number of the rule that you want to move in the From Rule Index field.**

5. **Type the number of the position to which you want to move the rule in the To Rule Index field.**

6. **Click the OK button.**

The rules reorder themselves to reflect the change you made. You must move each rule whose position you want to change.

7. **(Optional) Click the Verify Policy button at the top of the Policy Rules page to ensure that you have created a valid policy.**

Note – Edits do not affect the behavior of the Screen, nor of established connections with state entries, until you activate the policy.

▼ To Delete a Rule

Note – Do not delete all the packet filtering rules or you may lose complete access to the Screen.

1. **Execute the steps in “To Modify Rules” on page 130.**

2. **Select the rule you want to delete from the table in the Packet Filtering area.**

3. **Click the Delete button.**

The Delete Rule dialog box appears.



4. Click the Yes button.

Administrative Access Rules

You use administrative access rules to:

- Provide access to the Screen from additional remote Administration Stations
- Provide access for local administration from the administration GUI.

You can add new users that you have created, re-add users for whom new passwords have been defined, or change SecurID assigned names on the Administrative Access page. You can also add an access rule for users and change the encryption parameters.

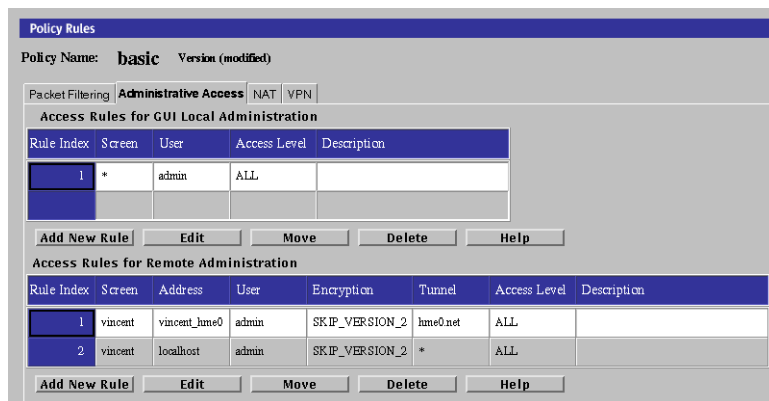
You must activate a new policy for any changes to take effect.

The fields of the Administrative access rules tab are described in the *SunScreen 3.2 Administrator's Overview*.

The following information describes using the administration GUI. Chapter 10 contains information about the command line interface.

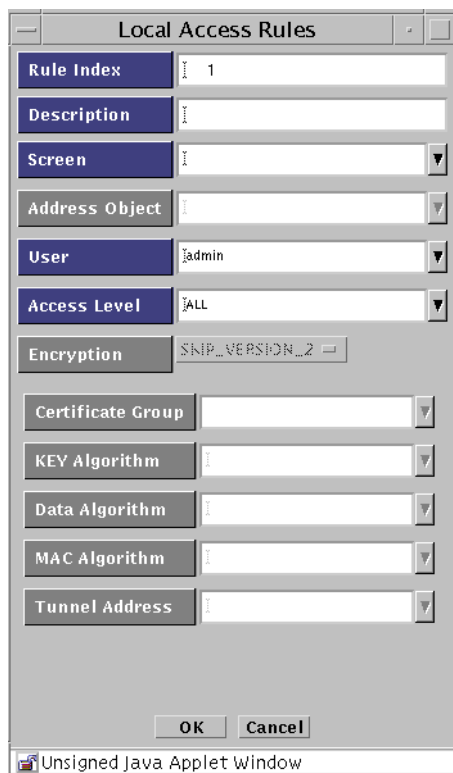
▼ To Add or Change an Administrative Access Rule for Local Administration

1. Execute the steps in "To Modify Rules" on page 130.
2. Click the Administrative Access tab to display the Administrative Access area.



3. Click the Add New Rule button, or Edit button, below the Access Rules for GUI Local Administration area.

The Local Access Rules dialog box appears.



The following table describes the controls for the Local Access Rules dialog box.

TABLE 3-3 Controls for the Local Access Rules Dialog Box

Control	Description
Rule Index	Assigns a number to a rule. By default, this field displays a number one greater than the last rule (indicating this rule will be placed bottom of the list). If you type a lower number, the new rule is inserted into the specified position in the list, and the rules currently in the configuration are renumbered.
Description	(Optional) Provides a brief description of the Administrative Access rule.
Screen	(Optional) Specifies the Screen for which you want the rule to apply. Type a specific Screen name in this field if you use centralized management and want a rule to apply to a specific Screen. The default All applies to <i>all</i> Screens.
User	Lists the user names of SunScreen administrators. Use the names that you defined for the Administrative User object.
Access Level	Specifies what actions the designated user can perform. <ol style="list-style-type: none">1. ALL – Allows the administrator to display and modify all setting for the Screen.2. WRITE – The administrator can perform all operations except modifying the Administration Access rules for any Policy.3. READ – The administrator can view both the Information and Policy. This level also allows the user to save and clear logs on the information page. With this access level users cannot modify any Policy data.4. STATUS – The administrator can display status information (logs, statistics, status information) but cannot display or modify management settings.5. NONE – The administrator no longer has any access. This switch prevents an administrator who had access from logging in without having to remove that administrator from the database.

▼ To Add or Change an Administrative Access Rule for Remote Administration

If you are adding an additional remote Administration Station, you must add a rule for it.

Note – If you change the encryption parameters, make a note of them; they have to match the encryption parameters on the remote Administration Station.

1. Execute the steps in “To Modify Rules” on page 130.
2. Click the Administrative Access tab in the Policy Rules area.

The screenshot shows the 'Policy Rules' configuration window. The 'Policy Name' is 'basic' and it is in 'Version (modified)' state. There are four tabs: 'Packet Filtering', 'Administrative Access', 'NAT', and 'VPN'. The 'Administrative Access' tab is selected, showing 'Access Rules for GUI Local Administration' with one rule (Rule Index 1, Screen *, User admin, Access Level ALL). Below this are buttons for 'Add New Rule', 'Edit', 'Move', 'Delete', and 'Help'. The 'Remote Administration' tab is also visible, showing 'Access Rules for Remote Administration' with two rules (Rule Index 1 and 2, both with Screen vincent, User admin, and Access Level ALL). The first rule has Address vincent_hme0, Encryption SKIP_VERSION_2, and Tunnel hme0.net. The second rule has Address localhost, Encryption SKIP_VERSION_2, and Tunnel *. Below this are buttons for 'Add New Rule', 'Edit', 'Move', 'Delete', and 'Help'.

3. Click the Add New Rule button in the Access Rules for Remote Administration area.

The Remote Access Rule dialog box appears.



The following table describes the controls for the Remote Access Rules dialog box.

TABLE 3-4 Controls for the Remote Access Rules Dialog Box

Control	Description
Rule Index	(Optional) Assigns a number to a rule. By default, this field displays a number one greater than the last rule (indicating this rule will be placed bottom of the list). If you type a lower number, the new rule is inserted into the specified position in the list, and the rules currently in the configuration are renumbered.
Description	(Optional) Provides a brief description of the remote administrative access rule.
Screen	(Optional) Specifies the Screen for which you want the rule to apply. Type a specific Screen name in this field if you use centralized management and want a rule to apply to a specific Screen. The default All applies to <i>all</i> Screens.
Address Object	Restricts addresses(es) from which users may initiate a connection..
User	Lists the user names of SunScreen administrators. Use the names that you defined for the Administrative User object.

TABLE 3-4 Controls for the Remote Access Rules Dialog Box (Continued)

Control	Description
Access Level	Specifies what actions the designated user can perform: <ol style="list-style-type: none">1. ALL – The administrator can display and modify all settings for the Screen.2. WRITE – The administrator can perform all operations except modifying the Administration Access rules for any Policy.3. READ – The administrator can view both the Information and Policy. This level also allows the user to save and clear logs on the information page. With this access level users cannot modify any Policy data.4. STATUS – The administrator can display status information (logs, statistics, status) but cannot display or modify management settings.5. NONE – The administrator does not have access.
Encryption	Specifies the type and version of encryption (SKIP or IKE) being used to encrypt traffic between the Screen and the Administration Station.
Certificate Group	(SKIP only) Specifies the name of the certificate group, which can correspond to a single certificate or a certificate group, allowed over this interface.
Key Algorithm	(SKIP only) Identifies the algorithm used to encrypt traffic-encrypting keys. The algorithms available depend on the strength of encryption (128 bit, or 56 bit) that you are using with SunScreen.
Data Algorithm	(SKIP only) Identifies the algorithm used to encrypt message traffic between the Screen and the Administration Station. The algorithms available depend on the strength of encryption (128 bit or 56 bit) that you are using with SunScreen.
MAC Algorithm	(SKIP only) Identifies the algorithm used to authenticate traffic.
Tunnel	Identifies the tunnel address used for the communication between the remote Administration Station and the Screen.
Move button	Enables you to assign a new rule index number for the rule that you highlighted in the Access Rules for Remote Administration panel of the Administrative Access tab.
Delete button	Deletes the access rule that you highlighted in the Access Rules for Remote Administration panel of the Administrative Access tab.
Help button	Displays the online help.

4. Select the user or group of administration users to which this access rule applies.

5. To associate this entry with a specific Screen, choose a Screen from the Screen list.

Note – If you are using the CMG (centralized management group) feature, and this field is left blank or contains an asterisk (“*”), the access rule being defined will, by default, allow access to all Screens in the cluster.

6. Select the address you want to use from the Address Object list.

7. Select the type of encryption you want to use from the Encryption list.

To use IPsec IKE, see “To Specify a SKIP/IPsec/IKE Action on a Remote Access Rule” on page 145.

To use SKIP (Simple Key-Management for Internet Protocol), follow these substeps:

- a. Select the version of SKIP you want to use from the Encryption list.

Use SKIP_VERSION_1 for communicating with an SPF-100. For later versions, choose SKIP_VERSION_2.

The required fields for SKIP_VERSION_1 are:

- Certificate Group
- Key Algorithm
- Data Algorithm

The required fields for SKIP_VERSION_2 are:

- MAC Algorithm
- Certificate Group
- Key Algorithm
- Data Algorithm

- b. Select the certificate group that you want to use from the Certificate Group list.

Specify the Screen’s certificate or certificate group (in this case, the certificate or certificate group that includes the remote Administration Station’s certificate) and administration IP address in the Screen’s Administration Certificate field.

- c. Select the key algorithm that you want to use from the Key Algorithm list.

- d. Select the data algorithm you want to use from the Data Algorithm list.

- e. (For SKIP_VERSION_2 *only*) Select the MAC algorithm that you want to use from the list of MAC algorithms.

- f. (Optional) Select the tunnel address of the remote Administration Station from the Tunnel list.

8. Type a description in the Description field.

9. **Select the level of access you wish to authorize for this user from the Access Level list.**

There are five access levels for remote administrators:

ALL —The administrator can display and modify all settings for the Screen.

STATUS — The administrator can display status information (logs, statistics, status) but cannot display or modify management settings

READ — The administrator can view both the Information and Policy. This level also allows the user to save and clear logs on the information page. With this access level users cannot modify any Policy data

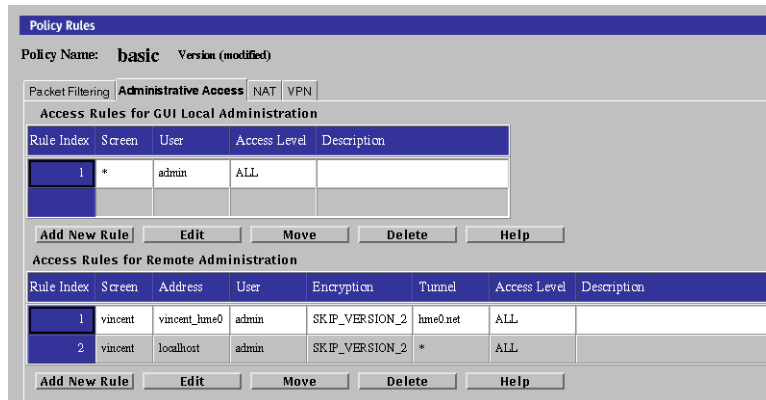
WRITE —The administrator can perform all operations except modifying the Administration Access rules for any Policy.

NONE (Default) — The administrator does not have access.

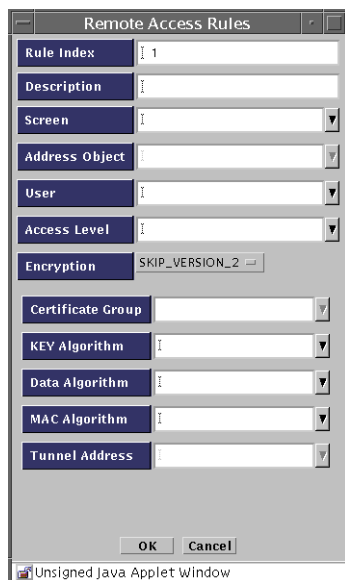
10. **Click the OK button.**
11. **Repeat the previous steps until you have added all the access rules for remote administration.**
12. **Click the Save Changes button.**
13. **Add the Screen's certificate MKID in the SKIP database of the remote Administration Station, and configure it to use SKIP to communicate with the Screen.**

▼ **To Specify a SKIP/IPsec/IKE Action on a Remote Access Rule**

1. **Execute the steps in "To Modify Rules" on page 130.**
2. **Select the Administration Access tab in the Policy Rules area.**
The Administration Access panel appears.



3. Click Add New Rule under the Access Rules for Remote Administration
The Remote Access Rules panel appears.



4. Select IPSEC IKE from the Encryption pulldown.
The Remote Access Rules panel for IPsec/IKE appears.

5. (Optional) Type a brief description for this rule.
6. Select the user or group of administration users to which this access rule applies.
7. To associate this entry with a specific Screen, choose a Screen from the Screen list.

Note – If you are using the CMG (centralized management group) feature, and this field is left blank or contains an asterisk (“*”), the access rule being defined will, by default, allow access to all Screens in the cluster.

8. Select the address you want to use from the Address Object list,
9. Select the level of access you wish to authorize for this user from the Access Level list.

There are five access levels for remote administrators:

ALL. Master administrators, who have the access level ALL, grant the various access levels to the other administrators.

STATUS. Status administrators, who have the access level STATUS, can monitor SunScreens, but cannot view the policies.

READ. Local administrators, who have the access level READ, are users responsible for reviewing their individual Screen's policy. Local Administrators are allowed to read policies, but cannot change them; to do so they must make a request for changes to executive or master administrators.

WRITE. Executive administrators, who have the access level WRITE, can define and change policies.

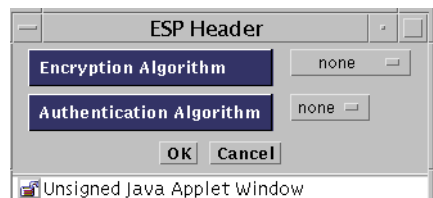
NONE (Default—obviously not for remote administrators)

10. If you are using IPsec, follow step 11 through step 17. If you are using IKE, follow step 18 through step 23.

Note – You must complete step 11 through step 17 plus step 18 through step 23 to perform remote administration for IKE.

11. (IPsec) To define the ESP, click the Edit button.

The ESP Header panel appears.



12. (IPsec) Select the Encryption Algorithm to be used. The options are none, Null, DES, 3DES, BLOWFISH, and AES.
13. (IPsec) Select the Authentication Algorithm to be used. The options are none, MD5, and SHA1.
14. (IPsec) Click the OK button
15. (IPsec) To define the authentication header (AH), click the Edit button.
The AH header appears.



16. **(IPsec)** Select the Authentication Algorithm to be used. The options are none, MD5, and SHA1.
17. **(IPsec)** Click the OK button
18. **(IKE)** Select the Encryption Algorithm to be used. The options are none, Null, DES, 3DES, BLOWFISH, and AES.
19. **(IKE)** Select the Hash Algorithm to be used. The options are none, MD5, and SHA1.
20. **(IKE)** Select the Oakley Group. The options are 1, 2, and 5.
21. **(IKE)** Select the Authentication Method to be used. The options are:

RSA-SIGNATURES
RSA-ENCRYPTION
DSS-SIGNATURES
22. **(IKE)** Select the name of the Source Certificate. You can click on the arrow to see a list of certificates that are defined.
23. **(IKE)** Click the OK button.

Network Address Translation (NAT) Rules

Note – You can use NAT with encryption to provide communication in an encrypted tunnel (secure *virtual private network*). Encryption at the source tunnel address takes place *after* the NAT mapping; decryption at the destination tunnel address must take place *before* the NAT translation.

NAT Mapping Overview

You use the NAT tab to set up mapping rules that translate IP addresses according to specific rules. These rules interpret the source and destination addresses of incoming IP packets, then translate either the apparent source or the intended destination and send the packets on. You can map hosts, lists of addresses, ranges of addresses, or specific groups, depending on what you have configured in your SunScreen installation.

The map used during the translation of a packet consists of rules. In general, you would translate addresses to:

- Ensure that internal addresses appear as registered addresses on the Internet
- Send traffic for a specific destination to a different, predetermined destination

When defining NAT rules, the first rule (lowest number) that matches a packet applies, and no other rules can apply. Therefore, you might define specific rules first, then broader cases later.

You can define the mappings of internal addresses to external addresses. Use the NAT tab in the Policy Rules area of the Policy Rules page to specify the address that is to be translated to a particular address and to specify static mapping or dynamic mapping. For additional information on NAT, see “Network Address Translation” in *SunScreen 3.2 Administrator’s Overview*.

All network address translations take place before a packet is tested against any of the screening rules. In this way, you can define all screening rules using only internal addresses.

NAT Administration Page

The meanings and uses of the specific fields in the NAT page are described in the following table.

TABLE 3-5 NAT Page Field Explanations

Field	Use
Rule Index	Use this field to assign a number to a rule. By default, this field displays a number that is one greater than the last rule, which indicates the rule is placed at the end of the list. If you type a specific number, the new rule is inserted into that position in the list, and the rules in the policy are consequently renumbered.
Screen	Use this field to specify the Screen for which you want the rule to apply. Type a specific Screen name in this field if you use Centralized Management and want a rule to apply to a specific Screen. If a Screen isn't specified, the rule applies for all Screens that are defined. If Centralized Management is in place, each NAT rule must be associated explicitly with the Screen to which it applies.
Mapping	<ul style="list-style-type: none">■ <i>Static</i> Specify static mapping to set up a one-to-one relationship between two addresses. You can use static mapping to set new apparent IP addresses for hosts on your network without having to reconfigure each host.■ <i>Dynamic</i> Specify dynamic mapping to map source addresses to other addresses in a many-to-one relationship. You can use dynamic mapping to ensure that all traffic leaving the firewall appears to come from a specific address or group of addresses, or to send traffic intended for several different hosts to the same actual IP access.
Source	Specify the source address to map from an untranslated packet. Source addresses are the actual addresses contained in the packet entering the firewall.
Destination	Specify the destination address for the untranslated packet. Destination addresses are the actual addresses contained in the packet entering the firewall.
Translated Source	Specify the translated source address for a packet. The address from which the packet appears to originate is the translated source.
Translated Destination	Specify the translated destination address for a packet. The translated destination is the actual address where the packet goes after it leaves the firewall. You cannot translate both source and destination addresses; that is, you cannot make packets appear to come from a different IP address and simultaneously direct the packets to a different destination.

TABLE 3-5 NAT Page Field Explanations (Continued)

Field	Use
Description	Use this field to provide a description of the rule.

All static NAT rules are unidirectional. They work precisely as defined and are *not* interpreted as also applying in the reverse direction. Thus, if you map an internal source address to an external source address and you want the mapping to apply in the reverse direction, you must use a second rule to map the external destination address to the internal destination address explicitly.

Dynamic NAT requires only one rule.

Your NAT Scenario

When building security policies using NAT, define the security policy rules in terms of internal addresses. All packets that are destined for external addresses used in NAT must be routed to the Screen.

Note – If you use static NAT to map a machine’s address, a machine on any other network can initiate traffic to that machine, given a properly defined reverse rule.

In routing mode (unlike stealth mode), the Screen does not automatically answer ARP requests for destination address. Consequently, the Screen must either route to a separate network that has a destination address, or a proxy ARP entry must be configured manually.

Static NAT is a one-to-one mapping of the internal address to an external address. Dynamic NAT is many-to-one or many-to-few mapping of internal addresses to an external address.

For more information on NAT and the possible set up, see “Network Address Translation” in *SunScreen 3.2 Administrator’s Overview*. For an example that uses NAT, see *SunScreen 3.2 Configuration Examples* manual.

Note – In cases where NAT will occur between the Administration station and the Screen, do not include the address of a remote Administration Station in any of your NAT rules.

If Centralized Management is in place, each NAT rule must be associated explicitly with the Screen to which it applies.

▼ To Manually Add an ARP Entry

- **For networks that attach to the Screen on the inside and have NAT mappings applied, use the following command.**

This is recommended for any network on which there are addresses to which you want to allow public access.

```
# arp -s IP_Address ether_address pub
```

You must add this entry each time you reboot the Screen, so you may want to modify a startup script to do this automatically when you reboot.

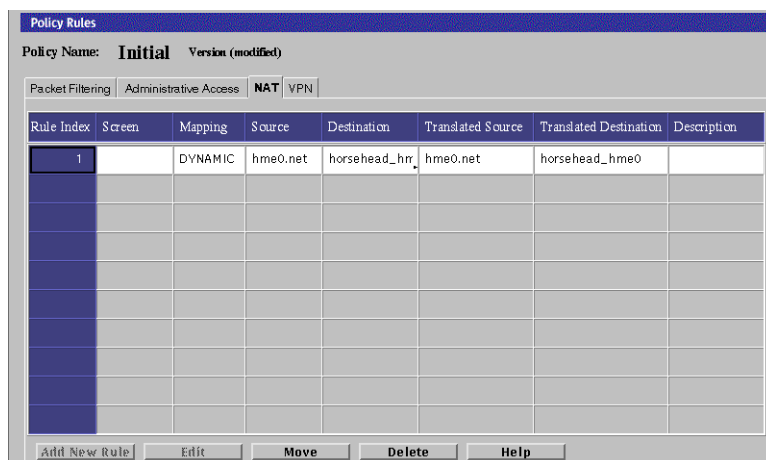
Note – This entry is **not** necessary in stealth mode.

The following information describes how to use the administration GUI. Chapter 10 contains information about the command line interface.

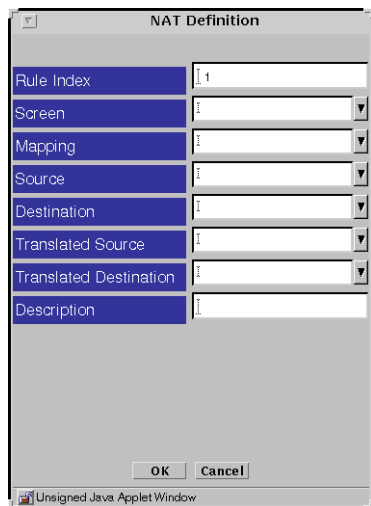
▼ To Define NAT Rules

When you design a static NAT mapping, be sure that the ranges and groups used in the Source and Translated Source fields and the ranges and groups used in the Destination and Translated Destination fields are exactly the same size.

1. **Execute the steps in “To Modify Rules” on page 130.**
2. **Select the NAT tab in the Policy Rules area.**
The Network Address Translation area is displayed.



3. Click **Add New Rule** below the Network Address Translation area. The NAT Definition dialog box is displayed.



4. Select the **Screen** that should use NAT mapping. The default is NAT applied to the policies of all Screens.
5. Select all four addresses in the NAT Definition dialog box.
6. Click the **OK** button.

7. Repeat the previous steps until you have configured all the rules as required.
8. Click the Save Changes button to save the edited mappings.
You must click the Activate button for the changes take effect.
In most cases, when you define a static mapping, the internal address and external address are both *single* addresses.

▼ To Edit the NAT Rules

1. Execute the steps in “To Modify Rules” on page 130.
2. Select the NAT tab in the Policy Rules area.
The Network Translation area appears.

Rule Index	Screen	Mapping	Source	Destination	Translated Source	Translated Destination	Description
1		DYNAMIC	hme0.net	horsehead_hrr	hme0.net	horsehead_hme0	

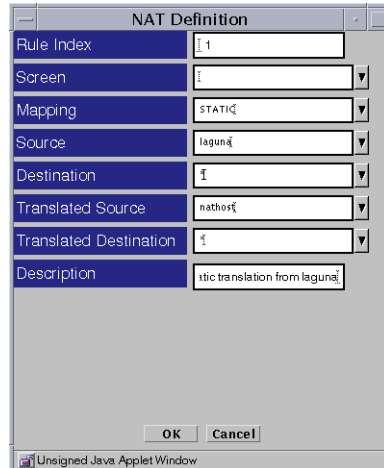
3. In the Mapping field, select the mapping on the table that you want to edit.
4. Click the Edit button below the Network Address Translation area.
The NAT Definition dialog box for that mapping appears.



5. **Select the type of mapping that you want in the Mapping field.**
6. **Select the address that you want in the Source field.**
The source address in the Source field should match the packet.
7. **Select the address that you want in the Destination field**
The destination address in the Destination field should match the packet.
8. **Select the translated source that you want.**
9. **Select the translated destination that you want.**
10. **Click the OK button of the NAT Definition dialog box to save your edits.**
11. **Repeat the previous steps until you have edited all the mappings as required.**
12. **Click the Save Changes button to save the edited mappings to a file.**
You must click the Activate button for the changes take effect.

Example: Static NAT of a Host to a Host

The following example translates the address of laguna to nathost for all destination addresses for all outgoing traffic.



The screenshot shows a dialog box titled "NAT Definition" with the following fields:

Field	Value
Rule Index	1
Screen	
Mapping	STATIC
Source	laguna
Destination	*
Translated Source	nathost
Translated Destination	*
Description	static translation from laguna

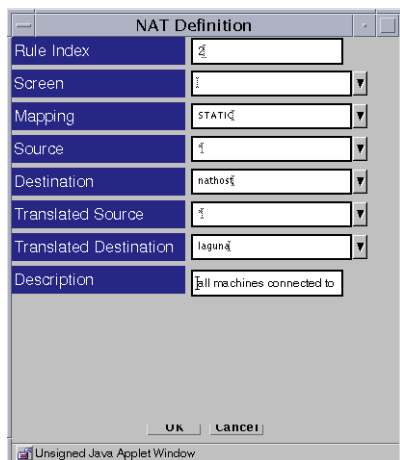
Buttons: OK, Cancel

Footer: Unsigned Java Applet Window

Example: Reverse Rule

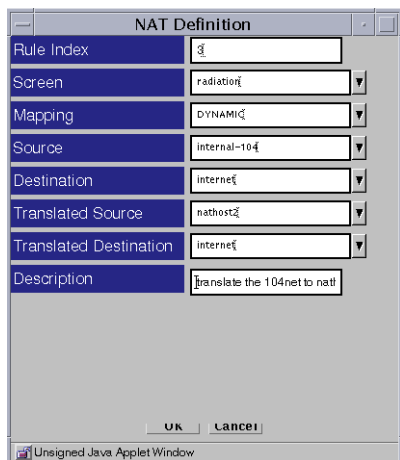
The following example translates the address nathost to laguna for all source addresses for all incoming traffic.

Note – Although one-way communication is allowed, and one of these rules may be used without the other, it is more common to use both together.



Example: Dynamic Translation of a Range Of Addresses to One Host

In the following example, the translation occurs only when the destinations match what is in the internet address group. If the address is not in this group, the source address cannot be translated.



Virtual Private Network (VPN) Rules

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.

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 VPN endpoints and give the definition for a VPN name. Then, you use the VPN name as part of a Packet Filtering rule with the VPN action. 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.

Note – SunScreen provides another option for creating a VPN gateway: Use the ENCRYPT action on Packet Filtering rules. In this scenario, you define the encrypted VPN endpoints as part of a regular Packet Filtering rule. The VPN 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

See the *SunScreen 3.2 Configuration Examples* manual for detailed examples of using VPN rules.

Before You Begin

Before you configure a VPN, you must complete several preliminary tasks:

- Install the SunScreen software on all Screens involved in the VPN.
For detailed information on Screen installation, refer to the *SunScreen Installation Guide*.

Note – Each Screen must have its own local certificate.

If you install a Screen with remote administration, this certificate is generated automatically. If not, refer to “To Generate SKIP UDHs Certificates” on page 76 for details on how to create this certificate if you are using SKIP or to “To Generate an IKE Certificate” on page 68 if you are using IKE.

- Add a certificate object to each Screen for every other Screen in the VPN.
For more information on adding certificates, refer to “To Associate SKIP Certificate” on page 81 if you are using SKIP or to “To Associate an IKE Certificate” on page 74 if you are using IKE.
- Create Address objects (host, group, or range) on each Screen for any address in the VPN, including an Address object for each Screen as well.
Refer to “Address Objects” on page 60 for more information.

Once you successfully complete these tasks, set up the VPN by defining VPN gateways and creating packet filtering rules as described in the following sections.

Configuring a VPN

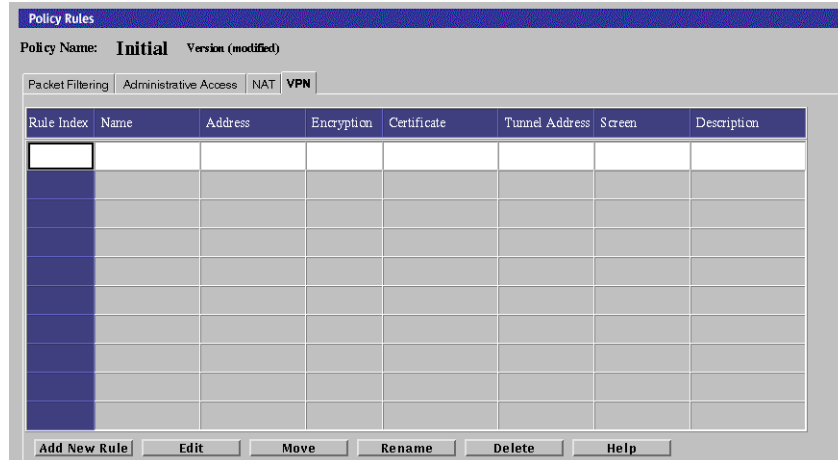
To define the systems that are taking part in a particular VPN, you need to create a VPN gateway for each Screen involved in the VPN. You create these gateway definitions by using the VPN tab in the Policy Rules area of the Policy Rules page.

Each VPN gateway definition associates a particular certificate with a set of hosts that are *protected* by that gateway. The protected hosts will have traffic protected by that certificate and its private key.

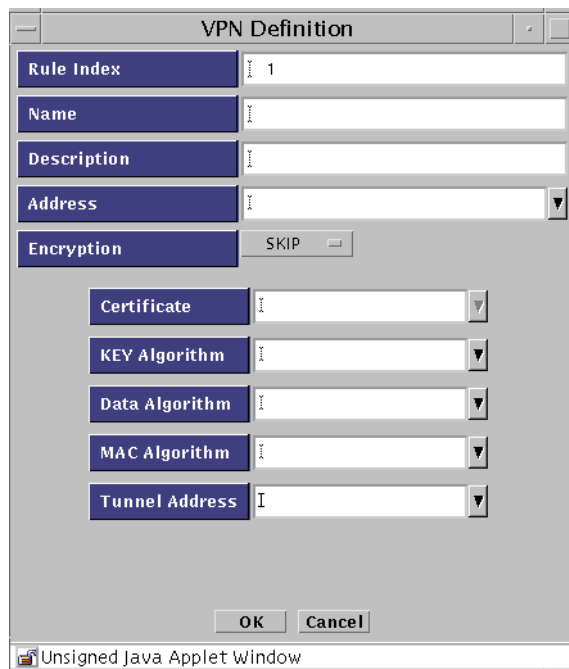
▼ To Add a VPN Gateway Definition

1. Execute the steps in “To Modify Rules” on page 130.

2. Click the VPN tab in the Policy Rules area.



3. Click the Add New Rule button in the VPN area.
The VPN Definition dialog box appears.



The following table describes the controls in the VPN Definition dialog box for defining VPN gateways.

TABLE 3-6 Controls in the VPN Definition Dialog Box

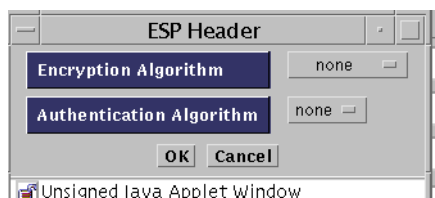
Control	Descriptions
Rule Index	(Optional) Assigns a number to a rule. By default, this field displays a number one greater than the last rule (indicating this rule will be placed the end of the list). Typing a lower number inserts the new rule into the specified position in the list and renumbers the rules currently in the configuration. Rules take effect in order.
Name	Specifies the Name of the VPN to which this gateway belongs. Type the same name in the Name field for each gateway that is in the VPN.
Description	(Optional) Provides a short description of the VPN gateway.
Address	Specifies the addresses to be protected by this VPN gateway.
Encryption	Specifies the type of encryption. Select either SKIP or IPsec IKE.
Certificate	Specifies the name of the certificate for this VPN gateway.
Key Algorithm	(SKIP only) Specifies the secret (key) algorithm the VPN uses. All gateways in the same VPN must use the same (key) algorithm.
Data Algorithm	(SKIP only) Specifies the data algorithm the VPN uses. All gateways in the same VPN must use the same data algorithm.
MAC Algorithm	(SKIP only) Specifies the MAC algorithm the VPN uses. All gateways in the same VPN must use the same MAC algorithm.
Tunnel Address	(SKIP only) Specifies the destination address on the outer (unencrypted) IP packet to which tunnel packets are sent.

4. **In the Name field, type the name of the VPN to which the gateway belongs.**
Type the same name for each gateway to be included in the VPN.
5. **(Optional) Type a description of the VPN gateway in the Description field.**
6. **In the Address field, select the addresses to be protected by this VPN gateway.**
7. **Select the encryption type. If you select IPSEC IKE, the following panel appears. Go to step 13 below for the IPsec IKE definitions**
8. **In the Certificate field, select the gateway's Certificate ID.**
9. **In the Key Algorithm field, select the key algorithm (or "none") to be used by the VPN.**
All gateways in the same VPN must use the same key algorithm.

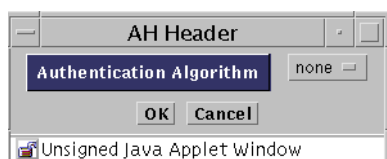
10. In the **Data Algorithm** field, select the data algorithm (or “none”) to be used by the VPN.
All gateways in the same VPN must use the same data algorithm.
11. In the **MAC Algorithm** field, select the MAC algorithm (or “none”) to be used by the VPN.
All gateways in the same VPN must use the same MAC algorithm.
12. In the **Tunnel Address** field, select the tunnel address to be used by the VPN.
13. If you selected **IPSEC IKE** for encryption, you can select the algorithms to be used as follows:

The screenshot shows the 'VPN Definition' dialog box with the 'Algorithms' tab selected. The 'Encryption' field is set to 'IPSEC IKE'. Under the 'Algorithms' section, there are three main categories: ESP, AH, and IKE. The ESP and AH sections have 'EDIT' buttons. The IKE section is expanded, showing several configuration fields: 'Encryption Algorithm' (none), 'Hash Algorithm' (none), 'Oakley Group' (1), 'Authentication Method' (RSA-SIGNATURES), 'Preshared Key', 'Source Certificate', and 'Destination Certificate'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The window title bar indicates it is an 'Unsigned Java Applet Window'.

- a. Click the **ESP Edit** button to define the ESP header encryption and authentication algorithms.



- b. Click the AH Edit button to define authentication headers.



- c. Select the Encryption Algorithm for IKE. The options are none, null, DES, 3DES, BLOWFISH, or AES.
 - d. Select the Hash Algorithm. The options are MD5 or SHA1.
 - e. Select the Oakley Group. The options are 1, 2, or 5.
 - f. Select the Authentication Method. The options are RSA-SIGNATURES, or DSS-SIGNATURES.
 - g. Select the Source Certificate. Click the arrow to see a list of available IKE certificated.
14. Click the OK button.

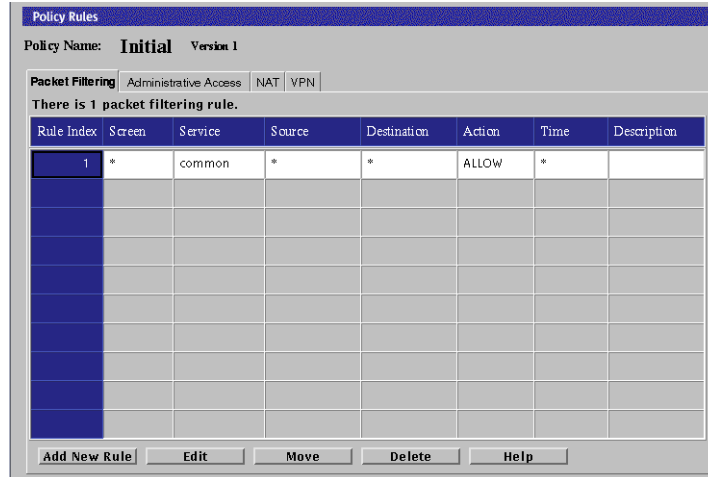
Note – Repeat step 3 through step 14 to define a VPN gateway for each Screen in the VPN. To make sure they are all included in this particular VPN, be sure to give all of them the same VPN name.

▼ To Create Packet Filtering Rules for a VPN

To use the VPN you have defined by creating VPN gateways, perform the following steps to add packet filtering rules:

1. Execute the steps in “To Modify Rules” on page 130.

2. Click the Packet Filtering tab of the Policy Rules area.



3. Click the Add New Rule button at the bottom of the rules.
The Rule Definition dialog box appears.

Rule Definition:Initial	
Rule Index	2
Screen	*
Service	*
Source Address	*
Destination Address	*
Action	VPN
Time	*
Description	*

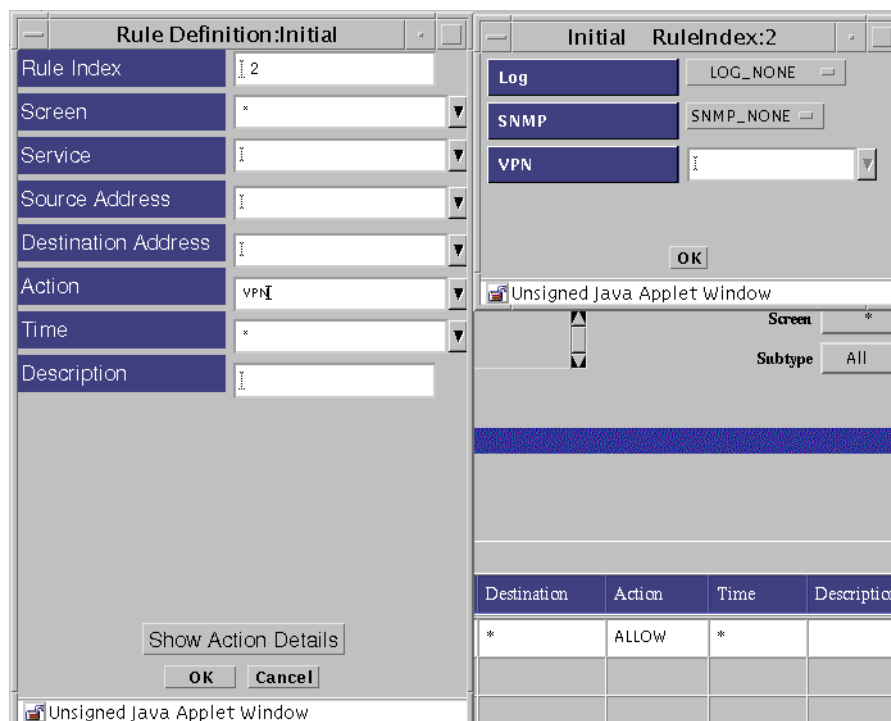
Show Action Details

OK Cancel

Unsigned Java Applet Window

4. Type the information into the fields as desired.

You may use the asterisk, or wildcard, character (“*”) in the source and destination fields. Using a wild card will check all traffic to see if it is part of the specified VPN. Select VPN in the action field. When the Action Details dialog box requires a VPN, select the name of the VPN used when defining the VPN gateways.



The one VPN-based rule will then generate all the VPN gateway pair-wise rules so that the hosts at each site can communicate with each other securely. Any host that cannot be secured (for example, if it is not protected by a VPN gateway) will *not* be allowed to communicate by the VPN-based rule. You can create a rule that allows that particular host to communicate, but you must set that up separately and explicitly.

5. Click the OK button for both the Action Details and the Add Rule dialog boxes.

Note – If you did not use “*” for source, destination, and service, repeat steps 2 through 4 for any additional rules. You must add VPN rules for each Screen that is part of the VPN.

Creating and Managing Policies

This chapter describes:

- Viewing the Policies List page
- Working with policies
- Adding, copying, renaming, and verifying a policy
- Deleting a policy
- Backing up all policies
- Restoring all policies
- Leaving an administration session
- Unlocking a policy
- Saving policy changes
- Canceling policy changes
- Activating a policy

The following table list the procedures in this chapter.

TABLE 4-1 Working With Policies

Policy Action	
	"To Work with Policies" on page 171
	"To Edit a Policy" on page 172
	"To Add a New Policy" on page 173
	"To Copy a Policy" on page 174
	"To Rename a Policy" on page 175
	"To Delete a Policy" on page 176
	"To Verify a Policy" on page 177
	"To Back Up All Policies" on page 179
	"To Restore All Policies" on page 181

TABLE 4-1 Working With Policies (Continued)

Policy Locks	"To Leave an Administration Session" on page 183
	"To Unlock a Policy" on page 183
	"To Forcibly Clear the Lock" on page 184

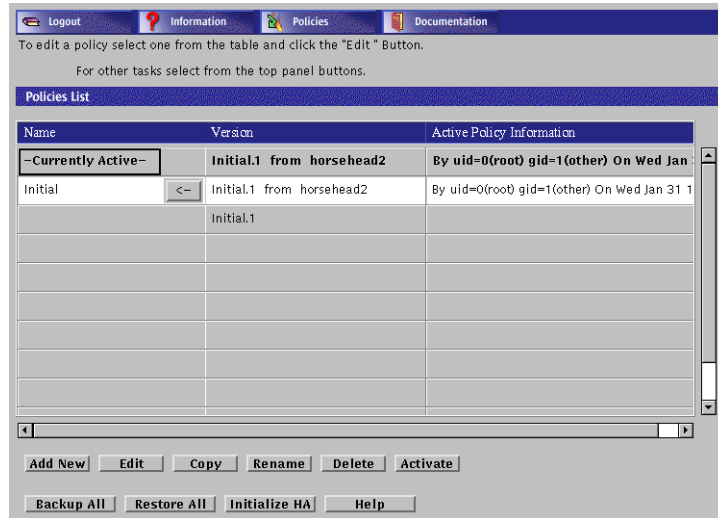
Activating Policies	"To Save Changes" on page 184
	"To Cancel Policy Changes" on page 186
	"To Activate a Policy" on page 186

Working With Policies

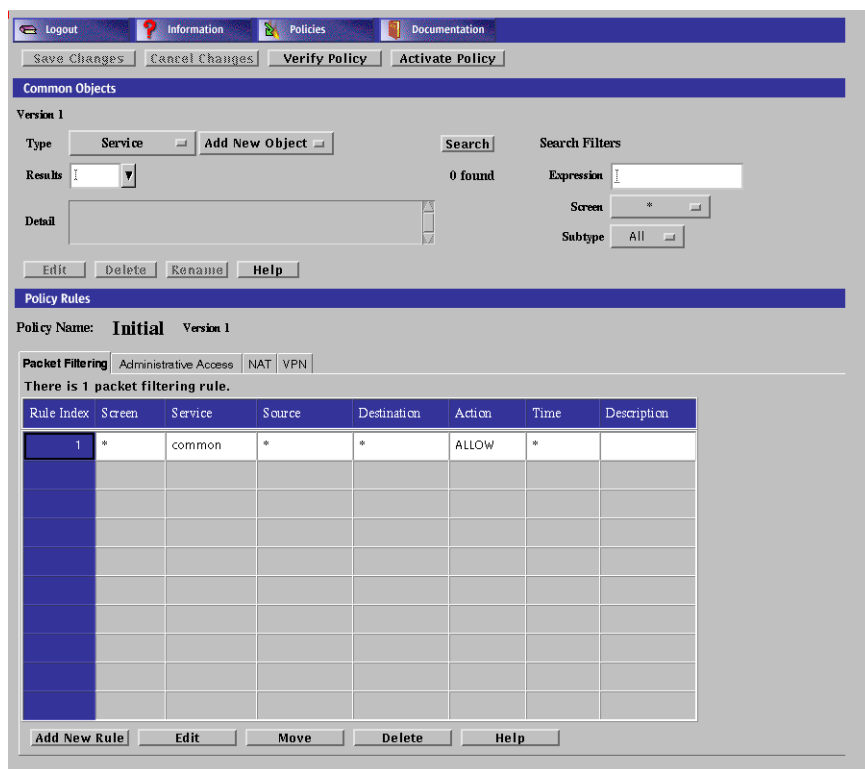
To reach the Policies List page, you can either choose Manage Policies for the Select Task field on the Login page before you click the Login button, or click the Policies button on the administration GUI's navigation bar.

