



Administration Guide

SunScreen EFS™ 3.0

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

Part No. 805-7745-11
August 1999, Revision B



Copyright 1999 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 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, SunSoft, SunDocs, SunExpress, 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.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

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 1999 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etats-Unis. 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 des systèmes 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, SunSoft, SunDocs, SunExpress, 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 REPENDRE 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.



Please
Recycle



Adobe PostScript

Contents

Who Should Use This Book	xxiii
How This Guide Is Organized	xxiv
Ordering Sun Documents	xxiv
Accessing Sun Documentation Online	xxv
What Typographic Changes Mean	xxv
Shell Prompts in Command Examples	xxvi
Related Books and Publications	xxvi

1. Preparing to Create a Policy 1

Basic Concepts	1
Required Patches	2
▼ To Apply the Patches	2
Java Plug-In Software	2
Other Features of SunScreen EFS 3.0	3
Configuring and Administering SunScreen EFS 3.0	4
Worksheets for Defining Your Security Policies	6
Creating Service Groups	6
Addresses	8
NAT Mapping	13

Rules	16
Using the Browser	19
▼ To Start the Browser	19
▼ To Set the Default Security Level for the Browser	19
▼ To Access Local System Resources	20
▼ To Use the Java Plug-in	21
▼ To Save the identitydb.obj File	21
▼ To Use the HotJava 1.1 Browser	22
Logging In to the Administration GUI	23
▼ To Log In to the Administration GUI	24
SunScreen Banner	25
Locking	25
Administration Access Levels	26
Administration GUI Session	26
2. Policies List Page	27
Policies List Page	27
▼ To View the Policies List Page	29
Name Field	29
Version Field	29
Active Policy Information Field	29
Policies	29
▼ To Add a New Policy	29
▼ To Copy a Policy	30
▼ To Rename a Policy	30
▼ To Delete a Policy	31
▼ To Back Up a Policy	31
▼ To Restore a Policy	33

▼	To Edit a Policy	34
▼	To View the SunScreen Help Page	35
3.	Common Objects	37
	The "Initial" Policy	38
▼	To Move to the Policy Edit Page	38
▼	To Change the Password	39
	Verifying, Saving, Activating, and Reverting	40
▼	To Verify a Policy	40
▼	To Save Changes	40
▼	To Activate a Policy	40
▼	To Revert Changes	40
	Adding Common Objects	41
	The Screen Field in all Policy Rules and Common Objects	41
▼	To Add a Common Object	42
▼	To Search for a Common Object	42
▼	To Edit a Common Object	42
▼	To View and Edit the Details of a Common Object	43
▼	To Delete a Common Object	43
▼	To Rename a Common Object	44
▼	To Add a Time Object	44
	Time Object Example	45
	Services and Service Groups	46
▼	To Add a Service	46
▼	To Add a Service Group	49
	Adding Addresses	51
▼	To Add a Host Address	51
▼	To Add a Range of Addresses	52

▼ To Add a Group of Addresses 53

Certificates 55

▼ To Add Screen Certificates From a File or Diskette 55

▼ To Generate Screen Certificates 56

▼ To Load an Issued Certificate 57

▼ To Load an Issued Public Certificate 58

▼ To Associate Certificate IDs 59

▼ To Add a Certificate Group 60

Screens 61

▼ To Add a Screen 62

SNMP Alert Receivers 63

▼ To Add a New SNMP Alert Receiver 63

▼ To Delete an SNMP Alert Receiver 64

Interfaces 65

▼ To Add or Edit Interfaces 65

4. Policy Rules 69

Packet Filtering Rules 69

▼ To View and Edit the Details of an Object 69

▼ To Edit a Rule 70

▼ To Add a New Rule 72

▼ To Use the Move Button 73

▼ To Delete a Rule 74

Administrative Access Rules 75

▼ To Add an Administrative Access Rule for Local Administration 75

▼ To Add an Administrative Access Rule for Remote Administration 77

▼ To Edit an Administrative Access Rule for Remote Administration 80

Network Address Translation (NAT) 81

	Defining the Type of Mapping for NAT	81
	NAT Administration GUI Tab	82
	Your NAT Scenario	84
▼	To Add ARP Manually on a Screen in Routing Mode	84
▼	To Define NAT Mappings	85
▼	To Edit the NAT Mappings	87
	Static NAT of a Host to a Host	88
	The Reverse Rule	89
	Dynamic Translation of a Range Of Addresses to One Host	90
	Virtual Private Network (VPN)	91
▼	To Add a VPN Gateway	91
▼	To Add a VPN Rule	92
▼	To Define a Single VPN	92
5.	Information	95
	Information Button	96
▼	To View the Information	96
	Statistics Button	97
▼	To View the Statistics	97
	Logs	98
▼	To Set the Retrieval Mode	98
▼	To Set a Log Viewing Filter	100
	Saving and Clearing the Log	102
▼	To Save the Log	102
▼	To Clear the Log	103
▼	To Save and Clear the Log	104
▼	To Alter the Log File Size for a Specific Screen	104

6. Special Tasks 105

Setting Up High Availability 105

HA Policy 106

Preparing to Install High Availability 106

Using the `/etc/hosts` File for Name Resolution 107

Modifying the HA Service Group 107

Using NAT with HA in Routing Mode 107

▼ To Install High Availability 108

▼ To Install HA on the Secondary HA Screen 109

▼ To Install HA on the Primary HA Screen 109

▼ To Add the Secondary HA Screen to the Primary HA Screen 110

Configuring HA 111

Defining HA 112

▼ To Define HA 112

▼ To Set (Change) the Primary HA Screen 113

Upgrading a SunScreen EFS 2.0 HA System 113

▼ To Upgrade the Primary HA Screen in an HA Cluster From SunScreen EFS 2.0 to SunScreen EFS 3.0 113

▼ To Upgrade Secondary HA Screens in an HA Cluster From SunScreen EFS 2.0 to SunScreen EFS 3.0 113

Removing HA 114

HA Logging 115

Setting Up and Using Proxies 115

Preparing to Use Proxies 116

▼ To Configure the Browser for the HTTP Proxy 116

Defining Proxy Data on the Policy Edit Page 117

Adding Jar Signatures and Jar Hashes 117

▼ To Add a Jar Signature 118

▼ To Add a Jar Hash 118

Proxy Users 119

▼ To Add an Authorized User 120

▼ To Add a Single Proxy User 121

▼ To Add a Proxy User Group 122

▼ To Add Spam Domains 123

▼ To Delete Spam Domains 124

Writing and Editing Policy Rules for Proxies 125

▼ To Write Policy Rules for the Proxies 125

FTP Proxy 130

▼ To Use the FTP Proxy 131

TELNET Proxy 133

▼ To Use the TELNET Proxy 133

SMTP Proxy 134

▼ To Use the SMTP Proxy 135

HTTP Proxy 135

▼ To Use the HTTP Proxy 135

Adding an Additional Remote Administration Station 137

Installing the Software on the New Remote Administration Station 137

▼ To Inform the Screen About the New Remote Administration Station 137

Setting Up the Access Control List on the New Remote Administration
Station 139

Configuring Centralized Management Groups 139

Configure a Centralized Management Group 140

▼ To Generate a Certificate for the Centralized Management Group's Primary
Screen 140

▼ To Associate the Primary Screen's Certificate ID with the Centralized
Management Group's Primary Screen Object 141

- ▼ To Add a Secondary Centralized Management Group Screen on the Primary Screen 143
- ▼ To Generate a Certificate ID for the Centralized Management Group's Secondary Screen on the Secondary Screen 144
- ▼ To Put the Centralized Management Group Secondary Screen's Certificate ID on the Primary Centralized Management Group Screen 145
- ▼ To Associate the Certificate with the Centralized Management Group's Secondary Screen 146
- ▼ To Put the Central Management Group's Primary Certificate ID on the Central Management Group's Secondary Screen 148
- ▼ To Verify that the Certificates are on the Screens 149
- ▼ To Create a Primary Centralized Management Screen on the Secondary Centralized Management Group Screen 150
- ▼ To Save and Activate the Centralized Management Secondary Group's Screen 151
- ▼ To Add a New Address Group on the Centralized Management Group's Primary Screen 151
- ▼ To Define the Central Management Group's Secondary Interfaces on the Centralized Management Group's Primary Screen 152
- ▼ To Allow Communication Between Screens 153
- ▼ To Activate the Policy 153

7. Using the Command Line 155

- ▼ To Install and Configure the Netscape Browser 155

Setting the CLASSPATH 157

Saving the identitydb.obj File 157

Unix (shell) Command Summary 158

Unix (shell) Commands 159

ss_install Command 159

ss_client Command 159

screenInstaller Command 159

adminInstaller Command	159
ssadm Command	160
Executing an ssadm Command on a Local Screen	161
Executing an ssadm -r Command on a Remote Administration Station	161
Remotely Logging Into and Out of SunScreen EFS 3.0	162
▼ To Remotely Log Into SunScreen EFS 3.0	162
▼ To Remotely Log Out of SunScreen EFS 3.0	162
ssadm Sub-Command Summary	163
Configuration Editor Commands	164
Command-Line Session	168
Creating a Policy	168
▼ To Create a New Policy	168
▼ To Copy a Policy	169
▼ To Rename a Policy	169
▼ To Delete a Policy	169
▼ To Back Up a Policy	170
▼ To Restore a Policy	170
▼ To Verify a Policy	170
▼ To Activate a Policy	171
▼ To Edit a Policy	171
Objects In a SunScreen Configuration	172
▼ To Add a New Single Service	172
▼ To Add a New Service Group	172
Modifying Service Groups	173
▼ To Rename a Service and Service Group and Its References	173
▼ To Rename a Service or Service Group	174

- ▼ To Delete Service or Service Group 174
- ▼ To Check References to Deleted Service or Service Group 174
- Addresses, Address Ranges, and Address Groups 175
- ▼ To Add a New Host Address 175
- ▼ To Add a Range of Addresses 175
- ▼ To Add an Address Group 176
- ▼ To Delete an Address, Address Range, or Address List 176
- ▼ To Check References to a Deleted Address, Address Range, or Address List 176
- ▼ To Rename an Address, Address Range, or Address Group 177
- Certificates 178
- ▼ To Add Screen Certificates From a Diskette or a File 178
- ▼ To Add Screen Local Identities 179
- ▼ To Add Self-Generated Screen Certificates 181
- ▼ To Add Other Certificates from a Diskette or a File 184
- ▼ To Add Certificate Groups 185
- ▼ To Add a New Member to a Certificate Group 185
- ▼ To Remove a Member From a Certificate Group 185
- ▼ To Rename a Certificate or Certificate Group 186
- ▼ To Delete a Certificate or Certificate Group 186
- ▼ To Check References to a Deleted Certificate 186
- ▼ To Check References to a Deleted Certificate Group 187
- Screens 187
- ▼ To Add a Screen 187
- ▼ To List the Screens 188
- ▼ To Add an SNMP Receiver to a Screen 188
- ▼ To Add Multiple SNMP Receivers to a Screen 188
- ▼ To Remove SNMP Receivers From a Screen 188

- ▼ To Set Logsize on a Screen 189
- ▼ To Set a Screen to Stealth Mode 189
- Interfaces 189
 - ▼ To Add Interfaces (in Routing Mode) 189
 - ▼ To Add Interfaces (in Routing Mode) with a Detailed Log 190
- Authorized Users 190
 - Adding or Modifying an Authorized User 190
 - ▼ To Add An Authorized User with Password Authentication 190
 - ▼ To Add An Authorized User and SecurID Name 191
 - ▼ To Modify Authorized Users 191
 - ▼ To Delete an Authorized User 192
- Policy Rules 192
 - Defining New Rules 192
 - ▼ To Create a Packet Filtering Rule 192
 - ▼ To Reorder the Rules 193
 - ▼ To Delete a Rule 194
 - ▼ To Edit Any Part of a Rule 194
 - ▼ To Add an Access Rule for GUI Local Administration 195
 - ▼ To Edit an Access Rule for GUI Local Administration 196
 - ▼ To Delete an Access Rule for GUI Local Administration 196
 - ▼ To Add an Access Rule for Remote Administration 197
 - ▼ To Edit an Access Rule for Remote Administration 197
 - ▼ To Delete an Access Rule for Remote Administration 198
- Network Address Translation 198
 - ▼ To Add ARP Manually 198
 - ▼ To Define NAT Mappings 199
 - ▼ To Delete NAT Mappings 199

▼ To List the NAT Mappings	200
Virtual Private Network (VPN)	200
▼ To Add a VPN Gateway	200
▼ To Replace a VPN Gateway	201
▼ To Remove a VPN Gateway	201
Information, Statistics, and Logs	202
▼ To View the Information	202
▼ To View the Statistics	202
▼ To Set Up Packet Logging	203
Examining Packets	203
▼ To Use <code>ssadm logdump</code> Command	203
▼ To View the Log	204
▼ To Save the Log	204
▼ To Clear the Log	204
▼ To Save and Clear the Log	205
Setting Up High Availability (HA)	205
▼ To Remove an HA Host	206
▼ To View HA Information	206
Centralized Management Group	207
▼ Change a Screen Object to be in a Cluster	207
▼ To Remove a Screen Object from a Cluster	207
Gathering Information From Your System to Report to SunService	208
Getting Support for SunScreen Products	208
Gathering Data From the Screen	209
▼ Using the <code>ssadm lib/statetables</code> Command	209
▼ Using the <code>ssadm lib/screeninfo</code> Command	209
▼ Using the <code>ssadm lib/support</code> Command	210

▼ To Use the Help Option 210

Troubleshooting 210

▼ To Use the `ssadm debug_level` Command 210

Figures

FIGURE 1-1	Example of a Network Map	9
FIGURE 1-2	The SunScreen EFS 3.0 Login Page	23
FIGURE 1-3	Policies List Page	24
FIGURE 1-4	SunScreen Banner	25
FIGURE 2-1	Policies List Page	28
FIGURE 2-2	Add New Policy Dialog Window	30
FIGURE 2-3	Copy... Dialog Window	30
FIGURE 2-4	Rename Dialog Window	31
FIGURE 2-5	Delete Policy Dialog Window	31
FIGURE 2-6	Select a backup file Dialog Window	32
FIGURE 2-7	Policy Edit Page	34
FIGURE 2-8	SunScreen Help Page	35
FIGURE 2-9	Policy Edit Page	38
FIGURE 2-10	Common Objects Area	41
FIGURE 2-11	Time Dialog Window	44
FIGURE 2-12	Example Time Object in a Rule	45
FIGURE 2-13	Service Dialog Window	47
FIGURE 2-14	List of Filter Engines	48
FIGURE 2-15	Add New Group Service Dialog Window	50
FIGURE 2-16	Address Dialog Window	51
FIGURE 2-17	Address Dialog Window	52

FIGURE 2-18	Address Dialog Window	54
FIGURE 2-19	Certificate Dialog Window	56
FIGURE 2-20	Certificate Dialog Window	57
FIGURE 2-21	Certificate Dialog Window	58
FIGURE 2-22	Certificate Dialog Window	60
FIGURE 2-23	Certificate Dialog Window	61
FIGURE 2-24	Screen Dialog Window, Miscellaneous Tab	62
FIGURE 2-25	Screen Dialog Window SNMP Area	64
FIGURE 2-26	Interface Definition Dialog Window	66
FIGURE 4-1	Policy Rules Area of the Policy Edit Page	70
FIGURE 4-2	Rule Definition Dialog Window	71
FIGURE 4-3	Rule Definition Dialog Window	72
FIGURE 4-4	Move Rule Dialog Window	73
FIGURE 4-5	Delete Rule Dialog Window	74
FIGURE 4-6	Administrative Access Area	76
FIGURE 4-7	Local Access Rules Dialog Window	76
FIGURE 4-8	Remote Access Rules Dialog Window	78
FIGURE 4-9	Network Address Translation Area	85
FIGURE 4-10	NAT Definition Dialog Window	86
FIGURE 4-11	Static Translation of a Host To a Host	88
FIGURE 4-12	The Reverse Rule	89
FIGURE 4-13	Dynamic Translation	90
FIGURE 4-14	Example Address Groups	93
FIGURE 5-1	SunScreen Banner	95
FIGURE 5-2	Status Page	96
FIGURE 5-3	Statistics Page	97
FIGURE 5-4	Retrieval Settings Tab in the Log Area	99
FIGURE 5-5	The Log Page	103

FIGURE 6-1	Wiring Before and During HA Configuration	108
FIGURE 6-2	Initialize HA Dialog Window	109
FIGURE 6-3	Screen Dialog Window HA/MasterConfig Area	110
FIGURE 6-4	Jar Signature Dialog Window	118
FIGURE 6-5	Jar Hash Dialog Window	119
FIGURE 6-6	User Dialog Window	120
FIGURE 6-7	Proxy User Dialog Window	121
FIGURE 6-8	Proxy User Dialog Window	122
FIGURE 6-9	Screen Dialog Window, Mail Proxy Tab	124
FIGURE 6-10	Rule Definition Dialog Window, Action ALLOW	126
FIGURE 6-11	Rule Definition Dialog Window, Action DENY	127
FIGURE 6-12	Rule Definition Dialog Window, PROXY_FTP	128
FIGURE 6-13	Rule Definition Dialog Window, PROXY_TELNET	129
FIGURE 6-14	Rule Definition Dialog Window, PROXY_SMTP	129
FIGURE 6-15	Rule Definition Dialog Window, PROXY_HTTP	130
FIGURE 6-16	PROXY_HTTP	136
FIGURE 6-17	Certificate Dialog Window	138
FIGURE 6-18	Certificate Dialog Window	141
FIGURE 6-19	Screen Dialog Window, Miscellaneous Tab	142
FIGURE 6-20	Screen Dialog Window, Miscellaneous Tab	143
FIGURE 6-21	Certificate Dialog Window	144
FIGURE 6-22	Certificate Dialog Window Showing the Certificate ID	145
FIGURE 6-23	Certificate Dialog Window	146
FIGURE 6-24	Certificate Dialog Window	147
FIGURE 6-25	Certificate Dialog Window	148
FIGURE 6-26	Screen Dialog Window, Miscellaneous Tab	150
FIGURE 6-27	Interface Definition Dialog Window	152

Tables

TABLE P-1	Typographic Conventions	xxiii
TABLE P-1	Shell Prompts	xxiv
TABLE A-1	SunScreen EFS 3.0 Unix (<code>shell</code>) Command Summary	158
TABLE A-2	SunScreen EFS 3.0 <code>ssadm</code> Sub-Command Summary	163
TABLE A-3	SunScreen EFS 3.0 Configuration Editor <code>ssadm edit</code> Sub-Command Summary	164
TABLE A-4	Table of Support Commands	208
TABLE P-1	Typographic Conventions	xxv
TABLE P-2	Shell Prompts	xxvi
WORKSHEET 1-A	Services or Service Groups	6
WORKSHEET 1-B	New Services	7
WORKSHEET 1-C	New Service Groups	7
WORKSHEET 2-A	Host Addresses	10
WORKSHEET 2-A	Host Addresses	11
WORKSHEET 2-B	Address Ranges	11
WORKSHEET 2-C	Address Group	12
WORKSHEET 2-D	NAT Map Table	13
WORKSHEET 2-E	Screen's Interfaces	14
WORKSHEET 2-F	Authorized Users	14
WORKSHEET 2-G	Administration Stations	15
WORKSHEET 3-A	Rules	16
WORKSHEET 2-B	Sample for worksheet 3-A, "Rules"	18

TABLE A-1	SunScreen EFS 3.0 Unix (<i>shell</i>) Command Summary	158
TABLE A-2	SunScreen EFS 3.0 <i>ssadm</i> Sub-Command Summary	163
TABLE A-3	SunScreen EFS 3.0 Configuration Editor <i>ssadm edit</i> Sub-Command Summary	164
TABLE A-1	Table of Support Commands	208

Preface

SunScreen[™] EFS 3.0 is part of the family of SunScreen products that provide a solution to security authentication and privacy requirements. SunScreen EFS 3.0 gives companies a means of securing department networks connected to a public internetwork.

This SunScreen EFS 3.0 Administration Guide provides all the information necessary to configure and administer SunScreen EFS 3.0 on your network. Other manuals in the SunScreen EFS 3.0 documentation set include the *SunScreen EFS 3.0 Installation Guide*, the *SunScreen EFS 3.0 Reference Manual*, and the *SKIP User's Guide for EFS 3.0 Remote Administration Stations*.

Who Should Use This Book

The SunScreen EFS 3.0 Administration Guide is intended for SunScreen EFS 3.0 system administrators 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, and with your network topology.

How This Guide Is Organized

The *SunScreen EFS 3.0 Administration Guide* contains the following chapters and appendixes:

- **Chapter 1, “Preparing to Create a Policy,”** covers the basic concepts, worksheets for defining your security policies, as well as the procedures for starting and configuring the Java-based browser, and logging in to the administration graphical user interface (GUI).
- **Chapter 2, “Policies List Page,”** describes the Policies List page in the administration GUI, and procedures for accessing local system resources, using the HotJava 1.1 Browser, and the actions that can be performed on policies (such as, adding, copying, renaming, deleting, and reordering policies).
- **Chapter 3, “Common Objects,”** contains the procedures for using the administration GUI to change the password, and add, delete, edit, and rename the common objects.
- **Chapter 4, “Policy Rules,”** describes packet filtering, administrative access rules, Network Address Translation (NAT), and Virtual Private Networks (VPN).
- **Chapter 5, “Information,”** contains the procedures for viewing information and statistics, and using the SunScreen banner.
- **Chapter 6, “Special Tasks,”** describes High Availability (HA), proxies, adding an additional remote administration station, and configuring Centralized Management groups.
- **Appendix A, “Using the Command Line,”** contains procedures for using the UNIX command line.

Ordering Sun Documents

The SunDocsSM program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals using this program.

For a list of documents and how to order them, see the catalog section of the SunExpressTM Internet site at <http://www.sun.com/sunexpress>.

Accessing Sun Documentation Online

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

What Typographic Changes Mean

The following table describes the type changes and symbols 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. <i>machine_name%</i> You have mail. Type <code>su -</code> to become superuser.
AaBbCc123	What you type, contrasted with on-screen computer output	<i>machine_name%</i> su - Password:
<i>AaBbCc123</i>	Command-line placeholder; replace with a real name or value	To delete a file, type <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new words or terms, or emphasized words	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.

Shell Prompts in Command Examples

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

TABLE P-2 Shell Prompts

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

Related Books and Publications

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

- Bruce Schneier. *Applied Cryptography*
John Wiley & Sons, 1996, 2nd edition,
ISBN 0-471-12845-7
- D. Brent Chapman and Elizabeth D. Zwicky. *Building Internet Firewalls*
O'Reilly & Associates, 1995
ISBN 1-56592-124-0
- Kathryn M. Walker and Linda Croswhite Cavanaugh. *Computer Security Policies and SunScreen Firewalls*
Sun Microsystems Press, 1998
ISBN 0-13-096015-0
- Bill Cheswick and Steve Bellovin. *Firewalls and Internet Security*
Addison-Wesley, 1994
ISBN 0-201-63357-4
- *Handbook of Computer-Communications Standards*
Volume 3: The TCP/IP Protocol Suite
William Stallings, Macmillan, 1990

- Douglas E. Comer. *Internetworking with TCP/IP, Volume 1*
Prentice Hall, 1995
ISBN 0-13-216987-8
- Simson Garfinkel and Gene Spafford. *Practical UNIX and Internet Security*
O'Reilly & Associates, 1996, 2nd edition
ISBN 1-56592-148-8
- Craig Hunt. *TCP/IP Network Administration*
O'Reilly & Associates, 1992
- William Stallings. *Handbook of Computer-Communications Standards
Volume 3: The TCP/IP Protocol Suite*
Macmillan, 1990
- William Stallings. *Network and Internetwork Security Principles and Practice*
Prentice Hall, 1995
ISBN 0-02-415483-0
- W. Richard Stevens. *TCP/IP Illustrated, Volume 1 The Protocols*
Addison-Wesley, 1994,
ISBN 0-201-63346-9
- *Network Security*
Charlie Kaufman, Radia Perlman, and Mike Speciner
Prentice Hall, 1995
- "SKIP IP-Level Encryption," [<http://skip.incog.com>]
- "Sun Network Security Solutions," [<http://www.sun.com/security>]

Preparing to Create a Policy

This chapter describes:

- Basic concepts
- Required patches
- Java plug-in software
- Features of SunScreen EFS 3.0
- Worksheets for defining the components for your new policy
- Saving the `identitydb.obj` file
- Using the browser
- Setting the default security level for the browser
- Logging in to the administration GUI
- Locking
- Administrative access levels

Basic Concepts

SunScreen EFS 3.0™ integrates the SunScreen EFS and SunScreen SPF firewall products. It allows the use of stealth-mode interfaces with an administration interface to create a stealth firewall, as well as allowing the configuration of a routing firewall.

SunScreen EFS 3.0 consists of two components: a *Screen* and its *Administration Station*. The Screen component is responsible for screening packets. You administer policies from the Administration Station component. For remote administration, the two components can be installed on a Screen, which is separate from its Administration Station for remote administration. The two components can be installed on a single machine (in routing mode only) for local administration.

SunScreen EFS, includes stealth-mode capabilities for setting up a dedicated perimeter defense and extranet firewall, and routing-mode capabilities for a firewall that is proven to be the fastest and among the easiest to use.

Stealth mode partitions an existing network and acts much like a network bridge; it is unnecessary to renumber or sub-net your network in order to install a stealth-mode fire wall.

SunScreen SKIP is used with SunScreen EFS 3.0 for encryption, authentication, and access-control software for Sun™ Solaris, Windows NT, and Windows 98 environments. You must log onto your Screen to administer SKIP directly or to gather data from any of the SKIP commands.



Caution – If you configure a network interface that you later set to Stealth mode, the Screen will hang upon activation. When this happens, you must first reboot the Screen in Single-User mode, then remove the `/etc/hostname.interface_name` file, (which unconfigures that interface) and reboot the Screen.

Required Patches

Two patches are required when you are running Solaris 2.6; they are included on the SunScreen EFS 3.0 CD-ROM.

▼ To Apply the Patches

- Apply the patches to a SPARC system by typing:

```
# cd /cdrom/cdrom0/Sparc/Patches
# patchadd 106125-06
# patchadd 105181-11
```

- Apply the patches to an x86 system by typing:

```
# cd /cdrom/cdrom0/i386/Patches
# patchadd 106126-06
# patchadd 105182-13
```

Java Plug-In Software

Java Plug-in software system requirements:

Windows 95, Windows 98, or Windows NT 4.0:

- Pentium 90 MHz or faster processor
- 10 MB free hard disk space (recommended 20 MB)
- 24 MB system RAM

Sun Solaris 2.5 or above:

- Sun SPARC or Intel x86 microprocessor
- 10 MB free hard disk space (recommended 20 MB)
- 32 MB system RAM (recommended 48 MB)

Java Plug-in software, which is provided is available at the following URL, free-of-charge: <http://java.sun.com/products/plugin/1.1.2/index-1.1.2.html>

Java Plug-in software enables you to direct Java technology-enabled applets on your Intranet Web pages to run using Sun's *Java Runtime Environment* (JRE), instead of the browser's default runtime. They enable you to support Microsoft Windows- and Sun Solaris-based browsers in your enterprise.

Other Features of SunScreen EFS 3.0

- *Flexible Rules and Policies* use ordered sets of rules to establish criteria for packet handling.
- *Dynamic Packet Filtering* examines each packet as it enters a Screen.
- *Transparent Encryption and Authentication* automatically encrypts and decrypts messages exchanged with other hosts running SKIP to ensure message privacy.
- *Tunneling* uses encrypted tunnels to hide network topology from intruders and to set up secure VPNs over insecure public networks.
- *Logging* allows you to log messages according to your policy definition.