▼ To Work with Policies

1. Select a policy in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.



Editing Policies

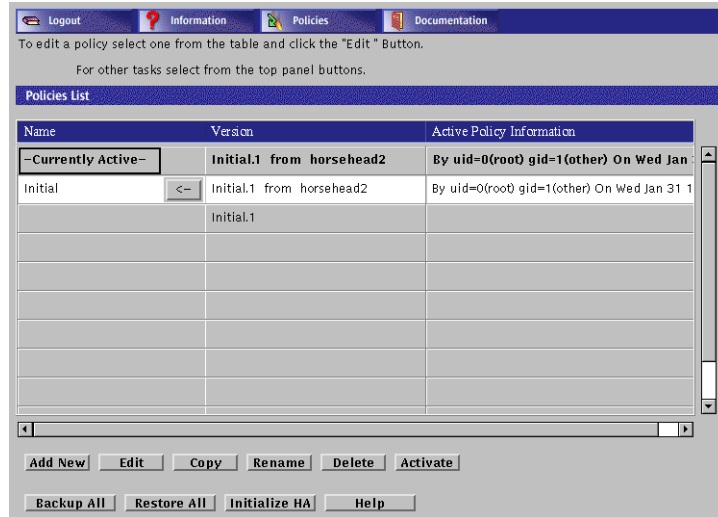
▼ To Edit a Policy

You can edit any policy to which you have WRITE access except the currently active policy. This policy is a READ ONLY copy of a policy that lets you view the rules currently in use by the firewall. The actual editable version of the currently active policy is available through the list of policies on this page.

When you installed SunScreen, a policy named `Initial` was created, containing enough information for you to start administering the Screen. You can work with this policy or create another policy and set it to be the currently active policy.

Note – Logging in as a user with an access level of ALL or WRITE puts you into a session. If you make changes to a policy, you cannot log out of the session until you either save or cancel those changes.

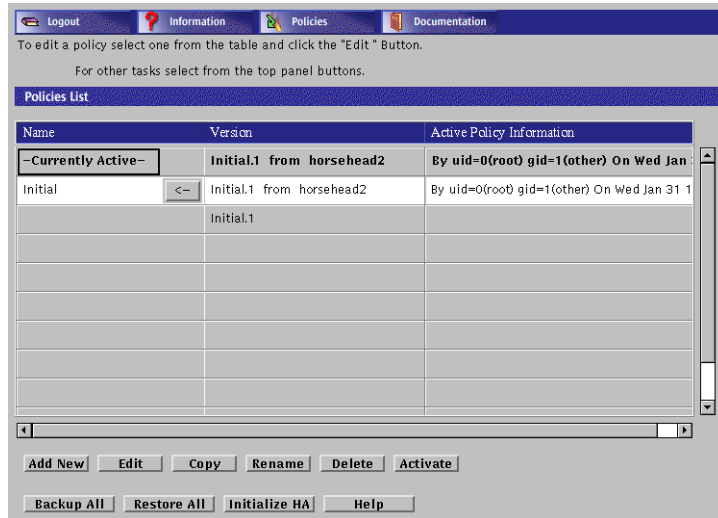
- **Select a policy in the Policies List page.**



Note – The View button appears if the policy you chose can only be read in read-only mode (for example, the Currently Active policy in the first row, and the policy versions in the Version column). See the *SunScreen 3.2 Administrator's Overview* for more information on policy types.

- ▼ **To Add a New Policy**

1. **Select a policy in the Policies List page.**



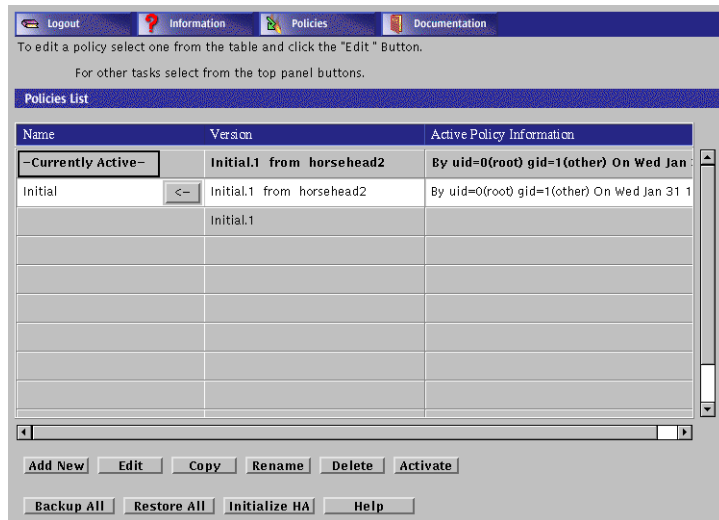
2. Click the Add New button.
The Add New Policy dialog box appears.



3. Type the name of the new policy in the Add New Policy dialog box.
4. Click the OK button.

▼ To Copy a Policy

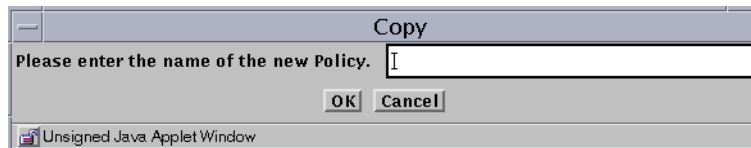
1. Select a policy in the Policies List page.



2. Select the policy you want to copy.

3. Click the Copy button.

The Copy dialog box appears.

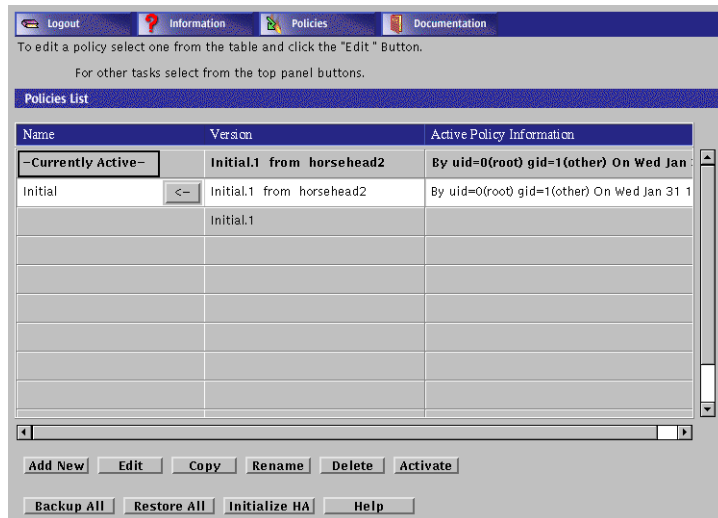


4. Type the name of the new policy in the Copy dialog box.

5. Click the OK button.

▼ To Rename a Policy

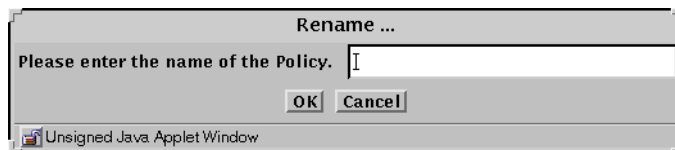
1. Select a policy in the Policies List page.



2. Select the policy you want to rename.

3. Click the **Rename** button.

The Rename dialog box appears.

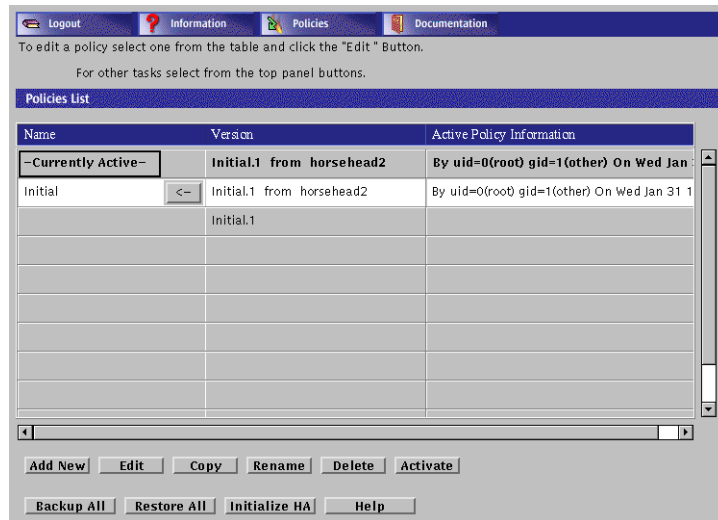


4. Type the name of the new policy in the **Rename** dialog box.

5. Click the **OK** button.

▼ To Delete a Policy

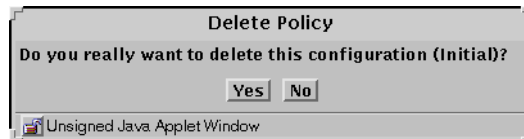
1. Select a policy in the **Policies List** page.



2. Select the policy you want to delete.

3. Click the Delete button.

The Delete Policy dialog box appears.

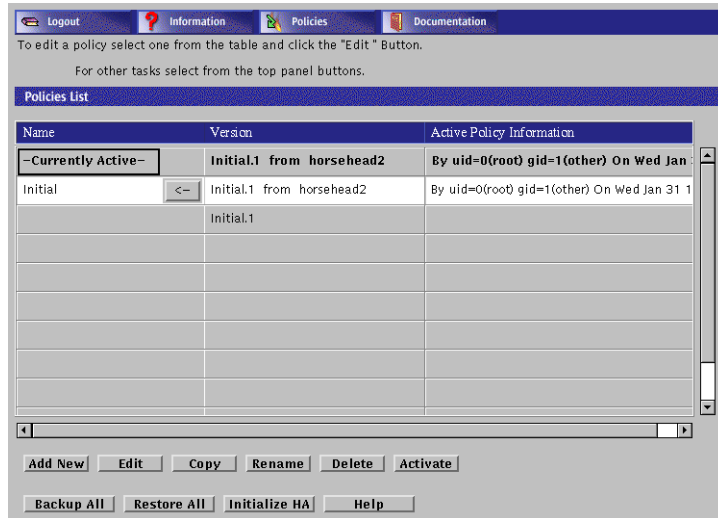


4. Click the Yes button in the Delete Policy dialog box to delete the policy.

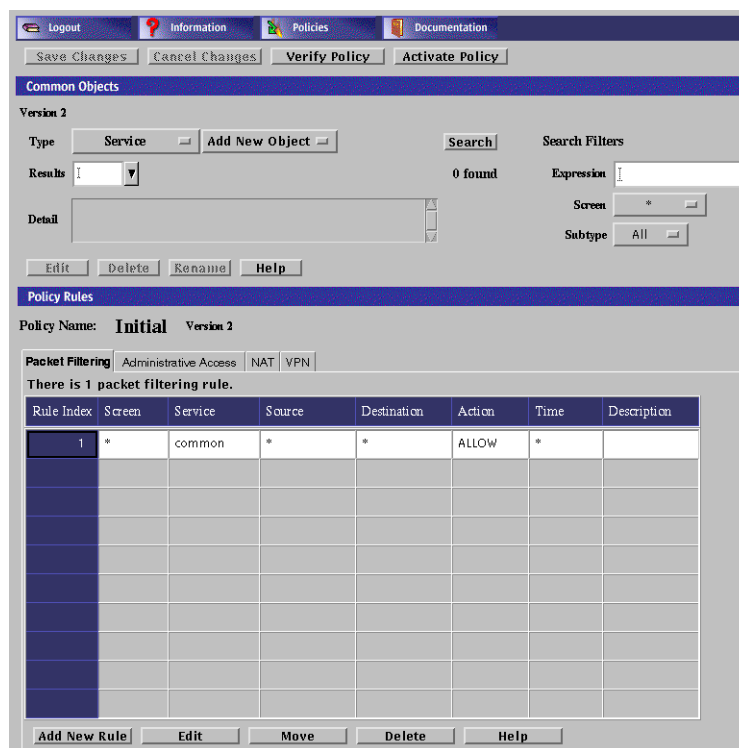
▼ To Verify a Policy

To verify that any changes you have made are stable:

1. Select a policy in the Policies List page.



2. Select the Policy you want to verify.
3. Click the Edit button.
The Policy page for the selected policy appears.



4. Click the Verify Policy button above the Common Objects area.

Clicking the Verify Policy button verifies that all the rules are valid and should compile successfully when you activate this policy. The rules in the chosen policy file are checked for errors, but the policy *is not activated*. Verifying a policy allows you to debug it without activating it.

You can activate the policy when verification has succeeded.

▼ To Back Up All Policies

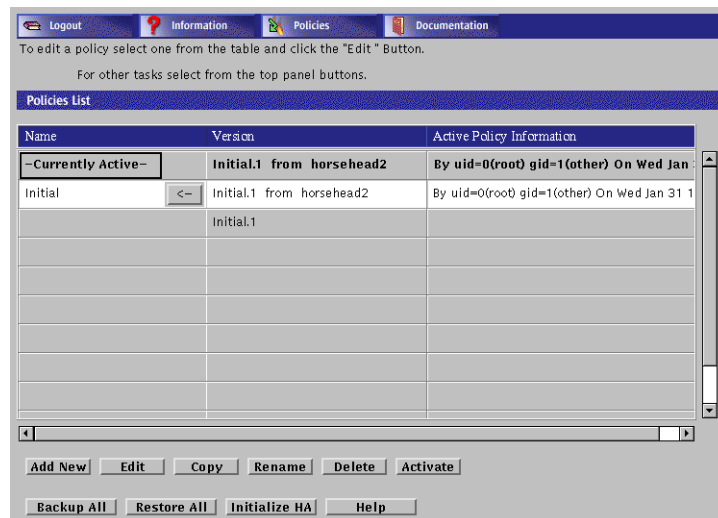
Backing up your policies is always good practice, especially if anything happens to the disk. You also should back up the original policy after you install SunScreen. This makes it easier to restore earlier policies, if necessary. Backing up from the administration GUI backs up only the current versions of all the policies.



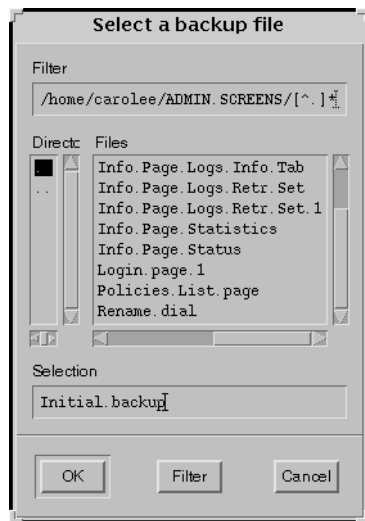
Caution – The backup medium contains copies of the local identities (the encryption keys and certificates) and must be stored securely and disposed of properly to avoid compromising your security.

Note – This procedure requires a browser that can be used to access Local files. You can use the HotJava Browser, Netscape, or Internet Explorer with Sun's Java Plug-In and the `identitydb.obj` file (copied to the correct location). See "To Install the Java Plug-In on the Screen" on page 23 for information on how to install the plug-in.

1. Select a policy in the Policies List page.



2. Click the **Backup All** button to back up the current version of the policies. The Select a backup file dialog box appears.



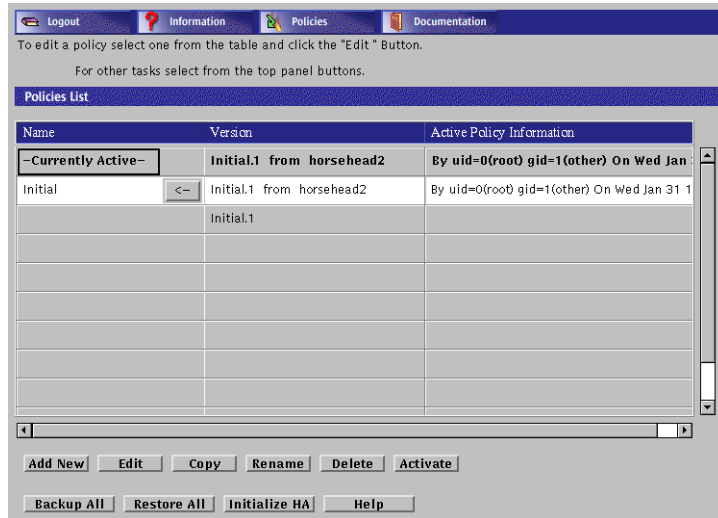
3. Type the path name of the directory in the Filter field and type the name of the backup file in the Selection field.

▼ To Restore All Policies

Note – This procedure requires a browser that can be used to access Local files. You can use the HotJava Browser, Netscape, or Internet Explorer with Sun's Java Plug-In and the `identitydb.obj` file (copied to the correct location). See "To Install the Java Plug-In on the Screen" on page 23 for information on installing the plug-in.

The Restore operation causes all current policy information, including common objects, to be overwritten by the new information from the backup file.

1. Select a policy in the Policies List page.



2. Click the Restore All button.
The Select a backup file dialog box appears.



3. Type the path name of the directory in the Filter field and the file name for the backup file in the Selection field.

4. Click the OK button.



Caution – Before you change the administration address (such as `1e0`, `qe0`, or `hme0`), the administration certificate, the local certificate, or the administration-group certificate, be sure that you understand how each one affects your ability to connect to the SunScreen. If you change these items, you risk losing connectivity from the Administration Station to the Screen. Reestablishing connectivity is difficult and requires that you log into the Screen directly or use an Administration Station that is still working. It also requires an exchange of encryption information.

Working With Policy Locks

▼ To Leave an Administration Session

- Logging in as a user with an access level of **ALL** or **WRITE** puts you into a session. If you make changes to a policy, you cannot log out of the session until you either save or cancel those changes.

▼ To Unlock a Policy

A *lock* is automatically acquired and held by the first person to change a policy. The lock is held on a per system basis; if someone acquires the lock, you cannot make changes to a policy.

The lock does not affect the buttons in the SunScreen banner. Anyone can request a search at any time and view the Documentation and Information pages.

If the Could not acquire the lock message appears (to indicate that someone has made changes to the policy):

- On the command line, type:

```
edit> QUIT  
Or
```

- In the administration GUI:

1. Click the **Cancel Changes** button.

2. Click the Policies button in the SunScreen banner.

You can try to edit the policy later.

Note – When you click the Save Changes button or log out, you give up the lock and others can work on the Screen.

▼ To Forcibly Clear the Lock

- To clear the lock forcibly, type the following at the command line:

```
# ssadm lock -c policy_name
```

Activating Policies

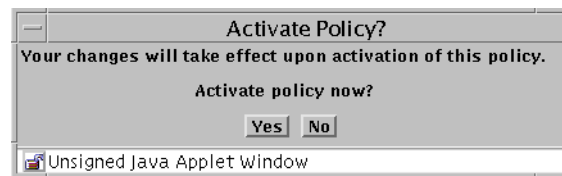
▼ To Save Changes

To save your changes:

1. Select a policy in the Policies List page.



2. Make required changes to the policy and rules.
3. Click the Save Changes button to save all changes made for all objects and rules in the policy.
An Activate Policy dialog box appears.



4. Select Yes if you wish to activate the policy.

▼ To Cancel Policy Changes

If you want to return to the previous saved version of a rule:

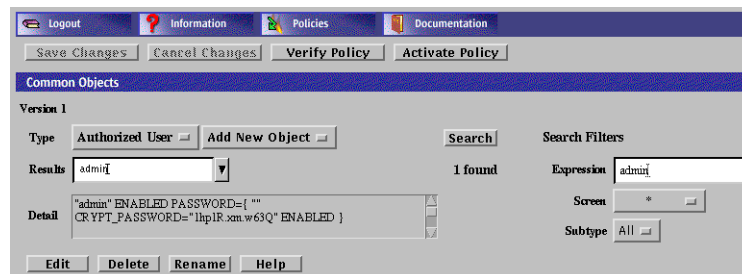
1. **Make changes to either the policies or the rules**
2. **Click the Cancel Changes button.**

Changes made before you click the Cancel Changes button are not saved.

▼ To Activate a Policy

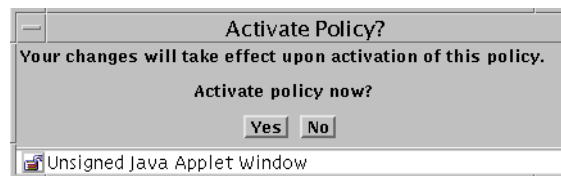
Use **Activate** when you want the rules you see to be the ones the Screen uses to filter traffic.

1. **Select the name of the policy in the Policies List page.**



2. **Click the Activate button to activate the policy.**

The Verifying/Activating window with the activation status appears.



Using High Availability

“High Availability”(HA) is a SunScreen configuration that consists of a primary Screen and a secondary Screen or Screens that mirror the operations on the primary Screen. In this way, the HA configuration behaves as a single system. Should anything cause the primary Screen to fail, the secondary Screen immediately takes over, providing uninterrupted operation. This chapter describes how to set up high availability Screens. You can also find a detailed example of a high availability configuration in “Stealth Mode With HA” in *SunScreen 3.2 Configuration Examples*.

Note – You can upgrade SunScreen EFS 2.0, 3.0, and 3.1 HA clusters to SunScreen 3.2. There is an upgrade script to aid the transition for 3.0 and 3.1 HA clusters to SunScreen 3.2. The Upgrade from EFS 2.0 is a more manual process. See the *SunScreen Installation Guide* for upgrade information.

The following table list the procedures in this chapter.

TABLE 5-1 Procedures for Using High Availability

HA	“To Edit the Policy” on page 192
	“To Install the SunScreen software in an HA Configuration” on page 193
	“To Install HA on the Secondary HA Screen” on page 194
	“To Define the HA Interface” on page 199
	“To Define the Screen Object for the HA Primary Screen” on page 201
	“To Initialize HA on the Primary HA Screen” on page 203
	“To Add the Secondary HA Screen to the Primary HA Screen” on page 203
	“To Allow Non-Administrative Traffic on an HA Network” on page 205

Setting Up High Availability

To use high availability, (you must install SunScreen as an HA system, as described in the *SunScreen Installation Guide*. High availability, its limitations, topology, set up, and capability are described in detail in "High Availability" in *SunScreen 3.2 Administrator's Overview*. For examples of HA configuration, see *SunScreen 3.2 Configuration Examples* manual.

Note – The network used for HA traffic must be kept physically secure because all secret keys and configurations are transmitted *in the clear* over the HA interface.

HA lets you deploy multiple Screens in situations where the connection between a protected inside network and an unprotected outside network is critical. One member of the HA cluster, the active HA Screen, performs packet filtering, network address translation, logging, and encryption/decryption of packets travelling between the inside and outside networks. The other members of the HA cluster, which can be as many as 31 passive HA Screens, receive the same packets, perform the same calculations, and mirror the configuration of the active HA Screen, but they do not forward traffic between the inside network and the outside network. If the active HA Screen fails, one of the passive HA Screens takes over (failover) as the active HA Screen and begins routing and filtering network traffic within seconds. Because the passive HA Screens mirror the active HA Screen, few connections are lost if a failover occurs.

The routing interfaces of all the systems in the HA cluster have the same interface names with the same IP addresses. When a firewall becomes a secondary Screen, the MAC address of each routing interface is changed so that it is the same as the MAC address of the same interface on the primary Screen. Each HA Screen, therefore, receives the same traffic, ensuring that passive Screens can duplicate the state of the packet filter engine should the active Screen fail. The secondary firewalls have the same rules and process the packets in the same way.

Note – Both Screens mirror configuration. They attempt to mirror state by independently building the same state table, since they see the same traffic. They do not exchange information about what is in each others' state tables, however. That means that if one Screen is rebooted, it will have the same rules, configuration, MAC addresses, etc., but will not have the same state in memory. This Screen will never learn old information from the other Screen; it will only be able to learn new information from listening on the wire. The internal state as far as memory and state tables are concerned will be out of sync for some undetermined amount of time, until all the old state entries time out or are closed from the other Screen.

HA Policy

When you set up an HA cluster, you designate one Screen as the primary HA Screen, and you configure it with the common objects and policy rules that the HA cluster will use. When you activate the policy, it is copied from the primary HA Screen to the other members of the HA cluster. The Solaris system and network configuration are not copied from the primary HA Screen; they must be identical on all the Screens in the HA cluster.



Caution – Be sure to keep the HA network physically secure. The HA cluster transmits secret keys and policies in the clear over the dedicated HA network.

The interfaces for network connections must be the same for each HA cluster member. For example, if one HA host uses the `le0` interface as its dedicated internal network connection, all HA hosts must use the `le0` network interface as their dedicated internal network connections. Similarly, all Screens in the HA cluster must use the same IP address on their non-dedicated interfaces.

Preparing to Install High Availability

HA is designed to maintain the great majority of network connections. During a reboot (an orderly shutdown), the active Screen being rebooted notifies the passive Screens, and the appropriate passive Screen takes over as the active Screen without loss of connections. Because the passive Screens do not forward, reject, or log packets, the load on passive Screens is less than the load on the active Screen. Consequently, load-induced faults that affect the active Screen are unlikely to have affected the passive Screens. Once the previously-passive secondary Screen becomes active, of course, it is subject to the same load that caused the failure.

The machines that are used as the HA Screen should all be of equivalent power, so that the passive HA Screen can keep up with nearly all the processing of the active HA Screen.

No traffic is allowed out of the passive HA Screens with the exception of administration traffic, such as normal GUI administration, HA administration, and HA heartbeat (the communication signal on the dedicated network that assures that the network is working). This means, for example, that you cannot use `telnet` to connect to the passive HA hosts. You can, however, use `telnet` to connect to active HA hosts.

Using the `/etc/hosts` File for Name Resolution

When you configure the hostname resolution in the `/etc/nsswitch.conf` file for HA hosts, the key word *files* must appear first in the “hosts line” because:

- Using the `/etc/hosts` file for hostname resolution is more reliable than using DNS or NIS or both.
- An HA Screen in the passive mode cannot send packets over the network; therefore, remote hostname resolution, such as DNS or NIS, will fail for passive HA Screens.

Defining HA

The *primary* HA Screen manages *secondary* HA Screens in an HA cluster. A *passive* HA Screen within an HA cluster mirrors the state of the *active* Screen, which can be the primary or a secondary HA Screen. When the active Screen fails, the passive Screen that has been running the longest takes over as the active Screen. Primary means the system is the *HA administration host* for the HA configuration. It does not necessarily mean that the system is the active host

You must use the unique HA interface address for administration. If you use one of the shared addresses, then that address will always resolve to the HA Screen that is currently active. Because the active host is not necessarily the primary administration host, you must use the unique HA interface address to ensure that you are communicating with the correct host.

If you do not use the unique HA interface address, then the connection will be lost and the administration GUI will hang immediately if the remotely administered primary HA Screen is shut down. You will still be able to administer the active HA Screen from the command line, using the command `ssadm`, but you will be unaware that you are administering a secondary HA Screen. This will not propagate the configuration to any other HA Screen; instead, the configuration will be overwritten when the primary HA Screen comes up again and a policy is activated.

Modifying the HA Service Group

You cannot connect directly to a passive HA Screen, nor can you connect from one HA Screen to another, except with remote administration to the HA interface. You can allow:

- Services and service groups other than the standard HA services
- Remote administration
- Router discover
- Heartbeat (the communication between or among HA Screens to assure that the dedicated HA network is working)

Adding additional services or service groups may be useful; for example, if you need to copy Solaris system files between the HA hosts or to be able to log into the active HA Screen remotely and then connect to the primary administration HA host with telnet. Adding a service to the HA service group circumvents the passive HA mode and allows the traffic that the added service permits through the SunScreen filters.

You can add any services to the HA service group by selecting Service in the Type list on the Edit Policy page, saving the change, and reactivating the configuration.

Note – The services or service groups that you add to the HA service group are allowed only between the HA hosts.

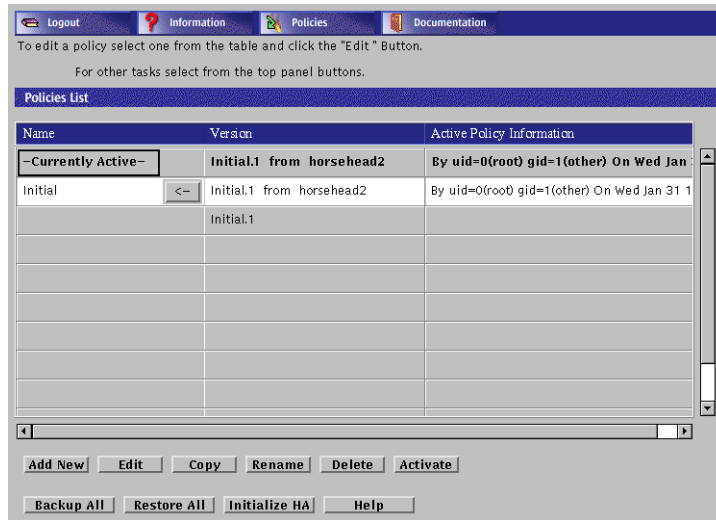
Using NAT With HA in Routing Mode

Depending on the configuration you use for NAT, you must add an ARP (Address Resolution Protocol) entry for static NAT mappings on all Screens in routing mode, active and passive, so that NAT can continue to work after a failover. You must replicate all non-SunScreen configurations, including static ARP entries, on all HA Screens. Because you must do this every time an HA Screen fails over or every time you reboot a Screen, you may want to automate this in one of your start-up scripts. For more information on configuring NAT, see “Network Address Translation” in *SunScreen 3.2 Administrator’s Overview*. For more information on ARP, see the man page for `arp(1M)`.

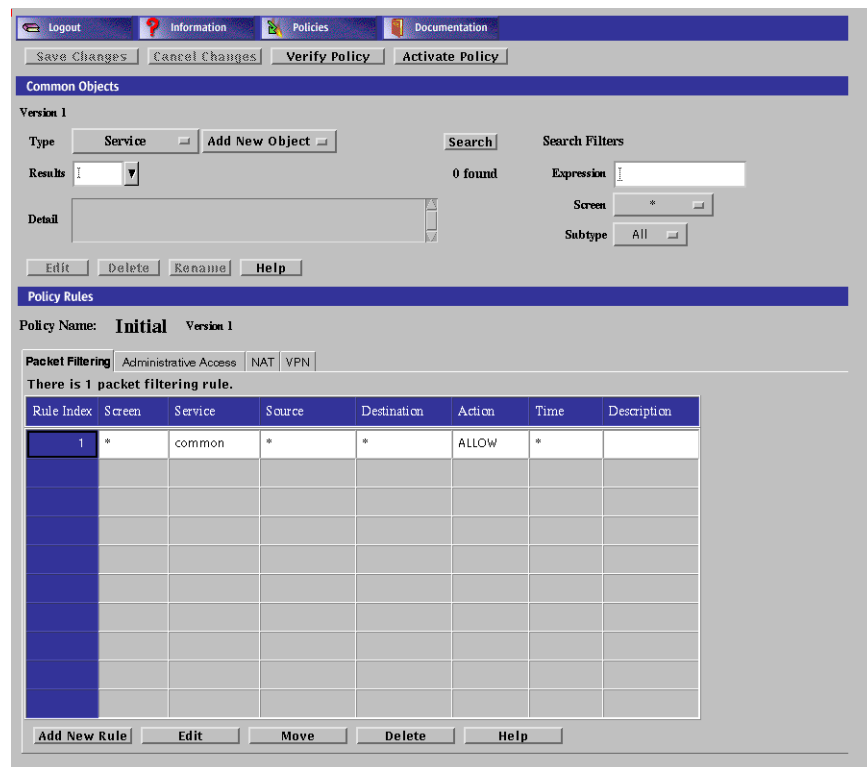
Installing High Availability

▼ To Edit the Policy

1. Choose a policy in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.



▼ To Install the SunScreen software in an HA Configuration

1. **Configure identical interfaces on all HA machines, by editing the `/etc/hostname.interface-name` file or running the `ifconfig` command.**
2. **Dedicate one interface on each machine to HA.**
 - You must have a dedicated network between the HA hosts that, for reasons of security, is not connected to any other network.
 - All the HA machines must be configured with the same interface names and be connected to the network and to each other in the same way.
 - The dedicated HA interface must have a unique address name and IP address (so that the configurations, including interface configurations, can be synchronized later).

3. **Connect the HA interfaces of the HA machines one at a time after installing the operating system (if necessary) and configuring the routing on these machines.**
 Since the HA hosts have the same names and IP addresses, you must connect the non-HA interfaces of *only one* of the HA machines (for example, HA1, as shown by the solid line in Figure 5–1). This machine will become the *primary* and *active* HA Screen. This approach prevents confusion from arising in the routing and ARP tables on the active HA Screen. After the HA configuration is complete, the HA software keeps the routing and ARP tables orderly.
4. **Connect the secondary Screen, for example, HA2 (as shown by the broken line in Figure 5–1) to the hubs.**
 You do not have to install any special software for HA other than SunScreen. The HA software is automatically installed as part of SunScreen.

Note – Do not perform this step until you have installed, configured, and tested the both the primary (active) and secondary HA Screens.

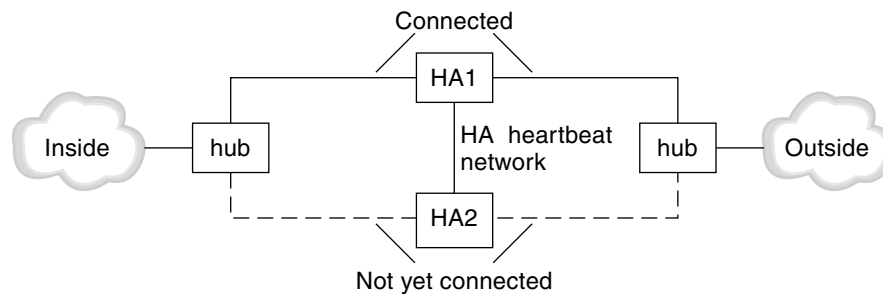


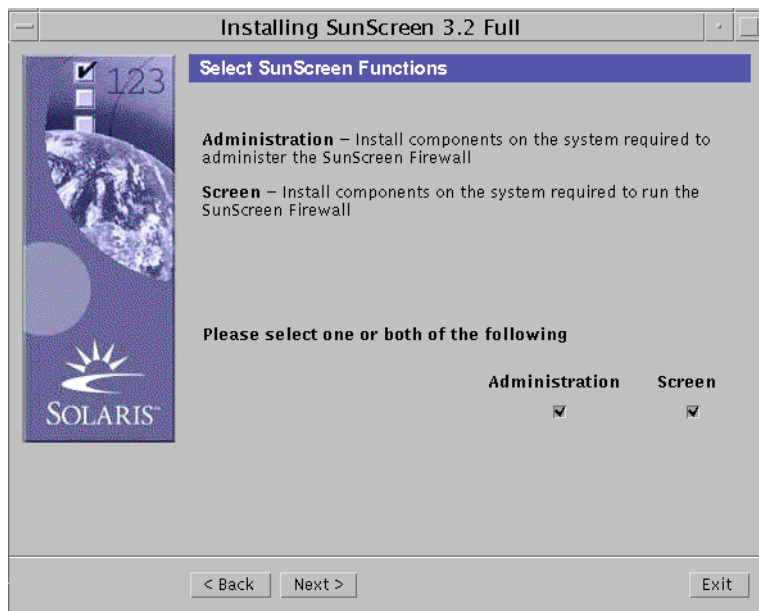
FIGURE 5-1 Wiring Before and During HA Configuration

▼ To Install HA on the Secondary HA Screen

1. **Start the full SunScreen install on the secondary HA Screen.**
2. **Select the “Custom” option on the Select Type of Install panel and click the Next button.**



3. Select which Sunscreen function you want to install



4. Click Next

The Component Selection Dialog appears.

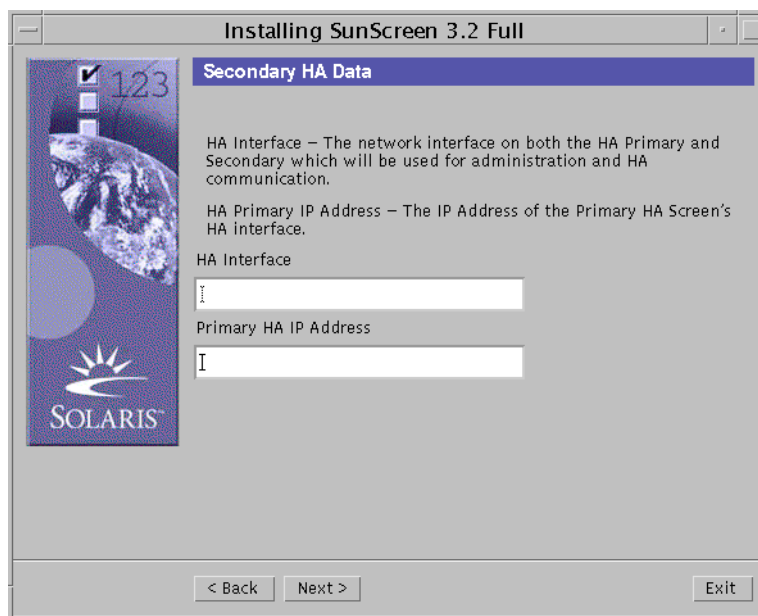


5. Select the components to be installed and click Next.

The Secondary HA Designation dialog appears.



6. **Select Yes and click the Next button.**
The secondary HA data dialog box appears.
7. **In the secondary HA Data dialog box:**



- a. Fill in the HA Interface field.
 - b. Fill in the secondary HA IP Address field.
8. Click the Next button.
 9. Reboot the secondary HA Screen when the final panel appears.



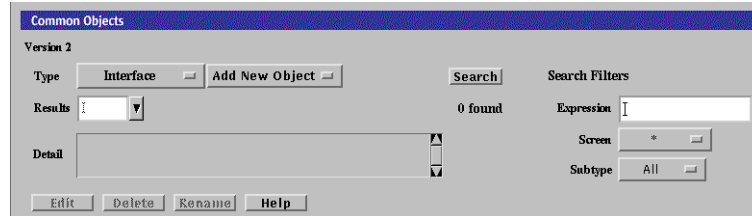
Note – You should ignore the plumbing error message on the stealth/routing interfaces during bootup. Once the HA configuration is pushed over from the primary, this error is eliminated.

▼ To Define the HA Interface

The dedicated HA interface can be any interface on the Screen that has been plumbed and is not defined as a screening interface. To define an HA interface, perform the following steps:

1. Execute the steps in “To Edit the Policy” on page 192.

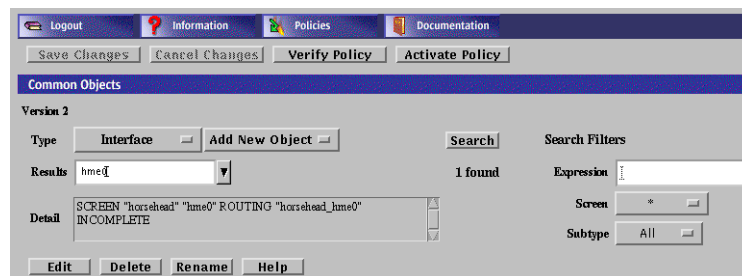
2. Select Interface from the Type list.



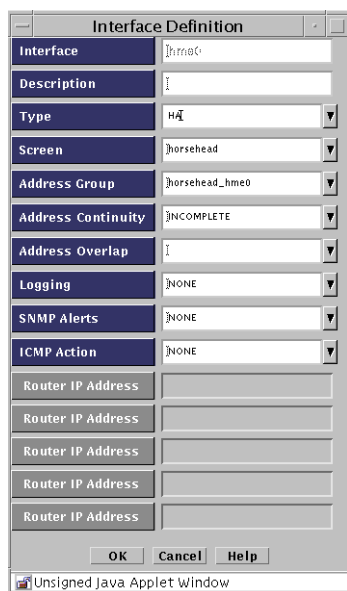
3. Click the Search button.

4. Select the interface name that you want to dedicate to HA and click Edit.

If the interface does not appear, select New from the Add New list.



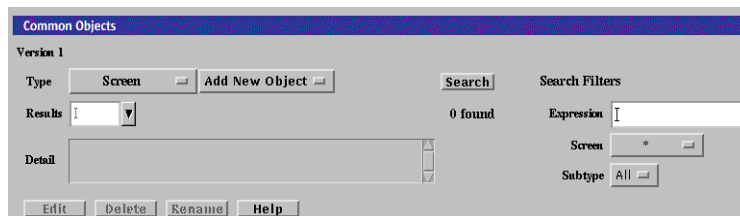
5. Define the interface, selecting HA as the Type.



6. Click the OK button.

▼ To Define the Screen Object for the HA Primary Screen

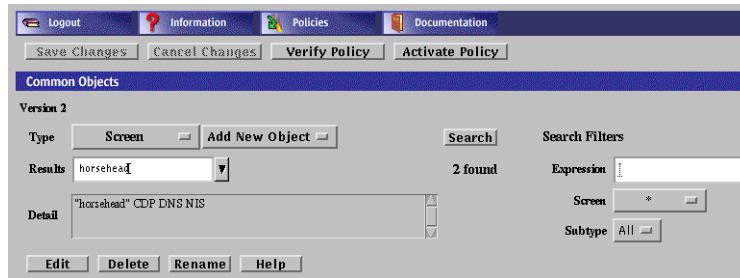
1. Execute the steps in "To Edit the Policy" on page 192.
2. Select Screen in the Type list.



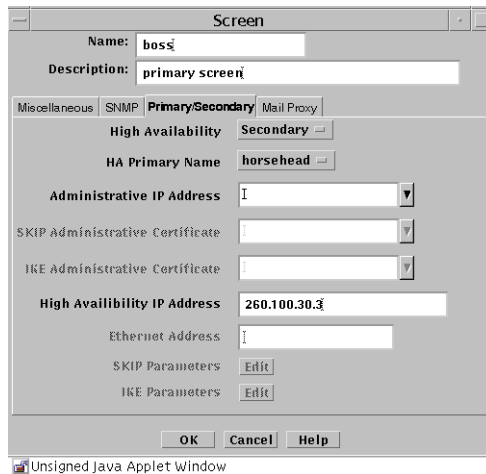
3. Click the Search button.

4. Select the name of the Screen that you want to use as the primary HA Screen, then click the Edit button.

If the Screen object is not yet defined for the primary Screen, select New from the Add New list and type the name of the primary Screen in the Name field.



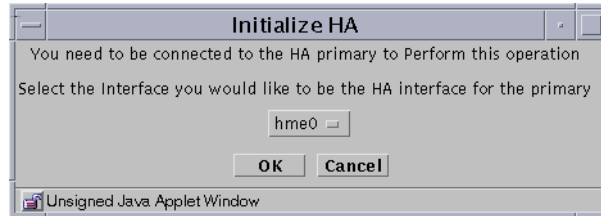
5. Click the Primary/Secondary tab.
6. Select Primary in the High Availability field.



7. Type the IP address of the primary Screen's dedicated HA interface in the High Availability IP Address field.
8. Type the Ethernet address of the interface on the primary Screen in the Ethernet Address field.
9. Click the OK button.

▼ To Initialize HA on the Primary HA Screen

1. Execute the steps in “To Edit the Policy” on page 192.
2. In the Policies List page, click on Initialize HA.
The Initialize HA dialog box appears.



3. Select the interface to be the HA interface from the Interface list.

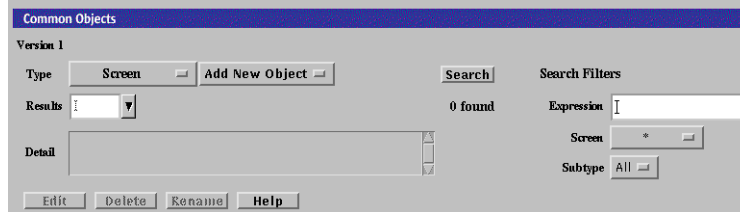
Note – The HA interface on the primary HA Screen and secondary HA Screen must be the same.

4. Click the OK button
The Policies List page appears.

▼ To Add the Secondary HA Screen to the Primary HA Screen

1. Execute the steps in “To Edit the Policy” on page 192.

2. Select Screen from the Type list.

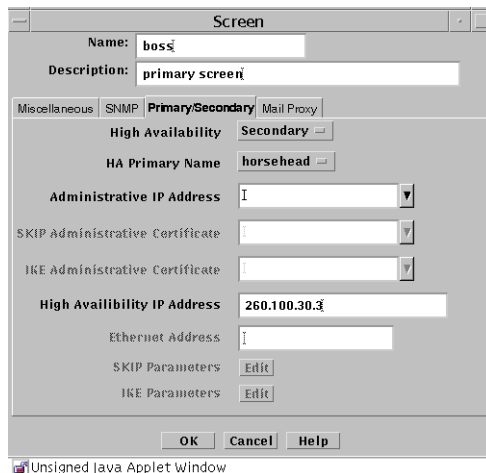


3. Select New from the Add New Object list.

The Screen dialog box appears.

4. Type the name of the secondary HA Screen in the Name field.

5. Click the Primary/Secondary tab in the Screen dialog box.

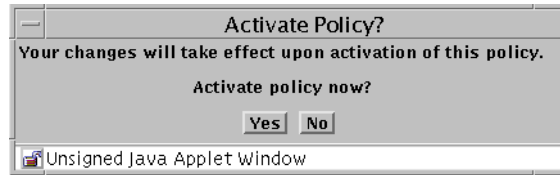


6. Set the following values in the Primary/Secondary area of the Screen dialog box:

High Availability	Secondary
Primary Name	Name of primary Screen
Administrative IP Address	Leave blank
High Availability IP Address	Secondary Screen IP address

7. Click the OK button.

8. Click the **Save Changes** button on the **Policies List** page.
The **Activate Policy** dialog box appears.



9. Click **Yes**.
10. Fully connect the secondary HA Screen to the network.

After adding an HA secondary Screen and activating your policy, the new secondary Screen may become active. If it does, you must direct the secondary Screen to become passive before you can perform additional administration on the primary Screen.

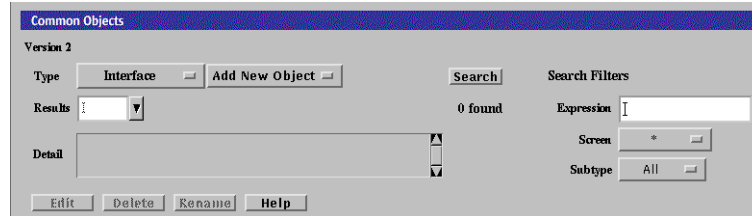
Note – Make sure all wires and cables are connected properly.

11. Configure the service and policy rules on the primary HA Screen.
All changes made on the primary HA Screen are automatically copied to all secondary HA Screens.
12. Save and activate the policy.

▼ To Allow Non-Administrative Traffic on an HA Network

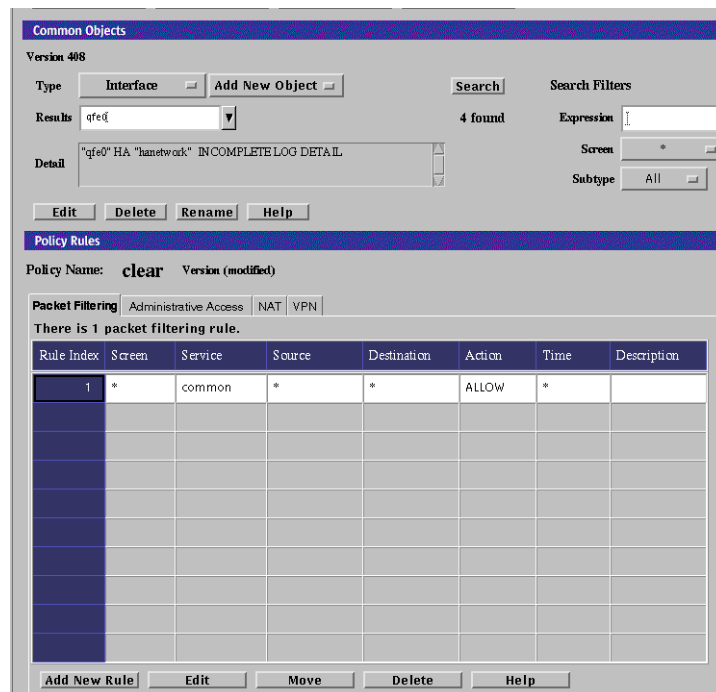
1. Execute the steps in “To Edit the Policy” on page 192.

2. Select Interface from the type list.



3. Click the Search button.

4. Select the interface name.



5. Click the Edit button.

Interface	Interface
Description	
Type	HA
Screen	
Valid Addresses	anetwork
Spoof Protection	INCOMPLETE
Address Overlap	
Logging	DETAIL
SNMP Alerts	NONE
ICMP Action	NONE
Router IP Address	
Router IP Address	
Router IP Address	
Router IP Address	
Router IP Address	

OK Cancel Help

Unsigned Java Applet Window

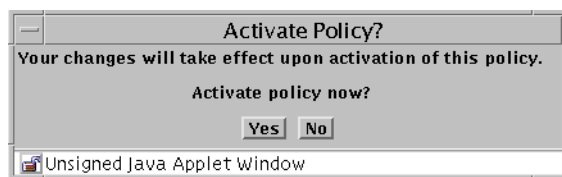
6. Note the name in the Valid Address field for later use as the Destination Address for the new rule to be defined.
7. Click the Cancel button to close the Interface Definition panel.
8. Click the Add New Rule button.
9. Fill in the fields. Make sure you set the Destination Address to the same name that was in the Valid Address field in step 6 above.



10. Click OK.

11. Click Save Changes.

The Activate Policy dialog box appears.



12. Click Yes to activate the policy.

Configuring Policies for an HA Cluster

You configure the HA cluster just as you configure a single Screen. Policy rules for passive HA Screens are configured when they connect to the primary HA Screen. You should write a rule for connecting to the unique address of each host in the HA service group.

Updates to the primary HA Screen are automatically relayed to all the other HA Screens. This synchronization takes place during activation. When a configuration is activated, the primary HA Screen transfers the configuration—including certificates, local keys, addresses, and policy rules—to all other secondary HA Screens.

When an HA host is in the passive mode, you cannot connect to that host directly, except with remote administration to the HA interface. This also applies to connections from one HA host to another on the HA interface.

You can allow services other than the standard HA service or remote administration and heartbeat. These services will only be allowed between the HA hosts. Add them to the HA service group by selecting Service in the Type list on the Edit Policy page, and add the services you want to include.

Removing HA

Removing HA involves removing both software and hardware. Simply disabling the HA configuration is insufficient and is only one part of the process. Because there is more than one Screen that has the same IP address on the network, simply disabling HA would leave two or more HA Screens on the network that are trying to route the same traffic, which would disrupt the network traffic through the Screens.

Remove the HA hosts one at a time to reduce the chances of disrupting the network. Remove the passive HA host or hosts first to avoid losing connections.

If you must remove the active HA host, use the following command on both the active HA host that you want to remove and on the passive HA host that will become the active HA host. This will help you to find out whether any connections will be lost.

- For local administration:

```
# ssadm lib/statetables
```

- For remote administration:

```
# ssadm -r Screen_Name lib/statetables
```

If the state tables are in an acceptable level of synchronization, you can proceed to remove the active HA host.

HA Logging

Information about the HA Screen is not shown as such in the Log Browser.

If you want to see the changes in state, be sure that `/etc/syslog.conf` contains the following lines:

```
*.err;kern.notice;auth.notice;user.none;daemon.info    /dev/console
*.err;kern.debug;daemon.info;mail.crit;user.none       /var/adm/messages
```

Note – Some HA messages are now sent to syslog and some sent to regular log.

Setting Up and Using Proxies

A proxy is a user-level application that runs on the Screen. The main purpose of proxies is to provide content filtering, as opposed to packet filtering. For example, you can use proxies to allow or deny access to Java applets through the firewall. Proxies can also provide user authentication, as in the case of `telnet` traffic. See *SunScreen 3.2 Configuration Examples* manual for an example using Proxies.

Note – There is no way for SunScreen High Availability systems to share the proxy state. Proxies do not work with SunScreen High Availability.

The following table shows the procedures in this chapter.

TABLE 6-1 Proxy Procedures

Proxy Users	“To Add a Single Proxy User” on page 215
	“To Add a Proxy User Group” on page 217
	“To Add Spam Domains” on page 218
	“To Delete Spam Domains” on page 221
Policy Rules	“To Write Policy Rules for the Proxies” on page 227
	“To Define PROXY_FTP” on page 228
	“To Define PROXY_HTTP” on page 230
	“To Define PROXY_SMTP” on page 231
	“To Define PROXY_Telnet” on page 232
FTP Proxy	“To Use the FTP Proxy” on page 233
Telnet Proxy	“To Use the Telnet Proxy” on page 235
SMTP Proxy	“To Use the SMTP Proxy” on page 236

TABLE 6-1 Proxy Procedures (Continued)

HTTP proxy	"To Configure the Browser to Use the HTTP Proxy" on page 237
-------------------	--

Matching Proxy Rules

Each proxy is an independent program that reads its own policy file. The file for each proxy consists of policy rules selected by the compiler. Rules may in turn reference data in the user database.

Each proxy follows a sequence of tests to determine whether a rule matches:

1. Does the source address of the packet fall within the source-address range in the policy rule?
2. Is the destination address of the final connection (the host that the user specifies) in the destination address in the policy rule?
3. If the policy rule requires user authentication, did the user authenticate correctly? Is that user enabled?
4. Is this (possibly anonymous) authenticated user included in the policy rule, either directly or by group membership?

Preparing to Use Proxies

SunScreen includes four proxies: FTP, HTTP, SMTP, and TELNET.

Each one is a completely separate user-level application, although they use some shared data and policy files for authentication. Certain proxies provide some content filtering or user authentication or both. They allow or deny sessions based on the source and destination addresses.

The `rc proxy` script is used to start up the proxies as needed. It is located in `/etc/init.d` and the symbolic link to `/etc/rc2.d/S79proxy`. The script verifies that:

- The proxy executable is in `/usr/lib/sunscreen/proxies`.
- The corresponding policy file is in `/etc/sunscreen/proxies`.
- The policy file has a size larger than zero.

If these requirements are not met, the proxy will not start.

The policy rule compiler uses this script to cause each proxy to reread its policy file as needed.

Note – You must disable the corresponding standard network service (if any) for HTTP proxies to function. If you have installed an HTTP daemon, you must disable it before the HTTP proxy will work. Conflicting standard Solaris servers for telnet, FTP, and SMTP are handled automatically during policy activation. See the *SunScreen 3.2 Administrator's Overview* for further details.

Defining Proxy Data

You define proxy data on the Policy Rules page. The databases for proxies are the Java archive (Jar) Signatures, Jar hashes, the Proxy Users, and SMTP Proxy data.

Setting Up Proxy Users

Proxy users are used in FTP, HTTP (if desired), and Telnet proxy rules. The proxy users database depends on information in the authorized users database. To take full advantage of the user authentication feature of the FTP, HTTP, and Telnet proxies, you must create entries for both authorized users and proxy users. Define a user as an Authorized User before defining that user as a Proxy user. See “Authentication” on page 121 for the procedure for setting up an Authorized user and “Authentication” in *SunScreen 3.2 Administrator's Overview* for information on the proxy database and the authorized user database.

Note – Define all necessary authorized users before attempting to define proxy users.

Note – You can define authorized and proxy user objects with identical names. Choose a naming strategy for each set that reflects naming systems already in use. For example, you might choose to name authorized users by employee identities, such as surname or employee number, and proxy users by their login names.

The proxy user database contains the mapping information for users of SunScreen proxies. FTP, HTTP, and Telnet rules reference the proxy user entries. Additionally, a

user connecting through either of these proxies will often be configured to require authentication by using an authorized user identity. Users logging in with a Telnet proxy are authenticated through the authorized user identity.

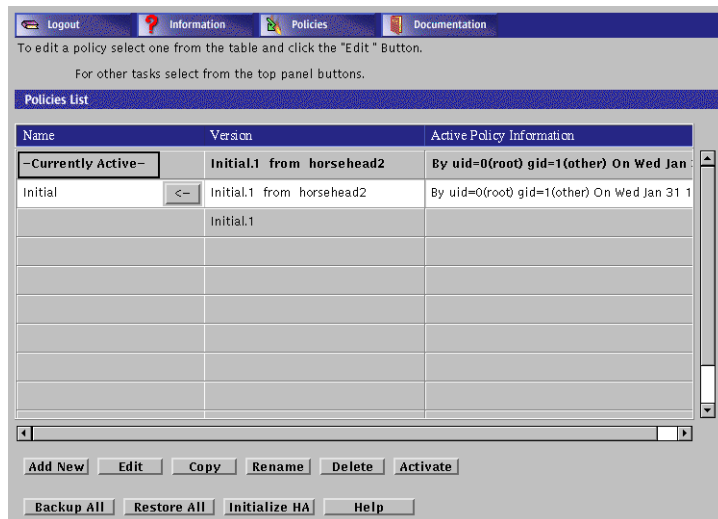
You can also use external authentication mechanisms, such as RADIUS or SecurID, to enable user authentication by using *special* proxy user entries, which create a translation.

By referencing these *special* mechanisms directly in rules, or by adding references to other proxy user groups, you can allow users authenticated by those mechanisms to behave as authenticated users in the referenced contexts.

Names of proxy users must not contain the following characters: !, @, #, \$, %, ^, &, *, {, }, [,], <, >, ", \, \, or ?, nor may they contain a NULL character.

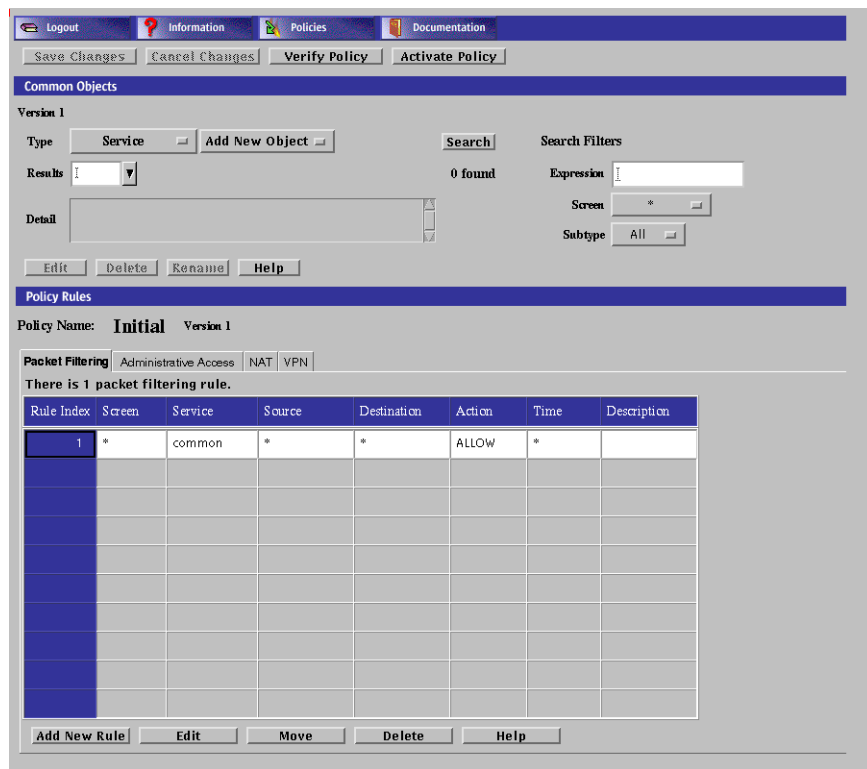
▼ To Set up Basic Proxy Users

1. Choose a policy in the Policies List page.



2. Click the Edit button.

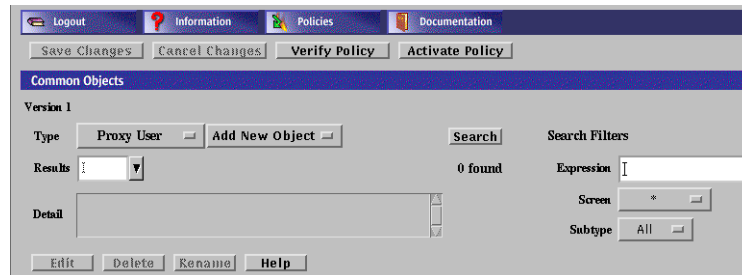
The Policy Rules page appears.



▼ To Add a Single Proxy User

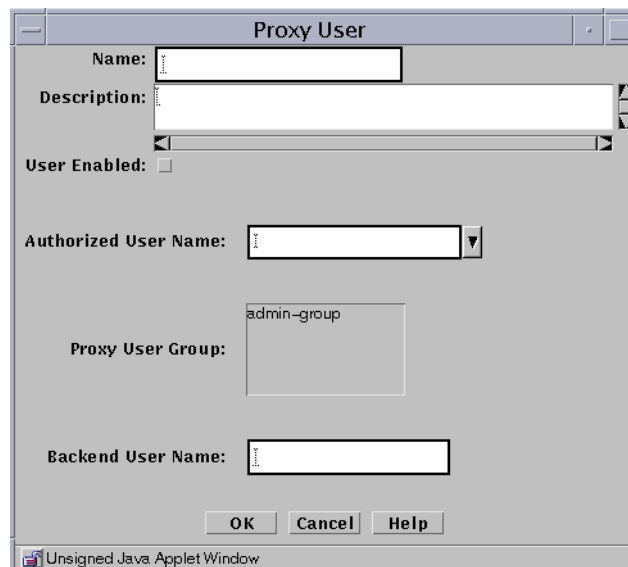
1. Execute the steps in "To Set up Basic Proxy Users" on page 214.

2. Select Proxy User from the Type list.



3. Select New Single from the Add New button.

The Proxy User dialog box is displayed.



4. Type a name for this Proxy User in the Name field.

5. (Optional) Type a description in the Description field.

6. Select the User Enabled check box. The default is disabled,
If this box is not selected, the proxy user remains inactive and cannot use the proxies.

7. Select the name of the authorized user that you want to place in the Authorized User Name field.

8. (Optional) Select the name or names of the user group or groups with which you want to associate this proxy user.
9. Type the name that the proxy user should use when connecting to the target server (which is also known as the “backend” server) in the Backend User Name field.
This name will be the identity that the proxy user assumes on any target server connected through this proxy user.

Note – Only the FTP proxy sends the backend user name to the destination host. Telnet and HTTP do not send the backend user information.

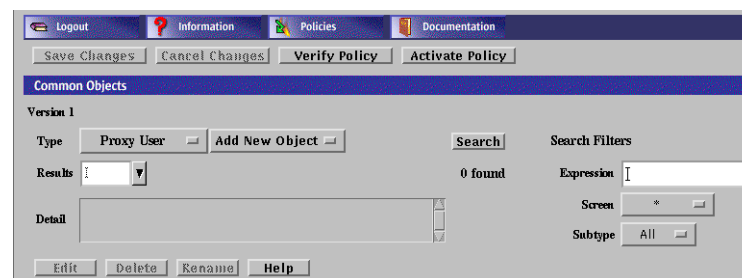
10. Click the OK button.
11. Repeat the above steps until you have added all the proxy users.

All changes are saved immediately. Changes are only put into effect upon policy activation.

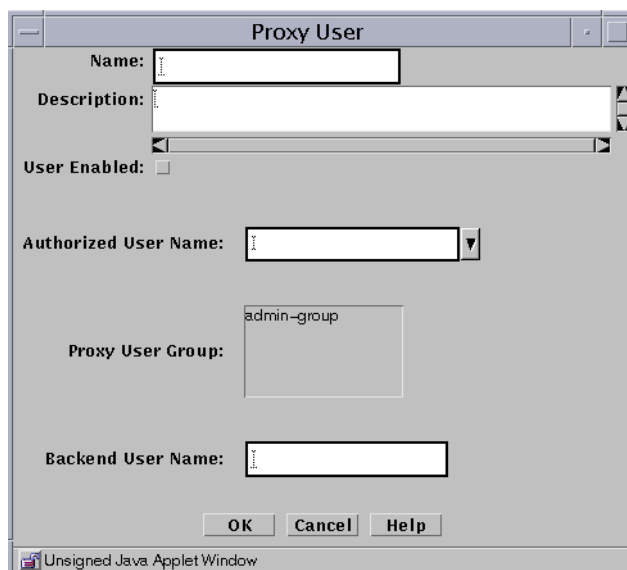
▼ To Add a Proxy User Group

You can place proxy users in logical groups for convenience; then you can use a group name instead of single names in a policy rule.

1. Execute the steps in “To Set up Basic Proxy Users” on page 214.
2. Select Proxy User from the Type list.



3. Select New Group from the Add New list.
The Proxy User dialog box appears.



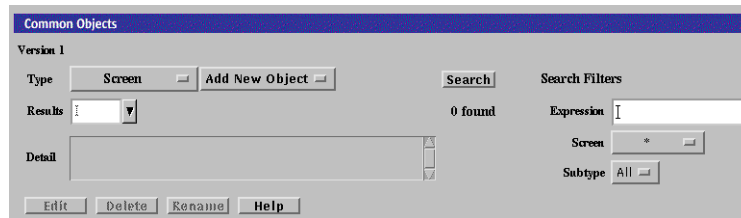
4. Type the name for this group of proxy users in the Name field.
5. (Optional) Type a short description of this definition in the Description field.
6. Select the User Enabled check box to enable the user group.
7. Use the Add or Remove buttons to move selected proxy users or groups of proxy users into or out of the list of Member Users.
8. Add all the proxy users and groups of proxy users that you wish to include in your definition.
9. Click the OK button.
10. Repeat the above steps until you have defined all the groups of users required.

▼ To Add Spam Domains

You can define the domains from which you think that you receive spam mail.

Note – For more information on spam control, see “SMTP Proxy” in *SunScreen 3.2 Administrator’s Overview*.

1. Execute the steps in “To Set up Basic Proxy Users” on page 214.
2. Select Screen from the Type list.



3. Select New from the Add New list.
The Screen dialog box appears.

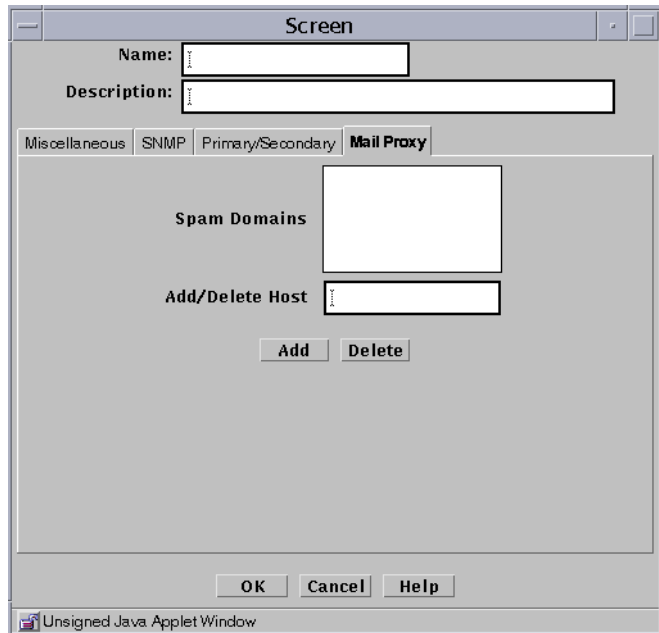


4. Type a name in the Name field.

5. (Optional) Type a brief description in the Description field.

6. Click the Mail Proxy tab.

The Spam Domain list appears.



7. Type the name you want to add to the Spam Domain list into the Add/Delete Host field.

8. Click the Add button.

9. Click the OK button.

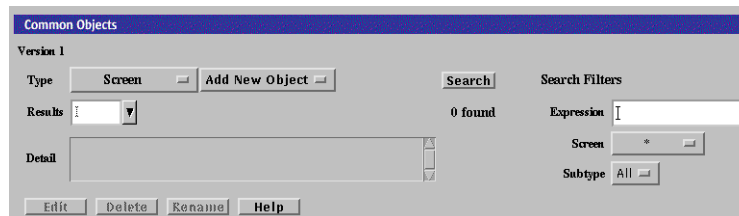
10. Repeat these steps until you have added all the domains from which you receive Spam mail.

11. Click the Save Changes button

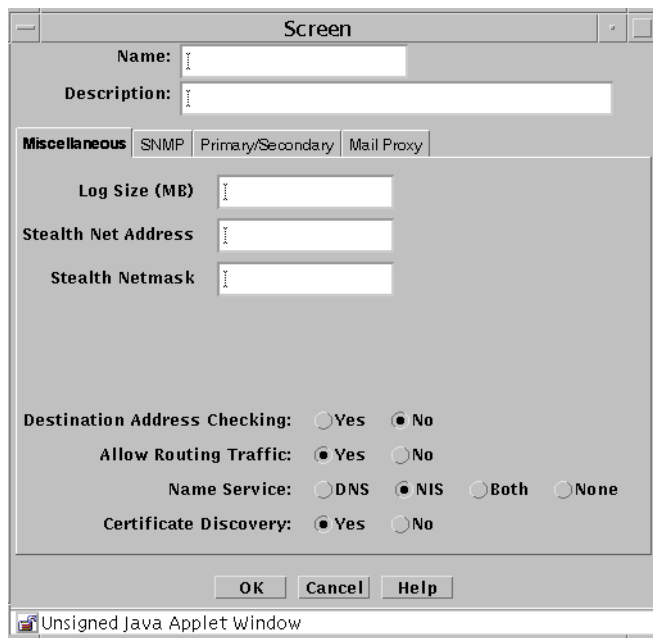
▼ To Delete Spam Domains

Note – For more information on spam control, see “SMTP Proxy” in *SunScreen 3.2 Administrator’s Overview*.

1. Execute the steps in “To Set up Basic Proxy Users” on page 214.
2. Select Screen from the Type list.

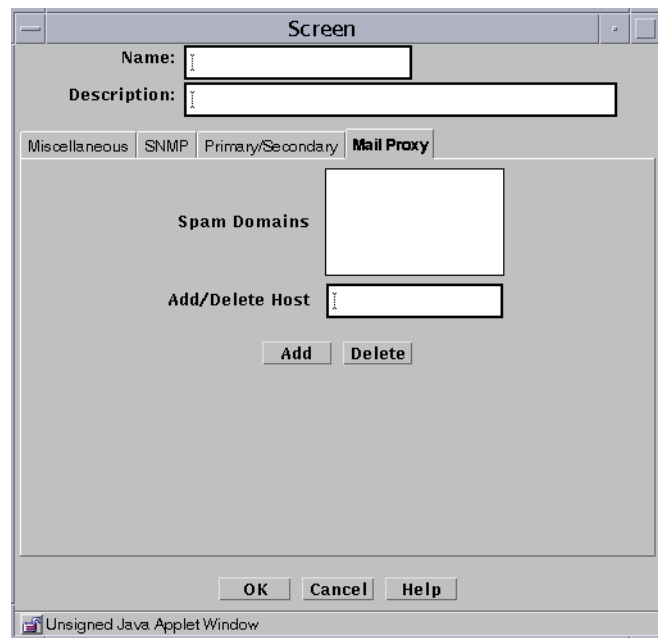


3. Click the Search button.
4. Select the Spam domain from the Results field.
5. Click the Edit button.
The Screen dialog box appears.



6. Click the Mail Proxy tab.

The Mail Proxy Screen appears



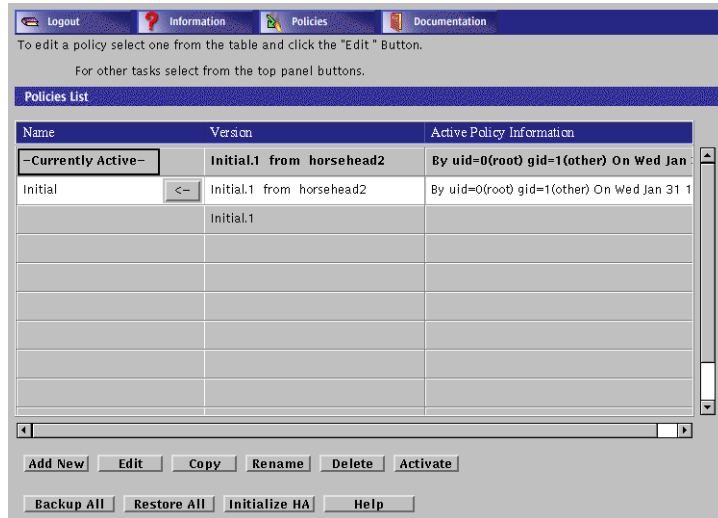
7. Select the Spam domain to be deleted in the Spam Domains field.
8. Click the Delete button.
9. Click the OK button.
10. Click the Save Changes button.

Writing and Editing Policy Rules for Proxies

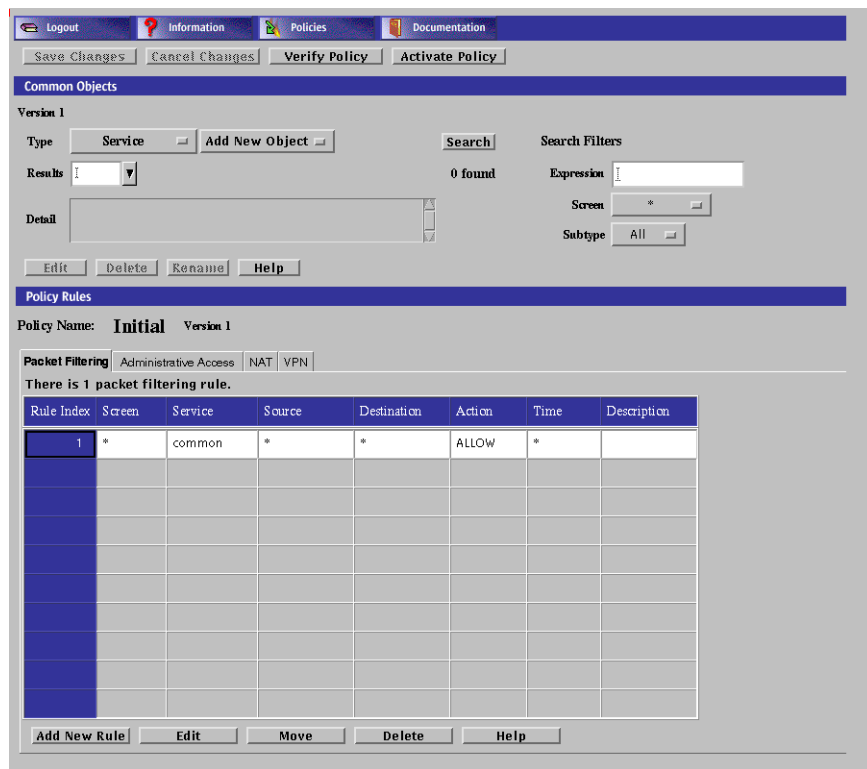
Policy Rules are strictly ordered; they take effect in the order in which they are listed. You may either define policy rules in the order in which you want them to take effect or rearrange them after they are defined.

▼ Basic Steps for Writing Policy Rules for Proxies

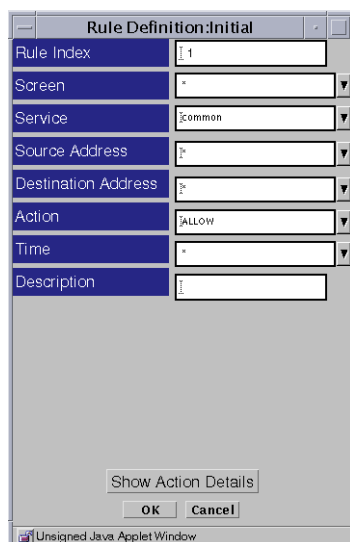
1. Choose the policy Initial in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.



3. Select the Packet Filtering tab in the Policy Rules area.
Proxies are defined in the Packet Filtering page.
4. Click the Add New Rule button in the Packet Filtering area.
The Rule Definition dialog box for that policy is displayed.



In the Rule Definition dialog box, the Rule Index field is filled with the next available rule index.

5. (Optional) If a rule is valid only for a particular Screen, select that Screen only in the Common Objects area.

The default is for the rule to be valid for all Screens.

6. In the Services box in the panel, select one of the services that is valid for proxies, for example:

- ftp
- www
- smtp
- telnet

7. Select the source and destination address that you want for the Source and Destination Address fields.

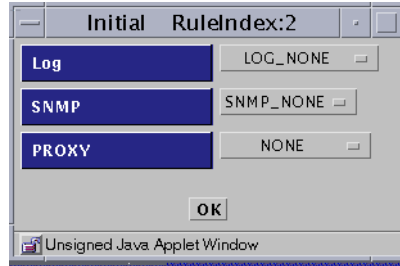
Be sure you have defined these addresses on the Policy Rules page.

8. For a proxy rule, select ALLOW or DENY in the Action field.

These are the only valid actions for proxies. The **Encrypt** or **VPN** action to not apply to proxies.

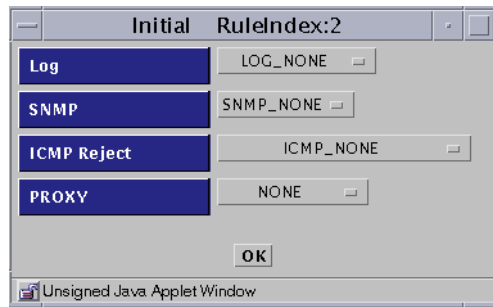
- LOG
- SNMP
- PROXY

When you select **ALLOW**, a new dialog box appears:



When you select **DENY**, a new dialog box appears:

- LOG
- SNMP
- ICMP Reject
- PROXY



▼ To Write Policy Rules for the Proxies

1. Execute the steps in "Basic Steps for Writing Policy Rules for Proxies" on page 224.
2. From the Proxy list, select the information that you want to put into the LOG and SNMP fields.

There are five items in the Proxy list:

- NONE
- PROXY_HTTP
- PROXY_FTP
- PROXY_SMTP
- PROXY_Telnet

3. Select the name of the proxy service for which you are writing this policy rule for the **Service** field.

If you plan to use proxies, you must select the appropriate proxy service:

TABLE 6-2 Proxies and Services

Choose This Service	For This Proxy
ftp	PROXY_FTP
www	PROXY_HTTP
smtp	PROXY_SMTP
telnet	PROXY_TELNET

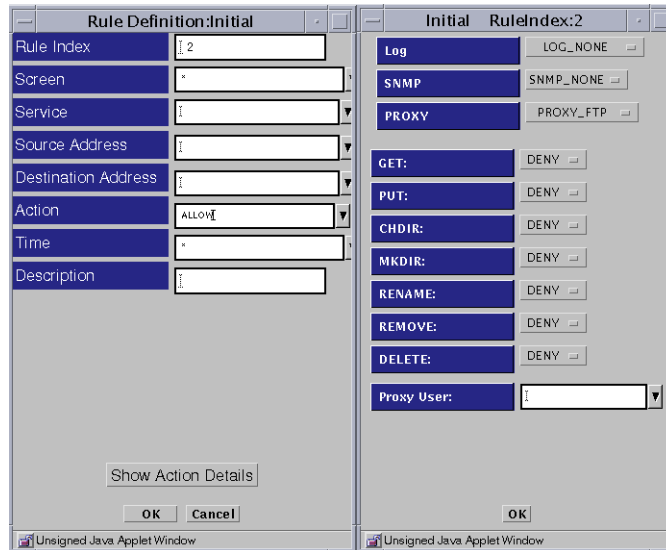
Each choice requires slightly different steps, which are listed below under the four proxy types.

▼ To Define PROXY_FTP

1. Execute the steps in “Basic Steps for Writing Policy Rules for Proxies” on page 224.

2. Select PROXY_FTP as the proxy

The Rule Definition Dialog Box for PROXY_FTP appears



3. Select PROXY_FTP from the Proxy list and eight fields appear below the Proxy field in the dialog box:

- GET
- PUT
- CHDIR
- MKDIR
- RENAME
- REMOVE
- DELETE
- Proxy User

4. Select an action for each field (GET, PUT, CHDIR, MKDIR, RENAME, REMOVE, and DELETE) or accept the default values. You can either allow (Allow) or disallow (Deny) use of these FTP commands based on the settings you choose.

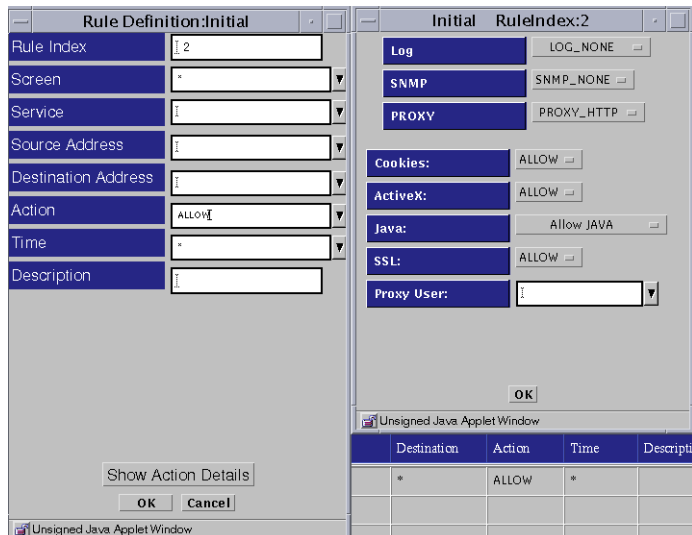
5. Select the name of a defined proxy user in the PROXY USERS field.

6. Click the OK button in the dialog box.

7. Click the Save Changes button.

▼ To Define PROXY_HTTP

1. Execute the steps in “Basic Steps for Writing Policy Rules for Proxies” on page 224.
2. Select PROXY_HTTP as the proxy, click that name to put it into the Proxy field.



Five fields then appear below the Proxy field:

- Cookies
- ActiveX
- Java
- SSL
- Proxy User

3. Set the action for each item.
 - a. For Cookies, ActiveX, and SSL, choose an action or accept the default under Proxy Details. You can either allow (Allow) or disallow (Deny) the use of cookies, ActiveX, or SSL based on the settings you choose for each field.
 - b. For the Java field, choose among the following under Proxy Details:
 - Allow all Java
 - Block all Java
 - Allow Java with signed Jars, with the signature in the Jar Signature database
 - Allow Java, with the Jar hash in the Jar Hash database
 - Allow both signed Jar signature and Jar Hash

Note – If you select Jar Signature or Jar Hash, they must be defined in the Common Objects area of the Policy Rules page.

4. (Optionally) Select a proxy user or group to be allowed through the proxy.
5. Click the OK button in the dialog box.
6. Click the Save Changes button.

▼ To Define PROXY_SMTP

1. Execute the steps in “Basic Steps for Writing Policy Rules for Proxies” on page 224.
2. Select PROXY_SMTP as the proxy.
the Relay field appears below the Proxy field in the dialog box.

Note – For more information on relay control, see “SMTP Proxy” in *SunScreen 3.2 Administrator’s Overview*.

Destination	Action	Time	De
*	ALLOW	*	

3. Determine whether you want to allow relaying of mail messages through the proxy in the Proxy Details area.

4. If you want to allow all relaying, select the RELAY: ALLOW setting.
5. If you want to restrict the relaying, define the local domain name for the Screen *or* create a list of valid relay (domain) targets as described in the following 2 substeps and select the RELAY: RESTRICT setting.

- a. Define the Local Domain Name

Create or edit the `/etc/defaultdomain` file to contain the domain suffix for the Screen.

Note – For this default domain to become active, you must either shut down and reboot the Screen or run the following command:

```
# domainname `cat /etc/defaultdomain`
```

- b. Create a List of Valid Relay Targets

Use the `mail_relay` feature of the `ssadm` command to create a list of valid relay (domain) targets (see “SMTP Proxy” in *SunScreen 3.2 Administrator’s Overview*).

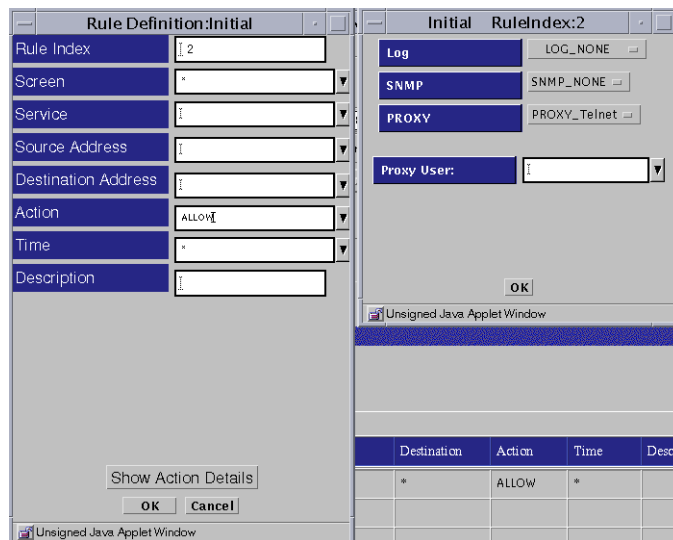
Note – The destination address in this rule should be the address of the SMTP server or servers that will spool and/or deliver email *after* it is restricted and filtered by the screen.

6. Click the OK button in the dialog box.
7. Click the Save Changes button.

▼ To Define PROXY_Telnet

1. Execute the steps in “Basic Steps for Writing Policy Rules for Proxies” on page 224.
2. Select PROXY_Telnet as the proxy.

The Proxy Users field appears below the Proxy field on the right side of the Rule Definition dialog box.



3. Select the proxy user or group that is allowed through the proxy.
4. Click the OK button in the dialog box.
5. Click the Save Changes button.

Using the FTP Proxy

To use the proxy and successfully make FTP connections through the Screen, you must FTP to the proxy on the Screen rather than directly to the end system. The Screen's policy rules will only allow FTP connections to and from the proxy.

For information on setting up the ftp proxy, see "To Define PROXY_FTP" on page 228.

▼ To Use the FTP Proxy

The following example steps show what happens when users wants to connect to the system named `ftp.sun.com`, which has an anonymous FTP account. To get there, they must first ftp to the SunScreen proxy named `Screen`.

Note – The anonymous proxy user is prefigured during the installation of the software. It is an unauthenticated proxy user, so any string provided before the first @ (“at” sign) in the password is ignored. The password after the first@ (here: zzz@thereisnohelp.com) is the backend user password—in this case, the user name, as is the custom for anonymous FTP.

1. Type the command:

```
% ftp screen
```

The following text appears:

```
Connected to screen
220-Proxy: SunScreen FTP Proxy Version 3.2
      : Username to be given as <proxy-user@<FTP-server-host>
      : Password to be given as <proxy-password@<FTP-server-password>
220 Ready
Name (screen:zzz):anonymous@ftp.sun.com
```

The format for the user name is the proxy user name and the destination server separated by an “at” sign.

2. Type your authorized user password at the prompt to authenticate you to this proxy:

```
331- Proxy: Authenticate & connect:
331 Password needed to authenticate 'anonymous'.
Password:
```

Note – The password is not echoed. Its format is two passwords separated by an “at” sign. The first password is the authorized user password for the proxy, and the second is the password for the destination ftp server. In the example, anonymous@zzz@thereisnohelp.com, anonymous is the password for the proxy and zzz@thereisnohelp.com is the email address that ftp.sun.com requires for anonymous ftp.

The following text appears:

```
230- Proxy:
      : Authentication mapped 'anonymous' to backend user 'anonymous'.
      : Connecting to ftp.sun.com (192.9.9.73) - done
Server:
      : 220 ftp.sun.com FTP server (Version 2.0.9) ready
      : 220-Welcome to Sun Microsystems Corporate FTP Server.
      : 220-
      : 220 ftp FTP server (ftpd Wed Oct 30 23:31:06 PST 1996) ready.
Proxy: Login on server as 'anonymou.
Server:331 Guest login ok, send your e-mail address as password.
Proxy supplying password to server
230 Guest login ok, access restrictions apply.
ftp>...
```

```
ftp>...
ftp>...
ftp> bye
221- Proxy: Quitting service.
221 Server: Goodbye.
%
```

Using the TELNET Proxy

The SunScreen `telnet` proxy logon process takes place in two stages:

1. First, you must `telnet` to the Screen and be authenticated by the proxy, which then forwards you to the destination host, which prompts you to log in.
2. You can then log in to the target system and be authenticated in the usual manner.

For information on setting up the `telnet` proxy, see “To Define `PROXY_Telnet`” on page 232.

▼ To Use the Telnet Proxy

The following steps illustrate what a user logging into a system through the `telnet` proxy experiences. In this example, the proxy is running on a Screen named `Screen`, and the user wants to connect to a system named `foo.com`:

1. **Type the following:**

```
% telnet Screen
```

The following text appears:

```
SunScreen Telnet Proxy Version: 3.2
```

2. **Type the user name at the prompt:**

```
Username@Hostname: username@foo.com
```

3. **Type your authorized user password to authenticate you to this proxy:**

```
password:
```

The password is not echoed. If you are successful, you will see the normal `telnet` connection information for the system `foo.com`, for example:

```
% Trying 172.16.6.74
Connected to foo.com
Escape character is '^]'.

```

```
UNIX(r) System V Release 4.0 (foo.com)
login:
```

4. **Log in to the system as you normally would, and if required, type a password.**

Using the SMTP Proxy

The SMTP proxy provides a relay for email. It can restrict access based on source address, as well as the domain name of the originating address, and the source and destination mailbox addresses presented within the SMTP protocol (envelope). The source (the sender's address) is compared to the list of spam domains; if the address matches any specific spam domain, the packet gets dropped. The destination (the recipient's address) is compared with the local domain to see if relaying is being attempted. If relaying is allowed, the email message gets passed through, if not, the email message gets dropped.

Be sure you have defined any necessary spam and relay restrictors (see "To Add Spam Domains" on page 218 and "To Delete Spam Domains" on page 221).

▼ To Use the SMTP Proxy

1. **Point the MX record for the domain to the proxy for mail to be processed properly.** SMTP connection is then made to the proxy rather than to the actual SMTP server.
2. **Point the destination in the rule to the actual SMTP server.**

Using the HTTP Proxy

The HTTP proxy provides a relay capability for the World Wide Web supporting the HTTP protocol. As with other proxies, it allows or denies sessions based on the source or destination address. It also provides selective filtering of content based on the source and destination of sessions. The selective filtering options include Java filtering, ActiveX, and cookies.

The HTTP proxy filters Java by reading the signatures encapsulated in Java Archives (Jars) or on a precomputed hash of Java Archive content.

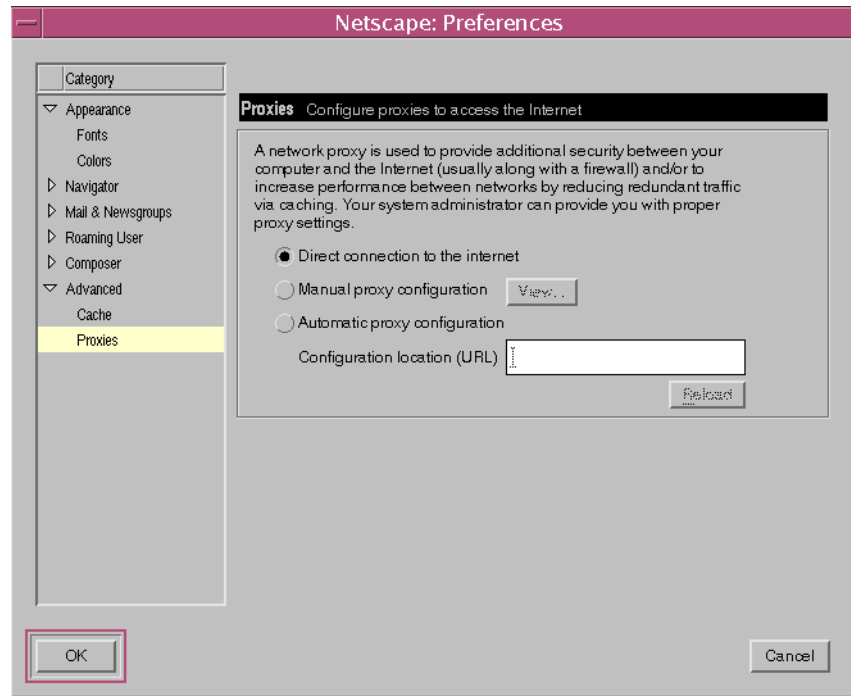
For user-based authentication, select a proxy user. For more information on configuring the HTTP proxy, see “To Define PROXY_HTTP” on page 230.

▼ To Configure the Browser to Use the HTTP Proxy

Basically, you point your browser at the Screen instead of allowing the browser to target HTTP servers directly. This example procedure is designed for configuring the Netscape browser. Consult the documentation for your browser to determine how to set the HTTP proxy server address and port number.

The server address should be the Screen’s address and the port number must be 80.