The following features are new in SunScreen EFS 3.0:

- *Centralized Management of Multiple Screens* provides a way for you to manage multiple Screens with a set of common objects through a specific primary Screen, as well as monitor logs on individual Screens, in a centralized management group or HA cluster. The primary Screen, where the objects reside, can be managed by many different Administration Stations, as in prior SunScreen firewall releases.
- *Choice of Stealth or Routing Modes* allows you to designate interfaces in either stealth or routing mode on a Screen-by-Screen basis. Stealth mode, as a layered product, no longer boots from a CD-ROM nor requires an installation diskette, and operating system (OS) hardening is optional. High availability is accessible in both modes. Proxies work in routing mode only.
- *High Availability* (HA) supports stealth- and routing-mode installations. The primary HA Screen manages secondary HA Screens in an HA cluster. The passive HA Screen(s) within a HA cluster are set to mirror the state of the active Screen, which can be the primary or a secondary HA Screen. If the active Screen fails or becomes unavailable, one of the passive Screens takes over within seconds.

- *Filtering Logs* allows you to search, sort, and filter log messages to find critical information quickly and easily. You specify the log size value and what information you want recorded in administrative log files when you set up SunScreen EFS 3.0. Once running, you can monitor logs by using the browser in real time or historical mode.
- *Network Address Translation (NAT)* enables a Screen to map an internal network address to a different network address. As it passes packets between an internal host and a public network, the addresses in the packet are replaced with new addresses transparently, checksums and sequence numbers are corrected, and the state of the address map is monitored. You specify when a packet using ordered NAT translations is applied, based on source or destination addresses.
- *Time-based Rules* allows you to set time-of-day rules to be more or less restrictive for specified hours.
- *Proxies* provide content filtering and user authentication.
- The *Virtual Private Network (VPN)* allows the user to specify generic encryption information and allow the system to generate specific SKIP-secured Rules.
- Each *version* of a policy has an associated version number. Edited policies automatically generate historical version numbers. You can edit, copy, rename, and activate policy versions, as well as delete them if they are no longer needed.
- *User authentication* supports ACE (SecurID's ACE 3.3 server), which authenticates indirectly through the RADIUS authentication protocol. User passwords and SecurID cards are supported.
- The *Command Line Interface* is embodied in the `ss_adm` command. All the functionality of SunScreen EFS 3.0 that is available through the administration GUI is also available through a command. Administering your Screens through the command line can be useful when you want to manage one or more remote Screens.

Configuring and Administering SunScreen EFS 3.0

SunScreen EFS 3.0 controls access to a network through policy rules, which are created in the Policy Rules area of the Policy Edit Screen. Policy objects are created with the global data that you define in the Common Objects area of the Policy Edit page of the administration GUI.

A *Policy* is a named set of policy rules. For example, when the SunScreen EFS 3.0 software is first installed, there is one policy, named “Initial.”

Policy rules define a security policy. They describe the relationships between the common objects (for example, hosts that can communicate with each other). The collection of these relationships comprise the security policy which they implement.

Policy rules are:

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

Common Objects are:

- *Service*, which describes network protocols.
- *Address*, which defines the network elements that make up the policy
- *Certificate*, which describes the certificate used for SKIP connections.
- *Screen*, which describes Screen objects and their relationships.
- *Interface*, which describes the physical interface ports of Screen objects.
- *Proxy User*, which describes the proxy user name for an authorized user
- *Admin Users* which describes an administrator for your Screen administration
- *Authorized User*, which creates a user identity/authentication mechanism
- *Jar Hash*, the Java archive hash for HTTP proxy dialog filtering
- *Jar Signature*, the Java archive signature for HTTP proxy dialog filtering
- *Time*, which describes time intervals for time-dependent rules

You administer the Screen through any browser that supports Java and is compliant with Java Developers Kit (JDK) 1.1.

The administration GUI works with any of the following browsers that support the Java Runtime Environment, Version 1.1 (JRE 1.1.3).

- HotJava 1.1
- Netscape, with Sun's Java plug-in
- Internet Explorer, with Sun's Java plug-in 1.1
- Specified versions of Netscape, with Netscape's own Java
- Specified versions of Internet Explorer, with Internet Explorer's own Java

Note – Web browsers other than HotJava 1.1 that use Java, and the different versions of HotJava, can vary from these instructions and figures. See the documentation that comes with the browser that you are using. See the *SunScreen EFS 3.0 Reference Manual* for more detailed information.

The various features of SunScreen EFS, parts of a policy, and the theory behind SunScreen EFS 3.0 are discussed in the *SunScreen EFS 3.0 Reference Manual*.

Worksheets for Defining Your Security Policies

Here are directions and worksheets to help you analyze and define your company's security policy requirements. Once established, SunScreen EFS 3.0 controls access to the network through a set of rules and interface definitions that are created in the administration GUI. The information you accumulate in this section will be used to define your policies. See *SunScreen EFS 3.0 Reference Manual* for more information

To begin the process, create a group of all the IP addresses that SunScreen EFS 3.0 needs to know. SunScreen EFS 3.0 identifies network elements—network, subnetworks, and individual hosts—by IP address. Before you can define the rule, you must define all the elements or parts that make up the rule. Several types of addresses need to be defined in SunScreen EFS 3.0.

Creating Service Groups

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

Worksheet 1-A Services or Service Groups

Name	Definition

Worksheet 1-B New Services

Name	Filter (State Engine)	Port	Broadcast	Parameters	Reverse	Definition

Worksheet 1-C New Service Groups

Name	Members

Addresses

SunScreen EFS 3.0 uses IP addresses to define the network elements that make up the configuration. These addresses are then used in defining SunScreen EFS 3.0's network interfaces and as the source and destination addresses for rules and NAT.

The address can be for a single computer, or it can be for a whole network or subnetwork. Additionally, addresses (individual and network) can be grouped together to form an address *group*. SunScreen EFS 3.0 allows you to define address groups that specifically include or exclude other defined addresses (single IP hosts, ranges, or groups).

Host addresses	For individual elements, such as the router and individual computers, you need to know the IP address, in standard dotted Internet-address notation (w.x.y.z format), and the name of the host.
Address Ranges	For networks and subnetworks, you need to know the beginning and ending addresses of the network or subnetwork, both in standard dotted Internet-address notation (w.x.y.z format).
Address Groups	Groups of host addresses, network addresses, and other address groups can be combined to form logical groups of addresses that can then be manipulated as a <i>single</i> element. Address groups are defined after all the single computer and network addresses are defined. Groups may be inclusive or exclusive or a combination of both, but may not be cyclic.

The illustration below shows an example of various types of addresses and can be used as a reference when completing your own network map.

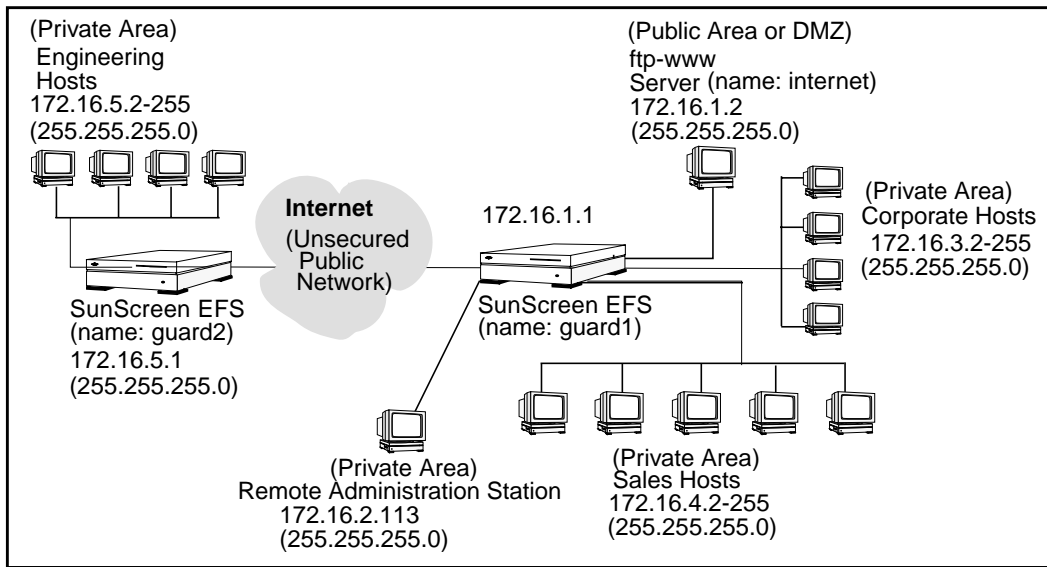


FIGURE 1-1 Example of a Network Map

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

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

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

The following worksheets (2-A through 2-J) are designed to help you organize the IP addresses. Expand them as necessary. Group the IP addresses and names for the following network elements:

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

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

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



Caution – *By default*, SunScreen EFS 3.0 drops any packets that do not specifically match a rule. This makes it easier to create rules, since you only have to write a rule for the services you want to pass.

Worksheet 2-A Host Addresses

Name	IP Address

Worksheet 2-A Host Addresses

Name	IP Address

Worksheet 2-B Address Ranges

Name	Address	
	Beginning	Ending

Worksheet 2-C Address Group

Name	Address	
	Include	Exclude

NAT Mapping

NAT enables you to map from unregistered addresses to registered addresses allocated by your Internet service provider (ISP). The NAT function of SunScreen EFS 3.0 uses this mapping to replace the IP addresses in a packet with other IP addresses. This allows you to use unregistered Internet addresses to number your internal networks and hosts and yet have full connectivity to the Internet. With this approach, with a small Class C network, which supports only 254 hosts (externally), you can use a private Class B network, which supports as many as 65,000 hosts or 255 networks of 254 hosts (internally).

Worksheet 2-D NAT Map Table

Type		Address		Translated Address	
Dynamic	Static	Source	Destination	Source	Destination

Worksheet 2-E Screen's Interfaces

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

Worksheet 2-F Authorized Users

Name	Authorized User	Details

Worksheet 2-G Administration Stations

“admin group” Certificates	Admin Station(s) Address	Key Algorithm	Data Algorithm	MAC Algorithm	Admin User Name	Access Level

Rules

Use worksheet 3-A to organize the individual rules you want to use. Space is provided for you to create your own service groups. Make copies of the worksheet, as necessary.

A filled-in sample of worksheet 3-A with the requisite services that you may want for a particular network.on and sales networks is shown in worksheet 3-B.

Worksheet 3-A Rules

Rule Index	Service or Service Group	Address		Action (See explanatory information below)	Encryption	User or Groups of Users (Optional)	Time of Day (Optional)	Screen (Optional)
		Source	Destination					

Four Action Types

- ALLOW options:
 - LOG_NONE
 - LOG_SUMMARY
 - LOG_DETAIL
 - SNMP_NONE
 - SNMP
 - A proxy type may be chosen if the service can be proxied by one of the SunScreen proxies.

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

- ENCRYPT options:
 - NONE
 - SKIP_Version_1 (for connection to a SunScreen SPF-100 *only*)
 - You must decide on:
 - Key Algorithm list (depends on the SKIP version chosen: U.S. and Canada, Export Controlled, or Global)
 - Data Algorithm list (depends on the SKIP version chosen: U.S. and Canada, Export Controlled, or Global)
 - SKIP_Version_2 (for connection to all other SKIP-enabled devices) (Optional: Tunnel addresses are allowed.)
 - You must decide on:
 - From Encryptor list
 - To Encryptor list
 - Key Algorithm list (depends on the SKIP version chosen: U.S. and Canada, Export Controlled, or Global)
 - Data Algorithm list (depends on the SKIP version chosen: U.S. and Canada, Export Controlled, or Global)
 - MAC Algorithm list (NONE or MD5)

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

Worksheet 2-B Sample for worksheet 3-A, “Rules”

Service or Service Group	From IP Address(es)	To IP Address(es)	Action	Encryption	Proxy
ftp	Internal-net	Internet	ALLOW	NONE	NONE
ftp	*	ftp Server	ALLOW	NONE	NONE
ftp	Internet	Internal-net	DENY	NONE	NONE

Note – For this example:

<i>ftp server</i>	172.16.1.2
<i>Internal-net</i>	Corporate Net, Sales Net
<i>Internet</i>	* but <i>not</i> Internal-net or ftp server

After you have defined and mapped out your network and decided on your policy, you use data objects, such as services and addresses, to configure SunScreen EFS 3.0 with the policy rules you create to control access to your network. When you installed SunScreen EFS 3.0, you created a Policy named “Initial,” so that you can connect to the Policy Edit page and build the Security Policies that you want to use.

Examples are given in this guide for the administration GUI. For the command line interface, see Appendix A.

Using the Browser

See Appendix A for steps to install and configure the Netscape browser for SunScreen administration at the command line.

▼ To Start the Browser

You administer, configure, edit, and manage SunScreen EFS 3.0 through a Java-based Web browser. To start the browser, follow the steps listed below:

1. **Make sure the browser's directory (/usr/dt/bin/) is in your path.**
2. **In a terminal window, open the browser by typing:**

```
% hotjava &
```

▼ To Set the Default Security Level for the Browser

Set the default security level to medium for both signed and unsigned applet windows.

1. **Click the Edit button of the browser to display the menu.**
2. **Click the arrow on Preferences to display the choice list.**
3. **Click and highlight Applet Security to display the Applet Security page.**
4. **Click Medium Security for both signed and unsigned applet windows.**
5. **Click the Apply button at the bottom of the Applet Security page to set these choices as defaults.**
 - **The Hotjava Security Violation window may appear when you add certificate IDs or backup or restore a policy.**
 - Check Allow reading all files.
 - (Optionally) leave Allow this action checked. (This window will then appear each time you add a certificate ID or restore a backed-up Policy.)
 - Click the OK button on the Security Violation window.

6. Connect with the Screen from the browser by typing:

`http://Name_of_the_Screen:3852`

The *Name_of_the_Screen* is the name of the machine that will be the Screen for the SunScreen EFS. You may use `localhost` instead of the name of the machine in the entry above if you are administering the Screen locally. You must use the name of the machine as the name of the Screen if you are administering the Screen remotely.

Note – Use the name of the interface dedicated to HA for all HA administration. Otherwise, you will only connect to the currently-active HA host instead of the primary HA host.

When using the Java plug-in software in Netscape or Internet Explorer, connect with the screen from the browser by typing: `http://Name_of_the_Screen:3852/plugin`.

▼ To Access Local System Resources

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.)

The operations that require access to your local system resources from the administration GUI are:

- Loading certificates from a diskette
- Backing up all policies
- Restoring all policies
- Saving log files
- Adding Jar signatures

To work around this limitation, do one of the following:

- Use the Java plug-in
- Use the HotJava browser version 1.1.

▼ To Use the Java Plug-in

If you use a version of Netscape Navigator or Internet Explorer that does not support the Java 1.1 features and API's, install the plug-in from one of the following links:

- Download the plug-in from the Sun Website (<http://java.sun.com/products/plugin>)
- Download the plug-in bundled with the SunScreen EFS 3.0 software

After you install the plug-in, save the file `identitydb.obj` from `/opt/SUNWicg/SunScreen/admin/htdocs/plugin/plugins` in the following locations (if it does not already exist in these locations).

- `$HOME` on Unix systems
- `C:\WINDOWS` directory for Windows 95 users
- `C:\WINDOWS\PROFILES\username` for multiuser Windows 95 & 98 systems
- `C:\WINNT\PROFILES\username` on Windows NT systems

If the file `identitydb.obj` already exists in these locations, add SunScreen as one of the accepted signers to the file `identitydb.obj` (see the `ss_addsigner` man page).

▼ To Save the `identitydb.obj` File

This file verifies the signature on the Java files and must be installed on the administration station if you are using the Java plug-in.

1. In the browser, go to <http://localhost:3852/plugin/plugins>.
2. Use the right mouse button to save the link as a file on Solaris systems.

When the Java plug-in is installed, connect to the administration GUI with the following URL:

- <http://localhost:3852/plugin>

Note – If the browser Save action does not save the file, use a floppy diskette to copy this file to other administration stations.

▼ To Use the HotJava 1.1 Browser

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. **In the browser's Edit choice list, choose Preferences.**
2. **Select Applet Security.**
3. **Select the Medium Security radio button from the Unsigned Applet column.**
4. **Select Apply.**

Logging In to the Administration GUI

In each session, the browser prompts you for a user name and password. Initially, the User Name, “admin,” and the Password, “admin” are the defaults. You must change them in the Common Objects area of the Policy Edit page.

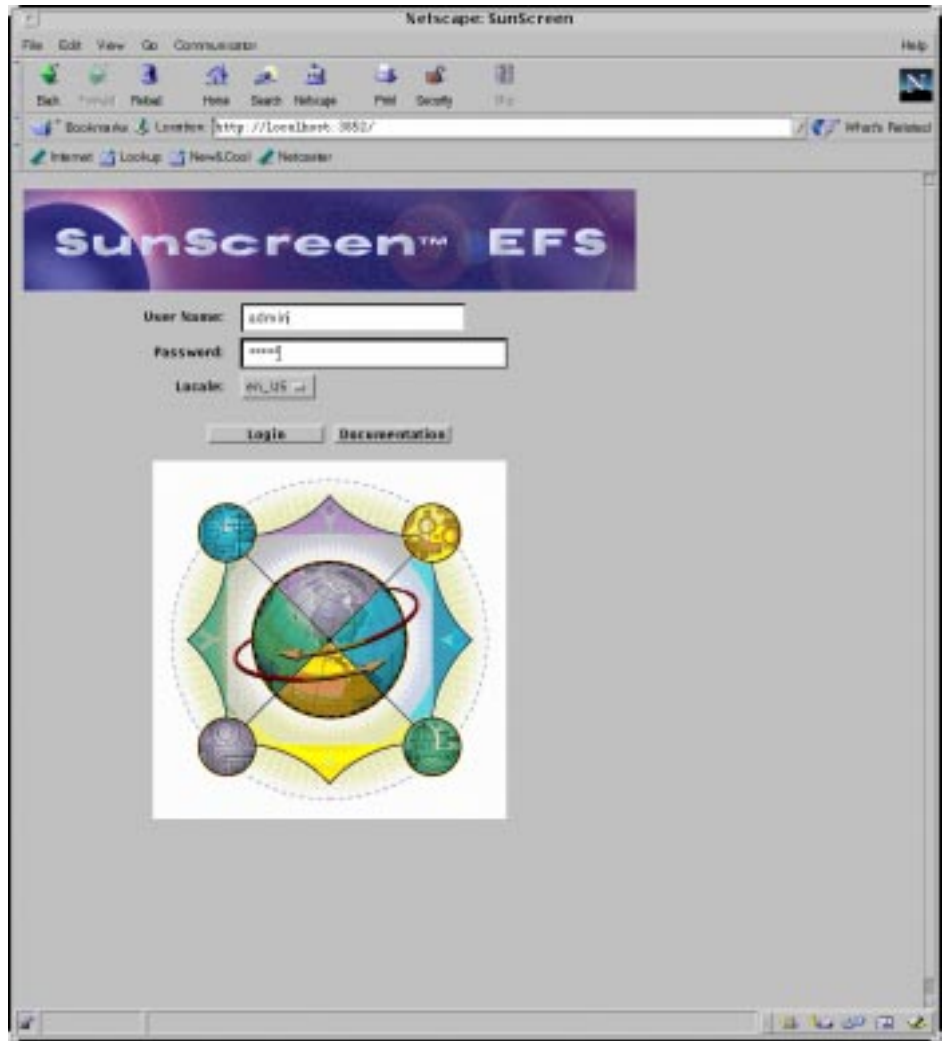


FIGURE 1-2 The SunScreen EFS 3.0 Login Page

▼ To Log In to the Administration GUI

1. Type your user name and your password:

User Name: **admin**

Password: **admin**

The password is shown here only for clarity. It is echoed as “*”.

2. Click the Login button.

If login is successful, the Policies List page is displayed for administrators with the required access level.



FIGURE 1-3 Policies List Page

SunScreen Banner

The SunScreen banner is located at the top of the Policies List and Policy Edit pages.

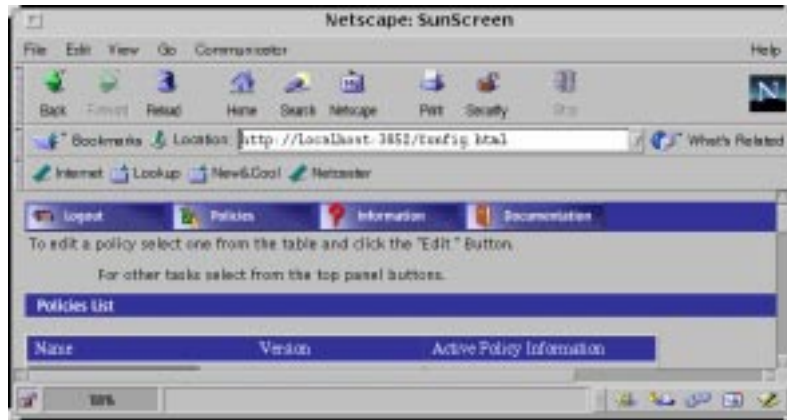


FIGURE 1-4 SunScreen Banner

Note – See Chapter 5 for descriptions of the Information pages.

Locking

The Policy List page is displayed, if you have the access level ALL, READ, or WRITE.

A lock is automatically acquired and held by the first person (only) to change a policy. The lock is held per policy: if someone acquires the lock while you are in an edit session, you cannot save your changes.

If the “Could not acquire the lock” message is displayed (to indicate that someone has made changes to the policy):

- On the command line, type: quit.

```
% quit
```

Or:

- In the administration GUI:

1. Click the **Revert Changes** button.
2. Click the **Policies** button in the SunScreen banner.

You can try to edit the policy later.

The lock does not affect the buttons in the SunScreen banner. Anyone, at any time, can view the Information page and Documentation.

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

Administration Access Levels

The administration GUI supports four administrative access levels.

- *Status* Administrators, who have the access level STATUS can only monitor SunScreens, but cannot view the policies.
- *Local* Administrators, who have the access level READ, are users responsible for implementing their individual Screen's policy. Local Administrators are allowed to read policies, but are not authorized to change policies, so they must make a request for changes to Executive or Master Administrators
- *Executive* Administrators, who have the access level WRITE, can define and change policies. Local Administrators send their policy change recommendations to Executive Administrators.
- *Master* Administrators, who have the access level ALL, grant the various access levels to the administrators.

Administration GUI Session

Logging in as a user with the access level ALL or WRITE puts you into a *session*. You cannot log out of a session until you have either saved or reverted the policy to the last saved version.

Policies List Page

This chapter describes:

- Viewing the Policies List page
- Adding a new policy
- Copying a policy
- Renaming a policy
- Verifying, saving, and activating a policy
- Deleting a policy
- Backing up a policy
- Restoring policy
- Using the Help button

The following information describes using the administration GUI. For the command line interface, see Appendix A.

Policies List Page

After you log into SunScreen EFS 3.0, the Policies List page is displayed.

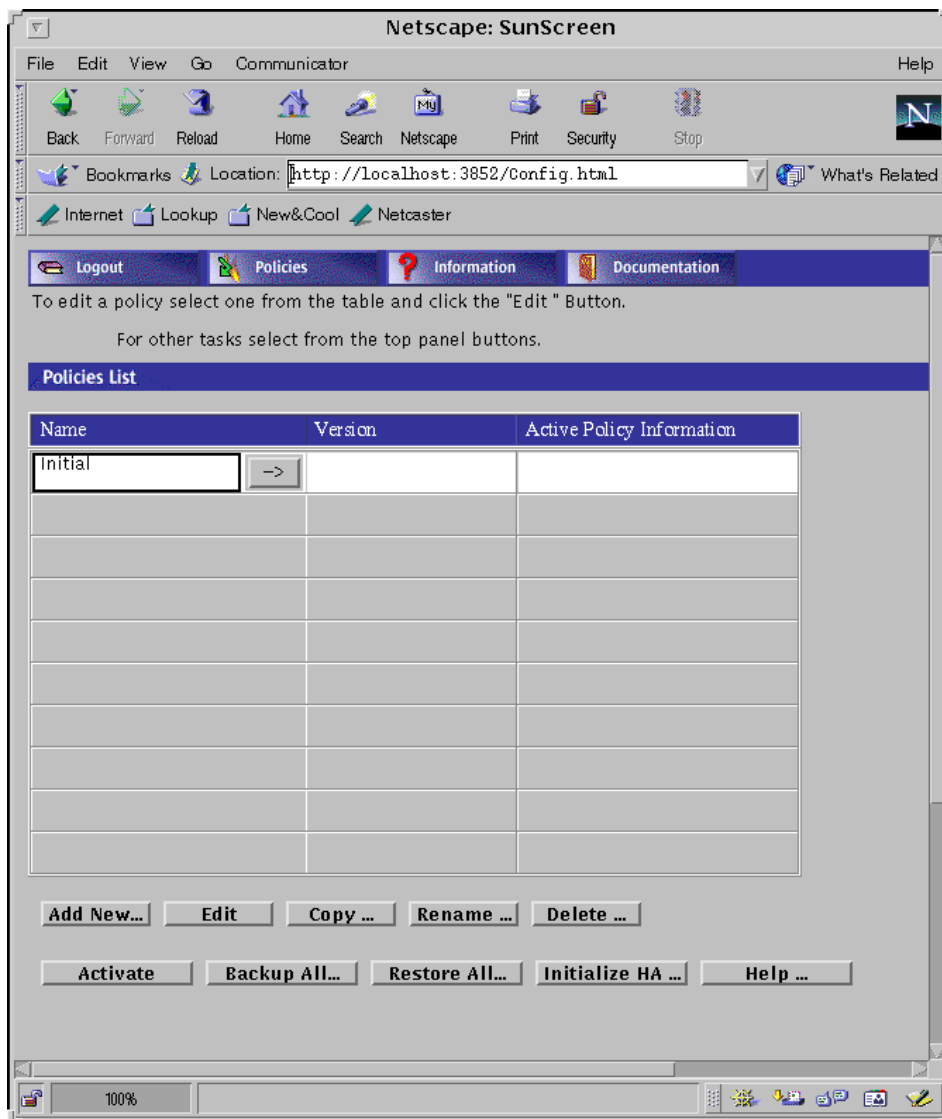


FIGURE 2-1 Policies List Page

When you installed the SunScreen EFS 3.0, you created a policy, named "Initial," that contains enough information so that you can administer the Screen.

▼ To View the Policies List Page

- **Click the Policies button in the SunScreen banner at the top of the administration GUI.**

The Policies List page is displayed when you click the Policies button.

Name Field

The names of your policies are listed in the Name field of the Policies List page.

Version Field

A version number is appended to a policy each time you click the Save Changes button, which is displayed in the Version field. You can see the policy versions by clicking the -> button in the Name field

Active Policy Information Field

Information about the active policy, including the date, is displayed in the Active Policy Information field. The active policy rule becomes green.

Policies

▼ To Add a New Policy

1. **Click the Add New... button in the Policies List page.**

The Add New Policy dialog window is displayed.



FIGURE 2-2 Add New Policy Dialog Window

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

▼ To Copy a Policy

1. Select the policy to be copied.
1. Click the Copy... button in the in the Policies List page.

The Copy... dialog window is displayed.

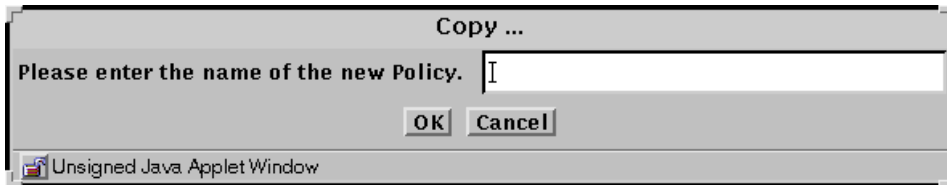


FIGURE 2-3 Copy... Dialog Window

2. Type the name of the new policy in the Copy... dialog window.
3. Click the OK button.

▼ To Rename a Policy

1. Select the policy to be renamed.
1. Click the Rename... button in the in the Policies List page.

The Rename... dialog window is displayed.

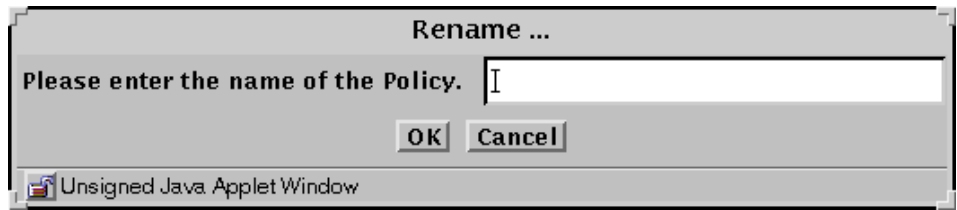


FIGURE 2-4 Rename Dialog Window

2. Type the name of the new policy in the Rename... dialog window.
3. Click the OK button.

▼ To Delete a Policy

1. Select the policy to be deleted.
1. Click the Delete button in the in the Policies List page.
The Delete Policy dialog window is displayed.

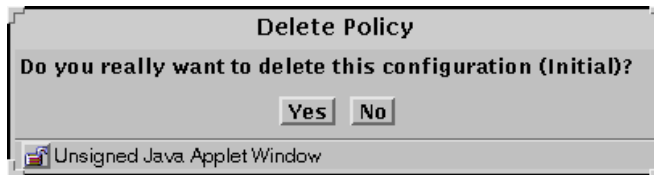


FIGURE 2-5 Delete Policy Dialog Window

2. Click the Yes button in the Delete Policy dialog window to delete the policy.

▼ To Back Up a Policy

Backing up your policies is useful, in case something should happen to the disk.

You should back up your policies frequently. You also should back up the original policy after you install SunScreen EFS 3.0. This makes it easier to restore earlier policies, if necessary. Backing up from the administration GUI backs up all the policies, but not the previous versions.



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 "Accessing Local System Resources."

1. Click the **Backup All...** button on the **Policies List** page to back up the current version of the policies.

The Select a backup file dialog window is displayed.

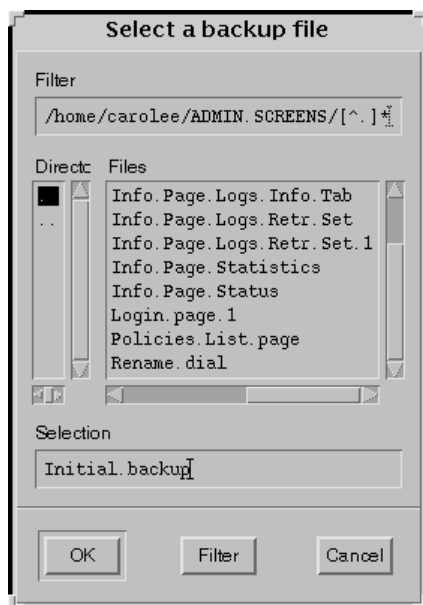


FIGURE 2-6 Select a backup file Dialog Window

2. Type the path name of the directory in the **Filter** field, and the name of the file in which the backup is to be saved in the **Selection** field.

▼ To Restore a Policy

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 "Accessing Local System Resources."

The Restore operation causes all current policy information to be over-written by the new information from the backup file.

1. **Select the policy to be restored.**
2. **Click the Restore All... button.**
3. **The Select a backup file dialog window is displayed.**
4. **Type the pathname of the directory in the Filter field, and the name of the file in which the logs are to be saved in the Selection field.**
5. **Click the OK button.**

▼ To Edit a Policy

The Policy Edit page is displayed when you click the Edit... button on the Policies List page.

Logout Policies Information Documentation

Save Changes Revert Changes Verify Policy

Common Objects

Type: Screen Add New

Search String Search on Screen Search Subtype: All Search

Results 0 found

Detail

Edit Delete Edit Detail Help

Policy Rules

Policy Name: Initial

Packet Filtering Administration Access NAT VPN

There is 1 packet filtering rule.

No.	Screen	Service	Source	Destination	Action	Time	Description
1		00000000	*	*	ALLOW		

Add New Edit Move Delete Help

FIGURE 2-7 Policy Edit Page

▼ To View the SunScreen Help Page

1. Click the **Help** button in the in the Policies List page.

The SunScreen Help page is displayed.

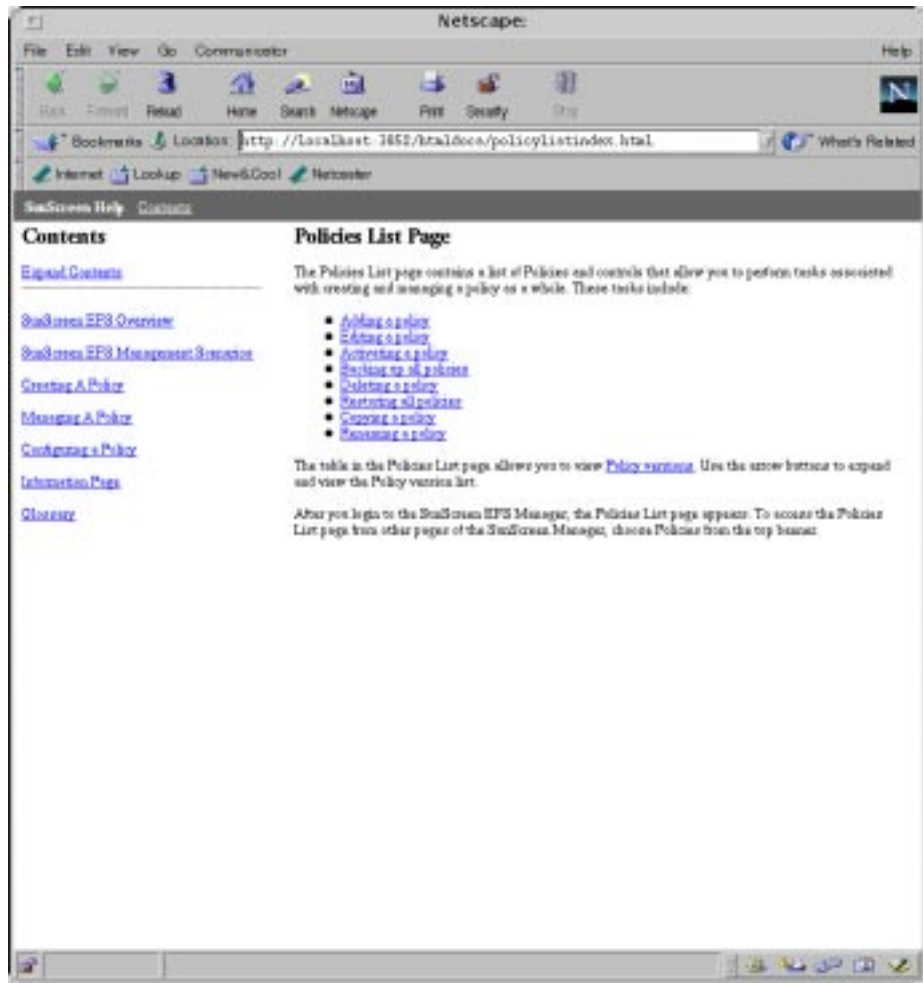


FIGURE 2-8 SunScreen Help Page

2. Click on a link to view the Help information on a particular subject.

Common Objects

This chapter describes:

- Changing the password
- Verifying, saving, and reverting a policy
- Common objects:
 - Adding a Common Object 42
 - Searching for a Common Object 42
 - Editing a Common Object 42
 - Viewing and Edit the Details of a Common Object 43
 - Deleting a Common Object 43
 - Renaming a Common Object 43
 - Adding a Time Object 44
- *Services and Service Groups*
- *Addresses*
- *Certificates*
- *Screens*
- *SNMP alert receivers*
- *Interfaces*

See Chapter 6 for information and procedures for:

- Proxy users
- Authorized users
- Spam
- Jar signatures
- Jar hashes

The "Initial" Policy

When you installed the SunScreen EFS 3.0, you created a policy, named “Initial,” that contains enough information so that you can administer the Screen.

▼ To Move to the Policy Edit Page

1. Select the policy “Initial.”
2. Click the Edit... button.

The Policy Edit page is displayed.



FIGURE 3-1 Policy Edit Page



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

During the installation, you created a default administration user account called `admin` with the password `admin`. Change this password as soon as possible to assure the security of the Screen.



Caution – Do not change the `admin` address (`1e0`, `qe0`, `hme0` and the like), the `admin` certificate, the local certificate, or the `admin-group` certificate. If you change these items, you risk losing your connectivity from the Administration Station to the Screen. Reestablishing your connectivity is difficult and requires that you log into the Screen directly or use an Administration Station that is still working. It also requires exchanging encryption information.

▼ To Change the Password

1. Select **Admin User** in the **Type** choice list in the **Policy Edit** page.
2. Click the **Search** button.
3. Select **Administrator** from the **Results** field.
4. Click the **Edit...** button.
Change the password in the **Authorized User** dialog window.
5. Click the **Save Changes** button.
6. Click the **Activate** button.

Verifying, Saving, Activating, and Reverting

▼ To Verify a Policy

- **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 selected policy file are verified for errors without activating the policy. Verifying a policy allows you to debug it without activating it.

▼ To Save Changes

- **Clicking the Save button saves all changes made for all objects and rules in the policy.**

An Activate Policy dialog window is displayed.

- **Choose Yes to activate the policy.**

▼ To Activate a Policy

1. **Click and highlight the name of the policy in the Policies List page.**
2. **Click the Activate button in the Policies List page to activate the policy.**

Messages are only returned if there are errors.

▼ To Revert Changes

- **To revert a policy to the last saved version, click the Revert Changes button after making any change.**

Changes made prior to clicking the Revert Changes button are not saved.

Adding Common Objects

Common objects are those objects common to all existing policies; hence, any modification to these objects would affect the operation of all policies. When changing these objects, consider the effect this can cause to any other policies. You add common objects in the Common Objects area of the Policy Edit page. The policy rules are constructed by using the common objects defined here.

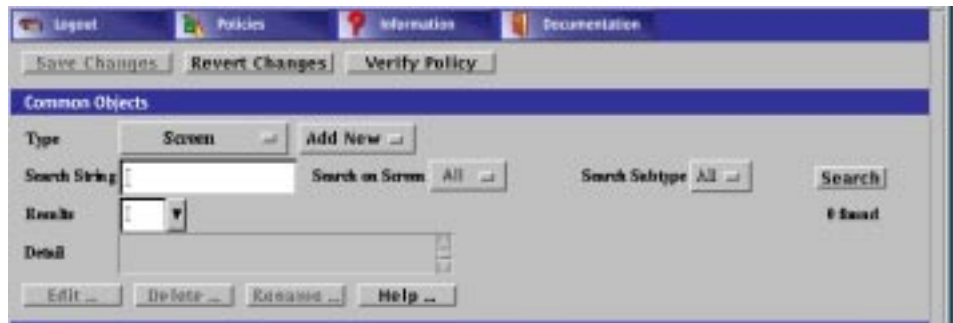


FIGURE 3-2 Common Objects Area

Note – The policy that is currently active is not affected by any changes until a policy is activated.

The Screen Field in all Policy Rules and Common Objects

The Screen field is a way to define the object or rule in a Screen-specific manner. It has no effect on a standalone Screen-administration scenario. Objects with the same name can be defined multiple times if they have different Screen objects selected. They can have different parameters, as well. Such objects are interpreted locally by the Screen to which they refer.

An *object* with "All" Screen objects selected applies to all Screens. This is the default, and is recommended for all objects, unless there is a need to define multiple definitions for a single name.

Similarly, *rules* with a blank Screen field apply to all Screens. Rules with a Screen object selected apply only to the Screen referred to in the rule.

▼ To Add a Common Object

All common objects are added by the same steps; the dialog windows displayed vary according to the common object selected.

1. **Select the common object in the Type choice list.**
2. **Click the Add New button to display the choices.**
3. **Type the necessary information in the dialog window that is displayed.**
4. **Click the OK button.**

▼ To Search for a Common Object

1. **Select a common object type in the Type choice list.**
2. **(Optional) Enter a character string that partly matches the name of the desired common object in the Search String field.**
3. **Click the Search button or click Enter in the Search String field.**

The results are returned after eliminating those that fail any one of the three search criteria for the selected type.

- **Search String:** This field restricts the search to names that match the character pattern in this field. Leaving the field blank returns all names.
 - **Search on Screen:** This field returns all objects when set to “All.” When a specific Screen is selected, it returns all objects that have a Screen object selected.
 - **Search Subtype:** This field returns all objects when set to “All.” If a specific subtype is selected, it returns those objects that are of that subtype
4. **Select a result from the Results field to retrieve and display its properties in the Detail field.**

After the common object has been retrieved, it can be edited, renamed, or deleted.

▼ To Edit a Common Object

1. **Select the Common Object in the Type choice list.**
2. **Select the search criteria.**
3. **Click the Search button.**
4. **From the Results list, highlight the name of the common object to edit.**

The details for the common object selected is displayed.

5. Click the Edit button.

The dialog window for the object is displayed.

6. Make the changes you wish in the common object dialog window.

7. Click the OK button.

▼ To View and Edit the Details of a Common Object

- **Click once on the cell in the Packet Filtering Table containing the object to be viewed or edited.**

The dialog window for the chosen object is displayed.

Note – Due to the non-uniqueness of names, sometimes it may not be possible to display the details for a cell. Users must then search for it, and select the relevant object.

▼ To Delete a Common Object

When you delete an address, range of addresses, or group of address, SunScreen EFS 3.0 checks to see that the address, range of addresses, or group of addresses is not being used in a policy object.

- 1. Select the Common Object in the Type choice list.**
- 2. Select the search criteria.**
- 3. Click the Search button.**
- 4. From the Results list, highlight the name of the common object to delete.**
- 5. Click the Delete button.**
- 6. Click Yes in the Delete Rule dialog window.**

▼ To Rename a Common Object

1. Select the Common Object in the Type choice list.
2. Click the Search button.
3. From the Results list, highlight the name of the common object to be renamed.
4. Click the Rename... button.

The Rename dialog window is displayed.

5. Type the new name in the Please enter the new name field.
6. Click the OK button.

Renaming a common object with no Screen object also renames all references to the object in the current policy, if the renamed object contains no references to a Screen object (that is, the object definition is not specific to any Screen).

▼ To Add a Time Object

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

1. Select Time in the Type choice list.
2. Select New... from the Add New choice list.

The Time dialog window is displayed.



FIGURE 3-3 Time Dialog Window

3. Enter a name in the Name field.

Example: `day`

4. (Optional) Enter a description in the Description field.

Example: `Business hours`

5. (Optional) Select a Screen from the Screen choice list.

6. Select Add Row.

7. Select the following;

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

8. Click the OK button.

Time Object Example

This Rule Definition dialog window shows use of the time object in a rule that allows all “www” service traffic during the “day” time (where “day” was defined in the Time dialog window).



FIGURE 3-4 Example Time Object in a Rule

By selecting a predefined Time object, this rule is applicable only for the time defined.

Services and Service Groups

Part of setting up your network security policy is to define the network services that will be available to hosts on your internal network and to hosts on the external network. Generally, most sites need to determine or set up policy rules that govern the basic services.

A number of *predefined* network services and service groups are provided, such as `ftp`, `telnet`, `dns`, and `rsh`. You can modify these services or define new services as needed.

Besides 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 the *SunScreen EFS 3.0 Reference Manual*.

SunScreen EFS 3.0 lets you define single services and service groups. Service groups consist of the single services that you want to use together. The services that are available for use in the policies were installed as part of the SunScreen EFS 3.0 software.

You can change the default values of a service or add a new service.

▼ To Add a Service

Note – Although you may change the default values for a service, to make any troubleshooting easier, it is better to add a new service with the new values.

1. **Select Service in the Type choice list.**
2. **Click New Single... from the Add New choice list**
The Service dialog window is displayed.



FIGURE 3-5 Service Dialog Window

3. Type the name for this new service in the Name field, for example:

ftp-34

4. (Optional) Type a description for this service in the Description field, for example:

ftp-34 uses port 34 instead of port 21. Use ftp-34 instead of the supplied ftp service.

The description will appear in the Service Details field that is displayed when you choose a service or service group for a rule using the Rule Definition dialog window.

5. (Optional) Select a Screen from the Screen choice list.
6. Click the down arrow of the Add Filter button on the Service panel to display the service filter choice list.
7. Select a filter from the Filter choice list.
 - You can use the Add Filter button as necessary to get the number of filters that you need for a particular service.
 - If you have too many filters, follow the steps below to delete them.
 - a. Click and highlight the parameters field of the line that contains the unwanted filter.

- b. Click the Delete button to delete the filter.**
- 8. Click the select box in the Filter field to display the list of service filter engines.**

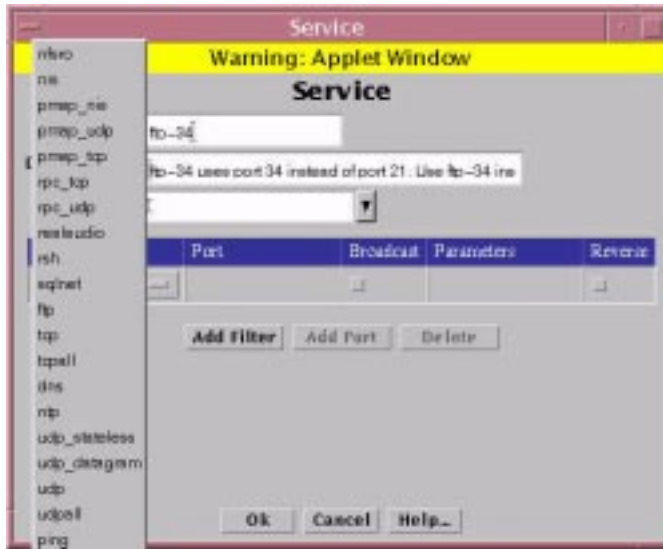


FIGURE 3-6 List of Filter Engines

- For each filter desired, follow the steps below:
 - a. **Click the select box under Filter.**
 - b. **Choose a filtering engine from the choice 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.
- 9. Type the port number for the new service in the Port field.**
- You can use the Add Port button as necessary to get the number of ports that you need for a particular filter.
 - 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. **Click the parameters field of the line that contains the unwanted port to highlight the line.**
 - c. **Click the Delete button to delete it.**

10. (Optional) Change the default values by typing the ones that you want to use, if you want to override the default values for the filter that you have selected.
11. 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.
12. Type the required number of parameters, separated by spaces, if you want to override the default parameters for the filter that you have selected.

You only need to type in parameters if you do not want to use the default values. The information for the default values for these fields is in the *SunScreen EFS 3.0 Reference Manual*.
13. Click **Reverse check box** if the service operates in the reverse direction.
14. Click the **OK** button to place this service definition in the policy file.
The service `ftp-34` now appears in the list of services.
15. Repeat the above steps until you have added all the services necessary for your policy.

▼ To Add a Service Group

Note – Although SunScreen EFS 3.0 lets you modify the default services in service groups, to make any troubleshooting easier, it is better to add a new service group that contains the services that you want.

1. Select **Service** in the **Type** choice list.
2. Select **New Group...** from the **Add New** choice list.
The Service dialog window is displayed.



FIGURE 3-7 Add New Group Service Dialog Window

- 3. Type the name for the new service group in the Name field in the Service dialog window.**
- 4. (Optional) Type a description for this new service group in the Description field.**
The description will appear in the Service Details field that is displayed when you choose a service or service group for a rule using the Rule Definition dialog window.
- 5. (Optional) Select a Screen from the Screen choice list.**
- 6. Click and highlight the service or service group that you want to include in this new service group.**
- 7. Click the Add button to move the selected service or service group to the Members list.**
- 8. Click the OK button.**
- 9. Repeat the above steps until you have added all the service groups required.**

Adding Addresses

SunScreen EFS 3.0 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. These address objects are then used in defining the network interfaces and as the source and destination addresses for Policy rules and for NAT. An address object can represent a single computer or a whole network. You can gather address objects representing individual and network addresses together 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.

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

An individual host is identified by linking its unique IP address to an address object, which can use the name or IP address of the host or some other identifier.

▼ To Add a Host Address

1. **Select Address in the Type choice list.**
2. **Click New Host... from the Add New choice list.**

The Address dialog window is displayed.

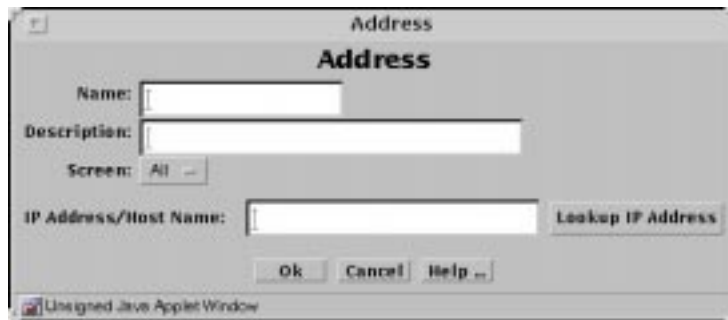


FIGURE 3-8 Address Dialog Window

3. Type the name for this new address in the Name field, for example:

NewAddr

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

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

5. (Optional) Select a Screen from the Screen choice list.

6. Type the IP address in the IP Address/Host Name field, for example:

100.100.20.10

7. Click the OK button.

▼ To Add a Range of Addresses

An address range is a set of numerically contiguous IP addresses. Networks and subnetworks are typically identified by an IP address range name. You use the beginning and ending addresses to identify an IP address range. You can set up an address object to represent an address range.

1. Select Address in the Type choice list.
2. Click New Range... from the Add New choice list.

The Address dialog window is displayed.



FIGURE 3-9 Address Dialog Window

3. Type the name for this new address range in the Name field, for example:

AddrRange

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

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

5. Select All from the Screen choice list.

6. Type the Starting IP address in the Starting IP Address field, for example:

100.100.20.10

7. Type the Ending IP address in Ending IP Address field, for example:

100.100.20.90

8. Click the OK button.

▼ To Add a Group of Addresses

1. Select Address in the Type choice list.
2. Click New Group... from the Add New choice list.
The Address dialog window is displayed.



FIGURE 3-10 Address Dialog Window

3. Type the name for this new address group in the Name field, for example:

GroupName

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

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

5. (Optional) Select a Screen from the Screen choice list.

6. Highlight the address in the Address list.

7. Click the top Add button to move to the Include list, or the bottom Add button to move to the Exclude list.

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

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

9. Click the OK button.

Certificates

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.

If you want to use encryption for traffic from the Screen (source address), you must either create a self-generated certificate, or use an existing certificate, and add a certificate for each address (destination address) to which the Screen will send traffic.

If you want to use encryption for traffic to the Screen (destination address) from an address on another network (source address), you must either add the issued public key for each address (source address) from which the Screen will receive traffic. The hash or public key must be sent to the destination address so that the traffic from the Screen can be decrypted.

Certificates can be combined into groups for ease of use and convenience.



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

▼ To Add Screen Certificates From a File or Diskette

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."

You can add new key pairs and local identities by using a SunScreen Key and Certificate diskette that is available from Sun Microsystems Certificate Authority. Contact Sun using the email address CArequest@sun.com. This diskette contains the private value, a signed certificate of the public value, and CA information. This type of key and certificate is known as an issued certificate. Certificates are described in the *SunScreen EFS 3.0 Reference Manual*.

You also can add new private keys from a directory that contains only one set of private key and certificate files.

▼ To Generate Screen Certificates

Note – The Installed On field in the Certificate dialog window allows you to select the Screen to whose SKIP database this certificate would be added.

The default is the Screen to which users are connected. It should be selected if Centralized Management Groups are being used.

Self-generated private keys use the SKIP NSID 8, signifying that the public value for that key has not been certified. 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), the public value can be certified by comparing the hash of the public value in the certificate with the certificate ID. Unsigned Diffie-Hellman certificates are described in the *SunScreen EFS 3.0 Reference Manual*.

1. Select **Certificate** in the **Type** choice list.
2. Select **Generate Screen Certificate...** in the **Add New** choice list.

The Certificate dialog window is displayed.



FIGURE 3-11 Certificate Dialog Window

3. Type a name in the **Name** field.
4. (Optional) Type a description in the **Description** field.
5. (Optional) Select the Screen from the **Screen** choice list.

6. (Optional) Type the name of the Screen on which the Certificate is installed in the Installed On field.
7. Click the radio button to specify the level of encryption the Screen uses.
8. Click the Generate New Certificate button.
The Certificate ID field displays the Certificate ID.
9. Click the OK button.

▼ To Load an Issued Certificate

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

1. Select Certificate in the Type choice list.
2. Select Load Issued Key Certificate... from the Add New choice list.
The Certificate dialog window is displayed.



FIGURE 3-12 Certificate Dialog Window

3. Type a name in the Name field.
4. (Optional) Type a description in the Description field.
5. Select the Screen from the Screen choice list.

6. Select the Screen the certificate is installed on from the Installed On choice list.
7. Click the Load Certificate button.
8. In the File dialog window:
 - a. select the directory of the floppy that contains the certificate files.
 - b. Click the Update button to make sure the directory contents are updated.
 - c. Select a file with .cert extension from the Files list.
 - d. Click the OK button.The Certificate ID field contains the value.
9. Click the OK button.

▼ To Load an Issued Public 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."

1. Select Certificate in the Type choice list.
2. Select Load Issued Public Certificate... from the Add New choice list.

The Certificate dialog window is displayed.

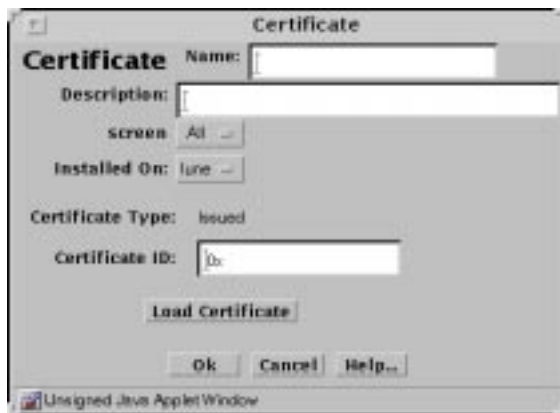


FIGURE 3-13 Certificate Dialog Window

3. Type a name in the Name field.
4. (Optional) Type a description in the Description field.
5. (Optional) Select the Screen from the Screen choice list.
6. (Optional) Select the Screen the certificate is installed on from the Installed On choice list.
7. Click the Load Certificate button.
8. In the File dialog window:
 - a. select the directory of the floppy that contains the certificate files.
 - b. Click the Update button to make sure the directory contents are updated.
 - c. Select a file with .crt extension from the Files list.
 - d. Click the OK button.

The Certificate ID field contains the value.
9. Click the OK button.

▼ To Associate Certificate IDs

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

Associate Certificate ID lets you assign a name to a Certificate that exists on another Screen. You associate a Certificate ID when you want to encrypt communication between two screens or between a Screen and an Administration Station.

1. Select Certificate in the Type choice list.
 2. Select Associate MKID... from the Add New choice list.
- The Certificate dialog window is displayed.



FIGURE 3-14 Certificate Dialog Window

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

▼ To Add a Certificate Group

After you have named Certificate ID s, you can group them into logical groups, so that you can use a group instead of single names in a policy object.

1. **Select Certificate in the Type choice list.**
2. **Select New Group... from the Add New choice list.**

The Certificate dialog window is displayed.



FIGURE 3-15 Certificate Dialog Window

3. Type a name in the Name field.
4. (Optional) Type a description in the Description field.
5. Select a Screen from the Screen choice list.
6. Click the Add >> button to move selections from the Available Certificates Area to the Group Members area.
7. Click the << Remove button to move selections from the Group Members area to the Available Certificates area.
8. Click the OK button.

Screens

You need to add a Screen only if you are configuring HA or Centralized Management Groups. For the standalone configuration, you may edit the Screen for adding SNMP or modifying miscellaneous properties.

▼ To Add a Screen

1. Select Screen in the Type choice list.
2. Select New... from the Add New choice list.

The Miscellaneous area in the Screen dialog window is displayed.



FIGURE 3-16 Screen Dialog Window, Miscellaneous Tab

3. In the Name field, type the name of the Administrative Interface of the Screen as it appears in the naming service or the `host` file.
4. Type a number in the Log Size (MB) field, to set the total size for log files (default is 100 Mb).
5. The SPF Network Address and SPF Netmask (of the network the Screen partitions) fields apply only if the Screen has SPF-type interfaces.
6. Click the Yes or No radio button to allow or deny Routing.
7. Click a Name Service radio button to select the name service the Screen will rely on.

8. Click the Yes or No radio button for Certificate Discovery.

This allows the Screen itself to participate in a certificate discovery exchange; not for traffic to go *through* the Screen.