1. **Select Preferences in the Edit pulldown.**
The Preference page is displayed.
2. **Select Advanced on the Preferences page.**
3. **Select Proxies under the Advanced selection.**



4. **Select Manual proxy configuration.**

5. Click the View button beside the Manual proxy configuration.

Netscape: View Manual Proxy Configuration

You may configure a proxy and port number for each of the internet protocols that Netscape supports.

FTP Proxy: Port:

Gopher Proxy: Port:

HTTP Proxy: Port:

Security Proxy: Port:

WAIS Proxy: Port:

You may provide a list of domains that Netscape should access directly, rather than via the proxy:

No Proxy for:

SOCKS Host: Port:

OK Cancel

6. Enter the IP address in the HTTP Proxy field.
7. Type the number 80 as the number of the Port in the Port field for HTTP.

The HTTP proxy is fixed at port 80 in the current version of SunScreen.

You may, as desired, set the values for the FTP Proxy and/or Security Proxy to the same values just used for the HTTP Proxy. This will cause browser-initiated requests for ftp:// and/or SSL references to be handled by the HTTP proxy on the Screen. See "Proxies" in *SunScreen 3.2 Administrator's Overview* for details on HTTP Proxy Port Restrictions and HTTP Proxy Access for ftp://.
8. Click the OK button in the View Manual Proxy Configuration dialog box.
9. Click the OK button in the Preferences dialog box.

Proxy Logging

You control proxy logging by selecting Logging as part of a rule's action *and* by configuring the log limiter variables.

When logging is specified in a proxy rule, all (non-debug) events relating to a session enabled by that rule are logged for the proxy. Events based on the limiters for a given proxy are also logged, regardless of rule action.

See *SunScreen 3.2 Administrator's Overview* for the specifications of log limiter variables.

Configuring Centralized Management Groups

This chapter describes how to configure centralized management groups (CMG) using the administration GUI. Centralized management enables you to administer configurations on a group of Screens remotely.

The following information describes how to use the administration GUI. For an example of a CMG setup, see the *SunScreen 3.2 Configuration Examples* manual.

The following table lists the procedures in this chapter.

TABLE 7-1 Procedures for Centralized Management

"To Generate an IKE or SKIP Certificate on the Primary Screen" on page 245
"To Associate the IKE or SKIP Primary Screen's Certificate with the Primary Screen Object" on page 247
"To Put the IKE or SKIP Primary Screen's Certificate on the Secondary Screen" on page 250
"To Add the IKE or SKIP Primary Screen Object to the Secondary Screen" on page 252
"To Generate an IKE or SKIP Certificate for the Secondary Screen" on page 254
"To Modify the IKE or SKIP Secondary Screen Object" on page 254
"To Configure the Secondary Screen for Management by the Primary Screen" on page 256
"To Add the Secondary Screen's Certificate ID to the Primary Screen" on page 260
"To Add a Secondary Screen Object to the Primary Screen" on page 261
"To Define the Secondary Screen's Interfaces on the Primary Screen" on page 265
"To Add a New Address Group to the Primary Screen" on page 263
"To Configure the Primary Screen to Manage the Secondary Screens" on page 267

CMG Overview

A centralized management group is comprised of a primary Screen and a number of secondary Screens. The primary Screen, where all configuration objects reside, manages both itself and the centralized management group's secondary Screens. The primary Screen's function is to push policy configurations to the secondary Screens in the CMG. This capability enables you to manage many Screens effectively from one location.

To configure a centralized management group, you have to exchange certificate information between the CMG primary and secondary Screens, then add these certificates, along with the Admin IP address information and encryption algorithms for the respective Screens, to the Screen objects.

On the CMG primary Screen, you need to specify each interface present on any secondary Screen. These interface definitions should include the related Screen object to make them Screen-specific.

Finally, you must add packet filtering rules to both the primary and secondary Screens so the primary Screen can push its policy to the secondary Screens.

CMG Requirements

Many configurations require cluster members to pass through a firewall in order to communicate with the primary Screen. In these configurations, any firewall being traversed must contain packet filtering rules that allow certain traffic from the primary Screen to pass through its interfaces to the secondary Screen or Screens. These rules must include the following services:

- SKIP
- Certificate Discovery Protocol
- IPsec/IKE

Note – Although SKIP and IPsec are different protocols and cannot interoperate (SKIP can communicate with any release of SKIP, but not with IPsec.) , you can have SKIP rules and IPsec rules on both machines as long as there is no host overlap. That is, you may set the secondary Screen up to use SKIP to encrypt all traffic between A and B and IPsec to encrypt all traffic between A and C. For this type of setup, the CMG primary Screen should have as its ADMIN_CERTIFICATE a certificate group containing one SKIP and one IKE certificate. Each secondary Screen will have as its ADMIN_CERTIFICATE either a SKIP or an IKE certificate and the appropriate encryption parameters.

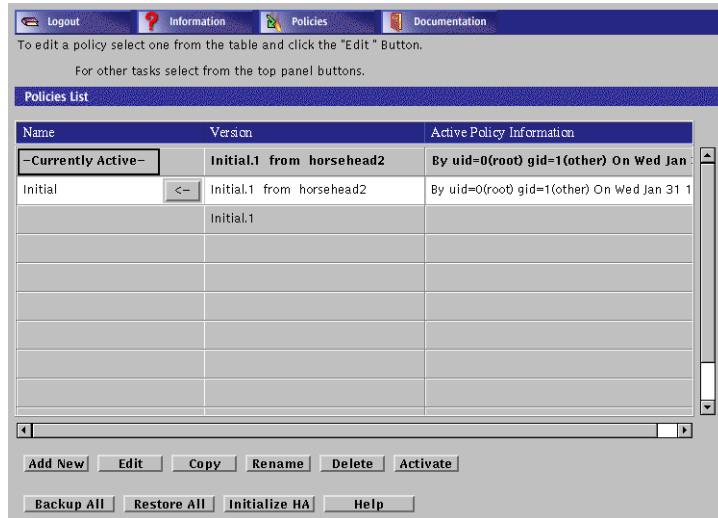
CMG Configuration Tasks

The following steps outline the workflow in setting up a centralized management group (CMG). Detailed steps for each task are provided in the following sections.

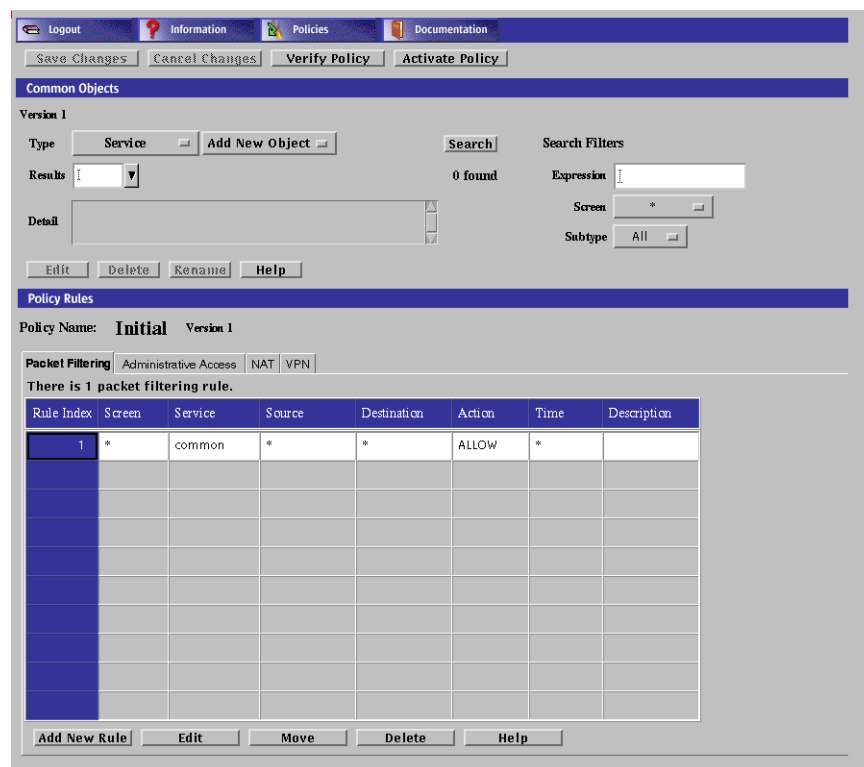
1. Generate a certificate for the primary Screen (if needed.)
2. On the primary Screen, associate this Certificate with the primary Screen object.
3. Add the primary Screen certificate to the secondary Screen.
4. Add a Screen object for the primary Screen to the secondary Screen.
5. Generate a certificate for the secondary Screen (if needed.)
6. On the secondary Screen, modify the secondary Screen object.
7. Add new rules on the secondary Screen allowing it to be managed by the primary Screen, and activate the policy.
8. Add the secondary Screen certificate to the primary Screen.
9. Add a Screen object for the secondary Screen to the primary Screen.
10. Add a new address group on the primary Screen.
11. Define the secondary Screen's interfaces on the primary Screen.
12. Add new rules on the primary Screen allowing it to manage the secondary Screen.
13. On the primary Screen, activate the policy for the CMG.

▼ Basic Centralized Management Procedure

1. Choose a policy in the Policies List page.



2. Click the Edit button.
The Policy Rules page appears.

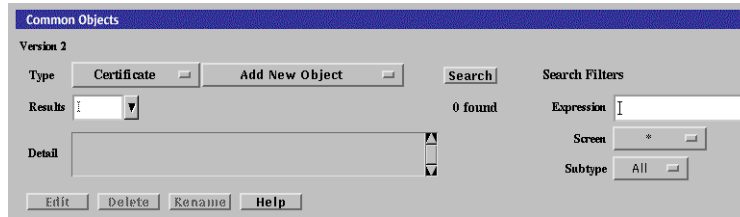


▼ To Generate an IKE or SKIP Certificate on the Primary Screen

If you selected remote administration during SunScreen installation, a certificate was automatically generated for the Screen, using the primary Screen's hostname with a .admin suffix. You can use this certificate to configure centralized management; you do not need to generate a new certificate.

If you did not select remote administration during SunScreen installation, perform the following steps on the primary Screen to generate a new certificate:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.
2. Select Certificate from the Type list.



3. (SKIP only) Select Generate SKIP UDH from the Add New list.

The certificate dialog box appears with options for the type of key to generate. The default value for the type is *highest available*.



4. (SKIP only) Type the name of the CMG's primary Screen (with the suffix .admin) in the Name field of the Certificate dialog box.

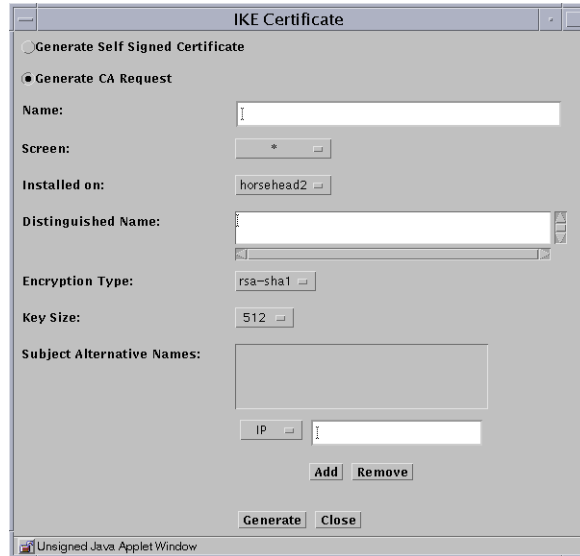
In this example, *boss* is the primary CMG Screen's host name.

5. (SKIP only) Click the Generate New UDH button.

Once generated, the Certificate ID field contains the Certificate Identifier for the CMG's primary Screen. You use the name of the Certificate Object (as specified in the Name field) to configure the secondary Screen.

6. (IKE only) Select Generate IKE Certificate from the Add New list.

The certificate dialog box appears with options for the type of key to generate. The default value for the type is *highest available*.



7. (IKE only) Type the name of the CMG's primary Screen (with the suffix .admin) in the Name field of the Certificate dialog box.

In this example, boss is the primary CMG Screen's host name.

8. Fill in the remainder of the fields as called out in "To Generate an IKE Certificate" on page 68.

9. (IKE only) Click the Generate button.

The IKE certificate is generated. You use the name of the Certificate Object (as specified in the Name field) to configure the secondary Screen.

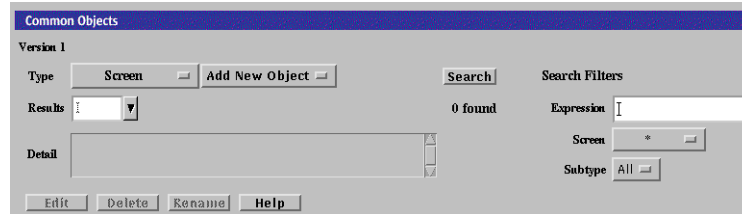
10. Click the OK button.

▼ To Associate the IKE or SKIP Primary Screen's Certificate with the Primary Screen Object

Perform the following steps on the primary Screen:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.

2. Select Screen from the Type list.



3. Click the Search button.

The results area now contains the name of the CMG's primary Screen.

4. Select the name of the CMG's primary Screen in the Results area.

Information about the Screen appears in the Details field

5. Click the Edit button.

The Screen dialog box appears.

The screenshot shows a Java applet window titled "Screen". At the top, there are two text input fields labeled "Name:" and "Description:". Below these are four tabs: "Miscellaneous" (selected), "SNMP", "Primary/Secondary", and "Mail Proxy". Under the "Miscellaneous" tab, there are three text input fields: "Log Size (MB)", "Stealth Net Address", and "Stealth Netmask". Below these are four groups of radio buttons: "Destination Address Checking:" with "Yes" and "No" (selected); "Allow Routing Traffic:" with "Yes" (selected) and "No"; "Name Service:" with "DNS", "NIS" (selected), "Both", and "None"; and "Certificate Discovery:" with "Yes" (selected) and "No". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help". The status bar at the bottom left of the window reads "Unsigned Java Applet Window".

6. Click the Primary/Secondary tab.

Be sure the IP address of the primary Screen appears in the Administrative IP Address field. If it is not present, provide it now.



7. Type the name of the CMG Primary's Certificate name (the Primary name with the suffix .admin) in the Administration Certificate field of the Primary/Secondary page.

This action associates the certificate with the CMG's primary Screen.

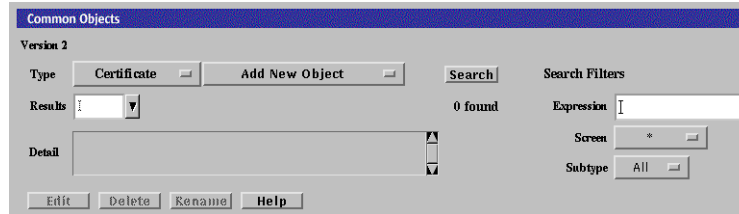
8. Click the OK button.

▼ To Put the IKE or SKIP Primary Screen's Certificate on the Secondary Screen

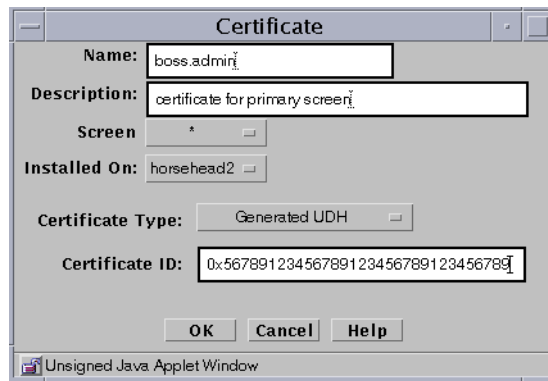
Perform the following steps on the secondary Screen:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.

2. Select Certificate from the Type list.



3. (SKIP only) Select Associate SKIP Certificate from the Add New list.
The Certificate dialog box appears.



4. (SKIP only) Type the primary Screen name (with .admin suffix) in the Name field.
5. (SKIP only) In the Certificate ID field, type the Certificate ID of the primary Screen.
6. (IKE only) Select Associate IKE Certificate from the Add New List.
The certificate dialog box appears.



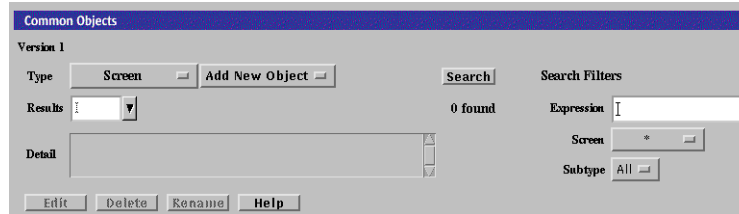
7. **(IKE only)** Type the primary Screen name (with `.admin` suffix) in the Name field.
8. **(IKE only)** In the Distinguished Name field, type the Distinguished Name of the primary Screen.
9. Click the OK button.

▼ To Add the IKE or SKIP Primary Screen Object to the Secondary Screen

Perform the following steps on the secondary Screen:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.

2. Select Screen from the Type list.



3. Click the Add New button.

The Screen dialog box appears with the Miscellaneous tab selected.



4. Type the name of the CMG's primary Screen in the Name field.

5. Click the Primary/Secondary tab.

Be sure the IP address of the primary Screen appears in the Administrative IP Address field. If it is not present, provide it now.

6. Type the name of the CMG Primary's Certificate name (the Primary name with the suffix .admin) in the IKE or SKIP Administration Certificate field of the Primary/Secondary page.

7. Click the OK button.

▼ To Generate an IKE or SKIP Certificate for the Secondary Screen

Note – If you selected Remote Administration during SunScreen installation, a certificate was automatically generated for the Screen. This certificate has a name containing the primary Screen’s hostname with a .admin suffix. You can use this certificate to configure Centralized Management; you do not have to generate a new certificate.

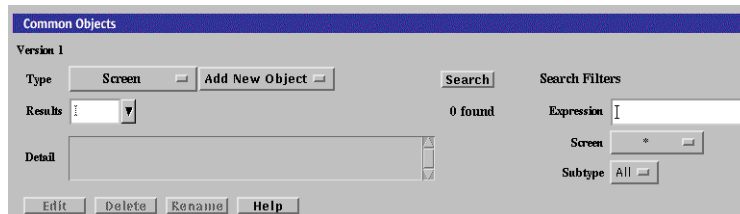
Perform the following steps on the secondary Screen:

1. **(IKE only)** Follow the steps in “To Generate an IKE Certificate” on page 68.
2. **(SKIP only)** Follow the steps in “To Generate SKIP UDHs Certificates” on page 76.

▼ To Modify the IKE or SKIP Secondary Screen Object

Perform the following steps on the secondary Screen:

1. Execute the steps in “Basic Centralized Management Procedure” on page 243.
2. Select Screen from the Type list.



3. Click the Search button.
4. Select the name of the CMG’s secondary Screen from the Results area.
5. Click the Edit button.
The Screen dialog box appears.

6. Select the Primary/Secondary tab in the Screen dialog box.

The screenshot shows a Java applet window titled "Screen". At the top, there are two text input fields: "Name:" with the value "horsehead2" and "Description:" with the value "secondary screen". Below these are four tabs: "Miscellaneous", "SNMP", "Primary/Secondary" (which is selected and highlighted), and "Mail Proxy". The "Primary/Secondary" tab contains several settings:

- High Availability:** A pull-down menu currently set to "No".
- Primary Name:** A pull-down menu currently set to "None".
- Administrative IP Address:** A text input field containing "260.100.33.3".
- SKIP Administrative Certificate:** A pull-down menu containing "efs-u5admin".
- IKE Administrative Certificate:** A pull-down menu containing "i".
- High Availability IP Address:** A text input field containing "i".
- Ethernet Address:** A text input field containing "i".
- SKIP Parameters:** An "Edit" button.
- IKE Parameters:** An "Edit" button.

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help". The status bar at the very bottom of the window reads "Unsigned Java Applet Window".

7. Select Secondary from the High Availability pulldown.



8. If not present, type the administration IP address of the CMG's secondary Screen in the **Administration IP Address** field.
9. **(IKE only)** Type the secondary Screen certificate name in the **IKE Administration Certificate** field.
In this example, the name is `efs-u5.admin`.
10. **(SKIP only)** Type the secondary Screen certificate name in the **SKIP Administration Certificate** field.
In this example, the name is `efs-u5.admin`.
11. Click the **OK** button.

▼ To Configure the Secondary Screen for Management by the Primary Screen

Perform the following steps from the CMG secondary Screen.

Note – The configuration changes in this step allow the primary Screen to download a policy to the secondary Screen. Once a policy is downloaded, the changes are no longer in effect. To download additional policies, see “To Configure the Primary Screen to Manage the Secondary Screens” on page 267.

1. Execute the steps in “Basic Centralized Management Procedure” on page 243.

2. Click the Packet Filtering tab of the Policy Rules area.

The policy rules that are currently defined for this policy are displayed.

3. Click the Add New button in the Policy Rules area.

The Rule Definition dialog box appears.

Rule Definition:Initial

Rule Index	1
Screen	
Service	certificate discovery
Source Address	boss
Destination Address	efs-u5
Action	ALLOW
Time	-
Description	

Show Action Details

OK Cancel

Unsigned Java Applet Window

4. Type 1 for the Rule Index.

This index will make the rule the first rule that gets enforced. You must place this rule before any other rule that could conflict with it. If you do not place it first, the primary Screen may not be able to manage the secondary Screen.

5. Fill in the following fields with real values for your configuration (values are provided for this example):

Screen	efs-u5
Service	certificate discovery (SKIP only)
Source	boss

Destination efs-u5

Action ALLOW

You can leave default values in all the other fields.

6. Click the OK button.

7. (SKIP only) Repeat Steps 2 through 6 using a Service of *skip* instead of *certificate discovery*

8. Verify that the rule definitions are correct.

The packet filtering rules should look like those in the following figure:

The screenshot shows a window titled "Policy Rules" with a sub-header "Policy Name: Initial Policy Version: 5". Below this, there are tabs for "Packet Filtering", "Administrative Access", "NAT", and "VPN". The "Packet Filtering" tab is active, and it displays the text "There are 2 packet filtering rules." Below this text is a table with the following data:

Rule Index	Screen	Service	Source	Destination	Action	Time	Description
1	efs-u5	skip	boss	efs-u5	ALLOW	*	
2	efs-u5	certificate dis	boss	efs-u5	ALLOW	*	

9. Create address groups for each interface on the secondary Screen:

a. From the Type list in the Common Objects area, select Address.

b. Select New Group from the Add New list.

c. Type the name of the address group that you wish to use (*bos_1e0* for example).

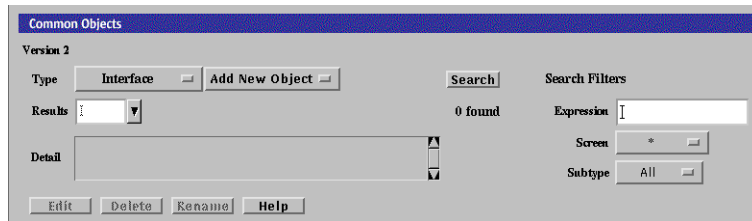
d. Add the address objects to the Include and Exclude lists.

Note – If the objects you need to make the appropriate group are not present, you may press Cancel. Follow the instructions in “To Add a Group of Addresses” on page 62 to create the necessary objects, then return to this section and start again at Step a.

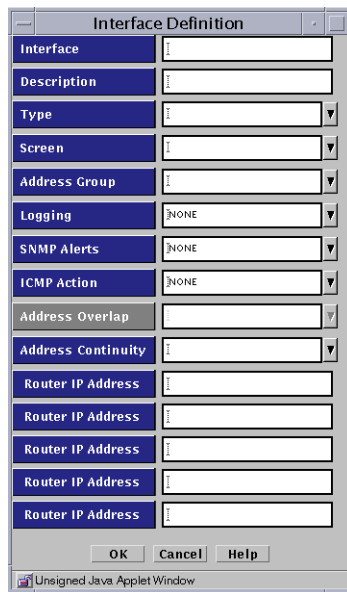
e. Click the OK button.

10. Define each interface on the secondary Screen as follows:

a. Select Interface from the Type list.



- b. Select New from the Add New list.
The Interface Definition window appears.

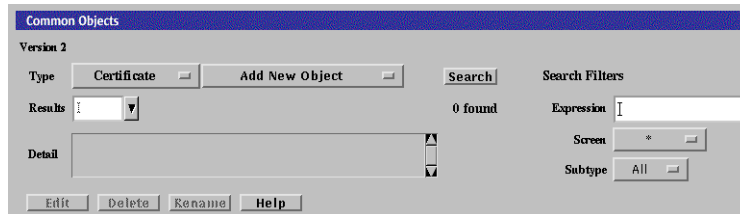


- c. Fill in the Interface, Type, Address Group, and Screen fields.
- d. Click the OK button.

▼ To Add the Secondary Screen's Certificate ID to the Primary Screen

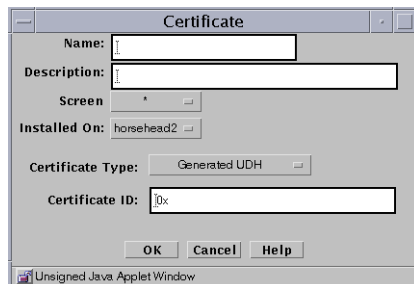
Perform the following steps on the primary Screen:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.
2. Select Certificate from the Type list.

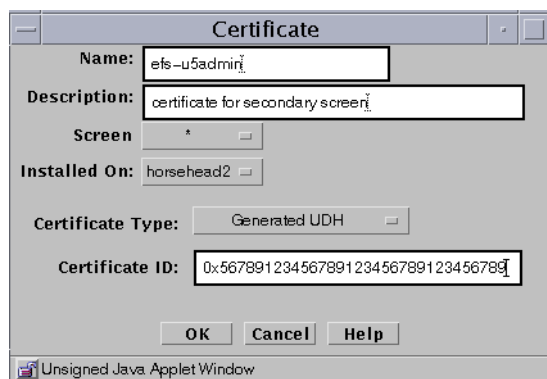


3. Select Associate SKIP Certificate from the Add New list.

The Certificate dialog box appears.



4. Type the secondary Screen name (with .admin suffix) in the Name field.



5. In the Certificate ID field, type the Certificate ID of the CMG's secondary Screen.
6. Click the OK button.

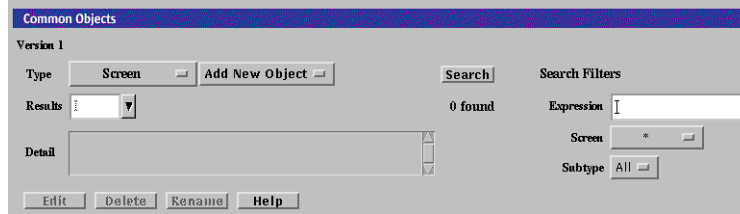
▼ To Add a Secondary Screen Object to the Primary Screen

Although SunScreen EFS 3.0 and 3.1 primary Screens can push rules to 3.2 secondary Screens, they can only do so using the functionality of the primary Screen's software release. A SunScreen primary Screen, however, can manage SunScreen EFS Version 3.0 and 3.1 secondary Screens effectively. If in doubt, install the latest software release on the *primary* Screen.

Perform the following steps on the primary Screen:

1. Execute the steps in "Basic Centralized Management Procedure" on page 243.

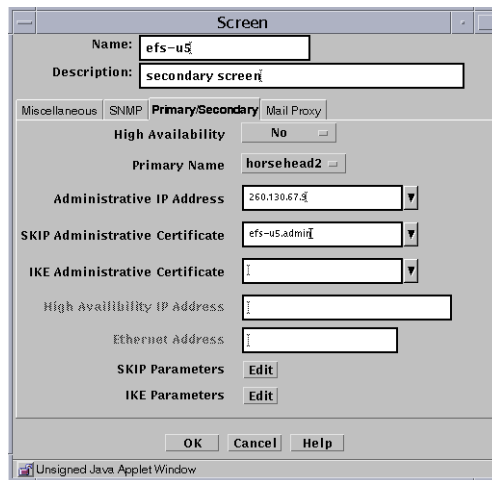
2. Select Screen from the Type list.



3. Click the New button.

The Screen dialog box appears with the Miscellaneous tab selected.

4. Type the name of the CMG's secondary Screen in the Name field then click the Primary/Secondary tab.



5. Select the primary Screen object name by selecting it from the Primary Name list.

This action tells the secondary Screen the name of its primary Screen.

6. Be sure the IP address of the secondary Screen appears in the Administrative IP Address field.

7. Type the CMG secondary certificate name (the Secondary name with the suffix .admin) in the Administration Certificate field of the Primary/Secondary page.

8. To edit either the SKIP or IKE parameters, click the appropriate Edit button.

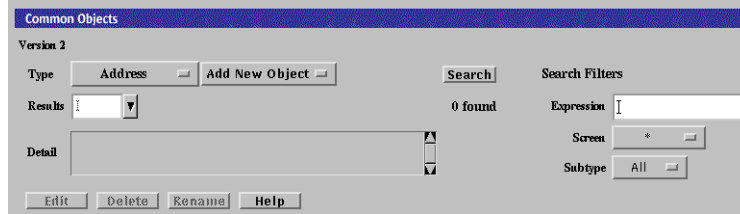
9. Click the OK button.

▼ To Add a New Address Group to the Primary Screen

Perform the following steps on the primary Screen:

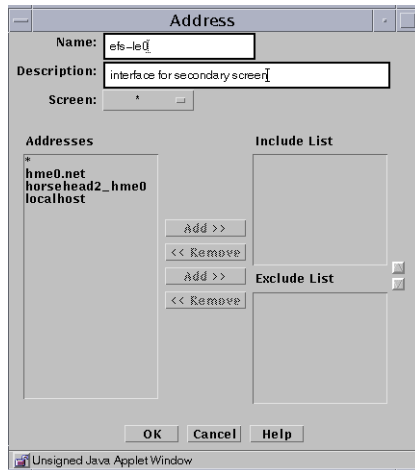
1. Execute the steps in “Basic Centralized Management Procedure” on page 243.

2. Select Address from the Type list.



3. Select New Group from the Add New list.

The Address dialog box appears.



4. Type the name of the Address Group.

In this example, you create the Address Group **efs-u5_1e0** to be used for the interface definition on the secondary Screen.

5. Select the name of the secondary Screen from the Screen list.

In this example, the Screen name is **efs-u5**.

6. Click the OK button.

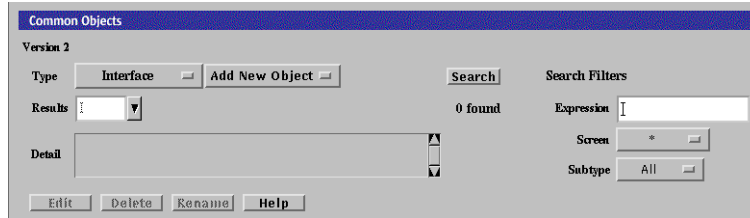
Select the address objects to include and exclude from this address group. If the required object is not listed, click the Cancel button and follow the instructions in “To Add a Group of Addresses” on page 62. After you create the required objects, return to this section and start again.

▼ To Define the Secondary Screen's Interfaces on the Primary Screen

Perform the following steps on the primary Screen:

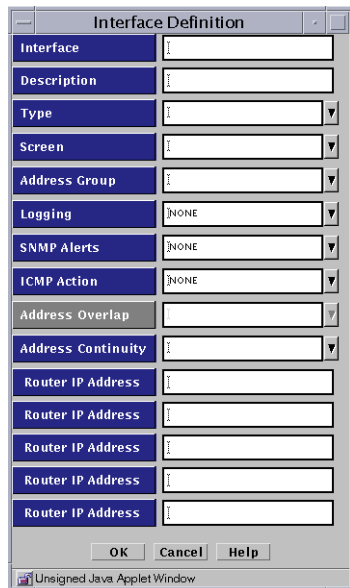
1. **Execute the steps in "Basic Centralized Management Procedure" on page 243.**

2. Select Interface from the Type list.



3. Select New from the Add New list.

The Interface Definition dialog box appears.



4. Define the interfaces of the secondary Screen:

The interface definition for `efs-u5_1e0` is shown in this figure. You must define each of the secondary Screen's interfaces on the primary Screen as follows, and each definition must contain one of the following:

- | | |
|-----------|---|
| Interface | The actual interface name on the secondary Screen |
| Type | STEALTH, ROUTING, or ADMIN |
| Screen | Screen name as defined in the Screen object |

Address Group Valid addresses for this interface

The Interface Definition dialog box is now identical on both screens.

5. **Click the OK button.**

▼ To Configure the Primary Screen to Manage the Secondary Screens

Perform this task on the CMG primary Screen. It adds policy rules to allow the primary Screen to pass management traffic through the secondary Screen's interfaces.

1. **Execute the steps in "Basic Centralized Management Procedure" on page 243.**

2. **Select the Packet Filtering tab of the Policy Rules area.**

The policy rules that are currently defined for this policy are displayed.

3. Click the Add New Rule button in the Policy Rules area.

The Rule Definition dialog box appears.

Rule Index	1
Screen	
Service	certificate discovery
Source Address	boss
Destination Address	efs-u5
Action	ALLOW
Time	-
Description	

4. Type 1 for the Rule Index.

Note – This index makes this rule the first rule that gets enforced. You must place this rule before any other rule that could conflict with it. If you do not place it first, the primary Screen may not be able to manage the secondary Screen.

5. Fill in the following fields with real values for your configuration (values are provided for this example):

Screen	efs-u5
Service	certificate discovery (SKIP only)
Source	boss
Destination	efs-u5
Action	ALLOW

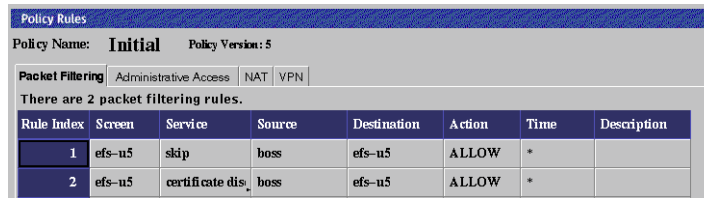
You can leave default values in all the other fields.

6. Click the OK button.

7. (SKIP only) Repeat Steps 1 through 5 using a service of *skip* instead of *certificate discovery*.

8. Verify that the rule definitions are correct.

The packet filtering rules should look like the following:



The screenshot shows a configuration window titled "Policy Rules" for a policy named "Initial" (version 5). It displays two packet filtering rules. The first rule (index 1) is named "efs-u5" and has a service of "skip", source of "boss", and destination of "efs-u5". The second rule (index 2) is named "efs-u5" and has a service of "certificate dis.", source of "boss", and destination of "efs-u5". Both rules have an action of "ALLOW" and a time of "*".

Rule Index	Screen	Service	Source	Destination	Action	Time	Description
1	efs-u5	skip	boss	efs-u5	ALLOW	*	
2	efs-u5	certificate dis.	boss	efs-u5	ALLOW	*	

9. Create address groups for each interface on the secondary Screen using the instructions in "To Add a New Address Group to the Primary Screen" on page 263.
10. Define each of the secondary Screens' interfaces using the instructions in "To Define the Secondary Screen's Interfaces on the Primary Screen" on page 265.
11. From the primary Screen, activate the policy to push it to all the CMG secondary Screens.

Note – Be sure to activate the policy on the secondary Screen first so it will be able to receive the pushed policy from the primary Screen.

Adding Remote Administration Stations After Installation

This chapter describes how to add a remote Administration Station after you have already installed SunScreen. There are three basic steps:

1. Install the administration software on the new remote Administration Station.
2. Set up the Screen to use the new Administration Station.
3. Set up the access control list on the new remote Administration Station.

Much of the information you need to perform this task is located in the *SunScreen Installation Guide*. Refer to it for detailed information on how to install the SunScreen administration software and certificates on the additional remote Administration Station.

Adding a Remote Administration Station

If you have already set up a remote Administration Station with your Screen (and you want to add an additional Administration Station), you should have a Screen certificate and admin certificate group, so you can skip most of these steps and go directly to “To Inform the Screen About the New Remote Administration Station” on page 272.

If this is the first remote Administration Station (Screen installed with local administration only), you need to create a certificate and admin certificate group before you add the remote Administration Station certificate. The following procedure explains how to accomplish this task.

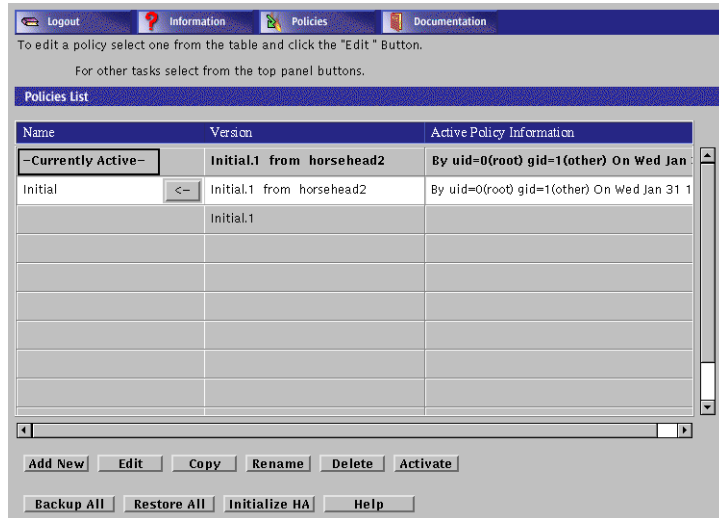
▼ To Set Up the Screen to Use the New Remote Administration Station

1. Generate a certificate for the Screen (see “To Generate SKIP UDHs Certificates” on page 76 if you are using a SKIP certificate or “To Generate an IKE Certificate” on page 68 if you are using an IKE certificate).
2. (SKIP only) Issue a `skipd_restart` command.
3. Add the certificate from remote Administration Station to the Screen (see “To Associate SKIP Certificate” on page 81 if you are using a SKIP certificate or “To Associate an IKE Certificate” on page 74 if you are using an IKE certificate).
4. Add a certificate group named `admin` with the Administration Station certificate as a member of this group (see “To Add a Certificate Group” on page 83).
5. Add an Administrative Access rule for Remote Administration using the `admin` user, `admin` certificate group, and encryption parameters that match those of the remote Administration Station (see “To Add or Change an Administrative Access Rule for Remote Administration” on page 140).
6. Save and activate the policy.

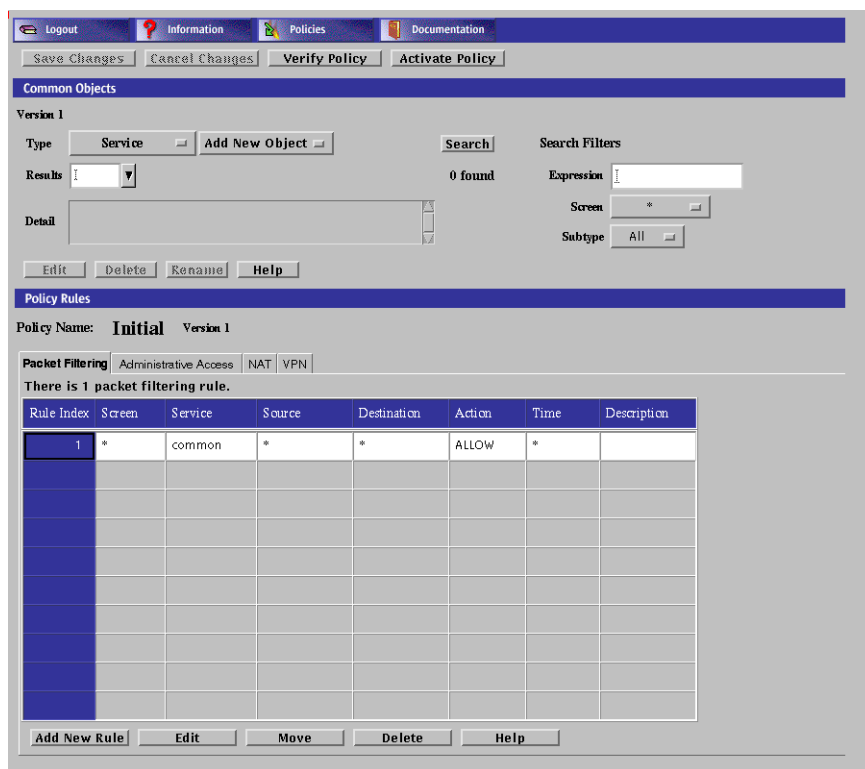
▼ To Inform the Screen About the New Remote Administration Station

After installing the SunScreen administration software and certificates, follow the steps below to inform the Screen about the new remote Administration Station.

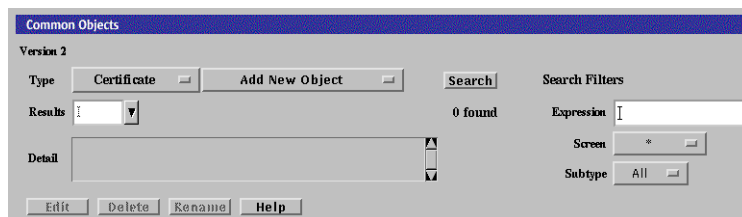
1. Choose the policy **Initial** in the **Policies List** page.



2. Click the **Edit** button.
The Policy Rules page appears.

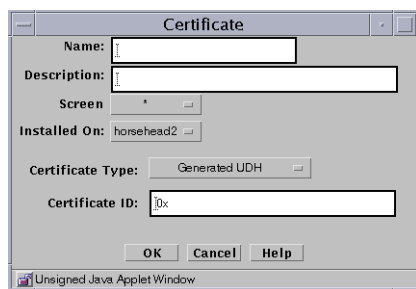


3. Select Certificate in the Type list.

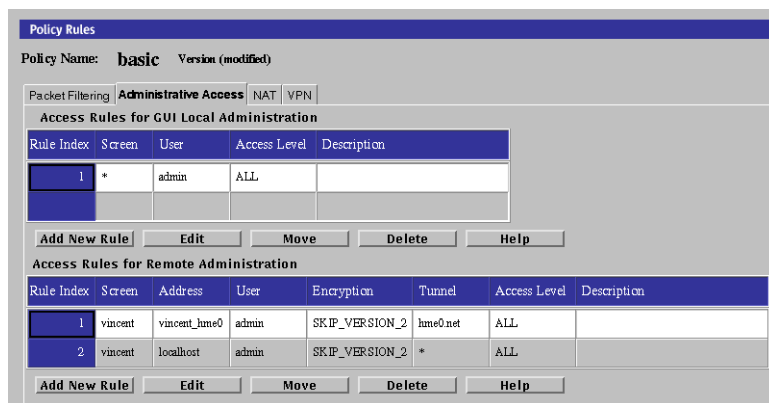


4. Select Associate SKIP Certificate from the Add New list.

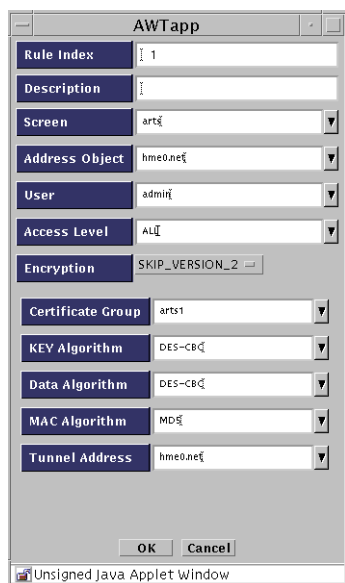
The Certificate dialog box appears.



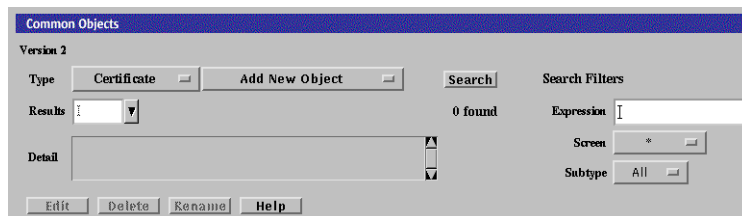
5. Type a name for the new remote Administration Station in the Name field.
6. Type the certificate number of the new remote Administration Station in the Certificate ID field.
The Certificate ID begins with 0x.
7. Click the OK button.
8. Click the Administrative Access tab in the Policy Rules area.
The Administrative Access area appears.



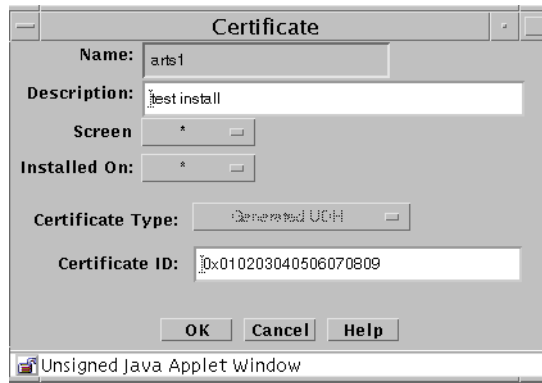
9. Click the Edit button below the Access Rules for Remote Administration table.
The Remote Access Rules dialog box appears. Note the name in the Certificate Group field. In the following steps, you must add the certificate of the new remote Administration Station to this group.



10. Click the Cancel button.
11. Select Certificate in the Type list.



12. Click the Search button.
13. Select the Certificate Group name in the Results area that was displayed in the Certificate Group field of the Remote Access Rules dialog box, in step 3 through step 7.
14. Click the Edit button.
The Certificate dialog box appears.



15. Select the certificate you created in step 5 from the Available Certificates field.
16. Click the Add button.
17. Click the OK button.
18. Save and activate the policy.

▼ To Set Up the Access Control List on the New Remote Administration Station

The last step is to add the Screen's certificate to the remote Administration Station.

- See "Completing SKIP Setup on the Administration Station" in *SunScreen Installation Guide* for the procedures to get the Certificate ID from the Screen and to use the `skiptool` GUI to set up the Access Control List.