9. Click the OK button.

SNMP Alert Receivers

You use the SNMP tab in the Screen dialog window to:

- Add a new SNMP trap receiver
- Delete an SNMP trap receiver

Actions that generate SNMP alerts are set as part of a security policy.

A management information base (MIB) that describes the SNMP trap is included with SunScreen EFS CD-ROM as part of the SUNWicgSA package. It is installed as:
`/opt/SUNWicg/SunScreenAdmin/etc/sunscreen.mib.`

Load this MIB into your SNMP manager to enable it to use the SNMP trap generated by the Screen.

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 then would be 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.

Setting SNMP in packet filtering rule's "Action," or in the default Reject Action of an interface causes the SNMP packets to be sent.

SNMP alerts are described in the *SunScreen EFS 3.0 Reference Manual*.

The following information describes using the administration GUI. For the command line interface, see Appendix A.

▼ To Add a New SNMP Alert Receiver

1. Click the SNMP tab in the Screen dialog window.

The SNMP area is displayed.

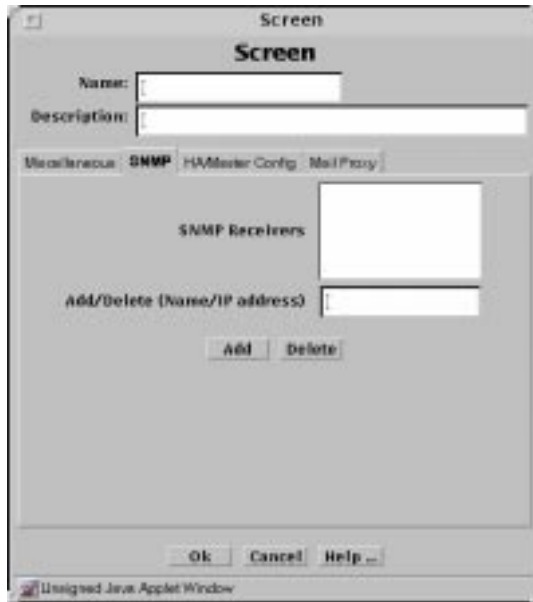


FIGURE 3-17 Screen Dialog Window SNMP Area

2. Type the name or IP address of the recipient of the SNMP trap in the Name field.
3. Click the Add button.
4. Click the OK button when you are finished.

▼ To Delete an SNMP Alert Receiver

1. Click the SNMP tab in the Screen dialog window for the Screen.

The SNMP area is displayed.

2. 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.

3. Click the Delete button.

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

Interfaces

A network interface is a network connection coming into a Screen through which one or more IP addresses are accessible. During installation in Routing mode, all empty address groups for all available network interfaces were defined. After you have completed the installation, you can add interfaces and redefine the addressees for the network interfaces, and set up High Availability. For each interface, specify the address group you have defined that contains all the addresses that can be reached through that interface.

The stealth-mode interfaces have optional Router entries.

Additional information can be found in the *SunScreen EFS 3.0 Reference Manual*.

Note – Define only the physical interface through the administration GUI if you are using a machine with logical (virtual) interfaces.

Note – Before you can configure a new interface, in the routing mode *only*, you must first configure it on your system using the documentation for your operating system.

▼ To Add or Edit Interfaces

Before you add a new interface, you must have defined the address group that this interface will use in the policy.

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

1. **Select Interface in the Type choice list.**
2. **Select New... from the Add New choice list beside the Interfaces area to display the Interface Definition dialog window.**

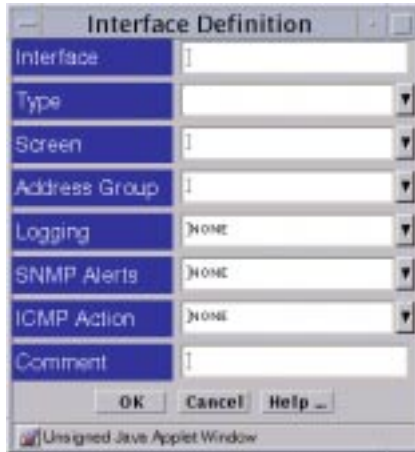


FIGURE 3-18 Interface Definition Dialog Window

- 3. Type the name of the interface that you want to add in the Interface field.**
- 4. Click the down arrow on the Type field to display the list of the interfaces.**
- 5. Click and highlight the type that you want.**
The type of interface appears in the Interface Type field.
- 6. Click the down arrow on the Screen field to display the list of Screens.**
- 7. Click and highlight the Screen that you want.**
- 8. Click the down arrow on the Address Group field to display the scrolling list of addresses and address lists.**
- 9. Click and highlight the address that you want.**
The address appears in the Address Group field.
- 10. Click the button to the right of the Logging field to display the list of kinds of logging available.**
- 11. Click and highlight the type of logging that you want.**
The type of logging appears in the Logging field.
- 12. Click the down arrow on the SNMP Alerts field to elect whether you want an SNMP alert.**
- 13. Click and highlight the type of SNMP alert that you want.**
The type of SNMP alert appears in the SNMP Alerts field.

14. Click the down arrow on the ICMP Action field to display the list of kinds of reject actions available.
15. Click and highlight the type of ICMP action that you want.
The type of reject action appears in the Reject Action field.
16. Click the OK button on the Interface Definition dialog window to save your interface definition.
17. Repeat the above steps until you have added all the interfaces that you require.

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

Policy Rules

This chapter describes:

- Packet filtering rules
- Viewing and Editing the details of an object in the Packet Filtering table
- Editing a rule
- Adding a rule
- Reordering rules
- Deleting rules
- Administrative access rules
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Verifying a policy

The following information describes using the administration GUI. For the command line interface, see Appendix A.

Packet Filtering Rules

▼ To View and Edit the Details of an Object

- **Click on the cell in the Packet Filtering Table containing the object to be viewed or edited.**

The dialog window for the chosen object is displayed.

▼ To Edit a Rule

1. Click and highlight the name of the policy whose rules you want to edit in the Policies List page.
2. Click the Edit button.

The Policy Edit page is displayed.

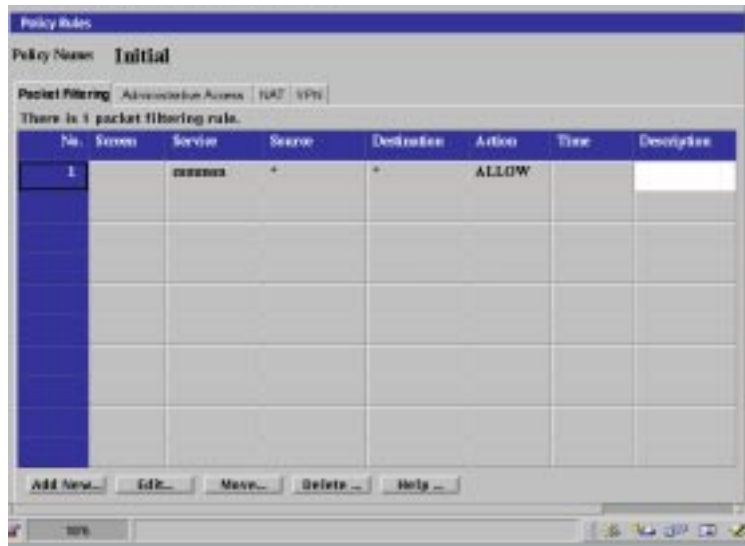


FIGURE 4-1 Policy Rules Area of the Policy Edit Page

3. Click the Packet Filtering tab in the Policy Rules area.
4. Click and highlight the rule to edit.
5. Click the Edit button.

The Rule Definition dialog window for the selected policy is displayed.

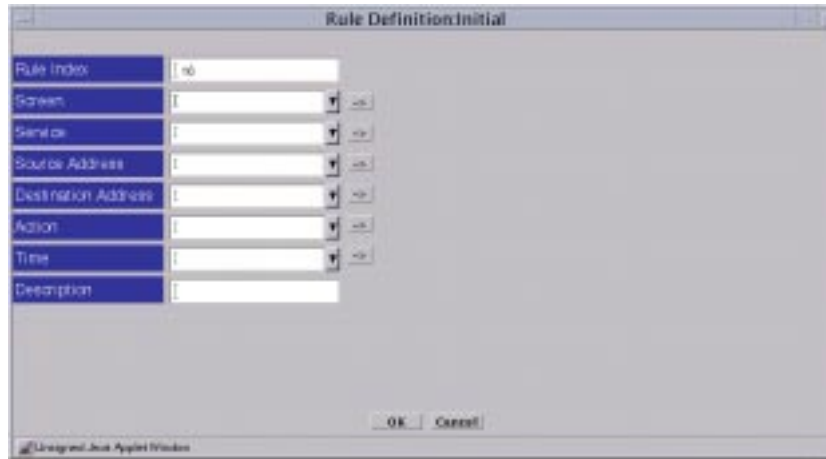


FIGURE 4-2 Rule Definition Dialog Window

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

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

7. Click the OK button in the Rule Definition dialog window when you have finished editing the rule.

8. Click the Verify Policy button at the top of the Policy Edit page to ensure that the changed rules will activate.

9. Click the Save Changes button.

▼ To Add a New Rule

1. Click the **Add New...** button in the **Policy Rules** area of the **Policy Edit** page.
The Rule Definition dialog window for the selected policy is displayed.

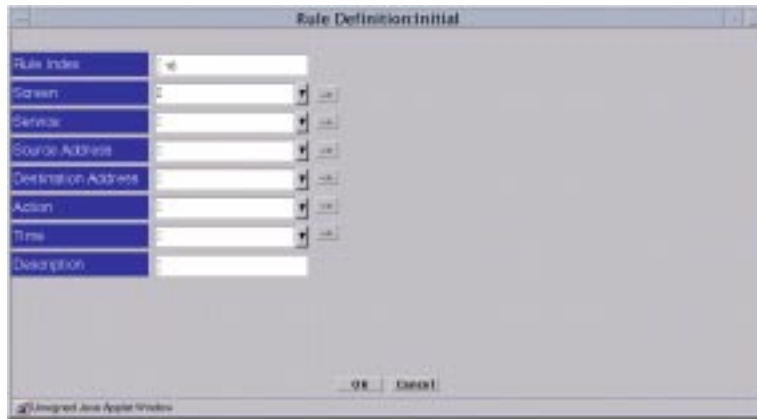


FIGURE 4-3 Rule Definition Dialog Window

2. Edit each field by clicking the down arrow to display the choice list.
3. Click the **OK** button when you have finished editing the rule.
4. Click the **Verify Policy** button at the top of the **Policy Edit** page to ensure that the rule will activate.
5. Click the **Save Changes** button.

▼ To Use the Move Button

1. Click the Move button to display the Move Rule dialog window.

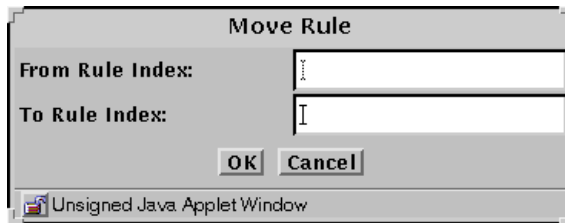


FIGURE 4-4 Move Rule Dialog Window

2. Type the number of the rule that you want to move in the From Rule Index field.
3. Type the number of the position to which you want to move the rule in the To Rule Index field.
4. 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.
5. Click the Verify button below the Rules area to confirm that the rules will operate successfully when you activate this policy.
6. Click the Save Changes button.
7. Click the Activate button in the Policy List page to activate this policy.

▼ To Delete a Rule



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

1. Select the rule to be deleted from the table in the Packet Filtering area.
2. Click the Delete... button.

The Delete Rule dialog window is displayed.



FIGURE 4-5 Delete Rule Dialog Window

3. Click the Yes button.

Administrative Access Rules

You use the Administrative Access Rules tab to:

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

You cannot create new users, passwords, or SecurID tokens on this page. (You add user, create and change passwords, and change SecurID names.) You can add new users that you have created and re-add users for whom new passwords have been defined or SecurID names have been assigned. You also can change the access level 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 EFS 3.0 Reference Manual*.

The following information describes using the administration GUI. For command line interface, see Appendix A.

▼ To Add an Administrative Access Rule for Local Administration

1. **Click the Administrative Access tab in the Policy Rules area of the Policy Edit page to move to the Administrative Access area.**



FIGURE 4-6 Administrative Access Area

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

The Local Access Rules dialog window is displayed.



FIGURE 4-7 Local Access Rules Dialog Window

In the Administrative Access definition dialog window, there are different fields for local and remote administration:

- Fields for Local Administration:
 - Rule Index
 - Screen
 - User
 - Access Level
 - Description

▼ To Add an Administrative Access Rule for Remote Administration

If you are adding an additional remote Administration Station, you must add a rule for it here either through the administration GUI or the command line (for the command line interface, see Appendix A).

Make a note of the encryption parameters that you are using, because they have to match the encryption parameters on the remote Administration Station.

- 1. Click the Administrative Access Rules tab in the Policy Rules area.**
- 2. Click the Add New... button in the for Access Rules for Remote Administration area.**

The Remote Access Rule dialog window is displayed.

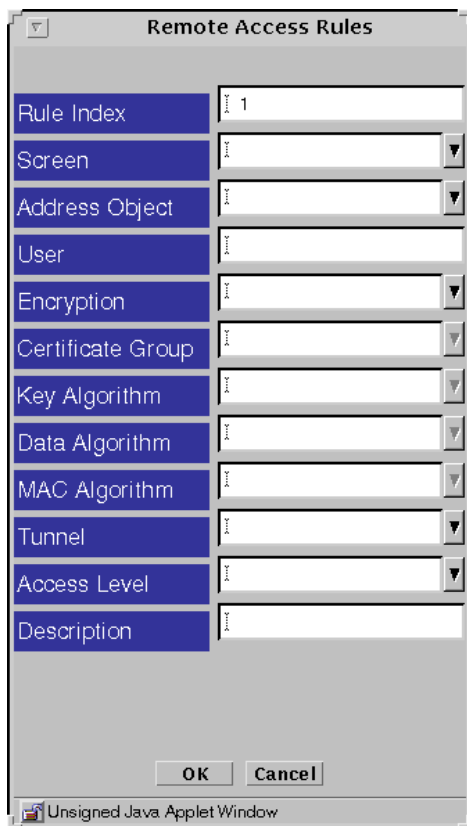


FIGURE 4-8 Remote Access Rules Dialog Window

Encryption can have two values: SKIP_VERSION_1, and SKIP_Version_2.

■ Fields for SKIP_VERSION_1:

- Select Certificate Group
- Select Key Algorithm
- Select Data Algorithm

■ Fields for SKIP Version 2:

- MAC Algorithm
- Access Level field:

ALL

WRITE

READ

STATUS

NONE

3. Click the down arrow on the Screen field to display the choice list of Screens.
4. Click the down arrow on the Address Object field to display the choice list of addresses.
5. Click and highlight the address that you want to use.
6. Type the authorized user name in the User field.
7. Click the down arrow on the Encryption field to display the choice list of the versions of SKIP.
SKIP_VERSION_1 is used for communicating with an SPF-100.
8. Click and highlight the version of SKIP that you want to use.
9. Click the down arrow on the Certificate Group field to display the choice list of certificate groups.
10. Click and highlight the certificate group that you want to use.
11. Click the down arrow on the Key Algorithm field to display the choice list of key algorithms.
12. Click and highlight the key algorithm that you want to use.
13. Click the down arrow on the Data Algorithm field to display the choice list of data algorithms.
14. Click and highlight the data algorithm that you want to use.
15. If you are using SKIP_VERSION_2 only, click the down arrow on the MAC Algorithm field to display the choice list of MAC algorithms.
16. Click and highlight the MAC algorithm that you want to use.
17. Click the down arrow on the Tunnel field to display the choice list of tunnel addresses.
18. Click and highlight the tunnel address that you want to use.
19. Click the down arrow on the Access Level field to display the choice list of the access levels.
20. Click and highlight the level of access that you want this user to have.

There are four access levels for remote administrators:

- ALL
- STATUS
- READ
- WRITE
- NONE (Default)

21. Click the OK button.
22. Repeat the above steps until you have added all the access rules for remote administration through the administration GUI, as required.
23. Click the Save Changes button.

▼ To Edit an Administrative Access Rule for Remote Administration

Make a note of the encryption parameters if you change them because they have to match the encryption parameters on the remote Administration Station.

Perform the following steps to make any changes through the administration GUI:

1. Click the Administrative Access Rules button to display the Access Rules page.
2. Click and highlight the rule that you want to edit in the area for Access Rules for Remote Administration Through the GUI.
3. Click the Edit button in the area for Access Rule for Remote Administration Through the GUI to display the Access Rules for Remote GUI Administration applet window access with the values for that rule.
4. Click the down arrow on the Address field to display the choice list of addresses.
5. Click and highlight the address that you want to use.
6. Type in Authorized User the User field to display the choice list of users.
7. Click and highlight the appropriate user.
8. Click the down arrow on the SKIP Version field to display the choice list of the versions of SKIP.
9. Click and highlight the version of SKIP that you want to use.
10. Click the down arrow on the Certificate Group field to display the choice list of certificate groups.
11. Click and highlight the certificate group that you want to use.
12. Click the down arrow on the Key Algorithm field to display the choice list of key algorithms.
13. Click and highlight the key algorithm that you want to use.
14. Click the down arrow on the Data Algorithm field to display the choice list of data algorithms.

15. Click and highlight the data algorithm that you want to use.
16. If you are using `SKIP_VERSION_2`, click the down arrow on the MAC Algorithm field to display the choice list of MAC algorithms (only available if selected `SKIP_Version_2`).
17. Click and highlight the MAC algorithm that you want to use.
18. Click the down arrow on the Access Level field to display the choice list of the access levels.
19. Click and highlight the level of access that you want this user to have.
20. (Optional) Type a description in the Description field.
21. Click the OK button on the Access Rules for Remote GUI Administration applet window access to enter your choices in the area for Access Rules for Remote Administration Through the GUI.
22. Repeat the above steps until you have edited all the access rules for remote administratyon through the administration GUI, as required.
23. Click the Save Changes button to save the definition to a file.

Network Address Translation (NAT)

Note – You can use NAT with SKIP when the encryption is used for communication in an encrypted tunnel (secure virtual private network). The encryption at the source tunnel address must take place *after* the NAT mapping and decryption at the destination tunnel address must take place *before* the NAT mapping.

The following information describes using the administration GUI. For the command line interface, see Appendix A.

Defining the Type of Mapping for NAT

The NAT tab allows you to set up mapping rules to translate IP addresses according to specific rules. These rules interpret the source and destination 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 EFS 3.0 installation.

In general, you would map addresses to:

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

Using the information from the worksheets and the addresses, ranges, and groups that you defined earlier, you can define the mappings of internal addresses to external addresses. Use the NAT tab in the Policy Rules area of the Policy Edit page to specify the address that is to be translated to a particular address, and to select whether you want static mapping or dynamic mapping. Additional information on NAT is in the *SunScreen EFS 3.0 Reference Manual*.

All network address translations happen before a packet is tested against any of the screening rules. In this way, all screening rules can be defined using only internal addresses. The four addresses NAT supports are:

- "Source"
- "Destination"
- "Translated Source"
- "Translated Destination"

NAT Administration GUI Tab

The meanings and uses of the specific fields in the NAT page are as follows:

No

- 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 (Optional)

- Use this field to specify the Screen for which you want the rule to apply. Enter 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.

Mapping

- *Static*

Specify static mapping to set up a one-to-one relationship between two addresses. Static mapping could be used to set new apparent IP addresses for hosts on your network without having to reconfigure each host.

- *Dynamic*

Specify dynamic mapping to map source addresses to other addresses in a many-to-one relationship. Dynamic mapping could be used 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 the packet appears to originate from is the translated source.

Translated Destination

- Specify the translated destination address for a packet. The translated destination is the actual address the packet goes to after it leaves the firewall.

Note – It is not possible to translate both source and destination addresses. That is, you cannot make packets appear to come from a different IP address and to simultaneously direct the packets to a different destination

Description

- Use this field to provide a description of the mapping defined in a rule.

All NAT rules are unidirectional. They work precisely as defined and are *not* interpreted as also applying in the reverse direction. So, 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 map the external destination address to the internal destination address with a second 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 to the external addresses that are 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.

Because in routing mode (unlike stealth mode), the Screen does not automatically answer ARP requests for destination address, the Screen must either route to a separate network that has a destination address, or an ARP request must be added manually.

Static NAT is a one-to-one mapping of the internal address to an external address, and 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 the *SunScreen EFS 3.0 Reference Manual*.

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

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

▼ To Add ARP Manually on a Screen in Routing Mode

- Type the following if the networks that attach to the Screen on the inside have NAT mappings applied, including any network on which there are addresses to which you want to allow public access:

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

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

▼ To Define NAT Mappings



Caution – When using NAT, be sure that:

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

1. Select the NAT tab in the Policy Rules area of the Policy Edit page to move to the Network Address Translation area.

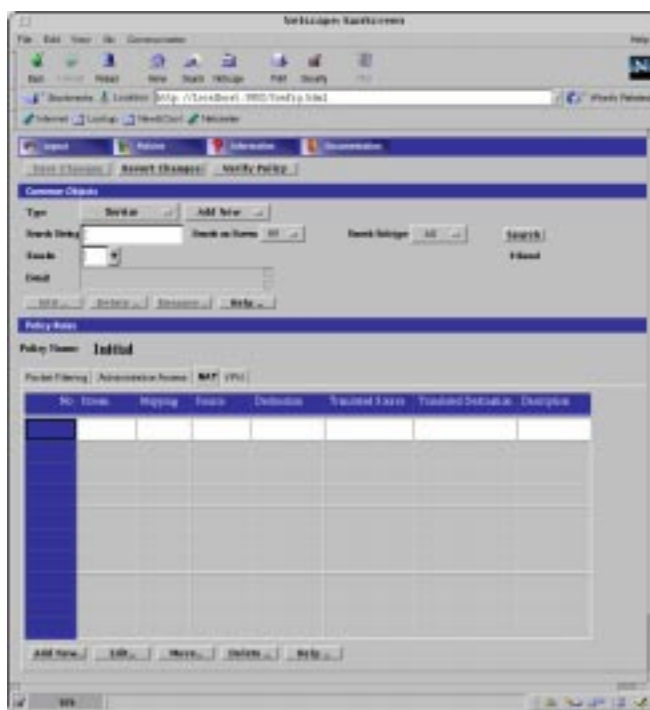


FIGURE 4-9 Network Address Translation Area

2. Click **New...** in the **Add New...** choice list below the **Network Address Translation** area to display the **NAT Definition** dialog window.

The image shows a Java Applet window titled "NAT Definition". It contains a form with the following fields: "Rule Index" (text input with "1"), "Screen" (dropdown menu), "Mapping" (dropdown menu), "Source" (dropdown menu), "Destination" (dropdown menu), "Translated Source" (dropdown menu), "Translated Destination" (dropdown menu), and "Description" (text area). At the bottom are "OK" and "Cancel" buttons. The status bar at the very bottom says "Unregistered Java Applet Window".

FIGURE 4-10 NAT Definition Dialog Window

3. Select a **Screen** if you want NAT mapping to be available for a particular **Screen**.
Default is NAT available for all **Screens**.
4. Select all four address in NAT Definition dialog window.
5. Click the **OK** button.
6. Repeat the above steps until you have edited all the mappings as required.
7. Click the **Save Changes** button to save the edited mappings to a file.

You must click the **Activate** button for the changes take effect.



Caution – When using NAT, be sure that:

- When you are defining a static mapping, the ranges and groups used in the **Source** and **Translated Source** fields are exactly the same size.
 - Also, when defining a static mapping, be sure that the ranges and groups used in the **Destination** and **Translated Destination** fields are exactly the same size
-

Note – Only source or destination addresses can be translated in a NAT rule, not both. Either the two source addresses are the same address or the two destination addresses are the same address.

In most cases when defining a static mapping, the internal address and external address are each a single address.

▼ To Edit the NAT Mappings

1. Select the NAT tab in the Policy Rules area of the Policy Edit page to move to the Network Translation area.
2. Click the Mapping field to choose the mapping on the table that you want to edit.
3. Click the Edit button below the Network Address Translation area to display the NAT Definition dialog window for that mapping.
4. Click the down arrow on the Mapping field to display the list of mappings.
5. Click and highlight the type of mapping that you want.

In most cases when defining a static mapping, the Source Address and Destination Address are each a single address.

6. Click the down arrow on the Source Address field to display the list of addresses.
7. Click and highlight the address that you want.

The new source address appears in the Source Address field.

8. Click the down arrow on the Destination Address field to display the list of addresses.
9. Click and highlight the address that you want.

The new destination address appears in the Destination Address field.

10. Click the OK button of the NAT Definition dialog window to save your edits.
11. Repeat the above 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.

Static NAT of a Host to a Host

The scenario illustrated below will translate the address of laguna to nathost for all destination addresses for all outgoing traffic.



The image shows a "NAT Definition" dialog box with the following fields and values:

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

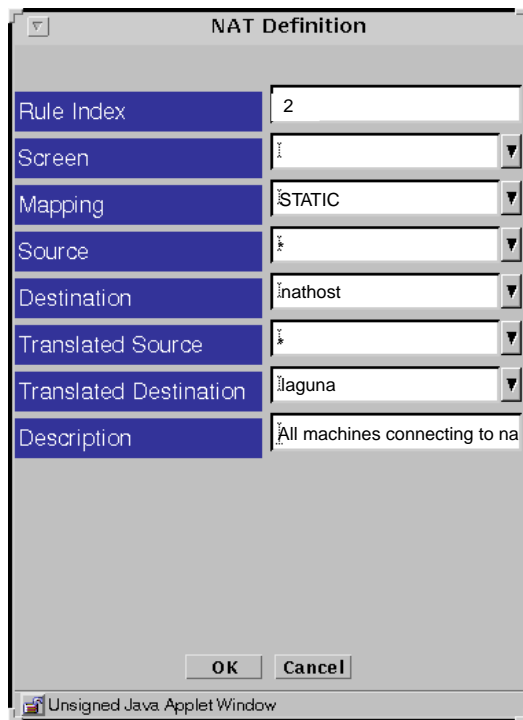
At the bottom of the dialog are "OK" and "Cancel" buttons. A status bar at the very bottom reads "Unsigned Java Applet Window".

FIGURE 4-11 Static Translation of a Host To a Host

The Reverse Rule

The scenario illustrated below will translate the address `nathost` to `laguna` for all source addresses for all incoming traffic.

One-way communication is allowed, so one of these rules may be used without the other.



The image shows a Java applet window titled "NAT Definition". It contains a table with the following fields and values:

Field	Value
Rule Index	2
Screen	1
Mapping	STATIC
Source	*
Destination	nathost
Translated Source	*
Translated Destination	laguna
Description	All machines connecting to na

At the bottom of the dialog are "OK" and "Cancel" buttons. The status bar at the bottom left indicates "Unsigned Java Applet Window".

FIGURE 4-12 The Reverse Rule

Dynamic Translation of a Range Of Addresses to One Host

In the scenario illustrated below, the translation occurs only when the destinations match what is in the “internet” address group. If the address was not in the “internet” address group, the source address would not be translated.

The image shows a "NAT Definition" dialog box with the following fields and values:

Field	Value
Rule Index	3
Screen	radiation
Mapping	DYNAMIC
Source	internal-104
Destination	internet
Translated Source	nathost2
Translated Destination	internet
Description	Translates the 104 net to nath

At the bottom of the dialog are "OK" and "Cancel" buttons. The window title bar at the very bottom reads "Unsigned Java Applet Window".