Note – To administer SKIP directly or to gather data from any of the SKIP commands, you must log on to the Screen system

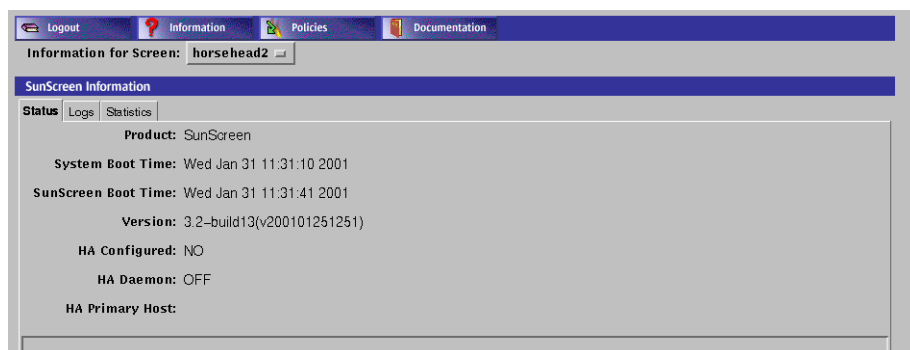
Getting Status and Managing Logs

This chapter describes the following tasks associated with the Information page in the administration GUI:

- Viewing status information
- Viewing SKIP statistics
- Viewing logs
- Setting the log retrieval mode
- Setting a log viewing filter
- Saving and clearing the log
- Changing the log file size for a Screen

The Information Page

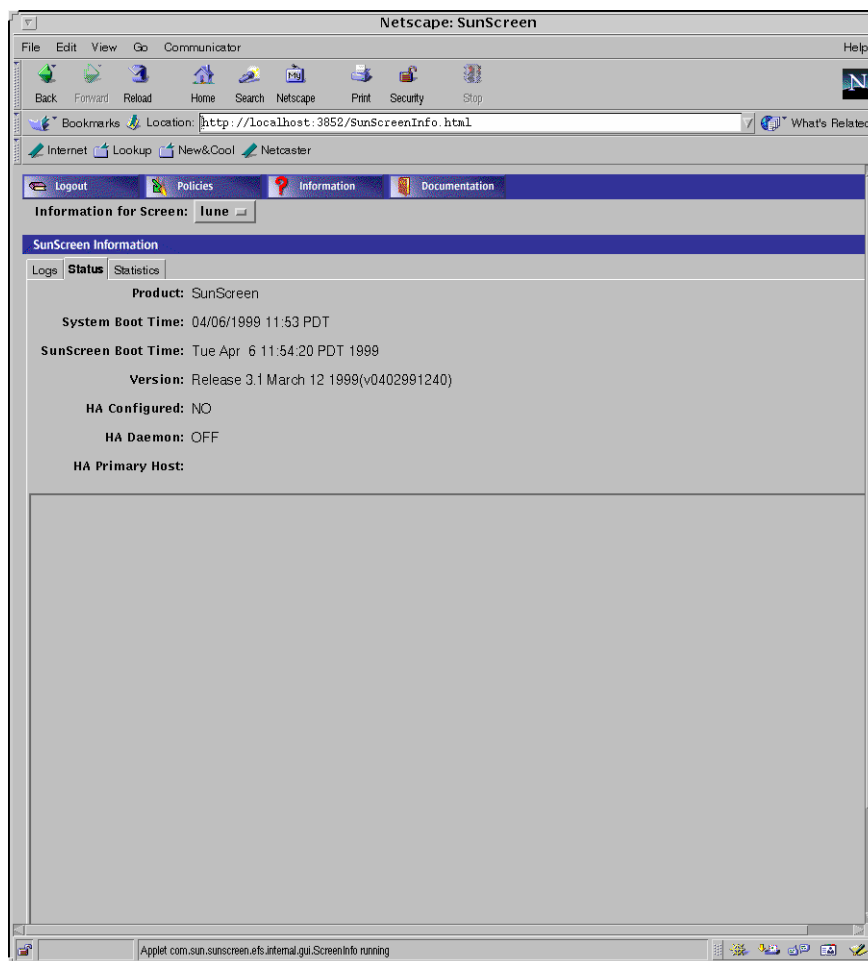
The Information page provides statistics, logs, and other information, such as system boot time, SunScreen boot time, version, and information about high availability. To display the Information page, click the Information button in the SunScreen banner.



Status Information

▼ To View Status Information

1. **Click the Information button in the SunScreen banner.**
The Information page displays.
2. **Click the Status tab.**
The Status page displays.



The Status page shows SunScreen product information as well as HA configuration information.

The following table describes the information presented on this page.

TABLE 9–1 Status Information

Title	Description
Product	The name of the software product.
System Boot Time	Date and time when the system was last restarted.

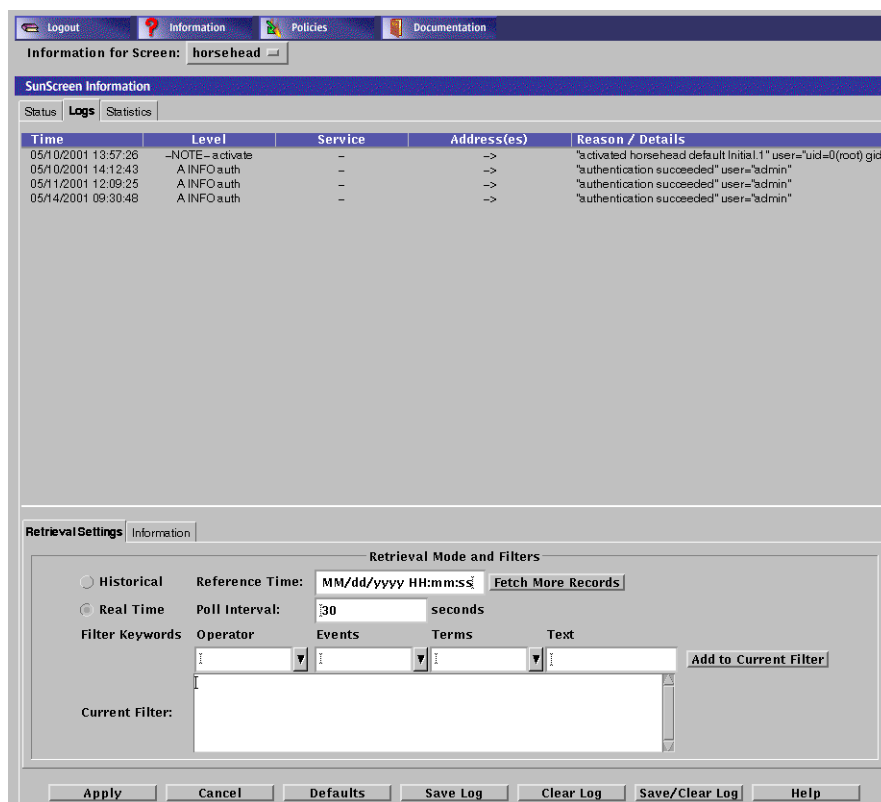
TABLE 9–1 Status Information (Continued)

Title	Description
SunScreen Boot Time	Date and time when the system was last restarted.
Version	The release of the software that is running.
HA Configured	Whether high availability (HA) is configured (YES or NO).
HA Daemon	Whether the high availability daemon is running (OFF or ON). If the HA daemon is running, the members of the HA cluster appear in the area below along with the state of each member of the HA cluster (Active or Passive).
HA Primary Host	The name or IP address of the primary host of the high availability cluster.
Host Names	Lists the hosts configured for HA. This information appears in the area set off from the rest of the information and is updated by default every 30 seconds. You can change the update interval by changing the poll interval in the Logs tab.
Status	Shows the status of the primary and secondary HA hosts. The status is ACTIVE, PASSIVE, and NONRESPONSIVE. This information appears in the area set off from the rest of the information and is updated by default every 30 seconds. You can change the update interval by changing the poll interval in the Logs tab.
Help button	Displays the online help for this page.

Log Page

▼ To View the Log Page

- 1. Click the Information button in the SunScreen banner.**
The Information page displays.
- 2. Click the Log tab.**
The Log page displays.



The following table describes the column headings for the log panel of the SunScreen Information page.

TABLE 9-2 Column Headings on the Log Panel of the SunScreen Information Page

Field	Description
Time	Indicates the time that the packet or event represented by this record was logged by the Screen. Use this time field to retrieve records in Historical mode as set in the Log Browser Tab Retrieval Setting.
Level	Indicates the type and severity level of the logged event.
Service	Indicates the network service or protocol, such as TCP, IP, NFS, Telnet, or HTTP, over which this packet was sent or to which the event is related.
Address(es)	Shows the address from which and to which a packet was sent. Arrows indicate direction. Some events that, by themselves, are not related to IP traffic will not have an address or addresses, as shown in the example.

TABLE 9-2 Column Headings on the Log Panel of the SunScreen Information Page
(Continued)

Field	Description
Reason/Detail	Shows the reason a packet or event was logged or the detail regarding the logging. This information depends on the requirements of the rules within a policy.

The logs tab also displays the Retrieval Setting tab and Information tab for the logs.

Logged packets are configured in the packet filtering rules so that a packet or an event is displayed which meets the requirements of a rule in a policy. The log has two retrieval modes: Historical and Real Time.

- The Historical mode allows you to examine a particular segment for a particular time.
- The Real Time mode displays information as the packets pass through the Screen while you are looking at the log.

Retrieval Setting Tab

The following table describes the controls on the Retrieval Setting tab.

TABLE 9-3 Controls on the Retrieval Setting Tab

Control	Description
Retrieval Mode radio buttons	<p>Specifies the time frame for which you want log messages:</p> <ul style="list-style-type: none"> ■ Historical allows you to examine a particular segment for particular time and shows the segment of that log the most closely matches the time that you see as the first item in the list of logged packets. You must use four digits in specifying the year, for example, 2000. ■ Real Time specifies that the system displays the most recently logged records. You can specify how often the Log Browser page updates the log display in the Real Time Poll Interval field. If you set the log to Real Time Poll Interval, click the apply button. Depending upon your configured settings, records are logged faster than the Log Browser polls for new records. Thus, the display falls more and more behind as time goes on. If you want to see the most recently logged records. Click the Apply button to force a retrieval. The Poll Interval field also sets the times when the information in the Statistics tab is updated.

TABLE 9-3 Controls on the Retrieval Setting Tab (Continued)

Control	Description
Fetch More Records button	Retrieves more log records in the historical mode only. If you check Historical Reference Time and click the Apply button after specifying a date and time for retrieving records, the display will retrieve log records using the date and time that the log file was last cleared. Using this button, you can display the next screen of later records.
Filter Keywords field	Provide the ability to create many simple filtering expressions from the choice lists available. These controls reduce typing effort as well as serving as reminders of filtering options. For more detail, see the following section, "Setting a Log Viewing Filter" on page 285.
Add to Current Filter button	Causes these items chosen in the Filter Keywords fields to be added to the Filter Keywords text entry box at its current insertion pointer. For more detail, see the following section, "Setting a Log Viewing Filter" on page 285. It adds all text that is currently selected in the four combo boxes.
Current Filter text box	Allows you to enter an expression of the log-browser filtering language. An arbitrary <code>logdump</code> expression can be entered there and activated using the Apply button. For more detail, see "Setting a Log Viewing Filter" on page 285 below.

Setting a Log Viewing Filter

The Log Browser filters log events to be displayed. The language that it uses is identical to the filtering options of the `logdump` command in the command-line program; it is a superset of the language used by the Solaris `snoop` packet monitor tool.

You have full access to this language typing an arbitrary `logdump` expression in the Current Filter text entry box in its Retrieval Settings tab and clicking the Apply button to activate it.

In addition, the Filter Keywords controls provide the ability to create many simple filtering expressions. These controls reduce typing effort as well as serving as reminders of filtering options.

The Filter Keywords controls are used by selecting one or more operations from their choice lists or entering a target (operand) in the Text box. After choosing or typing your entry, click the Add to Current Filter button to add these items to the Filter Keywords text entry box at its current insertion pointer.

The leftmost editable combo box contains the Boolean operators `and`, `or`, and `not`.

The Events box provides filtering terms that are complete and restrict the type of log event displayed. The following table describes the terms in the Events box.

TABLE 9-4 Filter Terms of the Events Box

Term	Description
loglvl pkt	Allows displaying network packet-type events
loglvl sess	Allows displaying network session-type events
loglvl auth	Allows displaying events related to authentication operations
loglvl app	Allows displaying events related to screen application (usually proxy) operations
logapp activate	Allows displaying events related to policy activation.
logapp auth	Allows displaying events from the authentication subsystem
logapp compiler	Allows displaying events related to policy compilation
logapp edit	Allows displaying events related to registry or policy editing
logapp ftp	Allows displaying events from the FTP proxy
logapp ha	Allows displaying events related to HA operation
logapp http	Allows displaying events from the HTTP proxy
logapp iked	Allows displaying events related to the IKE daemon
logapp log	Allows displaying events related to the logging facilities themselves
logapp restore	Allows displaying events related to policy restoration
logapp scan	Allows displaying events related to proxy content scanning and redirection
logapp smtp	Allows displaying events from the SMTP proxy
logapp telnet	Allows displaying events from the Telnet proxy
logsev emerg	Allows displaying events of an emergency severity
logsev alert	Allows displaying events of an alert severity or above
logsev crit	Allows displaying events of a critical severity or above
logsev err	Allows displaying events of an erroneous severity or above
logsev warn	Allows displaying events of a warning severity or above
logsev note	Allows displaying events of a notice severity or above
logsev info	Allows displaying events of an informative severity or above (all events that are not of debug severity)
logsev debug	Allows displaying events of a debug severity or above (all events)

The Terms box provides filtering terms most of which are incomplete and require an operand value, You type these in the Text box. They are added to the choice list of the Text box for reference so that you need not retype the value if you want to use it again. The following table describes the filter terms in the Terms box.

TABLE 9-5 Filter Terms in the Terms Box

Term	Description
logwhy <i>reason#</i>	Restricts display to packets that have the given logging reason why code
logiface <i>iface</i>	Restricts display to packets that arrived on the interface named <i>iface</i>
host <i>hostname</i>	Restricts display to events either from or to <i>hostname</i>
dst <i>hostname</i>	Restricts display to events destined for <i>hostname</i>
src <i>hostname</i>	Restricts display to events origination from <i>hostname</i>
port <i>hostname</i>	Restricts display to events related to the service <i>svcname</i>
dstport <i>hostname</i>	Restricts display to events targeted to the service <i>svcname</i>
srcport <i>svcname</i>	Restricts display to events originating from the service <i>svcname</i>
net <i>netaddr</i>	Restricts display to events either from or to the network whose number is <i>netaddr</i>
udp	Restricts display to events related to the UDP transport protocol
tcp	Restricts display to events related to the TCP transport protocol
icmp	Restricts display to packets of the ICMP control protocol
rpc	Restricts display to packets of the RPC protocol

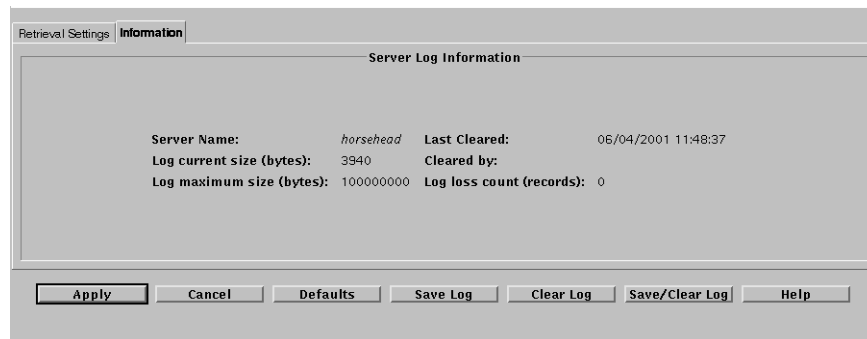
The terms in italics are variables for which you must supply a value or values in the when you choose this term from the choice list. The values for the variable are as follow:

- *reason #* The reason number is shown in “Error Messages” in *SunScreen 3.2 Administrator’s Overview*.
- *hostname* can be:
 - An IP address (dotted-quad a.b.c.d) (for example, 129.9.9.99)
 - An IP address range (a.b.c.d.e.f.g.h) (for example, 129.9.9.0..129.9.9.254)
 - A hostname known to the screen’s naming service (for example, the DNS name host.your-domain.com)
- *svcname* can be:
 - A numeric TCP or UDP port number (for example, 23 for Telnet)

- A numeric TCP or UDP port number range (for example, 6000 . . 6023 for X windows)
- A service name known to the screen's naming service (for example, domain found in `/etc/services`)
- *iface* can be:
 - The name of an interface (for example hme0)
- *netaddr* can be:
 - The IP network number (for example 199.12.200)

The Information Tab

The log-browser Information tab on the Screen Information page and shown in below provides the statistics for the current log.



The following table describes the fields on the Information tab. You cannot edit the fields on this page.

TABLE 9-6 Fields on the Information Tab

Control	Description
Server Name field	Indicates the name of the Screen to which the Log Browser is connected.
Log current size field (bytes)	Indicates the current size of the log file in bytes on the server.
Log maximum size field (bytes)	Indicates the maximum size of the log file in bytes on the server.
Last Cleared field	Indicates the date and time the log file was last cleared.

TABLE 9-6 Fields on the Information Tab (Continued)

Control	Description
Cleared By field	Identifies the login name of the administrator who last cleared the log file.
Log loss count (records) field	Indicates the number of log records that have been thrown away since the last “clear” operation. Log records are lost if the log grows beyond its maximum size or if the file system on which the log is written fills before that maximum is reached. Packets that cannot be logged because the traffic load exceeds the logger’s ability to store entries are not counted.

Action Buttons

The following table describes the action buttons on the SunScreen Information Page.

TABLE 9-7 Action Buttons on the SunScreen Information Page

Button	Description
Apply button	Applies any changes to the settings for the Log Browser page. You can click the Apply button to update the data displayed on the Log Browser page in the real time mode.
Cancel button	Undoes any changes that have not yet been applied.
Defaults button	Resets the Log Browser settings to their default values.
Save Log button	Saves the log file to a local file. If you are using Netscape Navigator or Internet Explorer, you must use the Java plug-in to save the log to a local file.
Clear Log button	Clears the log file, which clears the log record display area.
Save/Clear Log button	Saves and clears the log file. While the file is being saved, the Screen does not add records to the log. If you are using Netscape Navigator or Internet Explorer, you must use the Java plug-in to save the log to a local file.
Help button	Displays a browser window with the online help for the SunScreen Information Page. Two Help buttons appear on this page. They both display the same online help.

Statistics Page

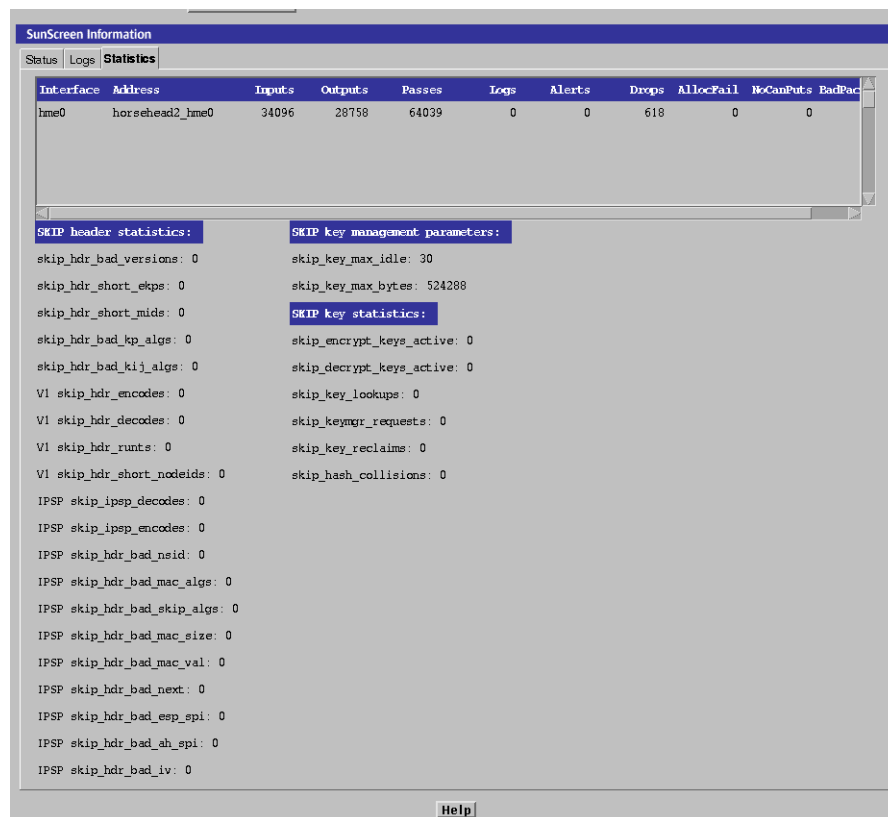
▼ To View the Statistics Page

1. Click the **Information** button in the SunScreen banner.

The Information page displays.

2. Click the **Statistics** tab.

The Statistics page displays.



SunScreen Information

Status | Logs | **Statistics**

Interface	Address	Inputs	Outputs	Passes	Logs	Alerts	Drops	AllocFail	ReCanPuts	BadPac
hme0	horsehead2_hme0	34096	28758	64039	0	0	618	0	0	0

SKIP header statistics:

- skip_hdr_bad_versions: 0
- skip_hdr_short_ekps: 0
- skip_hdr_short_mids: 0
- skip_hdr_bad_kp_algs: 0
- skip_hdr_bad_kij_algs: 0
- V1 skip_hdr_encodes: 0
- V1 skip_hdr_decodes: 0
- V1 skip_hdr_runts: 0
- V1 skip_hdr_short_nodeids: 0
- IPSP skip_ipsp_decodes: 0
- IPSP skip_ipsp_encodes: 0
- IPSP skip_hdr_bad_nsaid: 0
- IPSP skip_hdr_bad_mac_algs: 0
- IPSP skip_hdr_bad_skip_algs: 0
- IPSP skip_hdr_bad_mac_size: 0
- IPSP skip_hdr_bad_mac_val: 0
- IPSP skip_hdr_bad_next: 0
- IPSP skip_hdr_bad_esp_spi: 0
- IPSP skip_hdr_bad_ah_spi: 0
- IPSP skip_hdr_bad_iv: 0

SKIP key management parameters:

- skip_key_max_idle: 30
- skip_key_max_bytes: 524288

SKIP key statistics:

- skip_encrypt_keys_active: 0
- skip_decrypt_keys_active: 0
- skip_key_lookups: 0
- skip_keymgr_requests: 0
- skip_key_reclaims: 0
- skip_hash_collisions: 0

Help

The Traffic Statistics panel displays traffic statistics for each interface on the Screen. The following table describes the fields on the Traffic Statistics panel of the Statistics tab. The values displayed in these fields cannot be modified.

TABLE 9-8 Controls on the Traffic Statistics Panel of the Statistics Page

Control	Description
Interface field	Name of the interface.
Address field	Address of the interface.
Inputs field	Total number of packets seen on that network interface. This number includes packets processed by the Screen and intranet traffic. Because this counter records more than just the number of packets through the interface, the number can be much higher than the sum of the numbers in the Passes and Drops fields, which record the number of packets passed and dropped.
Outputs field	Total number of packets passed from other interfaces on the Screen and sent out over this interface.
Passes field	Number of packets received from another interface, matched to an ALLOW rule exactly, and sent out over the designated interface.
Logs field	Number of packets that have been logged by the Screen according to the actions in the active configuration.
Alerts field	Number of SNMP alerts generated because of the traffic on this network interface.
Drops field	Number of packets that have been dropped, either as a result of exactly matching a DENY rule or as a result of not matching any rule and being dropped as the default action of the Screen's interface.
AllocFail field	Error counter for packets lost because of the lack of resources.
NoCanPuts field	Error counter for packets lost because of the lack of stream flow control.
BadPackets field	Error counter for packets lost because of errors.

The SKIP Statistics panel shows the SKIP statistics for the SunScreen. The following table describes the fields on the SKIP Statistics panel of the Statistics page. The values displayed in these fields cannot be modified.

TABLE 9-9 Controls on the SKIP Statistics Panel of the Statistics Tab

Control	Description
skip_hdr_bad_versions field	Total number of SKIP headers with invalid protocol versions.
skip_hdr_short_ekps field	Number of SKIP headers with short encrypted packet fields.
skip_hdr_short_mids field	Number of SKIP headers with short MID fields.

TABLE 9-9 Controls on the SKIP Statistics Panel of the Statistics Tab *(Continued)*

Control	Description
skip_hdr_bad_kp_algs field	Number of SKIP headers with unknown cryptographic algorithms.
V1 skip_hdr_encodes field	Number of SKIP V1 headers encoded.
V1 skip_hdr_decodes field	Number of SKIP V1 headers decoded.
V1 skip_hdr_runts field	Number of SKIP V1 headers with short packets.
V1 skip_hdr_short_nodeids field	Number of SKIP V1 headers with short node identifiers.
IPSP skip_ipsp_decodes field	Number of SKIP V2 headers decoded.
IPSP skip_ipsp_encodes field	Number of SKIP V2 headers encoded.
IPSP skip_hdr_bad_nsid field	Number of headers with a bad V2 name space identifier.
IPSP skip_hdr_bad_mac_algs field	Number of headers with unknown or bad authentication algorithms.
IPSP skip_hdr_bad_mac_size field	The number of headers with an authentication error in the MAC size.
IPSP skip_hdr_bad_mac_val field	The number of headers with an authentication error in the MAC value.
IPSP skip_hdr_bad_next field	Number of headers with a bad Next Protocol field.
IPSP skip_hdr_bad_esp_spi field	Number of headers with a bad V2 SPI field.
IPSP skip_hdr_bad_ah_spi field	Number of headers with a bad V2 AH SPI field.
IPSP skip_hdr_bad_iv field	Number of headers with a bad V2 initialization vector.
IPSP skip_hdr_bad_short_r_mkeyid field	Number of headers with a short V2 receiver key identifier.
IPSP skip_hdr_bad_short_s_mkeyid field	Number of headers with a short V2 sender key identifier.
IPSP skip_hdr_bad_bad_r_mkeyid field	Number of headers with a bad V2 receiver key identifier.
skip_key_max_idle field	Time, in seconds, until an unused key is reclaimed.
skip_key_max_bytes field	Maximum number of bytes to encrypt before discarding a key.
skip_encrypt_keys_active field	Number of encryption keys in the cache.
skip_decrypt_keys_active field	Number of decryption keys in the cache.

TABLE 9-9 Controls on the SKIP Statistics Panel of the Statistics Tab (Continued)

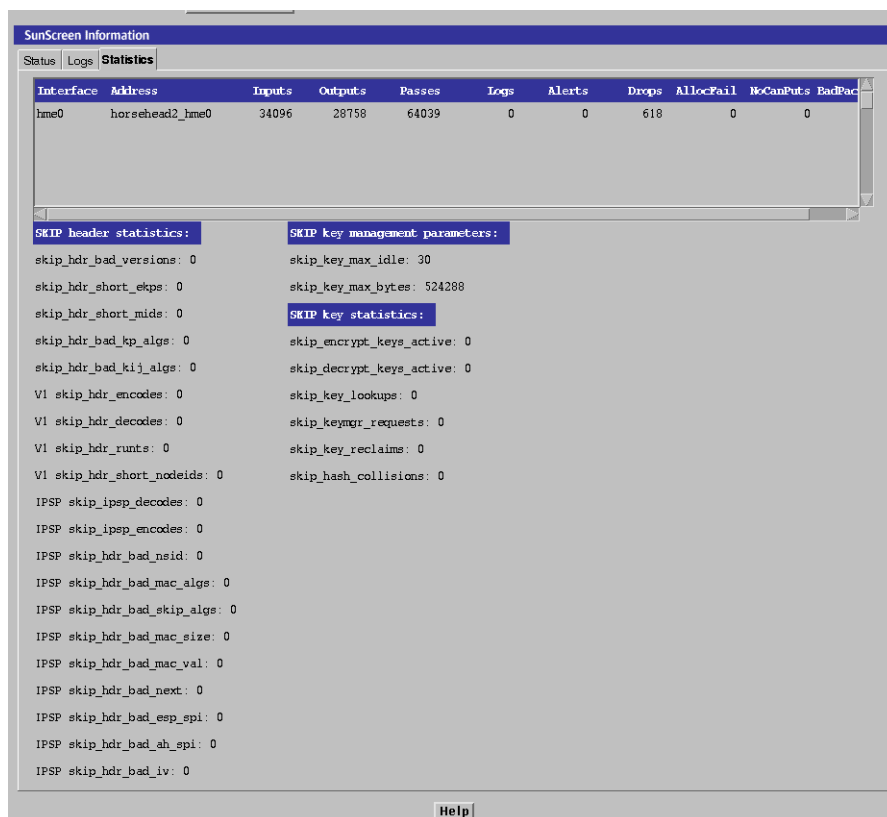
Control	Description
skip_key_lookups field	Total number of key cache lookups.
skip_keymgr_requests field	Total number of key cache misses (key not found).
skip_key-reclaims field	Total number of key entries reclaimed.
skip_hash_collisions field	Total number of table collisions.

Viewing Statistics

The Statistics area shows SKIP and traffic statistics for each network interface. Fields for the interface, SKIP key management, SKIP key statistics, and SKIP header statistics are described in “Logging” in *SunScreen 3.2 Administrator’s Overview*.

▼ To See the SKIP Statistics

1. **Click the Information button in the SunScreen banner.**
The Information page displays.
2. **Click the Statistics tab.**
The Statistics page displays.



Viewing Logs

Use the Log tab to view logged packets. You can configure policies in the packet filtering rules so that a packet is logged when it matches, or does not match, a particular policy rule criterion. For a complete description of logs, filtering, and retrieval settings, see “Logging” in *SunScreen 3.2 Administrator’s Overview*.

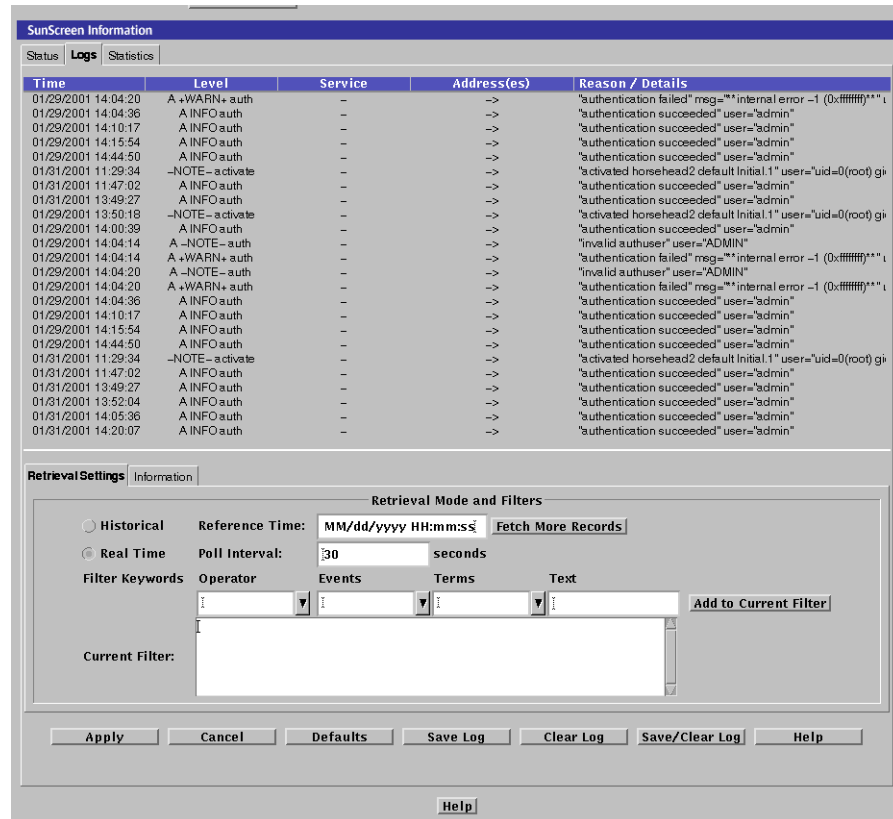
▼ To Set the Retrieval Mode

You can view packet activity logs in two modes: *real time* and *historical* (for a specified time period).

1. Click the Information button in the SunScreen banner.

2. Click the Log tab in the Information page.

The Log page displays.



3. Click the Retrieval Settings tab at the bottom of the log.

- Real time mode displays the information as the packets pass through the Screen.
- Historical mode enables you to examine a particular segment for specified time.

Note – If you are using historical mode, you must use four digits to specify the year, for example, 2001.

▼ To Set a Log Viewing Filter

1. Click the **Information** button in the SunScreen banner.
2. Click the **Log** tab in the Information page.

3. Select or type a Boolean operator (AND, OR, or NOT) in the Operator Filter Keywords fields.

The screenshot shows the SunScreen Information interface. At the top, there are tabs for Status, Logs, and Statistics. Below this is a table with columns: Time, Level, Service, Address(es), and Reason / Details. The table contains multiple rows of log entries, including authentication failures and successes for various users like 'admin' and 'ADMIN'. Below the table is the Retrieval Settings dialog box, which has tabs for Information and Settings. The dialog is titled 'Retrieval Mode and Filters' and includes options for Historical and Real Time data, a Reference Time field, a Poll Interval of 30 seconds, and a section for Filter Keywords with Operator, Events, Terms, and Text fields. There is an 'Add to Current Filter' button and a 'Current Filter' text area. At the bottom of the dialog are buttons for Apply, Cancel, Defaults, Save Log, Clear Log, Save/Clear Log, and Help.

Time	Level	Service	Address(es)	Reason / Details
01/29/2001 14:04:20	A +WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0x#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 13:50:18	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/29/2001 14:00:39	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:04:14	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:14	A +WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0x#####)**"
01/29/2001 14:04:20	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:20	A +WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0x#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:52:04	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:05:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:20:07	A INFO auth	-	->	"authentication succeeded" user="admin"

4. Either type the entire filter directly into the Current Filter field or perform the following steps:
 - a. Select or type a filtering term in the Events Filter Keywords field.
 - b. Select or type a filtering term in the Terms Filter Keywords field.
 - c. Type the operand value in the Text Filter Keywords field.
 - d. Click Add to Current Filter to add the items to the Current Filter field at the cursor insertion point.
 - e. Click Apply to activate the filter.

Note – For listings of the terms and values permitted in the four Filter Keywords fields, see the *SunScreen 3.2 Administrator's Overview*.

For example, you can type **host** in the Term field and your machine name in the Text field to only see records that apply to your machine.

Saving and Clearing the Log

The size of your network configuration and the logging rules you specify can cause log files to become extremely large. You should save and clear them periodically to prevent losing information. The default log size is 100MB, but it is configurable. If the log file fills up, the oldest data in the log is overwritten and information is lost. All Admin Users except those with an access level of STATUS can perform Save or Clear operations on the logs.

Some browsers do not allow you to save log files because save operations involve a local `write` operation, which is not allowed by the Java security model. If you use Netscape Navigator or Internet Explorer, you must use the Java Plug-In to enable save operations. The HotJava browser will allow you to perform these operations without the Java Plug-In with the `medium/low` security level set.

Note – Saving a log to a file does not clear the log records from the Log page.

▼ To Save the Log

1. **From the Information page, click the Log button.**

The Log page appears.

SunScreen Information

Status | **Logs** | Statistics

Time	Level	Service	Address(es)	Reason / Details
01/29/2001 14:04:20	A -WARN- auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 13:50:18	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/29/2001 14:00:39	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:04:14	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:14	A -WARN- auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:20	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:20	A -WARN- auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:52:04	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:05:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:20:07	A INFO auth	-	->	"authentication succeeded" user="admin"

Retrieval Settings | Information

Retrieval Mode and Filters

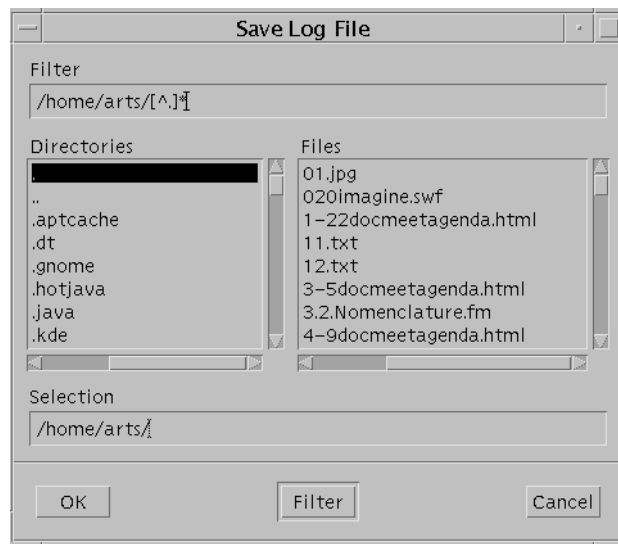
Historical Reference Time: MM/dd/yyyy HH:mm:ss [Fetch More Records](#)

Real Time Poll Interval: 30 seconds

Filter Keywords Operator Events Terms Text

Current Filter:

2. Click the Save Log button at the bottom of the Log page.
The Save File dialog box appears.
3. Type the full path (including file name) of the file where you want to store logs.



4. Click the OK button.

▼ To Clear the Log

The following steps clear the page of any log records without saving the records or the log file.

1. From the Information page, click the Log button.

The Log page appears.

SunScreen Information

Status **Logs** Statistics

Time	Level	Service	Address(es)	Reason / Details
01/29/2001 14:04:20	A -WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 13:50:18	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/29/2001 14:00:39	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:04:14	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:14	A -WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:20	A -NOTE- auth	-	->	"invalid authuser" user="ADMIN"
01/29/2001 14:04:20	A -WARN+ auth	-	->	"authentication failed" msg="** internal error -1 (0:#####)**"
01/29/2001 14:04:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:10:17	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:15:54	A INFO auth	-	->	"authentication succeeded" user="admin"
01/29/2001 14:44:50	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 11:29:34	-NOTE- activate	-	->	"activated horsehead2 default Initial.1" user="uid=0(root) gi
01/31/2001 11:47:02	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:49:27	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 13:52:04	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:05:36	A INFO auth	-	->	"authentication succeeded" user="admin"
01/31/2001 14:20:07	A INFO auth	-	->	"authentication succeeded" user="admin"

Retrieval Settings Information

Retrieval Mode and Filters

Historical Reference Time: MM/dd/yyyy HH:mm:ss [Fetch More Records](#)

Real Time Poll Interval: 30 seconds

Filter Keywords Operator Events Terms Text

Current Filter:

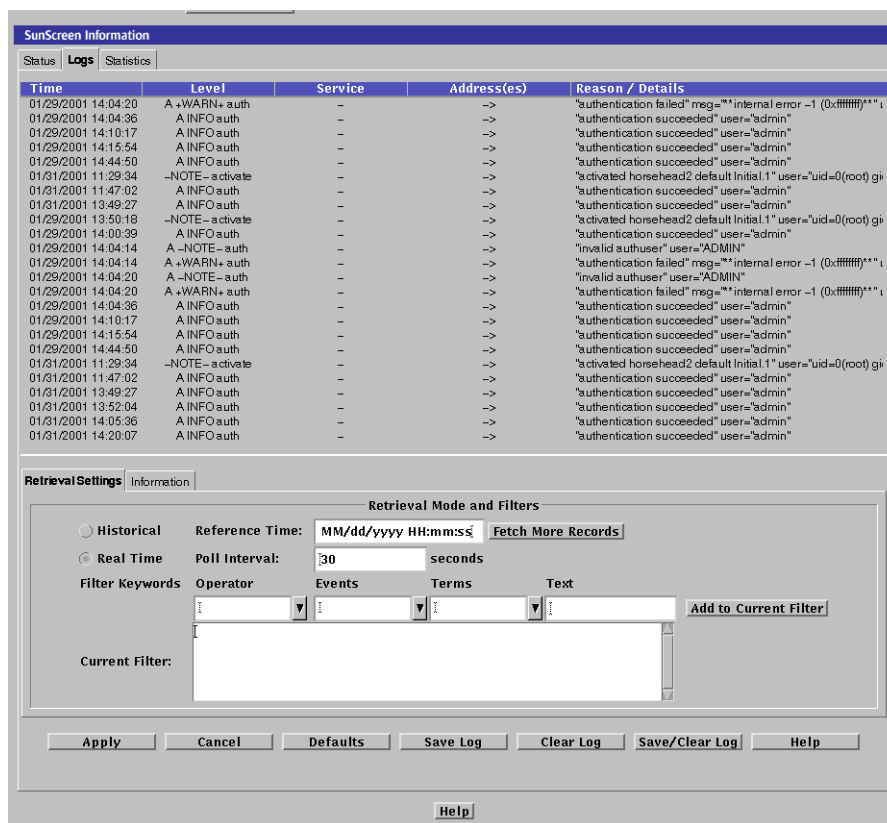
2. Click the Clear Log button at the bottom of the panel.

▼ To Save and Clear the Log

The following steps clear the display of any log records and save the log file.

1. From the Information page, click the Log button.

The Log page appears.



2. Click the Save/Clear Log button.
The Save File dialog box appears.
3. Type the full path (including file name) of the file where you want to store logs.
4. Click the Save button.

Changing the Size of the Log File

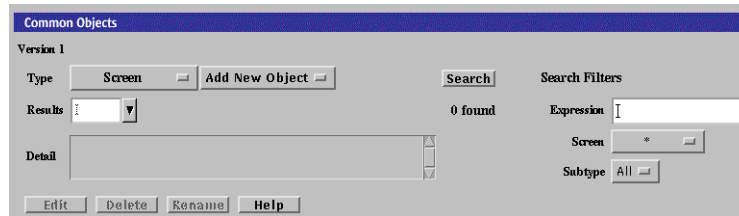
The *global* size of log files is set like other configuration items and controlled by the *LogSize* variable. You can set this variable with the command-line interface but not with the administration GUI; however, you can use the administration GUI to set the

size of the log file for a *specific Screen*. The default log size is 100MB, but it is configurable. If the log file fills up, it will overwrite the oldest data and information can be lost.

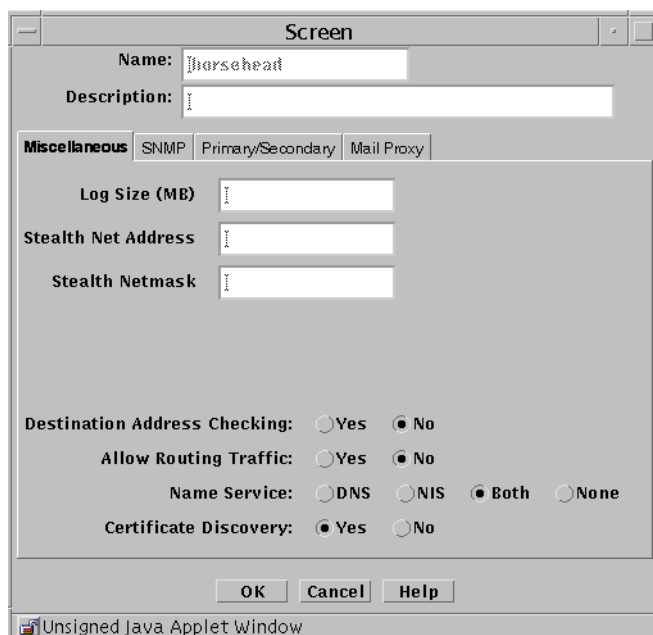
Note – The log file for a Screen is resized only when that Screen is restarted.

▼ To Change the Log File Size for a Specific Screen

1. Select the desired Common Object Type.



2. Click the Search button.
3. Select the entry from the Results area.
4. Click the Edit button.
5. Under the Miscellaneous tab, change the Log Size entry.



6. Click OK
7. Click the Save Changes button at the top of the Panel.
8. Click the Activate Policy button at the top of the panel.
9. Reboot the system.
Your changes to the log file size take effect when you reboot the computer.

Virus Scanning

The SunScreen HTTP proxy can be configured to use the third-party content scanning product InterScan™ from TrendMicro, Inc. See *SunScreen 3.2 Administrator's Overview* for information on using InterScan VirusWall

Using the Command Line Interface

All the SunScreen functionality that is available through the administration GUI is also available through a command line interface. Administering your Screens through the command line can be useful when you want to manage one or more remote Screens or if you use more than one network address.

You can use the command line to access a Screen from its own keyboard when the Screen is being administered locally; this requires that you have superuser (root) access. You can also use the command line to access a Screen from an Administration Station when the Screen is being administered remotely; this requires that you use SKIP or IPsec encryption and an admin user name and password.

For more information on the command line, see “Configuration Editor Reference” in *SunScreen 3.2 Administrator’s Overview*.

Command Summary

The following commands are available at your shell prompt when `/usr/sbin` is included in your `$PATH`. The following table lists the SunScreen UNIX (shell) commands and their descriptions. Many of these commands duplicate administration GUI functions; some provide context for other commands.

TABLE 10-1 SunScreen Command Summary

UNIX Command	Description
<code>ssadm</code>	Primary command line tool for SunScreen administration. <code>ssadm</code> subcommands perform various operations, such as editing and activating a SunScreen configuration and examining the status of a Screen.

TABLE 10-1 SunScreen Command Summary (Continued)

UNIX Command	Description
ss_client	Provide communication between a SunScreen Administration Station and a Screen that is running an earlier SunScreen firewall product release. <code>ss_client</code> is provided only for the purpose of remotely administering such products using the SunScreen system as a remote Administration Station.

Note – The commands used for administering SunScreen SKIP are meant to be run only on a pure Administration Station, not on a Screen. They can be found in “Using the Command-Line Interface” in *SunScreen SKIP User’s Guide, Release 1.5.1*.

UNIX (shell) Commands

ssadm Command

`ssadm` is the primary command line tool for SunScreen administration. `ssadm` has a number of subcommands that perform various operations such as editing and activating a configuration, and examining the status of a Screen.

`ssadm` runs directly on a locally administered Screen, or indirectly from a remote Administration Station that is using SKIP or IPsec to encrypt IP network communications passing between them. See “How SKIP Works” in *SunScreen SKIP User’s Guide, Release 1.5.1* for more information regarding SKIP encryption.