FIGURE 4-13 Dynamic Translation

Virtual Private Network (VPN)

▼ To Add a VPN Gateway

1. **Click the VPN tab in the Policy Rules area.**
2. **Click the Add New... button in the VPN area.**

The VPN Definition dialog window is displayed.
3. **(Optional) Type a number lower than the default entry in the VPN Gateway Index field, to place the rule in the position specified.**

The default for this field is one number higher than the last rule, which means its placement is at the bottom of the list. Typing a lower number in the VPN Gateway Index field places the rule in the position you specify.
4. **In the Name field, type the name of the VPN to which the gateway belongs.**

Type the same name for each gateway included in the VPN.
5. **Click the down arrow in the Address field to select the machine to be included in the VPN.**
6. **Click the down arrow in the Certificate field to select the gateway's Certificate ID.**
7. **Click the down arrow in the Key Algorithm field to select the key algorithm (or "none") to be used by the VPN.**

All gateways in the same VPN must use the same key algorithm.
8. **Click the down arrow in the Data Algorithm field to select the data algorithm (or "none") to be used by the VPN.**

All gateways in the same VPN must use the same data algorithm.
9. **Click the down arrow in the MAC Algorithm field to select the MAC algorithm (or "none") to be used by the VPN.**

All gateways in the same VPN must use the same MAC algorithm.
10. **Click the down arrow in the Data Algorithm field to 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. **Click the down arrow in the Tunnel Address field to select the tunnel address to be used by the VPN.**

12. (Optional) Type a description of the VPN gateway.
13. Click the OK button.
14. Click the Save Changes button.

▼ To Add a VPN Rule

When you have defined the gateways in your VPN, add a Packet Filtering Rule for the VPN.

The simplest rule uses "*" for the source and destination addresses, which allows encrypted use of the specified service for all addresses in the VPN.

▼ To Define a Single VPN

As a result of Centralized Management, the common objects and policy rules for all screens should be defined identically.

Create a VPN Gateway for each screen in the administration group. Associate them all with the same VPN name (for instance, "VPN"). Specify the certificate that each node will use to encrypt/decrypt packets (most likely the same Screen's certificate used for administration traffic).

Also specify the hosts "protected by" that VPN Gateway (probably the same as the Interface that connects to the internal secured network) with an Address from the common objects. Also select the set of algorithms to be used. Ideally, all VPN gateways in a VPN will have the exact same set of algorithms selected.

The simplest rule uses "*" for both the source and the destination addresses. To indicate that you want a rule to be part of the VPN, you refer to the VPN by name in the rule. You cannot use Proxies or SKIP-related data or DENY in a VPN-based rule.

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, it is not protected by a VPN gateway) will *not* be allowed to communicate by the VPN-based rule. You can create a separate rule that allows that particular host to communicate, but you must set that up by hand, as always.

The configuration described here is an example of a VPN with three screens (with their own certificates) that can communicate with each other:

- Screen-A is the Primary Screen, located in Los Angeles.

- Screen-B is a Secondary Screen, located in San Francisco.
- Screen-C is a Secondary Screens, located in New York.

Each screen protects its site, and the site names ("LA," "SF," and "NY" are the names of the Address Groups, which describe the networks behind the Screens.

In this example, the Address, "COMPANY" contains the Address Groups LA, SF, and NY. Furthermore, let the Address Group "Internet" be all ("*") minus COMPANY.

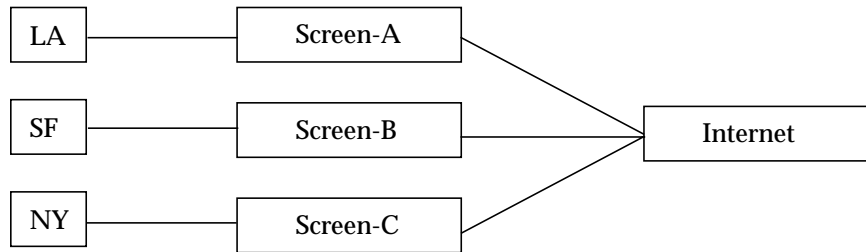


FIGURE 4-14 Example Address Groups

Define the three VPN rules as follows:

To telnet securely between sites, add rule at VPN gateway LA:

- Service: telnet
- Source address: COMPANY
- Destination address: COMPANY
- VPN name: VPN
- Comment: Sample

To allow LA to be able to ftp to SF securely, add rule at VPN gateway SF:

- Service: ftp
- Source address: LA
- Destination address: SF
- VPN name: VPN
- Comment: Sample

To allow SF to ping any host securely, add rule at VPN gateway SF:

- Service: ping
- Source address: SF

- Destination address: LA
- VPN name: VPN
- Comment: Sample

Information

This chapter describes these components of the Information page:

- Information
- Statistics
- Logs
- Documentation

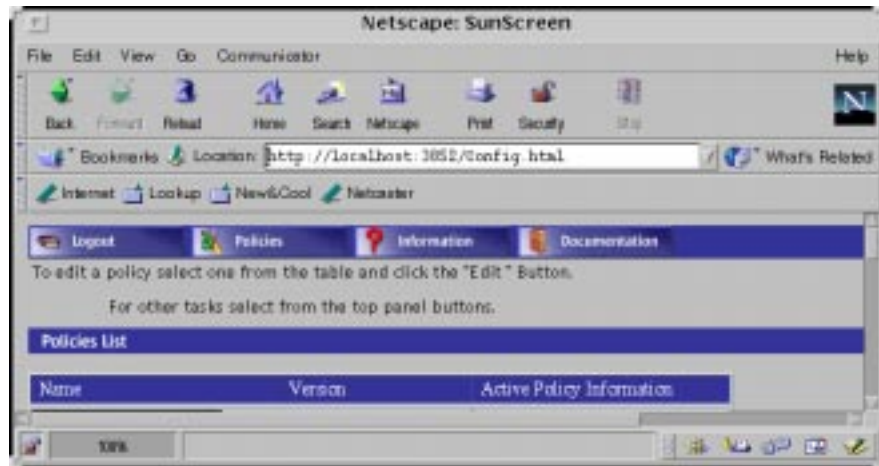


FIGURE 5-1 SunScreen Banner

Information Button

Click the Information button in the SunScreen banner to view statistics, logs and salient information such as product, system boot time, SunScreen boot time, version, and information about High Availability.

▼ To View the Information

1. **Click the Information button in the SunScreen banner.**

The Information page is displayed.

2. **Click the Status tab.**

The Status page is displayed.

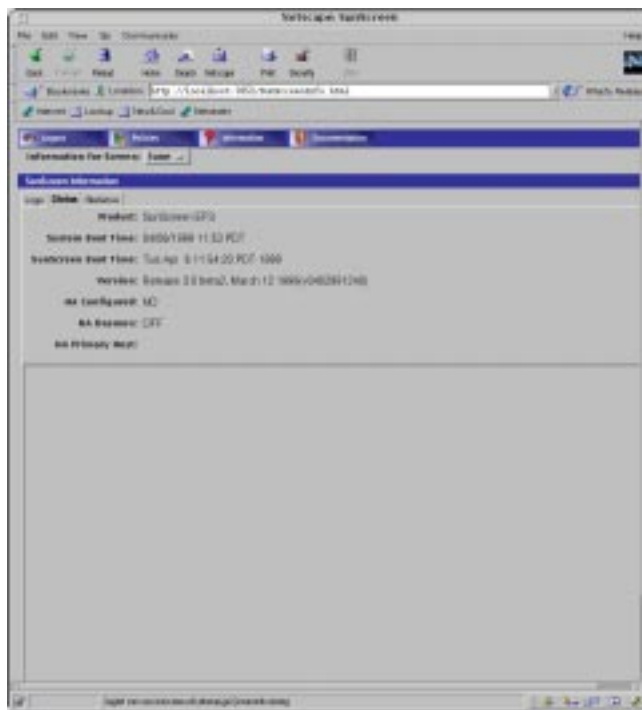


FIGURE 5-2 Status Page

The Status page shows SunScreen EFS 3.0 product information as well as HA configuration information.

Statistics Button

The Statistics area shows the traffic statistics for each interface.

The various fields for the interface, SKIP key management, SKIP key statistics, and SKIP header statistics are described in the *SunScreen EFS 3.0 Reference Manual*.

▼ To View the Statistics

- 1. Click the Information button in the SunScreen banner.

The Information page is displayed.

- 2. Click the Statistics tab.

The Statistics page is displayed.

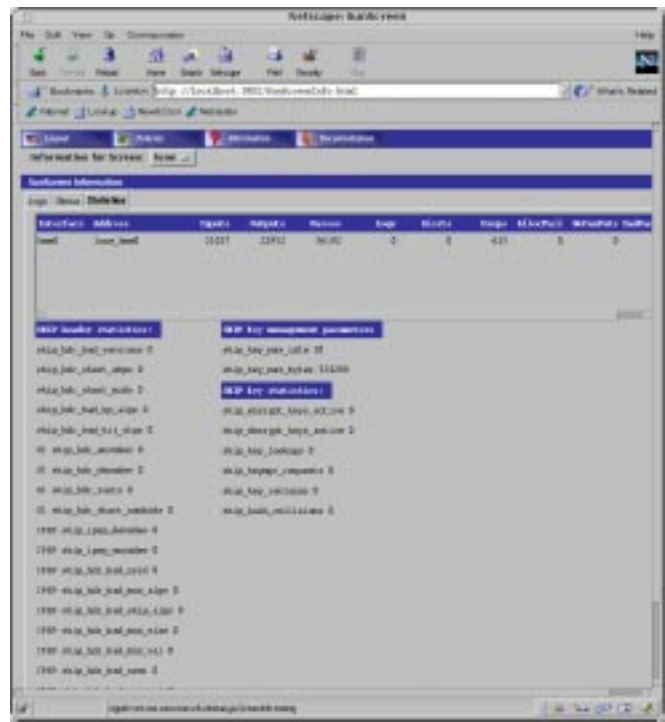


FIGURE 5-3 Statistics Page

Logs

Logged packets are viewed via the Log tab. SunScreen EFS3.0 can be configured in the packet filtering rules so that a packet can be logged when it matches or even when it does not match a particular policy rule criterion.

▼ To Set the Retrieval Mode

1. **Click the Information button in the SunScreen banner.**

You can read and change the retrieval settings of the log browser without acquiring the lock.

2. **Click the Log tab in the Information page.**

The Log page is displayed.



FIGURE 5-4 Retrieval Settings Tab in the Log Area

3. Click the Retrieval Settings tab at the bottom of the log.

The two retrieval modes are Historical and Real Time.

- Historical mode allows you to examine a particular segment for particular time.
- Real Time mode displays the information as the packet are passing through the Screen in real time.

Note – You must use four digits in specifying the year, for example, 2000.

The Historical... Reference Time 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.

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. This time is displayed on the Information page. Click the Fetch More Records button to retrieve more log records.

If the log is set to Real Time... Poll Interval and you click the Apply button again, the display is updated to show the most recently logged records. This is useful after the Log Browser has been running in Real Time mode for a while. Depending upon your configured settings, records will be logged faster than the Log Browser polls for new records. Thus, the display falls more and more behind as time goes on. Sometime you may want to see the most recently logged records.

The Information tab provides the current log statistics.

▼ To Set a Log Viewing Filter

The Log Browser uses a powerful language to filter log events to be displayed. This language is identical to the filtering options of the `logdump` command-line program; it is a superset of the language used by the Solaris `snoop` packet monitor tool.

The Log Browser allows full access to this language via the Current Filter text entry box in its Retrieval Settings tab. An arbitrary “logdump” expression can be entered there and activated using the Apply button.

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 and/or entering a target (operand) in the right-most pulldown. After this selection and/or entry, clicking the Add to Current Filter button causes these items to be added to the Filter Keywords text entry box at its current insertion pointer.

The left-center pulldown box provides filtering terms and which are self-complete and restrict the type of log event displayed. The items provided are:

loglvl pkt	Allows display of network packet-type events
loglvl sess	Allows display of network session-type events
loglvl auth	Allows display of events related to authentication operations
loglvl app	Allows display of events related to screen application (usu. proxy) operations
logapp edit	Allows display of events related to registry and/or policy editing
logapp ftp	Allows display of events from the FTP proxy
logapp log	Allows display of events related to the logging facilities themselves
logapp http	Allows display of events from the HTTP proxy
logapp smtp	Allows display of events from the SMTP proxy
logapp telnet	Allows display of events from the Telnet proxy
logsev emerg	Allows display of events of an emergency severity
logsev alert	Allows display of events of an alert severity or above
logsev crit	Allows display of events of a critical severity or above
logsev err	Allows display of events of an erroneous severity or above

logsev warn	Allows display of events of a warning severity or above
logsev note	Allows display of events of a notice severity or above
logsev info	Allows display of events of a informative severity or above (all non-debug events)
logsev debug	Allows display of events of a debug severity or above (all events)

The right-center pulldown box provides filtering terms most of which are incomplete, requiring an operand value (entered in the right-most pulldown box). The items provided are:

logwhy <i>reason#</i>	Restricts display to packets which have the given logging reason why code
logiface <i>iface</i>	Restricts display to packets which 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>
gateway <i>gwyaddr</i>	Restricts display to packets which used <i>gwyaddr</i> s a gateway
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

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`)

As previously mentioned, the right-most pulldown of Filter Keywords is used for entry of operand information.

Saving and Clearing the Log

Note – Users with access level STATUS cannot perform Save or Clear operations on the logs.

▼ To Save the Log

Note – Some browsers do not allow you to perform save operations. 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.

Note – Saving a log to a file does not clear the log records from the Log page.

1. **Click the Information button in the SunScreen banner.**

The Information page is displayed.

2. **Click the Log button.**

The Log page is displayed.



FIGURE 5-5 The Log Page

3. Click the **Historical...** button to set the **Historical** mode.
4. Click the **Save Log** button at the bottom of the **Log** page.
The **Save File** dialog window is displayed.
5. Type the pathname of the directory, and the name of the file in which the logs are to be saved.
6. Click the **Save** button.

▼ To Clear the Log

The following steps clear the page of any log records (without saving them) as well as the log file.

1. Click the **Information** button in the **SunScreen** banner.
The **Information** page is displayed.
2. Click the **Log** button.
The **Log** page is displayed.
3. Click the **Clear Log** button.

▼ To Save and Clear the Log

The following steps clear the display of any log records and save the log file.

1. **Click the Information button in the SunScreen banner.**

The Information page is displayed.

2. **Click the Log button at the bottom of the Log page.**

The Log page is displayed.

3. **Click the Save/Clear Log button.**

The Save File dialog window is displayed.

4. **Type the pathname of the directory, and the name of the file in which the logs are to be saved.**

5. **Click the Save button.**

▼ To Alter the Log File Size for a Specific Screen

1. **From the Policies page, select and edit the policy to be altered.**

2. **Select the desired Type: Screen common object.**

3. **Edit the Screen common object.**

4. **Alter the Log Size entry in the Miscellaneous tab.**

5. **Save the change in Save Changes.**

6. **Activate the policy.**

7. **Restart the Screen for the log file size change to take effect.**

Special Tasks

This chapter describes:

- Setting up High Availability
- Setting up and using Proxies
- Adding an additional Remote Administration Station
- Configuring Centralized Management Groups

The following information describes using the administration GUI. For the command line interface, see Appendix A.

Setting Up High Availability

To use High Availability (HA), you must install SunScreen EFS 3.0 as an HA system. High Availability, its limitations, topology and set up, and capability are described in the *SunScreen EFS 3.0 Reference Manual*.



Caution – The network that is 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 together in situations where the connection between a protected inside network and a nonsecure 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 as the active HA Screen, and mirror the state 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.

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 the HA cluster will use. When you activate the policy, the SunScreen EFS and SKIP policies are copied from the Primary HA Screen to the other members of the HA cluster. Solaris policy settings, such as network interfaces and routing configuration, are not copied from the Primary HA Screen, and must be identical on all the Screens in the HA cluster.



Caution – Keep the HA network physically secure because 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 the dedicated internal network connection. Similarly, you must assign Screens in the HA cluster the same IP addresses on their non-dedicated interfaces.

Preparing to Install High Availability

High availability consists of one active HA Screen (active host) and of at least one passive HA Screen (but no more than 31 passive HA Screens or passive hosts). For instance, if the active HA Screen fails, one of the passive HA Screens becomes active. Because the passive HA Screens do not forward, reject, or log packets, the CPU and I/O load on the passive HA Screens is less than that of the active host. This reduces the probability that software or load-induced faults affecting the active HA Screen will affect the passive hosts as well.

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

- It is more reliable to use the `/etc/hosts` file for hostname resolution than it is to use 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.

Modifying the HA Service Group

You cannot connect to a passive HA Screen directly except with remote administration to the HA interface. You also cannot 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, and heartbeat (the communication between or among HA Screens to assure that the dedicated HA network is working). Adding additional services or service groups might 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 using `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 EFS filters.

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

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

Using NAT with HA in Routing Mode

Depending on the configuration for NAT that you are using, 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 will work after a fail-over. You must replicate all non-EFS 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, it is easier if you automate this in one of your start-up scripts. For more information on configuring NAT, see the *SunScreen EFS 3.0 Reference Manual*, and for more information on ARP, see the man page for `arp`.

▼ To Install High Availability

The following is an overview for installing the SunScreen EFS 3.0 software and of configuring HA:

1. Configure identical interfaces on all HA machines, by editing the `/etc/inet/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. (This is 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 6-1. 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.) You connect the secondary Screen, for example, HA2 as shown by the broken line in FIGURE 6-1, to the hubs after you have installed, configured, and tested the Primary, active HA Screen and after you have installed and configured the Secondary HA Screen

You do not have to install any special software for HA other than installing SunScreen EFS. The HA software is automatically installed as part of SunScreen EFS.

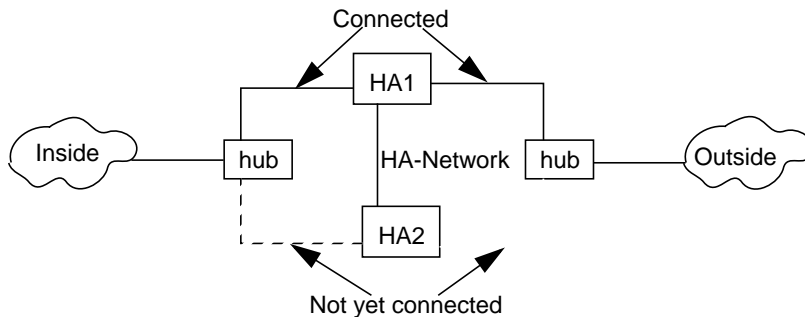


FIGURE 6-1 Wiring Before and During HA Configuration

▼ To Install HA on the Secondary HA Screen

1. Install EFS 3.0 on the Screen designated to be the Secondary HA Screen.

Accept default settings on all install screens except for the Secondary HA Configuration dialog window:

2. Select YES.

The Secondary HA Data dialog window is displayed.

3. In the Secondary HA Data dialog window:

- fill in the HA Interface field.
- fill in the Primary HA IP Address field.

4. Click the OK button.

The Secondary HA Configuration dialog window is displayed.

5. Reboot the Secondary HA Screen.

▼ To Install HA on the Primary HA Screen

1. Install EFS 3.0 on the Screen designated to be the Primary HA Screen.

Accept default settings on all install screens.

2. Log in to EFS 3.0.

The Policies List page is displayed.

3. In the Policies List page, click on Initialize HA.

The Initialize HA dialog window is displayed.

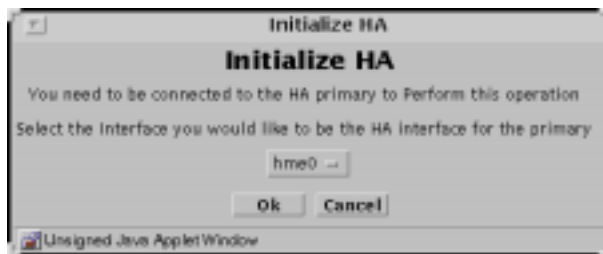


FIGURE 6-2 Initialize HA Dialog Window

4. Choose the interface to be the HA interface from the Interface choice list.

Note – The HA interface on the Primary HA Screen and Secondary HA Screen must be the same.

5. Click the OK button

The Policies List page is displayed.

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

1. Click the Edit button on the Policies List page.

The Edit Policy page is displayed.

2. Select Screen from the Type choice list.

3. Select New... from the Add New choice list.

The Screen dialog window is displayed

4. Enter the name of the Secondary HA Screen in the Name field.

5. Click the HA/Master Configuration tab in the Screen dialog window.



FIGURE 6-3 Screen Dialog Window HA/MasterConfig Area

6. Enter the following in the HA/MasterConfig area of the Screen dialog window:

- High Availability choice list: Secondary
- HA Primary Name: Name of Primary Screen
- Administrative IP Address: Leave blank.
- High Availability IP Address: Secondary Screen IP address

7. Click OK.

8. Click the Save Changes button on the Policies List page.

The Activate Policy? dialog window is displayed.

9. Click YES.

10. Fully connect the Secondary HA Screen to the network.

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, you must direct the Secondary Screen to become passive in order to communicate with the Primary Screen.

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.

Primary means the HA administration host for the HA configuration. It does not mean that it is the active host, necessarily.

Configuring HA

Policy Rules are configured by connecting to the active HA Screen. You configure the HA cluster just as you configure a single 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 active HA Screen transfers the configuration, including certificates, local keys, addresses, policy rules, and the like, to all other Secondary HA Screens.

When an HA host is in the passive mode, it is impossible to 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 other 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 choice list on the Edit Policy page, and add the services you want to include.

Adding these services to the HA service group permits you to circumvent the passive HA mode and allows the traffic through the SunScreen EFS filters even when the host is in the passive mode.

Defining HA

You must use the unique HA interface address for administration. If one of the shared address is used, then that address will always resolve to the HA host that is currently active. Since the active host is not necessarily the Primary administration host, there is no other way to ensure that you are communicating with the correct host.

If you do not do this, then, if the remotely administered Primary HA Screen is shut down, the connection will be lost and the administration GUI will hang immediately. You can still 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 that will not propagate the configuration to any other HA Screen. The configuration will be overwritten when the Primary HA Screen is up again.

▼ To Define HA

- 1. Select Screen from the Type choice list.**
- 2. Select New... from the Add New choice list.**
The Screen dialog window is displayed.
- 3. Click the HA/MasterConfig tab.**
The HA/MasterConfig area is displayed.
- 4. Click the OK button.**
- 5. Click the Save Changes button to save the new interface definition.**

▼ To Set (Change) the Primary HA Screen

1. Select Screen in the Type choice list.
2. Click and highlight the name of the HA Screen that you want as the Primary HA in the HA Host field.
3. Click the Set Primary button in the High Availability panel.

The HA host is set as the Primary HA Screen. All changes take place immediately.

Upgrading a SunScreen EFS 2.0 HA System

▼ To Upgrade the Primary HA Screen in an HA Cluster From SunScreen EFS 2.0 to SunScreen EFS 3.0

- Follow the instructions on upgrading and for filling in the data required as found in the Installation Guide.

Note – After upgrading the HA cluster primary Screen, it still knows that it is part of an HA cluster.

▼ To Upgrade Secondary HA Screens in an HA Cluster From SunScreen EFS 2.0 to SunScreen EFS 3.0

Note – Do *not* run the upgrade on an HA cluster secondary Screen.

1. Remove SunScreen EFS2.0 packages from the Screen by following the instructions found in the SunScreen EFS 2.0 Installation Guide.
2. Install SunScreen EFS 3.0 and set it up as an HA cluster secondary Screen by following the instructions found in the *SunScreen EFS 3.0 Installation Guide*.

Removing HA

Removing HA involves removing both software and hardware. Simply disabling 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 leaves two or more HA Screens on the network that are trying to route the same traffic. This would disrupt the network traffic through the Screens.

You should remove the HA hosts one at a time to reduce the chances of disrupting the network. If you remove the *active* HA host, you could lose some connections. If you are removing a *passive* HA host, no connections will be lost. You should, therefore, remove the passive HA host or hosts first to avoid losing connections.

If you must remove the active HA host, find out if any connections may be lost by running the following command on the active HA host that you want to remove and on the passive HA host that will become the active HA host after you remove the active HA host.

- **For local administration:**

```
# ssadm lib/statetables
```

- **For remote administration:**

```
# ssadm -r <Name_of_Screen> lib/statetables
```

Note – If SunScreen EFS 3.0 is running on a 32-bit Solaris, use `lib/statetables`; If SunScreen EFS 3.0 is running on a 64-bit Solaris, use `lib/statetables64`.

If the statetables 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`

Setting Up and Using Proxies

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

The following is the sequence of tests that each proxy makes to determine whether a rule matches:

1. Is the source address of the packet in source-address range in the policy rule?
2. Is the destination address of the final connection (that is, 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 correctly authenticate?
Is that user enabled?
4. Is the user who (possible anonymous) was authenticated is that user in the policy rule (either directly or by group membership)? If by group reference, is each entry on the path to the user entry enabled?

Note – At present, there is no way for SunScreen EFS 3.0 High Availability systems to share proxy state. Proxies are not highly available.

Preparing to Use Proxies

Four proxies have been developed for SunScreen EFS 3.0:

- FTP
- TELNET
- SMTP
- HTTP

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

The `rc` script, `proxy`, located in `/etc/init.d` and the symbolic link to `/etc/rc2.d/S79proxy` is used to start up the proxies as needed. The script checks if the proxy executable is in `/opt/SUNWicg/SunScreen/proxies`, that the corresponding policy file is in `/etc/opt/SUNWicg/SunScreen/proxies`, and that the policy file has a size larger than zero. If these requirements are not met, the proxy will not be started.

Note – Each policy rule compiler uses this script to cause the each proxy to reread its policy file as needed. You can also cause each proxy to reread its policy file.

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 EFS 3.0 Reference Manual* for further details.

▼ To Configure the Browser for the HTTP Proxy

This procedure is for configuring the HotJava browser. Consult the documentation for the browser that you are using to determine how to set the HTTP proxy sever address and port number. The server address should be the Screen's address and the port number must be 80.

1. Click the down arrow on Preferences to display the choice list.
2. Click and highlight Proxies to display the Proxies page.
3. Type the name of the Screen or its IP address in the HTTP field.

4. **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 EFS 3.0.

5. **Click the Apply button at the bottom of the Proxies page to set these choices as defaults.**

Defining Proxy Data on the Policy Edit Page

The databases for proxies are the Java archive (Jar) Signatures, Jar hashes, the Proxy Users, and SMTP Proxy data.

Adding Jar Signatures and Jar Hashes

Note – Make sure that you have set Medium Security for HotJava for both Signed and Unsigned Java as the default security settings. If you are using another browser, see the documentation that came with it.

You administer the Screen through any browser that supports Java and is compliant with Java Developers Kit (JDK) 1.1.

The administration GUI works with any of the following browsers that support the Java Runtime Environment, Version 1.1 (JRE 1.1.3).

- HotJava 1.1
 - Internet Explorer, with Sun's Java plug-in 1.1
 - Netscape, with Sun's Java plug-in
 - Specified versions of Netscape, with Netscape's own Java
 - Specified versions of Internet Explorer, with Internet Explorer's own Java
-

Jar Signatures and Jar hashes are described in the *SunScreen EFS 3.0 Reference Manual*.

▼ To Add a Jar Signature

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.)

1. Select Jar Signature from the Type choice list.
2. Select New... from the Add New choice list.

The Jar Signature dialog window is displayed.



FIGURE 6-4 Jar Signature Dialog Window

3. Type a name in the Name field.
4. Repeat the above steps until you have added all the certificates.
5. Click the Save Changes button to save this file.

▼ To Add a Jar Hash

1. Select Jar Hash from the Type choice list.
2. Select New... from The Add New button.

The Jar Hash dialog window is displayed.

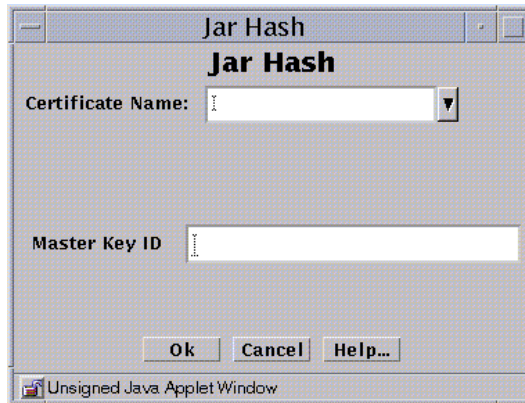


FIGURE 6-5 Jar Hash Dialog Window

3. Type the name for this certificate in the Certificate Name field.
4. Type the name for this certificate in the Certificate Name field.
5. Type the Master Key ID of the Jar file in the Master Key ID field.
6. Repeat the above steps until you have added all the certificates.
7. Click the Save Changes button to save this file.

Proxy Users

The Proxy Users database depends on information in the authorized users database. You must define a user first in the Authorized User area in the Policy Edit page.

You have to create entries for both authorized users and proxy users to use the authentication feature of the FTP and Telnet proxies.

The proxy user is a database that contains the mapping information for users of SunScreen EFS 3.0 proxies. The FTP and Telnet rules reference the proxy user entries. Additionally, a user connecting through either of these proxies will often be configured to require authentication using an authorized user identity.

Proxy users are used in FTP and Telnet proxy rules. Users logging in using a Telnet proxy are authenticated through the authorized user identity.

Names of proxy users must not contain the following characters: !, @, #, \$, %, ^, &, *, {, }, [,] , <, >, “, ‘, \ or, ?. It also must not contain a “NULL” character.

▼ To Add an Authorized User

1. Select Authorized User from the Type choice list.
2. Select New... from the Add New button.

The User dialog window is displayed.



FIGURE 6-6 User Dialog Window

3. Type the user name in the User Name field.
4. (Optional) Type a description in the Description field.
5. Click the User Enabled button.
6. (Optional) Type a password in the Password field.
7. (Optional) Type a SecurID name in the SecurID field.
Although the password and SecurID name are optional, the authentication mechanism requires one or the other.
8. Check 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. Click the OK button.
12. Save the Save Changes button.
13. Repeat the steps for each authorized user.

▼ To Add a Single Proxy User

1. Select **Proxy User** from the **Type** choice list.
2. Select **New Single...** from the **Add New** button.

The Proxy User dialog window is displayed.



FIGURE 6-7 Proxy User Dialog Window

3. Type a name for this Proxy User in the **Name** field.
4. (Optional) Type a description in the **Description** field.
5. Check the **User Enabled** box.
If this box is left unchecked or if you click on it so that it is no longer checked, the proxy user becomes inactive and can no longer use the proxies.
6. (Optional) Click and highlight the name of the authorized user that you want to place in the **Authorized User Name** field.
7. (Optional) Click and highlight the name or names of the user group or groups with which you want to associate this proxy user.
8. Type the name that the proxy user should assume when connecting to the target server (which is also known as the backend sever) in the **Backend User name** field.
This will be the identity the proxy user assumes on any target server connected through this proxy user.
9. Click the **OK** button.

10. Repeat the above steps until you have added all the proxy users.
11. Click the Save Changes button.

▼ To Add a Proxy User Group

You can group proxy users into logical groups so that you can use a group instead of single names in a policy rule.

1. Select Proxy User from the Type choice list.
2. Select New Group... from the Add New choice list.

The Proxy User dialog window is displayed.



FIGURE 6-8 Proxy User Dialog Window

3. Type a name in the Proxy User field.
4. Type the name for this group of proxy users.
5. (Optional) Type a short description of this definition in the Description field.
6. Click the User Enabled box to enable the user group.
7. Click and highlight the name of the proxy user or group of proxy users in the list of Proxy Users that you want to include in this group of Member Users.

8. Click the Add button to move it to the Member Users list.

Similarly, you can remove proxy users and lists of groups of proxy users from the Member Users list by clicking and highlighting the name and clicking the Remove button.

9. Do this for all the proxy users and groups of proxy users that you wish to include in your definition.

10. Click the OK button.

11. 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.

1. Select Screen from the Type choice list.

2. Select New... from the Add New choice list.

The Screen dialog window is displayed.

3. Type a name in the Name field.

4. Click the Mail Proxy tab.

The Spam Domain list is displayed.



FIGURE 6-9 Screen Dialog Window, Mail Proxy Tab

5. Click on the name you want to add to the Spam Domain list.
6. Click the Add button.
7. Click the OK button.
8. Repeat these steps until you have added all the domains from which you receive Spam mail.

All changes apply immediately.

▼ To Delete Spam Domains

1. Select the rule in the Policy Rules area.
2. Click the Search button.
3. Select the Spam domain from the Results field.
4. Click the Edit... button.

The Screen dialog window is displayed.

5. Click the Mail Proxy tab.
 6. Select and highlight the Spam domain to be edited in the Spam Domains field.
 7. Click the Delete button.
 8. Click the OK button.
 9. Repeat these steps until you have added all the domains from which you receive Spam mail.
- All changes apply immediately.

Writing and Editing Policy Rules for Proxies

Note – Policy Rules are strictly ordered; that is, they take effect 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 Write Policy Rules for the Proxies

1. Click the Edit button in the Policies List page to move to the Policy Edit page.
You can add a proxy rule to the activated policy, to another policy by highlighting it and clicking the policy on to get Edit policy Rules section
2. Select the Packet Filtering tab in the Policy Rules area of the Policy Edit page.
Proxies are defined in the Packet Filtering page.
3. Click the Add New... button in the Packet Filtering area to display the Rule Definition dialog window for that policy.
4. In the Rule Definition dialog window, the Rule Index field is filled with the next available rule index.
5. If a rule is valid for a particular Screen, select it; otherwise it is valid for all Screens.
6. Select Service from the Type choice list.

7. Click the Add New... button in the Packet Filtering area to display the Rule Definition dialog window.
8. Select the address in the Source Address field.
9. Select the address in the Destination Address field.
10. If it is a proxy rule, select ALLOW or DENY in the Action field.

There are four entries in the Action field: ALLOW, DENY, ENCRYPT, SECURE; proxy rules can only be defined with allow or deny.

When ALLOW is chosen, three fields are displayed on the right side of the Rule Definition dialog window:

- LOG
- SNMP
- PROXY



FIGURE 6-10 Rule Definition Dialog Window, Action ALLOW

When DENY is chosen, four fields are displayed on the right side of the Rule Definition dialog window:

- LOG
- SNMP
- ICMP Reject
- PROXY

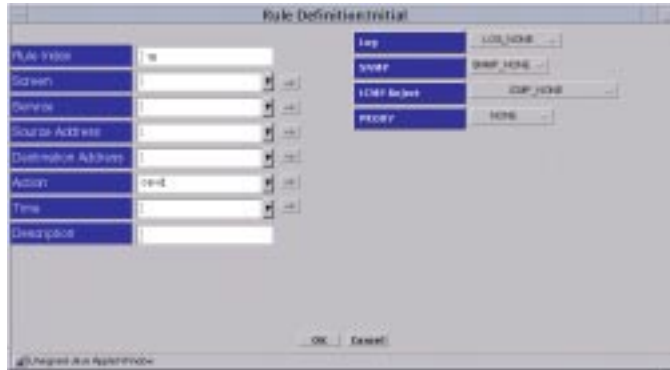


FIGURE 6-11 Rule Definition Dialog Window, Action DENY

11. Select the information into the LOG and SNMP fields.

There are five items in the Proxy choice list:

- NONE
- PROXY_HTTP
- PROXY_FTP
- PROXY_SMTP
- PROXY_Telnet

Select the proxy you want to use.

12. Click and highlight 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 proxy service for the proxy that you plan to use:

- Choose `ftp` as the service, if you are using the PROXY_FTP.
- Choose `www` as the service, if you are using the PROXY_HTTP.
- Choose `smtp` as the service, if you are using the PROXY_SMTP.
- Choose `telnet` as the service, if you are using the PROXY_TELNET.

Optionally, if you know the name of the service that you want, you can type the first few letters of its name and that service will appear in the field. You must type the first few letters exactly as they appear in the name because this feature is case sensitive.

13. Choose source and destination address that you want for the Source and Destination Address fields.

Be sure you have defined these addresses on the Policy Edit page.

14. Choose the action that you want for the Action field.

15. Click the name of the proxy for which you are writing this policy rule to put it in the Proxy field:

- Choose `PROXY_FTP` as the proxy for the Proxy field.

Eight fields are displayed below the Proxy field on the right side of the Rule Definition dialog window:

- GET
- PUT
- CHDIR
- MKDIR
- RENAME
- REMOVE
- DELETE

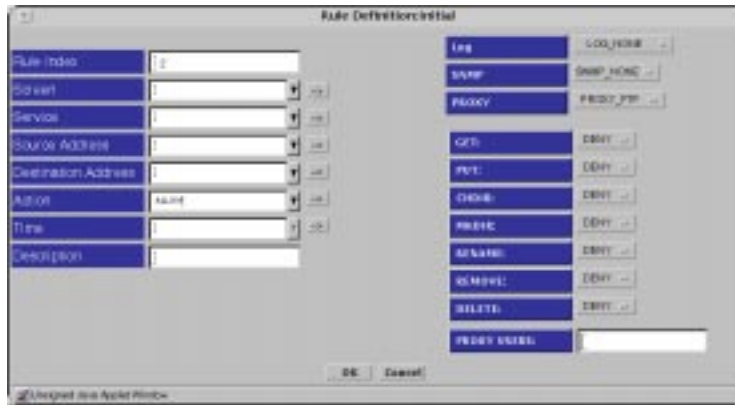


FIGURE 6-12 Rule Definition Dialog Window, `PROXY_FTP`

- Choose an action for GET, PUT, CHDIR, MKDIR, RENAME, REMOVE, and DELETE or accept the default in the Proxy Details area.
- Type a proxy user for the Proxy User in Proxy Details.
Be sure you have already defined the proxy user.
- Choose `PROXY_Telnet` as the proxy for the Proxy field.

The Proxy Users field is displayed below the Proxy field on the right side of the Rule Definition dialog window.



FIGURE 6-13 Rule Definition Dialog Window, PROXY_TELNET

- Choose the **PROXY_SMTP** as the proxy for the Proxy field.

The Relay field is displayed below the Proxy field on the right side of the Rule Definition dialog window.



FIGURE 6-14 Rule Definition Dialog Window, PROXY_SMTP

- Choose whether you want to allow Relay in the Proxy Details area.

If you want to use the `no_relay` function, you must define the local domain name in the file `defaultdomain`. You must have created or edited this file, if it does not exist, and have rebooted the Screen after creating or editing this file.

If you do not want to use the `no_relay` function, you do not need to create or edit this file.

- Click the name of the **PROXY_HTTP** to put it into the Proxy field.

Four fields are displayed below the Proxy field on the right side of the Rule Definition dialog window:

- Cookies
- ActiveX
- Java
- SSL

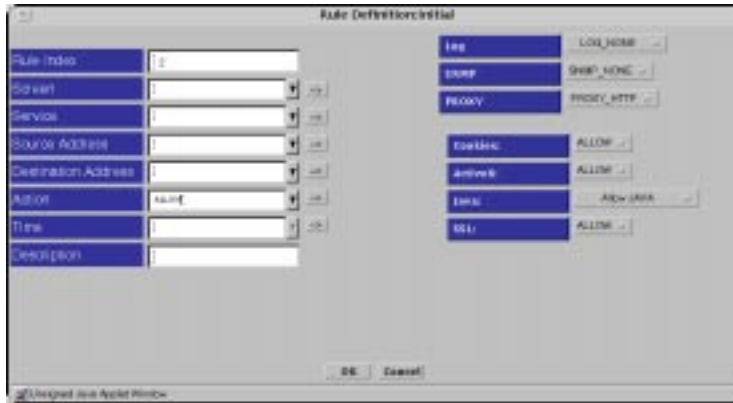


FIGURE 6-15 Rule Definition Dialog Window, PROXY_HTTP

- Chose an action for Cookies, ActiveX, and SSL or accept the default under Proxy Details.
- Click the button by the Java field, and choose the type of Java dialog window that you will permit under Proxy Details.

16. Click the OK button in the dialog window.

17. Click the Save Changes button.

FTP Proxy



Caution – At the present time there is the following limitation with proxies:

- Packets are only logged if logging is part of the action and according to the criteria for the Log Browser.

So that the end system can use the FTP proxy and be allowed to connect to other systems when this proxy is being used, the client connects to the proxy rather than the actual destination.

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.

In the example, the Screen is named `screen`.

▼ To Use the FTP Proxy

Follow these steps, if, for example, the proxy is running on the Screen that is named `screen`, you want to connect to the end system `ftp.sun.com`, and `ftp.sun.com` has an anonymous FTP account:

Note – The “anonymous” proxy user is prefigured during the installation of the software. It is an unauthenticated proxy user; as such, any string provided before the first “@” (“at” sign) in the password is ignored. The password after the first “@” (“at” sign) (here: `zzz@thereisnohelp.com`) is the back-end user password (in this case, the user name as is customary usage for anonymous FTP).

1. Type the command:

```
% ftp screen
```

The following is displayed:

```
Connected to screen
220-Proxy: SunScreen FTP Proxy Version 3.0
  : 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 username is the username and the destination server separated by an “at” sign.

2. Type your password at the prompt to authenticate you to this proxy:

```
331- Proxy: Authenticate & connect:
331 Password needed to authenticate 'anonymous'.
password:
```

The password is not echoed. Its format is two passwords separated by an “at” sign: The first password is the password for the proxy and the second is the password for the destination ftp server, for example, anonymous@zzz@thereisnohelp.com. “anonymous” is the password for the proxy and zzz@thereisnohelp is the email address that ftp.sun.com requires for anonymous ftp.

The following is displayed:

```
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 'anonymous'.
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.
%
```

TELNET Proxy



Caution – At the present time there is the following limitation with proxies:

- Packets are only logged if logging is part of the action and according to the criteria for the Log Browser. There is no content logging for this proxy.

▼ To Use the TELNET Proxy

Follow these steps, for example, if the proxy is running on the Screen that is named Screen and you want to connect to the end system `foo.com`:

1. Type the command:

```
% telnet Screen
```

The following is displayed:

```
SunScreen Telnet Proxy Version: 2.0
```

2. Type the username at the prompt:

```
Username@Hostname: username@foo.com
```

3. Type your 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 Screen 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 telnet session as you normally would for a normal telnet session and, if required, type a password.

SMTP Proxy



Caution – At the present time there is the following limitation with proxies:

- Packets are only logged if logging is part of the action and according to the criteria for the Log Browser. There is no content logging for this proxy.
-

The SMTP proxy provides a relay for email. It determines access based on source and destination addresses. The only content filtering that the proxy performs is based on the “source” and “destination” values for the mail itself. The “source,” or from whom the mail is sent, is compared to the list of spam domains and the “destination,” to whom the mail is sent, is compared with the local domain to see if relaying is being attempted.

Be sure you have defined the SMTP, if necessary, and defined any spam domains that you want on the Policy Edit page.

▼ To Use the SMTP Proxy

- **Point the MX record for the domain to the proxy for mail to be processed properly.**

SMTP connection will then be made to the proxy, rather than to the actual SMTP server.

HTTP Proxy



Caution – At the present time there is the following limitation with proxies:

- Packets are only logged if logging is part of the action and according to the criteria for the Log Browser. There is no content logging for this proxy.
-

The HTTP proxy provides a relay capability for the World Wide Web supporting the HTTP protocol. As with all proxies, it allows or denies sessions base on the source or destination address. It also provides selective filtering, such as Java filtering, Active-X, and cookies, of content based on the source and destination of sessions.

The HTTP proxy also filters Java, based on the signatures encapsulated in Java Archives (Jars) or on a precomputed hash of valid dialog windows.

▼ To Use the HTTP Proxy

1. **Click the down arrow on Preferences to display the choice list.**
2. **Click and highlight Proxies to display the Proxies page.**
3. **Type the name of the Screen or its IP address in the HTTP field.**
4. **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 EFS 3.0.

5. **Click the Apply button at the bottom of the Proxies page to set these choices as defaults.**

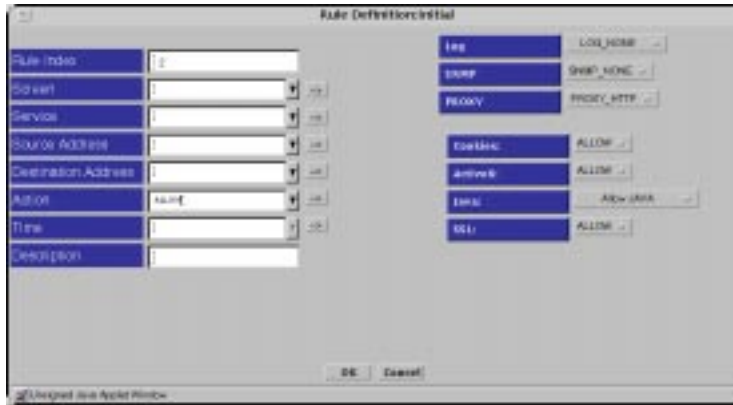


FIGURE 6-16 PROXY_HTTP

- Chose an action for Cookies, ActiveX, and SSL or accept the default under Proxy Details.
- Click the button by the Java field, and choose the type of Java you will permit under Proxy Details:

- a. Allow all Java
- b. Block all Java
- c. All Java with signed Jars, with the signature in the Jar Signature database
- d. All Java, with the Jar hash in the Jar Hash database
- e. Allow both c and d.

If you selected a through e, enter the Jar signature and Jar hash for these objects.

Note – If you selected Jar Signature or Jar Hash, they must be defined in the Common Objects area of the Policy Edit page.

6. Click the OK button in the dialog window.
7. Click the Save Changes button.

Adding an Additional Remote Administration Station

This section describes how to add an additional remote Administration Station after you have already installed SunScreen EFS 3.0.

Additional information can be found in the *SunScreen EFS 3.0 Reference Manual*.

The following information describes using the administration. For the command line interface, see Appendix A.

Installing the Software on the New Remote Administration Station

See Chapter 4 in the *SunScreen EFS 3.0 Installation Guide* to install the SunScreen EFS 3.0 software and certificates on the machine you are planning to use for the additional remote Administration Station.

▼ To Inform the Screen About the New Remote Administration Station

After installing the SunScreen EFS 3.0 software and certificates, follow the steps below to inform the Screen about the new remote administration station.

- 1. Select Certificate in the Type choice list.**
- 2. Select Associate MKID from the Add New choice list.**

The Certificate dialog window is displayed.

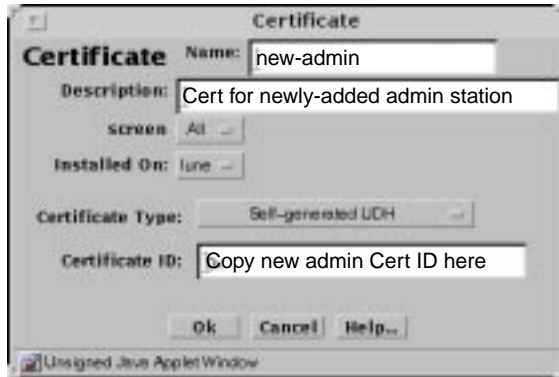


FIGURE 6-17 Certificate Dialog Window

3. **Type a name for the new remote administration station in the Name field.**
4. **Type the certificate number of the new remote administration station in the Certificate ID field.**

The Certificate ID begins with 0x.

5. **Click the OK button.**
6. **Click on the Administrative Access tab in the Policy Rules area.**

The Administrative Access area is displayed.

7. **Click and highlight the No. field in the Access Rules for GUI Remote Administration table.**
8. **Click the Edit... button below the Access Rules for GUI Remote Administration table.**

The Remote Access Rules dialog window is displayed. Note the name in the Certificate Group field (new-admin, in this example); you must add the certificate of the new remote Administration Station to this group.

9. **Click the Cancel button.**
10. **Select Certificate in the Type choice list.**
11. **Click the Search button.**
12. **Select the Certificate Group name in the Results field that was displayed in the Certificate Group field of the Remote Access Rules dialog window, in Steps one through five.**

13. Click the Edit button.

The Certificate dialog window is displayed.

14. Select the certificate you created in Step 3 from the Available Certificates field.

15. Click the Add>> button.

16. Click the OK button.

Setting Up the Access Control List on the New Remote Administration Station

See "Using SKIP for Encrypted Communication," in the *SunScreen EFS 3.0 Installation Guide* for the procedure to get the Certificate ID from the Screen and to use the `skiptool` GUI to set up the Access Control List.

Note – You must log on to the Screen system to directly administer SKIP or gather data from any of the SKIP commands.

Configuring Centralized Management Groups

The configuration for Centralized Management Groups requires that certificate information be exchanged between the Centralized Management Groups Primary and Secondary Screens. These certificates then must be added to the Screen objects, along with the Admin IP address information, and algorithms for the Centralized Management Group's Secondary Screen as they are enabled after selecting a Primary for the Screen in the HA/MasterConfig area.

Also, on the Centralized Management Groups Primary Screen, the interfaces (and the addresses referred by them) to each Screen should appear with the Screen object selected, to make them Screen specific.

Finally, a remote user rule is added on the Centralized Management Group's Primary Screen to allow it to administer all the Secondary Screens remotely.

The following information describes using the administration GUI. For the command line interface, see Appendix A.

Configure a Centralized Management Group

Centralized Management allows you to remotely administer configurations on a group of SunScreens. A Centralized Management Group is comprised of a Primary Screen and a number of Secondary Screens. The Primary Screen's function is to "push" Policy configurations to the other Secondary Screens in the Centralized Management Group.

In configurations where the members of the cluster have to traverse a firewall (including other members) to communicate with the Primary Screen, the firewall being traversed should allow the following traffic:

- SKIP
- Certificate discovery

▼ To Generate a Certificate for the Centralized Management Group's Primary Screen

Note – The Certificate ID (also known as an MKID) is provided when you generate a certificate. The Certificate ID is used to associate the Primary Screen's certificate on the Secondary Screen.

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

- 1. Install the SunScreen EFS 3.0 software.**
- 2. Log in to SunScreen EFS 3.0.**
- 3. Click the Edit button in the Policies List page.**
The Policy Edit page is displayed.
- 4. Select Certificate from the Type choice list.**
- 5. Select Generate Screen Certificate from the Add New choice list.**
The Certificate dialog window is displayed.
- 6. Type the name of the Centralized Management Group's Primary Screen, with the suffix ".admin" in the Name field of the Certificate dialog window.**
In this example, efs-u5 is the Primary Centralized Management Group Screen's host name.
A dialog window is displayed, with options for the type of key to generate. The default is "highest available."



FIGURE 6-18 Certificate Dialog Window

7. Click the Generate New Certificate button.

The Certificate ID field now contains the Certificate Identifier for the Centralized Management Group's Primary Screen. You will need to use this number in a later step.

8. Click the OK button.

▼ To Associate the Primary Screen's Certificate ID with the Centralized Management Group's Primary Screen Object

Perform the following steps on the Screen designated as the Centralized Management Group's Primary Screen:

- 1. Select Screen from the Type choice list in the Common Objects area of the Policy Edit page.**
- 2. Click the Search button.**

The results field now contains the name of the Centralized Management Group's Primary Screen and information appears in the Details field.

3. Select the name of the Centralized Management Group's Primary Screen in the Results field.
4. Click the Edit button.

The Screen dialog window is displayed.



FIGURE 6-19 Screen Dialog Window, Miscellaneous Tab

5. Type a number, to represent megabytes, in the Log Size field of the Screen dialog window.
6. Click the HA/Master Configuration tab.
7. Type the name of the Centralized Management Group's Primary Certificate name (the Primary name with the suffix ".admin") in the Administration Certificate field of the HA/Master Configuration page.

This associates the certificate with the Centralized Management Group's Primary Screen.

8. Click the OK button.

▼ To Add a Secondary Centralized Management Group Screen on the Primary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

1. Select Screen from the Type choice list in the Common Objects area of the Policy Edit page.
2. Click the add New button.

The Screen dialog window is displayed.

3. The Miscellaneous tab in the Screen dialog window is selected as a default.

The Miscellaneous page is displayed.



FIGURE 6-20 Screen Dialog Window, Miscellaneous Tab

4. Type the name of the Centralized Management Group's Secondary Screen in the Name field of the Miscellaneous page.

In this example, "boss" is the Secondary Centralized Management Group Screen's host name.

5. Type a number, to represent megabytes, in the Log Size field of the Miscellaneous page.
6. Click the OK button.

▼ To Generate a Certificate ID for the Centralized Management Group's Secondary Screen on the Secondary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Secondary Screen:

1. Install the SunScreen EFS 3.0 software.
2. Select Certificate from the Type choice list.
3. Select Generate Screen certificate from the Add New choice list.

The Certificate dialog window is displayed.



FIGURE 6-21 Certificate Dialog Window

4. The Select in Installed On field contains the name of the Centralized Management group's Secondary Screen.
5. Type the certificate name with .admin suffix.

6. Click on Generate New Certificate.

A new key is generated for the Centralized Management Group's Secondary Screen.



FIGURE 6-22 Certificate Dialog Window Showing the Certificate ID

7. Click the OK button.

▼ To Put the Centralized Management Group Secondary Screen's Certificate ID on the Primary Centralized Management Group Screen

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

1. Click the Edit button in the Policies List page.

The Policy Edit page is displayed.

2. Select Certificate from the Type choice list in the Policy Edit page.

3. Select Associate MKID from the Add New choice list.

The Certificate dialog window is displayed.

4. Type the name of the Centralized Management Group's Secondary Screen, with .admin suffix, in the Name field.

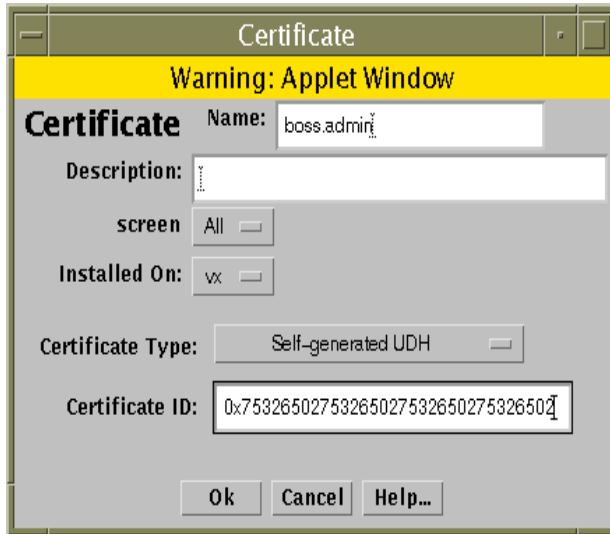


FIGURE 6-23 Certificate Dialog Window

5. **In the Certificate ID field, type the key of the Centralized Management Group's Secondary Screen.**

You can telnet or use a floppy (using the command `# skiplocal -l` on the Centralized Management group's Secondary Screen).

6. **Click the OK button.**

▼ To Associate the Certificate with the Centralized Management Group's Secondary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

1. **Select Screen from the Type choice list.**
2. **Click the Search button.**

The Results field displays the names of the Centralized Management Group's Primary and Secondary Screens. In this example, the names in the Results field are efs-u5 and boss.

3. **Select the name of the Centralized Management Group's Secondary Screen from the Results field.**

4. Click the Edit button.

The Screen dialog window is displayed.



FIGURE 6-24 Certificate Dialog Window

5. Select the HA/Master configuration tab in the Screen dialog window.

6. Select the name of the Centralized Management Group's Primary Screen from the Cluster Master Name field.

In this example, the name is efs-u5.

7. Type the administration IP address of the Centralized Management Group's Secondary Screen in the Administration IP Address field.

In this example, the administration IP address is 160.210.1.1.

8. Type the name of the Centralized Management Group's Secondary Screen in the Administration Certificate field.

In this example, the name is boss.admin.

9. You can keep the defaults or change the settings of the following fields:

- Key Algorithm
- Data algorithm
- Mac Algorithm

Note – If you choose to change the algorithms, be sure they are identical for the Centralized Management Group's Primary and Secondary Screens.

10. Click the OK button.

▼ To Put the Central Management Group's Primary Certificate ID on the Central Management Group's Secondary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Secondary Screen:

- 1. Select Certificate from the Type choice list in the Policy Edit page.**
- 2. Select Create Associated MKID from the Add New choice list.**

The Certificate dialog window is displayed.



FIGURE 6-25 Certificate Dialog Window

3. **Type the name of the Centralized Management Group's Primary Screen (the Primary name with the suffix .admin) in the Name field of the Certificate dialog window.**

In this example, the name is efs-u5.admin.

4. **Select the name of the Centralized Management Group's Primary Screen in the Installed On field**

In this example, the name is efs-u5.

5. **Do telnet to the Centralized Management Group's Primary Screen.**

6. **In a terminal window of the Centralized Management Group's Primary Screen, type the following at the command line:**