The `ssadm` command resides in the `/usr/sbin` directory. Include this directory in your directory search path to have access to the commands on the local Screen.

Usage:

```
ssadm [-b] [-n] subcommand [parameters...]
```

```
ssadm [-b] [-n] -r remotehost [-F ticketfile] subcommand [parameters...]
```

Options:

- b Allow binary data (instead of text) in standard input and output.
- n Do not read any input from standard input.

- r *remotehost* Access remote Screen using address or hostname *remotehost*.
- F *ticketfile* Use authorization ticket stored in *ticketfile*.

The available `ssadm` subcommands are described in “`ssadm` Subcommand Summary” on page 308.

The `-b` option normally is not needed since those subcommands that process binary data enable the binary mode automatically. For example, `ssadm backup`, `ssadm restore`, `ssadm log`, `ssadm logdump`, and `ssadm patch` handle binary data even if `-b` is not specified.

When `ssadm` is executed locally on the Screen (that is, without the `-r` option) no login or authentication is required, but you must be superuser to have any effect.

When `ssadm` is used with the `-r` option to access a remote Screen, login authentication is required. You must use the `ssadm login` command to get a ticket that is used by subsequent invocations of `ssadm` to allow access to the remote Screen. Normally, the ticket is stored in a *ticketfile*, the name of which can be specified using the `-F` option, or through the `SSADM_TICKET_FILE` environment variable. See the `ssadm login` command for information about ticket files and remote administration using `ssadm`.

▼ To Execute an `ssadm` Command on a Local Screen

- You can configure a local Screen by typing the commands listed in this appendix on the Screen’s keyboard. For example, to activate a policy called *Initial*, you would type:

```
# ssadm activate Initial
```

where `ssadm` is the command you want to execute, `activate` is the name of the `ssadm` subcommand, and *Initial* is the name of the policy you want to activate.

▼ To Execute an `ssadm -r` Command on a Remote Administration Station

- To configure a Screen from a remote Administration Station, precede the subcommands listed in this appendix with `ssadm -r` and the address or hostname of the Screen you want to administer. For example, to activate the policy *Initial* on a remote Screen called *SunScreen1*, you would type:

```
# ssadm -r SunScreen1 activate Initial
```

Logging In to and Out of SunScreen Remotely

If you are using remote administration, you must log in before you can perform most `ssadm` commands.

▼ To Log In to and Out of SunScreen Remotely

1. To log into SunScreen remotely, type the following on the remote Administration Station:

```
# SSADM_TICKET_FILE=$HOME/.ssadmticket
# export SSADM_TICKET_FILE
# touch $SSADM_TICKET_FILE
# chmod go= $SSADM_TICKET_FILE
# ssadm -r SunScreen1 login username password /
WRITE access <E23B344150C702EC>
```

2. To log out of SunScreen remotely, type the following:

```
# ssadm -r SunScreen1 logout
```

ssadm Subcommand Summary

The following table lists the SunScreen `ssadm` subcommands and their descriptions. Many `ssadm` subcommands duplicate administration GUI functions, while others provide a context for other subcommands.

TABLE 10-2 SunScreen `ssadm` Subcommand Summary

<code>ssadm</code> Subcommand	Description
<code>activate</code>	Activate a Screen policy
<code>active</code>	List information about the currently active policy
<code>algorithm</code>	List algorithms supported by SKIP
<code>backup</code>	Write a SunScreen backup file to standard output
<code>certdb</code>	Allows a user to manually administer the two databases of public key certificates used by SKIP and IKE. These databases store long term certificates so that they may be accessed by the key manager.
<code>certlocal</code>	A utility for managing the two local identity databases on a Screen. <code>ssadm certlocal</code> is the primary tool for administering local IDs.

TABLE 10-2 SunScreen `ssadm` Subcommand Summary (Continued)

<code>ssadm</code> Subcommand	Description
<code>certrldb</code>	A utility for managing the certificate revocations lists in the IKE certificate database. <code>ssadm certrldb</code> can add, delete, extract, and list IKE certificates based on the command option specified.
<code>configure</code>	Create an initial SunScreen configuration. <code>ssadm configure</code> , when combined with <code>pkgadd</code> , is equivalent to using the installation wizard graphical user interface.
<code>debug_level</code>	Set or clear the level of debugging output generated by a Screen
<code>edit</code>	Run the SunScreen configuration editor (see “Configuration Editor Reference” in <i>SunScreen 3.2 Administrator’s Overview</i>)
<code>ha</code>	Configure the features of a high availability (HA) Screen
<code>lock</code>	Examine or remove the protection lock that the configuration editor places on a policy file
<code>log</code>	Maintain the Screen log file
<code>logdump</code>	Interpret Screen logs and display their contents
<code>login</code>	Authenticate a user for administrative access through <code>ssadm</code> to a Screen from a remote Administration Station
<code>logmacro</code>	Expands SunScreen <code>logmacro</code> objects
<code>logout</code>	Terminate the session created by <code>ssadm login</code> .
<code>logstats</code>	Print information about the SunScreen log
<code>patch</code>	Install patch, as needed
<code>policy</code>	Create, delete, list, rename Screen policies
<code>product</code>	Print single line describing the SunScreen product in use
<code>restore</code>	Read a backup file from standard input
<code>securid</code>	Configure the client layer of the SecurID system
<code>sys_info</code>	Print a description of running SunScreen software
<code>traffic_stats</code>	Report summary information about the traffic flowing through the SunScreen, classified by interface

You maintain user-controlled data by using the `ssadm edit` subcommand.

To look at or change a policy in some way, invoke the configuration editor and type a series of commands that end with `save` and `quit` requests.

ssadm configure Command

`ssadm configure` is a text-based command line utility for creating an initial SunScreen configuration. `ssadm configure`, combined with `pkgadd`, is the command line equivalent of the installation wizard graphical user interface.

`ssadm configure` interactively queries you with various options for configuring the SunScreen, creates a configuration, stores it under the policy name *Initial*, and activates it. After `ssadm configure` finishes, you can administer the firewall.

Configuration Editor Subcommands

You use the `ssadm edit` subcommands when running the configuration editor, which is responsible for maintaining the SunScreen configuration database.

Note – Be sure to save changes made using commands such as `add`, `del`, `rename`, `renamereference`, `insert`, `replace`, and `move`, before you quit. Run `save` only once, just before the `quit` command to avoid accumulating too many policy versions.

The following table lists the SunScreen configuration editor `ssadm edit` subcommands and their descriptions. Many subcommands duplicate administration GUI functions; the remainder provide context for other subcommands.

TABLE 10-3 SunScreen Configuration Editor (`ssadm edit`) Subcommand Summary

<code>edit</code> Subcommand	Description
<code>add</code>	Create or redefine an entry
<code>add_member</code>	Add a member to a group or list
<code>authuser</code>	Manipulates the list of authorized users (see Table 10-4)
<code>del [ete]</code>	Delete the specified entry of the given TYPE
<code>del [ete]_member</code>	Delete a member from a centralized management group or list
<code>insert</code>	Insert a new object of one of the ordered (indexed) types in a specified position in the corresponding list
<code>jar_hash</code>	Manipulates the list of Jar hashes used by the HTTP proxy
<code>jar_sig</code>	Manipulates the list of Jar signatures used by the HTTP proxy
<code>list</code>	Display all data for all entries or a specific entry of a give TYPE

TABLE 10-3 SunScreen Configuration Editor (`ssadm edit`) Subcommand Summary
(Continued)

edit Subcommand	Description
<code>list_name</code>	Display the set of unique base names and subtype of all of a given TYPE
<code>load</code>	Load a policy into the configuration editor
<code>lock</code>	Lock the policy in anticipation of performing edits
<code>lock_status</code>	Return the status of the lock relative to this editor
<code>mail_relay</code>	Manipulates the list of mail relays used by the SMTP proxy
<code>mail_spam</code>	Manipulates the list of spam domains used by the SMTP proxy
<code>move</code>	Move an indexed entry from its current location in the ordered list to the new location
<code>proxyuser</code>	Manipulates the list of proxy users
<code>quit</code>	Cause the editor to terminate if there are no unsaved changes
<code>QUIT</code>	Cause the editor to terminate even if there are unsaved changes
<code>refer</code>	Determine if a named-object of a given TYPE is referred to in the current policy
<code>referlist</code>	Display a list of all entries in the current policy that refer to a specified named-object of a given TYPE
<code>reload</code>	Discard any and all edits, if made, and reload the data into the editor from the database
<code>rename</code>	Rename a specified named-object of a given TYPE
<code>renamereference</code>	Renames all references to a specified named-object of a given TYPE
<code>replace</code>	Replace an object at a specified index
<code>save</code>	Save all current edits to the policy or common objects
<code>save as</code>	Save the policy rules to a different policy name
<code>search</code>	Search for objects that match specified criteria
<code>vars</code>	The <code>vars</code> command in the configuration editor manipulates variables used for RADIUS configuration. See the section on RADIUS configuration in the "RADIUS User Authentication Details" in <i>SunScreen 3.2 Administrator's Overview</i> for more information
<code>verify</code>	Verifies the currently loaded configuration without saving it

Using the Configuration Editor

The configuration editor lets you edit only one policy at a time. When you are in an editing session, others are unable to edit the same policy, although they can read it. If you modify any of the common objects, other people are unable to modify common objects until you save your changes.

▼ To Edit a Policy

Invoke the configuration editor with the `edit` command, which is a subcommand of `ssadm`, and the name of your policy, such as `Initial`. Once the configuration editor is running, the prompt changes to: `edit>`.

1. For a locally administered Screen, type:

```
# ssadm edit policy_name
```

2. For a remotely administered Screen, type:

```
# ssadm -r Screen_name edit policy_name
```

Working With Policies

▼ To Create a New Policy

1. Use the `ssadm` command to add a new policy using local administration by typing:

```
# ssadm policy -a policy_name
```

2. Use `ssadm -r` to add the same policy using remote administration by typing:

```
# ssadm -r Screen_name policy -a policy_name
```

Note – If you create a new policy, it will not have the administrative access rules necessary for GUI or remote administration. It may be safer to copy an existing, working policy and modify it than to create a new policy.

▼ To Copy a Policy

1. Using local administration, use the `-c` option to copy a policy by typing:

```
# ssadm policy -c policy_name policy_copy_name
```

2. Using remote administration, use the `-c` option with the `ssadm -r` command to copy a policy by typing:

```
# ssadm -r Screen-name policy -c policy_name policy_copy_name
```

▼ To Rename a Policy

1. Using local administration, rename a policy by typing:

```
# ssadm policy -r old_name new_name
```

2. Using remote administration, rename a policy by typing:

```
# ssadm -r Screen_name policy -r old_name new_name
```

▼ To Delete a Policy

1. Using local administration, delete a policy by typing:

```
# ssadm policy -d name
```

2. Using remote administration, delete a policy by typing:

```
# ssadm -r Screen_name policy -d name
```

▼ To Verify a Policy

1. Verify the validity of a policy, for example, *myconfig*, using local administration by typing:

```
# ssadm activate -n myconfig
```

2. Verify the validity of a policy, for example, *myconfig*, using remote administration by typing:

```
# ssadm -r Screen_name activate -n myconfig
```

▼ To Activate a Policy

1. Activate a policy using local administration by typing:

```
# ssadm activate myconfig
```

2. Activate a policy using remote administration by typing:

```
# ssadm -r Screen_name activate myconfig
```

▼ To Back Up Your SunScreen Configuration

1. Using local administration, type the following to back up a policies:

```
# ssadm backup > filename
```

2. Using remote administration, type the following to back up a policies:

```
# ssadm -r Screen_name backup > filename
```

▼ To Restore Your SunScreen Configuration

1. Restore policies using local administration by typing:

```
# ssadm restore < filename
```

2. Restore policies for remote administration by typing:

```
# ssadm -r Screen_name restore < filename
```

Working With Services and Service Groups

The tasks in this section describe how to work with single services and service groups.

▼ To Add a New Single Service

1. Type the following to add the service `ftp-34`, service engine, discriminator, parameters, and description (which is optional) within quotation marks.

In the example below, all you need to type is "PARAMETERS 1200 1200 1" if you do not want to use the default values. See "Services and State Engines" in *SunScreen 3.2 Administrator's Overview* for the default parameters for the state engines

```
edit> add service ftp-34 SINGLE FORWARD ftp PORT 34 PARAMETERS 1200 1200 1
COMMENT "ftp-34 uses port 34 instead of port 21.
Use ftp-34 instead of the supplied ftp service."
```

2. Type the following to see the new service `ftp-34`:

```
edit> list service ftp-34
"ftp-34" SINGLE FORWARD "ftp" PORT 34 PARAMETERS 1200 1200 1
COMMENT "ftp-34 uses port 34 instead of port 21.
Use ftp-34 instead of the supplied ftp service."
```

▼ To Add a New Service Group

Note – SunScreen lets you change the default services in service groups; however, to make troubleshooting easier, it is better to add a new service group that contains the services that you want rather than modify an existing service group.

1. Type the following to add the service group `useful services` and description (which is optional) within quotation marks:

```
edit> add service "useful services" GROUP www archie gopher
COMMENT "A new service group that is used instead of common services."
```

The description will appear in the Service Details field that appears when you choose a service or service group for a policy rule using the Policy Rule Definition dialog box.

2. Type the following to list the new service group, `useful services`:

```
edit> list service "useful services"
"useful services" GROUP "www" "archie" "gopher"
COMMENT "A new service group that is used instead of common services."
```

This procedure needs more information and an accurate example.

▼ To Modify Service Groups

- Add the GROUP again with the modified member list. The new definition overwrites the old definition.

▼ To Rename a Service or Service Group

- Type the following to rename a service or service group without modifying references to it:

```
edit> rename service "useful services" "dmz services"
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To Rename References to a Service

Note – SunScreen lets you rename a single service or a service group. To make troubleshooting easier, do not rename the single services and service groups that are supplied with SunScreen.

- Type the following to rename all references to a service or service group:

For example:

```
edit> renamereference service "useful services" "dmz services"
```

▼ To Delete a Service or Service Group

Note – SunScreen lets you delete a single service or a service group. To make troubleshooting easier, do not delete the single services and service groups that are supplied with SunScreen.

- Type the following to delete a service or service group.

For example, to delete the service group *dmz service* type:

```
edit> del service "dmz services"
```

This command does not check for references to the single service or service group that you are deleting. The changes take effect when you activate the policy whose rules you have edited.

▼ To Check References to a Service or Service Group

To check references to the single service or service group that you want to delete or have deleted:

1. Type the following to find references to the service or service group that you want to delete or have deleted

For example:

```
edit> referlist service "dmz services"
```

This displays a list of all the instances where the service or service group is used.

2. Remove the service or service group if you have not already done so.
3. Edit the rule to remove obsolete references from the rule or rules displayed after typing the command in Step 1.

Addresses, Address Ranges, and Address Groups

The tasks in this section describe how to work with addresses, address ranges, and address groups.

▼ To Add a New Host Address

- Type the following to add the new host address 172.16.1.2 and a description (which is optional) within quotation marks:

```
edit> add address ftp-www HOST 172.16.1.2  
COMMENT "Address of the DMZ host"
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To Add a Range of Addresses

- Type the following to add an address range from 172.16.3.2 to 172.16.3.255 and a description (which is optional) within quotation marks:

```
edit> add address corp RANGE 172.16.3.2 172.16.3.255  
COMMENT "All hosts in corporate"
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To Add an Address Group

- Type the following to add an address group and a description (which is optional) within quotation marks, for example:

```
edit> add address Internet GROUP { corp sales ftp-www } {}  
COMMENT "The ranges corporate and sales and the host ftp-www  
have access to the Internet"
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To Add an Address Range in CIDR Format

- Type the following to add a network group and a description (which is optional) within quotation marks, for example:

```
edit> add address cidr2 RANGE 10.100.253.0/24  
COMMENT "The network group consists of an IP address  
and a mask."
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To Delete an Address, Address Range, or Address List

Note – To make troubleshooting easier, do not delete the names of the addresses, ranges of addresses, and lists of addresses that were defined when SunScreen was installed.

This command does not check for references to the address, range of addresses, or list of addresses that you are deleting.

- Type the following to delete an address, a range of addresses, or a list of addresses, for example:

```
edit> del address host0
```

To have the changes take effect, you must activate the policy.

▼ To Check References to a Deleted Address, Address Range, or Address List

- Type the following to find the reference to an address, a range of addresses, or a list of addresses that you want to delete or have deleted, for example:

```
edit> referlist address host0
```

This displays a list of all the instances where the address, range of addresses, or list of addresses is used. You can now remove the address, range of addresses, or list of addresses from the address list in which it is used and edit the policy rule to remove it from the rule or rules in which it is used.

▼ To Rename an Address, Address Range, or Address Group

Note – To make troubleshooting easier, do not delete or rename the names of addresses, ranges of addresses, or lists of address that were defined when SunScreen was installed.

1. Type the following to rename an address, a range of addresses, or a list of addresses and all reference to it, for example:

```
edit> renamereference address ftp-www DMZ
```

2. Type the following to rename an address, a range of addresses, or a list of addresses only, for example:

```
edit> rename address ftp-www DMZ
```

The changes take effect when you activate the policy whose rules you have edited.

Working With Certificates

Each SKIP certificate object requires a particular Name Space ID (NSID) and the Master Key ID (certificate ID) of the certificate. NSIDs and certificate IDs are described in “Common Objects” in *SunScreen 3.2 Administrator’s Overview*.

- Certificate IDs that use the IP address use the NSID 0 convention with the IP address as the MKID.

- Certificate IDs use the NSID 1 convention with an MKID of 8 hexadecimal digits (32 bits).
- Self-generated certificates use the NSID 8 convention with an MKID of 32 hexadecimal digits (128 bits).

You can add SKIP X.509 keys and certificates from a diskette or file, or from a directory that contains only one set of private key and certificate files.

▼ To Add Private Screen Certificates From a Diskette

Note – You cannot add Screen certificates remotely. To add Screen certificates to Screens that are administrated remotely, go to each Screen in turn and follow the steps to add Screen certificates from a diskette or a file.

1. **Insert the diskette that contains the private certificate into the diskette drive of the Administration Station.**
2. **Mount the diskette by typing:**

```
# volcheck
```

3. **Type the following command, including the path to the directory where the private key and certificate are stored:**

```
# install_skip_keys -icg /floppy/diskette_name
```

4. **Eject the diskette.**

```
# eject diskette_name
```

Note – Store the diskette that contains the private key and public certificate safely and securely. It contains sensitive information that is not encrypted.

5. **Type the following to restart the SKIP key manager to update the certificate database:**

```
# skipd_restart
```

6. **Type the following to name the private key and certificate you have just added, and an optional comment if desired:**

```
edit> add certificate sales-home SINGLE NSID 1 MKID "0xA00050E"  
COMMENT "Use this cert for tunnelling to home from NY"
```

where *sales-home* is the name that you are giving the certificate; 1 is the NSID; A00050E is the certificate ID.

▼ To Add Private Screen Certificates From a Directory

1. Type the following command, including the path to the directory where the private key and certificate are stored:

```
# install_skip_keys -icg /directory_name
```

2. Type the following to restart the SKIP key manager to update the certificate database:

```
# skipd_restart
```

3. Type the following to name the private key and certificate you have just added, and an optional comment if desired:

```
edit> add certificate sales-home SINGLE NSID 1 MKID "0xA00050E"  
COMMENT "Use this cert for tunnelling to home from NY"  
where sales-home is the name that you are giving the certificate; 1 is the NSID; A00050E  
is the certificate ID.
```

▼ To Add Screen Local Identities

You can add Screen local identities only with local administration; therefore, for a remotely administrated Screen, you must gain access to the Screen's shell prompt, for instance with the `rlogin` command.

Note – To use the `rlogin` command, you must first save the local identity and the secret key to separate files. For example, you may have extracted the self-generated certificate ID keys that you generated on a Screen to a diskette (because it is impossible to generate the same key later, should you have to reinstall the SunScreen software). Once you have swapped certificate IDs with a number of peer systems, it becomes difficult to fix things in a timely manner. If this seems cumbersome, use `telnet`, which is more secure than `rlogin`.

SunScreen installation programs re-key the Screen being installed, so you have to add your old keys back into the database before configuring the Screen for virtual private networks (see "Encryption, Tunneling, and Virtual Private Networks" in *SunScreen 3.2 Administrator's Overview* for more information about VPNs).

1. Type the following to use the `skiplocal` command to add the Screen's local identity.

```
# skiplocal -a -T soft -t x509 -n 1 -c certificate_filename -s secret_filename
```

This example shows adding a CA key and certificate. If you are adding a self-generated key and certificate, the value for `-t` is `dhpublic` and the value for `-n` is 8.

2. Type the following to restart the SKIP key manager to update the certificate database:

```
# skipd_restart
```

3. Type the following to name the private key and certificate you have just added, for example:

```
edit> add certificate sales-home SINGLE NSID 1 MKID "0xA000050E"  
COMMENT "certificate for home sales"  
where:
```

- *sales-home* is the name that you are giving the certificate
- *1* is the NSID
- *A00050E* is the MKID

▼ To Add Self-Generated Screen Certificates for Local Administration

The following example illustrates how to generate a global (512-bit) key.

1. Use the `skiplocal` command to create a self-generated Screen certificate.

For example:

```
# skiplocal -k -m 512
```

Note – If you have installed more than one encryption strength, use the `-m` flag followed by the modulus size, in bits, of the encryption for which you want to create a new certificate. The modulus sizes are:

- Global (1024 bits)
- U.S. and Canada Only (2048, 3072, or 4096 bits)

The highest modulus size that works with PC-SKIP in the U.S. and Canada is 2048.

You see the following message on the Screen:

```
generating local secret with 512 modulus size  
It would help the quality of the random numbers if you would  
type 50-100 random keys on the keyboard. Hit return when  
you are done.
```

2. Type 50 to 100 random keys.

As you type the random keys, the number of keys appears on the screen.

3. Press the Return key.

The continuation of the message appears on the screen:

```

100
Format: Hashed Public Key (MD5)
Name/Hash: 3f 3c f9 d0 52 85 a3 be 1e 6d 4e cb e4 9e 49 e7
Not valid Before: Fri Apr 17 17:00:00 1998
Not valid After: Thu Apr 17 17:00:00 2003
g: 2
p: f52aff3ce1b1294018118d7c84a70a72d686c40319c807297aca950cd9969
fabd00a509b0246d3083d66a45d419f9c7cbd894b221926baaba25ec355e92a055f
public key:
9945eb0a204efd9643a3aeb42f80d18a22a194232ef6e18809b4b80ac62271000
b24fbd0a01608a6b3fe92a3ab107efd1970c398cdc2d0f73effea55c1cb0565
Added local identity slot 12

```

4. Type the following to restart the SKIP key manager to update the certificate database:

```
# skipd_restart
```

5. Type the following to add the new certificate and its name to the certificate database, for example:

```

edit> add certificate sales-home SINGLE NSID 8 MKID
"0x3f3cf9d05285a3be1e6d4ecbe49e49e7"
COMMENT "This is the Screen's key for the home sales network."
Because this is a self-generated UDH certificate, the NSID is 8.

```

6. Type the certificate ID:

- a. Run the command `skiplocal -l` command.
- b. Cut the Name (certificate ID) for local ID Slot Name that has the same number that you noted above.
- c. Paste in the command certificate above.

▼ To Add Self-Generated Screen Certificates Using Remote Administration

The example shows generating a global (1024 bit) key.

1. Use the `ssadm -r` command to create a self-generated Screen certificate.

For example:

```
# ssadm -r Screen_name lib/skiplocal -k -m 1024-f
```

Note – You must use the `-f` flag with remote administration. This flag suppresses the prompt to type random keys on the keyboard.

If you have installed more than one encryption strength, use the `-m` flag followed by the modulus size, in bits, of the encryption for which you want to create a new certificate. The modulus sizes are:

- Global (1024 bits)
- U.S. and Canada Only (2048, 3072, or 4096 bits)

The highest modulus size that works with PC-SKIP in the U.S. and Canada is 2048.

The following message appears on the screen:

```
generating local secret with 1024 modulus size
Format: Hashed Public Key (MD5)
Name/Hash: 3f 3c f9 d0 52 85 a3 be 1e 6d 4e cb e4 9e 49 e7
Not valid Before: Fri Apr 17 17:00:00 1998
Not valid After: Thu Apr 17 17:00:00 2003
g: 2
p:
f52aff3ce1b1294018118d7c84a70a72d686c40319c807297aca950cd9969fabd
00a509b0246d3083d66a45d419f9c7cbd894b221926baaba25ec355e92a055f
public key:
9945eb0a204efd9643a3aeb42f80d18a22a194232ef6e18809b4b80ac622710
00b24fbd0a01608a6b3fe92a3ab107efd1970c398cdc2d0f73effea55c1cb0565
Added local identity slot 12
```

2. Type the following to restart the SKIP key manager to update the certificate database:

```
# ssadm -r Screen_name lib/skipd_restart
```

3. Start the editor on the remote Screen.

4. Type the following to add the new certificate and its name to the certificate database.

For example:

```
edit> add certificate sales-home NSID 8 MKID
"0x3f3cf9d05285a3be1e6d4ecbe49e49e7"
COMMENT "This is the Screen's key for the home sales network."
```

Because this is a self-generated UDH certificate, the NSID is 8.

5. Type the certificate ID:

a. Run the `skiplocal -l` command.

b. Cut the Name (certificate ID) for local ID Slot Name that has the same number that you noted above and paste in the command certificate above.

For tunnelling with a remote Administration Station, see the editor command `accessremote`. For tunnelling with encrypted packet filtering, see “Working With Policies” on page 312. Tunnelling is also described in “Encryption, Tunneling, and Virtual Private Networks” in *SunScreen 3.2 Administrator’s Overview*.

▼ To Add Public Certificates from a Diskette or a File

You can do this only with local administration; therefore, for a remotely administrated Screen, you must go to the Screen to add Screen certificates from a diskette or a file.

1. **Insert the diskette that contains the public certificate, if you are using issued certificates, into the diskette drive of the Administration Station.**

You also can add new private keys from a directory that contains only one set of certificate files. If you are adding private certificate from a directory, you do not need this step and step 2.

2. **Mount the diskette by typing:**

```
# volcheck
```

3. **Type the path to the directory where the public certificates are stored and the following command and the name of the directory to add the public certificate, for example:**

```
# /floppy/floppy0/install_skip_keys A00050B
```

This example shows adding a public certificate ID.

4. **If you are using issued certificates, type the following in the terminal window to eject the diskette:**

```
# eject floppy0
```

If you are adding a public certificate from a directory, you do not need this step.

5. **Type the following to name the public certificate you have just added, for example:**

```
edit> add certificate NYcert NSID 1 "0xA00050B"  
COMMENT "NY office public cert"
```

Where *NYcert* is the name that you are giving the certificate, *1* is the NSID, and *A00050B* is the certificate ID. NSIDs and certificate IDs are described in “Common Objects” in *SunScreen 3.2 Administrator’s Overview*.

Each SKIP certificate requires a particular Name Space ID (NSID) and the Master Key ID (certificate ID) of the certificate.

- Issued certificates that use the IP address use the NSID 0 convention with the IP address as the certificate ID.
- Issued certificates use the NSID 1 convention with a certificate ID of 8 hexadecimal digits (32 bit).

- Self-generated certificates use the NSID 8 convention with an certificate ID of 32 hexadecimal digits (128 bits).

Note – The tunnel address can be specified as an option in the rule that uses the certificate or in the remote administration rule.

Using Certificate Groups

These procedures describe how to create and work with certificate groups. The examples in these tasks use a list of U.S. sales offices (`sales-list`) as the certificate group and individual sales offices (such as `sales-il` for the Illinois office).

▼ To Add Certificate Groups

After you have named certificate IDs in the rule, you can group them into logical groups so that you can use a group instead of single names in a rule.

- Use the `GROUP` option to group named certificate IDs.

For example:

```
edit> add certificate sales-list GROUP
{sales-co sales-il sales-tx sales-sca sales-nca} {}
COMMENT "list of U.S. sales offices"
```

▼ To Add a New Member to a Certificate Group

- Use the `add_member` subcommand to add a new member to a certificate group.

For example:

```
edit> add_member certificate sales-list sales-wy
```

▼ To Remove a Member From a Certificate Group

- Use the `del_member` subcommand to remove a member from a certificate group.

For example:

```
edit> del_member certificate sales-list sales-wy
```

▼ To Rename a Certificate or Certificate Group

Note – To make troubleshooting easier, do not rename the certificates that were created when you installed SunScreen.

- Use the `renamereference` subcommand to rename a certificate or certificate group.

For example:

```
edit> renamereference certificate sales-ny sales-northeast
```

When you rename a certificate group using this command, SunScreen checks for all instances in the certificate policy object for the old name and changes them to the new name. It does not rename references in other places, such as administrative rules and policy rules.

▼ To Delete a Certificate or Certificate Group

Note – To make troubleshooting easier, do not delete the certificates that were created when you installed a remotely administered SunScreen.

This command does not check for references to the certificate or certificate group that you are deleting.

- Use the `del` subcommand to delete a certificate or certificate group.

For example:

```
edit> del certificate sales-la
```

▼ To Check References to a Deleted Certificate

- Use the `refer` subcommand to find the reference to a certificate and certificate group that you want to delete or have deleted.

For example:

```
edit> refer certificate sales-la
```

▼ To Check References to a Deleted Certificate Group

- Use the `referlist` subcommand to find the reference to a certificate and certificate group that you want to delete or have deleted, for example:

```
edit> referlist certificate sales-west
```

This displays a list of all the instances in the certificate database where the certificate group is used. You can remove it from the access entries in which it is used and edit any policy rule in which it is used to remove it.

IKE Policy Rule Syntax

For tunneling mode, pre-shared key usage:

```
[SCREEN scrn] svc srcaddr dstaddr \  
IPSEC { AH(authalg1) | ESP(encralg1[, authalg2]) }+ \  
IKE(encralg2, authalg3, oakleygroup, PRE-SHARED, pskey) \  
[SOURCE_SCREEN srcscrn] [DESTINATION_SCREEN dstscrn] \  
[SOURCE_TUNNEL srctunaddr] [DESTINATION_TUNNEL dsttunaddr] \  
ALLOW
```

For tunneling mode, certificate usage:

```
[SCREEN scrn] svc srcaddr dstaddr \  
IPSEC { AH(authalg1) | ESP(encralg1[, authalg2]) }+ \  
IKE(encralg2, authalg3, oakleygroup, authmethod, \  
srccert, dstcert) \  
[SOURCE_SCREEN srcscrn] [DESTINATION_SCREEN dstscrn] \  
[SOURCE_TUNNEL srctunaddr] [DESTINATION_TUNNEL dsttunaddr] \  
ALLOW
```

For tunneling mode, manual key usage:

```
[SCREEN ] \  
IPSEC { AH(spi1, authalg, key1) \  
| ESP(spi2, encralg2, key2 [, spi3, authalg3, key3]) } \  
[SOURCE_SCREEN srcscrn] [DESTINATION_SCREEN dstscrn] \  
[SOURCE_TUNNEL srctunaddr] [DESTINATION_TUNNEL dsttunaddr] \  
ALLOW
```

An alternative syntax follows:

```
[SCREEN scrn] svc srcaddr dstaddr \  
IPSEC { AH(spi1, authalg, key1) | ESP(spi2, encralg2, \  
key2 [, add key "key_des" SINGLE "1234567812345678" \  
edit> add key "key_ah" SINGLE "1234567890abcdef1234567890abcdef"
```


▼ To Add Rules Using Keys Added on Both Screens

Note – See the *SunScreen 3.2 Configuration Examples* manual for an example of how to use the GUI to perform this same function.

1. On Screen 1:

```
1 "telnet" "screen1_host" "screen2_host" IPSEC ESP(0x123,
"DES", "key_des") AH(0x345, "MD5", "key_ah") SOURCE_SCREEN
"screen1" ALLOW 2 "telnet" "screen2_host" "screen1_host"
IPSEC ESP(0x123, "DES", "key_des") AH(0x345, "MD5", "key_ah")
DESTINATION_SCREEN "screen1" ALLOW
```

2. On Screen 2:

```
1 "telnet" "screen2_host" "screen_host1" IPSEC ESP(0x123,
"DES", "key_des") AH(0x345, "MD5", "key_ah") SOURCE_SCREEN
"screen2" ALLOW 2 "telnet" "screen1_host" "screen2_host"
IPSEC ESP(0x123, "DES", "key_des") AH(0x345, "MD5", "key_ah")
DESTINATION_SCREEN "screen2" ALLOW
```

Note – The hex values 0x123, 0x345 are SPI values and must be between 0x000 and 0xFFF.

3. If you choose different algorithms, like 3DES or SHA1, define manual keys of the proper length.

In hex strings, the lengths are respectively.

- CBC 16
- 3DES 48
- MD5 32
- SHA1 40

4. Save and activate the policy.

▼ To Work with IKE Rules with Pre-Shared Key

Note – See the *SunScreen 3.2 Configuration Examples* manual for an example of how to use the GUI to perform this same function.

1. Add the pre-shared secret key on both Screens

```
edit> add key "shared-secret" SINGLE "shared_secret"
```

2. Add rules like the following using keys added on both Screens.

a. On Screen1:

```
1 "telnet" "screen1_host" "screen2_host" IPSEC ESP("DES")
IKE("DES", "MD5", 2, PRE-SHARED, "shared-secret")
SOURCE_SCREEN "screen1" ALLOW 2 "telnet" "screen2_host"
"screen1_host" IPSEC IPSEC ESP("DES") IKE("DES",
"MD5", 2, PRE-SHARED, "shared-secret") DESTINATION_SCREEN
"screen1" ALLOW
```

b. On Screen2:

```
1 "telnet" "screen2_host" "screen1_host" IPSEC ESP("DES")
IKE("DES", "MD5", 2, PRE-SHARED, "shared-secret")
SOURCE_SCREEN "screen2" ALLOW 2 "telnet" "screen1_host"
"screen2_host" IPSEC IPSEC ESP("DES") IKE("DES",
"MD5", 2, PRE-SHARED, "shared-secret") DESTINATION_SCREEN
"screen2" ALLOW
```

3. Save and activate policy.

▼ To Work with IKE Rules with Self-Signed Certificates

Note – See the *SunScreen 3.2 Configuration Examples* manual for an example of how to use the GUI to perform this same function.

1. Generate certificates or private keys on both Screens using `ssadm certlocal`:

a. On Screen1:

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D "C=US,\
O=YourOrg, CN=screen1_name"
```

b. On Screen2:

```
# ssadm certlocal -Iks -m 512 -t rsa-md5 -D "C=US,\
O=YourOrg, CN=screen2_name"
```

2. Export the certificates to the other Screen.

a. On Screen1:

```
# ssadm certdb -I -e "SUBJECT=C=US, \
O=YourOrg, CN=screen1_name" > /tmp/cert1
```

b. On Screen2:

```
# ssadm certdb -I -e "SUBJECT=C=US, \
O=YourOrg, CN=screen2_name" > /tmp/cert2
```

3. Securely transport the file /tmp/cert1 to the Screen1 and /tmp/cert2 to Screen 2.

4. Import the exported certificate to the Screen certificate database.

a. On Screen2:

```
# ssadm certdb -I -a < /tmp/cert1
```

b. On Screen1:

```
# ssadm certdb -I -a < /tmp/cert2
```

5. Add certificate objects on both systems:

```
edit> add certificate "screen1_cert" SINGLE IKE "C=US,  
O=YourOrg,CN=screen1_name"  
edit> add certificate "screen2_cert" SINGLE IKE "C=US,  
O=YourOrg,CN=screen2_name"
```

6. Mark the certificate you imported in Steps 3 and 4 as trusted on both systems using ssadm edit:

a. On Screen 1:

```
edit> add member certificate "IKE manually verified  
certificates" "screen2_cert"
```

b. On Screen 2:

```
edit> >add member certificate "IKE manually verified  
certificates" "screen1_cert"
```

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

7. Add packet filtering rules on both Screens.

a. On Screen1:

```
1."telnet" "screen1_host" "screen2_host" IPSEC ESP("DES")  
IKE("DES", "MD5", 2, RSA-SIGNATURES, "screen1_cert",  
"screen2_cert") ALLOW 2 "telnet" "screen2_host" "screen1_host"  
IPSEC IPSEC ESP("DES") IKE("DES", "MD5", 2, RSA-SIGNATURES,  
"screen2_cert", "screen1_cert") ALLOW
```

b. On Screen2:

```
1."telnet" "screen2_host" "screen1_host" IPSEC ESP("DES")  
IKE("DES", "MD5", 2, RSA-SIGNATURES, "screen2_cert",  
"screen1_cert") ALLOW 2 "telnet" "screen1_host" "screen2_host"  
IPSEC IPSEC ESP("DES") IKE("DES", "MD5", 2, RSA-SIGNATURES,  
"screen1_cert", "screen2_cert") ALLOW
```

8. Refer to the man page of ssadm-certlocal (1M) and ssadm-certdb (1M) for more information.

9. Save and activate the policy.

▼ To Work with IKE Rules with Issued Certificates

Note – See the *SunScreen 3.2 Configuration Examples* manual for an example of how to use the GUI to perform this same function.

1. Generate keys and certificate requests on each Screen.

- a. On Screen1:

```
# ssadm certlocal -Ikc -m 512 -t rsa-md5 -D "C=US, \  
O=YourOrg, CN=screen1_issued"
```

- b. On Screen2:

```
# ssadm certlocal -Ikc -m 512 -t rsa-md5 -D "C=US, \  
O=YourOrg, CN=screen2_issued"
```

2. Bring the requests to a certificate server and have them signed and you should get three files from the CA:

```
screen1_issued.cert: screen1's cert.  
screen2_issued.cert: screen2 's cert  
root.cert: the CA's cert
```

Further detailed instructions on this step depends on your certificate server.

3. Securely transport the files to each system under /tmp and import them.

4. Import three certificates on each Screen:

```
# ssadm certdb -I -a < /tmp/screen1_issued.cert  
# ssadm certdb -I -a < /tmp/screen2_issued.cert  
# ssadm certdb -I -a < /tmp/root.cert
```

In this example, it is assumed you are using a certificate server with CA's subject

```
DN = "C=US, O=YourOrg.com, OU=sunscreen, CN=Certificate Manager"
```

5. Add certificate objects for each Screen and mark the root CA as trusted. On each Screen:

```
edit> add certificate root_cert SINGLE IKE "C=US,  
O=YourOrg.com, OU=sunscreen, CN=Certificate Manager"  
edit> add certificate screen2_issued_cert SINGLE IKE "C=US,  
O=YourOrg, CN=screen2_issued"  
edit> add certificate screen1_issued_cert SINGLE IKE "C=US,  
O=YourOrg, CN=screen1_issued"  
edit> add_member certificate "IKE root CA certificates" root_cert
```

The group name "IKE root CA certificates" is reserved for a trusted Certificate Group.

6. Add packet filtering rules on both Screens.

a. On Screen1:

```
1."telnet" "screen1_host" "screen2_host" IPSEC ESP("DES")
IKE("DES", "MD5", 2, RSA-SIGNATURES, "screen1_issued_cert",
"screen2_issued_cert") ALLOW 2 "telnet" "screen2_host" "screen1_host"
IPSEC IPSEC ESP("DES") IKE("DES", "MD5", 2, RSA-SIGNATURES,
"screen2_issued_cert", "screen1_issued_cert") ALLOW
```

b. On Screen2:

```
1."telnet" "screen2_host" "screen1_host" IPSEC ESP("DES")
IKE("DES", "MD5", 2, RSA-SIGNATURES, "screen1_issued_cert",
"screen2_issued_cert") ALLOW 2 "telnet" "screen1_host" "screen2_host"
IPSEC IPSEC ESP("DES") IKE("DES", "MD5", 2, RSA-SIGNATURES,
"screen2_issued_cert", "screen1_issued_cert") ALLOW
```

7. Save and activate the policy.

Working With Screen Objects

A Screen object controls much of the identity of a Screen. It contains information for your stealth, HA, cluster, and administrative rules. Upon installation, a Screen object that you can edit is created. As with other common objects, when you redefine a Screen object, you must specify all the parameters that you want to set; otherwise the parameters are set to default values.

▼ To Add a Screen

- To add a screen object with a previously-created certificate, using DNS and NIS for Name Service and passing routing information, type the following:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin RIP DNS NIS
COMMENT "The screen that protects the sales office"
```

Note – Adding a comment is optional.

▼ To List the Screens

- Type the following to list all the Screens:

```
edit> list screen
```

▼ To Add an SNMP Receiver to a Screen

- To add an SNMP receiver to the Screen used in the previous procedure:

```
edit> add screen vorticity ADMIN_CERTIFICATE  
vorticity.admin RIP DNS NIS SNMP 10.100.253.200
```

▼ To Add Multiple SNMP Receivers to a Screen

- To add multiple SNMP receivers to the previous Screen object:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin  
ROUTING DNS NIS SNMP 10.100.253.200 10.100.253.254
```

▼ To Add a Time Status Indicator to a Screen

- To add a Time Status Indicator of 30 minutes to the previous Screen object:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin  
ROUTING DNS NIS SNMP_TIMER 30 SNMP 10.100.253.200 10.100.253.254
```

▼ To Remove SNMP Receivers From a Screen

- To remove SNMP receivers from the Screen, do not include them in the Screen object when you set it:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin RIP DNS NIS
```

▼ To Set a Screen to Stealth Mode

- At the editor prompt, type:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin RIP
STEALTH_NET 10.100.253.0 255.255.255.0 COMMENT "The screen in Stealth Mode"
```

Interfaces

For Routing interfaces, there are two types of spoof detection : Complete and Incomplete. On the Interface Definition panel (see “To Add or Edit Interfaces” on page 105), you can set the spoof detection by clicking on the “Spoof Protection” pulldown and making the selection (see “Interface Object” in *SunScreen 3.2 Administrator’s Overview* for information on Complete and Incomplete spoof detection).

For Stealth interfaces, the type of spoof detection is always set to Complete and is not modifiable.

Overlapping Interfaces

Note – The maximum number of stealth interfaces per Screen is 15; however, the number of routing interfaces is virtually limitless.

▼ To Add Interfaces (in Routing Mode)

Before you add a new interface, you must define the address group that the interface will use.

- Type the following to define the interface named `qe0` with no logging, no SNMP alerts, and `ICMP_PORT_UNREACHABLE`:

```
edit> add interface qe0 ROUTING qe0 ICMP PORT_UNREACHABLE
```

▼ To Add Interfaces (in Routing Mode) with a Detailed Log

- Type the following to define the interface `qe0` with detailed logging and SNMP alerts:

```
edit> add interface qe0 ROUTING qe0 LOG DETAIL SNMP ICMP PORT_UNREACHABLE
```

▼ To Remove an Interface

1. List the currently active interfaces by typing:

```
edit> list interface
```

A list of active interfaces is displayed.

2. Find the interface you want to delete and type the following:

```
edit> del interface interface_name
```

Note – Any interfaces that you remove with this procedure remain active until you reactivate a policy.

Adding or Modifying an Authorized User

The authorized user object is used to establish a user identity and provide a mechanism to authenticate it by:

- Password
- SecurID

Configuration Editor authuser Subcommands

To manipulate authorized user objects, use the `authuser` subcommand. `authuser` is unusual in that it uses its own subcommands, which are listed in the following table.

TABLE 10-4 authuser Subcommands

authuser Subcommand	Description
add "name" item...	Creates or overwrites an object. This subcommand takes a complete description of the object, beginning with its name, followed by desired items and subitems.
delete "name"	Deletes a named object.
names [,sortopt]	Displays the names of all authorized user objects. The default is asc. The sort options are: asc ascending order by name (case-sensitive) desc descending order by name (case-sensitive). i asc ascending order by name (case-insensitive). i desc descending order by name (case-insensitive). raw order stored in database.
print [,sortopt] ["name"]	Displays one or more objects. With no object specified, print displays all AUTHUSER objects; specifying a name causes only that object's definition to be displayed.

▼ To Add An Authorized User with Password Authentication

- Type the following to add an authorized user named Audrey Farber for local administration:

```
edit> authuser add admin1 PASSWORD={ "foo" }  
CONTACT_INFO=bj@bobo REAL_NAME="Audrey Farber"  
DESCRIPTION="created for remote administration"
```

Although the password is in plain text when you add a user, it is automatically encrypted, and the password will be displayed as empty quotation marks (""). Enabled is the default.

Note – The description field cannot contain single (' ') or double (" ") quotation marks, as in the description: This user, test_user, is for 'testing' only.

All changes apply to the object immediately; however, for the changes to take effect in policy and administrative access rules, you must activate the policy.

▼ To Add An Authorized User and SecurID Name

1. Type the following to add an authorized user named Audrey Farber for local administration:

```
edit> authuser add admin1 SECURID={ "C2BR" }  
CONTACT_INFO=bj@bobo  
REAL_NAME="Audrey Farber"  
DESCRIPTION="created for local administration"
```

2. Type the following to add an authorized user for remote administration:

```
edit> authuser add admin1 SECURID={ "C2BR" }  
CONTACT_INFO=bj@bobo  
DESCRIPTION="created for remote administration"
```

Enabled is the default. All changes apply to the object immediately; however, for the changes to take effect in policy and administrative access rules, you must activate the policy.

▼ To Display Authorized Users

- Type the following to display a list of authorized user objects as they appear in the database:

```
edit> authuser names,raw
```

The following list is displayed:

```
barbara.bobo  
admin  
melanie.haber  
admin  
audry.farber  
admin
```

▼ To Modify Authorized Users

- Use the `authuser add` subcommand to modify the information for a user.

For example, to change the SecurID name from C3BR to C4BR:

```
edit> authuser add admin1 SECURID={ "C4BR" }  
CONTACT INFO=bj@bobo REAL_NAME="Audrey Farber"  
DESCRIPTION="created for remote administration"
```

The new parameters for the user will overwrite the old parameters. All changes apply immediately.

Modifications to passwords or SecurID passcodes take place immediately. For other changes to take effect in policy and administrative access rules, you must activate the policy.

▼ To Delete an Authorized User

- Use the `authuser delete` subcommand to delete an authorized user, for example:

```
edit> authuser delete admin1
```

All changes apply immediately.

Working With Policy Rules

Policy Rules are ordered, that is, they are executed in the order in which they are listed. You can define them in the order in which you want them to take effect or you can reorder your policy rules after you have defined them.

▼ To Create a Packet Filtering Rule

1. Type the following to add a new rule at the end of a policy with the attributes listed below:

```
edit> add Rule ping * * ALLOW SKIP_VERSION_2 cert-1 cert-2  
DES-CBC RC2-40 MD5 NONE LOG SUMMARY
```

Service ping

Source Address *

Destination Address *

Encryption SKIP Version 2

Encryption Details:

- Source Certificate is cert-1
- Destination Certificate is cert-2
- Key algorithm is DES-CBC
- Data algorithm is RC2-40
- MAC algorithm is MD5
- NONE for the compression (This is the only possible value, at present.)

Action ALLOW

Action Details ALLOW

Compression NONE

Note – All other options assume default values unless specified (for example, SNMP is off).

2. Type the following to add a new rule at a particular position, for example, 1 to add it at the beginning of the policy:

```
edit> insert Rule 1 ping * * ALLOW SKIP_VERSION_2 cert-1 cert-2
DES-CBC RC2-40 MD5 NONE LOG SUMMARY
```

Note – If a filtering rule fails to detect any issued certificate (key) encryption algorithms, it may display the following error message:

An error occurred in detecting the Encryption algorithms.
Please check if skipd process is running.

If this occurs, restart the `skipd` process with the `skipd_restart` command.

▼ To Reorder the Rules

1. Use the `list` subcommand to produce an ordered list of rules for the policy:

```
edit> list rule
```

An ordered list of policy rules is displayed, as shown in this example.

```
1 "www" "*" "*" ALLOW
2 "finger" "*" "*" ALLOW
3 "ftp" "*" "localhost" USER "admin"
ALLOW LOG DETAIL PROXY_FTP
FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "daytime" "localhost" "*" ALLOW
5 "telnet" "*" "*" ALLOW
6 "echo" "localhost" "*" ALLOW
```

2. Use the `move` subcommand to move a policy rule to a new position, for example, from fourth to fifth position:

```
edit> move rule 4 5
```

The list of policy rules now shows the change in the order of the rules.

```
1 "www" "*" "*" ALLOW
2 "finger" "*" "*" ALLOW
3 "ftp" "*" "localhost" USER "admin"
ALLOW LOG DETAIL PROXY_FTP
FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "telnet" "*" "*" ALLOW
5 "daytime" "localhost" "*" ALLOW
6 "echo" "localhost" "*" ALLOW
```

▼ To Delete a Rule

1. Use the `del` subcommand to delete policy rule 5:

```
edit> del rule 5
```

2. Generate the ordered list of policy rules:

```
edit> list rule
```

The new list of policy rules reflects the deletion of rule 5; the former rule 6 now occupies the fifth position.

```
1 "www" "*" "*" ALLOW
2 "finger" "*" "*" ALLOW
3 "ftp" "*" "localhost" USER "admin"
ALLOW LOG DETAIL PROXY_FTP
FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "telnet" "*" "*" ALLOW
5 "echo" "localhost" "*" ALLOW
```

▼ To Edit Any Part of a Rule

You can edit a component or the components of a policy rule by using the following procedure. The example shows how to modify the action.

1. List all the rules in the policy:

```
edit> list rule
```

An ordered list of policy rules is displayed.

```
1 "www" "*" "*" ALLOW
2 "finger" "*" "*" ALLOW
3 "ftp" "*" "localhost" USER "admin"
ALLOW LOG DETAIL PROXY_FTP FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "telnet" "*" "*" ALLOW
5 "echo" "localhost" "*" ALLOW
```

2. Use the `replace` subcommand to edit the policy. For example, to change the action of policy rule 4 from `ALLOW` to `DENY`, insert a new policy rule with the action changed:

```
edit> replace rule 4 telnet * * DENY LOG DETAIL
```

3. List the rules for the policy:

```
edit> list rule
```

The list of policy rules is displayed, showing the rule with the new values replaces the old rule.

```
1 "www" "*" "*" ALLOW
2 "finger" "*" "*" ALLOW
3 "ftp" "*" "localhost" USER "admin"
```

```
ALLOW LOG DETAIL PROXY_FTP
FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "telnet" "*" "*" DENY LOG DETAIL
5 "echo" "localhost" "*" ALLOW
```

The changes take effect when you activate the policy whose rules you have edited.

Modifying Access Rules for GUI Local Administration

▼ To Add an Access Rule for GUI Local Administration

- Use the `add` subcommand with the `accesslocal` argument to add an administrative access rule for local administration.

For example:

```
edit> add accesslocal USER admin3 PERMISSION ALL
```

▼ To Edit an Access Rule for GUI Local Administration

1. List the administrative access rules for local administration:

```
edit> list AccessLocal
```

By default, an admin user is created during installation.

The following approximates the output that is displayed:

```
1 USER "admin" PERMISSION ALL
2 USER "admin3" PERMISSION ALL
```

2. Use the `replace` subcommand to replace an administrative access rule with a new value for a particular user for local administration:

```
edit> replace AccessLocal 2 USER "admin3" PERMISSION STATUS
```

▼ To Delete an Access Rule for GUI Local Administration

Note – Do not delete *all* the administrative access rules.

- Use the `del` subcommand to delete the administrative access rule for local administration.

For example, to delete rule 2, type:

```
edit> del AccessLocal 2
```

Modifying Access Rules for Remote Administration

▼ To Add an Access Rule for Remote Administration

- Use the `add` subcommand with the `accessremote` argument to add an administrative access rule for remote administration:

```
edit> add accessremote USER admin3 * SKIP_VERSION_2 admin-group  
DES-CBC DES-CBC MD5 NONE
```

This administrative access rule allows the access level ALL for the admin 3 user at a remote Administration Station on the Internet to use the GUI and command line to administer the Screen.

Note – Make a note of the encryption parameters if you change them, because they have to match the encryption parameters on the remote Administration Station.

▼ To Edit an Access Rule for Remote Administration

1. List the administrative access rules for remote administration, for example:

```
edit> list accessremote
```

The following approximates the output that is displayed:

```
1 USER "admin" "*" SKIP_VERSION_2 "admin-group" "DES-CBC"  
"DES-CBC" "NONE" "NONE" PERMISSION  
ALL  
2 USER "admin3" "*" SKIP_VERSION_2 "admin-group" "DES-CBC"  
"DES-CBC" "NONE" "NONE" PERMISSION  
ALL
```

Note – Make a note of the encryption parameters if you change them, because they have to match the encryption parameters on the remote Administration Station.

2. Use the `replace` subcommand to replace an administrative access rule with the value or values for a particular user for remote administration with a new value (for example, `STATUS`, for the access level):

```
edit> replace accessremote USER admin3 * SKIP_VERSION_2 admin-group  
DES-CBC DES-CBC NONE NONE PERMISSION STATUS
```

This administrative access rule changes the access level for `admin3` at a remote Administration Station on the Internet to `STATUS`.

▼ To Delete an Access Rule for Remote Administration

Note – Do not delete *all* the administrative access rules.

- Use the `del` subcommand to delete an administrative access rule for remote administration:

```
edit> del accessremote 2
```

Where 2 is the number, in the ordered rules, that you want to delete.

Network Address Translation (NAT)



Caution – If you are using NAT, the when you define a static mapping, be sure that the ranges and groups used in the Source, Destination, Translated Source, and Translated Destination fields are exactly the same size.

▼ To Add ARP Manually

- Use the `arp` command with the `-s` flag if the networks that attach to the Screen on the inside have internal addresses (including any network on which there are addresses to which you want to allow external access):

```
# arp -s IP_Address ether_address pub
```

Note – You must either add this entry each time you reboot the Screen or write your own script to automate this function. If you are administering the Screen remotely, you must either go to the Screen to add this entry or have a rule in your policy that allows you to use a command or protocol such as `telnet` or `ssh` to access the Screen. See also the `arp(1M)` man page.

▼ To Define NAT Mappings

For local administration, you can create either a static or a dynamic NAT entry by specifying either the `STATIC` or `DYNAMIC` option.

1. Use the `add` subcommand to create a static NAT entry that maps an internal address to an external address:

```
edit> add nat STATIC src dest translated_src translated_dest
```

When you define a static mapping, the internal address and external address are both single addresses, but either *can* be a range or a list. In most cases, you should add a reverse entry for static mapping.

2. To create the equivalent dynamic NAT entry, substitute the `DYNAMIC` option for the `STATIC` option.

```
edit> add nat DYNAMIC src dest translated_src translated_dest
```

Note – You can also use a range of addresses or a group of addresses.

3. Activate the policy to have the changes take effect.

▼ To Delete NAT Mappings

- Use the `del` subcommand to delete a NAT entry that maps an internal address to an external address, regardless of whether mapping is static or dynamic:

```
edit> del nat 1
```

The changes take effect when you activate the policy whose rules you have edited.

▼ To List the NAT Mappings

- Use the `list` subcommand to list a NAT entry that maps internal address to a external address, regardless of whether mapping is static or dynamic:

```
edit> list nat
```

You will see a listing that shows type of NAT, the internal address, and the external address:

```
1 STATIC "105-range" "*" "nat-range" "*"

```

Virtual Private Network (VPN)

▼ To Add a VPN Gateway

Setting up a VPN requires you to have a certificate per Screen and to define the address groups involved. For descriptions and concepts of the virtual private network, see "Encryption, Tunneling, and Virtual Private Networks" in *SunScreen 3.2 Administrator's Overview*.

1. At the command line prompt, type:

```
edit> add vpngateway vpn-net addrgrp-a SKIP cert-a KEY
DES-CBC DATA RC4-40 MAC MD5 COMPRESSION NONE
```

Where:

- `vpn-net` is the name of the VPN
- `addrgrp-a` is an address group that uses the following certificate
- `SKIP cert-a` is the certificate

If you are using a tunnel address, append `TUNNEL address_name` to the add/replace.

To setup the VPN completely, you should have all the certificates, address groups, and VPN gateways defined on each Screen. In a VPN configuration that has two networks connected, you would see something like the following:

```
edit> list vpngateway
1 "vpn-net" "addrgrp-a" SKIP "cert-a" KEY "DES-CBC" DATA "RC4-40"
MAC "MD5" COMPRESSION "NONE"
2 "vpn-net" "addrgrp-b" SKIP "cert-b" KEY "DES-CBC" DATA "RC4-40"
MAC "MD5" COMPRESSION "NONE"

```

2. Create an address group to contain the address groups for both networks, for example:

```
edit> add address vpn-grp GROUP { addrgrp-a addrgrp-b } {}
```

3. Define a rule to specify the VPN gateway:

```
edit> add rule common vpn-grp vpn-grp ALLOW VPN vpn-net
```

▼ To Replace a VPN Gateway

VPN gateways are set up in an ordered manner.

- To change values, at the command line prompt, type (for example):

```
edit> replace vpngateway 1 vpn-net addrgrp-a SKIP cert-new KEY  
DES-CBC DATA RC4-40 MAC MD5 COMPRESSION NONE
```

▼ To Remove a VPN Gateway

To remove the VPN gateway, you must delete the rules and VPN object.

- At the command line prompt, type (for example):

```
edit> del vpngateway 1
```

Information, Statistics, and Logs

▼ To View the Information

The `ssadm sys_info` subcommand provides information such as product, system boot time, SunScreen boot time, and version.

1. To display information using local administration, type the following:

```
# ssadm sys_info
```

2. To display the equivalent information using remote administration, use the `-r` flag and specify the name of the remote Screen:

```
# ssadm -r Screen_name sys_info
```

▼ To View the Statistics

The `traffic_stats` option displays information about the traffic flowing through a Screen.

1. **Using local administration, type the following:**

```
# ssadm traffic_stats
```

2. **Using remote administration:**

```
# ssadm -r Screen_name traffic_stats
```

▼ To Set Logsize on a Screen

You can use `LOGSIZE` to set the maximum size of your log file. The values are expressed in Mbytes, where 200 represents 200 Mbytes.

- **At the editor prompt, type:**

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin CDP RIP DNS  
SNMP 10.100.253.200 LOGSIZE 200
```

▼ To Set Up Packet Logging

SunScreen provides flexible logging of packets. A packet can be logged when it matches a policy rule, when it does not match a policy rule, or when it matches a policy rule whose action is DENY.

1. **Configure SunScreen to log packets that do not match any particular policy rule.**
Most frequently, packets are logged because of the DENY action in a rule or because they do not match any policy rule.
2. **Set the type of logging you want in the details for the ALLOW action in a policy rule.**
3. **Set the type of ICMP reject in the details for the DENY action in a policy rule.**
4. **On the Interfaces panel of the Interface page, set logging for packets that are dropped because they do not match any policy rule.**

▼ To Examine Packets

- **Once a log is retrieved, use the `ssadm logdump` command to examine it.**

Examining logged packets can be useful for troubleshooting problems encountered while you set up security policies. For example, when first creating policies, make the default DENY action "log packets." This enables you to review the logs easily. You can also use logging to capture any attempts to break in.

▼ To Display Packets in the Log File

You can examine a saved log file only from the command line.

- **Use the `ssadm logdump` command to display packets in the log file:**

```
# ssadm logdump -i ssadm_log_file
```

ssadm_log_file is the name of a log file that has been downloaded from the Screen.

▼ To View the Log

- **Type the following to view the current log using local administration:**

```
# ssadm log get | ssadm logdump -i -
```

Note – See the `ssadm-logdump` manpage for a list of options.

▼ To Save the Log

1. **Using local administration, use `ssadm log get` to save a log record to a file for local administration:**

```
# ssadm log get > filename
```

2. **Using remote administration use `ssadm` with the `-r` option:**

```
# ssadm -r Screen_name log get > filename
```

▼ To Clear the Log

This action clears the log browser's display of any log records without saving them and clears the SunScreen log file.

1. Using local administration, type the following to clear the log file:

```
# ssadm log clear
```

2. Using remote administration, use `ssadm` with the `-r` option:

```
# ssadm -r Screen_name log clear
```

▼ To Save and Clear the Log

This action saves a log to a file and clears the display of any log records.

1. Using local administration, type the following to save the log to a file and clear the log:

```
# ssadm log get_and_clear > filename
```

2. Using remote administration, use the `ssadm` with the `-r` option:

```
# ssadm -r Screen_name log get_and_clear > filename
```

Setting Up High Availability (HA)

See Chapter 5 and “Encryption, Tunneling, and Virtual Private Networks” in *SunScreen 3.2 Administrator’s Overview* before using the command line to set up HA.

1. To install HA on the Screen designated to be the primary HA Screen, type the following:

```
# ssadm ha init_primary interface
```

This step creates a new HA cluster containing one Screen.

2. To install HA on the Screen designated to be the secondary HA Screen type the following:

```
# ssadm ha init_secondary interface primaryIP
```

Where:

- *interface* is the interface to be used for the HA heartbeat and synchronization
- *primaryIP* is the IP address (on the HA network) of the primary Screen in the cluster

Note – You can receive the following error message after you issue the `ssadm ha init_secondary` command because the primary screen has not sent the policy to the secondary screen. This is normal and the error message can be ignored.

```
Error: No filtering interfaces defined.
```

3. To add the HA secondary Screen to the existing HA cluster, execute the following command on the primary machine in the cluster:

```
# ssadm ha add_secondary secondaryIP
```

Where *secondaryIP* is the IP address (on the dedicated HA network) of the secondary Screen to be added.

Note – After adding an HA secondary Screen and activating your policy, the new secondary Screen may become active. If you need to perform additional administration on the primary Screen, first direct the secondary Screen to become passive so that you can communicate with the primary Screen.

▼ To Allow Non-Administrative Traffic on an HA Network

By default, only administrative traffic is allowed on the HA interface (ping and SunScreen Administration services). This design keeps the network as secure as possible. However, sometimes administrators have some need to open up other services on this private network.

This can be accomplished by adding filtering rules that include the HA network as the destination address. For example, suppose that the dedicated HA network is 172.16.0.0/24. The following policy would allow telnet traffic to and from any address on the HA network.

- Add the filtering rule as follows:

```
edit> list interface qfe0
"qfe0" HA "hanetwork" INCOMPLETE
edit> list address
hanetwork "hanetwork" RANGE 172.16.0.0/24
edit> list rule 1
1 "telnet" "hanetwork" "hanetwork" ALLOW
```

The destination address must be the same network object that is used in the interface definition. An equivalent object with a different name will not work.

For example, the following change would work, since only the source is a newly defined object.

```
edit> add address hanetwork2 RANGE 172.16.0.0/24
edit> replace rule 1 telnet hanetwork2 hanetwork ALLOW
```

However, the below change would not work, since the destination address object is not the same exact object that is defined in the HA interface definition:

```
edit> add address hanetwork2 RANGE 172.16.0.0/24
edit> replace rule 1 telnet hanetwork hanetwork2 ALLOW
```

▼ To Remove an HA Screen

HA setup requires commands that are outside the configuration editor. Removing the HA setup consists of removing the HA_* options from the Screen objects on the appropriate machines. The three steps below assume the following:

```
edit> list screen
"vorticity" MASTER "barotropic" CDP
RIP NIS HA_SECONDARY HA_IP 129.192.1.2
"barotropic" ADMIN_CERTIFICATE "barotropic.admin" CDP
DNS NIS HA_PRIMARY HA_IP 129.192.1.5 HA_ETHER 8:0:20:9e:e0:66
```

1. Remove the HA Screen:

```
edit> del screen vorticity
```

2. Redefine the primary Screen to no longer be an HA-PRIMARY::

```
edit> add screen barotropic ADMIN_CERTIFICATE barotropic.admin CDP DNS NIS
```

3. Save and activate your configuration.

▼ To View HA Information

The next two steps display information such as the current active or passive status of the HA machine in question and the current state of the HA daemon.

1. Using local administration, type the following:

```
# ssadm ha status
```

2. Using remote administration, use the `-r` flag `ssadm` with the `-r` option to display the same information:

```
# ssadm -r Screen_name ha status
```

3. To view the status of all HA machines in a cluster, type the following from the primary HA machine:

```
# ssadm ha status -Z
```

Centralized Management Groups (CMG)

Use the following commands to set up a CMG cluster. Centralized management groups are explained in Chapter 7 and in “Centralized Management Group” in *SunScreen 3.2 Administrator’s Overview*.

▼ To Change a Screen Object to Put It in a Cluster

The example below illustrates a two-machine cluster setup.

- Type the following on both machines in the cluster:

```
edit> add screen sphere ADMIN_CERTIFICATE "sphere.admin"  
CDP RIP NIS LOGSIZE 100  
edit> add screen velocity ADMIN_IP 10.100.105.5 ADMIN_CERTIFICATE  
vorticity.admin KEY"DES" DATA "RC4-40"  
MAC "MD5" COMPRESSION "NONE" MASTER sphere CDP DNS NIS
```

▼ To Remove a Screen from a Cluster

- Type the following on the primary Screen ("sphere" in this example):

```
edit> del screen vorticity
```

Getting Support for SunScreen Products

If you have any support issues, call your authorized service provider. For further information about support, use the following URL to contact Enterprise Services: <http://www.sun.com/service/contacting>.

You can collect useful diagnostic information by saving the output of the SunScreen support commands shown in the following table.

TABLE 10-5 SunScreen Support Commands

Command	Description
config	Brings over configuration files for the active configuration

TABLE 10-5 SunScreen Support Commands (Continued)

Command	Description
date	Sets and gets current time/date
disks	Checks disk space (df -k)
eeeprom	Checks EEPROM settings
findcore	Checks for a core file
help	Provides a list of the available support commands
last	Checks boot history
packages	Checks pkginfo and patch history
procs	Checks processes (ps -elf)
skip	Checks contents of /etc/skip/ directory
stats	Checks the kernel networking statistics (netstat -k)
streams	Checks the STREAMS statistic (netstat -m)
versions	Brings over version information on major SunScreen components

These commands, sent from a remote Administration Station, are used for remote diagnostics.

1. Type the following to start any of these support commands:

a. From a local administration station, type:

```
# ssadm Screen_name lib/support Command_Name
```

b. From a remote administration station, type:

```
# ssadm -r Screen_name lib/support Command_Name
```

2. The following table list additional support commands that are available using lib/Command_Name instead of lib/support::

TABLE 10-6 Other Support Commands

Command	Description
nattables	List the contents of internal NAT tables.
screeninfo	List all of the information about the SunScreen installation including packages installed, patched installed on the system, etc. This command produces copious amounts of data.
statetables	Displays internal protocol state tables

TABLE 10-6 Other Support Commands (Continued)

Command	Description
support help	List the support commands available.

3. Type the following to start any of these other support commands:

a. From a local administration station, type:

```
# ssadm Screen_name lib/Command_Name
```

b. From a remote administration station, type:

```
# ssadm -r Screen_name lib/Command_Name
```

Gathering Data From the Screen

You can use several commands to gather system information from the Screen. This information may be requested by Sun Service, should you encounter problems with your Screen.

Note – These commands should only be used for debugging in conjunction with a support call.

▼ To use the `ssadm lib/statetables` Command

● To see internal statetable information, type:

```
# ssadm lib/statetables
```

▼ To Use the `ssadm lib/screeninfo` Command

This command gathers a complete set of data for your Sun Service representative, including:

- State tables
- ARP table information
- Disk usage
- Streams information
- SunScreen configuration information and files
- Uptime
- SKIP information

- **At the command line prompt, type:**

```
# ssadm lib/screeninfo > output_filename
```

▼ To Use the `ssadm lib/nattables` Command

- **To list the contents of the internal NAT tables, type:**

```
# ssadm lib/nattables
```

▼ To Use the `ssadm lib/support` Command

This command gives you access to the commands in the support directory, all of which are invoked by the `screeninfo` command. However, if you are seeking limited data, you may want to run this command alone.

- **At the command line prompt, type:**

```
# ssadm lib/support subcommand [parameters...]
```

See the following procedure for information on the subcommands or parameters used with this CLI.

▼ To Use the `ssadm lib/support help` Option

- **At the command line prompt, type:**

```
# ssadm lib/support help
```

A list of the subcommnads is displayed.

Troubleshooting

You can use the `ssadm debug_level` command to control the printing of debugging information from the SunScreen kernel.

If you type the command with no arguments, `ssadm debug_level` displays the current debug-level mask. By default, this mask has a value of `1`, which means it reports only significant errors.

If you specify a hexadecimal number as an argument for `ssadm debug_level`, the command sets the kernel debugging mask to that level.

▼ To Use the `ssadm debug_level` Command

1. To list the debugging bit choices, type the following:

```
# ssadm debug_level ?
```

2. Select a `ssadm debug_level` mask by setting all of the debugging bits in which you are interested.

Probably the most useful example of the `ssadm debug_level` debugging bit is `DEFAULT_DROP`.

Installing and Configuring the Netscape Browser from the Command Line

When using the Java Plug-In for Netscape Navigator, follow the instructions in the Netscape release notes. In particular, define the `MOZILLA_HOME` environment variable and include the Netscape installation directory in your `PATH`, so you do not have to type the full path name every time you run Netscape.

▼ To Install and Configure the Netscape Browser

1. Set up an environment for installing and running the Java Plug-In.

- For `sh` or `ksh` users, type:

```
# unset CLASSPATH
# MOZILLA_HOME=/opt/netscape
# PATH=$MOZILLA_HOME:$PATH
# export PATH MOZILLA_HOME
```

- For `csh` users, type:

```
% unsetenv CLASSPATH
% setenv MOZILLA_HOME /opt/netscape
% set path = ( $MOZILLA_HOME $path )
```

2. Install the Java Plug-In by typing:

```
# sh Java_Plugin_File_Name.sh
```

3. Save the `identitydb.obj` file. See “To Save the `identitydb.obj` File” on page 358.

4. Access the SunScreen administration GUI in one of two ways:

- Access the SunScreen administration GUI with no access to local files by typing:

```
# netscape http://screenhost:3852/
```

- Access the SunScreen administration GUI using the Java Plug-In, with access to local files for backup and restore, by typing:

```
# netscape http://screenhost:3852/plugin/
```

5. Set the CLASSPATH environment variable only if you need to install special Java files in Netscape Communicator.

Communicator uses CLASSPATH to find local .class files. If CLASSPATH is set in your environment, only the .jar files and directories specified in the CLASSPATH are searched. If you set your CLASSPATH, you must make sure that each .jar file in \$MOZILLA_HOME/java/classes is listed individually in your CLASSPATH.

▼ To Save the identitydb.obj File

After installing the Java Plug-In, save the identitydb.obj file to distribute to the Administration Stations.

1. Save the file identitydb.obj by going to the following URL:

```
http://localhost:3852/plugin/plugins/
```

2. In Netscape, press mouse button 3 and choose Save Link As.

If your browser does not support this save operation, access identitydb.obj in the /usr/lib/sunscreen/admin/htdocs/plugin/plugins/ directory.

3. Copy the identitydb.obj file onto a diskette to distribute to all Administration Stations.

4. If the identitydb.obj file already exists in its proper location, add SunScreen as an accepted signer.

Operating System	Proper Location
UNIX	\$HOME
Single-user Win95	C:\WINDOWS
Multi-user Win95/98	C:\WINDOWS\PROFILES\username
WinNT	C:\WINNT\PROFILES\username

Note – If the `identitydb.obj` file does not exist, copy the file from the diskette to one of the above locations, then perform Step 4.

About SunScreen Lite

Differences Between SunScreen and SunScreen Lite

SunScreen Lite is a stateful, packet-filtering firewall that utilizes a subset of the features in SunScreen. It is designed to protect individual servers and small work groups.

This manual describes procedures for managing both SunScreen Lite and the full version of SunScreen. When configuring and administering SunScreen Lite, please keep the following differences and similarities in mind.

Supported Features

SunScreen Lite supports the following SunScreen features. A SunScreen Lite firewall can:

- Provide basic packet filtering.
- Administer a Screen from a remote Administration Station.
- Be used in virtual private networks (VPNs).
- Be used for CMG secondary machines.
- Use SunScreen SKIP (Simple Key-Management for Internet Protocols) for encryption.

SunScreen SKIP is included as part of SunScreen Lite and is installed automatically.

Limitations

SunScreen Lite does not support the following SunScreen features. Consequently, a SunScreen Lite firewall:

- Cannot be a member of a high availability (HA) cluster.
- Does not support stealth-mode operation.
- Does not support proxies.
- Can neither create nor be made the primary Screen in a CMG group.
- Only supports two routing interfaces when `ip_forwarding` is enabled on the Screen. Any additional interfaces that are configured on this system will not have filtering rules applied to them. Lite supports virtually unlimited routing interfaces when the Screen is not acting as a router; that is, `ip_forwarding` is turned off. This is ideal for protecting server systems that have multiple interfaces for connectivity, administration, and backup, but that are not routing packets between interfaces
- Cannot support more than ten unregistered IP addresses that can be translated to registered address using Network Address Translation (NAT); it is limited to two NAT rules.
- Ignores the time-of-day field. It makes all rules active while that policy is active.
- Can neither support nor create time objects.
- Can neither support nor create the ADMIN, HA, or STEALTH interfaces.

Quick Start Procedures

This section contains cookbook-style instructions for setting up the following:

- Telnet proxy service with and without proxy user authentication
- FTP proxy service with and without proxy user authentication
- HTTP proxy service
- SMTP proxy service
- Configuring RADIUS Authentication
- Telnet and FTP proxy service with RADIUS user authentication
- SecurID clients supported by SunScreen
- Telnet and FTP proxy service with SecurID user authentication

Telnet Proxy Service Without Proxy User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	none
Authorized user password	none
Backend user name	bu1
Backend Telnet server name	telnet_server
SunScreen proxy name	sunscreen_fw
Client machine name	tiny

▼ To Set Up the SunScreen Environment

1. Add an entry in the `/etc/hosts` file if it is accessible, for example:

```
1.2.3.4 telnet_server
```

2. Type the following to make sure the backend Telnet server is accessible:

```
ping -s telnet_server
```

▼ To Configure the Telnet Proxy Service

Note – There is no need to create an authorized user.

1. Create the proxy user:

- a. In the Common Objects section, select Proxy User from the Type list.

- b. Select New Single from the Add New list.

The Proxy User dialog box appears.

- c. Type a name for this Proxy User in the Name field, for example:

```
pu1
```

- d. Select the User Enabled check box.

- e. Leave the Authorized User Name field empty.

- f. Type a name in the Backend User Name field, for example:

```
bu1
```

- g. Click the OK button.

2. Create a Policy Rule.

- a. Click the Add New button in the Policy Rules area of the Policy Rules page.

The Rule Definition dialog box appears.

- b. Select the following values for each field as follows by clicking the down arrow to display the list:

Service	telnet
Source Address	*
Destination Address	*

Action	ALLOW
PROXY list	PROXY_TELNET

3. Save the changes:

- a. Click the Verify Policy button.
- b. Click the Save Changes button.

4. Test the Telnet Proxy Service

From the client machine:

- a. Make sure the physical connections are good.
- b. Make sure the client machine can access the SunScreen proxy:

```
ping -s sunscreen_fw
```

c. Test the Telnet proxy service:

Command issued	telnet sunscreen_fw
Username@Hostname	pu1@telnet_server
Password	Press the Return key

```
tiny# telnet sunscreen_fw
Trying 70.70.70.1...
Connected to sunscreen_fw.
Escape character is "^]".
SunScreen Telnet Proxy Version 3.2
```

```
Username@Hostname: pu1@telnet_server
Password: <press return>
Trying telnet_server (1.2.3.4) ...
Connected to telnet_server
```

```
SunOS 5.6
```

```
login: bul
Password: bul_pw
```

Telnet Proxy Service With Proxy User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	au1
Authorized user password	au1_pw
Backend user name	bu1
Backend Telnet server name	telnet_server
SunScreen proxy name	sunscreen_fw
Client machine name	tiny

▼ To Set Up the SunScreen Environment

1. Type the following to make sure the backend Telnet Server is accessible:

```
# ping -s telnet_server
```

2. Add an entry in the `/etc/hosts` file if it is accessible. For example:

```
1.2.3.4 telnet_server
```

▼ To Configure the Telnet Proxy Service

1. Create an authorized user:

- a. In the Common Objects section, select Authorized User from the Type list.

- b. Select New from the Add New list.

The Authorized User dialog box appears.

- c. Type a name for this authorized user in the Name field, for example:

```
au1
```

- d. Select the User Enabled check box.

- e. Type the password:

```
au1_pw
```

- f. Select the Enabled check box after the Password field.

- g. Retype the password:

```
au1_pw
```

- h. Click the OK button.

2. Create the Proxy User:

- a. In the Common Objects section, select Proxy User from the Type list.
- b. Select New from the Add New list.
The Proxy User dialog box appears.
- c. Type a name for this Proxy User in the Name field, for example:
pu1
- d. Select the User Enabled check box.
- e. Type the following in the Authorized User Name field:
au1
- f. Type a name in the Backend User Name field, for example:
bu1
- g. Click the OK button.

3. Create a Policy Rule:

- a. Click the Add New button in the Policy Rules area of the Policy Rules page.
The Rule Definition dialog box appears.
- b. Select the following values for each field:

Service	telnet
Source Address	*
Destination Address	*
Action	ALLOW
PROXY list	PROXY_TELNET
- c. Click the OK button.

4. Save the changes:

- a. Click the Verify Policy button.
- b. Click the Save Changes button.

5. Test the Telnet Proxy Service

From the client machine:

- a. Make sure the physical connections are good.

b. Make sure the client machine can access the SunScreen proxy:

```
ping -s sunscreen_fw
```

c. Test the Telnet proxy service:

Command issued	telnet sunscreen_fw
Username	pu1@telnet_server
Password	<i>au1's password</i> , for example, au1-pw. (Password is not seen because it is echo suppressed.)

```
tiny# telnet sunscreen_fw
Trying 70.70.70.1...
Connected to sunscreen_fw.
Escape character is '^]'.
SunScreen Telnet Proxy Version 3.2

Username@Hostname: pu1@telnet_server
Password: au1_pw
Trying telnet_server (1.2.3.4) ...
Connected to telnet_server

SunOS 5.6

login: bu1
Password: au1_pw
```

FTP Proxy Service Without Proxy User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	none
Authorized user password	none
Backend user name	bu1
Backend user password	bu1_pw
Backend FTP server name	ftp_server

SunScreen proxy server name screenshot_fw
Client machine name tiny

▼ To Set Up the SunScreen Environment

Note – The ping command must be enabled in the Rules page before you can perform the following procedure.

1. Type the following to make sure the backend FTP Server is accessible:

```
ping -s ftp_server
```

2. Add an entry in the /etc/hosts file if it is accessible. For example:

```
1.2.3.4 ftp_server
```

▼ To Configure the FTP Proxy Service

Note – There is no need to create an authorized user.

1. Create the proxy user:

- a. In the Common Objects section, select Proxy User from the Type list.

- b. Select New Single from the Add New list.

The Proxy User dialog box appears.

- c. Type a name for this Proxy User in the Name field, for example:

```
pu1
```

- d. Select the User Enabled check box.

- e. Leave the Authorized User Name field empty.

- f. Type a name in the Backend User Name field, for example:

```
bu1
```

- g. Click the OK button.

2. Create a Policy Rule

- a. Click the **Add New** button in the Policy Rules area of the Policy Rules page.

The Rule Definition dialog box appears.

- b. Select the following values for each field:

Service proxy_ftp

Source Address *

Destination Address *

Select Action ALLOW

- c. From the **PROXY** list, select **PROXY_FTP**.

- d. Enable the **FTP** command options, for example:

GET ALLOW

CHDIR ALLOW

PROXY USERS pu1

- e. Click the **OK** button.

3. Save the changes:

- a. Click the **Verify Policy** button.
- b. Click the **Save Changes** button.

▼ To Test the FTP Proxy Service

From the client machine:

1. Make sure the physical connections are good.
2. Use the `ping` command to make sure the client machine can access the SunScreen proxy:

```
# ping -s sunscreen_fw
```

Note – The `ping` command must be enabled in the Rules page before you can perform this procedure.

3. Test the FTP proxy service.

For example, the following values produce the screen output in Example C-1:

Command issued **ftp sunscreen_fw**
User name *pu1@ftp_server*
Password *put_anything@bu1_pw*
 OR:
 <none>@bu1_pw
 For example, *zzz@bu1_pw*
 Password is not seen because it is echo suppressed.

EXAMPLE B-1 Screen Output

```
tiny# ftp sunscreen_fw
Connected to sunscreen_fw.
220- Proxy: SunScreen FTP Proxy Version 3.2
: Username to be given as <proxy-user>'@'<FTP-server-host>
: Password to be given as <proxy-password>'@'<FTP-server-password>
220 Ready.
Name (sunscreen_fw: root): pu1@ftp_server
331- Proxy: Authenticate & connect:
331 Password needed to authenticate 'pu1'.
Password:           <zzz@bu1_pw>
OR
Password:           <@bu1_pw>
230- Proxy:
: Authentication mapped 'pu1' to backend user 'bu1'.
: Connecting to ftp_server (1.2.3.4) - done.
Server: 220 ftp_server FTP server (SunOS 5.6) ready.
Proxy: Login on server as 'bu1'.
Server: 331 Password required for bu1.
Proxy: Supplying password to server.
230 Server: User bu1 logged in.
ftp> ls
```

FTP Proxy Service With Proxy User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	au1
Authorized user password	au1_pw
Backend user name	bu1
Backend user password	bu1_pw

Backend FTP server name	ftp_server
SunScreen proxy server name	sunscreen_fw
Client machine name	tiny

▼ To Set Up the SunScreen Environment

1. Use the `ping` command to make sure the backend FTP Server is accessible:

```
ping -s ftp_server
```

2. Add an entry in the `/etc/hosts` file if it is accessible. For example:

```
1.2.3.4 ftp_server
```

▼ To Configure the FTP Proxy Service

1. Create the authorized user:

- a. In the Common Objects section, select Authorized User from the Type list.

- b. Select New from the Add New list.

The Authorized User dialog box appears.

- c. Type a name for this authorized user in the Name field, for example:

```
au1
```

- d. Select the User Enabled check box.

- e. Type the password:

```
au1_pw
```

- f. Select the Enabled check box after the Password field.

- g. Retype the password:

```
au1_pw
```

- h. Click the OK button.

2. Create a Proxy User:

- a. In the Common Objects section, select Proxy User from the Type list.

- b. Select New from the Add New list.

The Proxy User dialog box appears.

c. Type a name for this Proxy User in the Name field, for example:

pu1

d. Select the User Enabled check box.

e. Type a name in the Authorized User Name field:

au1

f. Type a name in the Backend User Name field, for example:

bu1

g. Click the OK button.

3. Create a Policy Rule:

a. Click the Add New button in the Policy Rules area of the Policy Rules page.
The Rule Definition dialog box appears.

b. Select the following values for each field:

Service	ftp
Source Address	*
Destination Address	*
Action	ALLOW
PROXY list	PROXY_FTP

c. Enable the FTP command options, for example:

GET	ALLOW
CHDIR	ALLOW
PROXY USERS	pu1

4. Click the OK button.

5. Save the changes:

a. Click the Verify Policy button.

b. Click the Save Changes button.

6. Test the FTP Proxy Service

From the client machine:

a. Make sure the physical connections are good.

b. Make sure the client machine can access the SunScreen proxy:

```
# ping -s sunscreen_fw
```

c. Test the FTP proxy service:

Command issued	ftp sunscreen_fw
Username	pu1@ftp_server
Password	For example, au1_pw@bu1_pw (Password is not seen because it is echo suppressed.)

EXAMPLE B-2 Screen Output

```
tiny# ftp sunscreen_fw
Connected to sunscreen_fw.
220- Proxy: SunScreen FTP Proxy Version 3.2
: Username to be given as <proxy-user>'@'<FTP-server-host>
: Password to be given as <proxy-password>'@'<FTP-server-password>
220 Ready.
Name (sunscreen_fw: root): pu1@ftp_server
331- Proxy: Authenticate & connect:
331 Password needed to authenticate 'pu1'.
Password: <au1_pw@bu1_pw>
230- Proxy:
: Authentication mapped 'pu1' to backend user 'bu1'.
: Connecting to ftp_server (1.2.3.4) - done.
Server: 220 ftp_server FTP server (SunOS 5.6) ready.
Proxy: Login on server as 'bu1'.
Server: 331 Password required for bu1.
Proxy: Supplying password to server.
230 Server: User bu1 logged in.
ftp> ls
```

HTTP Proxy Service

Note – User authentication does not apply.

The following information is used in this example:

Backend HTTP Server name	gobaby
Backend HTTP Server URL	gobaby/Sun.Net

SunScreen proxy name	sunscreen_fw
Client machine name	tiny

▼ To Set Up the SunScreen Environment

1. **Disable the HTTP daemon (for example, httpd), if it is running.**
2. **Type the following to make sure the backend HTTP Server is accessible:**

```
ping -s gobaby
```
3. **Add an entry in the /etc/hosts file if it is accessible. For example:**

```
1.2.3.4 gobaby
```

▼ To Configure the HTTP Proxy Service

1. **Create the Proxy User:**
 - a. **In the Common Objects section, select Proxy User from the Type list.**
 - b. **Select New from the Add New list.**
The Proxy User dialog box appears.
 - c. **Type a name for this Proxy User in the Name field, for example:**

```
pu1
```
 - d. **Leave the Authorized User Name field blank.**
 - e. **Leave the Backend User Name blank.**
 - f. **Click the OK button.**
2. **Create a Policy Rule:**
 - a. **Click the Add New button in the Policy Rules area of the Policy Rules page.**
The Rule Definition dialog box appears.
 - b. **Select the following values for each field:**

Service	http
Source address	*
Destination address	*
Action	ALLOW

PROXY list	PROXY_HTTP
Cookies, ActiveX, Java, and SSL	ALLOW/DENY

c. Click the OK button.

3. Save the changes:

a. Click the Verify Policy button.

b. Click the Save Changes button.

4. Test the HTTP Proxy service

From the client machine:

a. Make sure the physical connections are good.

b. Make sure the client machine can access the SunScreen proxy:

```
ping -s sunscreen_fw
```

c. Configure the browser to use the HTTP proxy:

```
HTTP Proxy    sunscreen_fw
```

```
Port          80
```

d. Type the following URL:

```
http://gobaby/Sun.Net
```

The screen output appears on the web page.

SMTP Proxy Service

Note – User authentication does not apply.

▼ To Set Up the SunScreen Environment

1. Configure addresses and rules for DNS servers and address(es) for SMTP server(s) as follows:

```
ssadm edit Initial
edit> add Address dns0 HOST 1.2.3.4
edit> add Address dns1 HOST 1.2.3.5
```



```
edit> add Address dns-servers GROUP { dns0 dns1 } { }
edit> add Address smtp-server HOST ...
edit> add Rule dns localhost dns-servers ALLOW
```

2. Test spam filtering.

The rule below allows any address to all inbound mailboxes, no relay checking.

```
edit> add Rule smtp "*" smtp-server ALLOW PROXY_SMTP RELAY
edit> save
```

3. Type the following to create a basic mail spam list (list of domains and/or addresses which won't be allowed to send mail):

```
ssadm edit Initial mail_spam add spam.com
ssadm edit Initial mail_spam add 0.0.0.0..255.255.255.255
```

Note – For more information on spam control, see “SMTP Proxy” in *SunScreen 3.2 Administrator’s Overview*.

4. Type the following to activate the configuration:

```
ssadm activate Initial
```

This refuses mail from any named host in `spam.com`, any host that has an unregistered address, and any originator name (in MAIL FROM: command) within `spam.com`.

Now a connection from an unregistered host, or from a registered host under the domain `spam.com`, looks like this:

```
% telnet efs 25
Trying 1.2.3.4...
Connected to efs
Escape character is "^]".
455 Smells like ... bacon ... no, spam!
Connection closed by foreign host.
```

The reverse-translated name (or lack thereof) has determined the originator is a *spammer*.

A connection from a registered host not under the domain `spam.com` looks like this:

```
% telnet efs 25
Trying 1.2.3.4...
Connected to efs
Escape character is "^]".
220 efs ESMTP Sendmail 8.7.4/8.7.3;
Thu, 11 Mar 1999 19: 34: 40 -0800 (PST)
helo me.com
250 efs Hello me.com [3.4.5.6],
pleased to meet you
mail from: elvis-lives@spam.com
455 Smells like ... bacon ... no, spam!
```

Connection closed by foreign host.

The connection is aborted because the originating user was determined to be a spammer. `elvis-lives@spam.com` is an alternate syntax for the mailbox.

▼ To Test Relay Blocking

1. **Type the following to replace the previous rule with a rule that checks relaying:**

```
edit> add Rule smtp "*" smtp-server ALLOW PROXY_SMTP
```

This allows only configured domains in inbound mailbox names.

2. **Type the following to create a basic mail relay list (a list of domains and/or hosts which will/will not be allowed as recipient):**

```
ssadm edit Initial mail_relay add good.org
ssadm edit Initial mail_relay add !too.good.org
ssadm edit Initial mail_relay add !too-mailer
ssadm edit Initial mail_relay add plenty.org
```

The `!` prefix indicates that the domain or host is *not* to be allowed; if you are using `csh`, remember to escape the `!`, which is a shell meta-character.

Relay processing first compares the recipient domain(s) to those which are NOTs (that is, begin with `!`); if the recipient is found there, the message is refused.

Second, the recipient domain(s) are compared to the list of OK domains (that is, without `!`); if found, the recipient is allowed.

3. **Activate the configuration.**

This refuses mail to any mailbox in the subdomain `too.good.org` or for the host `too-mailer`, but accepts messages bound for any mailbox in other parts of `good.org`, or any mailbox in `plenty.org` (from `RCPT TO:` command).

This example shows mail for allowed recipients, ending in one which will not be relayed-to:

```
% telnet efs 25
Trying 1.2.3.4...
Connected to efs
Escape character is "^]".
220 efs ESMTTP Sendmail 8.7.4/8.7.3;
Thu, 11 Mar 1999 19: 34: 40 -0800 (PST)
helo me.com
250 efs Hello me.com [3.4.5.6],
pleased to meet you
mail from: me@me.com
250 me@me.com... Sender ok
rcpt to: <johnny.b@good.org>
250 Recipient ok
rcpt to: extra@extra@good.org
250 Recipient ok
```

```
rcpt to: <chinz@plenty.org>
250 Recipient ok
rcpt to: but.not@too.good.org
454 Relay refused
Connection closed by foreign host.
```

The connection was aborted because the recipient would require a forbidden relay operation.

Other examples of relay addresses that will not be allowed are:

- bad1@too-mailer
- bad2@too-mailer@good.org
- bad3@too.good.org@good.org
- @good.org,bad4@too.good.org
- @too.good.org,bad5@ok.good.org

Note – The last two bullet items are examples of older, ARPANET-style path naming, and most modern mail transfer agents (MTA), such as `sendmail`, are not configured to accept them, regardless of whether they pass our relay filtering. Also, mailbox names surrounded by <> are treated as if they there are no <>s.

4. Test default relay.

If there is no configured relay list, the domain name of the SunScreen host itself is used as the allowed domain. For example, if the SunScreen name is `host@domain.com`, the relay checking behaves as if the following command was configured as the entire relay list:

```
ssadm edit Initial mail_relay domain.com
```

The following example shows mail which actually gets through:

```
% telnet efs 25
Trying 1.2.3.4...
Connected to efs
Escape character is "^]".
220 efs ESMTP Sendmail 8.7.4/8.7.3; Thu, 11 Mar 1999 19: 34: 40 -0800 (PST)
helo me.com
250 efs Hello me.com [3.4.5.6], pleased to meet you
mail from: me@me.com
250 me@me.com... Sender ok
rcpt to: you@good.com
250 Recipient ok
rcpt to: really@really.good.org
250 Recipient ok
rcpt to: i-got@plenty.org
250 Recipient ok
rcpt to: good@and.plenty.org
250 Recipient ok
data
354 Enter mail, end with "." on a line by itself
```

Subject: I Love Candy

I really, really love good candy ... yummm! Send me some!

```
.  
250 UAA01234 Message accepted for delivery  
quit  
221 efs closing connection  
Connection closed by foreign host.
```

After the `.` (ending the mail session), the proxy and mailer return to the state where the mailer expects a next message (starting with a `MAIL FROM:` command).