```
% skiplocal -1
```

The Certificate Number number is displayed.

7. **Type the Certificate Number in the Certificate ID field of the Certificate dialog window, to put the Certificate ID of the Centralized Management Group's Primary Screen on the Centralized Management Group's Secondary Screen.**

Put the Certificate ID on a floppy diskette or some other portable medium and send it to the location of the Centralized Management Group's Secondary Screen.

8. **Click the OK button.**

▼ To Verify that the Certificates are on the Screens

Perform the following steps on the Screen designated the Centralized Management Group's Secondary Screen:

1. **Select Certificate from the Type choice list in the Policy Edit page.**
2. **Click the Search button.**

The Results field displays the names of the Centralized Management Group's Primary and Secondary Screens.

In this example, the names are efs-u5 and boss.

▼ To Create a Primary Centralized Management Screen on the Secondary Centralized Management Group Screen

Perform the following steps on the Screen designated the Centralized Management Group's Secondary Screen:

1. **Select Screen from the Type choice list.**
2. **Click the Add New button.**
The Screen dialog window is displayed.
3. **Click the Miscellaneous tab in the Screen dialog window.**
The Miscellaneous page is displayed.

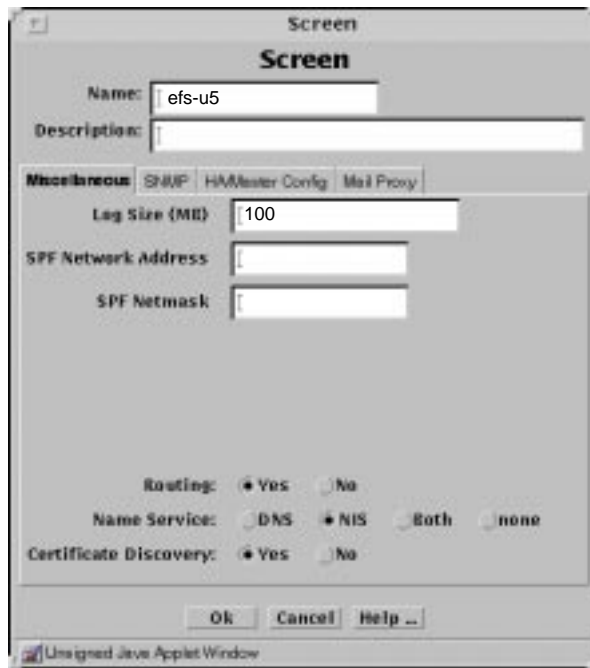


FIGURE 6-26 Screen Dialog Window, Miscellaneous Tab

4. **Type the name of the Centralized Management Group's Primary Screen in the Name field of the Miscellaneous page.**
In this example, the name is efs-u5.

5. **Type a number, to represent megabytes, in the Log Size field of the Miscellaneous page.**
6. **Select the HA/Master Configuration tab in the Screen dialog window.**
7. **Type the name of the machine designated as the Centralized Management Group's Primary Screen Certificate in the Administration Certificate field**
In this example, the name is efs-u5.admin.
8. **Click the OK button.**

To Save and Activate the Centralized Management Secondary Group's Screen

1. **Click the Save Changes button.**
The Activate Policy? dialog window is displayed.
2. **Click Yes in the Activate Policy? dialog window.**

▼ To Add a New Address Group on the Centralized Management Group's Primary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

1. **Select Address from the Type choice list.**
2. **Select New Group... from the Add New choice list.**
The Address dialog window is displayed.
3. **Type the name of the Address Group on the Centralized Management Group's Secondary Screen.**
In this example, the Address Group on boss in the Interface Definition dialog window is "boss_le0."
4. **Select the name of the Centralized Management Group's Secondary Screen from the Screen choice list.**
In this example, the name is "boss."
5. **Click the OK button.**

▼ To Define the Central Management Group's Secondary Interfaces on the Centralized Management Group's Primary Screen

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

1. Select Interface from the Type choice list.
2. Select New... from the Add New choice list.

The Interface Definition dialog window is displayed.

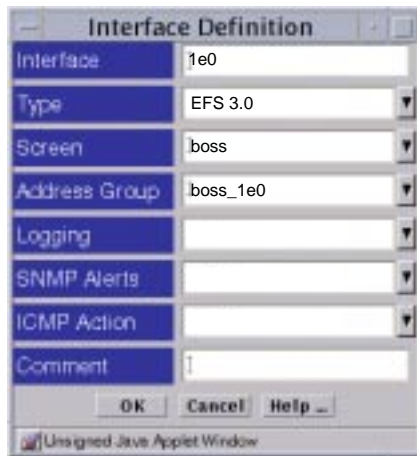


FIGURE 6-27 Interface Definition Dialog Window

- ### 3. Define the interfaces of the Centralized Management Group's Secondary Screen:

In this example, the interfaces are:

- | | |
|-----------------|-----------------------------------|
| ■ Interface | 1e0 |
| ■ Type | EFS 3.0 |
| ■ Screen | boss (<i>Name of Secondary</i>) |
| ■ Address Group | boss_1e0 |

The Interface Definition dialog window is now identical on both screens.

- 4. Click the OK button.**

The Policy Edit page is displayed.

▼ To Allow Communication Between Screens

Add a remote access rule on the Primary to allow the Primary Screen to connect to the Secondary Screens in the Centralized Management Group.

From the Policy Rules area:

1. Click the **Administrative Access** tab.
2. Click the **Add New...** button in the **Access Rules for Remote Administration** area.
The Remote Access Rules dialog window is displayed.
3. Leave the **Screen** field blank.
4. Select ***** in the **Address Object** field.
5. Type the name of an administrative user in the **User** field.
6. Select **SKIP_VERSION_2** in the **Encryption** field.
7. Select the name of the Primary Screen's certificate of certificate group that contains the Primary Screen's certificate.
8. Select the appropriate item in the **Key Algorithm** field.
9. Select the appropriate item in the **data Algorithm** field.
10. Select the appropriate item in the **MAC Algorithm** field.
11. Leave the **Tunnel** field blank.
12. Select the appropriate item in the **Access Level** field.
13. Click the **OK** button.

Note – You can configure packet filtering rules to make a specific rule apply to only one Screen. The rules apply globally by default.

▼ To Activate the Policy

Perform the following steps on the Screen designated the Centralized Management Group's Primary Screen:

- 1. Click the Save Changes button.**

The Activate Policy? dialog window is displayed.

- 2. Click the YES button.**

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

- 4. Click the Activate button.**

Using the Command Line

All the functionality of SunScreen EFS 3.0 that is available through the administration GUI is also available through a command. Administering your Screens through the command line can be useful when you want to manage one or more remote Screen or if you use more than one network address.

You can access a Screen using the command line from its own keyboard, when the Screen is being administered locally and requires that you have superuser (`root`) access; or you can access a Screen using the command line from an Administration Station, when the Screen is being administered remotely and requires that you use SKIP encryption and an Administration User name and password.

For more information on the command line, see the *SunScreen EFS 3.0 Reference Manual*.

▼ To Install and Configure the Netscape Browser

Note – When using the Java Plug-in for Netscape Navigator, follow the instructions in the Netscape release notes. In particular, you should 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.

Perform the following steps to install and configure the Netscape browser for SunScreen EFS 3.0 administration.

1. **Set up environment for installing and running the Java Plug-in.**

a. For sh or ksh users, type:

```
# unset CLASSPATH
# MOZILLA_HOME=/opt/netscape
# PATH=$MOZILLA_HOME:$PATH
# export PATH MOZILLA_HOME
```

b. 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 “Saving the identitydb.obj File”).

4. Access the SunScreen EFS 3.0 administration GUI in one of two ways:

a. Access the SunScreen EFS 3.0 administration GUI with no access to local files by typing:

```
# netscape http://screenhost:3852/
```

b. Access the SunScreen EFS 3.0 administration GUI using the Java Plug-in with access to local files for backup and restore by typing:

```
# netscape http://screenhost:3852/plugin/
```


Setting the CLASSPATH

Only set the CLASSPATH environment variable if you need to install special Java files in 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.

Saving 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:**

`http://localhost:3852/plugin/plugins/`

2. **Press your MENU mouse button and save the link as a file.**

Note – If your browser does not support this save, access identitydb.obj in the directory: /opt/SUNWicg/SunScreen/admin/htdocs/plugin/plugins/.

3. **Copy the identitydb.obj file onto a diskette to distribute to all Administration Stations.**

If the identitydb.obj file already exists in its proper location, per the following:

```
UNIX: $HOME
single-user Win95: C:\WINDOWS
multi-user Win95/98: C:\WINDOWS\PROFILES\username
WinNT: C:\WINNT\PROFILES\username
```

4. **Add SunScreen as an accepted signer.**

Note – If the identitydb.obj file does not exist, copy the file from the diskette to one of the above locations.

Note – You can also copy identitydb.obj from the diskette to its proper location.

Unix (shell) Command Summary

The following Unix (shell) commands are available at your shell prompt when `/opt/SUNWicg/SunScreen/bin` is included in your `$PATH`. The following table lists the SunScreen EFS 3.0 Unix (shell) commands and their descriptions. Many of these commands duplicate administration GUI functions, while others provide a context for other commands.

TABLE A-1 SunScreen EFS 3.0 Unix (shell) Command Summary

Unix Command	Description
<code>ss_install</code>	Create an initial SunScreen configuration. <code>ss_install</code> , when combined with <code>pkgadd</code> , is equivalent to using the install-wizard graphical user interface.
<code>ss_client</code>	Provide communication between an Administration Station and a Screen that was configured by an earlier SunScreen firewall product release. <code>ss_client</code> is provided only for the purpose of remotely administering such products using the SunScreen EFS 3.0 system as a remote Administration Station.
<code>screenInstaller</code>	Run the graphical user interface for installing the SunScreen EFS 3.0 software on the Screen and for setting up an initial policy.
<code>adminInstaller</code>	Run the graphical user interface for installing the SunScreen EFS 3.0 software on the Administration Station and for setting up an initial SunScreen EFS 3.0 policy. <code>adminInstaller</code> is an easy way to add packages for the remote Administration Station.
<code>ssadm</code>	Primary command-line tool for SunScreen EFS 3.0 administration. <code>ssadm</code> sub-commands perform various operations such as editing and activating a SunScreen configuration, and examining the status of a Screen.

Note – The commands used by `skiptool` can be found in the *SunScreen SKIP 1.5 User's Guide*.

Unix (shell) Commands

`ss_install` Command

`ss_install` is a text-based command-line utility for creating an initial SunScreen EFS 3.0 configuration. `ss_install`, combined with `pkgadd`, is the command-line equivalent to the installation wizard graphical user interface.

`ss_install` interactively queries you with various options for configuring the SunScreen, creates a configuration, stores it under the policy name “Initial”, and activates it.

After `ss_install` is complete, the SunScreen is ready to be administered.

`ss_client` Command

`ss_client` is equivalent to the command of the same name provided with earlier SunScreen firewall products, such as *SunScreen EFS, Release 2.0*, or *SunScreen SPF-200*. `ss_client` is provided only for the purpose of remotely administering such products using the SunScreen EFS 3.0 system as a remote Administration Station.

For information on how to use `ss_client` to administer an earlier SunScreen firewall product, see the documentation for that product.

`screenInstaller` Command

Runs the installation wizard that installs the SunScreen EFS 3.0 software on the Screen and sets up an initial SunScreen EFS 3.0 policy.

`adminInstaller` Command

Runs the installation wizard that installs the SunScreen EFS 3.0 software on the Administration Station and sets up an initial SunScreen EFS 3.0 policy. It is also an easy way to add packages for the remote Administration Station.

ssadm Command

`ssadm` is the primary command-line tool for SunScreen EFS 3.0 administration. `ssadm` has a number of sub-commands 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 SunScreen SKIP to encrypt IP network communications passing between them. See the *SunScreen SKIP User's Guide* for more information regarding SKIP encryption.

Usage:

```
ssadm [-b] [-n] sub-command [parameters...]
```

```
ssadm [-b] [-n] -r remotehost [-F ticketfile] sub-command [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` sub-commands are each described in the *ssadm Sub-Command* section of this document.

The -b option normally is not needed since those commands 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`.

Executing an `ssadm` Command on a Local Screen

You can configure a local Screen by typing the commands listed in this appendix using 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.

The `ssadm` command resides in the `/opt/SUNWicg/SunScreen/bin` directory. Include this directory in your directory search path to have access to the commands on the local Screen.

Executing an `ssadm -r` Command on a Remote Administration Station

You can configure a Screen from a remote Administration Station by preceding the commands listed in this appendix with the `ssadm -r` command and the name 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
```

where `ssadm -r` indicates that you want to execute a command on a remote Screen called `SunScreen1`, `activate` is the name of the `ssadm` sub-command, and `Initial` is the name of the policy you want to activate.

Note – A local `ssadm` command can be turned into a remote `ssadm` command by adding `-r remote_Screen_name` immediately after `ssadm`.

When `ssadm` is used with the `-r` option to access a remote Screen, the name of the ticketfile can be specified using the `-F` option, or through the `SSADM_TICKET_FILE` environment.

Remotely Logging Into and Out of SunScreen EFS 3.0

If you are using remote administration, you must log in before you can perform most `ssadm` commands.

▼ To Remotely Log Into SunScreen EFS 3.0

- Type the following:

```
# SSADM_TICKET_FILE=$HOME/.ssadmticket
# export SSADM_TICKET_FILE
# touch $SSADM_TICKET_FILE
# chmod go= $SSADM_TICKET_FILE
# ssadm -r screenname login username password
WRITE access <E23B344150C702EC>
```

▼ To Remotely Log Out of SunScreen EFS 3.0

- Type the following:

```
# ssadm -r screenname logout
```

ssadm Sub-Command Summary

The following table lists the SunScreen EFS 3.0 `ssadm` sub-commands and their descriptions. Many `ssadm` sub-commands duplicate administration GUI functions, while others provide a context for other sub-commands.

TABLE A-2 SunScreen EFS 3.0 `ssadm` Sub-Command Summary

<code>ssadm</code> Sub-command	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>debug_level</code>	Set or clear the level of debugging output generated by a Screen.
<code>edit</code>	Run the SunScreen configuration editor. See <i>Configuration Editor Sub-Command Summary</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 displays 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 of descriptive SunScreen EFS 3.0 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 edit command that is a sub-command of `ssadm`.

When you need to look at or change a policy in some way like Move or Delete, you invoke the configuration editor and enter a series of commands that end with save and quit requests.

Note – Be sure to save change commands, such as add, del, rename, renamereference, insert, replace, and move, before you quit. Run save just before the quit command to avoid accumulating too many policy versions.

Configuration Editor Commands

The `ssadm edit` commands are used when running the configuration editor, which is responsible for maintaining the SunScreen EFS 3.0 configuration database.

The following table lists the SunScreen EFS 3.0 configuration editor `ssadm edit` sub-commands and their descriptions. Many sub-commands duplicate administration GUI functions, while others provide a context for other sub-commands.

TABLE A-3 SunScreen EFS 3.0 Configuration Editor `ssadm edit` Sub-Command Summary

edit Sub-Command	Description
list	Display all data for all entries or a specific entry of a give TYPE.
list_name	Display the set of unique basenames and sub-type of all of a given TYPE.
search	Search for objects that match specified criteria.
add	Create or redefine an entry.
add_member	Add a member to a group or list.
del[ete]	Delete the specified entry of the given TYPE.
del[ete]_member	Delete a member from a centralized management group or list.
insert	Insert a new object of one of the ordered (indexed) types in a specified position in the corresponding list.
move	Move an indexed entry from its current location in the ordered list to the new location.

TABLE A-3 SunScreen EFS 3.0 Configuration Editor `ssadm edit` Sub-Command Summary

edit Sub-Command	Description
<code>replace</code>	Replace an object at a specified index.
<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>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>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>save</code>	Save all current edits to the policy.
<code>reload</code>	Discard any and all edits, if made, and reload the data into the editor from the database.
<code>verify</code>	Takes no arguments and verifies the currently loaded policy.
<code>authuser</code>	Manipulates the list of authorized users.
<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>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>proxyuser</code>	Manipulates the list of proxy users.
<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 <i>SunScreen EFS 3.0 Reference Manual</i> for more information.
<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.

This appendix describes using the UNIX command line interface for the following:

- Creating a Policy
- To Create a New Policy
- To Copy a Policy
- To Rename a Policy
- To Delete a Policy
- To Back Up a Policy
- To Restore a Policy
- To Verify a Policy
- To Activate a Policy
- To Edit a Policy
- To Add a New Single Service
- To Add a New Service Group
- To Rename a Service and Service Group and Its References
- To Rename a Service or Service Group
- To Delete Service or Service Group
- To Check References to Deleted Service or Service Group
- To Add a New Host Address
- To Add a Range of Addresses
- To Add an Address Group
- To Delete an Address, Address Range, or Address List
- To Check References to a Deleted Address, Address Range, or Address List
- To Rename an Address, Address Range, or Address Group
- To Add Screen Certificates From a Diskette or a File
- To Add Screen Local Identities
- To Add Self-Generated Screen Certificates
- To Add Other Certificates from a Diskette or a File
- To Add Certificate Groups
- To Add a New Member to a Certificate Group
- To Remove a Member From a Certificate Group
- To Rename a Certificate or Certificate Group
- To Delete a Certificate or Certificate Group
- To Check References to a Deleted Certificate
- To Check References to a Deleted Certificate Group
- To Add a Screen
- To List the Screens
- To Add an SNMP Receiver to a Screen
- To Add Multiple SNMP Receivers to a Screen
- To Remove SNMP Receivers from a Screen
- To Set Logsize on a Screen
- To Set a Screen to Stealth Mode
- To Add Interfaces (in Routing Mode)
- Adding or Modifying an Authorized User
- To Add An Authorized User with Password Authentication
- To Add An Authorized User and SecurID Name

- To Modify Authorized Users
- To Delete an Authorized User
- Defining New Rules
- To Create a Packet Filtering Rule
- To Reorder the Rules
- To Delete a Rule
- To Edit Any Part of a Rule
- To Add an Access Rule for GUI Local Administration
- To Edit an Access Rule for GUI Local Administration
- To Delete an Access Rule for GUI Local Administration
- To Add an Access Rule for Remote Administration
- To Edit an Access Rule for Remote Administration
- To Delete an Access Rule for Remote Administration
- Network Address Translation
- To Add ARP Manually
- To Define NAT Mappings
- To Delete NAT Mappings
- To List the NAT Mappings
- Virtual Private Network (VPN)
- To Add a VPN Gateway
- To Replace a VPN Gateway
- To Remove a VPN Gateway
- To View the Information
- To View the Statistics
- To Set Up Packet Logging
- Examining Packets
- To Use `ssadm logdump` Command
- To View the Log
- To Save the Log
- To Clear the Log
- To Save and Clear the Log
- Setting Up High Availability (HA)
- To Remove an HA Host
- To View HA Information
- Centralized Management Group
- Change a Screen Object to be in a Cluster
- To Add a Screen Object to a Cluster
- Gathering Information From Your System to Report to SunService
- Troubleshooting
- To Use the `ssadm debug_level` Command

Command-Line Session

Unlike many of the other `ssadm` sub-commands, the configuration editor allows editing only one policy at a time. When you are in an editing session, others are unable to edit, and can only read the policy.

You invoke the configuration editor with the `edit` command, which is a sub-command of `ssadm`, and the name of your policy, such as `Initial`. Once it is running, the prompt becomes: `edit>`.

- **For a locally administered Screen, type:**

```
# ssadm edit policy_name
```

For a remotely administered Screen, type:

```
# ssadm -r Screen_name edit policy_name
```

Creating a Policy

To Create a New Policy

- **Add a new policy, for example, `myconfig`, by typing:**

- **For local administration:**

```
# ssadm policy -a myconfig
```

- **For remote administration:**

```
# ssadm -r sunscreen1 policy -a myconfig
```

▼ To Copy a Policy

- Copy a policy by typing:
 - For local administration:

```
# ssadm policy -c myconfig myconfigcopy
```

- For remote administration:

```
# ssadm -r policy -c myconfig myconfigcopy
```

▼ To Rename a Policy

- Rename a policy by typing:
- For local administration:

```
# ssadm policy -r old name new name
```

- For remote administration:

```
# ssadm -r sunscreen1 policy -r old name new name
```

▼ To Delete a Policy

- Delete a policy by typing:
- For local administration:

```
# ssadm policy -d name
```

- For remote administration:

```
# ssadm -r sunscreen1 policy -d name
```

▼ To Back Up a Policy

- Type the following to back up a policy:

- For local administration:

```
# ssadm policy -c old_name new_name
```

- For remote administration:

```
# ssadm -r machinename policy -c old_name new_name
```

▼ To Restore a Policy

- Restore a policy, for example, *myconfig*, by typing:

- For local administration:

```
# ssadm restore < myconfig
```

- For remote administration:

```
# sssadm -r machinename restore < myconfig
```

To Verify a Policy

- Verify the validity of a policy, for example, *myconfig*, by typing:

- For local administration:

```
# ssadm activate -n myconfig
```

- For remote administration:

```
# ssadm -r sunscreen1 activate -n myconfig
```

To Activate a Policy

- For local administration:

```
# ssadm activate myconfig
```

- For local administration:

```
# ssadm -r sunscreen1 activate myconfig
```

▼ To Edit a Policy

- Edit a policy, for example, `myconfig`, by typing:

- For local administration:

```
# ssadm edit myconfig
```

- For remote administration:

```
# ssadm -r sunscreen1 edit myconfig
```

Objects In a SunScreen Configuration

▼ To Add a New Single Service

1. Type the following to add the service `ftp-34`, service engine, discriminator, parameters, and an optional description within quotation marks.

You only need to type in the “PARAMETERS 1200 1200 1” in the example below if you do not want to use the default values. See the *SunScreen EFS Reference Manual* 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 – Although SunScreen EFS 3.0 lets you change the default services in service groups, to make any troubleshooting easier, it is better to add a new service group that contains the services that you want.

1. Type the following to add the service group "useful services" and an optional description within quotation marks:

- For local administration:

```
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 window.

2. Type the following to list the new service group "useful services."

```
edit> list service "useful services"
```

Modifying Service Groups

Add the GROUP again with the modified member list. The new version will overwrite the old version.

▼ To Rename a Service and Service Group and Its References

Note – SunScreen EFS 3.0 lets you rename a single service or a service group. To make any troubleshooting easier, do not rename the single services and service groups that are supplied with SunScreen EFS 3.0.

- Type the following to rename the old service or service group to the new name and all references to it, for example:

```
edit> renamereference service "useful services" "dmz services"
```

▼ To Rename a Service or Service Group

- **Type the following to rename the old service or service group to the new name only, for example:**

```
edit> rename service "useful services" "dmz services"
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Delete Service or Service Group

Note – SunScreen EFS 3.0 lets you delete a single service or a service group. To make any troubleshooting easier, do not delete the name of the single services and services groups that are supplied with SunScreen EFS 3.0.

This command does not check for references to the single service or service group that you are deleting.

- **Type the following to delete a service or service group, for example to delete the service group "dmz service":**

```
edit> del service "dmz services"
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Check References to Deleted Service or Service Group

If you want to check references to the single service or service group that you want to delete or have deleted, you:

- **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"
```

You see a list of all the instances where the service or service group is used. You, then, can remove the service or service group from the service group in which it is used, and edit the rule to remove it from the rule or rules in which it is used.

Addresses, Address Ranges, and Address Groups

▼ To Add a New Host Address

SunScreen EFS 3.0 lets you define a new host address.

- **Type the following to add the new host address and an optional description within quotation marks:**

```
edit> add address ftp-www HOST 172.16.1.2 COMMENT "Address of the  
DMZ host"
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Add a Range of Addresses

- **Type the following to add an address range and an optional description within quotation marks, for example:**

```
edit> add address corp RANGE 172.16.3.2 172.16.3.255 COMMENT "All  
hosts in corporate"
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Add an Address Group

- Type the following to add an address group and an optional description 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"
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Delete an Address, Address Range, or Address List

Note – To make any troubleshooting easier, do not delete the names of addresses, ranges of addresses, and lists of address that were defined when SunScreen EFS 3.0 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 address, 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

If you want to check references to the address, range of addresses, or list of addresses that you want to delete or have deleted, use these commands:

- **Type the following to find the reference to an address, a range of addresses, or a list of address that you want to delete or have deleted, for example:**

```
edit> referlist address host0
```

You see a list of all the instances where the address, range of addresses, or list of addresses is used. You, then, can 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 any troubleshooting easier, do not rename the addresses, ranges of addresses, and lists of address that were defined when SunScreen EFS 3.0 was installed.

Part 1

- **Type the following to rename an address, a range of addresses, or a list of address and all reference to it, for example:**

```
edit> renamereference address ftp-www DMZ
```

Part 2

- **Type the following to rename an address, a range of addresses, or a list of address only, for example:**

```
edit> rename address ftp-www DMZ
```

To have the changes take effect, you must activate the policy whose rules you edited.

Certificates

▼ To Add Screen Certificates From a Diskette or a File

Presently, you can only do this 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.

This example shows adding a private certificate key and certificate.

1. **Insert the diskette that contains the private certificate, if you are using X.509 keys and certificates, into the diskette drive of the Administration Station.**

You also can add new private keys and certificates from a directory that contains only one set of private key and certificate files.

If you are adding a private key and 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 private key and certificate are stored and the following command and the name of the directory to add the private key and certificate, for example:**

```
# install_skip_keys -icg /floppy/unnamed_floppy
```

4. **Type the following to eject the diskette, if you are using X.509 keys and certificates:**

```
# eject unnamed_floppy
```

If you are adding a private certificate from a directory, you do not need this step.



Caution – 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, for example:

```
edit> add certificate sales-home SINGLE NSID 1 MKID "0xA0050E"  
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, and SUNSCREEN is the type of certificate.

Each type of certificate requires a particular Name Space ID (NSID) and the Master Key ID (certificate ID) of the certificate:

- Certificate IDs that use the IP address use the NSID0 convention with the IP address as the MKID.
- Certificate IDs use the NSID1 convention with an MKID of 8 hexadecimal digits (32 bits).
- Diffie-Hellman certificates use the NSID8 convention with an MFKID of 32 hexadecimal digits (128 bits).

NSIDs and certificate IDs are described in the *SunScreen EFS 3.0 Reference Manual*.

▼ To Add Screen Local Identities

Presently, you can only do this with local administration; therefore, for a remotely administrated Screen, you must somehow gain access to the Screen's `crt.file`, then the commands will work. One means of gaining access to this file might be through the `rlogin` command, if you have a policy rule that allows this.

To use this command you must first have saved 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. You do this because it is impossible to generate the same key later, should you have to reinstall the SunScreen EFS 3.0 software. Once you have swapped certificate IDs with a number of peer systems, it becomes difficult to fix things in a timely manner.

The SunScreen EFS 3.0 installation programs all intrinsically rekey the SunScreen EFS 3.0 being installed. While this is not a serious problem, it means that you have to add your old keys back into the database before configuring the Screen for any virtual private networks (VPN) that existed. See the *SunScreen EFS Reference Manual* for information about VPNs.

1. Type the following 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, and SUNSCREEN is the type of certificate.

Each type of certificate requires a particular Name Space ID (NSID) and the Master Key ID (certificate ID) of the certificate.

- Certificate IDs that use the IP address use the NSID0 convention with the IP address as the certificate ID.
- Certificate IDs certificates use the NSID1 convention with a certificate ID of 8 hexadecimal digits (32 bits).
- Diffie-Hellman certificates use the NSID8 convention with a certificate ID of 32 hexadecimal digit (128 bits).

NSIDs and certificate IDs are described in the *SunScreen EFS 3.0 Reference Manual*.

▼ To Add Self-Generated Screen Certificates

- For local administration:

1. Type the following to create a self-generated Screen certificate, for example:

```
# skiplocal -k -m 512
```

The example shows generating a global (512-bit) key.

Use the `-m` followed by the modulus size in bits of the encryption for which you want to create a new certificate, if you have installed more than one encryption strength. The modulus sizes are:

- Global (512 bits)
- Export Controlled (1024 bits)
- U.S. and Canada Only (2048 bits)

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.