Note – Backslash `\` and end-of-line denote command line continuation.

Configuring RADIUS Authentication

A typical RADIUS configuration uses two Screens, each of which protects the site. With multiple sites, a given site may use the RADIUS server of another site as a backup.

▼ To Configure RADIUS Authentication

1. Identify the RADIUS servers:

```
# ssadm edit Policy  
edit> vars add prg=auth name=RADIUSServers  
VALUES={ host=radius_server_name }  
DESCRIPTION="RADIUS server name(s) or addresses to query"
```

2. Add the node secret used by the RADIUS protocol to secure traffic between the RADIUS client and server:

```
# ssadm edit Policy  
edit> vars add sys=screen_name prg=auth  
name=RADIUSNodeSecret VALUE="xxxxxxxxx"  
Where xxxxxxxxx is the RADIUS Node Secret.
```

3. Add a rule to allow the SunScreen machine to communicate with the RADIUS servers:

```
# ssadm edit Policy  
edit> add rule radius EFS_hostname radius_server_name ALLOW  
edit> save  
# ssadm activate Policy
```

Telnet Proxy Service With RADIUS User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	au1
Authorized user password	au1_pw
Backend user name	bu1
Backend user password	bu1_pw
Backend Telnet server name	telnet_server
SunScreen proxy server name	sunscreen_fw

▼ To Configure the Telnet Proxy Service With RADIUS User Authentication

1. Follow the steps in the previous section, “Configuring RADIUS Authentication” on page 380.
2. Add a rule to enable the Telnet Proxy for a pre-defined RADIUS user:

```
# ssadm edit Policy
edit> Add Rule telnet USER radius ALLOW PROXY_Telnet
edit> save
# ssadm activate Policy
```

3. Test the Telnet Proxy with RADIUS authentication:

Telnet command issued	telnet sunscreen_fw
Username@Hostname	/radius/bu1@telnet_server
Password	bu1_radpw

```
# telnet sunscreen_fw
Username @Hostname: /radius/bu1@telnet_server
Password: bu1_radpw
```

FTP Proxy Service With RADIUS User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	au1
Authorized user password	au1_pw
Backend user name	bu1
Backend user password	bu1_pw
Backend FTP server name	ftp_server
SunScreen proxy server name	sunscreen_fw
Radius user name	bu1
Radius user password	bu1_radpw

▼ To Configure the FTP Proxy Service With RADIUS User Authentication

1. Follow the steps in the section above, "Configuring RADIUS Authentication" on page 380.
2. Configure the FTP Proxy Service:
 - a. Create a Proxy user group, for example, ftp-grp.
 - b. Add predefined users radius and securid to ftp-grp.

```
# ssadm edit Policy
> proxyuser add ftp-grp GROUP
> proxyuser addmember ftp-grp radius
> proxyuser addmember ftp-grp securid
```
 - c. For each user that will be using the FTP Proxy:
 - i. Create a record in the Authorized User database.
 - ii. Create a record in the Proxy User database.

iii. Add the user as member of ftp-grp:

```
# ssadm edit Policy
> authuser add aul PASSWORD=\{ aul_pw \}
> proxyuser add pul auth_user_name=aul backend_user_name=bul
> proxyuser addmember ftp-grp pul
```

This example assumes C shell. The backslash \ before the brackets is the escape key from special characters { and }. For Bourne shell, the backslash is not necessary.

Since there are typically many users to administer, this is a good task to automate with a script.

d. Add a rule to allow the FTP proxy for the proxy user group, ftp-grp.

```
# ssadm edit Policy
edit> Add Rule ftp USER ftp-grp ALLOW PROXY_FTP FTP_GET FTP_CHDIR
edit> save
# ssadm activate Policy
```

3. Test the FTP Proxy with RADIUS authentication:

FTP proxy login	ftp sunscreen_fw
Username@Hostname	bul@ftp_server
Password	bul_radpw@bul_pw

```
# ftp sunscreen_fw
Username@Hostname: radius_user@ftp_server
Password: radius_user_pw@password_at_ftp_server
```

SecurID Clients Supported by SunScreen

SunScreen supports two mechanisms for SecurID clients:

- Install ACE/Agent 3.3 on *each* user desktop.
- Or:
1. Install SunScreen SecurID stub client on the SunScreen machine, which supports Solaris 2.6, Solaris 7, and Solaris 8 operating systems, on both SPARC and Intel platforms.
 - a. As root, install a copy of `sdconf.rec` from the ACE server after it has been configured to have SunScreen as the ACE client.

b. Type the following in the directory containing `sdconf.rec`:

```
# /usr/lib/sunscreen/lib/securid_stubclient_setup sdconf.rec
```

The ACE/Agent 3.3 is supported only on the Solaris 2.6 SPARC platform. It replaces the system login module with an ACE login module. When the Ace/Agent 3.3 is installed on each user desktop, ACE accounting will show that the user is authenticated through the user's desktop.

Note – The EFS SecurID stub client supports Solaris 2.6, Solaris 7, and Solaris 8, on both SPARC and Intel platforms. Install it only on the SunScreen EFS firewall. ACE accounting will show that the users are authenticated through the EFS machine.

▼ To Configure SecurID Authentication

1. Follow ACE documentation to set up the ACE server and configure SecurID users.
2. Install either ACE/Agent 3.3 on each user desktop or the SunScreen SecurID stub client on the EFS machine.
3. Add a rule to allow the SunScreen machine to communicate with the ACE servers:

```
# ssadm edit Policy
edit> Add Rule securid EFS_hostname secureid_server_name ALLOW
edit> save
# ssadm activate Policy
```

Telnet Proxy Service With SecurID User Authentication

▼ To Set Up the Telnet Proxy Service With SecurID User Authentication

The following information is used in this example:

Proxy user name	pu1
Authorized user name	au1
Authorized user password	au1_pw


```
Backend user name          bu1
Backend user password      bu1_pw
Backend Telnet server name telnet_server
SunScreen proxy server name sunscreen_fw
```

1. Follow the steps in “To Configure SecurID Authentication” on page 384.
2. Add a rule to allow telnet proxy for predefined SecurID user:

```
# ssadm edit Policy
edit> Add Rule telnet USER securid ALLOW PROXY_Telnet
edit> save
# ssadm activate Policy
```

3. Test the Telnet Proxy with SecurID Authentication:

```
Telnet proxy login command issued    telnet sunscreen_fw
Username@Hostname                    /securid/bu1@telnet_server
Password                              securid_passcode
```

```
# telnet sunscreen_fw
Username@Hostname: /securid/bu1@telnet_server
Password: securid_passcode
```

FTP Proxy Service With SecurID User Authentication

▼ To Set Up the FTP Proxy Service With SecurID User Authentication

The following information is used in this example:

```
Proxy user name          pu1
Authorized user name      au1
Authorized user password  au1_pw
Backend user name        bu1
```

Backend user password bu1_pw
 Backend FTP server name ftp_server
 SecurID user name bu1
 SecurID user passcode securid_passcode

1. Follow the steps in “To Configure SecurID Authentication” on page 384.

2. Configure the FTP Proxy Service

a. Create a Proxy user group, for example, ftp-grp.

b. Add predefined users radius and securid to ftp-grp:

```
# ssadm edit Policy
> proxyuser add ftp-grp GROUP
> proxyuser addmember ftp-grp radius
> proxyuser addmember ftp-grp securid
```

c. For each user that will be using the FTP Proxy:

i. Create a record in the Authorized User database.

ii. Create a record in the Proxy User database.

iii. Add user as member of ftp-grp:

```
# ssadm edit Policy
> authuser add au1 PASSWORD=\{ au1_pw\}
> proxyuser add pu1 auth_user_name=au1 backend_user_name=bu1
> proxyuser addmember ftp-grp pu1
```

Since there are typically many users to administer, this can be done through a script.

d. Add a rule to allow FTP proxy for proxy user group ftp-grp:

```
# ssadm edit Policy
edit> Add Rule ftp USER ftp-grp ALLOW PROXY_FTP FTP_GET FTP_CHDIR
edit> save
# ssadm activate Policy
```

3. Test the FTP Proxy with SecurID Authentication:

FTP proxy login	ftp sunscreen_fw
Username@Hostname	/securid/bu1@ftp_server
Password	securid_passcode@bu1_pw

```
# ftp sunscreen_fw
Username@Hostname: /securid/bu1@ftp_server
Password: securid_passcode@bu1_pw
```


Glossary

active Screen	Screen in a high availability cluster that is keeping state and passing traffic. There is always exactly one active Screen in a correctly operating high availability cluster. See primary Screen and passive Screen.
address	In networking, a unique code that identifies a node to the network. SunScreen uses IP addresses.
ADP	Algorithm Discovery Protocol. Enables one entity to inform another of the capabilities it supports.
AH	Authentication Header. A mechanism for providing strong integrity and authentication for IP datagrams.
algorithm	Sequence of steps designed to solve a problem or execute a process such as drawing a curve from a set of control points, or encrypting a block of data.
AMI	Authentication Management Infrastructure.
API	application program interface. Set of calling conventions defining how a service is invoked through a software package. An interface between the operating system and application programs, which includes the way the application programs communicate with the operating system, and the services the operating system makes available to the programs.
argument	Item of information following a command. It may, for example, modify the command or identify a file to be affected. Sometimes the term parameter is used.
ATM	asynchronous transfer mode. Transmits data, voice, video, and frame relay traffic in real time. With ATM, digital information is broken up into standard-sized packets, each with the address of its final destination.
attack	Attempted cryptanalysis or an attempt to compromise system security.

authentication	Property of knowing that the claimed sender is in fact the actual sender.
broadcast	Packet delivery system, where a copy of a given packet is distributed to all hosts attached to the network.
CA	See <i>certificate authority</i> .
cache	Buffer of high-speed memory used to store frequently accessed memory or values. A cache increases effective memory transfer rates and processor speed.
CBC	Cipher Block Chaining (see also DES). A mode used to chain a feedback mechanism, which essentially means the previous block is used to modify the encryption of the next block.
CDP	Certificate Discovery Protocol. Request and response protocol used by two parties to transfer certificates.
Centralized Management group	Multiple secondary Screens that are managed by the Centralized Management group's primary Screen. Note that a Screen in a centrally managed group, whether primary or secondary, can also be part of a HA cluster. See HA cluster.
certificate	Data structure that binds the identity of an entity with a public-key value.
certificate authority	Trusted network entity that digitally signs a certificate containing information identifying the user; such as, user's name, issued certificate, and the certificate's expiration date.
certificate identifier (ID)	Generic naming scheme term used to identify a particular self-generated or issued certificate. It effectively decouples the identification of a key for purposes of key lookup and access control from issues of network topology, routing, and IP addresses.
CFB	Cipher Feedback. Uses a block cipher to implement a stream cipher.
cipher	Cryptographic algorithm used for encryption or decryption.
ciphertext	Encrypted message.
cluster	Screens in an HA cluster connected by a high-speed network that work together as if they were one Screen. See high availability.
common objects	Data objects that are relevant to all SunScreen policies. They include: address, screen, state engine, service, interface, certificate, time, and VPN gateway groups.
confidentiality	Property of communicating such that only the sender and the intended recipients know what is being sent, and unintended parties cannot determine what is sent.
configuration	Union of one policy with the common objects to form a complete description of the behavior of one or more Screens.

content filtering	Practice of allowing or disallowing traffic based on the content of the data being sent.
decryption	Process of converting ciphertext back to plaintext.
demilitarized zone	Small protected inside network or subnetwork that provides limited public access to resources such as web servers, FTP servers, and other information resources.
DES	Data encryption standard. A common algorithm for encrypting and decrypting data.
DMZ	See demilitarized zone.
DNS	domain naming system. Distributed name and address mechanism used in the Internet.
DST	Destination addresses.
dynamic packet screening	Process to ALLOW or DENY examined traffic.
dynamic translation	NAT converts a set of internal private addresses into external public addresses. It allows internal hosts to contact external hosts, but cannot be used to allow external hosts to contact internal hosts.
encapsulation	Technique used by layered protocols in which a layer adds header information to the protocol data unit from the layer above. In Internet terminology, for example, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. See tunneling.
encryption	Process of protecting information from unauthorized use by making the information unintelligible. Encryption is based on a code, called a key, which is used to decrypt the information. Contrast with decryption.
ESP	Encapsulating Security Payload. Mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances it can also provide authentication to IP datagrams, depending on which algorithm or algorithm mode is used. It does not provide nonrepudiation and protection from traffic analysis.
Ethernet	LAN that enables real-time communication between machines connected directly through cables.
failover	Process by which a passive Screen in a high availability group becomes the active Screen if the active Screen becomes unavailable.
filter	Program that reads the standard input, acts on it in some way, and then prints the results as standard output.

firewall	Computer situated between your internal network and the rest of the network that filters packets as they go by according to user-specified criteria.
fragmentation	Process of dividing a packet into multiple smaller packets so that they can be sent over a communication link that only supports a smaller size.
FTP proxy	Can be configured to allow or deny specific FTP commands such as put or get.
gateway	A device that connects networks that use different communication protocols. It transfers information and converts it to a compatible format to the receiving network. See virtual private network.
HA	See high availability.
HA cluster	High availability-specific groups. Multiple secondary HA cluster Screens are managed by the primary HA cluster Screen. One Screen in an HA cluster (secondary or primary) is the active Screen that is actively filtering. Additional HA cluster Screens remain passive until one detects the failure of the active HA cluster Screen and takes over the routing and filtering of the network traffic. See high availability.
heartbeat	Periodic message sent between the machines within an HA cluster over a private network to maintain state. If the heartbeat is not detected after a specified interval and number of retries, a passive machine in the HA cluster becomes the active machine. See high availability.
high availability	Consists of one active Screen and at least one passive Screen. If the active Screen fails, a passive Screen takes over the filtering of the network traffic and other functionality of the failed firewall.
host	Name of any device on a TCP/IP network that has an IP address. In SunScreen, host is only used when referring to a source or destination of a packet.
HTTP proxy	Can be configured to ALLOW or DENY Java applets, and ActiveX controls and cookies.
ICMP	Internet Control Message Protocol. IP protocol that handles errors and control messages, to enable routers to inform other routers (or hosts) of IP routing problems or make suggestions of better routes. See ping.
IKE	See Internet Key Exchange.
Initial configuration	When installing SunScreen, the user creates, compiles, and activates a configuration named <code>Initial</code> , which enables a user to connect to the Screen where the configurations used to implement their security policy are built.

integrity	Property of ensuring that data is transmitted from the source to destination without undetected alteration.
interfaces	Describes the physical interface ports of Screen objects.
Internet Key Exchange	The Internet Key Exchange (IKE) protocol is a key management protocol standard that is used in conjunction with the IPSec standard.
Internet Protocol	Suite of protocols within TCP/IP used to link networks worldwide on the Internet. See IP.
IP	Internet Protocol. Network layer protocol for the Internet Protocol suite.
IPsec	An IP security feature that provides robust authentication and encryption of IP packets.
issued certificate	Certificate that is issued by a certificate authority. See self-generated certificate.
JDK	Java Development Kit. Software tools used to write Java applets or application programs.
JRE	Java Runtime Environment.
key	Code for encrypting or decrypting data.
key and certificate diskette	Medium that contains the private key and certificate, and should be kept secure. The identifier for the certificate is on the label.
log browser	Facility in SunScreen administration GUI that enables the display and printing of log messages.
MAC	Message Authentication Code. (Also known as media access control, an IEEE standard.) See authentication.
media access control	(MAC) The lower sublayer of the OSI Reference Model layer 2, the data-link layer. It controls access to a transmission medium such Token Ring, CSMA/CD, Ethernet, and the like.
Message Authentication Code	Message Authentication Code. (Also known as media access control, an IEEE standard.) See authentication.
message transfer agent	The program responsible for delivering email messages from a mail user agent or other MTA.
MIB	Management Information Base. SNMP structure that describes the particular device being monitored. See SNMP.
MTA	See message transfer agentt.
multicast	Special form of broadcast where copies of the packet are delivered to only a subset of all possible destinations.
NAT	See network address translation.

network address translation	Function used when packets passing through a firewall have their addresses changed (or translated) to different network addresses. Address translation can be used to translate unregistered addresses into a smaller set of registered addresses, allowing internal systems with unregistered addresses to access systems on the Internet.
network layer	Third of the seven layers in the ISO model for standardizing computer-to-computer communications.
network mask	Number used by software to separate the local subnet address from the rest of a given IP address.
node	Junction at which subsidiary parts originate or center.
nodename	Name by which the system is known to a communications network. Every system running Solaris is assigned a nodename. The nodename can be displayed using the Solaris <code>uname -n</code> command. Each Screen has a name that is normally the same as the nodename.
nonrepudiation	Property of a receiver being able to prove that the sender of a message did in fact send the message, even though the sender might later want to deny ever having sent it.
NSID	Name space identifier. Used to identify a naming scheme for a SKIP key. See key.
OLTP	Online transaction processing. Handles real-time transactions.
OSI	Open Systems Interconnection. Suite of protocols and standards sponsored by ISO to communicate data between incompatible computer systems.
OSPF	Open shortest path first. A network routing protocol.
packet	Group of information in a fixed format that is transmitted as a unit over communications lines.
parameter	See argument.
passive Screen	Screen in a high availability cluster that is keeping state with the active Screen but not actually passing traffic. A passive Screen will become active if the cluster's active Screen fails. See active Screen.
passphrase	Collection of characters used in a similar manner to, although longer than, password. Letters in both uppercase and lowercase can be used, as well as special characters and numbers. See password.
password	Unique string of characters that a user types as an identification code as a security measure to restrict access to computer systems and sensitive files.
peer	Any functional unit in the same layer as another entity.
PFS	Perfect Forward Secrecy. Captured packets that are decrypted cannot be used to decrypt other packets.

ping	Packet Internet Groper. Program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. See ICMP.
plaintext	Unencrypted message.
plumb	To install and configure a network interface.
Point-to-Point Protocol	PPP (the successor to SLIP) provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.
	TCP/IP connectivity, usually for PCs over a telephone line.
policy	Named set of policy data. For example, when the SunScreen software is first installed, it configures a default policy named <code>Initial</code> .
PPP	See Point-to-Point Protocol.
primary Screen	In a high availability cluster, the Screen that controls the configuration of the cluster. In a centralized management group, the Screen that controls the configuration of the other Screens in the group. Each high availability cluster or centralized management group has exactly one primary Screen. See high availability.
private key	Corresponds to a public key and is never disclosed to the public. See secret key.
protocol	A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.
proxies	Proxies are separate user-level applications and provide content filtering and user authentication. Proxies are used to control the content of various network services. See HTTP proxy, FTP proxy, Telnet proxy, and SMTP proxy.
pseudorandom	Pseudorandom numbers appear random but can be generated reliably on different systems or at different times.
public certificate diskette	Medium that contains only the certificate containing the public key. The identifier for the certificate is on the label.
public-key certificate	A digitally signed data structure containing a user's public key, as well as information about the time and date during which the certificate is valid.
public-key cryptography	Also known as asymmetric key cryptography. In public-key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key (also frequently called a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a

communications network. This protocol provides privacy without the need for the secure channels that a conventional cryptosystem requires.

real time	Event or system that must receive a response to some stimulus within a narrow, predictable time frame, provided that the response is not strongly dependent on highly variable system-performance parameters, such as a processor load or interface.
remote	System in another location that can be accessed through a network.
router	Intermediary device responsible for making decisions about which of several paths network (or Internet) traffic will follow.
routing mode	Routing-mode interfaces have IP addresses and perform IP routing. Routing mode requires that you subnet the network. All proxies are accessed through the transmission control protocol (TCP) and, therefore, can only run on systems with at least one interface configured in routing mode.
rules	Formulas that define a security policy in terms of the common data objects for SunScreen. Policy data include filtering rules, NAT rules, and administration access rules.
Screen-specific objects	Data objects relevant to the policies of one Screen. See common objectscommon objects.
SDNS	Secure Data Network Service.
secondary Screen	Screen that receives its configuration from a primary Screen. Normally, no administration is performed on a secondary Screen. A secondary Screen does, however, maintain its own logs and status, which can be examined. See high availability.
secret key	Corresponds to a public key and is never disclosed to the public. See private key.
self-generated certificate	See self-signed certificate and UDH certificate. Compare with issued certificate.
self-signed certificate	A digitally signed collection of data, whose content can be checked for authenticity, and optionally used to check the authenticity of other digitally signed collections (issued certificate). In SKIP, the CA certificates are self-signed. Obtained out-of-band, they are used as the basis for issued certificate from a CA, no matter how they are obtained
session key	Common cryptographic component to encrypt each individual conversation between two people with a separate key.
SET	Secure Electronic Transaction. Protocol that is an emerging standard for Internet bank card transactions.

shell	Program within which a user communicates with the operating system.
SKIP	Simple Key-Management for Internet Protocols. IP-layer encryption package integrated into SunScreen, which provides a system with the ability to encrypt any protocol within the TCP/IP suite efficiently. Once installed, systems running SunScreen SKIP can encrypt all traffic to any SKIP-enabled product, including SunScreen products.
SMTP	Simple Mail Transfer Protocol. Used on the Internet to route email.
SMTP proxy	TCP/IP protocol that sends messages from one computer to another on a network and is used on the Internet to route email.
SNMP	Simple Network Management Protocol. Network management protocol that enables a user to monitor and configure network hosts remotely.
snoop	Sun Microsystems, Inc. UNIX utility that captures packets from the network and displays their contents.
source code	Uncompiled version of a program written in a language such as C, C++, or Java. The source code must be translated to machine language by a program (the compiler) before the computer can execute the program.
stateful packet filter	Packet filter that bases its decision to allow or deny the packet using both the data in the packet and information (that is, state) saved from previous packets or events. A stateful packet filter has memory of past events and packets.
stateless packet filter	Packet filter that bases its decision to allow or deny a packet using only the data in that packet. A stateless packet filter has no memory of past events and packets.
static translation	Address translation that provides fixed translation between an external address and a private (possibly unregistered) address. It provides a way for external hosts to initiate connections to internal hosts without actually using an external address. See network address translation.
stealth mode	Stealth-mode interfaces do not have IP addresses. They bridge the MAC layer. Stealth mode interfaces partition an existing single network and, consequently, do not permit you to subnet the network. If all of your interfaces are in stealth mode, SunScreen offers optional hardening of the OS, which removes packages and files from the Solaris operating system that are not used by SunScreen.
subnet	In the Internet Protocol, a mechanism to subdivide (registered) networks into locally defined pieces. This technique provides better use of the IP address space while minimizing routing-table complexity. See subnet mask.

subnet mask	Specifies which bits of the 32-bit IP address represent network information. The subnet mask, like an IP address, is a 32-bit binary number: a 1 is entered in each position that will be used for network information and a 0 is entered in each position that will be used as node number information. See node.
SunScreen	Name of the family of security products produced by Sun Microsystems, Inc.
SunScreen SKIP	See SKIP.
TCP	See Transmission Control Protocol .
TCP/IP	Transmission Control Protocol/Internet Protocol. Protocol suite originally developed by the Department for Defense for the Internet. It is also called the Internet protocol suite. SunOS networks run on TCP/IP by default.
Telnet proxy	Enables users of one host to log into a remote host and interact as normal terminal users of that host.
traffic analysis	Analysis of network traffic flow for the purpose of deducing information such as frequency of transmission, the identities of the conversing parties, sizes of packets, flow identifiers used, and the like.
Transmission Control Protocol	The protocol within TCP/IP that governs breaking data messages into packets that are sent using IP, reassembling these packets into the complete message, and verifying the reassembled message as the same as the original data message.
tunnel address	Destination address on the outer (unencrypted) IP packet to which tunnel packets are sent. Generally used for encrypted gateways where the IP address of the host serves as the intermediary for any or all hosts on a network whose topography must remain unknown or hidden from the rest of the world.
tunneling	Process of encrypting an entire IP packet, and wrapping it in another (unencrypted) IP packet. The source and destination addresses on the inner and outer packets may be different.
UDH certificate	Unsigned Diffie-Hellman certificate. UDH public value can be used when entities are named using the message digest of their DH public value, and these names are securely communicated. This term is now mostly replaced by self-signed certificate. See certificate identifier (ID).
UDP	User Datagram Protocol. All CDP communication uses UDP.
unicast	Packet sent to a single destination. Compare broadcast, multicast.
version	Manner in which a policy's historical versions are preserved.
virtual private network	A network with the appearance and functionality of a regular network, but which is really like a private network within a public one.

The use of encryption in the lower protocol layers provides a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers.

VPN

See virtual private network.

VPN gateway

See virtual private network.

Index

Numbers and Symbols

3DES

IKE, 149, 164

IPsec, 148

A

access level

remote access rule, 147

accesslocal, 342

activate, 51

add a screen, 333

Add Filter button, 55

add multiple SNMP receivers to a screen, 334

add self-generated certificate, 322

add SNMP receivers to a screen, 334

adding IKE Rules, 329

address, 44

add, 60, 61

add a host, 60

add range, 64

admin, 60, 183

defining, 60

deleting, 50

destination, 60, 150

external, 152

group, 62

individual, 60

IP, 60, 64, 99, 101, 103, 150, 189, 287

network, 60, 305

new host, 61

address (*continued*)

new range, 65

pre-defined, 60

range, 64

remove, 51, 64, 85

source, 60, 150

tunnel, 163

address group, 51, 62

address list, 60

defining, 62

deleting, 50

address range, 64

defining, 64

deleting, 50

add_secondary, 351

admin certificate, 60

ADMIN interface

SunScreen 3.1 Lite, 362

admin-group certificate, 60, 183

administration

HA, 27

local, 138, 342

remote, 67, 138, 140, 153, 271

administration access rule, 138

adding for local administration, 138

adding for remote administration, 140

encryption, 144

administration GUI, 78, 190, 358

defining VPN gateways, 162

documentation button, 30

instructions, 39

navigation bar, 29

- administration GUI (*continued*)
 - navigation buttons, 29
 - Policies List page, 39
 - Save As button
 - Edit(RO) button, 41
- Administration Station, 60, 183, 305, 358
 - adding an additional, 140, 271
 - remote, 99, 141, 307
- administrative access rule, 22
- Administrative Access tab, 138, 141, 145, 275
- AES
 - IKE, 149, 164
 - IPsec, 148
- algorithm
 - Data, 144, 163
 - Key, 144, 162
 - MAC, 163
- anti-spoofing, 99
- ARP, 191
- arp command, 344
- ARP request, 152, 194
- associate
 - IKE certificate, 74
- authentication, 336
- authentication algorithm, 149
- authentication method, 149
- Authorized User, 44
- authorized user, 336, 339
 - add, 121, 213
- authuser delete subcommandeas, 339

B

- banner, 279
- BLOWFISH
 - IKE, 149, 164
 - IPsec, 148
- broadcast, 57
- Broadcast button, 57
- browser
 - configure for HTTP proxy, 237
 - Internet Explorer, 22
 - log, 285
 - Netscape, 22
 - starting, 26

C

- Centralized Management, 151, 153
- centralized management
 - certificate for Screen, 95
- certificate, 44, 67
 - adding, 78
 - admin, 60, 183
 - admin group, 60, 183
 - associating, 81
 - associating SKIP Certificate, 81
 - .crt file, 81
 - deleting, 328
 - generate
 - SKIP UDH, 76
 - renaming, 327
 - screen object, 95
 - SKIP CA private
 - loading, 78
 - SKIP CA public, 78
 - SKIP UDH, 76
 - Unsigned Diffie-Hellman, 320
- certificate authority signed IKE certificate, 69
- Certificate Discovery Protocol (CDP), 76
- certificate group, 83, 84, 86, 326, 328
- Certificate ID, 162
- Certificate ID field, 275
- certlocal, 330
- check references to a deleted certificate
 - group, 328
- check references to deleted certifiactae, 327
- CIDR, 67
- CIDR Syntax tab, 67
- clear log button, 301
- command line, 305
- common object
 - delete, 50
 - rename, 51
- common objects
 - adding, 46
 - deleting, 50
 - details, viewing and editing, 49
 - editing, 48
 - modifying, 37
 - renaming, 51
 - searching, 47
- configuration
 - editing, 342

- configuration editor, 312
- controls
 - Policies List page, 41
- Current Filter, 297

D

- data algorithm, 144
- date, 279
- day of the week
 - time objects, 127
- DES
 - IKE, 149, 164
 - IPsec, 148
- destination address, 60
- Destination Address Checking, 99
- dialog box
 - screen object Primary/Secondary tab, 95
 - screen object SNMP tab, 93
- distinguished name, 75
- DNS, 190
- dynamic NAT, 345

E

- editing
 - screen object, 90
- editing a Screen object, 92
- editing a screen object
 - Miscellaneous tab, 90
 - Primary/Secondary tab, 95
- editor
 - configuration, 312
- Edit(RO) button, 41
- encryption, 60, 99, 141, 150, 183, 188, 305
 - choosing, 141, 322, 324
 - modulus size, 322, 324
 - SunScreen 3.1 Lite, 361
- encryption algorithm, 149
- end time
 - time objects, 127
- /etc/hosts file, 190
- Events Filter, 297
- exporting IKE certificate, 70

F

- file
 - identitydb.obj, 357
 - log, 300
 - Solaris, 191
- filter
 - add, 55
 - Current, 297
 - delete, 56
 - Events, 297
 - Operator, 297
 - parameters, 57
 - Terms, 297
 - Text, 297
- filter, log viewing, 296
- filtering
 - packet, 22, 188
 - proxy dialog, 45

G

- generate
 - IKE Certificate, 68
- GUI, 78, 140, 190, 358
 - interoperability with command line, 305
 - locale, 28
 - logging in, 27
 - online documentation, 29
 - password, 27, 28
 - starting, with plugin, 26
 - starting, without plugin, 26
 - viewing information, 28

H

- HA
 - and NAT, 191
 - certificate for Screen, 95
 - definition, 189
 - installing, 193, 198
 - remove, 191
 - removing, 209
 - set up, 188
 - SunScreen 3.1 Lite, 362
 - viewing current information about, 279

- HA interface
 - SunScreen 3.1 Lite, 362
- hash, 76
 - Jar, 45
- host, 53
 - HA, 27, 190
 - IP, 60
- HTTP, 45

I

- identity
 - local, 78
- IKE
 - associate, 74
 - certificate authority signed, 69
 - distinguished name, 75
 - common name, 69, 75
 - country, 69, 75
 - organization, 69, 75
 - organizational unit, 69, 75
 - exporting certificate, 70
 - importing certificate, 72
 - issued certificates, 332
 - pre-shared key, 329
 - remote access rule, 145
 - access level, 147
 - self-generated certificate, 69
 - self-signed certificates, 330
- IKE Certificate
 - generating, 68
- IKE Rule Syntax, 328
- importing IKE certificate, 72
- individual servers
 - SunScreen 3.1 Lite, 361
- Information button, 279
- Information page, 279
- init_secondary, 350, 352
- install_skip_keys command, 320, 321
- interface, 27, 44, 51, 103, 293
 - activate, 105
 - define, 60
 - HA, 188
 - HA cluster, 189
 - port, 44
 - statistics, 293

- interface object
 - add or edit, 105
 - ADMIN, 106
 - DISABLED, 106
 - HA, 106
 - removing, 107
 - ROUTING, 106
 - routing, 107
 - STEALTH, 106
 - stealth interface, 109
- interface objects, 103
- interfaces
 - routing mode, 335
 - SunScreen 3.1 Lite, 362
- Internet Explorer, 78, 289, 298
- IP address, 60, 64
- IP host, 60
- IPsec
 - remote access rule, 145, 147
- IPsec key, 88
 - adding, 88
 - key size, 89
 - manually entering, 88
 - random number generator, 88
- issued certificates, 332

J

- Jar
 - hash, 45, 213, 230
 - signature, 45, 230
- Jar hash, 45
- Jar signature, 118
- Java
 - Jar hash, 45
 - Jar signature, 45
- Java Plug-in, 298, 357
- JDK, 117

K

- key, 76
 - secret, 188
 - SunScreen, 78
- Key algorithm, 144

L

- lib/screeninfo, 355
- lib/statetables, 355
- lib/support, 356
- lib/support help, 356
- list a screen, 334
- loading
 - SKIP CA private, 79
 - SKIP CA public, 79
- local certificate, 60, 183
- local identity, 78
- local resources, 23
 - backing up all policies, 23
 - identitydb.obj, 24
 - installing Java plugin, 23
 - loading certificates from a diskette, 23
 - loading Jar signatures, 23
 - restoring all policies, 23
 - saving log files, 23
- log
 - clear, 300
 - save, 298
 - save and clear file, 301
- Log
 - set viewing filter, 285
- log
 - set viewing filter, 279
 - view, 279
- log button, 298
- log size, changing, 303
- Log tab, 282, 295, 296
- log viewing filter, 296
- logdump command, 349

M

- Mail Proxy tab, 220, 222
 - spam, 97
- management information base (MIB), 99
- master key identity (MKID), 320, 321
- MIB, *See* management information base
- Miscellaneous tab, 253, 262, 303
 - editing a screen object, 90
- mode
 - historical, 295
 - log retrieval, 279, 294

- mode (*continued*)
 - real time, 295
 - routing, 152
 - stealth, 152

N

- name service, 190
- name space ID (NSID), 320, 321
- NAT, 22, 60, 150, 191, 344, 346
 - edit mapping, 155
 - mapping, 154, 191
 - reverse rule, 155
 - SunScreen 3.1 Lite, 362
- NAT Mapping
 - dynamic, 150
- NAT mapping
 - static, 150
- NAT rule
 - define, 150
- NAT tab, 150, 153, 155
- nattables, 354
- Netscape, 78, 298, 357
- Netscape Navigator, 289
- network, 22, 64, 152, 190
 - internal, 53
- network address
 - CIDR address, 67
 - network mask, 67
- Network Address Translation, 22, 60, 150
- network element, 44
- network interface, 60, 103
- network protocol, 45
- NIS, 190

O

- Operator Filter, 297

P

- packet
 - broadcast, 57
 - filtering, 22

- packet (*continued*)
 - IP, 150
 - non-broadcast, 57
 - SNMP, 99
 - Packet Filter rules, 130
 - Packet Filtering tab, 133, 165, 225, 257, 267
 - packet logging, setting up, 348
 - password, 27, 28, 305, 336, 337
 - changing, 30
 - password enabled, 33
 - user enabled, 33
 - Policies List page, 39
 - controls, 41
 - policy, 53, 60, 172
 - activate, 51, 105, 107, 336
 - definition, 22
 - Policy Rules page
 - panel tabs, 132
 - port
 - add, 56
 - delete, 56
 - interface, 44
 - pre-shared key, 329
 - Primary/Secondary tab, 202, 204, 249, 253, 255, 262
 - editing a Screen object, 95
 - protocol, 53
 - network, 45
 - proxies, 362
 - SunScreen 3.1 Lite, 362
 - proxy
 - databases, 213
 - FTP, 233
 - HTTP, 236
 - set up, 212
 - SMTP, 236
 - TELNET, 235
 - use, 212
 - user, 45
 - user, add, 215

R

- random keys, entering, 322

Registry

- addresses, address ranges, address lists, 317, 319
 - authorized users, 336, 339
 - certificates, 319, 328
 - services and service groups, 317
- Rename button, 52
- Retrieval Settings tab, 295
- RIP, *See* routing traffic
- rip service, 57
- rlogin command, 321, 345
- routing, 194
- Routing Interface, 107
- routing traffic, 99
- rule, 60
 - activate, 105, 107
 - add new, 135
 - Administrative Access, 22
 - creating and managing, 130
 - deleting, 137, 341
 - modifying, 130
 - moving, 136
 - policy, 22
 - time-dependent, 45
 - view and edit details, 133

S

- Save As button, 41
- save log button, 299
- save/clear log button, 302
- Screen, 26, 45, 51, 59, 60, 64, 99, 152, 183, 235, 295, 305
 - adding certificate, 67, 78
 - administer, 172
 - certificate for in centralized management group, 95
 - certificate for in HA cluster, 95
 - HA active, 188
 - HA cluster, 189
 - HA passive, 188
 - primary, 242
 - secondary, 242
 - screen object
 - certificate, 95
 - editing, 90

- screen object (*continued*)
 - Mail Proxy tab, 97
 - Miscellaneous tab, 90, 92
 - Primary/Secondary tab, 95
 - Primary/Secondary tab dialog box, 95
 - SNMP tab dialog box, 93
- screen objects, 90
 - adding, 98
 - log size, 98
 - routing traffic, 99
 - stealth interface, 99
- screeninfo, 354
- Search button, 50
- SecurID, 336, 338
- self-generated IKE certificate, 69
- self-signed certificates, 330
- service, 45, 191
 - add, 53
 - checking references to, 316
 - default values, 53
 - new group, 58
 - predefined, 53
- service group
 - add, 57
 - checking references to, 316
 - deleting, 316
 - modifying, 315
 - predefined, 53
 - renaming, 316
- signature
 - Jar, 45
- SKIP, 44, 242, 293, 305
- skip, 354
- SKIP
 - and NAT, 150
 - key manager, 322, 323, 324
 - statistics, 293
 - SunScreen 3.1 Lite, 361
- SKIP statistics, 293
- SKIP UDH, 76
 - level of encryption, 78
- skipd_restart command, 272, 321, 322
- skiplocal command, 321, 324
- small work groups
 - SunScreen 3.1 Lite, 361
- SNMP
 - timed status indicator, 92
 - SNMP alert receiver, 99
 - add, 100, 102
 - add trap receiver, 99
 - delete trap, 99
 - deleting, 101
 - set timer, 99
 - SNMP receivers
 - adding multiples, 334
 - adding to a screen, 334
 - SNMP tab, 99, 100, 101, 102
 - editing a screen object, 92
 - SNMP traps, supported, 94
 - source address, 60
 - Spam, 218, 219, 236
 - delete, 221
 - spam
 - Mail Proxy tab, 97
 - ssadm, 306
 - activate a policy, local administration, 314
 - activate a policy, remote administration, 314
 - adding a policy, local administration, 312
 - adding a policy, remote administration, 312
 - authuser subcommands
 - add, 337
 - add an authorized user and SecurID name, 338
 - add an authorized user with passwoerd authentication, 337
 - delete, 337
 - delete authorized users, 339
 - display authorized users, 338
 - modify authorized users, 338
 - name, 337
 - print, 337
 - backup configuration, local administration, 314
 - backup configuration, remote administration, 314
 - copy a policy, local administration, 313
 - copy a policy, remote administration, 313
 - debug_level, 357
 - delete a policy, local administration, 313
 - delete a policy, remote administration, 313
 - edit subcommands, 310
 - accesslocal, 342
 - add, 310, 315, 317, 318, 322
 - add a network group, 318

ssadm, edit subcommands (*continued*)

- add a range of addresses, 317
- add a screen, 333
- add access rule, local administration, 342
- add access rule, remote administration, 343
- add an address group, 318
- add certificate, 320, 321, 324
- add certificate groups, 326
- add host address, 317
- add interfaces in routing mode, 335
- add interfaces with detailed log, 336
- add member to a certificate group, 326
- add multiple SNMP receivers to a screen, 334
- add NAT mapping, dynamic, 345
- add NAT mapping, static, 345
- add new service group, 315
- add new single service, 315
- add private key, 322
- add public certificate, 325
- add self-generated certificate, 322
- add SNMP receivers to a screen, 334
- add time status indicators to a screen, 334
- add VPN gateway, 346
- add_member, 310, 326
- authuser, 310
- change a screen object to put it in a cluster, 353
- check references to a deleted address, 319
- check references to a deleted address list, 319
- check references to a deleted address range, 319
- check references to a deleted certificate group, 328
- check references to a service or service group, 316
- check references to deleted certificate, 327
- create packet filtered rule, 339
- del, 316, 318, 327
- del[ete], 310
- delete a certificate or certificate group, 327

ssadm, edit subcommands (*continued*)

- delete a service or service group, 316
- delete access rule, local administration, 342
- delete access rule, remote administration, 344
- delete an address, 318
- delete an address list, 318
- delete and address range, 318
- del[ete]_member, 310
- delete NAT mapping, 345
- delete rule, 341
- del_member, 326
- edit access rule, local administration, 342
- edit access rule, remote administration, 343
- insert, 310
- jar_hash, 310
- jar_sig, 310
- list, 310, 315
- list a screen, 334
- list NAT mapping, 346
- list rule, 341
- list_name, 311
- load, 311
- lock, 311
- lock_status, 311
- mail_relay, 311
- mail_spam, 311
- move, 311
- proxyuser, 311
- QUIT, 311
- quit, 311
- refer, 311, 327
- referlist, 311, 316, 319, 328
- reload, 311
- remove a member from a group, 326
- remove a screen from a cluster, 353
- remove an HA screen, 352
- remove an interface, 336
- remove SNMP receivers from a screen, 334
- remove VPN gateway, 347
- rename, 311, 316
- rename a address, 319
- rename a certificate or certificate group, 327

ssadm, edit subcommands (*continued*)

- rename a service or service group, 316
- rename an address group, 319
- rename an address range, 319
- rename reference, 319
- rename references to a service, 316
- renamereference, 311, 316, 319, 327
- reorder rules, 340
- replace, 311
- replace part of rule, 341
- replace VPN gateway, 347
- save, 311
- save as, 311
- search, 311
- set a screen to stealth mode, 335
- set logsize, 348
- vars, 311
- verify, 311
- f, 324
- ha subcommands
 - add_secondary, 351
 - init_secondary, 350
 - redefine primary screen, 352
 - set up high availability, 350
 - status, 352
 - view HA status, 352
- lib/screeninfo, 355
- lib/statetables, 355
- lib/support, 356
- lib/support help, 356
- log subcommands
 - clear log, 349
 - save and clear log, 350
 - save log, 349
- logdump command
 - examine packets, 349
- logdump subcommands
 - display packets in log file, 349
 - view log, 349
- on local screen, 307
- on remote station, 307
- r, 323
- remote log in, 308
- remote log out, 308
- rename a policy, local administration, 313
- rename a policy, remote administration, 313
- restore policies, local administration, 314

ssadm, logdump subcommands (*continued*)

- restore policies, remote administration, 314
- subcommand
 - activate, 308
 - active, 308
 - algorithm, 308
 - backup, 308
 - certdb, 308
 - certlocal, 308
 - configure, 309
 - debug, 309
 - edit, 309
 - ha, 309
 - lock, 309
 - log, 309
 - logdump, 309
 - login, 309
 - logmacro, 309
 - logout, 309
 - logstats, 309
 - patch, 309
 - policy, 309
 - product, 309
 - restore, 309
 - securid, 309
 - summary, 308
 - sys_info, 309
 - traffic_stats, 309
- verify a policy, local administration, 313
- verify a policy, remote administration, 314
- ssadm options
 - b, 306
 - F, 307
 - n, 306
 - r, 307
- start time
 - time objects, 127
- state engine, 53
- statetables, 354
- static mapping
 - define, 155
- static NAT, 153, 345
- statistics, 279
 - interface, 293
- Statistics tab, 290, 293
- Status page, 281
- Status tab, 280

- STEALTH interface
 - SunScreen 3.1 Lite, 362
- stealth mode
 - SunScreen 3.1 Lite, 362
- stealth mode, setting, 335
- subnetwork, 64
- SunScreen 3.1 Lite, 361, 362
 - ADMIN interface, 362
 - encryption, 361
 - HA, 362
 - HA interface, 362
 - individual servers, 361
 - limitations, 362
 - NAT, 362
 - number of interfaces, 362
 - small work groups, 361
 - STEALTH interface, 362
 - stealth mode, 362
 - time-of-day rules, 362
- SunScreen 3.1 Lite compared with SunScreen, 361
- SunScreen banner, 279
- SunScreen compared with SunScreen 3.1 Lite, 361
- SunScreen EFS 3.0
 - resources, 17
- SunScreen Key, 78
- superuser, 305
- support, 355
- support command
 - config, 353
 - date, 354
 - disks, 354
 - EEPROM, 354
 - findcore, 354
 - last, 354
 - nattables, 354
 - packages, 354
 - procs, 354
 - screeninfo, 354
 - skip, 354
 - statetables, 354
 - stats, 354
 - streams, 354
 - support, 355
 - versions, 354
- Syntax, IKE rules, 328

- sys_info command, 347
- system information, 347

T

- tabs
 - Administrative Access, 138, 141, 145, 275
 - CIDR Syntax, 67
 - Log, 282, 295, 296
 - Mail Proxy, 220, 222
 - Miscellaneous, 253, 262, 303
 - NAT, 150, 153, 155
 - Packet Filtering, 133, 165, 225, 257, 267
 - Primary/Secondary, 202, 204, 249, 253, 255, 262
 - Retrieve Settings, 295
 - SNMP, 99, 100, 101, 102
 - Statistics, 290, 293
 - Status, 280
 - VPN, 160, 161
- Terms Filter, 297
- Text Filter, 297
- time, 45, 279
- time objects, 362
 - creating, 125
 - day of the week, 127
 - define, 125
 - end time, 127
 - example of time object, 125
 - start time, 127
 - SunScreen 3.1 Lite, 362
- time status indicators, 334
- timed status indicator, 99
 - SNMP, 92
- time-of-day rules
 - SunScreen 3.1 Lite, 362
- traffic statistics, 293
- traffic_stats command, 348
- trap receiver, 99
- tunnel, 150

U

- Unsigned Diffie-Hellman certificate,, *See* certificate, Unsigned Diffie-Hellman

user
 admin, 27, 28
 authorized, 45, 121, 213, 216, 336, 339
 proxy, 45, 121, 213

V

version, 279
Virtual Private Network, 22, 150
virus scanning, 304
VPN, 22, 321
 add gateway, 159
VPN tab, 160, 161
vpngateway, 346