After you press the Return key, you see the continuation of the message 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:  
f52aff3ce1b1294018118d7c84a70a72d686c40319c807297aca950cd9969fab  
d00a509b0246d3083d66a45d419f9c7cbd894b221926baaba25ec355e92a055f  
public key:  
9945eb0a204efd9643a3aeb42f80d18a22a194232ef6e18809b4b80ac6227100  
0b24fbd0a01608a6b3fe92a3ab107efd1970c398cdc2d0f73effea55clcb0565  
Added local identity slot 12
```

3. Type the following to restart the SKIP key manager to update the certificate database:

```
# skipd_restart
```

4. 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.

Do the following to enter the certificate ID:

- a. Run the command `skiplocal list` 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.

■ For remote administration:

1. Type the following to create a self-generated Screen certificate, for example:

```
# ssadm -r sunscreen1 lib/skiplocal keygen -k -m 512 -f
```

Note – You must use the `-f` flag with remote administration. This flag suppresses the prompt to type random keys on the keyboard.

The example shows generating a global (512 bit) key.

Use the `-m` flag followed by the modulus size in bits of the encryption for which you want to create a new certificate, if you have installed more than one encryption strength. The modulus sizes are:

- Global (512 bits)
- Export Controlled (1024 bits)
- U.S. and Canada Only (2048 bits)

You see the following message on the screen:

```
generating local secret with 512 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:
f52aff3ce1b1294018118d7c84a70a72d686c40319c807297aca950cd9969fab
d00a509b0246d3083d66a45d419f9c7cbd894b221926baaba25ec355e92a055f
public key:
9945eb0a204efd9643a3aeb42f80d18a22a194232ef6e18809b4b80ac6227100
0b24fbd0a01608a6b3fe92a3ab107efd1970c398cdc2d0f73effea55c1cb0565
Added local identity slot 12
```

2. Type the following to restart the SKIP key manager to update the certificate database:

```
# ssadm -r sunscreen1 lib/skipd_restart
```

3. After entering the editor (remote login), 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.

- Do the following to enter the certificate ID:
 - a. Run the `skiplocal list` 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 “Policy Rules.” Tunnelling is also described in the *SunScreen EFS 3.0 Reference Manual*.

▼ To Add Other Certificates from a Diskette or a File

Presently, you can only do this 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 certificate 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. **Type the following in the terminal window to eject the diskette, if you are using issued certificates:**

```
# 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; A00050B is the certificate ID, and SUNSCREEN is the type of certificate.

Each type of 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 NSID0 convention with the IP address as the certificate ID.
- Issued certificates use the NSID1 convention with a certificate ID of 8 hexadecimal digits (32 bit).
- Diffie-Hellman certificates use the NSID8 convention with an certificate ID of 32 hexadecimal digits (128 bit).

NSIDs and certificate IDs are described in the *SunScreen EFS 3.0 Reference Manual*.

Note – The tunnelling address is specified as an option in the rule that uses the key, or in the remote administration rule.

▼ 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:

```
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

- Type the following 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

- Type the following to remove a new member to a certificate group, for example:

```
edit> del_member certificate sales-list sales-wy
```

▼ To Rename a Certificate or Certificate Group

Note – To make any troubleshooting easier, do not rename the certificates that were created when you installed a remotely administered SunScreen EFS 3.0.

When you rename a certificate group using this command, SunScreen EFS 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, like administrative rules and policy rules.

- **Type the following to rename a certificate or certificate group, for example:**

```
edit> renamereference certificate sales-ny sales-northeast
```

▼ To Delete a Certificate or Certificate Group

Note – To make any troubleshooting easier, do not delete the certificates that were created when you installed a remotely administered SunScreen EFS 3.0.

This command does not check for any references to the certificate or certificate group that you are deleting and, then, delete them.

- **Type the following to delete a certificate or certificate group, for example:**

```
edit> del certificate sales-la
```

▼ To Check References to a Deleted Certificate

If you want to check references to the certificate that you want to delete or have deleted,

- **Type the following 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
```

You see a list of all the instances in the certificate database where the certificate is used. You, then, 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.

▼ To Check References to a Deleted Certificate Group

If you want to check references to the certificate group that you want to delete or have deleted,

- **Type the following 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
```

You see a list of all the instances in the certificate database where the certificate group is used. You, then, 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.

Screens

The Screen object controls much of the identity of SunScreen EFS 3.0. It contains information for your stealth, HA, cluster, and administrative rules. Upon installation, a Screen object is created, which you can edit. As with other common objects you can edit, you must specify all the options that you want to set; otherwise the options are set to off, the default.

▼ To Add a Screen

To add a screen object with a previously- created certificate, using DNS and NIS for Name Service, pass routing information, and a comment, type the following:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin  
ROUTING DNS NIS COMMENT "The screen that protects the sales office"
```

▼ To List the Screens

- Type the following to list all the Screens:

```
edit> list screen
"sphere" ADMIN_CERTIFICATE "sphere.admin" CDP ROUTING DNS COMMENT
"This is the data center screen"
```

▼ To Add an SNMP Receiver to a Screen

- To add an SNMP receiver to the previous Screen:

```
edit> add screen sphere ADMIN_CERTIFICATE sphere.admin ROUTING DNS
NIS SNMP 10.100.253.200
```

▼ To Add Multiple SNMP Receivers to a Screen

- To add multiple SNMP receiver 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 Remove SNMP Receivers From a Screen

- To remove SNMP receivers from the Screen, do not include it in the Screen object when you set it:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin
ROUTING DNS NIS
```


▼ To Set Logsize on a Screen

1. The Screen object allows you to set the maximum size of your log file. The value is in Mb, where 200 is 200 Mb.
- At the command line prompt, type:

```
edit> add screen sphere ADMIN_CERTIFICATE sphere.admin CDP ROUTING  
DNS SNMP 10.100.253.200 LOGSIZE 200
```

▼ To Set a Screen to Stealth Mode

- Type the following:

```
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin  
ROUTING SPF 10.100.253.0 255.255.255.0 COMMENT "The screen in  
Stealth Mode"
```

Interfaces

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 qe0 with no logging, no SNMP alerts, and ICMP_PORT_UNREACHABLE:

```
edit> add interface qe0 EFS qe0 ICMP PORT_UNREACHABLE
```

▼ To Add Interfaces (in Routing Mode) with a Detailed Log

- Type the following:

```
edit> add interface qe0 EFS qe0 LOG DETAIL SNMP ICMP  
PORT_UNREACHABLE
```

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

Authorized Users

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

To Add An Authorized User with Password Authentication

- Type the following to add an authorized user:
 - For local administration:

```
edit> add authuser admin1 PASSWORD={ "foo" }  
CONTACT_INFO=br@nncc REAL_NAME="Ben Ruhmduhm"  
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, for example, the description: This user, "test_user" is for 'testing' only.

All changes apply immediately.

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

- Type the following to add an authorized user:

- For local administration:

```
edit> add authuser admin1 SECURID={ "C2BR" }  
CONTACT_INFO=br@nncc  
REAL_NAME="Ben Ruhmduhm"  
DESCRIPTION="created for remote administration"
```

- For remote administration:

```
edit> add authuser admin1 SECURID={ "C2BR" }  
CONTACT_INFO=br@nncc  
DESCRIPTION="created for remote administration"
```

Enabled is the default.

All changes apply immediately.

For the changes to take effect in policy and administrative access rules, you must activate the policy.

To Modify Authorized Users

- Type the following to modify the information for a user, for example to change the SecurID name from C3BR to C4BR:

```
edit> add authuser admin1 SECURID={ "C4BR" } CONTACT  
INFO=br@nncc REAL_NAME="Ben Ruhmduhm" 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

- Type the following to delete an authorized user, for example:

```
edit> authuser delete admin1
```

All changes apply immediately.

Policy Rules

Defining New Rules

Note – 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

- Type the following to add a new rule at the end of a policy with the following attributes:
 - ping as the service
 - * as the Source Address
 - * as the Destination Address
 - SKIP Version 2 as the encryption with Encryption Details:
 - From Encryptor is cert-1
 - To Encryptor 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.)
- ALLOW as the Action and Action Details:
 - NONE for the compression (This is the only possible value, at present.)

```
edit> add Rule ping * * ALLOW SKIP_VERSION_2 cert-1 cert-2 DES-CBC
RC2-40 MD5 NONE LOG SUMMARY
```

Note – All other options assume default values unless specified (for example, SNMP is off).

- Type the following to add a new rule at a particular position, for example, 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
```

▼ To Reorder the Rules

1. Type the following 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. Type the following to move a policy rule to a new position.:

```
edit> move rule 4 5
```

▼ To Delete a Rule

1. Type the following to display the ordered list the rules in a policy, for Type the following to delete the policy rule 5:

```
edit> del rule 5
```

2. Type the following to list the edited ordered list of policy rules:

```
edit> list rule
```

The new 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 "daytime" "localhost" "*" ALLOW
5 "telnet" "*" "*" ALLOW
6 "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. Type the following to 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-proxy" "*" "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. Type the following to change the action of policy rule 5 from ALLOW to DENY by inserting a new policy rule with the action changed.:

```
edit> replace rule 5 telnet * * DENY LOG DETAIL
```

3. Type the following to remove the policy rule with the old action.
 - For local administration:

```
edit> del rule 5
```

4. Type the following to list the rules for the policy, for example.:

```
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-proxy" "*" "localhost" USER "admin" ALLOW LOG DETAIL
  PROXY_FTP FTP_GET FTP_CHDIR FTP_RENAME FTP_DELETE
4 "daytime" "localhost" "*" ALLOW
5 "telnet" "*" "*" DENY
6 "echo" "localhost" "*" ALLOW
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To Add an Access Rule for GUI Local Administration

- Type the following to add an administrative access rule for local administration:

```
edit> add accesslocal USER admin3 PERMISSION ALL
```

▼ To Edit an Access Rule for GUI Local Administration

1. Type the following to 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. Type the following 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



Caution – Do not delete all the administrative access rules.

- Type the following to delete the administrative access rule for local administration:

```
edit> del AccessLocal 2
```

Where 2 is the number, in the ordered rules, that you want to delete.

▼ To Add an Access Rule for Remote Administration

- **Type the following 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.

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

Make a note of the encryption parameters if you change them because they have to match the encryption parameters on the remote Administration Station.

1. **Type the following to 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
```

2. **Type the following 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



Caution – Do not delete all the administrative access rules.

- **Type the following 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



Caution – When using NAT, be sure that:

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

▼ To Add ARP Manually

- **Type the following 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 that you reboot the Screen or you can write your own script to automate this function. If you are remotely administering the Screen, you either must go to the Screen to add this entry or have a rule in your policy that will allow you to `rlogin` to the Screen.

▼ To Define NAT Mappings

1. Type the following command to create a *static* NAT entry that maps a internal address to an external address.

- For local administration:

```
edit> add nat STATIC src dest translated src translated dest
```

In most cases when defining a static mapping, the internal address and external address are each a single address, but can be a range or a list.

2. Repeat for every mapping that you want.

Use the same command to map for *dynamic* NAT. Use DYNAMIC instead of STATIC as the type of NAT entry desired.

You may also use a range of addresses or a group of addresses.

To have the changes take effect, you must activate the policy whose rules you edited

▼ To Delete NAT Mappings

1. Type the following command to delete a NAT entry that maps internal address to an external address, regardless of whether mapping is static or dynamic:

```
edit> del nat 1
```

To have the changes take effect, you must activate the policy whose rules you edited.

▼ To List the NAT Mappings

- Type the following command 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 define the address groups involved. For descriptions and concepts of the Virtual Private network, the *SunScreen EFS 3.0 Reference Manual*.

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 network
- addrgrp-a is an address group that uses the following certificate

SKIP cert-a is the certificate

- If you are using a tunnel, append **TUNNEL** address name to the add/replace.

To setup the VPN completely, you should have all the keys, address groups, and vpngateways on each screen. So 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 containing the address groups for both networks, for example:

```
edit> add address vpn-grp GROUP { addrgrp-a addrgrp-b } {}
```

3. Define a rule specifying the VPN Gateway:

```
edit> add rule common vpn-grp vpn-grp ALLOW VPN vpn-net
```

▼ To Replace a VPN Gateway

- VPN Gateway are setup 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 setup you need to delete the rules and the VPN object. 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

1. Type the following to display information, such as Product, System Boot Time, SunScreen Boot Time, and Version:

- For local administration:

```
# ssadm sys_info
```

- For remote administration:

```
# ssadm -r machinename sys_info
```

▼ To View the Statistics

- Type the following to display the statistics about the traffic flowing through the Screen:

- For local administration:

```
# ssadm traffic_stats
```

- For remote administration:

```
# ssadm -r machinename traffic_stats
```

All changes apply immediately.

▼ To Set Up Packet Logging

SunScreen EFS provides flexible logging of packets. A packet can be logged when it matches a policy rule, when does not match a policy rule, or when it matches a policy rule whose action is DENY.

- 1. Configure SunScreen EFS 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 that you want in the details for the ALLOW action in a policy rule and the type of ICMP reject in the details for DENY action.**
- 3. Set logging for packets that are dropped because they do not match any policy rule on the Interfaces panel of the Interface page.**

Examining Packets

Once a log is retrieved, it can be examined using the `ssadm logdump` command.

Examining logged packets can be a very useful for troubleshooting problems in setting up security policies. For example, when first creating policies, make the default DENY action “log packets.” This way, you can review the logs easily. You can also use logging to capture any attempts to break in.

▼ To Use `ssadm logdump` Command

You can only examine a saved log file from the command line.

- **Type the following to display packets in the log file:**

```
# ssadm logdump < 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 log:
 - For local administration:

```
# ssadm log get | ssadm logdump -i -
```

▼ To Save the Log

- Type the following to save a log record to a file:
 - For local administration:

```
# ssadm log get > filename
```

- For remote administration:

```
# ssadm -r machinename 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 EFS 3.0 log file.

- Type the following to clear the log file:
 - For local administration:

```
# ssadm log clear
```

- For remote administration:

```
# ssadm -r machinename log clear
```


▼ To Save and Clear the Log

This action saves a log to a file and clears the display of any log records.

- **Type the following to save the log-record to a file and clear the log-file:**
 - For local administration:

```
# ssadm log get_and_clear > filename
```

- For remote administration:

```
# ssadm -r machinename log get_and_clear > filename
```

Setting Up High Availability (HA)

See Chapter 6, “High Availability,” and the *SunScreen EFS 3.0 Reference Manual* before using the command line to set up HA.

- **To install HA on the Screen designated to be the Primary HA Screen (thereby creating a new HA cluster containing one Screen), type the following:**

```
# ssadm init_primary interface
```

- **To install HA on the Screen designated to be the Secondary HA Screen type the following:**

```
# ssadm 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.

- 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, you must direct the Secondary Screen to become passive in order to communicate with the Primary Screen.

▼ To Remove an HA Host

An HA setup is installed by using commands outside the configuration editor. Removing the HA setup would consist of removing the HA_* options from the Screen objects on the machines. For example, a list of the HA setup would be:

```
edit> list screen
"vorticity" MASTER "barotropic" CDP ROUTING 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

edit> del screen vorticity
edit> add screen barotropic ADMIN_CERTIFICATE barotropic.admin CDP
DNS NIS
```

- Save and activate your configuration.

▼ To View HA Information

- Type the following to display information, such as the current Active or Passive status of the local HA machine and the current state of the HA daemon.

- For local administration:

```
# ssadm ha status
```

- For remote administration:

```
# ssadm -r machinename ha status
```

Centralized Management Group

▼ Change a Screen Object to be in a Cluster

Use the following commands to set up a Cluster. Centralized Management Groups are explained in Chapter 6 and in the *SunScreen EFS 3.0 Reference Manual*.

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
ROUTING NIS LOGSIZE 100
edit> add screen velocity ADMIN_IP 10.100.105.5 ADMIN_CERTIFICATE
vorticity.admin KEY"DES-CBC" DATA "RC4-40" MAC "MD5" COMPRESSION
"NONE" MASTER sphere CDP DNS NIS
```

▼ To Remove a Screen Object from a Cluster

1. Type the following on the Primary Screen ("sphere" in this example):

```
edit> del screen vorticity
```

2. Type the following on the Secondary (“vorticity” in this example):

```
edit> del screen sphere
edit> add screen vorticity ADMIN_CERTIFICATE vorticity.admin CDP
ROUTING DNS
```

Gathering Information From Your System to Report to SunService

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>.

Collect this information by saving the output of the following SunScreen EFS 3.0 support commands, as shown in Table A-1.

TABLE A-1 Table of Support Commands

Command	Description
config	Brings over configuration files for the active configuration
date	Sets and gets current time/date. (See the caution below!)
disks	Checks disk space (df -k)
eeprom	Checks EEPROM settings.
findcore	Checks for a core file.
last	Checks boot history.
packages	Checks pkginfo and patch history.
procs	Checks processes (ps -elf)
skip	Checks contents of /etc/skip/ directory.
statetables	Displays internal protocol state tables.

TABLE A-1 Table of Support Commands

Command	Description
stats	Checks the kernel networking statistics (netstat -k)
streams	Checks the STREAMS statistic (netstat -m).
versions	Brings over version information on major SunScreen components.

The commands are used for remote diagnostics and are sent from a remote Administration Station. Type the following to start these support commands:

```
# ssadm -r Name_of_the_Screen lib/support Command
```

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.

▼ Using the ssadm lib/statetables Command

- To gather data for a Screen, type:

```
# ssadm lib/statetables
```

▼ Using the ssadm lib/screeninfo Command

Use this command to gather a complete set of data for your Sun Service representative, including:

- Statetables
- ARP table information
- Disk usage
- Streams information
- SunScreen configuration information and files
- Uptime
- SKIP information

- At the command line prompt, type:

```
# ssadm lib/screeninfo
```

▼ Using the `ssadm lib/support` Command

This command gives you access to the commands in the support directory. All the commands in the support directory are invoked by the `screeninfo` command, yet it may be advantageous to run this command alone if you are seeking limited data.

- At the command line prompt, type:

```
# ssadm lib/support subcommand parameters
```

▼ To Use the Help Option

- At the command line prompt, type:

```
# ssadm lib/support help
```

Troubleshooting

You can use the `ssadm debug_level` command to control the printing of debugging information from the SunScreen EFS 3.0 kernel.

▼ To Use the `ssadm debug_level` Command

If you type it with no arguments, `ssadm debug_level` displays the current debug-level mask. By default, this mask is “1,” which means it only reports significant errors.

If you specify a hexadecimal number as an argument for `ssadm debug_level`, it sets the kernel debugging mask to that level.

- **Type the following to list the debugging bit choices:**

```
# ssadm debug_level -h
```

- **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`.

Index

A

access

- local system resources 22

- access level 26, 79

- access-control software 2

ACE

- see also

- SecurID 4

- activate 39

- Add Filter button 47

- address 5, 10, 18, 37

- add 51

- add range 52

- admin 39

- defining 51

- deleting 43

- destination 4, 8, 51, 55, 81, 87

- example 9

- external 84

- group 9, 53

- host 9

- individual 8, 10, 51

- IP 6, 8, 10, 13, 51, 52, 63, 64, 65, 81, 101, 106

- map 4

- network 8, 10, 51, 155

- pre-defined 51

- range 8, 9, 52

- registered 13

- remove 39, 54

- replace 4

- source 4, 8, 51, 55, 81, 87

- tunnel 91

- unregistered 13

- address group 10, 39, 53

- address list 51

- defining 53

- deleting 43

- address range 52

- defining 52

- deleting 43

- addresses 8

- admin certificate 39

- Admin User 5

- admin-group certificate 39

- administration

- HA 20

- local 1, 75, 195–196

- remote 1, 55, 75, 77, 81, 84, 137

- administration GUI 4, 5, 18, 55, 106, 117, 156

- Administration Station 1, 3, 39, 155, 157

- adding an additional 77, 137

- remote 63, 80, 161

- administrative access rule 5, 81

- algorithm

- Data 17, 79, 80, 91

- Key 17, 79, 80, 91

- MAC 17, 91

- applet

- Java-enabled 3

- ARP 107

- ARP request 84, 108

- authentication 2, 3, 190

- RADIUS 4

- user 4
- authorized user 5, 37, 190–192
 - add 119

B

- banner 96
- bridge 2
- broadcast 49
- Broadcast button 49
- browser 3, 4, 5, 19, 23
 - configure for HTTP proxy 116
 - differences among 5
 - HotJava 20
 - HotJava 1.1 5
 - Internet Explorer 5
 - log 100
 - Netscape 5
 - starting 19–20

C

- Centralized Management 84
- centralized management group 3
- certificate 5, 37, 80
 - adding 55
 - admin 39
 - admin group 39
 - associating IDs 59
 - deleting 187
 - loading from diskette 20
 - renaming 186
 - signed 55
 - Unsigned Diffie-Hellman 179
- Certificate Authority (CA) 55
- Certificate Discovery Protocol (CDP) 56
- certificate group 60, 79, 187
- Certificate ID 91, 140
- command line 4, 155
- common object 4, 5
 - delete 43
 - rename 44
- configuration
 - creating 18–??
 - editing 27–195
- configuration editor 168

D

- data algorithm 79
- Data Algorithm list 17
- date 96
- destination address 51
- DNS 107
- documentation xxiv
- dynamic NAT 199

E

- editing 26
- editor
 - configuration 168
- element
 - define 6
 - see also
 - network element 8
- e-mail 6
- encrypted tunnel 3
- encryption 2, 3, 4, 10, 39, 55, 63, 80, 81, 105, 155
 - choosing 77, 181
 - modulus size 181
 - see also SKIP
 - using 55
- /etc/hosts file 107

F

- features
 - SunScreen 3
- file
 - identitydb.obj 21, 156, 157
 - log 4, 20, 103
 - Solaris 107
- filter
 - add 47
 - delete 47
 - log messages 4
 - packet 3
 - parameters 49
- filtering
 - content 4
 - packet 3, 5, 105
 - proxy dialog 5
- firewall 1, 3, 140

FTP 6

G

gateway 17

group

- address 9, 10

- service 6, 16

GUI 4, 5, 18, 55, 77, 106, 117, 156

- interoperability with command line 4, 155

H

HA 3, 20

- administration 20

- and NAT 107

- cluster 3

- defining 112-??

- definition 106

- installing 108-111

- remove 107

- removing 114

- Screen 3

- set up 105

- viewing current information about 96

hard disk space 3

hash 55, 56

- Jar 5, 37

help

- documentation xxiv

host 4, 6, 13, 46

- address 9

- HA 20, 106

- IP 8, 51

HotJava 117

HotJava 1.1 5

HTTP 5

I

identity

- local 55

Information button 96

Information page 96

installation 39

interface 2, 5, 20, 39, 65, 97, ??-115

- activate 65

- define 8, 51

- HA 105

- HA cluster 106

- statistics 97

interface port 5

Internet 13

- example 9

Internet Explorer 5, 20, 55, 102, 117

IP address 6, 8, 10, 13, 51, 52

IP host 51

issued public key 55

J

Jar

- hash 5, 117, 136

- signature 5, 136
20

Jar hash 5, 37

Jar signature 37

Java

- Jar hash 5

- Jar signature 5

Java Developers Kit 5

Java Plug-in 2, 3, 20, 21, 102, 155, 156

Java Plug-In software 2

Java plug-in software 20

Java Runtime Environment 3, 5, 117

- see also

- JRE 3

JDK 5, 117

JRE 5

- see also

- Java Runtime Environment 3

K

key 56

- public 55

- secret 105

- SunScreen 55

Key algorithm 17, 79

L

list

- Key algorithm 17
- local administration 1
- local certificate 39
- local identity 55
- localhost 20
- lock, GUI 25-??
- Log
 - set viewing filter 100
- log
 - clear 103
 - file 4, 20
 - filtering 4
 - save 102
 - save and clear file 104
 - view 96
- log out 26
- logging 3
- Login button 24

M

- management information base (MIB) 63
- master key identity (MKID) 179
- MD5 17
- MKID 140
- mode
 - historical 4, 99
 - log retrieval 98
 - real time 4, 99
 - routing 1, 3, 84
 - single-user 2
 - stealth 2, 3, 84

N

- name service 107
- name space ID (NSID) 179
- NAT 5, 13, 51, 81, 82, 105, 107, ??-200
 - edit mapping 87
 - mapping 86, 107
 - reverse rule 87
 - see also
 - Network Address Translation 4
- NAT Mapping 13
 - dynamic 82
- NAT mapping

- static 82
- NAT rule
 - define 82
- Netscape 5, 20, 55, 102, 117, 155
- network 5, 6, 8, 10, 16, 18, 52, 84, 106
 - access 18
 - Class B 13
 - Class C 13
 - internal 46
 - public 4
- Network Address Translation 5, 51, 81
 - see also
 - NAT 4
- network element 5, 6, 8, 10
- network interface 51, 65
- network protocol 5
- NIS 107

P

- packet 3, 4, 13
 - broadcast 49
 - filtering 5
 - IP 81
 - non-broadcast 49
 - SNMP 63
- packet filtering 3
- password 4, 23, 24, 37, 39, 155, 190
 - changing 39
- patch 2
 - apply 2
 - required 2
 - Solaris 2.6 2
 - x86 2
- Patches 2
- path 19
- Pentium 3
- Plug-in
 - install 21
- policy 18, 38, 46, 51
 - activate 39, 65, 153
 - back up 20
 - define 6
 - definition 4
 - restore 20
 - revert 37
 - save 37

verify 37
Policy Edit page 39

port
add 48
delete 48
interface 5

protocol 46
network 5

proxy
databases 117
FTP 130
HTTP 135
routing mode 3
set up 115
SMTP 134
TELNET 133
use 115
user 37
user authentication 4
user, add 121

proxy user 5
public key 55

R

RADIUS 4

RAM 3

range
address 8, 9

Registry
addresses, address ranges, address lists 175–177
authorized users 190–192
certificates ??–187
services and service groups ??–175

remote administration 1

Rename... button 44

revert 37

rip 49

rip service 49

rlogin command 179, 199

routing 84, 108

routing firewall 1

routing mode 1, 3
proxies 3

Rule

access control 10

rule 3, 16, 18, 51

activate 65

Administrative Access 5

define 6

deleting ??–194

policy 5

see also action; address; administrative access
rule; configuration; encryption; service; user
time-based 4
time-dependent 5

S

Screen 1, 2, 4, 5, 20, 37, 39, 50, 54, 55, 63, 84, 99, 133, 155

active 3

adding certificate 55

administer 38

connecting to 20

HA 3

HA active 105

HA cluster 106

HA passive 105

in centralized management group 3

individual 3

local administration 20

logging in to 23

multiple 3

passive 3

primary 3, 140

remote 4

remote administration 20

secondary 140

Search button 43

SecurID 190, 191

see also

ACE 4

self-generated certificate 55

service 5, 18, 107

add 46

checking references to 174

default values 46

group 6

network 6

pre-defined 6

predefined 46

rip 49

service group 16

- add 49
- checking references to 174
- creating 6
- defining ??-173
- predefined 46
- session 23
- signature
 - Jar 5, 37
- SKIP 2, 3, 4, 5, 80, 97, 140, 155
 - and NAT 81
 - key manager 179, 180, 182, 183
 - statistics 97
 - version 79
- SNMP alert receiver 37, 63, 64
 - add 63
- Solaris 2.5 3
- Solaris 2.6 2
- source address 8, 51
- space
 - hard disk 3
- Spam 37, 123, 134
 - delete 124
- state engine 46
- static mapping
 - define 87
- static NAT 85, 86, 198, 199
- statistics 96, ??-202
 - interface 97
- Status page 96
- stealth firewall 1
- stealth mode 3
- subnetwork 6, 8, 10, 52
- Sun SPARC 3
- SunScreen banner 96
- SunScreen Key 55
- superuser 155
- system information 202

T

- time 5, 96
 - define 44
 - example of time object 45
- traffic statistics 97
- tunnel 3, 81

- tunnel address 79

U

- Unsigned Diffie-Hellman certificate, *see* certificate, Unsigned Diffie-Hellman
- user
 - admin 24, 39
 - authorized 5, 37, 39, 119, 121, 190-192
 - proxy 5, 37, 119
- user authentication 4
- user name 23

V

- version 4, 96
 - number 4
- Virtual Private Network 3, 4, 5, 17, 81
 - see also*
 - VPN 3
- virtual private network 3
- VPN 3, 4, 5, 17, 180
 - add gateway 91
 - define 92

W

- Windows 95 2, 21
- Windows 98 2, 21
- Windows NT 2, 21
- Worksheets 6
- WWW 6

X

- x86 2, 3